Ανώτατο Τεχνολογικό Εκπαιδευτικό Ίδρυμα Μεσολογγίου
Παράρτημα Ναυπάκτου
Τμήμα Τηλεπικοινωνιακών Συστημάτων και Δικτύων

Πτυχιακή εργασία

Υλοποίηση VoIP σε μικρομεσαίες επιχειρήσεις.

Παναγιώτης Μαρκουλιδάκης

Επιβλέπων: Γεωργουδάκης Μάνος

Ναύπακτος, Απρίλιος 2013

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Ναύπακτος, Τρίτη 30 Απριλίου 2013

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

Γεωργουδάκης Μάνος,

Αλεφραγκής Παναγιώτης,

Βώρος Νικόλαος,

Την πτυχιακή εργασία μου την αφιερώνω στου γονείς μου Κώστα και Λιάνα για την υποστήριξη τους όλα αυτά τα χρόνια, στην Ειρήνη, τον Δημήτρη και τον Πάνο που με βοήθησαν να φτάσω ως εδώ και στον υπεύθυνο καθηγητή μου Γεωργουδάκη Μάνο για όλη την βοήθεια που προσέφερε…

Πίνακας περιεχομένων

Ευρετήριο Πινάκων

Ευρετήριο Εικόνων

Κεφάλαιο 1

Εισαγωγή

1 Εισαγωγή

1.1 Ιστορία των τηλεπικοινωνιών

Ένας από τους κυριότερους κλάδους της πληροφορικής και του σημερινού «κόσμου» είναι οι τηλεπικοινωνίες. Ήχος, εικόνα, δεδομένα διαδίδονται καθημερινά με την χρήση των τηλεπικοινωνιακών δικτύων. Η πρώτη μορφή τηλεπικοινωνίας χρονολογείται κατά την περίοδο του Τρωικού πολέμου. Οι Αχαιοί χρησιμοποίησαν τις Φρυκτωρίες για να αναγγείλουν την πτώση της Τροίας . Από τότε μέχρι σήμερα οι τηλεπικοινωνίες έχουν εξελιχθεί και από την χρήση της φωτιάς έχουμε μεταβεί στην χρήση μικροκυματικών, οπτικών και ηλεκτρικών ζεύξεων. Μια σημαντική εξέλιξη στην ιστορία των τηλεπικοινωνιών ήταν η εφεύρεση του τηλεφώνου.

Το τηλέφωνο είναι ένα όργανο επικοινωνίας που έχει ως σκοπό να μεταδώσει την ομιλία και άλλους ήχους από ένα σημείο Α σε ένα απόμακρο σημείο Β και να τους αναπαράγει με τη βοήθεια της ηλεκτρικής ενέργειας. Το τηλέφωνο περιέχει ένα εξάρτημα, το διάφραγμα, το οποίο ταλαντώνεται όταν διεγείρεται από τα ηχητικά κύματα. Η ταλάντωση των προσπιπτόντων κυμάτων μετατρέπεται σε ηλεκτρική ώθηση και διαβιβάζεται σε έναν δέκτη, ο οποίος την μετατρέπει σε ήχο. Το τηλέφωνο έχει αποδειχθεί ως μία από τις σημαντικότερες για τον άνθρωπο ανακαλύψεις, καθώς συνέβαλε στην ταχύτερη εξέλιξη της τεχνολογίας και άλλαξε τον τρόπο ζωής του ανθρώπου.

1.1.1 Οι πρόδρομοι του τηλεφώνου

Είναι κοινώς αποδεκτό ότι οι τηλεπικοινωνίες έχουν γίνει αναπόσπαστο κομμάτι της καθημερινότητας του ανθρώπου και επηρεάζουν με την λειτουργία τους -ή όχι- τον εμπορικό και βιομηχανικό τομέα και γενικότερα τις καθημερινές ζωές μας. Σε αυτό συμβάλουν κυρίως οι τεχνολογικές εξελίξεις που έχουν σημειωθεί τις τελευταίες δεκαετίες. Μέσα σε αυτές βρίσκονται το τηλέφωνο, η τηλεόραση και ο ηλεκτρονικός υπολογιστής ˙ συσκευές που επιτρέπουν την πληροφόρηση και την ανταλλαγή δεδομένων μέσα σε ελάχιστο χρονικό διάστημα ανεξάρτητα από την απόσταση. Παρ' όλα αυτά, η ανάγκη του ανθρώπου για επικοινωνία προϋπήρχε των εφευρέσεων αυτών. Από τα προϊστορικά χρόνια μέχρι και τον Μεσαίωνα υπήρχαν δύο βασικά είδη τηλεπικοινωνιών: η οπτική τηλεπικοινωνία και η ακουστική. Η οπτική τηλεπικοινωνία ξεκίνησε από τη στιγμή που ανακαλύφθηκε η φωτιά. Οι άνθρωποι επινόησαν διάφορους κώδικες και με τη βοήθεια σημάτων καπνού, πυρσών ή ακόμα και πολύχρωμων σημαιών (μεταγενέστερα) μπορούσαν να επικοινωνούν από μακρινές αποστάσεις. Η αρχαιότερη, όμως, μορφή τηλεπικοινωνίας είναι η ηχητική. Πρώτος την

χρησιμοποίησε ο προϊστορικός άνθρωπος και περιοριζόταν σε ηχητικά σήματα που προέρχονταν από διάφορα είδη τυμπάνων. Στη συνέχεια αυτά αντικαταστάθηκαν με διάφορα άλλα όργανα (κόρνες, τρομπέτες) και χρησιμοποιούνταν ευρέως για στρατιωτικούς σκοπούς μέχρι την εμφάνιση πιο αποτελεσματικών μέσων. Στα πλαίσια των παραπάνω τάσεων αρκετές εφευρέσεις παρουσιάζουν ιδιαίτερο ενδιαφέρον. Οι πιο χαρακτηριστικές από αυτές είναι εκείνες των αρχαίων Ελλήνων. Οι αρχαίοι Έλληνες είχαν καταφέρει να αναπτύξουν ένα πρωτότυπο σύστημα τηλεπικοινωνιών που βασιζόταν τόσο στο οπτικό όσο και στο ηχητικό τηλεπικοινωνιακό πρότυπο. Εφευρέσεις όπως το ακουστικό κέρας, ο οπτικός τηλέγραφος (ή πυρσεία), ο υδραυλικός τηλέγραφος και το σύστημα των φρυκτωριών έπαιξαν σημαντικό ρόλο στην εξέλιξη των τηλεπικοινωνιών. Πολλοί, λοιπόν, ήταν εκείνοι που στα ύστερα χρόνια τις βελτίωσαν ή έκαναν εφευρέσεις βασισμένες πάνω σε αυτές. Αρκετά χρόνια αργότερα, με την βιομηχανική επανάσταση η ανάγκη για ένα γρήγορο και αξιόπιστο μέσο επικοινωνίας είχε γίνει πλέον επιτακτική. Έτσι δεν άργησε να εμφανιστεί ο σπουδαιότερος πρόδρομος του τηλεφώνου, ο τηλέγραφος. Η ιδέα του τηλεγράφου αν και προέρχεται, όπως είδαμε προηγουμένως, από τα αρχαία χρόνια υλοποιήθηκε το 1774 από τον Ελβετό George Luis που κατασκεύασε μια πρώιμη μορφή τηλεγράφου. Αργότερα εμφανίστηκαν οι τηλέγραφοι του Semmering (1810), του Ampere και των Cooke και Wheaton. Ο Αμερικανός, όμως, Samuel Morse (1791-1872) το 1837 παρουσίασε τον τηλέγραφό του, που είχε την δυνατότητα να μεταδίδει μηνύματα σε πολύ μακρινές αποστάσεις γρήγορα και χωρίς μεγάλο κόστος. Το πρώτο μήνυμα από αυτόν τον τηλέγραφο στάλθηκε το 1844 από την Ουάσιγκτον στην Βαλτιμόρη. Καθώς, λοιπόν, οι παραπάνω εφευρέσεις τελειοποιήθηκαν και οι δυνατότητές τους χρησιμοποιήθηκαν στο έπακρο δημιουργήθηκε η ανάγκη κατασκευής μιας συσκευής που θα μπορούσε να μεταφέρει ήχους και πάνω από όλα την ανθρώπινη ομιλία.

1.2 Το Τηλέφωνο

Ο Alexander Graham Bell γεννήθηκε στις 3 Μαρτίου του 1847, στο Εδιμβούργο της Σκωτίας. Σπούδασε στα πανεπιστήμια του Εδιμβούργου και του Λονδίνου και μετακινήθηκε στον Καναδά το 1870 ενώ το 1871 στις Ηνωμένες Πολιτείες όπου άρχισε να διδάσκει σε κωφάλαλους το σύστημα ορατής (οπτικής) ομιλίας. Το σύστημα αυτό που αναπτύχθηκε από το πατέρα του, Alexander Melville Bell, δείχνει πώς τα χείλη, η γλώσσα, και ο λαιμός χρησιμοποιούνται στην άρθρωση του λόγου. Το 1872 το Bell ίδρυσε ένα σχολείο για τους κωφαλάλους στη Βοστόνη της Μασαχουσέτης. Το σχολείο έγινε στη συνέχεια μέρος του πανεπιστημίου της Βοστόνης, όπου ο Bell διορίστηκε καθηγητής της φωνητικής φυσιολογίας. Έγινε αμερικάνος πολίτης το 1882. Από την ηλικία των 18 ο Bell εργαζόταν πάνω στην ιδέα

της διαβίβασης της ομιλίας. Το 1874, ενώ δούλευε σε ένα είδος τηλεγράφου, ανέπτυξε τις βασικές ιδέες του για το τηλέφωνο. Το καλοκαίρι του 1875 ο Bell κάνοντας πειράματα μαζί με το βοηθό του Thomas Watson παρατήρησε ότι ένα έλασμα από ατσάλι όταν δονείτο από διάφορους ήχους επηρέαζε το ρεύμα ενός ηλεκτρομαγνήτη. Παρατήρησε ακόμη ότι σε κάποιο άλλο σημείο ένας άλλος ηλεκτρομαγνήτης επηρεαζόταν από αυτές τις αλλαγές του ρεύματος και με τη σειρά του έκανε ένα άλλο έλασμα να πάλλεται. Τα πειράματά του αυτά αποδείχθηκαν τελικά επιτυχή στις 10 Μαρτίου του 1876, όταν διαβιβάστηκε η πρώτη πλήρης πρόταση μέσω του τηλεφώνου: "Watson, έλα εδώ, σε θέλω ". Οι επόμενες επιδείξεις, ιδιαίτερα μια το 1876 στη Φιλαδέλφεια της Πενσυλβανία, εισήγαγαν το τηλέφωνο στον κόσμο και οδήγησαν στην οργάνωση της τηλεφωνικής επιχείρησης του Bell το 1877. Άλλοι εφευρέτες προσπάθησαν επίσης να δημιουργήσουν μία συσκευή επικοινωνίας. Ειδικά ο Antonio Meutsi, ο οποίος εφηύρε μια ακουστική συσκευή στις αρχές του 1870 και ο Elisha Gray που υπέβαλε μία αίτηση ευρεσιτεχνίας με τη κατασκευή του τηλεφώνου λίγες ώρες μετά τον Bell στο Σικάγο. Το 1880 η Γαλλία απονέμει στο Bell το βραβείο Volta, το οποίο συνοδευόταν από χρηματικό έπαθλο 50.000 φράγκων, για την εφεύρεσή του. Με αυτά τα χρήματα ίδρυσε το εργαστήριο Volta στην Ουάσιγκτον, όπου τον ίδιο χρόνο οι συνεργάτες του και εκείνος εφηύραν το φωτόφωνο (photophone), το οποίο διαβίβαζε την ομιλία μέσω ακτινών φωτός. Ο Bell ήταν ένας από τους ιδρυτές της National Geographic Society και υπηρέτησε ως πρόεδρός της από το 1896 έως το 1904. Ίδρυσε επίσης το περιοδικό Science το 1883. Μετά από το 1895 τα ενδιαφέροντα του Bell στράφηκαν στην αεροναυτική στα πλαίσια της οποίας μαζί με τους συνεργάτες του δημιούργησε μερικές ενδιαφέρουσες εφευρέσεις. Ο Bell συνέχισε αργότερα τις μελέτες του πάνω στις αιτίες και στην κληρονομικότητα της κώφωσης. Πέθανε στις 2 Αυγούστου του 1922, στο Baddeck του Καναδά όπου σήμερα υπάρχει ένα μουσείο που είναι αφιερωμένο στο έργο και στη ζωή του.

Το μαγνητικό τηλέφωνο του Μπελ και η εξέλιξη του τηλεφώνου

Το 1854 ο Γάλλος εφευρέτης Charles Bourseul σκέφτηκε ότι οι δονήσεις που προκαλούνται από την ομιλία σε έναν εύκαμπτο δίσκο ή ένα διάφραγμα θα μπορούσαν να χρησιμοποιηθούν για να συνδέσουν και να αποσυνδέσουν ένα ηλεκτρικό κύκλωμα, παράγοντας με αυτόν τον τρόπο παρόμοιες δονήσεις σε ένα διάφραγμα που βρίσκεται σε μια άλλη θέση, όπου ο αρχικός ήχος θα αναπαραγόταν. Μερικά έτη αργότερα, ο Γερμανός φυσικός Johann Philip Reis εφηύρε ένα όργανο που διαβίβαζε τους μουσικούς τόνους αλλά που δε μπορούσε να αναπαραγάγει την ομιλία. Μια μορφή ακουστικής συσκευής επικοινωνίας αναπτύχθηκε γύρω

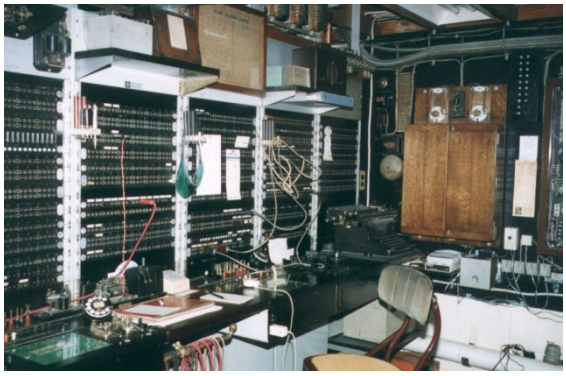
στα 1870 από τον ιταλό-αμερικάνο Antonio Meucci. Το 1876, ανακαλύπτοντας ότι μόνο ένα σταθερό ηλεκτρικό ρεύμα θα μπορούσε να χρησιμοποιηθεί για να διαβιβάσει την ομιλία, ο αμερικανικός εφευρέτης Αλέξανδρος Graham Bell παρήγαγε το πρώτο τηλέφωνο ικανό και την ανθρώπινη ομιλία με την ποιότητα και τη χροιά της. Τη βασική μονάδα της εφεύρεσης του Bell αποτελούσαν μια συσκευή αποστολής σημάτων (πομπός), μια συσκευή λήψης σημάτων (δέκτης) και ένα ενιαίο καλώδιο που τις συνέδεε. Ο πομπός και ο δέκτης ήταν ίδιοι, κάθε ένας περιείχε ένα εύκαμπτο μεταλλικό διάφραγμα και ένα πεταλοειδή μαγνήτη με μια σπείρα καλωδίων. Τα ηχητικά κύματα χτυπούσαν το διάφραγμα αναγκάζοντάς το να δονηθεί στο πεδίο του μαγνήτη. Αυτή η δόνηση παρήγαγε ηλεκτρικό ρεύμα στη σπείρα των καλωδίων. Το ρεύμα ταξίδευε μέσω των καλωδίων σε έναν άλλο δέκτη, ο οποίος μετέφερε τις αλλαγές αυτές στη δύναμη του μαγνητικού πεδίου με αποτέλεσμα να προκαλεί τη δόνηση του διαφράγματος και έχοντας ως σκοπό την αναπαραγωγή του αρχικού ήχου. Στο ακουστικό του σύγχρονου τηλεφώνου ο πεταλοειδής μαγνήτης έχει αντικατασταθεί από έναν επίπεδο μαγνήτη και το μαγνητικό πεδίο που ενεργεί στο διάφραγμα έχει γίνει εντονότερο και ομοιόμορφο. Η σύγχρονη συσκευή αποστολής σημάτων – πομπός αποτελείται ένα λεπτό διάφραγμα που τοποθετείται πίσω από μια διάτρητη σχάρα. Στο κέντρο του διαφράγματος υπάρχει ένας μικρός θόλος που διαμορφώνει μια περίφραξη που περιέχει κόκκους άνθρακα. Τα ηχητικά κύματα που περνούν μέσω της σχάρας αναγκάζουν το θόλο να κινείται μέσα και έξω. Όταν το διάφραγμα πιέζει προς τα μέσα το θόλο, οι κόκκοι συμπυκνώνονται, δημιουργώντας μια αύξηση στη ροή του ρεύματος.

Τα μέρη ενός τηλεφωνικού συνόλου

Ένα βασικό τηλεφωνικό σύνολο περιέχει μια συσκευή αποστολής σημάτων (πομπός – transmitter), έναν δέκτη (receiver), έναν πίνακα με πλήκτρα (dial), έναν κωδωνοκρούστη (ringer) και ένα δίκτυο καλωδίων (antisidetone network). Στα ενιαία τηλεφωνικά σύνολα, η συσκευή αποστολής σημάτων και ο δέκτης τοποθετούνται στο ακουστικό, ο κωδωνοκρούστης είναι χαρακτηριστικά στη βάση και τα πλήκτρα και το δίκτυο καλωδίων μπορεί να είναι είτε στη βάση είτε στο ακουστικό, αλλά βρίσκονται συνήθως και στα δύο. Τα πολυπλοκότερα τηλέφωνα έχουν ένα μικρόφωνο και ένα μεγάφωνο στη βάση εκτός από τη συσκευή αποστολής σημάτων και έναν δέκτη στο μικροτηλέφωνο (τηλεφωνικές συσκευές με δυνατότητα ανοιχτής ακρόασης). Σε ένα ασύρματο τηλέφωνο το καλώδιο του ακουστικού αντικαθίσταται από μια ράδιο σύνδεση μεταξύ του μικροτηλεφώνου και της βάσης, αλλά ένα σκοινί γραμμών (καλώδιο) χρησιμοποιείται ακόμα. Ένα κυψελοειδές τηλέφωνο (cellular phone) περιέχει ένα πομπό και ένα δέκτη εξαιρετικά μικρού μεγέθους. Για τη λειτουργία του δεν απαιτείται κανένα απολύτως καλώδιο, δηλαδή είναι μια φορητή και αυτόνομη συσκευή.

1.3 Τηλεφωνικά Κέντρα

Όταν εμφανίστηκαν τα πρώτα συστήματα τηλεφωνίας, κάθε τηλέφωνο ήταν φυσικά συνδεδεμένο με το τοπικό τηλεφωνικό κέντρο, το οποίο χειριζόταν ένας υπάλληλος. Όταν κάποιος ήθελε να πραγματοποιήσει μια κλήση σήκωνε το ακουστικό για να μιλήσει με το τηλεφωνικό κέντρο. Το κέντρο αντιλαμβανόταν την αλλαγή κατάστασης του κυκλώματος και ένας προειδοποιητικός ήχος (κουδούνισμα) ή μία ενδεικτική λυχνία άναβε, ειδοποιώντας έτσι τον χειριστή του τηλεφωνικού κέντρου ότι κάποιος ήθελε να πραγματοποιήσει κλήση. Ο χειριστής απαντούσε στο αίτημα του καλούντος, ρωτώντας το με ποιόν ήθελε να μιλήσει. Στη συνέχεια, ο χειριστής επικοινωνούσε με τον καλούμενο τον ενημέρωνε ότι κάποιος είναι στη γραμμή και εφόσον αποδεχόταν την κλήση σύνδεε τα δύο άκρα μεταξύ τους, πραγματοποιώντας έτσι την σύνδεση των δύο χρηστών. Παράλληλα με την εξέλιξη των τηλεπικοινωνιών αρχίζει να υπάρχει ενδιαφέρον για τον "αυτοματισμό γραφείου" οι γραφομηχανές εξελίσσονται σε ηλεκτρονικούς υπολογιστές και τα κλασικά τηλέφωνα αρχίζουν να γίνονται ανεπαρκή. Τις αυξανόμενες ανάγκες που έχουν δημιουργηθεί θα τις καλύψουν τα PBX. Το PBX είναι τα αρχικά των λέξεων Private Branch Exchange, είναι δηλαδή ένα ιδιωτικό τηλεφωνικό σύστημα που χρησιμοποιείται μέσα σε μια εταιρεία. Οι χρήστες του τηλεφωνικού συστήματος του PBX που επιθυμούν να καλέσουν κάποιον προορισμό εκτός του εταιρικού δικτύου χρησιμοποιούν τις εξωτερικές γραμμές. Οι εξωτερικές γραμμές δεν είναι κάτι παραπάνω από έναν απλό τηλεφωνικό αριθμό. Βέβαια όπως θα δούμε και παρακάτω μια εξωτερική γραμμή μπορεί να παρέχεται από κάποιον πάροχο μέσω γραμμής PSTN/ISDN ή ακόμη και μέσω internet. Μία από τις τελευταίες τάσεις στην εξέλιξη των τηλεφωνικών συστημάτων PBX είναι το VoIP PBX και οι λύσεις ενοποιημένης επικοινωνίας.



Εικόνα 1: Αναλογικό τηλεφωνικό κέντρο.

1.3.1 Εξέλιξη

Τα πρώτα τηλεφωνικά κέντρα ήταν ηλεκτρομηχανικά. Δηλαδή περιελάμβαναν όργανα με κινούμενα μηχανικά τμήματα, όπως επιλογείς, ηλεκτρομαγνήτες κ.λπ., Τα κέντρα αυτά βελτιώνονταν συνεχώς και στις μέρες μας παρέχουν υπηρεσίες ενοποιημένης επικοινωνίας. Οι κυριότεροι τύποι τηλεφωνικών κέντρων παρουσιάζονται παρακάτω

1.3.1.1 Συνδρομητικά κέντρα

Τα συνδρομητικά κέντρα εξυπηρετούν την ενδοεπικοινωνία σε επιχειρήσεις και μεγάλους ιδιωτικούς ή δημόσιους οργανισμούς, που απασχολούν πολλούς χρήστες τηλεφώνων με τακτική μεταξύ τους

επικοινωνία. Υπάρχει, επίσης, η δυνατότητα επικοινωνίας με συνδρομητές δημόσιων εγκαταστάσεων. Γενικά, ένα συνδρομητικό κέντρο εξασφαλίζει:

I. Εσωτερική επικοινωνία μεταξύ των χρηστών, χωρίς τη μεσολάβηση οργάνων του αστικού κέντρου.

II. Αστική υπεραστική επικοινωνία.

III. Επικοινωνία με άλλα συνδρομητικά κέντρα.

Το συνδρομητικό κέντρο συνδέεται με το αστικό κέντρο μέσω μιας ή περισσότερων κύριων γραμμών. Οι τηλεφωνικές συσκευές του ονομάζονται εσωτερικές και οι αριθμοί κλήσης τους εσωτερικοί αριθμοί της εγκατάστασης.

Αυτόματα τηλεφωνικά κέντρα. Ο καλών συνδρομητής αναγγέλλει στο κέντρο τον αριθμό κλήσης του καλούμενου, αποστέλλοντας στο κέντρο τις εντολές του μετασχηματισμένες σε ηλεκτρικούς παλμούς ή συνδυασμούς συχνοτήτων , και το κέντρο απαντά με διάφορα ηχοσυστήματα . Όταν ο καλών σηκώσει το μικροτηλέφωνό του, κλείνει το κύκλωμα της συνδρομητικής γραμμής και το κέντρο διαπιστώνει την επιθυμία του να πραγματοποιήσει συνδιάλεξη στέλνοντας το ηχόσημα έναρξης επιλογής, που αντιστοιχεί στο α του τηλεγραφικού κώδικα Morse. Επιλογή είναι ο σχηματισμός του αριθμού κλήσης του καλούμενου.

Κάθε σύνδεση περιλαμβάνει ορισμένα τμήματα γραμμών, που ενώνονται μεταξύ τους μέσω επιλογέων. Η εύρεση μιας ελεύθερης γραμμής γίνεται με διαδοχικό έλεγχο των γραμμών που μπορούν να χρησιμοποιηθούν στη σύνδεση. Η λειτουργία αυτή ονομάζεται δοκιμή. Η πρώτη ελεύθερη γραμμή που εντοπίζεται καταλαμβάνεται, και αμέσως μετά ακολουθεί η φραγή, δηλαδή η λειτουργία με την οποία εμποδίζεται νέα κατάληψη της γραμμής. Αν όλες οι γραμμές είναι κατειλημμένες ή ο καλούμενος πραγματοποιεί άλλη συνδιάλεξη, τότε η σύνδεση δεν μπορεί να εξελιχθεί και ο καλών δέχεται το ηχόσημα κατειλημμένου, που αντιστοιχεί στο **‘ε’** του κώδικα Morse. Αν βρεθεί ελεύθερη γραμμή και ο καλούμενος δεν είναι απασχολημένος, τότε η σύνδεση προχωρεί και ο καλών δέχεται σήμα ελεύθερου, που αντιστοιχεί στο **τ** του κώδικα Morse. Με τον ίδιο ρυθμό στέλνεται στον καλούμενο το κλητήριο ρεύμα, που προκαλεί το κουδούνισμα της συσκευής του. Με το σήκωμα του τηλεφώνου του καλούμενου συνδρομητή, κλείνει το συνδρομητικό του κύκλωμα και αρχίζει η συνδιάλεξη. Η έναρξη της συνδιάλεξης αποτελεί κριτήριο για την έναρξη της χρέωσής της, ενώ το τέλος της συνδιάλεξης και της χρέωσης πραγματοποιείται με απόθεση του μικροτηλεφώνου στο άγκιστρο. Από τη στιγμή αυτή αρχίζει η απόλυση της σύνδεσης, δηλαδή η απελευθέρωση των χρησιμοποιούμενων οργάνων και γραμμών.

Τα αυτόματα τηλεφωνικά κέντρα, ανάλογα με τα κατασκευαστικά στοιχεία που χρησιμοποιούν ,διακρίνονται σε τρεις μεγάλες κατηγορίες:

Ηλεκτρομηχανικά , που χρησιμοποιούν αποκλειστικά ηλεκτρομηχανικά στοιχεία στις διατάξεις καθοδήγησης και στο δίκτυο των γραμμών ομιλίας για τη σύνδεση των γραμμών. Στην κατηγορία αυτή ανήκουν τα συστήματα με ρωστήρες και επιλογείς.

Ο ρωστήρας (ηλεκτρονόμος ή ρελέ) είναι ένας μηχανικός διακόπτης που λειτουργεί ηλεκτρομαγνητικά. Με τη βοήθεια ρεύματος που διοχετεύεται στο κύκλωμα οδήγησης μιας κλήσης, ανοίγουν ή κλείνουν επαφές και, μαζί με αυτούς, ένα ή περισσότερα ξεχωριστά κυκλώματα.

Ο **επιλογέας** προσδιορίζει στο τηλεφωνικό κέντρο την εισερχόμενη γραμμή, που αφορά τον συνδρομητή που καλεί, και την εξερχόμενη, που αφορά τον καλούμενο συνδρομητή, και τις συνδέει. Για τη σύνδεση ενός εισερχόμενου με έναν εξερχόμενο αγωγό, ακολουθούνται στην αναλογική Τηλεφωνία δύο βασικές τεχνικές. Σύμφωνα με την πρώτη τεχνική, ο εισερχόμενος αγωγός είναι συνδεδεμένος στο ένα άκρο ενός κινητού βραχίονα, ενώ οι εξερχόμενοι αγωγοί είναι συνδεδεμένοι σε επαφικές θέσεις, κατάλληλες να συνδεθούν με το άλλο άκρο του βραχίονα μέσω ενός περιστροφικού επιλογέα. Σύμφωνα με τη δεύτερη τεχνική, ο εισερχόμενος αγωγός διασταυρώνεται με όλους τους εξερχόμενους, αλλά αγώγιμη σύνδεση συμβαίνει μόνο με έναν, μέσω ενός κατάλληλου ραβδό-επαφικού επιλογέα.

Ημιηλεκρονικά , που περιλαμβάνουν ηλεκτρονικές διατάξεις καθοδήγησης και ηλεκτρομηχανικά στοιχεία για τη σύνδεση των γραμμών.

Ηλεκτρονικά, που περιλαμβάνουν μόνο ηλεκτρονικές διατάξεις. Τα ψηφιακά και γενικά τα ηλεκτρονικά κέντρα πλεονεκτούν σε σχέση με τα γνωστά ηλεκτρομηχανικά, διότι:

I. Καταλαμβάνουν πολύ μικρότερο χώρο και χαρακτηρίζονται από πολύ μεγαλύτερη ταχύτητα λειτουργίας.

II. Έχουν χαμηλό κόστος συντήρησης, διότι δεν περιλαμβάνουν κινητά όργανα. Ο έλεγχος γίνεται με πρόγραμμα ενταμιευμένο σε ηλεκτρονικό υπολογιστή.

III. Δίνουν δυνατότητα επέκτασης των προσφερόμενων στους συνδρομητές υπηρεσιών, όπως επικοινωνία Η/Υ μέσω τηλεφωνικού δικτύου, μεταβίβαση κειμένων μέσω τηλεφωνικού δικτύου με όλα τα σύμβολα μιας κοινής γραφομηχανής (υπηρεσίες FAX ή TELETEXT) και μεταβίβαση κειμένων και σχεδίων στους κοινούς τηλεοπτικούς δείκτες μέσω τηλεφωνικού δικτύου(υπηρεσία VIDEOTEXT).

1.3.1.2 Συστήματα ψηφιακής Τηλεφωνίας

Η ψηφιακή τεχνολογία στην Τηλεφωνία είναι συνδυασμένη με την τεχνική της πολύπλεξης με διαίρεση χρόνου, δηλαδή διαθέτει μια γραμμή σε μια ομάδα χρηστών, όπου ο κάθε χρήστης καταλαμβάνει τη γραμμή για ένα ποσοστό του χρόνου. Αρχικά εμφανίστηκαν τα ηλεκτρονικά κέντρα, για τη λειτουργία των οποίων το συνεχούς πλάτους-συνεχούς χρόνου σήμα της φωνής έπρεπε να μετατραπεί σε συνεχούς πλάτους-διακριτού χρόνου, δηλαδή να ληφθούν δείγματα φωνής. Η δειγματοληψία γίνεται με ρυθμό 8.000 δειγμάτων/s ή, αλλιώς κάθε 125 μs (1μs=10-^{6}s). Η διάρκεια ενός παλμού δείγματος ανέρχεται σε 0,5 μs. Μετά από κάθε παλμό δείγματος ακολουθεί κενό διάρκειας 0,5 μs με σκοπό την αποφυγή των παρεμβολών και τη διευκόλυνση του συγχρονισμού του συστήματος. Συνεπώς, είναι δυνατή η ταυτόχρονη μετάδοση 125 συνδιαλέξεων. Οι παλμοί των δειγμάτων είναι παλμοί διαμορφωμένοι κατά πλάτος. Τα ψηφιακά κέντρα είναι εξέλιξη των ηλεκτρονικών, στην περίπτωση κατά την οποία το αναλογικό σήμα της φωνής μετατρέπεται σε ψηφιακό. Εκτός από τη δειγματοληψία, λαμβάνει χώρα και κωδικοποίηση του σήματος φωνής, συνήθως με τη μέθοδο της παλμοκωδικής διαμόρφωσης PCM και μέσω της κοινής γραμμής μεταδίδονται μόνο στα ψηφιακά σήματα ομιλίας. Στα ψηφιακά σήματα PCM γίνεται ομαδοποίηση των συνδρομητών ανά 30. Στις ομάδες αυτές γίνεται δειγματοληψία του σήματος φωνής κάθε συνδρομητή 8.000 φορές/s δηλαδή ανά 125 μs. Το χρονικό πλαίσιο των 125 μs λέγεται PCM-frame. Κάθε δείγμα κωδικοποιείται με 8 δυαδικά ψηφία. Το χρονικό διάστημα που εκχωρείται σε κάθε συνδρομητή έχει διάρκεια3,9 μσκαι λέγεται συνδρομητική σχισμή(time slot). Σε αυτό το χρονικό διάστημα αποστέλλονται τα αντίστοιχα 8 δυαδικά ψηφία του δείγματος ομιλίας του συνδρομητή. Στο πλαίσιο των 125 μs υπάρχουν επιπλέον δύο σχισμές, που δεν εκχωρούνται σε συνδρομητές, αλλά χρησιμοποιούνται για ρυθμίσεις, συγχρονισμό του συστήματος, σηματοδοσία κ.ά. Σύνδεση δύο συνδρομητών σημαίνει ότι κάθε 125 μs τα 8 δυαδικά ψηφία ομιλίας του πρώτου, που μεταβιβάζονται στην κοινή γραμμή κατά τη διάρκεια της συνδρομητικής σχισμής που του ανήκει, πρέπει να μεταφερθούν στη σχισμή του δεύτερου, και αντίστροφα Η εφαρμογή ψηφιακών τεχνικών συνδυάζεται με τη χρήση οπτικών ινών ως μέσου μετάδοσης. Οι συχνότητες που διαδίνονται στις οπτικές ίνες είναι της τάξης των 10^{14} Hz , δηλαδή αφορούν την υπέρυθρη περιοχή. Είναι δυνατό να γίνει εκμετάλλευση εύρους ζώνης συχνοτήτων, που κυμαίνεται από 10-25 MHz. Γίνεται, επομένως φανερό ότι, εφαρμόζοντας την τεχνική των φερέσυχνων συστημάτων σε συνδυασμό με πολύπλεξη με διαίρεση χρόνου, είναι δυνατό να αυξηθεί εντυπωσιακά ο αριθμός των τηλεφωνικών καναλιών που μπορούν ταυτοχρόνως να διέλθουν μέσα από μία μόνο οπτική ίνα.

1.4 Public Switched Telephone Network

Οι τηλεφωνικές κλήσεις δρομολογούνται μέσα από το δημόσιο Τηλεφωνικό δίκτυο(PSTN). Ο ορισμός PSTN αναφέρεται στα διασυνδεδεμένα τηλεφωνικά δίκτυα. Τα δίκτυα αυτά έχουν δημόσιο προσανατολισμό όσον αφορά την εμπορική τους εκμετάλλευση και το ιδιοκτησιακό τους καθεστώς και συχνά τα ονομάζουμε " Απλή Παλαιά Τηλεφωνική Υπηρεσία" (POTS). Πλέον το POTS έχει

εξελιχθεί και χρησιμοποιεί στο μεγαλύτερο μέρος του ψηφιακή τεχνολογία. Στην πραγματικότητα το PSTN αποτελεί το backbone μέρος του διαδικτύου και στα περισσότερα δυτικά κράτη τον έλεγχό του τον έχει δημόσιος φορέας. Είναι κατανοητό ότι κανένα ιδιωτικό δίκτυο δεν είναι ικανό να καλύψει όλες τις ανάγκες των χρηστών του, έτσι οι πάροχοι έχουν προβεί σε συμφωνίες προκειμένου να ανταλλάσσονται δεδομένα ανάμεσα στα δίκτυα και να μην επιβαρύνονται οι χρήστες. Το Δημόσιο Τηλεφωνικό Δίκτυο Μεταγωγής είναι το κέντρο των τηλεπικοινωνιών υπηρεσιών τόσο για τις επιχειρήσεις όσο και για την σύνδεση μας με το διαδίκτυο και το PSTN είναι η κύρια υπηρεσία του δικτύου που παρέχουν οι τηλεπικοινωνιακές εταιρίες στους επιχειρηματίες-πελάτες τους.

1.5 Integrated Services Data Digital Network

Όπως είπαμε τα πρώτο τηλεφωνικό δίκτυο χρησιμοποιούσε αναλογικά συστήματα για την σύνδεση των συνδρομητών. Το δίκτυο αυτό δεν ήταν αποδοτικό και ήταν επιρρεπές στον θόρυβο. Κατά την δεκαετία του 60’ το τηλεφωνικό δίκτυο αρχίζει να εξελίσσεται και οι εσωτερικές συνδέσεις αρχίζουν να μετατρέπονται σε ένα σύστημα μεταγωγής πακέτων. Με την πάροδο των χρόνων η αύξηση των τηλεπικοινωνιακών αναγκών και η εμπορική αξιοποίηση του διαδικτύου ωθεί την ανάπτυξη του ISDN στην Αμερική. Έτσι στις αρχές τις δεκαετίας του ΄90 γίνεται μια μεγάλη προσπάθεια για την ανάπτυξη ISDN δικτύου στην Αμερική του οποίου η δομή θα επιτρέπει στους τελικούς χρήστες να επιλέξουν τερματικές συσκευές της επιλογής τους. Το ISDN έρχεται να αντικαταστήσει τις συνδέσεις POTS που αποτελούσε μέχρι τότε μεγάλο μέρος του δικτύου. Σήμερα POTS γραμμές είναι οι PSTN που αποτελούν την βασική τηλεφωνική υπηρεσία (φωνητική επικοινωνία), για μικρές επιχειρήσεις, αλλά κυρίως για οικιακούς συνδρομητές. Το όνομά του, υποδηλώνει την απλή τηλεφωνική υπηρεσία που είναι διαθέσιμη μέχρι σήμερα, ακόμα και έπειτα από την έλευση νεώτερων τεχνολογιών τηλεφωνίας όπως το ISDN, τα δίκτυα κινητής τηλεφωνίας (ασύρματα δίκτυα κυψέλης), αλλά και το VoIP. Η PSTN παρέχεται περίπου από την αρχή της λειτουργίας του δημόσιου τηλεφωνικού δικτύου στα τέλη του 19ου αιώνα, σχεδόν απαράλλακτη ως προς τον τελικό χρήστη, παρόλη την διείσδυση νέων ψηφιακών τεχνολογιών όπως η δυνατότητα τονικής κλήσης, των ηλεκτρονικών ψηφιακών τηλεφωνικών κέντρων, και η χρήση οπτικών ινών στο backbone. Η ISDN αποτελείται από ένα σύνολο τηλεπικοινωνιακών προτύπων που επιτρέπουν την ταυτόχρονη ψηφιακή μετάδοση φωνής, βίντεο, δεδομένων και άλλων υπηρεσιών, μέσω του δημόσιου τηλεφωνικού δικτύου μεταγωγής κυκλώματος (PSTN). Το βασικό χαρακτηριστικό και πλεονέκτημα του ISDN, είναι ότι ενσωματώνει φωνή και δεδομένα στην ίδια γραμμή, προσθέτοντας παράλληλα χαρακτηριστικά που δεν ήταν διαθέσιμα στην κλασική τηλεφωνία. Κάθε γραμμή ISDN αποτελείται από B-channels, το καθένα από το οποία προσφέρει ρυθμό μετάδοσης 64 kbps, και ένα κανάλι για σηματοδοσίες γνωστό ως D-channel για σηματοδοσία. Κάθε B-channel στο ISDN, μπορεί είναι ανεξάρτητο από τα υπόλοιπα και έτσι μπορεί να μεταφέρει φωνή ή και δεδομένα. Στην Ελλάδα το ISDN παρέχεται εμπορικά ως ISDN-BRI, διαθέτει 2 κανάλια B προσφέροντας εύρος ζώνης έως 128kbps και δίνετε η επιλογή για χρήση MSN ή DDI.

1.6 Μικρομεσαίες επιχειρήσεις.

1.6.1 Τι είναι μικρομεσαία επιχείρηση

Προτού επεκταθούμε στην μελέτη τον σχεδιασμό και την υλοποίηση ενός εταιρικού τηλεφωνικού δικτύου είναι αναγκαία η αναφορά στο περιβάλλον των μικρομεσαίων επιχειρήσεων (πλήθος υπαλλήλων/οικονομικά μεγέθη) καθώς αυτοί οι παράγοντες αποτελούν τους σχεδιαστικούς περιορισμούς για την υλοποίηση του τελικού δικτύου.

Σύμφωνα με την Ευρωπαϊκή νομοθεσία[1] επιχείρηση θεωρείται κάθε μονάδα, ανεξάρτητα από τη νομική της μορφή, που ασκεί οικονομική δραστηριότητα, ως τέτοιες νοούνται ιδίως οι μονάδες που ασκούν βιοτεχνική ή άλλη δραστηριότητα, ατομικά ή οικογενειακά, προσωπικές εταιρείες ή ενώσεις προσώπων που ασκούν τακτικά μια οικονομική δραστηριότητα. Σύμφωνα με τον ίδιο νόμο (άρθρο 2) η κατηγορία των πολύ μικρών, μικρών και μεσαίων επιχειρήσεων (ΜμΕ) αποτελείται από επιχειρήσεις που απασχολούν λιγότερους από 250 εργαζομένους και ο ετήσιος κύκλος εργασιών δεν υπερβαίνει τα 50 εκατομμύρια ευρώ ή το σύνολο του ετήσιου ισολογισμού δεν υπερβαίνει τα 43 εκατομμύρια ευρώ.

Οι μικρομεσαίες επιχειρήσεις στην Ελλάδα αποτελούν την συντριπτική πλειονότητα (Εθνική Τράπεζα, 2012)των επιχειρήσεων που λειτουργούν. Σύμφωνα με στατιστικά (Ινστιτούτο Μικρών Επιχειρήσεων, 2012) στην Ελλάδα αριθμούν περίπου τις 727.883 (Εθνική Συνομοσπονδία Ελληνικού Εμπορίου, 2012) μικρομεσαίες επιχειρήσεις, με κατά μέσο όρο δύο απασχολούμενους ανά επιχείρηση. Σύμφωνα με στοιχεία της EUROSTAT, η Ελλάδα είναι η χώρα με την μεγαλύτερη αναλογία επιχειρήσεων σε σχέση με τον πληθυσμό της στην Ευρωπαϊκή Ένωση. Από αυτές οι περισσότερες κατατάσσονται στην κατηγορία πολύ μικρές επιχειρήσεις (δηλαδή έως 10 εργαζόμενους) και έχουν έντονα οικογενειακό χαρακτήρα. Ταυτόχρονα η Ελλάδα χαρακτηρίζεται από πολύ υψηλό ποσοστό αυτοαπασχολούμενων. Αναφορικά με την απασχόληση , για το έτος 2003 οι επιχειρήσεις που απασχολούν μέχρι 10 άτομα αποτελούν το 74% της απασχόλησης στον ιδιωτικό τομέα. Από τα παραπάνω στατιστικά στοιχεία μπορούμε να εξάγουμε δύο βασικά συμπεράσματα πάνω στα οποία θα στηριχθούν τα συμπεράσματα της πτυχιακής:

- Για τα Ελληνικά δεδομένα ΜμΕ θεωρείται οποιαδήποτε επιχείρηση με λιγότερο από 50 απασχολούμενους
- Λόγου του μικρού αριθμού των απασχολούμενων οι Ελληνικές ΜμΕ δεν διαθέτουν τμήμα IT

[1] Ευρωπαϊκή Επιτροπή: Σύσταση 6 Μαΐου 2003 άρθρο 1.

- Ο προϋπολογισμός για την υλοποίηση ενός τηλεφωνικού δικτύου δεν θα πρέπει να ξεπερνάει τα 6.000€[2]

Στα πλαίσια της παρούσας πτυχιακής εργασίας θεωρώ ως ΜμΕ τις επιχειρήσεις που απασχολούν έως 50 άτομα και με ετήσιο τζίρο μικρότερο των δέκα εκατομμυρίων ευρώ. Ενδιαφέρον παρουσιάζει ο ακόλουθος πίνακας ο οποίος παρουσιάζει το πλήθος ανά κατηγορία επιχείρησης στην Ελλάδα.

[2] Η υλοποίηση ενός δικτύου αποτελεί πάγιο έξοδο και το ενδεικτικό κόστος 6.000€ αφορά για ΜμΕ με 50 απασχολούμενους.

2 Δίκτυα

2.1 Εισαγωγή:

Ένα δίκτυο υπολογιστών είναι ένα σύστημα επικοινωνίας δεδομένων που συνδέει δύο ή περισσότερους αυτόνομους και ανεξάρτητους μεταξύ τους. Δύο υπολογιστές θεωρούνται διασυνδεδεμένοι όταν μπορούν να ανταλλάσσουν μεταξύ τους δεδομένα. Τα δίκτυα δημιουργήθηκαν για να εξυπηρετήσουν τις ανάγκες που προέκυψαν από την εξάπλωση της χρήσης των υπολογιστών. Βασικός σκοπός της ύπαρξης των δικτύων είναι ο διαμερισμός των πόρων του συστήματος και η ανταλλαγή δεδομένων μεταξύ των τερματικών συσκευών. Πόρους του συστήματος μπορούμε να θεωρήσουμε το υλικό (hardware), όπως εκτυπωτές, plotters, σκληροί δίσκοι ή ακόμη και το λογισμικό (software), π.χ. δεδομένα, προγράμματα εφαρμογών, υπηρεσίες. Έτσι με τα δίκτυα τα προγράμματα, τα δεδομένα και οι συσκευές (σκληροί δίσκοι, εκτυπωτές, κλπ) είναι διαθέσιμα σε οποιονδήποτε είναι

Κεφάλαιο 2

Δίκτυα

συνδεδεμένος στο δίκτυο, ανεξάρτητα από τη φυσική του θέση. Με τον τρόπο αυτό επιτυγχάνεται εξοικονόμηση χρημάτων, αύξηση της απόδοσης του συστήματος, κεντρικός έλεγχος και εύκολη επεκτασιμότητα. Σε ένα δίκτυο μπορούμε να έχουμε ανταλλαγή δεδομένων, προγραμμάτων, χρήση κοινών βάσεων δεδομένων, αρχείων, αποστολή μηνυμάτων. Επιπλέον, ανεξάρτητα της τεχνολογίας, ένα δίκτυο είναι ένα πανίσχυρο μέσο επικοινωνίας ανθρώπων που βρίσκονται σε διαφορετικά μέρη.

2.1.1 Αρχιτεκτονική των δικτύων.

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

Είδη Δικτύων:

Ο διαχωρισμός των δικτύων γίνεται με βάση το γεωγραφικό εύρος που καλύπτουν και την τοπολογία τους. Οι βασικότερες κατηγορίες δικτύων ανάλογα με το μέγεθος παρουσιάζονται παρακάτω:

- **Δίκτυα ευρείας περιοχής:** Τα δίκτυα ευρείας περιοχής (WAN) καλύπτουν αποστάσεις πολλών χιλιομέτρων (συνήθως άνω των 5 km) στην ίδια πόλη, μέχρι χιλιάδων χιλιομέτρων σε διαφορετικές πόλεις - κράτη - ηπείρους. Αποτελούν συνήθως τα δίκτυα των τηλεπικοινωνιακών παρόχων και αποτελούν το backbone του internet.

- **Τοπικά δίκτυα:** Τοπικά δίκτυα καλύπτουν μικρές αποστάσεις (μερικών εκατοντάδων μέτρων και περιορίζονται στα πλαίσια μιας επιχείρησης. Ο διαχωρισμός τους από τα δίκτυα ευρείας περιοχής οφείλεται στην τεχνολογία που χρησιμοποιούν αλλά κυρίως στην ιδιοτηκότητα που τα διέπει.

- **Αστικά δίκτυα:** Τα αστικά δίκτυα (MAN) καλύπτουν περιοχές μεγέθους αστικού κέντρου. Είναι ταχύτερα από τα τοπικά δίκτυα και μπορούν να μεταδώσουν εικόνα, φωνή και δεδομένα αποδοτικότερα.

Τοπολογία δικτύου: Η τοπολογία καθορίζει τον τρόπο με τον οποίο συνδέονται μεταξύ τους οι συσκευές του δικτύου. Η πιο απλή σύνδεση ονομάζεται "Point-to -Point" και συνδέει δύο σημεία μεταξύ τους. Οι υπόλοιπες τοπολογίες χαρακτηρίζονται σαν δίκτυα "κοινού-μέσου", όπου κάθε κόμβος συνδέεται με όλους τους υπόλοιπους. Τέτοιες τοπολογίες είναι:

- αρτηρίας ή διαύλου (bus)
- δακτυλίου (ring)
- αστέρα (star)
- δένδρου (tree)
- Mesh.

Μέθοδος πρόσβασης:

Στα δίκτυα ακρόασης, όπου όλοι οι κόμβοι έχουν πρόσβαση στο κοινό μέσο, απαιτείται ένας αλγόριθμος που εξασφαλίζει ποιος κόμβος μεταδίδει κάθε φορά. Οι βασικές μέθοδοι είναι τρεις :

- με ανταγωνισμό (π.χ. Ethernet)
- με διαβούλευση (π.χ. Token Ring)
- με πολυπλεξία (π.χ. Time Division Multiplexing)

Τεχνική Μετάδοσης και κωδικοποίησης των δεδομένων: Η πληροφορία, προκειμένου να μεταδοθεί, πρέπει να μετατραπεί στη μορφή που το μέσο μπορεί να μεταδώσει. Οι κυριότερες τεχνικές μετάδοσης είναι:

- βασικής / ευρείας ζώνης
- ψηφιακού / αναλογικού σήματος
- διαμόρφωση / αποδιαμόρφωση
- σύγχρονη / ασύγχρονη

Ταχύτητα μετάδοσης. Μετρείται σε bits/sec και εξαρτάται από το μέσο, την τεχνική μετάδοσης, το εύρος ζώνης και τη μέθοδο πρόσβασης στο μέσο.

2.2 Πρωτόκολλα επικοινωνίας.

Η λέξη "πρωτόκολλο" αναφέρεται στους κανόνες που ακολουθεί ένα δίκτυο για την αποστολή ή λήψη δεδομένων μεταξύ των κόμβων. Το πρωτόκολλο επικοινωνίας είναι μια σειρά κανόνων στους οποίους στηρίζεται η επικοινωνία των συσκευών σε ένα δίκτυο. Οι κανόνες αυτοί καθορίζουν τη μορφή, το χρόνο και τη σειρά μετάδοσης των πληροφοριών στο δίκτυο. Η πιο γνωστή οικογένεια πρωτοκόλλων είναι το TCP/IP, στην οποία βασίζεται το Διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων. Η ονομασία TCP/IP προέρχεται από τις συντομογραφίες των δυο κυριότερων πρωτοκόλλων που περιέχει, το TCP ή Transmission Control Protocol και το IP ή Internet Protocol (Πρωτόκολλο Διαδικτύου). Εκτενής περιγραφή για την λειτουργία των χρησιμοποιούμενων πρωτοκόλλων γίνεται σε άλλη ενότητα του κεφαλαίου.

Το internet είναι το "δίκτυο των δικτύων" μια συλλογή. από διασυνδεδεμένους Η/Υ και δίκτυα Η/Υ που συνδέονται μεταξύ τους βάσει ενός συνόλου πρωτοκόλλων. Με τα πρωτόκολλα αυτά γίνεται δυνατή η επικοινωνία μεταξύ υπολογιστών, πολλές φορές μη συμβατών μεταξύ τους, που βρίσκονται σε διαφορετικά δίκτυα. Το internet διασύνδεει τοπικά δίκτυα εκπαιδευτικών ιδρυμάτων, νοσοκομείων, εταιριών κ.α. σε ένα υπέρ-δίκτυο που διαρκώς επεκτείνεται. Το πραγματικό μέγεθος του διαδικτύου δεν μπορεί να αναπαρασταθεί, καθώς νέες συσκευές και δίκτυα προστίθενται διαρκώς.

2.2.1 Internet Protocol

Το Πρωτόκολλο IP αποτελεί το κύριο πρωτόκολλο επικοινωνίας για τη μετάδοση datagrams σε ένα δίκτυο και είναι μέρος του TCP/IP. Το Πρωτόκολλο IP είναι υπεύθυνο για τη δρομολόγηση των πακέτων ανάμεσα στα διάφορα δίκτυα, ανεξάρτητα από την υποδομή τους, και αποτελεί το κύριο πρωτόκολλο πάνω στο οποίο είναι βασισμένο το διαδίκτυο. Το πρωτόκολλο IP, ανήκει στο επίπεδο δικτύου, στο μοντέλο OSI και στο TCP/IP. Καθορίζει τη μορφή των πακέτων που στέλνονται μέσω

ενός δικτύου, καθώς και τους μηχανισμούς που χρησιμοποιούνται για την προώθηση των πακέτων από έναν υπολογιστή προς έναν τελικό προορισμό μέσω ενός ή περισσότερων δρομολογητών. Γι' αυτούς τους σκοπούς, το IP, χρησιμοποιεί συγκεκριμένες μεθόδους διευθυνσιοδότησης και δομές για την ενθυλάκωση των πακέτων δεδομένων.

Το Πρωτόκολλο IP εισήχθη από τους Vint Cerf και Bob Kahn το 1974. Συνδέεται στενά με το πρωτόκολλο ελέγχου μετάδοσης (TCP), με αποτέλεσμα ολόκληρη η σουίτα των πρωτοκόλλων του Διαδικτύου να αναφέρεται απλά ως σουίτα TCP/IP. Η πρώτη μεγάλης κλίμακας έκδοση του Πρωτοκόλλου IP, ήταν η έκδοση 4 (IPv4) η οποία επικρατεί μέχρι και σήμερα σε όλο το Διαδίκτυο. Με την αύξηση των διαδικτυακών συσκευών και του περιορισμένου εύρους διευθύνσεων, έχει προκύψει ανάγκη αντικατάστασης του πρωτοκόλλου IPv4 από το διάδοχο IPv6[Βλ.Κεφ 6]. Οι τελευταίες διευθύνσεις IPv4 παραδόθηκαν σε ειδική τελετή, στις 3 Φεβρουαρίου του 2011, στο Μαϊάμι (ICANN, 2011).

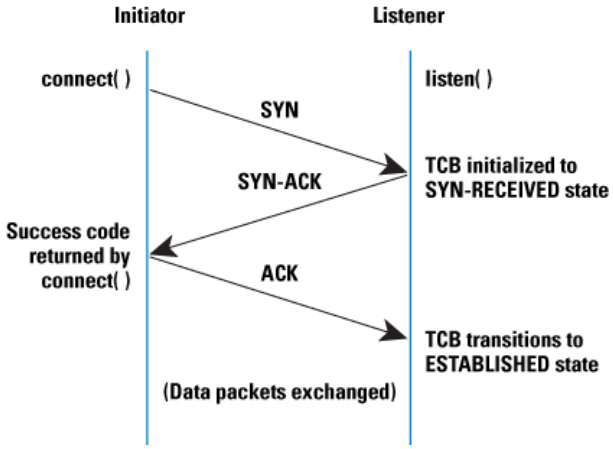
2.2.2 Transmission control protocol

Το TCP (Transmission Control Protocol) είναι ένα από τα κυριότερα πρωτόκολλα του TCP/IP. Βρίσκεται πάνω από το πρωτόκολλο IP και οι κύριοι στόχοι του είναι η αξιόπιστη αποστολή και λήψη δεδομένων, η μεταφορά δεδομένων χωρίς λάθη μεταξύ των επιπέδου δικτύου και εφαρμογής και η ταξινόμηση των πακέτων ώστε να δοθούν στο επίπεδο εφαρμογής με την σειρά που στάλθηκαν. Υπηρεσίες που χρησιμοποιούν το TCP είναι το SMTP το Telnet το FTP και το HTTP.

2.2.2.1 Χαρακτηριστικά λειτουργίας

3-way handshake

Το πρωτόκολλο ελέγχου μεταφορών (TCP) είναι συνδεσμοστρεφές (connection oriented), δηλαδή η μεταφορά δεδομένων γίνεται μέσω σύνδεσης, η οποία οριοθετείται από ένα σήμα έναρξης και ένα σήμα τέλους ή διακοπής. Πριν ο client συνδεθεί με τον server, ο server πρέπει να δεσμεύσει μια θύρα. Όταν γίνει αυτό, ο client μπορεί να ξεκινήσει την μέσω μιας διαδικασίας που καλείται τριπλή χειραψία.



Εικόνα 2 TCP 3way handshake

1. Αρχικά αποστέλλεται ένα πακέτο SYN. Ο client θέτει το sequence number του TCP header στον αρχικό αριθμό ακολουθίας του(ISN).

2. Ο server στο απαντάει:

   - SYN για την αποστολή του ISN του και ACK (με SEQ=ISN_{client}+1) για να επιβεβαιώσει τοαρχικό μήνυμα.

   - SYN/RST για να ενημερώσει τον client ότι αρνείται τη σύνδεση και η διαδικασία σταματά.

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

Κατά τη διάρκεια του three-way handshake, τα δύο μέρη διαπραγματεύονται επίσης όλες τις ειδικές επιλογές που θα χρησιμοποιηθούν κατά τη διάρκεια της σύνδεσης TCP, όπως ECN κ.α.

Μεταφορά δεδομένων

Αφού ολοκληρωθεί η τριπλή χειραψία και ξεκινήσει ροή δεδομένων ανάμεσα στον client και τον server το TCP κάνει διαρκή έλεγχο ροής και έλεγχο συμφόρησης. Χωρίς την ύπαρξη των προαναφερθέντων ελέγχων η εφαρμογή θα στείλει πακέτα στο δίκτυο προς τον παραλήπτη, εφόσον υπάρχουν δεδομένα να σταλούν και εφ' όσον ο αποστολέας δεν υπερβαίνει το window size που του έχει υποδείξει ο παραλήπτης. Όταν ο παραλήπτης δέχεται πακέτα TCP, στέλνει επιβεβαιώσεις (πακέτα ACK), για το ποιο πακέτο έχει λάβει σωστά. Σε αυτές τις επιβεβαιώσεις περιέχεται επίσης το επόμενο window size που καθορίζει πόσα byte επιθυμεί να δεχτεί στη συνέχεια ο παραλήπτης.

Έλεγχος ροής

Ο έλεγχος ροής βασίζεται στα ACK/NACK που ανταλλάσσονται . Οι αλγόριθμοι μεταβαλλόμενου μεγέθους παραθύρου που χρησιμοποιεί το TCP, επιτρέπουν σε πολλαπλά πακέτα δεδομένων να μεταφέρονται ταυτόχρονα για να χρησιμοποιείται αποδοτικότερα το εύρος ζώνης ενός δικτύου. Για

παράδειγμα, εάν ένας υπολογιστής Α στείλει 4 byte με αριθμό ακολουθίας (sequence number) 100 - συνεπώς, τα 4 bytes έχουν αριθμό ακολουθίας 100, 101, 102 και 103 - τότε ο παραλήπτης πρέπει να απαντήσει με επιβεβαίωση (acknowledgement) που φέρει sequence number 104. Αυτό πρόκειται να είναι το επόμενο byte που περιμένει στο επόμενο πακέτο. Εάν για κάποιο λόγο, τα τελευταία δύο bytes περιέχουν σφάλματα τότε η τιμή της επιβεβαίωσης θα είναι 102, εφόσον τα bytes με αριθμό 100 και 101 έχουν φτάσει με επιτυχία.

Έλεγχος συμφόρησης

Αν και το TCP δεν ενδιαφέρεται για όσα συμβαίνουν στο επίπεδο δικτύου είναι αρκετά "έξυπνο", ώστε να αντιληφθεί και να χειριστεί κατάλληλα μια συμφόρηση στο δίκτυο. Για αυτόν τον λόγο, το TCP περιλαμβάνει διάφορους αλγορίθμους που έχουν ως σκοπό είτε να αποφύγουν εξ αρχής τη συμφόρηση, ή να ανταποκριθούν σε αυτή. Οι κύριοι μηχανισμοί που κάνει χρήση για την αποφυγή συμφόρησης είναι οι:

- τον αλγόριθμο slow-start,
- τον αλγόριθμο congestion avoidance,
- τον αλγόριθμο fast retransmit και
- τον αλγόριθμο fast recovery

Οι παραπάνω μηχανισμοί αναφέρονται στο RFC 2001.

Τερματισμός

Η σύνδεση τερματίζεται με το four-way handshake, με την κάθε πλευρά να τερματίζει ανεξάρτητα:

1. Όταν κάποιο άκρο επιθυμεί να τερματίσει την σύνδεση, στέλνει ένα πακέτο FIN.
2. Το πακέτο αυτό επιβεβαιώνει η άλλη πλευρά με ένα ACK.
3. Το άλλο άκρο στέλνει επίσης ένα FIN πακέτο.
4. Η πλευρά που ξεκίνησε τον τερματισμό, μπορεί να το επιβεβαιώσει στέλνοντας ένα πακέτο ACK.

Μια σύνδεση μπορεί να είναι "half-open", δηλαδή η μία πλευρά να έχει τερματίσει, όχι όμως και η άλλη. Η πλευρά που έχει τερματίσει δεν μπορεί να στείλει πλέον δεδομένα, ενώ η άλλη μπορεί. Τέλος, είναι δυνατό, αν και λιγότερο πιθανό, οι δύο host να στείλουν ταυτόχρονα ένα πακέτο FIN ο ένας στον άλλο. Στη συνέχεια ο καθένας επιβεβαιώνει το FIN που δέχτηκε με ένα πακέτο ACK. Στο σημείο αυτό και οι δύο διακόπτουν τη σύνδεση.

2.2.3 User datagram protocol

Το άλλο πρωτόκολλο μεταφοράς που χρησιμοποιείται στο TCP/ IP είναι το User Datagram Protocol (UDP). Διάφορες υπηρεσίες χρησιμοποιούν το πρωτόκολλο UDP όπως το DNS, το SNMP και το RIP. Ένα από τα κύρια χαρακτηριστικά του UDP είναι ότι δεν εγγυάται αξιόπιστη επικοινωνία. Τα πακέτα UDP που αποστέλλονται μπορεί να φτάσουν στον παραλήπτη με λάθος σειρά, να φτάσουν διπλά ή αν το δίκτυο έχει συμφόρηση να μην φτάσουν. Η έλλειψη παρόμοιων μηχανισμών με αυτούς του TCP καθιστά το πρωτόκολλο UDP αρκετά πιο γρήγορο και αποτελεσματικό.

Οι εφαρμογές audio και video streaming χρησιμοποιούν κατά κόρον το UDP. Για τις εφαρμογές αυτές είναι πολύ σημαντικό τα πακέτα να παραδοθούν στον παραλήπτη το συντομότερο δυνατόν ούτως ώστε να μην υπάρχει διακοπή στην ροή του ήχου ή της εικόνας. Κατά συνέπεια προτιμάται το πρωτόκολλο UDP διότι είναι αρκετά γρηγορότερο, παρόλο που υπάρχει η πιθανότητα μερικά πακέτα UDP να χαθούν. Στην περίπτωση που χαθεί κάποιο πακέτο, οι εφαρμογές αυτές διαθέτουν ειδικούς μηχανισμούς διόρθωσης και παρεμβολής ούτως ώστε ο τελικός χρήστης να μην παρατηρήσει αλλοίωση ή διακοπή στην ροή λόγω του χαμένου πακέτου. Σε αντίθεση με το πρωτόκολλο TCP, το UDP υποστηρίζει broadcasting, δηλαδή την αποστολή ενός πακέτου σε όλους τους υπολογιστές ενός δικτύου, και multicasting, δηλαδή την αποστολή ενός πακέτου σε κάποιους συγκεκριμένους υπολογιστές ενός δικτύου. Η τελευταία δυνατότητα χρησιμοποιείται πολύ συχνά στις εφαρμογές audio και video streaming ούτως ώστε μία ροή ήχου ή εικόνας να μεταδίδεται ταυτόχρονα σε πολλούς συνδρομητές.

2.3 Διευθυνσιοδότηση

2.3.1 Διευθύνσεις IP

Μία διεύθυνση IP (IP address) είναι μια μοναδική ακολουθία αριθμών που χρησιμοποιείται από τις συσκευές για τη μεταξύ τους αναγνώριση κι επικοινωνία σε ένα δίκτυο υπολογιστών που χρησιμοποιεί το IP σαν πρωτόκολλο επιπέδου δικτύου. Πρέπει σε κάθε συσκευή στο δίκτυο να αναθέσουμε μια διεύθυνση IP. Όπως αναφέραμε παραπάνω υπάρχουν δυο εκδόσεις του IP σε χρήση οι οποίες χρησιμοποιούν διαφορετικό τρόπο αναπαράστασης των διευθύνσεων. Για το IPv4 οι διευθύνσεις IP είναι δεκαδικοί αριθμοί της μορφής xxx.xxx.xxx.xxx όπου xxx ένας αριθμός από 0 έως 255 ενώ στο IPv6 είναι δεκαεξαδικοί αριθμοί μορφής xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.xxx.xxx.xxx.xxx.

2.3.1.1 IPv4

Το IPv4 χρησιμοποιεί διευθύνσεις των 32-bit (4 byte), που περιορίζουν το πλήθος διευθύνσεων σε 4.294.967.296 (232) πιθανές μοναδικές διευθύνσεις. Εντούτοις, πολλές παρακρατούνται για ειδικούς λόγους, όπως για χρήση σε ιδιωτικά δίκτυα (~18 εκατομμύρια) ή διευθύνσεις multicasting (~1 εκατομμύριο). Κατά αυτόν τον τρόπο, μειώνεται ο αριθμός που μπορεί να διατεθεί για δημόσιες διευθύνσεις Διαδικτύου.

2.3.1.2 IPv6

Το πρωτόκολλο IPv6 έχει σχεδιαστεί με σκοπό να αντικαταστήσει το πρωτόκολλο IPv4, το οποίο χρησιμοποιείται εδώ και τριάντα χρόνια. Το IPv6 προσφέρει επιπλέον χαρακτηριστικά από το IPv4. Το κυριότερο είναι ο διευρυμένος χώρος διευθύνσεων από 32 bit σε 128 bit, η απλοποίηση της κεφαλίδας, καθώς και η υποστήριξη επιλογών και επεκτάσεων. Τέλος προσφέρει δυνατότητα μαρκαρίσματος των ροών κίνησης και δυνατότητα ασφαλείας. Το πρωτόκολλο IPv6 περιγράφεται αναλυτικά στο κεφάλαιο 7.

2.3.2 Dynamic Host Configuration Protocol.

Όπως είπαμε πιο πάνω, κάθε συσκευή στο δίκτυο πρέπει να έχει μια διεύθυνση IP. Ο μηχανισμός DHCP δίνει την δυνατότητα αυτόματης απόδοσης διευθύνσεων IP σε ένα δίκτυο. Το πρωτόκολλο είναι ουσιαστικά ένα λογισμικό που υλοποιείται σε έναν ή περισσότερους δρομολογητές του δικτύου. Ο διαχειριστής του δικτύου ρυθμίζει το εύρος των διευθύνσεων που αποδίδονται, ποιες συσκευές θα διευθυνσιοδοτούνται καθώς επίσης και για το χρονικό διάστημα που θα τους ανήκει η IP. Όλα τα σύγχρονα λειτουργικά συστήματα υλοποιούν έναν DHCP-client.

Αντιστοίχηση IP διευθύνσεων

Το DCHP υποστηρίζει 3 μηχανισμούς για την ανάθεση IP διευθύνσεων. Αυτοί είναι:

- Αυτόματη ανάθεση (με ανάθεση μόνιμης διεύθυνσης)
- Δυναμική ανάθεση (διεύθυνση με ημερομηνία λήξης)
- Χειροκίνητη ανάθεση (ο διαχειριστής ορίζει τις ρυθμίσεις)

Η εφαρμογή του πρωτοκόλλου

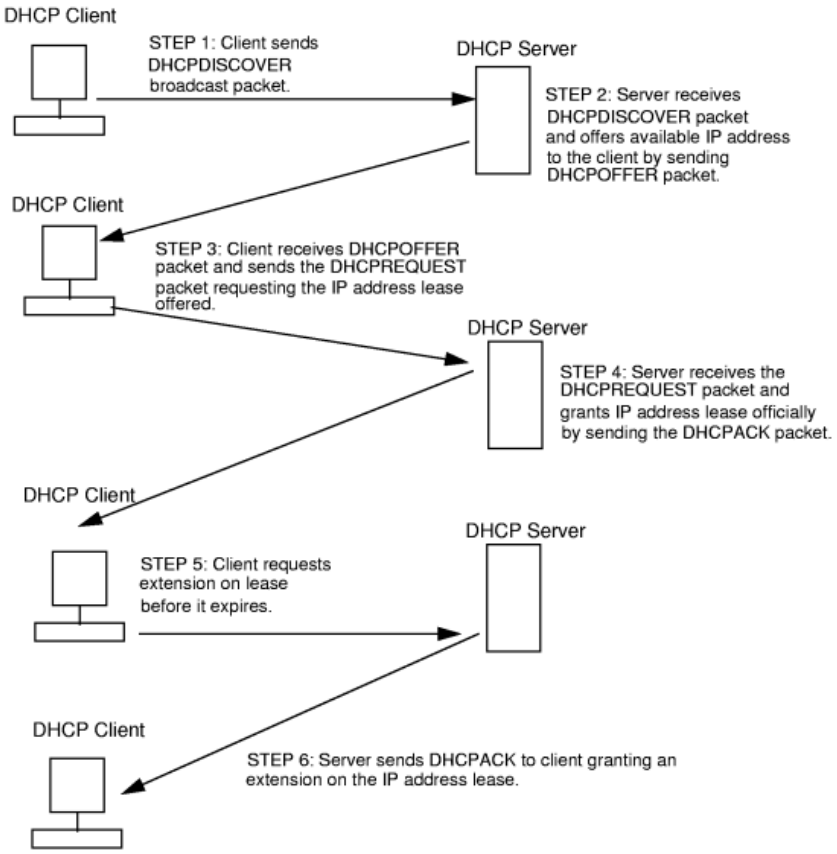
Στα εταιρικά δίκτυα λόγω του πλήθους των κόμβων συχνά προτιμάται η αυτόματη ανάθεση διευθύνσεων από έναν router/server. Ένας άλλος λόγος που προτιμούνται οι αυτόματες διευθύνσεις στα εταιρικά δίκτυα, είναι για την διευκόλυνση των χρηστών. Έτσι, υπάλληλοι που βρίσκονται εκτός γραφείου συχνά, μπορούν να συνδέονται σε ξένα δίκτυα χωρίς να χρειάζεται να επεμβαίνουν στις ρυθμίσεις του υπολογιστή τους. Η υλοποίηση της υπηρεσίας DHCP σε ένα δίκτυο δεν μας υποχρεώνει να έχουμε αυτόματη απόδοση των διευθύνσεων για όλους τους υπολογιστές. Μια συνήθης πρακτική είναι η χειροκίνητη απόδοση διευθύνσεων σε servers, πολυμηχανήματα και γενικότερα σε συσκευές που αποτελούν πάγιο μέρος του εταιρικού δικτύου.

Η υπηρεσία DHCP βασίζεται στην αρχιτεκτονική client-server με τον ρόλο του client να τον έχει η εκάστοτε συσκευή που ζητάει να της χορηγηθεί μια διεύθυνση IP. Αντίστοιχα το ρόλο του server τον έχει ο κόμβος στον οποίο έχουμε υλοποιήσει την υπηρεσία DHCP. Να σημειωθεί ότι το πρωτόκολλο DHCP δεν είναι το μοναδικό πρωτόκολλο απονομής διευθύνσεων, αλλά έρχεται να αντικαταστήσει παλαιότερα πρωτόκολλα απόδοσης IP διευθύνσεων, όπως το πρωτόκολλο BOOTR. Ανάμεσα στα δύο πρωτόκολλα υπάρχει συμβατότητα που σημαίνει πως ένας υπολογιστής που χρησιμοποιεί το πρωτόκολλο BOOTR μπορεί να ζητήσει IP διεύθυνση από έναν DHCP server, εν τούτοις το DHCP παρέχει πολλές βελτιώσεις έναντι του πρωτοκόλλου BOOTR. Ένα σημαντικό πλεονέκτημα του πρωτοκόλλου DHCP έναντι του πρωτοκόλλου BOOTR είναι πως μια IP διεύθυνση μπορεί να χορηγηθεί σε έναν υπολογιστή του δικτύου για συγκεκριμένο χρονικό διάστημα. Αυτή η δυνατότητα είναι πολύ χρήσιμη στις περιπτώσεις που οι υπολογιστές του δικτύου είναι περισσότεροι σε ένα χρονικό διάστημα από τις διαθέσιμες διευθύνσεις IP. Έτσι αποδίδοντας μια IP διεύθυνση σε έναν κόμβο για πεπερασμένο χρόνο, δεν κινδυνεύουμε να μείνουμε χωρίς ελεύθερες διευθύνσεις. Από την άλλη πλευρά, εάν οι διευθύνσεις που διαθέτουμε είναι περισσότερες από τους υπολογιστές του δικτύου, μπορούμε να αποδώσουμε διευθύνσεις σε κάποιους από αυτούς για απεριόριστο χρόνο. Ένα άλλο πλεονέκτημα του πρωτοκόλλου DHCP έναντι του πρωτοκόλλου BOOTR, είναι πως το

πρώτο είναι πιο ευέλικτο όσον αφορά την επικοινωνία ανάμεσα στον DHCP client και στον DHCP server. Έτσι στο πρωτόκολλο DHCP αυτή η επικοινωνία πραγματοποιείται με τη χρήση επτά διαφορετικών τύπων μηνυμάτων σε αντίθεση με το πρωτόκολλο BOOTR το οποίο χρησιμοποιεί μόνο δύο τέτοια μηνύματα (request και reply).

Η λειτουργία του πρωτοκόλλου

Όταν ένας υπολογιστής συνδέεται στο δίκτυο, κάνει broadcast ένα ειδικό πλαίσιο ελέγχου (control frame) που ονομάζεται DHCPDISCOVER και έχει ως στόχο να εντοπίσει τους διαθέσιμους DHCP servers που είναι συνδεδεμένοι στο τοπικό δίκτυο. Όταν ο DHCP server λάβει ένα τέτοιο μήνυμα απαντάει με ένα μήνυμα που ονομάζεται DHCPOFFER και περιλαμβάνει την διεύθυνση IP το χρονικό πλαίσιο και τις υπόλοιπες παραμέτρους του δικτύου. Μετά τη λήψη της διεύθυνσης και των ρυθμίσεων ο κόμβος στέλνει ένα τελευταίο μήνυμα DHCPACK προκειμένου να ενημερώσει το δίκτυο για τις ρυθμίσεις που αποδέχτηκε. Σε ορισμένες περιπτώσεις ο DHCP server πριν αποδώσει την IP διεύθυνση στον DHCP client πραγματοποιεί έναν έλεγχο για να διαπιστώσει εάν αυτή η διεύθυνση χρησιμοποιείται ήδη από κάποιον άλλο υπολογιστή . Αυτός ο έλεγχος γίνεται με τη βοήθεια ειδικών πρωτοκόλλων όπως είναι το ARP (address resolution protocol) και το ICMP (interface control message protocol) .



Εικόνα 3: Αναπαράσταση του μηχανισμού DHCP

Όταν λοιπόν κάποιος υπολογιστής του εξωτερικού περιβάλλοντος επιθυμεί να επικοινωνήσει με τον δικό μας αποστέλλει το μήνυμα στον κεντρικό διακομιστή του τοπικού μας δικτύου ο οποίος αναλαμβάνει να το προωθήσει στον υπολογιστή μας με τη **MAC address** της κάρτας δικτύου που περιέχει . Από την παραπάνω περιγραφή είναι προφανές πως θα πρέπει να υπάρχει η δυνατότητα μετατροπής μιας IP διεύθυνσης κάποιου υπολογιστή στη MAC address της κάρτας δικτύου που περιέχει και αντίστροφα έτσι ώστε να είναι δυνατός ο παραπάνω τρόπος επικοινωνίας . Το σύνολο των κανόνων που καθιστούν δυνατή μια τέτοια μετατροπή ονομάζεται πρωτόκολλο ανάλυσης διευθύνσεων (address resolution protocol) , ενώ η εντολή που υλοποιεί τη λειτουργία του φέρει το όνομα ARP .

2.3.3 Address Resolution Protocol

Ο τρόπος που λειτουργεί το πρωτόκολλο ARP είναι εξαιρετικά απλός. Κάθε φορά που πρέπει να γίνει γνωστή η διεύθυνση MAC που αντιστοιχεί σε κάποια συγκεκριμένη διεύθυνση IP , λαμβάνει χώρα εκπομπή σε όλους τους υπολογιστές (broadcasting) ενός πακέτου δεδομένων που περιέχει τη διεύθυνση IP που θέλουμε να μεταφράσουμε . Ο κάθε ένας από τους υπολογιστές του δικτύου , παραλαμβάνει αυτό το πακέτο , συγκρίνει τη διεύθυνση IP που περιέχει , με τη δική του διεύθυνση IP και εάν οι δύο διευθύνσεις είναι οι ίδιες , αποστέλλει μια απάντηση στον υπολογιστή που υπέβαλλε το ερώτημα . Η απάντηση αυτή περιέχει τη MAC διεύθυνση του υπολογιστή αποστολέα η οποία ταχτοποιείται , απομονώνεται και αποθηκεύεται σε μια ειδική μνήμη ARP cache , έτσι ώστε να μπορεί να χρησιμοποιηθεί στο μέλλον . Η μνήμη αυτή ανανεώνεται σε τακτά χρονικά διαστήματα , διότι τα περιεχόμενα της μπορούν σε κάποια χρονική στιγμή να μεταβληθούν , όπως συμβαίνει για παράδειγμα σε περιπτώσεις κατά τις οποίες αντικαθιστούμε την κάρτα δικτύου του υπολογιστή με κάποια άλλη η οποία έχει τη δική της MAC address . Η εντολή arp καλείται στις πιο συνηθισμένες περιπτώσεις με την παράμετρο –a η οποία εμφανίζει τα περιεχόμενα του πίνακα arp (arp table) ο οποίος περιέχει την παραπάνω αντιστοιχία διευθύνσεων .

2.4 Routing

Στα δίκτυα υπολογιστών ο όρος δρομολόγηση αναφέρεται στη διαδικασία με την οποία επιλέγεται η διαδρομή μέσα σε ένα δίκτυο πάνω από την οποία θα σταλούν δεδομένα. Η δρομολόγηση κατευθύνει, προωθεί, το πέρασμα των λογικά διευθυνσιοδοτημένων πακέτων από την πηγή τους προς τον απόλυτο προορισμό τους μέσω ενδιάμεσων κόμβων (που λέγονται δρομολογητές). Η διαδικασία της δρομολόγησης κατευθύνει τα δεδομένα προωθώντας τα με βάση τους πίνακες δρομολόγησης που βρίσκονται στους δρομολογητές, οι οποίοι διατηρούν μια εγγραφή για την καλύτερη διαδρομή προς διάφορες κατευθύνσεις στο δίκτυο. Κατά συνέπεια η κατασκευή των πινάκων δρομολόγησης είναι πολύ σημαντική για αποτελεσματική δρομολόγηση. Η δρομολόγηση διαφέρει από τη γεφύρωση στην υπόθεσή της ότι οι δομές διευθύνσεων υπονοούν την εγγύτητα των παρόμοιων διευθύνσεων μέσα στο δίκτυο, επιτρέποντας κατά συνέπεια σε έναν πίνακα δρομολόγησης εισόδου, να αντιπροσωπεύσει τη

διαδρομή προς μια ομάδα διευθύνσεων. Για αυτό και η δρομολόγηση ξεπερνά τη γεφύρωση σε μεγάλα δίκτυα, και έχει γίνει βασικός τρόπος εύρεσης διαδρομής στο Internet. Σε μικρά δίκτυα οι πίνακες δρομολόγησης μπορούν να ορισθούν χειροκίνητα. Σε μεγάλα δίκτυα, όπου εμπλέκονται πολύπλοκες και διαρκώς μεταβαλλόμενες τοπολογίες, η χειροκίνητη κατασκευή των πινάκων δρομολόγησης είναι προβληματική. Εντούτοις, τα περισσότερα δημόσια τηλεφωνικά δίκτυα μεταγωγής (PSTN) χρησιμοποιούν προϋπολογισμένους πίνακες δρομολόγησης, με εφεδρικές διαδρομές αν η πιο σύντομη μπλοκαριστεί. Η δυναμική δρομολόγηση προσπαθεί να λύσει αυτό το πρόβλημα κατασκευάζοντας τους πίνακες δρομολόγησης αυτόματα, βασιζόμενη στις πληροφορίες που μεταφέρονται από τα πρωτόκολλα δρομολόγησης, και αφήνει το δίκτυο να ενεργεί σχεδόν αυτόνομα στο να αποφεύγει βλάβες και μπλοκαρίσματα.

Η δυναμική δρομολόγηση κυριαρχεί στο Internet. Εντούτοις όμως, η ρύθμιση των πρωτοκόλλων δρομολόγησης απαιτεί ικανότητες και δεν θα πρέπει κάποιος να υποθέσει ότι η τεχνολογία των δικτύων έχει εξελιχθεί μέχρι το σημείο της πλήρους αυτοματοποίησης της δρομολόγησης.

Τα δίκτυα μεταγωγής πακέτων όπως το Internet, χωρίζουν τα δεδομένα σε πακέτα που το καθένα περιέχει πληροφορίες για τον προορισμό του και δρομολογούνται ξεχωριστά. Τα δίκτυα μεταγωγής κυκλώματος όπως τα τηλεφωνικά δίκτυα, εκτελούν και αυτά δρομολόγηση, με σκοπό να βρουν διαδρομές για κυκλώματα (όπως τηλεφωνικές κλήσεις) πάνω από τις οποίες μπορούν να στείλουν μεγάλες ποσότητες δεδομένων χωρίς να επαναλαμβάνουν συνεχώς τη διεύθυνση του προορισμού. Το υλικό που χρησιμοποιείται στη δρομολόγηση περιλαμβάνει συγκεντρωτές, μεταγωγείς, και δρομολογητές.

2.4.1 Στατική δρομολόγηση

Η στατική δρομολόγηση αποτελεί την πιο απλή μορφή δρομολόγησης σε ένα δίκτυο. Ο διαχειριστής του δικτύου αποφασίζει για τους πίνακες δρομολόγησης και τους εφαρμόζει στους δρομολογητές. Οι πίνακες δρομολόγησης δεν ενημερώνονται στις αλλαγές κατάστασης του δικτύου εκτός και αν το κάνει ο διαχειριστής. Για τον λόγο αυτόν η στατική δρομολόγηση προτιμάται σε πολύ μικρά δίκτυα. Τέλος να προσθέσουμε ότι οι απ ευθείας συνδέσεις των δρομολογητών αποτελούν μέρος της στατικής δρομολόγησης.

Δρομολόγηση συντομότερης διαδρομής

Ο όρος 'συντομότερη' δεν αφορά απαραίτητα φυσική απόσταση, αλλά μπορεί να είναι οποιοδήποτε κριτήριο, το οποίο ποικίλει από υλοποίηση σε υλοποίηση. Σε κάποιο πρωτόκολλο δρομολόγησης μπορεί ένα κριτήριο απόστασης να είναι το πλήθος των αλμάτων από κόμβο σε κόμβο, η μέση καθυστέρηση μετάδοσης το εύρος ζώνης κλπ. Σε κάθε περίπτωση, υπολογίζονται (βάσει ενός κριτήριου) οι αποστάσεις από κάθε δρομολογητή προς τους γειτονικούς του. Δεδομένων των αποστάσεων μεταξύ γειτονικών δρομολογητών, μπορούν να χρησιμοποιηθούν διάφοροι αλγόριθμοι για τον υπολογισμό της συντομότερης διαδρομής μεταξύ δύο (όχι απαραίτητα γειτονικών)

δρομολογητών. Ο πιο γνωστός αλγόριθμος εύρεσης της συντομότερης διαδρομής είναι ο Dijkstra. Έτσι, κάθε δρομολογητής υπολογίζει τη συντομότερη διαδρομή προς κάθε προορισμό και βάσει αυτού αποφασίζει σε ποιον δρομολογητή να στείλει το πακέτο IP.

Δρομολόγηση πλημμύρας (flooding)

Σε έναν τέτοιο αλγόριθμο δρομολόγησης, κάθε εισερχόμενο πακέτο στέλνεται σε κάθε εξερχόμενη γραμμή εκτός από αυτή από την οποία έφτασε. Με τον τρόπο αυτό, δημιουργούνται άπειρα αντίγραφα του πακέτου και θα πρέπει να ληφθούν μέτρα για την ανακοπή της πλημμύρας. Ένα μέτρο είναι να περιέχεται ένας μετρητής αλμάτων στην κεφαλίδα κάθε πακέτου IP. Πρέπει όμως ο μετρητής αλμάτων να μην έχει τιμή μικρότερη από το πλήθος των αλμάτων που χρειάζονται για να φτάσει το πακέτο από την πηγή στον προορισμό. Για κάθε άλμα, ο μετρητής μειώνεται κατά ένα. Όταν μηδενιστεί, το πακέτο δεν θα αναμεταδοθεί, αλλά θα απορριφθεί.

2.4.2 Βασικές έννοιες της δυναμικής δρομολόγησης

Όταν συγκεκριμένη διαδρομή γίνει μη διαθέσιμη, οι υπάρχοντες κόμβοι πρέπει να αποφασίσουν μια εναλλακτική διαδρομή που θα χρησιμοποιήσουν για να στείλουν τα δεδομένα στον προορισμό τους. Συχνά το πετυχαίνουν αυτό χρησιμοποιώντας τα πρωτόκολλα δρομολόγησης που χρησιμοποιούν μία από τις δυο ευρείες κλάσεις αλγορίθμων δρομολόγησης: αλγορίθμους διανύσματος απόστασης και αλγορίθμους κατάστασης συνδέσμων, οι οποίες περιέχουν σχεδόν το κάθε αλγόριθμο δρομολόγησης που χρησιμοποιείται σήμερα στο internet.

2.4.2.1 Αλγόριθμοι distance vector

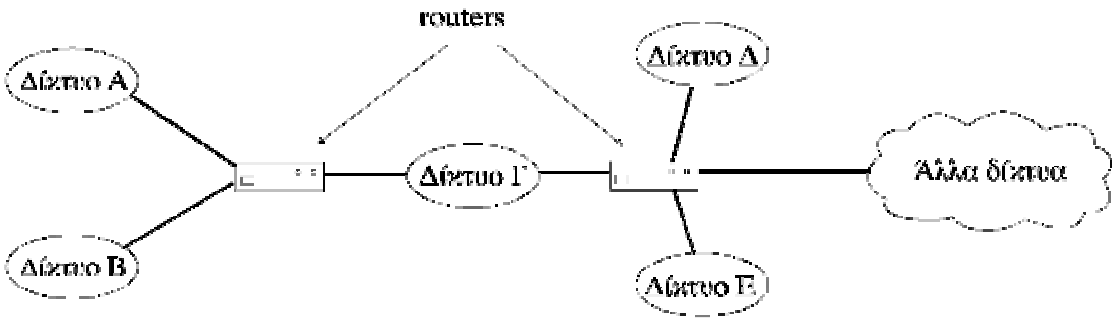
Οι αλγόριθμοι διανυσμάτων απόστασης' χρησιμοποιούν τον αλγόριθμο Bellman-Ford. Αυτή η διαδικασία αναθέτει έναν αριθμό, το κόστος, σε κάθε ένα από τις συνδέσεις μεταξύ των κόμβων σε ένα δίκτυο. Οι κόμβοι θα στέλνουν πληροφορίες από το σημείο Α στο σημείο Β μέσω της διαδρομής που έχει το μικρότερο συνολικό κόστος (δηλ. το αποτέλεσμα που βγαίνει από την άθροιση του κόστους μεταξύ των κόμβων που χρησιμοποιήθηκαν).

Ο αλγόριθμος λειτουργεί με πολύ απλό τρόπο. Όταν ξεκινάει ένας κόμβος ξέρει μόνο τους άμεσους γείτονές του, και το κόστος που εμπλέκεται ώστε να φτάσει σε αυτούς. (Αυτές οι πληροφορίες, η λίστα με τους προορισμούς, το εμπλεκόμενο κόστος για να φτάσει κανείς σε αυτόν, και στον επόμενο κόμβο (hop), σχηματίζουν τον πίνακα δρομολόγησης ή πίνακα αποστάσεων). Κάθε κόμβος, σε τακτικά χρονικά διαστήματα, στέλνει σε κάθε γείτονά του την δική του παρούσα αντίληψη για το κόστος που εμπλέκεται μέχρι να φτάσει σε όλους τους προορισμούς που του είναι γνωστοί. Οι γειτονικοί κόμβοι εξετάζουν αυτές τις πληροφορίες, τις συγκρίνουν με αυτές που ήδη 'ξέρουν'· ότι τους παρουσιάζει μια βελτίωση σε σχέση με αυτά που ήδη έχουν το εισάγουν στον δικό τους πίνακα δρομολόγησης. Με τον καιρό, όλοι οι κόμβοι του δικτύου θα ανακαλύπτουν το καλύτερο επόμενο βήμα (hop) για όλους τους προορισμούς και το καλύτερο συνολικό κόστος.

Ένα πρωτόκολλο που χρησιμοποιεί αλγόριθμο διανυσμάτων απόστασης είναι το RIP, το αρχικό εσωτερικό πρωτόκολλο πύλης δικτύου του Internet. Αργότερα, αντικαταστάθηκε από το OSPF, το οποίο αποτελεί υλοποίηση ενός αλγορίθμου κατάστασης συνδέσεων.

2.4.2.2 Αλγόριθμοι link state

Όταν εφαρμόζονται αλγόριθμοι κατάστασης συνδέσμων, ο κάθε κόμβος χρησιμοποιεί σαν αρχικά δεδομένα ένα χάρτη του δικτύου με την μορφή γράφου. Για να παραχθεί αυτός, κάθε κόμβος πλημμυρίζει ολόκληρο το δίκτυο με πληροφορίες σχετικά με το με ποιούς άλλους κόμβους μπορεί να συνδεθεί, εν συνεχεία κάθε κόμβος συγκεντρώνει όλες αυτές τις πληροφορίες και σχηματίζει έναν χάρτη. Χρησιμοποιώντας αυτό το χάρτη, κάθε δρομολογητής αποφασίζει ανεξάρτητα την καλύτερη διαδρομή από τον εαυτό του προς κάθε άλλο κόμβο. Ο αλγόριθμος που χρησιμοποιείται για να επιλεγεί η βέλτιστη διαδρομή, ο αλγόριθμος του Dijkstra, το κάνει αυτό δημιουργώντας μια δομή δεδομένων, ένα δέντρο, με τον τρέχοντα κόμβο σαν ρίζα του δέντρου, που περιέχει όλους τους υπόλοιπους κόμβους του δικτύου. Ξεκινάει με ένα δέντρο που περιέχει μόνο τον εαυτό του. Μετά, έναν ένα τη φορά, από το σύνολο των κόμβων που δεν έχουν προστεθεί στο δέντρο, προσθέτει τον κόμβο που έχει το μικρότερο κόστος για να φτάσει έναν γειτονικό κόμβο ο οποίος ήδη υπάρχει στο δέντρο. Αυτό συνεχίζεται μέχρις ότου όλοι οι κόμβοι να υπάρχουν στο δέντρο. Αυτό το δέντρο εξυπηρετεί στην κατασκευή του πίνακα δρομολόγησης του κάθε κόμβου, δείχνοντας το καλύτερο επόμενο βήμα (hop), για να φτάσει από τον εαυτό του σε οποιονδήποτε άλλο κόμβο στο δίκτυο.



Εικόνα 4 Παράδειγμα δικτύου

Η δουλειά των routers είναι να δρομολογούν τα πακέτα των δεδομένων μέσα από τα διάφορα δίκτυα που αποτελούν το Internet μέχρις ότου τα επιδώσουν στον προορισμό τους. Ας δούμε πώς γίνεται αυτό:

Ας θεωρήσουμε πάλι ότι ένας υπολογιστής που βρίσκεται κάπου στο Internet θέλει να στείλει δεδομένα σε κάποιον άλλον υπολογιστή. Τα δεδομένα κόβονται σε πακέτα και το IP που εκτελείται στον υπολογιστή - αποστολέα ετοιμάζεται να στείλει το κάθε πακέτο. Εισάγει λοιπόν στην επικεφαλίδα του πακέτου τις IP διευθύνσεις του αποστολέα και του παραλήπτη και κατόπιν, βάσει των διευθύνσεων αυτών, ελέγχει αν ο παραλήπτης βρίσκεται στο ίδιο δίκτυο με τον αποστολέα. Εάν ναι, το πακέτο στέλνεται κατευθείαν στον παραλήπτη χωρίς να χρειαστεί να διαβεί τα όρια του δικτύου. Εάν όχι, προωθείται στον router που είναι συνδεμένος με το δίκτυο. Ο router με τη σειρά του ελέγχει αν ο παραλήπτης βρίσκεται σε κάποιο από τα υπόλοιπα δίκτυα με τα οποία είναι συνδεδεμένος. Εάν ναι, το πακέτο στέλνεται κατευθείαν στον παραλήπτη στο δίκτυο αυτό. Εάν όχι, το πακέτο προωθείται στον επόμενο router, κ.ο.κ. μέχρις ότου το πακέτο προωθηθεί τελικά στον router που είναι συνδεδεμένος στο ίδιο δίκτυο με τον παραλήπτη. Το πακέτο μπορεί έτσι να περάσει από πολλούς routers μέχρις ότου φτάσει στον προορισμό του.

Οι routers διατηρούν πίνακες που προσδιορίζουν την κατεύθυνση που πρέπει να πάρει ένα πακέτο προκειμένου να φτάσει στον προορισμό του. Βάσει αυτών των πινάκων αποφασίζουν ποιος θα είναι ο επόμενος router στον οποίο θα πρέπει να προωθήσουν το πακέτο. Κάθε φορά, το πακέτο μετακινείται όλο και πιο κοντά προς τον προορισμό του έως ότου τελικά τον φτάσει. Ένα μεγάλο πλεονέκτημα αυτής της μεθόδου είναι ότι η διαδρομή που ακολουθεί ένα πακέτο δεν είναι προκαθορισμένη, αλλά επιλέγεται δυναμικά. Έτσι, οι routers μπορούν να επιλέγουν εναλλακτικούς δρόμους για ένα πακέτο σε περίπτωση που μια συγκεκριμένη σύνδεση του δικτύου παρουσιάζει πρόβλημα και βρίσκεται προσωρινά σε αχρηστία.

2.4.3 Network Address Translation

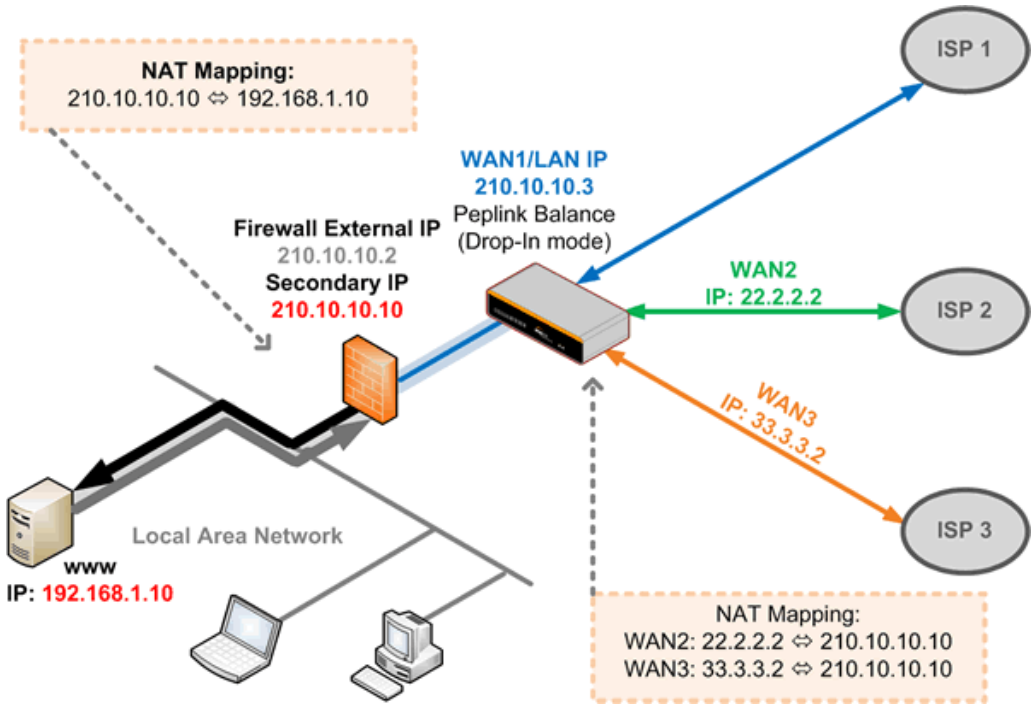
Όπως αναφέραμε πιο πάνω, κάθε υπολογιστής για να επικοινωνήσει μέσα σε ένα δίκτυο θα πρέπει να έχει μια μοναδική διεύθυνση IP. Επίσης είδαμε ότι το πρωτόκολλο TCP χρησιμοποιεί θύρες για να επικοινωνήσει. Η διεθυνσιοδότηση των κόμβων μέσα σε ένα δίκτυο δεν γίνεται αυθαίρετα αλλά βάσει κανόνων που ορίζονται στο RFC 1918 ενώ την εποπτεία για τις δημόσιες διευθύνσεις την έχει η IANA. Εκτός από τις δημόσιες διευθύνσεις ένα μέρος του εύρους των διευθύνσεων έχει κρατηθεί για την χρησιμοποίηση σε ιδιωτικά δίκτυα. Η χρήση των ιδιωτικών διευθύνσεων είναι ελεύθερη ενώ οι δημόσιες διευθύνσεις διατίθενται έναντι χρηματικού ποσού. Αξίζει επίσης να σημειωθεί ότι για τα ιδιωτικά δίκτυα υπάρχουν τρεις κλάσεις διευθύνσεων με το ανάλογο εύρος η καθεμία έτσι ώστε να εξυπηρετούνται δίκτυα διαφορετικού μεγέθους.

- 10.0.0.0 - 10.255.255.255 (Class A)
- 172.16.0.0 - 172.31.255.255 (Class B)
- 192.168.0.0 - 192.168.255.255 (Class C)

Είναι εύκολα κατανοητό ότι δύο ιδιωτικά δίκτυα μπορούν να χρησιμοποιούν το ίδιο εύρος ιδιωτικών διευθύνσεων χωρίς να αποτρέπει τους υπολογιστές τους να επικοινωνούν μέσω του διαδικτύου. Αυτό είναι απόλυτα θετικό – θα ήταν αδύνατον κάθε φορά που δημιουργούσαμε ένα τοπικό δίκτυο και αποδίδαμε διευθύνσεις στους υπολογιστές του, να εξετάζαμε αν σε κάποιο άλλο δίκτυο στον κόσμο υπάρχει κάποια κοινή διεύθυνση. Από την άλλη πλευρά όμως, αυτό το χαρακτηριστικό γίνεται μειονέκτημα όταν χρειαστεί να συνδεθούν δύο τέτοια δίκτυα – στο νέο μεγαλύτερο δίκτυο που δημιουργείται, είναι πιθανό να βρεθούν δύο υπολογιστές με την ίδια IP διεύθυνση - αυτό βέβαια δεν πρέπει να επιτραπεί να συμβεί. Το παραπάνω λοιπόν είναι ένα πρόβλημα που συναντά κανείς κατά τη διασύνδεση δύο τοπικών δικτύων με σκοπό την υλοποίηση ενός μεγαλύτερου VPN. Δύο είναι οι βασικοί τρόποι να αντιμετωπιστε: με χρήση proxy server ή με τον μηχανισμό NAT.

2.4.3.1 Τρόπος λειτουργίας

Το NAT είναι ένας μηχανισμός που υλοποιείται στις πύλες (gateways). Η λειτουργία του βασίζεται στην αλλαγή της διεύθυνσης IP στο αντίστοιχο πεδίο των πακέτων που στέλνει ένας κόμβος διαμέσου της πύλης.



Εικόνα 5: Γραφική απεικόνιση NAT

Πιο συγκεκριμένα, το NAT δουλεύει ως εξής: Κάθε υπολογιστής ενός ιδιωτικού δικτύου που ζητάει να συνδεθεί με κάποιον εκτός δικτύου, κάνει αίτηση στον Network Address Translator (που υπάρχει στην πύλη (gateway ή firewall)) για να πάρει μία νέα διεύθυνση. Ο NAT διαθέτει ένα σύνολο

διαθέσιμων IP διευθύνσεων («address pool») και μία από αυτές τις αναθέτει στον υπολογιστή. Ταυτόχρονα, κρατάει μία βάση δεδομένων στην οποία καταγράφει τη διεύθυνση που απέδωσε σε κάθε υπολογιστή (διαδικασία MAP). Έτσι, κάθε πακέτο που φεύγει από τον υπολογιστή του ιδιωτικού δικτύου και «ταξιδεύει» στο Internet έχει σαν διεύθυνση αποστολέα τη νέα αυτή διεύθυνση. Αντίστροφα, κάθε υπολογιστής που θέλει να στείλει δεδομένα στον συγκεκριμένο υπολογιστή του ιδιωτικού δικτύου, στέλνει πακέτα με διεύθυνση παραλήπτη τη νέα διεύθυνση. Ο NAT είναι πάλι υπεύθυνος σε αυτήν την περίπτωση για να παραλάβει ο υπολογιστής τα πακέτα που προορίζονται για αυτόν: συγκεκριμένα, ο NAT κοιτάει τη βάση δεδομένων και βλέπει ποια είναι η πραγματική IP διεύθυνση του υπολογιστή (δηλαδή η διεύθυνση που έχει στο ιδιωτικό του δίκτυο) και, με βάση αυτήν την πληροφορία, δρομολογεί τα εισερχόμενα πακέτα. Τα παραπάνω απεικονίζονται στο σχήμα – όπου η διαδικασία Exlude υποδηλώνει το γεγονός ότι κάποιες διευθύνσεις κάποιες φορές δεν χρειάζεται να αλλάξουν (να «μεταγλωττιστούν») σε κάποια άλλη (π.χ. αν αντιστοιχούν σε κάποιον mail server).

Στο παρακάτω παράδειγμα εξηγείται αναλυτικά το NAT

Στάδιο 1. Ένας υπολογιστής εντός ιδιωτικού δικτύου με διεύθυνση 10.0.0.3 θέλει να συνδεθεί με ένα απομακρυσμένο υπολογιστή (server – π.χ ένας ftp server) που έχει διεύθυνση 128.32.32.68. Παρακολουθούμε τα πεδία από το TCP/IP πλαίσιο που μας ενδιαφέρουν: τα SADDR, DADDR είναι οι διευθύνσεις αποστολέα και προορισμού αντίστοιχα. Τα SPORT, DPORT είναι οι TCP θύρες αποστολέα και προορισμού αντίστοιχα και σχετίζονται κυρίως με την εφαρμογή που αιτείται ο χρήστης (τα νούμερα στο σχήμα είναι τυχαία). Το CKSUM είναι το πεδίο εκείνο του TPC/IP πλαισίου που υπολογίζεται με σκοπό την ανίχνευση σφάλματος – δηλαδή εκτελεί μια συνάρτηση κατακερματισμού πάνω σε όλο το υπόλοιπο πακέτο και η τιμή που υπολογίζεται είναι αυτή που μπαίνει στο CHKSUM (επίσης τυχαία η τιμή που αναγράφεται στο σχήμα).

Στάδιο 2. Ο NAT μεταβάλλει τη διεύθυνση του υπολογιστή. Στο συγκεκριμένο παράδειγμα την κάνει 24.1.70.210 (οπότε και αλλάζει η τιμή του πεδίου SADDR στο TCP/IP πακέτο). Αντίστοιχα αλλάζει και η τιμή του SPORT (επίσης τυχαία η τιμή του σχήματος), ενώ προφανώς, αφού 2 πεδία του πακέτου έχουν μεταβληθεί, αναγκαστικά θα αλλάξει και η τιμή του CKSUM. Ταυτόχρονα, ο NAT ενημερώνει τον πίνακά του σχετικά με την αλλαγή στη IP διεύθυνση που πραγματοποίησε (διαδικασία MAP, όπως αναφέρθηκε νωρίτερα). Η νέα καταχώρηση που τοποθετείται στον πίνακα περιέχει την αρχική IP διεύθυνση και TCP θύρα του υπολογιστή, την IP διεύθυνση και TCP θύρα του υπολογιστή-προορισμού, καθώς και την TPC θύρα του NAT.

Στάδιο 3. Παρατηρούμε τώρα το TCP/IP πακέτο-απάντηση που στέλνει ο απομακρυσμένος υπολογιστής. Προφανώς, η τιμή του SADDR είναι η διεύθυνση του υπολογιστή αυτού – δηλαδή 128.32.32.68. Η τιμή του DADDR είναι η διεύθυνση του αρχικού υπολογιστή που «βλέπει» ο 128.32.32.68 – δηλαδή, η νέα διεύθυνση 24.1.70.210. Οι τιμές του SPORT και DPORT είναι προφανώς 80 και 40960 – δηλαδή, εναλλάσσονται οι αντίστοιχες τιμές του πακέτου που είχαμε στο

στάδιο 2. Και, τέλος, επισημαίνεται ότι φυσικά η τιμή του CKSUM είναι διαφορετική από όλες τις προηγούμενες (αφού το εν λόγω IP πακέτο δεν είναι ίδιο με κανένα από τα προηγούμενα).

Στάδιο 4. Ο NAT κοιτάει το πακέτο που λαμβάνει (αυτό του σταδίου 3) και ψάχνει τον πίνακά του να βρει καταχώρηση που να έχει ως NAT θύρα τη 40960 (δηλαδή το DPORT του πακέτου που έλαβε), ως διεύθυνση προορισμού την 128.32.32.68 (που είναι η SADDR του πακέτου που έλαβε) και ως θύρα προορισμού την 80. Στο συγκεκριμένο παράδειγμα βρίσκει την καταχώρηση, η οποία σαν διεύθυνση και TCP θύρα αποστολέα έχει τις 10.0.0.3 και 1049 αντίστοιχα. Άρα, ξέρει σε ποιον υπολογιστή εντός του ιδιωτικού δικτύου να προωθήσει το πακέτο. Προσέξτε τα πεδία του προωθημένου αυτού πακέτου: πρέπει ο ο υπολογιστής 10.0.0.3 να μην αντιλαμβάνεται τον NAT, συνεπώς δεν φαίνεται πουθενά ούτε η διεύθυνση που απέδωσε ο NAT ούτε η θύρα του. Με άλλο λόγια, οι τιμές των πεδίων του πακέτου 4 είναι οι αντίστροφες αυτών του σταδίου 1 (δηλαδή η DADDR του σταδίου 1 γίνεται SADDR του σταδίου 4 κ.ο.κ). Και, βέβαια, πάλι έχουμε μια διαφορετική τιμή του CKSUM, σε σχέση με όλες τις προηγούμενες.

Όταν σε έναν υπολογιστή ανατίθεται πάντα μία νέα συγκεκριμένη IP διεύθυνση, μιλάμε για στατική μεταγλώττιση διεύθυνσης – διαφορετικά, αν κάθε φορά του αποδίδεται διαφορετική διεύθυνση, τότε αναφερόμαστε σε δυναμική μεταγλώττιση (που είναι και η συνηθέστερη περίπτωση). Πρέπει να σημειωθεί ότι το NAT, όπως περιγράφηκε παραπάνω, έχει τον ίδιο περιορισμό με τον Proxy server ως προς το ότι λειτουργεί μόνο πάνω σε TCP.

2.4.3.2 Port Forward

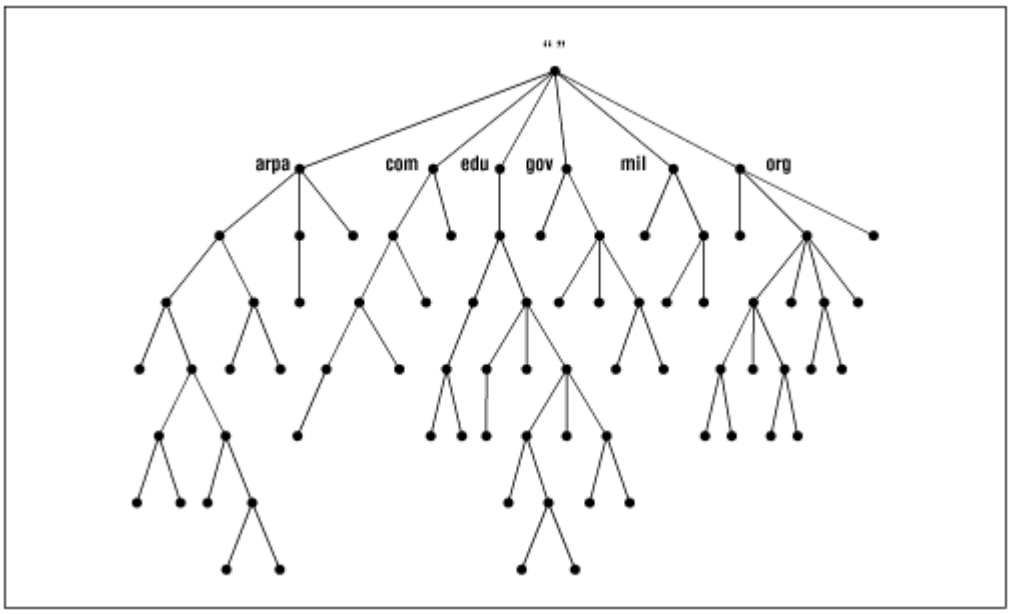
Η τεχνική port forward επιτρέπει την κοινή χρήση μιας δημόσιας διεύθυνσης IP από μια ομάδα υπολογιστών εντός ενός ιδιωτικού δικτύου. Μέσω του DHCP ορίζετε σε κάθε ηλεκτρονικό υπολογιστή του τοπικού δικτύου μια διαφορετική εσωτερική διεύθυνση IP, της μορφής 192.168.x.x ή 10.1.x.x και με το NAT μια κοινή εξωτερική IP με την οποία αναγνωρίζονται από άλλα συστήματα συνδεμένα στο Internet. Το NAT βρίσκει εφαρμογή σε ιδιωτικά και εταιρικά δίκτυα που συνδέονται στο Internet μέσω routers και συνδέσεων ADSL ή μισθωμένων γραμμών. Πολλές φορές ο διαχειριστής των δικτύων αυτών θα πρέπει να ρυθμίσει κατάλληλα τους κανόνες NAT, ώστε να είναι εφικτή η πρόσβαση από το Internet σε υπηρεσίες και εφαρμογές που εκτελούνται σε συγκεκριμένο υπολογιστή του εσωτερικού δικτύου. Η ρύθμιση αυτή ονομάζεται και port forwarding. Επειδή όλοι οι ηλεκτρονικοί υπολογιστές εμφανίζονται στο διαδίκτυο με την ίδια διεύθυνση IP, ένας κανόνας NAT ή port forwarding καθορίζει σε ποιον από όλους θα πρέπει να αναζητηθεί μια συγκεκριμένη υπηρεσία. Αυτό γίνεται με την αντιστοίχηση του port της εν λόγω υπηρεσίας (π.χ. port 80 για HTTP server) στην εσωτερική διεύθυνση του υπολογιστή του τοπικού δικτύου όπου αυτή εκτελείται. Η υπηρεσία UPnP (Universal Plug and Play) που υποστηρίζεται σήμερα από πολλές εφαρμογές, λειτουργικά συστήματα και routers έχει περιορίσει σημαντικά την ανάγκη καθορισμού κανόνων NAT, χωρίς όμως να την έχει

εξαλείψει πλήρως. Είναι σημαντικό να αναφέρουμε ότι σε εταιρικά δίκτυα η υπηρεσία UPnP θα πρέπει να απενεργοποιείται καθώς μπορεί να χρησιμοποιηθεί από κακόβουλο λογισμικό και να δημιουργήσει ζητήματα ασφαλείας (Whittaker, 2013).

Η μεγάλη διάδοση των δικτύων υπολογιστών τα τελευταία χρόνια , έκανε επιτακτική την ανάγκη δημιουργίας μιας διαφορετικής μορφής διευθύνσεων οι οποίες να είναι πιο εύκολες στη χρήση τους. Είναι πολύ πιο δύσκολο για κάποιον να απομνημονεύσει μια διεύθυνση της μορφής 83.212.116.13 , όλοι όμως μπορούν να μάθουν τη διεύθυνση www.hotplug.gr.Για αυτό το λόγο πολύ σπάνια χρησιμοποιούμε τη διεύθυνση IP στη δεκαδική της μορφή και σχεδόν πάντοτε επικοινωνούμε με τους άλλους υπολογιστές δίνοντας μια συμβολική διεύθυνση που είναι πιο εύκολο να απομνημονευθεί . Το πρωτόκολλο IP φυσικά δε γνωρίζει τίποτα για αυτές τις συμβολικές διευθύνσεις και χρησιμοποιεί για τη λειτουργία του τις δεκαδικές διευθύνσεις IP . Θα πρέπει λοιπόν να υπάρχει ένας μηχανισμός, ο οποίος να δέχεται ως είσοδο τη συμβολική διεύθυνση του υπολογιστή στον οποίο θέλουμε να συνδεθούμε και να τη μεταφράζει στην αντίστοιχη δεκαδική διεύθυνση και αντίστροφα. Ο μηχανισμός αυτός είναι γνωστός με το όνομα Domain Name Service (DNS). Πως είναι δυνατόν ο μηχανισμός DNS γνωρίζει ποια είναι η συμβολική διεύθυνση που αντιστοιχεί σε κάποια διεύθυνση IP. Η απάντηση είναι ότι υπάρχουν διασκορπισμένες σε όλο τον κόσμο τεράστιες βάσεις δεδομένων, οι οποίες περιέχουν ζεύγη της μορφής (συμβολική διεύθυνση – πραγματική διεύθυνση). Όταν λοιπόν ο μηχανισμός DNS δέχεται ως είσοδο κάποια διεύθυνση IP, συνδέεται σε κάποια από αυτές τις βάσεις, αναζητά σε αυτή το ζεύγος που περιλαμβάνει τη διεύθυνση IP που του έχει δοθεί και εμφανίζει την αντίστοιχη συμβολική διεύθυνση. Το ίδιο ακριβώς συμβαίνει και κατά τη μετάφραση μιας συμβολικής διεύθυνσης σε διεύθυνση IP. Οι τεράστιες αυτές αποθηκευμένες σε ειδικούς υπολογιστές με αποθηκευτικές διατάξεις μεγάλης χωρητικότητας οι οποίοι ονομάζονται DNS servers. Ως υπολογιστές του δικτύου θα έχουν και αυτοί τη δική τους διεύθυνση IP η οποία επομένως θα πρέπει να δηλωθεί στο λειτουργικό σύστημα , προκειμένου αυτό να γνωρίζει που να αναζητεί αυτούς τους υπολογιστές έτσι ώστε να συνδεθεί μαζί τους. Συνήθως καθορίζουμε δύο ή περισσότερες τέτοιες διευθύνσεις (primary DNS και secondary DNS) έτσι ώστε όταν ο ένας από τους υπολογιστές αυτούς δε μπορεί να μας εξυπηρετήσει για κάποιο λόγο να απευθυνόμαστε σε κάποιον άλλο υπολογιστή. Με άλλα λόγια θα μπορούσαμε να πούμε ότι το Domain Name Service αποτελεί μια υπηρεσία μετάφρασης μεταξύ ονομάτων και IP διευθύνσεων στο Internet. Κάθε δρομολογητής και κάθε υπολογιστής στο Internet διαθέτει ένα όνομα Η ιεραρχία ονομάτων περιλαμβάνει ονόματα υπολογιστών, εταιριών, δικτύων χωρών ή και ευρύτερων περιοχών (domain) . Για παράδειγμα το υποθετικό όνομα του εταιρικού δικτύου ouranos.hotplug.gr ακολουθεί την ιεραρχία της εταιρίας (ouranos), του δικτύου που την εξυπηρετεί (hotplug) και της ευρύτερης περιοχής (gr). Το τελευταίο συστατικό του ονόματος χαρακτηρίζει το υψηλότερο επίπεδο ομαδοποίησης που διακρίνεται σε δύο μεγάλες κατηγορίες, **τα γενικού τύπου domain** και τα **γεωγραφικά**. Τα γενικού τύπου domain είναι:

- Com (commercial – εμπορικά)

- Edu (educational – ακαδημαϊκά)
- Org (organizational – οργανισμοί μη κερδοσκοπικού χαρακτήρα)
- Net (network providers – πάροχοι δικτύου)
- Mil (military – κυρίες Αμερικάνικες στρατιωτικές υπηρεσίες)
- Gov (government – Αμερικάνικες κυβερνητικές υπηρεσίες)
- Int (international – διεθνείς οργανισμοί)



Εικόνα 6: Domain name tree

Σε ένα δίκτυο που εξυπηρετεί αρκετούς υπολογιστές κάτω από το ίδιο όνομα δικτύου πρέπει να λειτουργεί ένας DNS server που θα δίνει τη διεύθυνση του προς τον DNS server του αμέσως ανώτερου επιπέδου. Αυτό επαναλαμβάνεται έως ότου καλυφθεί ολόκληρη η ιεραρχία ονομάτων. Οι διάφορες εφαρμογές στο διαδίκτυο όπως FTP, SMTP, Telnet ή www για να εντοπίσουν μια διεύθυνση απευθύνουν ένα ερώτημα προς τον DNS server ο οποίος είτε δίνει την απάντηση από τους πίνακες καταχωρήσεων που διαθέτει είτε παραπέμπει προς τη διεύθυνση του DNS server που έχει την απάντηση . Εάν ο ίδιος ο DNS server δώσει την απάντηση , αυτή μπορεί να προέρχεται είτε από τους δικούς του πίνακες καταχωρήσεων είτε από άλλους DNS servers που ψάχνει για λογαριασμό της εφαρμογής .

Κεφάλαιο 3

Voice over IP

3 Voice over IP

3.1 Εισαγωγή

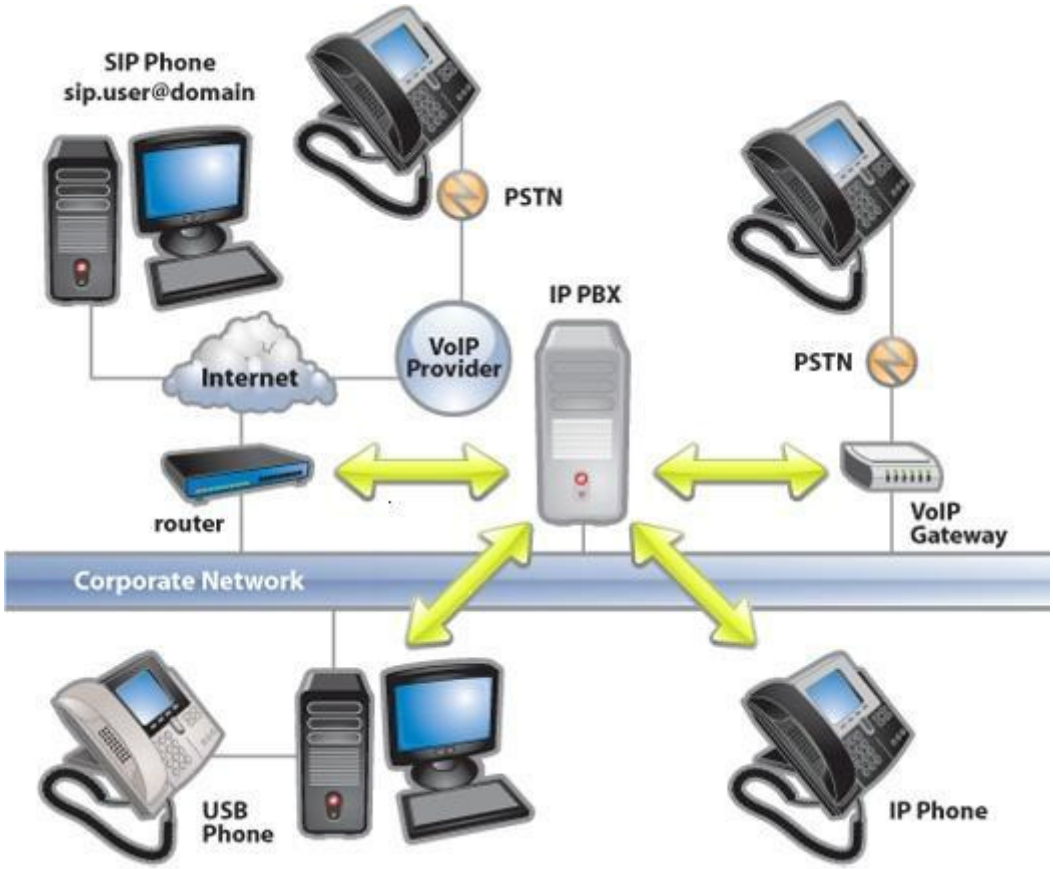
Η τεχνολογία Voice over Internet Protocol (VoIP) επιτρέπει τη μετάδοση φωνής μέσω IP δικτύων, αλλά και το Διαδίκτυο (internet). Το VoIP αλλάζει σταδιακά τον τρόπο με τον οποίο επικοινωνούμε, αντικαθιστώντας σιγά σιγά την παραδοσιακή τηλεφωνία. Υπάρχουν πολλοί τρόποι ώστε να υλοποιηθεί ένα VoIP δίκτυο. Μπορεί να δομηθεί πάνω σε οποιοδήποτε IP-based δίκτυο όπως LAN, WLAN, WAN, ή το διαδίκτυο. Ακόμη και τα δίκτυα κινητής τηλεφωνίας νέας γενιάς έχουν ήδη ξεκινήσει δειλά να μεταφέρουν VoIP κίνηση, χάρη στην εκμετάλλευση των δυνατοτήτων των «έξυπνων» συσκευών και των αντίστοιχων υπηρεσιών internet που προσφέρουν οι πάροχοι κινητής τηλεφωνίας. Ένα VoIP δίκτυο μπορεί επίσης να διασυνδεθεί με τα PSTN (Public Switched Telephone Network) δίκτυα (συμπεριλαμβανομένων των δικτύων κινητής τηλεφωνίας). Τα στοιχεία και εν γένει ο εξοπλισμός που μπορούν να χρησιμοποιηθούν σε ένα δίκτυο VoIP είναι ποικίλα, όπως συμβατικά τηλέφωνα, ATA, Gateways, Gatekeepers, PBX, VoIP phones (IP phones – Softphones):

- ATA (Analog Telephone Adapter): είναι η συσκευή μέσω της οποίας μια συμβατική τηλεφωνική συσκευή μπορεί να συνδεθεί σε ένα VoIP δίκτυο. Μετατρέπει το αναλογικό σήμα του τηλεφώνου σε μορφή κατάλληλη για χρήση σε VoIP δίκτυα και αντίστροφα. Πρακτικά, ένα συμβατικό τηλέφωνο με ένα ATA είναι ίδιο λειτουργικά με ένα VoIP Hardphone. Το ATA ορισμένες φορές αναφέρεται γενικά και ως gateway.

- VoIP gateway: είναι συσκευή ανάλογη με τους IP Gateways που συνδέει συμβατικά τηλεφωνικά δίκτυα (πχ. PSTN, GSM) και συσκευές, με VoIP δίκτυα και αντίστροφα.

- VoIP Gatekeeper: είναι ένα πολύ χρήσιμο αλλά προαιρετικό στοιχείο ενός δικτύου

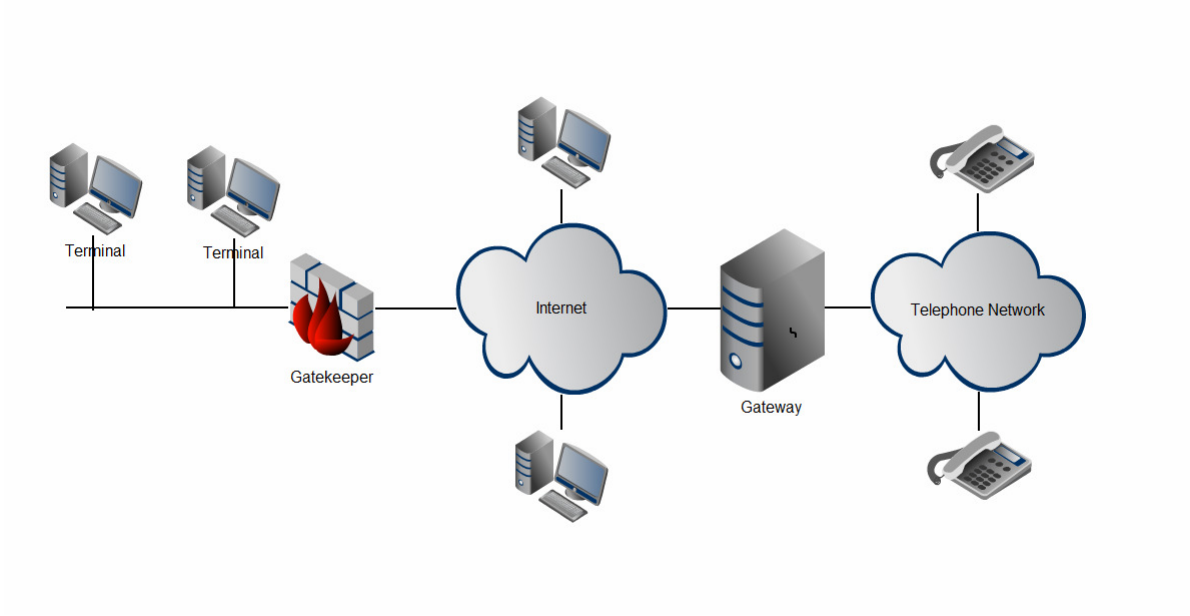
- VoIP. Συνήθως βρίσκεται σε VoIP υλοποιήσεις όπου χρησιμοποιούν το πρωτόκολλο H.323. Παρέχει υπηρεσίες, όπως δρομολόγηση και έλεγχο πρόσβασης στο δίκτυο για τερματικά H.323, gateways και MCUs (Multipoint Control Units). Επίσης μπορεί να παρέχει άλλες υπηρεσίες όπως διαχείριση εύρους ζώνης, κοστολόγηση, καθώς επίσης και πλάνα κλήσεων (dial plans). Οι gatekeepers είναι «λογικά» διαχωρισμένοι από τα τερματικά, τα οποία επιβάλλεται να χρησιμοποιούν τις υπηρεσίες τους, εάν αυτοί υπάρχουν. Ένας gatekeeper και τα τερματικά που διαχειρίζεται, αποτελούν μια ζώνη, η οποία μπορεί να εξυπηρετείται από έναν μόνο gatekeeper ανά πάσα στιγμή.



Εικόνα 7 Ενδεικτικό VoIP δίκτυο

3.2 H.323

Το H323 είναι ένα σύνολο προτύπων από την ITU-T και ορίζει ένα σύνολο πρωτοκόλλων για την παροχή οπτικοακουστικής επικοινωνίας. Αναπτύχθηκε το 1996 με τη σύσταση H.323 της ITU με τίτλο «Συστήματα και εξοπλισμός οπτικής τηλεφωνίας για δίκτυα τοπικής περιοχής που παρέχουν μη εγγυημένη ποιότητα υπηρεσιών ". Το πρωτόκολλο αναθεωρήθηκε το 1998 και ήταν η βάση για τα πρώτα συστήματα τηλεφωνίας μέσω του διαδικτύου. Το H.323 αποτελεί αρχιτεκτονική επισκόπηση της τηλεφωνίας παρά ένα πρωτόκολλο επικοινωνίας. Αναφέρεται σε μεγάλο πλήθος συγκεκριμένων πρωτοκόλλων για την κωδικοποίηση φωνής, εγκαθίδρυση κλήσεων, σηματοδοσία, μεταφορά δεδομένων, και άλλα θέματα αντί να προδιαγράφει αυτό τα αντίστοιχα ζητήματα. Στην εικόνα που ακολουθεί φαίνεται το γενικό μοντέλο λειτουργίας του H.323.



Εικόνα 8 Μοντέλο λειτουργίας του H.323

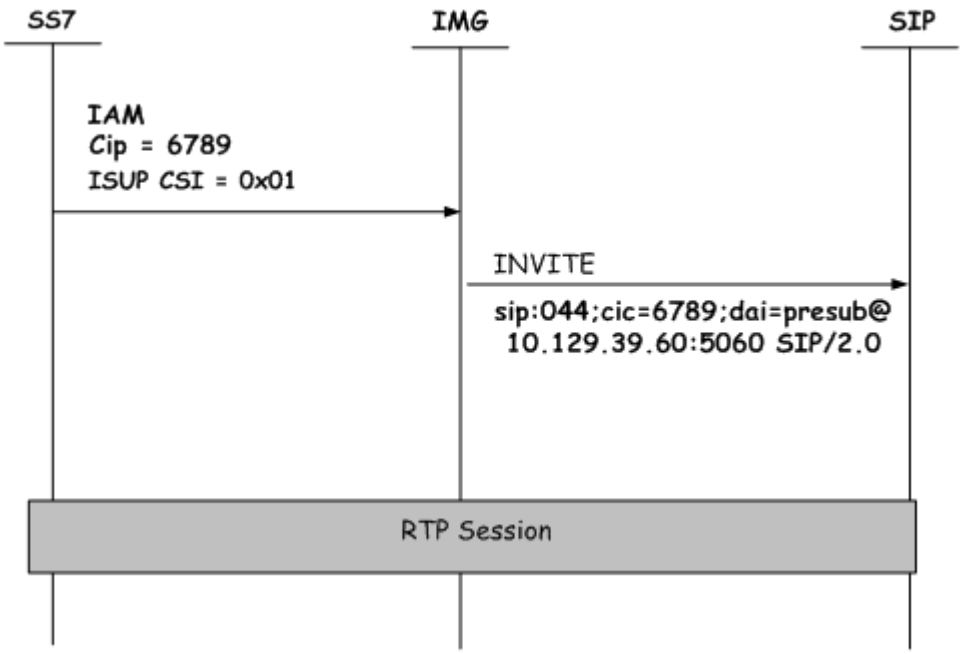
Στο κέντρο βρίσκεται το gateway και συνδέει τον παγκόσμιο ιστό με το τηλεφωνικό δίκτυο. Το gateway επικοινωνεί με τις τερματικές συσκευές χρησιμοποιώντας το H.323 ενώ με τις τηλεφωνικές συσκευές χρησιμοποιώντας τα πρωτόκολλα του PSTN. Όλα τα συστήματα H.323 πρέπει να υποστηρίζουν τον G.711 για την κωδικοποίηση φωνής ενώ δίνεται η δυνατότητα να χρησιμοποιηθούν κι άλλοι αλγόριθμοι. Ένα βασικό μειονέκτημα του H.323 είναι η απουσία ελέγχου ποιότητας υπηρεσίας(QoS) η οποία θα πρέπει να υλοποιηθεί από το επίπεδο δικτύου.

3.3 Session initiation protocol

Το SIP είναι πρωτόκολλο σηματοδοσίας, το οποίο άνοιξε το δρόμο για τη ταχύτατη ανάπτυξη του VoIP και εφαρμογών πολυμέσων. Επειδή η κοινότητα του Internet θεωρούσε ότι το H.323 δεν είναι παρά ένα προϊόν των εταιριών τηλεφωνίας, η IETF (Internet Engineering Task Force) ανέπτυξε το πρωτόκολλο SIP το οποίο περιγράφεται στο RFC2543 του 1999. Το μεγάλο ενδιαφέρον και η απήχηση που είχε το νέο αυτό πρωτόκολλο, τόσο ερευνητικά όσο και εμπορικά, οδήγησε στη δημιουργία της δεύτερης έκδοσής του, SIPv2 το 2002, με την αντίστοιχη δημοσίευση RFC3261, η οποία περιλαμβάνει βελτιώσεις και επιπλέον διευκρινίσεις σε σχέση με την προηγούμενη. Το SIP περιγράφει πως εγκαθιδρύονται τηλεφωνικές κλήσεις, βιντεοδιασκέψεις και άλλες συνδέσει πολυμέσων μέσω του διαδικτύου. Σε αντίθεση με το προγενέστερο H.323 το SIP έχει σχεδιαστεί για να παρέχει λειτουργικότητα με τις υπάρχουσες εφαρμογές του internet. Για παράδειγμα ορίζει του τηλεφωνικούς αριθμούς με την μορφή URL έτσι ώστε να μπορούν να εμπεριέχονται σε ιστοσελίδες επιτρέποντας έτσι την πραγματοποίηση κλήσεων με ένα κλικ.

Το SIP μπορεί να εγκαθιδρύσει συνδιαλέξει 2μερών συνδιαλέξεις πολλών μερών και συνδιαλέξεις multicast(ένας αποστολέας πολλοί παραλήπτες). Το SIP δεν περιορίζεται μόνο στον ήχο και το βίντεο καθώς μπορεί να χρησιμοποιηθεί και για δεδομένα καθιστώντας το ικανό για την χρήση από Online-

games. Το πρωτόκολλο SIP σχεδιάστηκε αμιγώς ως πρωτόκολλο σηματοδοσίας ενώ ενσωματώνει στοιχεία του HTTP (Hyper Text Transfer Protocol) και του SMTP (Simple Mail Transfer Protocol). Η "client - server" αρχιτεκτονική και η χρήση URLs(URI στο SIP) είναι χαρακτηριστικά που υιοθέτησε από το HTTP, ενώ από το SMTP, δανείστηκε τη μορφή κειμένου (text-encoding style) και τη μορφή των κεφαλίδων (headers).



Εικόνα 9 Παράδειγμα URI

Το SIP σαν πρωτόκολλο ανήκει στο «επίπεδο εφαρμογής και χρησιμοποιείται για τον έλεγχο (Δημιουργία/ Τροποποίηση/ Τερματισμό) unicast/multicast συνόδων επικοινωνίας. Η τροποποίηση μπορεί να περιλαμβάνει αλλαγή διευθύνσεων και θυρών, την πρόσκληση επιπλέον συμμετεχόντων, την προσθήκη η αφαίρεση φορέων ροής δεδομένων, την αλλαγή του τρόπου κωδικοποίησης , κ.α. Είναι σχεδιασμένο έτσι ώστε να είναι ανεξάρτητο από το επίπεδο μεταφοράς , και έτσι μπορεί να υλοποιηθεί με χρήση TCP,UDP ή SCTP (Stream Control Transmission Protocol). Μια βασική λειτουργία του SIP είναι η δυνατότητα διαπραγμάτευσης των παραμέτρων της συνόδου, έτσι ώστε όλοι οι συμμετέχοντες να ενημερώνονται και να «συμφωνούν» για τα βασικά χαρακτηριστικά της επικοινωνίας, όπως για παράδειγμα τον κωδικοποιητή (codecs) ήχου που θα χρησιμοποιηθεί, την θύρα επικοινωνίας, κ.α. Η περιγραφή, ωστόσο, όλων αυτών των παραμέτρων μιας VoIP κλήσης, δεν μπορεί να πραγματοποιηθεί άμεσα από το SIP, και για το λόγο αυτό, το SIP κάνει χρήση SDP(Session Description Protocol) για τον προσδιορισμό των παραμέτρων της συνόδου. Αφού εγκατασταθεί μια σύνοδος μέσω SIP οι ροές δεδομένων (μετάδοση πακέτων φωνής στην περίπτωση του VoIP) μεταφέρονται χρησιμοποιώντας RTP πάνω από UDP πρωτόκολλο.

3.3.1 Οι οντότητες του SIP

SIP Proxy Servers

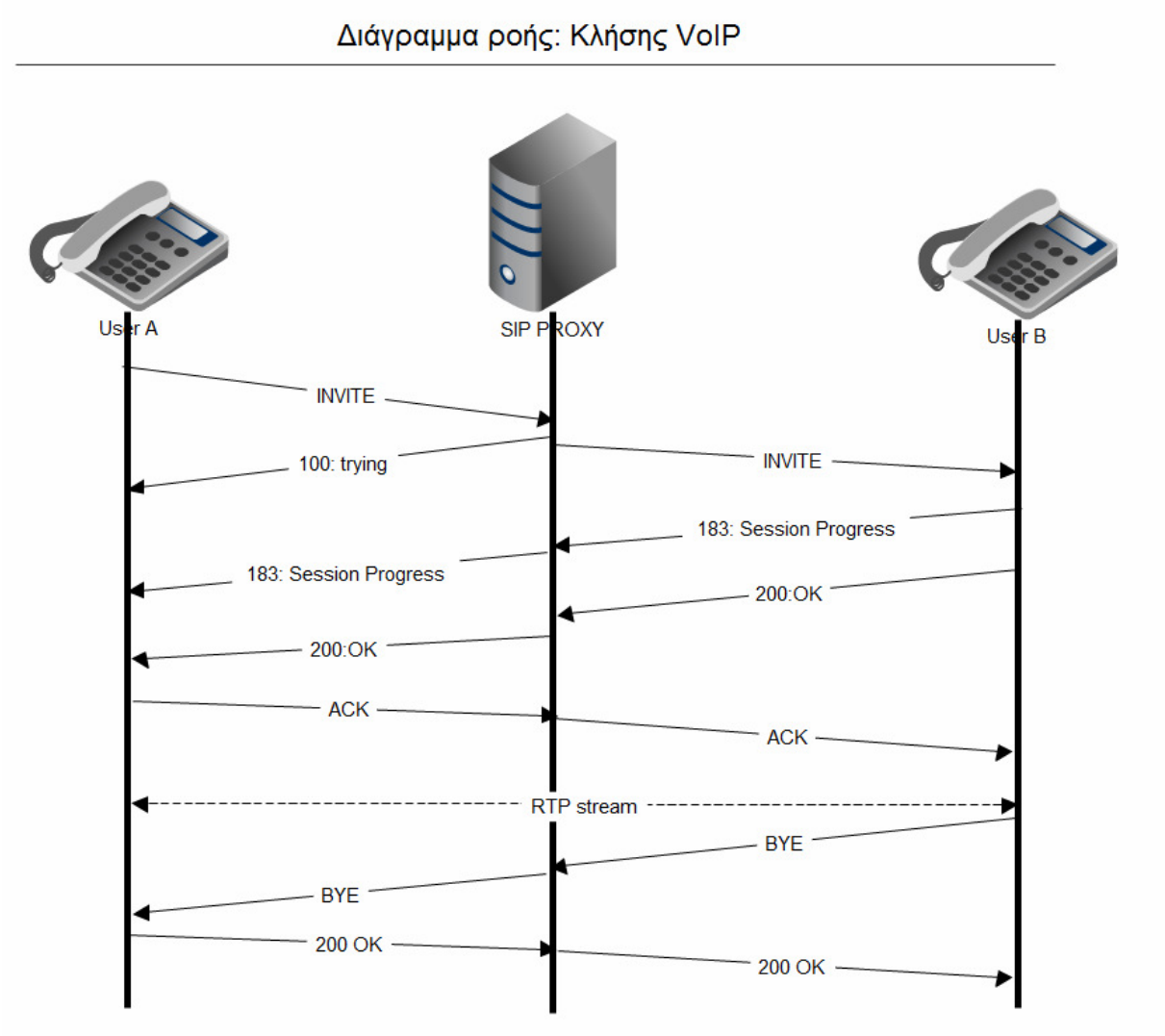
Οι SIP Proxy Servers είναι το λογισμικό που εκτελείται από τους κεντρικούς κόμβους ενός VoIP δικτύου και αποδέχεται τα requests που υποβάλλονται από τους SIP UAs (UAC) για εγκατάσταση επικοινωνίας. Όταν οι SIP Proxy Servers λαμβάνουν ένα τέτοιο SIP request από ένα χρήστη, αρχικά επικοινωνούν με τον SIP Registrar Server για να λάβουν πληροφορία για την τρέχουσα θέση του χρήστη που καλείται. Στην περίπτωση που ο χρήστης αυτός εντοπιστεί τότε το SIP request προωθείται στον UAS του χρήστη, αλλιώς το SIP request προωθείται στον επόμενο κόμβο SIP Proxy Server. Εάν ο χρήστης που καλείται δεν βρεθεί μετά από έναν αριθμό προσπαθειών, τότε ο SIP Proxy Server απαντά κατάλληλα, αποστέλλοντας ένα SIP response, στον αρχικό χρήστη που έστειλε το αίτημα για επικοινωνία. Ένας SIP Proxy Server ερμηνεύει και εάν είναι απαραίτητο, τροποποιεί ένα SIP request πριν το αποστείλει στον αντίστοιχο SIP UA ή σε άλλον SIP Proxy Server.

SIP Redirect Server

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

SIP Registrar Server

Ένας SIP Registrar Server αποδέχεται REGISTER requests και δημιουργεί εγγραφές που αντιστοιχούν στις λογικές διευθύνσεις των χρηστών του domain για το οποίο είναι υπεύθυνοι, με φυσικές διευθύνσεις της τρέχουσας θέσεις τους. Για παράδειγμα, η λογική διεύθυνση sip:user@hotplug.gr του χρήστη user, αντιστοιχείται για παράδειγμα στη φυσική διεύθυνση sip:user@83.212.116.13, η οποία περιέχει πληροφορία για την τρέχουσα θέση του. Οι SIP Registrar Servers δημιουργούν βάσεις δεδομένων με τέτοιες εγγραφές για όλους τους ενεργούς χρήστες (UAs) του domain τους. Κατά την διάρκεια εγκατάστασης μιας κλήσης ο SIP Registrar Server ανακτά Μελέτη και υλοποίηση συστήματος τηλεφωνίας μέσω διαδικτύου (VoIP) και στέλνει την τρέχουσα φυσική διεύθυνση του καλούμενου χρήστη στον SIP Proxy Server για την κατάλληλη προώθηση του αρχικού SIP request. Να σημειωθεί εδώ, ότι ο διαχωρισμός ανάμεσα στους SIP servers είναι λογικός, και όχι φυσικός, μιας και οι λειτουργίες των UAS εκτελούνται συνήθως από τον ίδιο server.

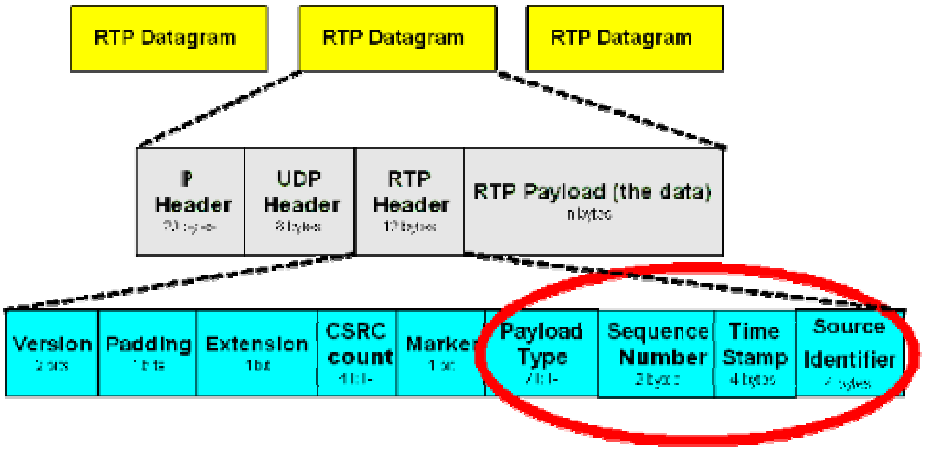


Εικόνα 10: Ανταλλαγή μηνυμάτων SIP.

3.4 Real time protocol

Οι εφαρμογές πολυμέσων χαρακτηρίζονται από αυστηρούς χρονικούς περιορισμούς στη μετάδοση των δεδομένων, κάτι που δε λαμβάνουν υπόψη τα γνωστά πρωτόκολλα μεταφοράς δεδομένων (UDP/TCP). Το RTP χρησιμοποιεί τα πρωτόκολλα επιπέδου δικτύου για την μεταφορά του (ως επί το πλείστον με UDP) προσθέτοντάς τους μηχανισμούς που επιτρέπουν την αποτελεσματική μετάδοση χρονικά κρίσιμων δεδομένων. Τέτοιοι μηχανισμοί είναι η χρονοσήμανση (time stamping) και η σειριακή αρίθμηση των πακέτων (sequence numbering). Η χρονοσήμανση παρέχει σημαντικές πληροφορίες στις εφαρμογές πραγματικού χρόνου. Ο αποστολέας βάζει σε κάθε πακέτο μια χρονοσήμανση (timestamp) (βλ. Εικόνα 11), την οποία χρησιμοποιεί ο παραλήπτης για να βρει τη χρονική στιγμή που πρέπει να παρουσιάσει τα δεδομένα του συγκεκριμένου πακέτου στον χρήστη. Δηλαδή, η χρονοσήμανση παρέχει την απαραίτητη πληροφορία ώστε να είναι δυνατό στους παραλήπτες να ανακατασκευάσουν τα αρχικά δεδομένα όπως αυτά μεταδόθηκαν από τον αποστολέα.

Η χρονοσήμανση χρησιμοποιείται επίσης για το συγχρονισμό διαφορετικών ροών δεδομένων, όπως ροές δεδομένων βίντεο και ήχου. Χρησιμεύει επίσης στον υπολογισμό στατιστικών στοιχείων μιας ροής ως μια ένδειξη της ποιότητας της παρεχόμενης υπηρεσίας, όπως η διακύμανση της καθυστέρησης (jitter). Το UDP, το οποίο συνήθως χρησιμοποιείται για τη μεταφορά των RTP πακέτων, δεν παραδίδει τα πακέτα με τη σειρά με την οποία στάλθηκαν για αυτό τα RTP πακέτα αριθμούνται τη στιγμή που στέλνονται (πεδίο sequence number) (βλ. Εικόνα 11), έτσι ώστε να μπορεί ο παραλήπτης να τα βάλει στη σωστή σειρά. Οι αριθμοί αυτοί χρησιμοποιούνται επίσης για να ανιχνεύονται απώλειες στη μετάδοση των πακέτων. Πέρα από αυτούς τους μηχανισμούς το RTP παρέχει και άλλους, όπως η πληροφόρηση για την ταυτότητα του αποστολέα και για το περιεχόμενο της πληροφορίας (payload type). Το payload type είναι σημαντικό για τον παραλήπτη ώστε να γνωρίζει το είδος της πληροφορίας που λαμβάνει και έτσι να μπορέσει να ανασυνθέσει και να παρουσιάσει την πληροφορία. Κάθε ροή πολυμέσων (π.χ. mpeg, G.711) καθορίζεται από έναν αριθμό – κωδικό (payload type) και σχετίζεται με κάποιο RTP profile. Το RTP profile καθορίζει λεπτομέρειες για το πώς μια συγκεκριμένη πολυμεσική κωδικοποίηση μεταδίδεται μέσω του RTP, για παράδειγμα καθορίζει το τι ακριβώς σημαίνει η χρονοσήμανση για αυτήν την κωδικοποίηση. Έτσι ο παραλήπτης μέσω του payload type μπορεί να αναγνωρίσει το περιεχόμενο μιας ροής και με βάση το RTP profile της να μπορέσει να τη χειριστεί. Τα RTP profile για αρκετές κωδικοποιήσεις καθορίζονται στο RFC1890. Ένα RTP πακέτο αποτελείται από την RTP επικεφαλίδα (header) ακολουθούμενη από τα δεδομένα (payload). Το header ενός RTP πακέτου έχει μέγεθος 12 bytes και περιέχει πεδία με δομή όπως φαίνεται στο σχήμα παρακάτω



Εικόνα 11: RTP datagram

Τα σπουδαιότερα από τα πεδία του RTP header περιγράφονται παρακάτω:

Payload Type (PT) (7 bits): Το payload type καθορίζει τον τύπο των δεδομένων που ακολουθούν το RTP header.

Sequence Number (16 bits): Το Sequence Number (αύξων αριθμός) μετρά τα πακέτα που στέλνει ο αποστολέας και αυξάνεται κατά ένα για κάθε πακέτο που μεταδίδεται. Επιτρέπει στον παραλήπτη να εντοπίσει κάποιο πακέτο που χάνεται και να αποκαθιστά την σωστή ακολουθία των πακέτων.

Timestamp (32 bits): Το timestamp αντανακλά την στιγμή δειγματοληψίας του πρώτου δείγματος που περιέχεται στο RTP πακέτο είτε σε μονάδες χρόνου είτε σε αριθμό δειγμάτων που έχουν μεταδοθεί.

Το RTP μεταδίδεται μέσω του UDP και του IP. Το header του IP είναι 20 bytes, του UDP είναι 8 bytes και του RTP 12 bytes. Άρα ένα RTP/UDP/IP πακέτο έχει συνολικό header 40 bytes. Το RTP/UDP/IP header μπορεί να μειωθεί στα 2 ή στα 4 bytes [4] αν χρησιμοποιηθεί το συμπιεσμένο RTP (cRTP) το οποίο προτιμάται σε WAN point-to-point links συνδέσεις, προφανώς για ελαχιστοποίηση και εξοικονόμηση του χρησιμοποιούμενου εύρους ζώνης του μέσου μεταφοράς.

3.5 Real Time Control Protocol

Το RTCP πρωτόκολλο χρησιμεύει στον έλεγχο των RTP ροών-συνόδων. Πιο συγκεκριμένα το RTCP παρέχει υπηρεσίες όπως παρακολούθηση ποιότητας υπηρεσίας (QoS monitoring), αναγνώριση αποστολέα (source identification), συγχρονισμός ανάμεσα σε διαφορετικά μέσα, τερματισμός συνόδου κ.λπ. Η παρακολούθηση ποιότητας υπηρεσίας (QoS monitoring) είναι μια από τις βασικές λειτουργίες του RTCP. Το RTCP παρέχει πληροφορίες ανάδρασης (feedback) στις εφαρμογές για την ποιότητα της μετάδοσης των δεδομένων. Οι κυριότερες από αυτές τις πληροφορίες είναι ο αριθμός των πακέτων δεδομένων που χάθηκαν, η διακύμανση της καθυστέρησης λήψης πακέτων (interarrival jitter), καθώς και πληροφορίες χρόνου που επιτρέπουν τον υπολογισμό του round trip time. Το RTCP στηρίζει τις λειτουργίες του στην ανταλλαγή RTCP πακέτων, διαφόρων ειδών, πάνω από το UDP. Τα είδη των RTCP πακέτων είναι:

Αναφορά αποστολέα (Sender Report - SR) και αναφορά παραλήπτη (Receiver Report - RR). Οι παραλήπτες πληροφορίας σε μία RTP / RTCP σύνοδο επιστρέφουν στον εκάστοτε αποστολέα δεδομένα που αφορούν την ποιότητα μετάδοσης. Αν ένα μέλος μιας συνόδου είναι μόνο παραλήπτης πληροφορίας αποστέλλει αναφορές παραλήπτη, ενώ αν είναι και αποστολέας πληροφορίας αποστέλλει και αναφορές αποστολέα. ·

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

- Πακέτο αποχαιρετισμού – τερματισμού συνόδου (Goodbye - BYE). Ο τύπος αυτός σηματοδοτεί την αποχώρηση από τη σύνοδο ενός ή περισσοτέρων μελών.

- Συγκεκριμένες συναρτήσεις εφαρμογής (Application Specific - APP). Είναι πακέτα, που μπορεί να καθορίσει και να χρησιμοποιήσει μια εφαρμογή για δικές της λειτουργίες και ανάγκες.

Το bandwidth που καταναλώνει η RTCP κίνηση μιας RTP ροής, δεν πρέπει να υπερβαίνει το 5% (IETF: RFC3611) του συνολικού bandwidth που καταναλώνει η ροή. Επιπλέον το ελάχιστο χρονικό διάστημα ανάμεσα στην αποστολή δύο RTCP πακέτων δεν μπορεί να υπερβαίνει τα 5 δευτερόλεπτα.

3.6 Session description protocol

Το Session Description Protocol προσδιορίζεται στο RFC4566. Σκοπός του είναι να περιγράφει τις ροές που συνάπτει το SIP και θεωρείται περισσότερο ένα περιγραφικό σύστημα παρά πρωτόκολλο(με την αυστηρή έννοια του όρου). Πιο συγκεκριμένα, το SDP περιέχει τις παρακάτω πληροφορίες για τη σύνοδο:

- Την IP διεύθυνση (host name ή κατά IPv4, IPv6),
- τον αριθμό της θύρας.
- τον τύπο των δεδομένων (ήχος, video, διαδραστικές πλατφόρμες κ.λπ.),
- τον αλγόριθμο κωδικοποίησης των δεδομένων (PCM A-Law, MPEG II video κ.λπ.),
- το θέμα της συνόδου
- το χρόνο έναρξης και λήξης της συνόδου.

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

3.7 Πλεονεκτήματα IPPBX

Ένα τηλεφωνικό σύστημα IPPBX ή VoIP αντικαθιστά ένα παραδοσιακό PBX (τηλεφωνικό σύστημα). Παρέχει στους χρήστες του έναν εσωτερικό αριθμό ο οποίος με την κατάλληλη ρύθμιση λειτουργεί ως μοναδικό αναγνωριστικό στο δίκτυο. Οι χρήστες του PBX έχουν τη δυνατότητα να πραγματοποιήσουν κλήσεις, να τις μεταβιβάσουν, να λάβουν μέρος σε μια συνδιάσκεψη και άλλες πιο προχωρημένες δυνατότητες .Οι κλήσεις αποστέλλονται διαμέσου του LAN υπό μορφή πακέτων δεδομένων. Το IPPBX δεν μας υποχρεώνει να δρομολογούμε τις κλήσεις μας μέσω του διαδικτύου. Με τη χρήση του κατάλληλου εξοπλισμού [Βλ. 4.3.2] μπορούμε να συνδέσουμε το τηλεφωνικό μας κέντρο στις ήδη υπάρχουσες γραμμές PSTN ή ISDN.

Ο όρος «τηλεφωνία μέσω IP» έχει την ίδια έννοια με τον όρο «φωνή μέσω πρωτοκόλλου Internet» και είναι γνωστός ως VoIP. Ο όρος αυτός αναφέρεται στη διάχυση της φωνητικής κίνησης μέσω δικτύων που βασίζονται στο internet. Το πρωτόκολλο IP αρχικά σχεδιάστηκε για τη δικτύωση δεδομένων και μετά την επιτυχία του προσαρμόστηκε για φωνητική δικτύωση. Η φωνή μέσω IP μπορεί να διευκολύνει τις εργασίες και να παράσχει υπηρεσίες που ίσως είναι βραδυκίνητες ή δαπανηρές στην εφαρμογή τους αν χρησιμοποιηθεί παραδοσιακό PSTN:

Μπορεί να γίνει ταυτόχρονη μετάδοση πολλαπλών κλήσεων χρησιμοποιώντας μια απλή ευρυζωνική σύνδεση. Με τον τρόπο αυτό, η φωνή μέσω IP μπορεί να διευκολύνει την προσθήκη τηλεφωνικών γραμμών στις επιχειρήσεις. Τα χαρακτηριστικά που συνήθως χρεώνουν ξεχωριστά οι εταιρείες τηλεπικοινωνιών, όπως η προώθηση κλήσεων, η αναγνώριση καλούντος ή η αυτόματη επανάκληση, αποτελούν εγγενή χαρακτηριστικά των τηλεφωνικών συστημάτων IPPBX.

Τα IPPBX εκτός από την παραδοσιακή τηλεφωνία παρέχουν ενοποιημένες επικοινωνίες, αφού επιτρέπουν την ενσωμάτωση άλλων υπηρεσιών που είναι διαθέσιμες στο διαδίκτυο, όπως η συνομιλία μέσω βίντεο, η ανταλλαγή μηνυμάτων κ.λπ.

Ένα τηλεφωνικό σύστημα VOIP διαθέτει ένα περιβάλλον διαμόρφωσης με βάση το Web, το οποίο επιτρέπει την διαχείριση του εύκολα ακόμα και από άτομα που δεν είναι τόσο εξοικειωμένα με την ορολογία της τηλεφωνίας και των δικτύων. Αυτό επιτρέπει να γίνουν βασικές αλλαγές στο σύστημα χωρίς την ύπαρξη προσωπικού IT. Καλό θα ήταν βέβαια οπουδήποτε σημαντική αλλαγή στο δίκτυο (π.χ. η προσθήκη ή η κατάργηση γραμμών) να γίνεται από εξειδικευμένο προσωπικό για να αποφευχθούν δυσλειτουργίες στο τηλεφωνικό σύστημα ή και απώλεια της τηλεφωνίας σαν υπηρεσία.

Τα IPPBX μπορούν να βοηθήσουν στην εξοικονόμηση χρημάτων καθώς με ένα ελάχιστο ετήσιο κόστος (περίπου 40€[3]) μας δίνετε η δυνατότητα αγοράς ενός trunk για πολλαπλές κλήσεις ενώ η χρέωση από του παρόχους VoIP είναι συνήθως φθηνότερη έναντι των παραδοσιακών παρόχων. Ένα άλλο πλεονέκτημα που παρέχουν τα IPPBX είναι δωρεάν κλήσεις ανάμεσα στα διασυνδεδεμένα δίκτυα.

Τα τηλεφωνικά συστήματα VoIP υλοποιούνται στο ήδη υπάρχον LAN εξοικονομώντας χρήματα από την εγκατάσταση ενός νέου δικτύου. Τα σύγχρονα τηλέφωνα ενσωματώνουν λειτουργίες switch έτσι οι υπολογιστές συνδέονται πάνω σε αυτά με αποτέλεσμα να μειώνεται ο αριθμός των απαιτούμενων RJ plugs. Μια συνήθης πρακτική των εταιριών για την μείωση του κόστους είναι η αντικατάσταση των switches τους με νέα που υποστηρίζουν το IEEE 802.3at-2009 η αλλιώς Power Over Ethernet. Η τεχνολογία PoE δίνει τη δυνατότητα παροχής ηλεκτρικού ρεύματος σε συσκευές μέσω του καλωδίου

[3] Με βάση τον ισχύοντα τιμοκατάλογο της VIVA για τον Απρίλη 2013

δικτύου, έτσι μειώνεται και ο αριθμός ηλεκτρικών παροχών που χρειαζόμαστε. Επίσης η χρήση Softphones (τηλέφωνο-λογισμικό) μετατρέπει τους ηλεκτρονικούς υπολογιστές σε τηλέφωνα εξαλείφοντας έτσι την ανάγκη αγοράς νέων τηλεφώνων. Αυτό είναι ιδιαίτερα βολικό για τις εταιρίες αφού τους παρέχει τη δυνατότητα να μεταβούν σε μια σύγχρονη μορφή επικοινωνίας με σχετικά μικρό κόστος.

Τα ιδιόκτητα συστήματα μπορεί να ξεπεραστούν εύκολα. Η προσθήκη περισσότερων τηλεφωνικών γραμμών ή επεκτάσεων απαιτεί συχνά δαπανηρές αναβαθμίσεις. Σε ορισμένες περιπτώσεις απαιτείται ένα εντελώς καινούριο τηλεφωνικό σύστημα. Στα IPPBX το πρόβλημα έχει εξαλειφθεί αφού μπορούμε να αναβαθμίσουμε το τηλεφωνικό μας κέντρο όποτε θελήσουμε. Στο κάτω-κάτω ένας υπολογιστής είναι!

Όπως αναφέραμε παραπάνω οι κλήσεις δρομολογούνται μέσω του υπολογιστή κάνοντας ευκολότερο για τους κατασκευαστές λογισμικού να ενσωματώσουν το λογισμικό τους στις επαγγελματικές εφαρμογές. Για παράδειγμα: μία εισερχόμενη κλήση μπορεί να αναγνωριστεί και να εμφανίσει αυτόματα το αρχείο του πελάτη, βελτιώνοντας σημαντικά την εξυπηρέτηση των πελατών μειώνοντας τον μέσο χρόνο εξυπηρέτησης. Οι εξερχόμενες κλήσεις μπορούν να πραγματοποιηθούν απευθείας από το Outlook, χωρίς να απαιτείται η πληκτρολόγηση του τηλεφωνικού αριθμού από τον χρήστη.

Τα IPPBX είναι κατά βάση λογισμικό επιτρέποντας έτσι την προσθήκη νέων χαρακτηριστικών και βελτιώσεων πιο γρήγορα σε σχέση με τα κλασικά τηλεφωνικά κέντρα. Οι εταιρίες κατασκευής τέτοιων συστημάτων έχουν τη δυνατότητα να παρέχουν στους χρήστες τους μια πλήρως παραμετροποιήσιμη πλατφόρμα επικοινωνίας. Χαρακτηριστικά όπως η αναγνώριση καλούντος, η αυτόματη διανομή κλήσεων και άλλα χαρακτηριστικά μπορούν να προστεθούν ή να τροποποιηθούν κατά το δοκούν. Ενδεικτικά σε ένα τηλεφωνικό σύστημα Panasonic η προσθήκη αναγνώρισης κλήσεων κοστίζει 400€[4]. Επομένως, τα περισσότερα τηλεφωνικά συστήματα VoIP συνοδεύονται από μια πλούσια γκάμα χαρακτηριστικών, στην οποία περιλαμβάνεται το σύστημα δρομολόγησης και διαχείρισης τηλεφωνικών κλήσεων, ο τηλεφωνητής, η αναμονή κλήσεων και πολλά ακόμη. Οι επιλογές αυτές είναι συχνά εξαιρετικά δαπανηρές στα ιδιόκτητα συστήματα.

Τέλος με τα IPPBXτο εταιρικό τηλέφωνο δεν έχει γεωγραφικό περιορισμό. Οι χρήστες απλά παίρνουν το τηλέφωνό τους, το τοποθετούν στην κοντινότερη θύρα ethernet και διατηρούν τον αριθμό που ήδη έχουν ενώ με την κατάλληλη ρύθμιση γίνεται εκτροπή των κλήσεων, οπουδήποτε στον κόσμο, χάρη στα χαρακτηριστικά του πρωτοκόλλου SIP.

[4] Η τιμή δόθηκε τηλεφωνικά από αντιπρόσωπο της εταιρίας.

3.8 Codecs

3.8.1 Εισαγωγή

Το codec είναι ένα πρόγραμμα το οποίο κωδικοποιεί και αποκωδικοποιεί (**CO**ding/**DEC**oding) ή συμπιέζει και αποσυμπιέζει (**CO**mpressing/**DEC**ompressing) μια ψηφιακή ροή δεδομένων. Πιο απλά, μπορούμε να δούμε το codec σαν έναν αυτόματο μεταφραστή, που ερμηνεύει το συμπιεσμένο/κωδικοποιημένο περιεχόμενο της ροής από μια μορφή σε κάποια άλλη. Η επιλογή του codec είναι κρίσιμης σημασίας καθώς επηρεάζει το δίκτυο με την παραγόμενη κίνηση που δημιουργούν οι κλήσεις, προσθέτει φόρτο στον server, και καθορίζει τις τερματικές συσκευές που θα χρησιμοποιήσουμε. Οι δύο βασικοί τύποι codecs είναι: οι codecs κυματομορφής(waveform) και οι codecs φωνής(vocoders).

- **Waveform codecs:** Πρόκειται για αλγόριθμους κωδικοποίησης χαμηλής πολυπλοκότητας. Η κωδικοποίηση της φωνής γίνεται προσπαθώντας η κυματομορφή του παραγόμενου συστήματος να παρεκκλίνει όσο το δυνατόν λιγότερο από αυτή του αρχικού. Λόγω των απλών αλγορίθμων που χρησιμοποιεί αυτή η κατηγορία κωδικοποιητών συναντώνται συχνά σε συστήματα χαμηλών προδιαγραφών. Γνωστοί waveform codecs είναι ο G.711 και ο G.726.

- **Vocoders:** Οι vocoders είναι πιο πολύπλοκοι αλγόριθμοι οι οποίοι προσπαθούν να αναπαράγουν την ανθρώπινη φωνή. Στους περισσότερους vocoders το εισερχόμενο σήμα περνάει από διάφορα ζωνοπερατά φίλτρα προκειμένου να χωριστεί το φάσμα και να κωδικοποιηθεί. Επίσης οι περισσότεροι vocoders παρακολουθούν τα χαρακτηριστικά της φωνής τροποποιώντας ανάλογα τον αλγόριθμό, αυτό έχει σαν αποτέλεσμα την χρήση μικρότερου εύρους ζώνης. Από τους πιο γνωστούς vocoders είναι ο G.729, ο speex και ο GSM.

Εκτός του τρόπου λειτουργίας του αλγόριθμου κωδικοποίησης οι codecs διαφέρουν και σε άλλα χαρακτηριστικά τα οποία είναι και το κριτήριο για τον πιο τελικά codec θα χρησιμοποιήσουμε στο δίκτυο μας.

- **Συχνότητα δειγματοληψίας**: Εκφράζει το πλήθος των δειγμάτων που έχουν ληφθεί από τον δειγματολήπτη σε διάρκεια ενός δευτερολέπτου. Η συχνότητα δειγματοληψίας είναι ανάλογη με το ακουστικό αποτέλεσμα.

- **Bit rate**: Εκφράζει των ρυθμό μετάδοσης που απαιτείται για την διάδοση της κωδικοποιημένης πληροφορίας.

- **Latency**: Με τον όρο latency αναφερόμαστε στο χρονικό διάστημα που απαιτείται για την ολοκλήρωση μιας διαδικασίας. Στην προκειμένη περίπτωση αναφερόμαστε στον χρόνο που χρειάζεται ο κωδικοποιητής για την κωδικοποίηση της φωνής.

- **Bits per Sample**: Εκφράζει το πλήθος των bit που χρησιμοποιούνται για την αναπαράσταση των δειγμάτων.

•

Codec	$F_{δειγματοληψίας}$	Bit rate	Latency	CBR	VBR
GSM-EFR	8 kHz	12.2 kbit/s	20-30ms	Ναι	Όχι
GSM-FR	8 kHz	13 kbit/s	20-30ms	Ναι	Όχι
GSM-HR	8 kHz	5.6 kbit/s	25ms	Ναι	Όχι
iLBC	8 kHz	13.33, 15.20 kbit/s	30, 20ms	Ναι	Όχι
iSAC	16 kHz ή32 kHz	10- 52 kbit/s	33-63ms	Ναι	Ναι
MP3	8- 48 kHz	8- 320 kbit/s	>100ms	Ναι	Ναι
SILK	8,12,16, 24 kHz	6 -40 kbit/s	25ms	Ναι	?
Speex	8,16,32,48 kHz	2.15-24.6 kbit/s(NB) 4-44.2 kbit/s(WB)	30ms(NB) 34ms(WB)	Ναι	Ναι
G.711	8 kHz	64 kbit/s	125μs (typical)	Ναι	Όχι
G.711.1	8 ή 16 kHz	64, 80, 96 kbit/s	11.875 ms	Ναι	Ναι
G.719	48 kHz	32-128 kbit/s	40 ms	Ναι	Όχι
G.721	8 kHz	32-88 mod8 kbit/s.)	4 ms	Ναι	Όχι
G.722	16 kHz	32 kbit/s	40 ms	Ναι	Όχι
G.722.1	16 kHz	64 kbit/s	40 ms	Ναι	Όχι
G.722.1C	32 kHz	48,56,64	25 ms	Ναι	Όχι
G.722.2	16 kHz	24,32 kbit/s	125μs	Ναι	Ναι
G.723	8 kHz	24,32,48 kbit/s	15 ms	Ναι	Όχι
G.726	8 kHz	6.60-23.85 kbit/s	15 ms	Ναι	Όχι
G.729	8 kHz	24,40 kbit/s	48.9375 ms	Ναι	Όχι
G.729D	8 kHz	16,24,32,40 kbit/s		Ναι	Όχι
G.729E	8 kHz	8 kbit/s		Ναι	Όχι
G.729.1	8 ή 16 kHz	6.4 kbit/s		Ναι	Ναι

Πίνακας 1: Σύγκριση κωδικοποιητών ήχου

3.8.2 Mean Opinion Score

Ένα από τα πιο συχνά ερωτήματα σχετικά με την τεχνολογία VoIP αφορά το ακουστικό αποτέλεσμα. Η βαθμολογία MOS προσπαθεί να βαθμολογήσει το ακουστικό αποτέλεσμα. Η βαθμολόγηση ενός codec γίνεται με την εξής διαδικασία: Δίνεται σε μια ομάδα ανθρώπων ένα δείγμα ήχου και αυτοί το βαθμολογούν από το 1 ως το 5. Έπειτα οι βαθμολογίες αθροίζονται κι εξάγεται ο μέσος όρος ο οποίος αποτελεί και την βαθμολογία. Είναι εύκολο να συμπεράνουμε ότι η κλίμακα MOS δεν αποτελεί αντικειμενικό κριτήριο της ποιότητας ενός codec καθώς αγνοεί παραμέτρους όπως το αρχικό σήμα της κλήσης και δεν ακολουθεί κάποια τυποποιημένη διαδικασία βαθμονόμησης. Στον παρακάτω πίνακα παρουσιάζεται η βαθμολογία για τους κυριότερους codecs όπως αυτοί παρουσιάζονται στο Wiki και στο vocal.com. Αξίζει να σημειωθεί ότι οι αλγόριθμοι κυματομορφής προσφέρουν καλύτερη ποιότητα ήχου.

Codec	Data rate	MOS wiki	vocal.com
G.711u	64	4.1	4.45
G.723.1	6.3	3.9	4.08
G.726	32	3.85	4.3
G.729a	8	3.7	4.04
GSM	12.2	3.5	4.14
iLBC	15.2	4.14	4.1
Speex			3.84

Πίνακας 2: Σύγκριση MOS

3.8.3 Παράμετροι επιλογής codec

Απώλεια πακέτων

Υπάρχει άμεση σχέση μεταξύ της απώλειας πακέτων και της ποιότητας ήχου. Οι ροές φωνής καθώς και όλες οι υπηρεσίες «πραγματικού χρόνου» είναι επιρρεπείς στην απώλεια πακέτων και έχουν αναπτυχθεί διάφορες τεχνικές οι οποίες αποκρύπτουν την επίδραση του φαινομένου. Αυτές οι τεχνικές είναι κατάλληλες για απώλεια της τάξης 2-3% των πακέτων. Ποσοστά απώλειας μεγαλύτερης τάξης υποβαθμίζουν ραγδαία την ποιότητα των κλήσεων, ακόμη και αν χρησιμοποιηθεί κάποια τεχνική απόκρυψης του φαινομένου. Οι τεχνικές απόκρυψης «απώλειας πακέτου» δεν έχουν όφελος για δεδομένα ομιλίας (ζώνης συχνότητας ανθρώπινης φωνής[5]) χωρίς να τις συνδυάσουμε με τεχνικές packet-redundancy. Για να αποφευχθεί απώλεια κλήσεων σε ροές voice-band απαιτείται packet loss τάξης 10^{-5}. Το πρόβλημα συνήθως αντιμετωπίζεται με την χρήση jitter buffer αυξάνοντας όμως το latency.

Έλεγχος Latency

[5] voiceband

Το ITU-T Recommendation [G.114] καθορίζει τα πρότυπα για την καθυστέρηση στα δίκτυα. Συγκεκριμένα, μια end-to-end καθυστέρηση των 150ms θεωρείται αποδεκτή για τις περισσότερες διαδραστικές εφαρμογές. Για την επίτευξη αυτού απαιτείται σωστή παραμετροποίηση όσον αφορά την εφαρμογή και τους πόρους του συστήματος. Οι παράμετροι καθυστέρησης κατά την διάδοση μιας ροής σε ένα δίκτυο είναι αρκετοί και υπάρχουν σε κάθε σημείο της διαδρομής από τον ένα άκρο στο άλλο.

Οι κύριες παράμετροι στην δημιουργία καθυστέρησης σε μια ροή είναι:

- Δειγματοληψία ήχου ή βίντεο και μετατροπή από αναλογική σε ψηφιακή ροή.
- Αποθήκευση σε προσωρινή μνήμη των δειγμάτων.
- Διαδικασία συμπίεσης της ροής.
- Ενθυλάκωση των συμπιεσμένων δεδομένων σε πακέτα.
- Πρόσβαση στο μέσον.
- Δρομολόγηση στο δίκτυο κορμού.
- Καθυστέρηση μετάδοσης.
- Αποθήκευση σε προσωρινή μνήμη για την ανάταξη των καθυστερημένων πακέτων.
- Αποκωδικοποίηση, αποσυμπίεση και ανασυγκρότησης της ροής.

3.8.3.1 Διαχείριση Jitter Buffer

Όπως αναφέραμε στην προηγούμενη ενότητα η καθυστέρηση υποβαθμίζει την ποιότητα των κλήσεων. Μεγαλύτερο όμως πρόβλημα προκαλεί η διακύμανση της καθυστέρησης ανάμεσα στα πακέτα. Ο Jitter Buffer είναι μια προσωρινή μνήμη που απαιτείται για να εξομαλύνει το φαινόμενο που δημιουργεί ή διακύμανση της καθυστέρησης ανάμεσα στα πακέτα προκειμένου να έχουμε μια συνεχόμενη ροη αναπαραγωγής. Η ρύθμιση του μεγέθους του jitter buffer επηρεάζει την end-to-end καθυστέρηση και το ποσοστό απώλειας πακέτων. Για μικρότερες τιμές του Jitter buffer έχουμε μικρότερη καθυστέρηση και μεγαλύτερο packet-loss ενώ αντίστοιχα για μεγαλύτερο μέγεθος jitter buffer έχουμε μικρότερο packet-loss και μεγαλύτερη καθυστέρηση. Οι ροές φωνής ενώ είναι ευαίσθητες στην καθυστέρηση είναι ανεκτικές στην απώλεια πακέτων καθώς το ανθρώπινο αφτί μπορεί να καταλάβει το νόημα μιας πρότασης από τα συμφραζόμενα. Για τον λόγο αυτό είναι καλύτερο να χρησιμοποιήσουμε ένα προσαρμοστικό jitter-buffer ο οποίος αυξομειώνεται ανάλογα με τις συνθήκες της κλήσης. Τα περισσότερα IPPBX προσαρμόζουν τον jitter-buffer χρησιμοποιώντας τα στατιστικά που τους παρέχει το RTCP. Από την άλλη όμως τα Voiceband δεδομένα είναι λιγότερο ευαίσθητα στην καθυστέρηση και επιρρεπή στην απώλεια πακέτων, λειτουργούν καλύτερα με έναν σταθερό jitter buffer ο οποίος δεν μεταβάλλεται ακόμα και σε περιπτώσεις μικρότερου jitter. Στην

περίπτωση ενός πακέτου που φτάσει μετά τον αναμενόμενο χρόνο του, και οι δύο τύποι jitter-buffer θα προσαρμόσουν το πρόγραμμα τους ώστε να καλύψουν την πιο αργή άφιξη.

3.8.3.2 Framing

Ένας τρόπος για την ελαχιστοποίηση της καθυστέρησης και των προβλημάτων που δημιουργεί είναι η αποστολή πακέτων με μικρό packet-size. Ωστόσο, αυτή η τεχνική αυξάνει το απαιτούμενο εύρος ζώνης για την αποστολή της ροής καθώς χρησιμοποιώντας πακέτα μικρότερου μεγέθους αυξάνουμε το Overhead λόγο των επικεφαλίδων. Αυτό σημαίνει ότι το βέλτιστο μέγεθος πακέτου για εφαρμογές ομιλίας είναι αρκετά μικρό, και θα πρέπει να ρυθμιστεί ώστε να χωράει συμπιεσμένη πληροφορία για ήχο χρονικής διάρκειας 10, 20 ή 30ms του ήχου[10] (ένα ή δύο πλαίσια συμπιεσμένου ήχου). Για ροές βίντεο(video-conference) το μέγεθος αυτό δεν είναι αποδεκτό. Για να αποφευχθεί περαιτέρω καθυστέρηση στους buffers, τα πακέτα στέλνονται σε ίσα ακέραια πολλαπλάσια του ρυθμού δειγματοληψίας του κωδικοποιητή. Για να επιτευχθεί αυτό απαιτείται μια Lockstep διαδικασία από πλευράς κωδικοποιητή και αποστολής πακέτων. Η διαδικασία Lockstep απαιτεί ότι οι εμπλεκόμενες διαδικασίες(encoding-packetazation) είναι συγχρονισμένες μεταξύ τους.

Επιλογή Codec

Όπως έχουμε ήδη αναφέρει η επιλογή codec αποτελεί μια απόφαση αρκετά σημαντική. Πριν επιλέξουμε τον κωδικοποιητή για το τηλεφωνικό μας σύστημα θα πρέπει να έχουμε λάβει υπόψη μας τα προαναφερθέντα ζητήματα. Για τηλεφωνικά δίκτυα που προορίζονται για ενδοεταιρική χρήση ή για δρομολόγηση των κλήσεων μέσω γραμμών ISDN/PSTN προτείνετε η χρήση του g.711 ενώ για δίκτυα που δρομολογούν τις κλήσεις στον πάροχο μέσω του διαδικτύου συστήνεται η χρήση του g.729.

Ελαχιστοποίηση απαιτούμενου Bandwidth

Υπάρχουν τρεις βασικοί μηχανισμοί που μπορούν να χρησιμοποιήσουν οι τερματικές συσκευές προκειμένου να ελαχιστοποιήσουν το απαιτούμενο bandwidth για τις εφαρμογές τους.

- Χρήση ενός συμπιεσμένου κωδικοποιητή χαμηλού ρυθμού
- Χρήση πακέτων με μεγάλο packet-size ώστε να χωράνε περισσότερα frames ήχου.
- Χρήση κωδικοποιητή με μεταβλητό ρυθμό μετάδοσης.

Η επιλογή του κωδικοποιητή συμβαίνει κατά την κρίση της συσκευής μέσω των ρυθμίσεων του δικτύου ή με χειροκίνητη επιλογή από τον διαχειριστή. Ανεξάρτητα από αυτά, κατά την αρχικοποίηση των παραμέτρων της κλήσης τα εμπλεκόμενα μέρη αποφασίζουν για τον κωδικοποιητή που θα χρησιμοποιήσουν. Η μετάδοση με χρήση μεταβλητού ρυθμού πραγματοποιείται με τεχνικές μείωσης του ρυθμού μέσα σε μια ροή δεδομένων. Τέτοια τεχνική είναι η VAD (voice activity detection). Η λειτουργία της βασίζεται στην μετάδοση δεδομένων όταν υπάρχει ομιλία και διακοπή της στις

παύσεις (συχνά την συναντούμε και ως Silence detection). Έτσι κατά την διάρκεια που δεν μιλάει κάποιο άκρο στέλνονται ελάχιστα ή και κανένα δεδομένα. Πιο προηγμένες τεχνικές μετάδοσης μεταβλητού ρυθμού χρησιμοποιούνται στα δίκτυα κινητής τηλεφωνίας όπου ο κωδικοποιητής προσαρμόζει την συμπίεση των δεδομένων για να ανταποκριθεί στις αλλαγές που συμβαίνουν στο δίκτυο.

3.9 Quality of Service

Αναφέραμε ήδη ότι οι ροές «πραγματικού χρόνου» είναι επιρρεπείς στο latency και ότι ένα από τα βασικά πλεονεκτήματα της IP τηλεφωνίας είναι η χρήση ενός ενιαίου δικτύου για την μετάδοση φωνής και δεδομένων. Πως λοιπόν το δίκτυο αναγνωρίζει τις ροές αυτές; Πως τους εξασφαλίζει προτεραιότητα. Η προτεραιότητα αυτή στα δίκτυα ονομάζεται Quality of Service και αποτελεί εγγενές χαρακτηριστικό του IPv6. Για την παροχή «ποιότητας υπηρεσίας» έχουν αναπτυχθεί διάφοροι μηχανισμοί.

3.9.1 Μηχανισμοί QoS

Υπάρχουν διάφοροι μηχανισμοί που μπορούν να χρησιμοποιηθούν για να παρέχουν ποιότητα υπηρεσίας για τα δίκτυα IP. Παρακάτω παρουσιάζονται οι γνωστές τεχνικές :

- Integrated Services (IntServ)
- Differentiated Services (Diffserv)
- MPLS (MPLS -TE).

3.9.1.1 Ολοκληρωμένες υπηρεσίες (IntServ)

Η μέθοδος IntServ, αποτελεί μια αρχιτεκτονική που καθορίζει τα συστατικά για τη παροχή ποιότητας υπηρεσιών σε IP δίκτυα. Η μέθοδος βασίζεται στην εξής ιδέα: Κάθε δρομολογητής του δικτύου υλοποιεί το IntServ και κάθε εφαρμογή που χρειάζεται κάποια μορφή εξασφάλισης πρέπει να κάνει μια κράτηση. Το πρωτόκολλο που είναι υπεύθυνο για την σηματοδοσία στο δίκτυο είναι το RSVP. Η αρχιτεκτονική IntServ και η εφαρμογή του RSVP περιγράφονται στο RFC2210 της IETF. Στην περίπτωση μιας συνόδου φωνής ο SIP client στέλνει ένα μήνυμα διαδρομής (RSVP path message) μέσω του δικτύου στο απομακρυσμένο δέκτη Κάθε κόμβος κατά μήκος της πορείας προσδιορίζει ότι το μήνυμα διαδρομής δηλώνει μια νέα σύνοδο RSVP και ελέγχει τους πόρους του πρίν προωθήσει το μήνυμα. Κάθε κόμβος που υποστηρίζει το IntServ κατά μήκος της διαδρομής αποθηκεύει μια στοιχεία για την σύνοδο και τα ανανεώνει περιοδικά ανάλογα με τα μηνύματα που λαμβάνει. Μόλις το μήνυμα διαδρομής φτάσει στο χρήστη, οι παράμετροι κίνησης που περιέχονται στο μήνυμα ελέγχονται και εάν ο χρήστης μπορεί να υποστηρίξει την σύνοδο, απαντάει με μήνυμα δέσμευσης. Δεδομένου ότι οι δεσμεύσεις RSVP είναι μονόδρομες η διαδικασία θα πρέπει να πραγματοποιηθεί και αντίστροφα προκειμένου να έχουμε ένα αμφίδρομο κύκλωμα φωνής.

Παρόλο που τα δίκτυα IP είναι συνδεσμοστρεφήδίκτυα, το RSVP χρησιμοποιεί ειδικό μηχανισμό για να διασφαλίσει ότι το μήνυμα «δέσμευσης» επιστρέφει από την ίδια διαδρομή με τα μηνύματα «διαδρομής». Κάθε δρομολογητής κατά μήκος της ‘διαδρομής’ RSVP ελέγχει το μήνυμα δέσμευσης RSVP αναφορικά με τους διαθέσιμους πόρους του και καθορίζει εάν μπορεί να υποστηρίξει το αίτημα δέσμευσης. Εάν είναι σε θέση να ικανοποιήσει το αίτημα, τότε το μήνυμα δέσμευσης προωθείται στον

αποστολέα των δεδομένων, διαφορετικά η κράτηση ακυρώνεται. Τέλος να προσθέσουμε ότι σύμφωνα με τον ορισμό του πρωτοκόλλου πρέπει να στέλνονται περιοδικά ειδικά μηνύματα για την διατήρηση της κράτησης.

3.9.1.2 Διαφοροποιημένες υπηρεσίες (Diffserv)

Η Diffserv αποτελεί μια αρχιτεκτονική που ορίζει έναν απλό τρόπο για τον διαχωρισμό και την διαχείριση της κίνησης παρέχοντας ποιότητα υπηρεσιών στα IP δίκτυα. Έτσι μπορούμε να παρέχουμε σε μια ροη ήχου μετάδοση χαμηλού latency ενώ όλη την υπόλοιπη κίνηση δεδομένων να την εξυπηρετούμε με την μέθοδο «best-effort".Η αρχιτεκτονική DiffServ περιγράφεται στα RFC2474 και RFC3260 και κάνει χρήση του πεδίου DS του IP header. Η λειτουργία της αρχιτεκτονικής στηρίζεται στον διαχωρισμό της κίνησης σε συγκεκριμένο αριθμό κατηγοριών. Κάθε δρομολογητής στο δίκτυο πρέπει να ρυθμιστεί ώστε να διαφοροποιεί την κίνηση ανάλογα με την κλάση της. Ενώ ο μηχανισμός προτείνει κάποιες ομάδες προτεραιότητας δεν καθορίζει ποιο είδος κίνησης αντιστοιχεί σε κάθε ομάδα. Η αρχιτεκτονική καθορίζει μόνο το μηχανισμό «μαρκαρίσματος», είναι υποχρέωση του διαχειριστή να παραμετροποιήσει τον δρομολογητή ώστε να αντιστοιχεί την κίνηση στην ανάλογη κλάση.

3.9.1.3 MPLS (MPLS-TE)

Η μηχανική κίνησης MPLS επεκτείνει τις ικανότητες του MPLS ώστε να ενσωματωθεί η ποιότητα εξυπηρέτησης και επομένως να παρέχει ένα ενδεχομένως χρήσιμο εργαλείο σε έναν χειριστή δικτύου που θέλει να υποστηρίξει υπηρεσίες φωνής. Το MPLS μπορεί να χρησιμοποιηθεί μέσα σε ένα δίκτυο για να οργανώσει διαδρομές με μεταγωγή ετικέτας (label switched paths) μεταξύ των σημείων εισόδου και εξόδου. Με την ανάθεση ενός εύρους ζώνης στη διαδρομή με μεταγωγή ετικέτας είναι δυνατό να εξασφαλιστεί ότι η κίνηση που μεταφέρεται σε μια διαδρομή με μεταγωγή ετικέτας είναι εγγυημένο να παραδοθεί στο σημείο εξόδου υπό τον όρο ότι η συνολική κίνηση που ανατίθεται στη διαδρομή με μεταγωγή ετικέτας δεν υπερβαίνει το εύρος ζώνης που διατίθεται σ' αυτή.

Αυτό είναι ένα χρήσιμο εργαλείο για τα δίκτυα IP που μεταφέρνουν φωνή αφού επιτρέπει την αποτελεσματική συνολική δέσμευση μεταξύ δύο σημείων μέσω της οποίας πολλές μεμονωμένες ροές μπορούν να μεταφερθούν χωρίς την απαίτηση της ρητής δέσμευσης των πόρων για κάθε μεμονωμένη ροή. Επιπλέον αυτή η συνολική δέσμευση μπορεί να μεταβληθεί με το χρόνο να επιτρέψει τις κυμαινόμενες ροές κίνησης σε ένα δίκτυο και όταν συνδυάζεται με τη γρήγορη επαναδρομολόγηση MPLS, επιτρέπει να δημιουργηθεί ένα ελαστικό δίκτυο όπου ακόμη και οι σημαντικές αποτυχίες του δικτύου έχουν πολύ περιορισμένη επίδραση στην κυκλοφορία που μεταφέρεται από μια συγκεκριμένη διαδρομή με μεταγωγή ετικέτας.

3.9.2 Στόχοι της ποιότητας εξυπηρέτησης

Για να διασφαλίσουν ότι το VoIP είναι μια αποδεκτή αντικατάσταση για τις καθιερωμένες υπηρεσίες τηλεφωνίας του PSTN, οι πελάτες πρέπει να λάβουν την ίδια συνεπή υψηλής

ποιότητας μετάδοση φωνής που λαμβάνουν με τις βασικές τηλεφωνικές υπηρεσίες. Όπως άλλες εφαρμογές πραγματικού χρόνου, έτσι και το VoIP είναι εξαιρετικά ευαίσθητο σε ζητήματα σχετικά με το εύρος ζώνης και την καθυστέρηση. Για να διασφαλιστεί ότι οι μεταδόσεις VoIP είναι καταληπτές στο δέκτη, τα πακέτα φωνής δεν μπορούν να απορριφθούν, να καθυστερήσουν υπερβολικά, ή να εκτεθούν σε μεταβολές της καθυστέρησης (jitter). Μια επιτυχής υλοποίηση VoIP πρέπει να παρέχει ένα αποδεκτό επίπεδο ποιότητας φωνής καλύπτοντας τις απαιτήσεις της κίνησης VoIP για ζητήματα σχετικά με το εύρος ζώνης, το χρόνο αντίδρασης και το jitter.

Η ποιότητας εξυπηρέτησης αναφέρεται στην ικανότητα ενός δικτύου να παρέχει βελτιωμένη εξυπηρέτηση σε συγκεκριμένη κίνηση του δικτύου μέσω των διαφόρων θεμελιωδών τεχνολογιών όπως της Frame Relay, του ATM, του Ethernet και των δικτύων 802.1, του SONET, και των δικτύων με δρομολόγηση IP. Το VoIP εγγυάται μετάδοση φωνής υψηλής ποιότητας μόνο εάν τα πακέτα της σηματοδοσίας και τα πακέτα των καναλιών φωνής έχουν προτεραιότητα σχετικά με άλλα είδη δικτυακής κίνησης.

Συγκεκριμένα, τα χαρακτηριστικά της ποιότητας εξυπηρέτησης παρέχουν βελτιωμένη και πιο προβλέψιμη υπηρεσία δικτύου με την υλοποίηση των ακόλουθων υπηρεσιών:

- Υποστήριξη εγγυημένου εύρους ζώνης: Σχεδιασμός του δικτύου ούτως ώστε το απαραίτητο εύρους ζώνης είναι πάντα διαθέσιμο να υποστηρίζει την κίνηση φωνής και δεδομένων
- Βελτίωση των χαρακτηριστικών απώλειας: Σχεδιασμός του δικτύου Frame Relay, για παράδειγμα, ούτως ώστε η επιλεξιμότητα απόρριψης να μην είναι ένας παράγοντας για τα πλαίσια που περιέχουν φωνή, κρατώντας τη φωνή κάτω από το δεσμευμένο ρυθμό πληροφοριών (committed information rate - CIR)
- Αποφυγή και διαχείριση της συμφόρησης του δικτύου: Εξασφάλιση ότι η υποδομή του LAN και του WAN μπορεί να υποστηρίξει τον όγκο της κίνησης δεδομένων και των κλήσεων φωνής.
- Διαμόρφωση της κίνησης του δικτύου: Χρησιμοποίηση των εργαλείων διαμόρφωσης κίνησης για να εξασφαλιστεί η ομαλή και συνεπής παράδοση των πλαισίων στο WAN.
- Καθορισμός προτεραιοτήτων κίνησης διαμέσου του δικτύου: Χαρακτηρισμός τη κίνησης φωνής ως υψηλής προτεραιότητας και τοποθετώντας την πρώτη στη σειρά αναμονής.

4 Σχεδιασμός του δικτύου.

Αναφερθήκαμε νωρίτερα στα οικονομικά στοιχεία μιας μικρομεσαίας επιχείρησης και πως ορίζεται αυτή νομικά. Πριν επεκταθούμε στις τεχνικές λεπτομέρειες για την ανάπτυξη ενός τηλεφωνικού δικτύου σε μια επιχείρηση θα πρέπει να μελετήσουμε το υφιστάμενο δίκτυο. Σε ένα εταιρικό δίκτυο οι συσκευές που αναμένουμε να συναντήσουμε είναι: ηλεκτρονικοί υπολογιστές ασύρματες συσκευές(π.χ. κινητά τηλέφωνα), δικτυακοί εκτυπωτές και ενδεχομένως κάποιον server. Όλες αυτές οι συσκευές παράγουν δικτυακή κίνηση η οποία μπορεί να επηρεάσει την ποιότητα των κλήσεων.

4.1 Υπολογισμός τηλεπικοινωνιακού όγκου

Ο αριθμός των κλήσεων σε εξέλιξη μεταβάλλεται με ένα τυχαίο τρόπο σε κάθε κλήση ξεχωριστά ενώ αρχίζει και τελειώνει με τυχαίο τρόπο. Κατά την διάρκεια της νύχτας ο τηλεφωνικός όγκος είναι μικρότερος ενώ μεγιστοποιείται κατά το μέσον της ημέρας.

Ώρα αιχμής

ή ώρα

Κεφάλαιο 4

Σχεδιασμός του δικτύου

μέγιστης απασχόλησης καλείται η περίοδος μιας ώρας που αντιστοιχεί στην αιχμή του φόρτου κίνησης. Το πλήθος των αναγκαίων καναλιών εξαρτάται από την μεταφερόμενη κίνηση και πρέπει να είναι επαρκές για να καλύψει την παραγόμενη κίνηση κατά της ώρες αιχμής. Μια ορθή πρακτική κατά τον σχεδιασμό του τηλεφωνικού δικτύου είναι η μακροπρόθεσμη πρόβλεψη για την κίνηση (προοπτικές εξέλιξης.). Όλες τις υπόλοιπες ώρες ο εξοπλισμός μας παραμένει ανενεργός, η τουλάχιστον ένα μεγάλο μέρος του.

Η ένταση της κίνησης καθορίζεται από τον μέσο αριθμό κλήσεων που βρίσκονται σε εξέλιξη. Η μονάδα κίνησης καλείται erlang(E) και ο μέσος αριθμός κλήσεων εν εξελίξει εξαρτάται από τον ρυθμό άφιξης των κλήσεων και από την μέση διάρκεια τους. Η κίνηση σε erlangs ισούται με το μέσο αριθμό των κλήσεων που φτάνουν κατά τη διάρκεια μιας περιόδου ίσης με τη μέση διάρκεια των κλήσεων. Μαθηματικά η κίνηση σε erlangs εκφράζεται από τον τύπο:

$$A = \frac{C * h}{T}$$ A= η κίνηση σε erlang,

C= ο μέσος όρος αφίξεων των κλήσεων κατά τη διάρκεια Τ.

h= η μέση διάρκεια κλήσεων.

Στην περίπτωση που T=h τότε A=C τότε ο τύπος μας δείχνει την προσφερόμενη κίνηση. Σε συστήματα με ένα μόνο κανάλι το Α μας δείχνει το ποσοστό που είναι απασχολημένο το κανάλι.

4.1.1 Grade of Service

Ο βαθμός εξυπηρέτησης (Grade of Service, GOS) είναι ένα μέτρο της πιθανότητας ανεπιτυχούς πρόσβασης κάποιου χρήστη στο σύστημα κατά την ώρα αιχμής, και ορίζεται ως ο λόγος του αριθμού των ανεπιτυχών κλήσεων προς τον συνολικό αριθμό κλήσεων την ώρα αιχμής. Στην ουσία, υποδηλώνει την πιθανότητα φραγής (πιθανότητα να μην εξυπηρετηθεί ένας χρήστης). Με άλλα λόγια, θα ήταν ορθότερο να ονομάζεται «βαθμός μη εξυπηρέτησης ». Ο βαθμός εξυπηρέτησης είναι ένας δείκτης επίδοσης ενός συγκεκριμένου συστήματος. Στόχος των Τηλεπικοινωνιακών μηχανικών (δηλαδή εγώ) είναι να σχεδιάσουν το σύστημα με ώστε να παρέχει ένα προκαθορισμένο GoS(2%).

4.2 Προετοιμασία του δικτύου.

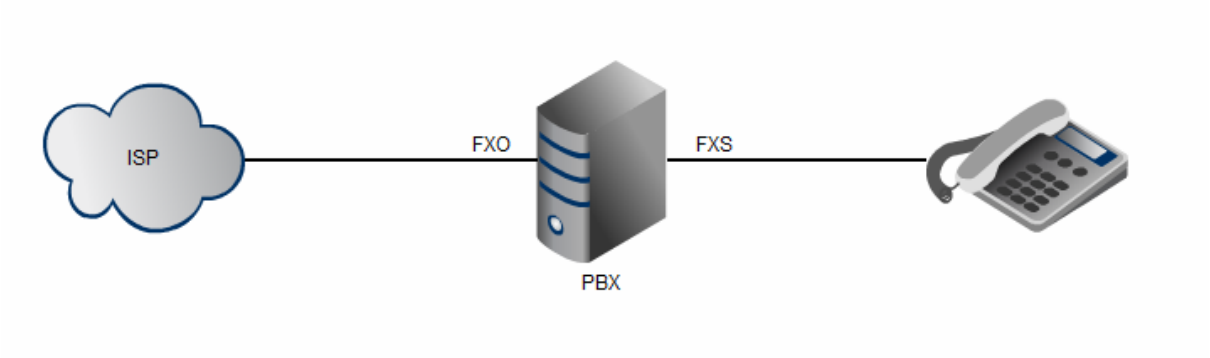
Η προετοιμασία του δικτύου και η σωστή σχεδίαση πριν την μετάβαση στο VoIP είναι μια διαδικασία που δεν πρέπει να αγνοηθεί. Έρευνες δείχνουν ότι υπάρχει 50% πιθανότητα η υλοποίηση VoIP να αποτύχει αν δεν προηγηθεί μια φάση σχεδιασμού πριν από την ανάπτυξη. Σύμφωνα με στατιστικά από τις επιτυχείς υλοποιήσεις VoIP που έγιναν αγνοώντας την διαδικασία του σχεδιασμού και του ελέγχου στο 60% των περιπτώσεων αναφέρουν ότι το δίκτυο χρειάζεται μηνιαία συντήρηση ενώ τα 2/3 αναφέρουν ότι η συντήρηση αυτή επηρεάζει την επιχειρηματική δραστηριότητα και υπάρχει απώλεια κερδών.

4.2.1 Επιλογή πλάνου τηλεφωνίας

Είναι σημαντικό να έχουμε προαποφασίσει τον τρόπο που θα υλοποιήσουμε το τηλεφωνικό μας κέντρο πριν τον σχεδιασμό του εσωτερικού δικτύου. Υπάρχουν δυο βασικά πλάνα υλοποίησης VoIP

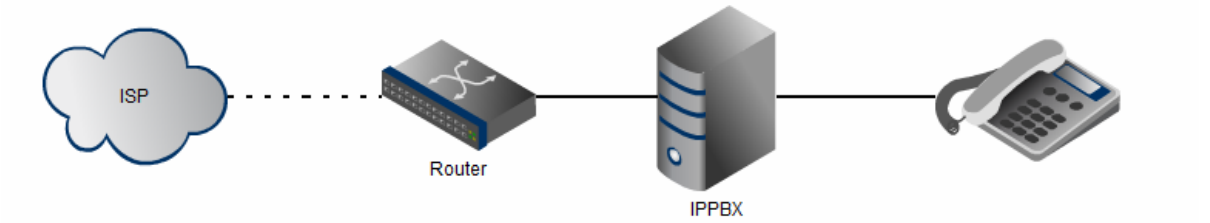
A. Ενδοεταιρικό IPPBX
B. IPPBX με πάροχο VoIP

Ενδοεταιρικό IPPBX:Το πλάνο υλοποίησης «ενδοεταιρικό IPPBX» προβλέπει την χρήση του τηλεφωνικού κέντρου για ενδοεταιρικές κλήσεις ενώ οι κλήσεις προς εξωτερικούς τηλεφωνικούς αριθμούς δρομολογούνται από το IPPBX μέσω PSTN/ISDN γραμμών. Στην παρακάτω εικόνα παρουσιάζεται σχηματικά η τοπολογία.



Εικόνα 12: VoIP εντός του εσωτερικού δικτύου.

IPPBX με πάροχο VoIP: Αντίθετα στην περίπτωση χρήσης κάποιου παρόχου VoIP οι κλησεις δρομολογούνται στον πάροχο μέσω του διαδικτύου. Οι κλήσεις μας είναι πλήρως ψηφιακές αφού "ταξιδεύουν" σε πακέτα. Οι κλήσεις δρομολογούνται στο IPPBX από εκεί στον δρομολογητή και τέλος στον πάροχο. Στην παρακάτω εικόνα παρουσιάζεται η τοπολογία γραφικά.



Εικόνα 13: End-to-End VoIP

4.2.2 Σχεδιασμός δικτύου

4.2.2.1 Εισαγωγή

Ο σχεδιασμός ενός δικτύου είναι μια επαναλαμβανόμενη διαδικασία που περιλαμβάνει τον σχεδιασμό της τοπολογίας, της σύνθεσης, της ανάλυσης και εν τέλει την υλοποίηση ενός δικτύου το οποίο ικανοποιεί τις ανάγκες και τις απαιτήσεις του φορέα εκμετάλλευσης του.

Η γενική μέθοδος σχεδιασμού δικτύου χωρίζεται σε πέντε στάδια. Πιο συγκεκριμένα:

- Επιχειρηματικός σχεδιασμός
- Μακροπρόθεσμη και μεσοπρόθεσμη σχεδίαση του δικτύου
- βραχυπρόθεσμος σχεδιασμός του δικτύου
- Προμήθεια υλικού
- Λειτουργία και συντήρηση.

Κάθε ένα από αυτά τα στάδια περιλαμβάνει σχέδια για διαφορετικούς χρονικούς ορίζοντες, δηλαδή ο επιχειρηματικός σχεδιασμός καθορίζει το πλάνο που ο φορέας εκμετάλλευσης πρέπει να εκτελέσει για

να διασφαλίσει ότι το δίκτυο θα είναι πλήρως λειτουργικό για τον προβλεπόμενο κύκλο ζωής του. Ωστόσο το στάδιο της συντήρησης εξετάζει την καθημερινή λειτουργία του δικτύου και τους τρόπους αντιμετώπισης πιθανών προβλημάτων.

Η διαδικασία σχεδιασμού του δικτύου αρχίζει με την απόκτηση των εξωτερικών πληροφοριών.:

- Προβλέψεις για το πώς το νέο δίκτυο θα λειτουργήσει
- Οικονομικές πληροφορίες σχετικά με το κόστος
- Τεχνικές λεπτομέρειες των δυνατοτήτων του δικτύου

και περιλαμβάνει τρία βασικά στάδια:

1. **Σχεδιασμός τοπολογίας:** Καθορίζει την τοπολογία του δικτύου τόσο λογικά όσο και φυσικά και υποδεικνύει τον τρόπο σύνδεσης των συστατικών μερών του δικτύου. Σε αυτό το στάδιο επίσης γίνεται και βελτιστοποίση της τοπολογίας η οποία βασίζεται στην θεωρία των γράφων. Οι μέθοδοι αυτοί έχουν σκοπό να μειώσουν το κόστος μεταγωγής(switching) μέσα στο δίκτυο και να μας υποδείξουν τον βέλτιστο τρόπο σύνδεσης.

2. **Σύνθεση δικτύου:** Αυτό το στάδιο περιλαμβάνει τον προσδιορισμό του μεγέθους των χρησιμοποιούμενων συστατικών. Αυτό γίνεται βάσει κριτηρίων απόδοσης, όπως το GoS. Η χρησιμοποιούμενη μέθοδος είναι γνωστή ως "Μη Γραμμική Βελτιστοποίηση", και περιλαμβάνει τον καθορισμό της τοπολογίας, το απαιτούμενο GoS, το κόστος μεταφοράς, κλπ.

3. **Υλοποίηση δικτύου:** Περιλαμβάνει τους τρόπους τήρησης των απαιτήσεων σε bandwidth και τη διασφάλιση της αξιοπιστίας του δικτύου. Περιλαμβάνει τον καθορισμό όλων των πληροφοριών σχετικά με τη ζήτηση, το κόστος και την αξιοπιστία, και στη συνέχεια, χρησιμοποιώντας τις πληροφορίες προκύπτει το πραγματικό φυσικό σχέδιο του δικτύου

4.2.2.2 Πρόβλεψη

Κατά τη διαδικασία σχεδιασμού του δικτύου γίνονται διάφορες εκτιμήσεις(Network forcasting) για την αναμενόμενη κίνηση και τον φόρτο που θα πρέπει το δίκτυο να υποστηρίξει. Στην περίπτωσης που υπάρχει υφιστάμενο δίκτυο παρόμοιας φύσης οι παραδοχές είναι περιττές καθώς μπορούμε να εξάγουμε δεδομένα από αυτό. Εάν δεν υπάρχει υφιστάμενο δίκτυο τότε θα πρέπει να αρκεστούμε στις προβλέψεις μας.

Τα στάδια για την διαδικασία πρόβλεψης είναι:

- Ορισμός του προβλήματος
- Συλλογή των δεδομένων

- Επιλογή της μεθόδου πρόβλεψης
- Η ανάλυση / πρόβλεψη
- Τεκμηρίωση και ανάλυση των αποτελεσμάτων.

4.2.2.3 Διαστασιολόγηση

Η διαστασιολόγηση ενός νέου δικτύου καθορίζει τις ελάχιστες απαιτήσεις χωρητικότητας που θα εξακολουθούν να επιτρέπουν την μετάδοση των δεδομένων μας με το επιθυμητό GoS. Για τον λόγο αυτό ο σχεδιασμός μας γίνεται βάση της κίνησης κατά τις ώρες αιχμής της κυκλοφορίας, τις ώρες εκείνες δηλαδή όπου η κίνηση είναι στο αποκορύφωμά της. Για τις μικρομεσαίες επιχειρήσεις ώρες αιχμής θεωρείται μεταξύ 11:30-14:00. Η διαδικασία περιλαμβάνει τον καθορισμό της τοπολογία του δικτύου, την δρομολόγηση και της απαιτήσεις σε QoS ώστε να μπορέσουμε να εκτιμήσουμε τον απαιτούμενο εξοπλισμό.

Βασικός κανόνας της διαστασιολόγισης είναι: ο φόρτος δεν θα πρέπει να προσεγγίσει το εκατό τοις εκατό. Για την σωστή εκτίμηση της αναμενόμενης κίνησης θα πρέπει να χρησιμοποιήσουμε μοντέλα προσομοίωσης κίνησης ή αναφορές από υφιστάμενα δίκτυα. Ένας άλλος λόγος για την υπερκάλυψη της αναμενόμενης κίνησης είναι η παροχή εναλλακτικού μονοπατιού στην περίπτωση προβλήματος στο δίκτυο.

4.2.2.4 Υπολογισμός τηλεφωνικού όγκου

Όπως αναφέραμε νωρίτερα υπάρχουν δυο τρόποι για την πραγματοποίηση κλήσεων με χρήση VoIP

A) Με χρήση εξοπλισμού FXO για την σύνδεση του PBX με το τηλεφωνικό δίκτυο

B) Με την χρήση ενός VoIP provider

Ανάλογα με την τεχνική που θα υλοποιήσουμε αλλάζει και ο τρόπος σχεδιασμού του δικτύου. Στη περίπτωση χρήσης εξοπλισμού FXO ο μέγιστος τηλεφωνικός όγκος που μπορεί να υπάρξει ισούται με το πλήθος των τηλεφωνικών γραμμών. Στην περίπτωση όμως της χρήσης ενός τρίτου παρόχου για την δρομολόγηση των κλήσεων ο όγκος πλέον εξαρτάται από την σύνδεση του PBX και του παρόχου.

4.2.2.5 Έλεγχος δικτυακής υποδομής

Πριν αγοραστεί καινούργιος τηλεφωνικός εξοπλισμός ή γίνει εγκατάσταση του PBX θα πρέπει να έχει ελεγχθεί το δίκτυο ώστε να είναι σίγουρο ότι θα μπορεί να ανταπεξέλθει στην κίνηση που παράγει το VoIP και τον αυξημένο αριθμό πακέτων. Υπάρχουν διάφορα online εργαλεία που μπορούν να υπολογίσουν το θεωρητικό MOS αλλά τα αποτελέσματα είναι έγκυρα για την δεδομένη χρονική στιγμή και δεν μπορεί η ανάπτυξη ενός δικτύου να βασιστεί μόνο σε αυτά. Για καλύτερα αποτελέσματα θα πρέπει να χρησιμοποιηθούν επαναλαμβανόμενα τεστ που να καλύπτουν ολόκληρη την ημέρα ώστε το δίκτυο να ελεγχθεί υπό διαφορετικές συνθήκες κίνησης.

4.2.3 Βελτίωση του δικτύου

Πριν την πραγματοποίηση των δοκιμών για την μετάβαση στο VoIP θα πρέπει να έχουν γίνει κάποιες βασικές εργασίες συντήρησης στο δίκτυο. Αυτές οι εργασίες έχουν σκοπό να μειώσουν στο δίκτυο την συμφόρηση να βελτιώσουν την υπάρχουσα υποδομή. Με αυτό τον τρόπο θα γλυτώσουμε λεφτά όχι μόνο από την αγορά του νέου εξοπλισμού αλλά και από την συντήρηση του.

Μείωση των hops

- Στο δίκτυο πρέπει να υπάρχουν μόνο οι απαραίτητες δικτυακές συσκευές. Αποσυνδέοντας οποιαδήποτε περιττή συσκευή από το δίκτυο(Router,switch) γλυτώνουμε το δίκτυο από περιττά πακέτα καθώς και από παράγοντες «καθυστέρησης».

- Αντικαθιστούμε τα hub με switch. Τα hubs λόγω του τρόπου λειτουργίας τους δημιουργούν συγκρούσεις, άρα καθυστέρηση στα πακέτα.

- Αν η ανάπτυξη του καινούργιου δικτύου γίνει πάνω από την παλιά καλωδίωση τότε το δίκτυο θα πρέπει να παραμετροποιηθεί για να αναγνωρίζει την VoIP κίνηση και να την χειριστή ανάλογα. Μια καλή αρχή είναι η δημιουργία VLAN.

- Οι ροές φωνή όπως είπαμε παραπάνω είναι επιρρεπείς στο Latency, για τον λόγο αυτό θα πρέπει να εξασφαλίσουμε ότι το δίκτυο μας υποστηρίζει QoS.

Έλεγχος Broadcast κίνησης: Ένα συχνό πρόβλημα που υπάρχει στα δίκτυα είναι η συμφόρηση που προκαλείται από τα μηνύματα Broadcast. Αυτά τα μηνύματα λαμβάνονται από όλες τις δικτυακές συσκευές που βρίσκονται στο ίδιο broadcast domain. Drivers δικτυακών συσκευών λάθος παραμετροποιημένο λογισμικό έχει ως αποτέλεσμα την δημιουργία broadcast μηνυμάτων. Ένας εύκολος τρόπος για τον έλεγχο του δικτύου για τέτοιο είδους μηνύματα είναι η χρήση κάποιου αναλυτή πακέτου όπως το Wireshark.

4.2.4 Protocol analyzer

Οι αναλυτές πρωτοκόλλων είναι συσκευές που συνδέονται σε ένα τηλεπικοινωνιακό δίκτυο και καταγράφουν την κίνηση σε αυτό. Επειδή η επικοινωνία μεταξύ υπολογιστών γίνεται με πακέτα που μεταφέρονται σε δυαδική μορφή απαιτείται μια σύνθετη διαδικασία για την ανάκτηση δεδομένων από το δίκτυο. Κατά την καταγραφή πακέτων από το δίκτυο αυτά αποθηκεύονται με την σειρά που τα λαμβάνει ο «δέκτης» μας και απαιτείται ταξινόμηση προκειμένου να έχουμε μια σωστή ροή δεδομένων. Ένα δεύτερο πρόβλημα που υπάρχει είναι ότι τα δεδομένα είναι εμφωλευμένα δηλαδή κάθε επίπεδο βρίσκεται κρυμμένο μέσα στο κατώτερό του κάνοντας αδύνατο για έναν άνθρωπο να διαβάσει τις ακολουθίες. Όλα αυτά τα κάνουν οι αναλυτές δικτύου. Αναλαμβάνουν να αναγνωρίσουν τις ροές δεδομένων, να ταξινομήσουν τα πακέτα να ξεχωρίσουν τα δεδομένα των διαφορετικών επιπέδων κ.τ.λ. Η βασική χρήση τέτοιων προγραμμάτων (ή συσκευών) από τους διαχειριστές δικτύων είναι ή επιδιόρθωση σφαλμάτων, ο έλεγχος του δικτύου για κακόβουλη κίνηση, την παραγωγή

στατιστικών στοιχείων κίνησης κ.τ.λ. Εκτός από τους διαχειριστές δικτύων οι αναλυτές πρωτοκόλλων αποτελούν βασικό εργαλείο απόσπασης πληροφοριών για τους Hackers.

4.3 Μελέτη περιπτώσεων: Εξοπλισμός

Έχοντας καλύψει το θεωρητικό υπόβαθρο γύρω από τα τηλεφωνικά κέντρα μπορούμε να προχωρήσουμε στην υλοποίηση τους. Μέσα από μελέτες περιπτώσεων θα δείξουμε την διαφορά ανάμεσα στα παραδοσιακά τηλεφωνικά κέντρα και στα VoIP. Τα σενάρια που θα καλύψουμε είναι τα εξής:

A. Δίκτυο Μικρομεσαίας επιχείρησης

B. Δίκτυο Ατομικής επιχείρησης

4.3.1 Μικρομεσαίες επιχειρήσεις.

Το δίκτυο που θα αναλύσουμε αποτελείται από 15χρήστες έχει 4 κανάλια φωνής(2 ISDN) για την δρομολόγηση των κλήσεων, επιθυμεί την υποστήριξη «θυρωρού», και την υποστήριξη φωνητικού ταχυδρομείου.

4.3.1.1 Υπόθεση 1:

Για την υλοποίηση του IPPBX θα χρησιμοποιήσουμε ένα Jetway JNC9MGL-525 ενώ για την περίπτωση απλού τηλεφωνικού κέντρου ένα Panasonic kX-TDA30

Panasonic		**Intel Atom-VoIP**		**Intel Atom-ISDN**	
		Κόστος σε ευρώ: Τηλεφωνικό κέντρο			
Συσκευής	1000	Motherboard	114	Motherboard	114
Κάρτα ISDN	180	Hardware	141	Hardware	141
24 Εσωτερικά	660			ISDN card	290
Τηλεφωνήτρια	220	Μεταφορικά	30	Μεταφορικά	30
Switch	70	PoE/Qos Switch	272	PoE/Qos Switch	272
Συσκευές	420	VoIP Συσκευή	1199	VoIP	1199
Τηλεφωνικό δίκτυο	**???**				
Σύνολο	2.639,00 €	Σύνολο	1.756,00 €	Σύνολο	2.046,00 €
		Διαφορά	883,00€	Διαφορά	593,00€

Στον παραπάνω πίνακα εμφανίζεται το ενδεικτικό κόστος του δικτύου. Η ελάχιστη διαφορά που έχουμε από την υλοποίηση ενός IPPBX είναι περίπου 600 ευρώ **χωρίς** να λάβουμε υπόψη το κόστος εγκατάστασης του αναλογικού τηλεφωνικού κέντρου και το κόστος ανάπτυξης του τηλεφωνικού δικτύου. Στην περίπτωση του IPPBX η εγκατάσταση μπορεί να γίνει από τον πελάτη [Βλ. Παράρτημα Α] ενώ δεν υφίσταται τηλεφωνικό δίκτυο αφού χρησιμοποιούμε το LAN. Ο PBX server θα εγκατασταθεί σε ένα μηχάνημα με επεξεργαστή Intel Atom και 4GB RAM.[6] Ενδιαφέρον έχει ότι με

[6] Οι τιμές προέρχονται από το skroutz.gr, cosmodata.gr, allvoip.gr , mini-itx.com και ισχύουν για τον Απρίλη 2013.

την διαφορά μπορούμε να αγοράσουμε έναν μικρό Server και να αναπτύξουμε πλατφόρμα ενοποιημένης επικοινωνίας προσφέροντας περισσότερα χαρακτηριστικά. Αξίζει επίσης να σημειωθεί ότι στην περίπτωση του IPPBX έχουμε την δυνατότητα καταγραφής των κλήσεων.

Το δίκτυο που θα αναλύσουμε ανήκει σε ένα κέντρο τηλεφωνικής εξυπηρέτησης αποτελείται από 50χρήστες διαθέτει 30 κανάλια φωνής για την δρομολόγηση των κλήσεων, επιθυμεί την υποστήριξη «θυρωρού», καθώς και καταγραφή των κλήσεων για τουλάχιστον 2μήνες.

Για την εύρεση του κατάλληλου εξοπλισμού θα πρέπει να βρούμε την μέγιστη κίνηση που μπορεί να παράγει το δίκτυο μας. Έτσι μπορούμε να πούμε ότι έχουμε το πολύ 40 ταυτόχρονες κλήσεις.(30εξωτερικές και 10εσωτερικές). Για την ελαχιστοποίηση του Bandwidth θα χρησιμοποιήσουμε τον G.729. Ο G.729 απαιτεί 32kb/s για την πραγματοποίηση μιας κλήσης. Έτσι για το σύνολο των κλήσεων μας απαιτείται 1280kb/s.

4.3.1.2 Υπόθεση 2:

Θεωρώ ότι το τηλεφωνικό κέντρο λειτουργεί επτά ημέρες την εβδομάδα δεκαπέντε ώρες την μέρα και ανά πάσα στιγμή έχουμε 16κλήσεις. Έτσι ανά ημέρα το τηλεφωνικό κέντρο παράγει κλήσεις 864,000 δευτερολέπτων ή 51.840.000 τους δυο μήνες δηλαδή όγκο 1.658.880.000kbits δηλαδή 197,75GB (396GB για αμφίδρομη καταγραφή).

Panasonic KX-TDA200		**DELL PE T110 II -VoIP**		**DELL PE T110 II -ISDN**	
Κόστος σε ευρώ: Τηλεφωνικό κέντρο					
Συσκευής	2100	Server	951	Server	951
Κάρτα ISDN PRI	500			ISDN card	350
50 Εσωτερικά	1040				
Τηλεφωνήτρια	450				
Switch	210	PoE/Qos Switch	816	PoE/Qos Switch	816
Καταγραφή	2300				
Συσκευές	3750	VoIP Συσκευή	400	VoIP	400
Τηλεφωνικό δίκτυο	**???**				
Σύνολο	10.350,00 €	Σύνολο	2.167,00 €	Σύνολο	2.517,00 €
		Διαφορά	8183,00€	Διαφορά	7833,00€

Είναι φανερό ότι όσο μεγαλώνει το δίκτυο συμφέρει περισσότερο η ανάπτυξη ενός δικτύου VoIP. Μελανό σημείο συνεχίζει να παραμένει η ανάπτυξη του τηλεφωνικού δικτύου ενώ αξίζει να σημειώσουμε ότι σε ειδικά περιβάλλοντα όπου οι χρήστες του τηλεφωνικού κέντρου είναι συνεχώς μπροστά σε ηλεκτρονικό υπολογιστή μπορούν να αντικατασταθούν οι τηλεφωνικές συσκευές από ακουστικά για ηλεκτρονικό υπολογιστή μειώνοντας το κόστος κατά πολύ. Από πλευράς υλικού ο

server είναι εφοδιασμένος με έναν τετραπύρηνο Intel Xeon με RAID1 και 8Gb RAM. Το switch που χρησιμοποιούμε παραμένει το ίδιο με την «Μελέτη 1» ενώ αυξάνεται ο αριθμός σους σε τρία. Τέλος η τιμή για την υποστήριξη της καταγραφής των κλήσεων είναι ενδεικτική και έχει προκύψει από συζητήσεις μέσα σε φόρουμ από χρήστες οι οποίοι έχουν ήδη υλοποιήσει τέτοια λύση.

4.3.2 Ατομική εταιρεία

Εικόνα 14 Raspberry Pi

Όπως προκύπτουν από τα στατιστικά της Eurostat[Βλ Κεφ.1.] η συντριπτική πλειονότητα των μικρομεσαίων επιχειρήσεων απασχολούν δυο εργαζομένους. Έτσι σε αυτή την ενότητα θα κοστολογήσουμε την ανάπτυξη ενός μακρού VoIP server. Πρόσφατα η Elastix κυκλοφόρησε το uElastix μια έκδοση της πλατφόρμας για ενσωματωμένες συσκευές. Η συγκεκριμένη έκδοση υποστηρίζει το Raspberry Pi. Το Pi είναι ένας μικρό-ελεγκτής σε μέγεθος τηλεκάρτας με αρκετά καλά τεχνικά χαρακτηριστικά. Για να φτιάξουμε το μικρό αυτό δίκτυο θα χρειαστούμε ένα PI(64Ευρώ) μια κάρτα τύπου SD(6€) ένα μικρό Switch(10€) και τέλος έναν VoIP αντάπτορα όπως ο Cisco SPA112(49€). Έτσι με κόστος μόλις 130ευρώ και μια απλή τηλεφωνική συσκευή μπορεί μια μικρή εταιρεία να αποκτήσει όλα τα πλεονεκτήματα ενός μεγάλου τηλεφωνικού κέντρου. Επίσης το κόστος μπορεί να μειωθεί στα 80ευρώ αν χρησιμοποιηθεί κάποιος VoIP πάροχος.

4.4 Μελέτη περιπτώσεων: Λύσεις τηλεφωνίας.

Για να έχουμε ένα ολοκληρωμένο IPPBX θα πρέπει να χρησιμοποιούμε κάποιον πάροχο. Όπως θα εξηγήσουμε παρακάτω ο πάροχος που θα μας δρομολογεί τις κλήσεις μπορεί να είναι κάποιος πάροχος που μας παρέχει ISDN ή PSTN γραμμή ή να είναι VoIP πάροχος να πηγαίνουν οι κλήσεις μας προς αυτό μέσω του διαδικτύου. Στην δεύτερη περίπτωση ο πάροχος δεν χρειάζεται να βρίσκεται στην Ελλάδα καθώς τα δεδομένα μπορούν να ταξιδέψουν παντού. Στον επόμενο πίνακα θα συγκρίνουμε τα πακέτα τηλεφωνίας τεσσάρων Ελληνικών παρόχων καθώς και ενός VoIP provider. Η σύγκριση γίνεται βάση των εμπορικά διαθέσιμων πακέτων τους και αφορά εταιρικά προγράμματα. Η σύγκριση αφορά την παροχή Internet ταχύτητας 24/1, την παροχή δυο γραμμών ISDN (4 κανάλια φωνής), και την παροχή στατικής IP. Τέλος οι χρήστες μας υποθέτουμε ότι μιλούν 4000 λεπτά σε εθνικά σταθερά και 900 λεπτά προς κινητά.

	ADSL	Double play			Δωρεάν Χρόνος				Πρόγραμμα Κινητών 1			Πρόγραμμα Κινητών 2			Τιμή Καταλόγου		Στόχος 1			Ετήσιο Κόστος		Μηνιαίο
ISP	Τιμή/Μήνα	Internet	Static IP	Call slots	Σταθερά	Κινητά	Κόστος/μήνα	Εφάπαξ	Κόστος	Λεπτά	Κόστος/Λεπτό	Κόστος	Λεπτά	Κόστος/Λεπτό	σταθερά	κινητά	Σταθερά 3000'	Κινητά 1 900'	Κινητά 2 900	Κινητά1	Κινητά2	
OTE	29,68	24/1	yes	4	Απεριόριστα	90	78,86	54,14	47,7	1000	0,0477	29,2	600	0,0487	0	0,0616	0	47,7	42,14	1572,86	1506,09	125,5077
Cyta	25,5	24/1	yes	4	6000'	0	63	60	44	900	0,0489	30,0	600	0,0500	0,029	0,095	0	44	58,50	1344	1518	112
Forthnet		24/1	yes	4	Απεριόριστα	180	67,50	51,57	62,21	960	0,0648	32,57	480	0,0679	0	0,1622	0	62,21	71,50	1608,09	1719,55	134,0075
HOL	60,8	24/1	yes	3	Απεριόριστα	240	60	50	90	1020	0,0882	40,50	450	0,0900	0	0,1619	0	90	74,50	1850	1663,99	138,6657
Viva		-	-	10	-	0	1,5		0			0	0		0,019	0,1	57	90	90,00	2088		174
VoIPVoIP	25,5	Με ελληνικό αριθμό		4			48	48							0,019	0,0319	57	28,71		1958,52		163,21
Hybrid	25,5			0			1,5	20							0,019	0,0419	57	28,71		1372,52		

Εικόνα 15 Συγκριτικός πίνακας εταιρικών προγραμμάτων τηλεφωνίας Ελλήνων παρόχων.

Ο συγκριτικός πίνακας χωρίζεται σε οκτώ ενότητες. Η βασική ενότητα εμφανίζεται με μωβ ανοιχτό, και δείχνει τον χρόνο ομιλίας που προσφέρει κάθε εταιρεία με το πακέτο της. Συγκεκριμένα η VIVA δεν προσφέρει χρόνο ομιλίας αλλά δεν χρεώνει μηνιαίο πάγιο αλλά όπως φαίνεται αυτό δεν αρκεί για να αντισταθμίσει το κόστος κάνοντας της έτσι πιο ακριβή κατά 744€ ετησίως. Στην τελευταία ενότητα εμφανίζεται το ετήσιο κόστος που προκύπτει για κάθε εταιρεία, δύο προγράμματα χρόνου ομιλίας (ένα μεγαλύτερου του στόχου και ένα μικρότερου).

Από τον παραπάνω πίνακα συμπεραίνουμε ότι το VoIP στην Ελλάδα δεν είναι ανταγωνιστικό όταν καλούμε συχνά κινητά ενώ η χρήση ενός ξένου παρόχου για την δρομολόγηση των κλήσεων δεν συμφέρει λόγω ακριβής χρέωσης των Ελληνικών αριθμών. Όπως φαίνεται μια υβριδική λύση είναι η ιδανική διαφέροντας μόνο 30ευρώ από την χρήση του δικτύου PSTN. Στην υβριδική λύση οι εισερχόμενες κλήσεις καθώς και η προμήθεια του τηλεφωνικού αριθμού γίνεται από την ViVA ενώ οι εξερχόμενες κλήσεις δρομολογούνται στην VoIPVoIP.

4.5 Επιλογή Server

Το IPPBX είναι η βασική οντότητα κάθε VoIP δικτύου. Είναι σημαντικό λοιπόν προτού προβούμε στην προμήθεια ενός server για την παροχή υπηρεσιών φωνής στο νέο μας τηλεφωνικό δίκτυο να κατανοήσουμε τον ρόλο του server μας και του έργου που επιτελεί. Κυριότερο κριτήριο επιλογής για την προμήθεια οποιοδήποτε πράγματος στις επιχειρήσεις αποτελεί το κόστος. Η φθηνή λύση σίγουρα θα ικανοποιήσει την εταιρεία αλλά δεν είναι σίγουρο ότι το μηχάνημα που θα αγοράσουμε θα μπορέσει να υποστηρίξει την τηλεπικοινωνιακή κίνηση. Το πόσο ισχυρό θα είναι το μηχάνημα μας εξαρτάται από τους εξής παράγοντες:

1. Αριθμός γραμμών
2. Αριθμός χρηστών
3. Παραμετροποίηση του συστήματος
4. Πλήθος κλήσεων

Οι πλατφόρμες παροχής VoIP δεν περιορίζονται σε απλές τηλεφωνικές κλήσεις αλλά παρέχουν ένα σύνολο τηλεπικοινωνιακών υπηρεσιών όπως τηλεφωνικά μενού, υπηρεσίες τηλεφωνητή, βιντεοκλήσεις, υπηρεσίες καταλόγου, υπηρεσίες ηλεκτρονικού ταχυδρομείου, υπηρεσίες

παρουσιάσεων κ.τ.λ. Είναι κατανοητό λοιπόν ότι ανάλογα με το λογισμικό που θα χρησιμοποιήσουμε και τις υπηρεσίες που θα αξιοποιήσουμε είναι ανάλογο και το απαιτούμενο hardware.

4.5.1 Εξοπλισμός VoIP

4.5.1.1 FXS/FXO

Τα FXS και FXO είναι τα ονόματα των θυρών που χρησιμοποιούνται για να συνδέσουν το IPPBX μας με τις αναλογικές τηλεφωνικές γραμμές και παρέχουν στο τηλεφωνικό μας κέντρο την δυνατότητα δρομολόγησης κλήσεων στο δημόσιο τηλεφωνικό δίκτυο.

FXS: Η διεπαφή Foreign eXchange Subscriber είναι η θύρα που παρέχει την αναλογική γραμμή στο συνδρομητή. Με άλλα λόγια, είναι η 'πρίζα στον τοίχο' που παρέχει το σήμα επιλογής.

FXO: Η διεπαφή Foreign eXchange Office είναι η θύρα που λαμβάνει την αναλογική γραμμή. Είναι η πρίζα στο τηλέφωνο ή στη συσκευή φαξ, ή η πρίζα στο αναλογικό τηλεφωνικό μας σύστημα. Παρέχει μια ένδειξη της κατάστασης του βρόχου. Λόγω του ότι η θύρα FXO βρίσκεται πάνω σε μια συσκευή, όπως ένα φαξ ή ένα τηλέφωνο, η τελευταία αποκαλείται συχνά 'συσκευή FXO'.

Πύλη FXO: Για τη σύνδεση αναλογικών τηλεφωνικών γραμμών σε ένα IPPBX χρειάζεται μία πύλη FXO. Αυτή σας επιτρέπει να συνδέσετε τη θύρα FXS με τη θύρα FXO της πύλης, η οποία στη συνέχεια μετατρέπει το αναλογικό σήμα σε πακέτα VoIP και αντίστροφα.

Πύλη FXS: Μία πύλη FXS συνδέει συνήθως μία ή περισσότερες γραμμές ενός παραδοσιακού PBX με ένα τηλεφωνικό σύστημα ή παροχέα VoIP.

Προσαρμογέας FXS: Ένας προσαρμογέας FXS χρησιμοποιείται για τη σύνδεση ενός αναλογικού τηλεφώνου ή μιας συσκευής φαξ με ένα τηλεφωνικό σύστημα ή παροχέα VoIP.

4.6 Έλεγχος ποιότητας κλήσεων

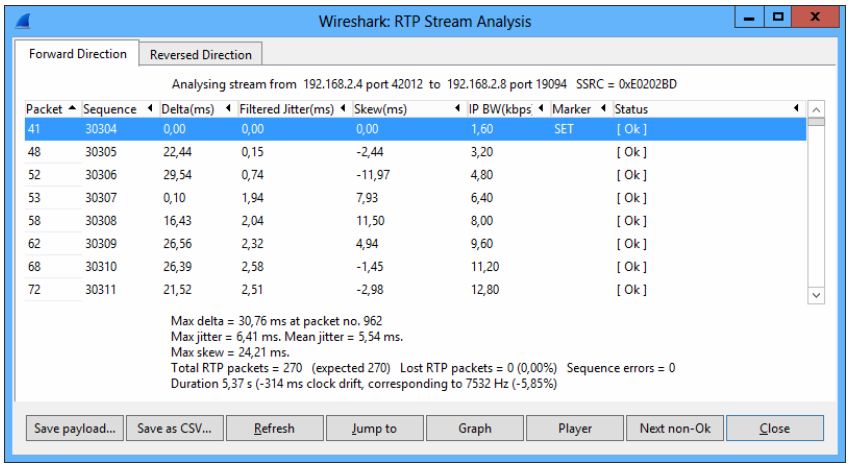
Μέχρι τώρα έχουμε εγκαταστήσει το FreePBX έχουμε προσθέσει χρήστες και έχουμε δημιουργήσει ένα τηλεφωνικό μενού. Ήρθε λοιπόν η ώρα να ελέγξουμε το δίκτυο και τον server. Για την διαδικασία του ελέγχου θα χρειαστούμε:

1) Υπολογιστή για τον έλεγχο με:
    a) SIP client και το wireshark
2) Τερματική συσκευή(PC/Smartphone)
    a) SIP client

Το Wireshark παρέχει πολλά στατιστικά για την ανάλυση κλήσεων VoIP. Παρακάτω παρουσιάζεται μια βασική διαδικασία ελέγχου των κλήσεων. Αρχικά χρειαζόμαστε δεδομένα από κλήσεις του δικτύου. Για τον σκοπό αυτό θα πραγματοποιήσουμε κλήσεις από τον υπολογιστή προς την δεύτερη συσκευή ενώ το wireshark καταγράφει τα πακέτα. Καλό θα ήταν η κλήση να διαρκέσει αρκετή ώρα(5λεπτά περίπου) ώστε τα δεδομένα να είναι αξιόπιστα. Για ακόμη καλύτερα δεδομένα προτείνετε η επανάληψη του ελέγχου σε διαφορετικές χρονικές στιγμές και ιδίως τις ώρες αιχμής.

Από το wireshark ο έλεγχος των κλήσεων γίνεται από το μενού “Telephony” – “RTP” – “Show all streams”

Στο παράθυρο που εμφανίζεται φαίνονται όλες οι ροές RTP που κατέγραψε το Wireshark. Επιλέγουμε λοιπόν μια από τις ροές και πατάμε “Analyze”



Εικόνα 16: Ανάλυση κλήσης

Στην [Εικόνα 21] εμφανίζεται η ανάλυση κλήσης. Οι δύο σημαντικότερες τιμές είναι ή “Max jitter” και το “Packet loss”. Το packet loss θα πρέπει να είναι πάντα μηδενικό (για κλήσεις εντός του εσωτερικού δικτύου). Απώλειες πακέτων μπορούμε να έχουμε από ανεπαρκή δικτυακό εξοπλισμό(buffer-overflow) ή ακόμη και από κακή καλωδίωση. Μεγάλη τιμή του Jitter από την άλλη μπορεί να οφείλεται σε κακή παραμετροποίηση του server(packet size) η στην ύπαρξη μεγάλης διαδικτυακής κίνησης στο δίκτυο.

5

Κεφάλαιο 5

Ασφάλεια

5. Ασφάλεια

5.1 Εισαγωγή

Όπως κάθε δικτυακό σύστημα έτσι και τα IPPBX είναι εκτεθειμένα σε διαδικτυακές απειλές. 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 πιστοποίηση των κλήσεων, ούτε end-to-end μέτρα ακεραιότητας(integrity) και εμπιστευτικότητας. Η ασφάλεια στο VoIP είναι ένα πολύπλοκο ζήτημα λόγω των πολλών παραμέτρων και των συσκευών που το απαρτίζουν. Έτσι ασφάλεια του τηλεφωνικού δικτύου συνεπάγεται εξασφάλιση όλων των συσκευών.

Απόρρητο (Privacy): 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 την 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 εύκολα διαθέσιμα. θεωρητικά κάθε πακέτο μπορεί να υποκλαπεί από όποιον έχει πρόσβαση στο δίκτυο, να αποθηκευτεί και στη συνέχεια να αναπαραχθεί, μαζί με τα υπόλοιπα πακέτα, στο τερματικό του. Το απόρρητο των συνομιλιών μπορεί να ενισχυθεί κρυπτογραφώντας τις συνομιλίες. Παρόλα αυτά τα περισσότερα εταιρικά δίκτυα δεν την χρησιμοποιούν (αν και έχει αποδειχθεί ότι το 70-80% των υποκλοπών για την απόσπαση ευαίσθητων δεδομένων γίνεται από «μέσα»).[33] Ο λόγος για την απροθυμία αυτή είναι ότι η διαδικασία κρυπτογράφησης/αποκρυπτογράφησης καταναλώνει μεγάλη υπολογιστική ισχύ και εισάγει αισθητή καθυστέρηση. Καθώς, όμως, οι υπολογιστικές ταχύτητες των επεξεργαστών αυξάνονται ταχύτατα, σύντομα το πρόβλημα θα εξαλείφει .

Ένας άλλος παράγοντας που κάνει τα IPPBX ευάλωτα είναι η σηματοδοσία ή οποία μπορεί να παρέχει στους επιτιθέμενους κωδικούς πρόσβασης χρηστών, PINs και τηλεφωνικούς αριθμούς SIP. Κάποιος που επιτυγχάνει πρόσβαση σε πληροφορίες λογαριασμών χρηστών μπορεί να επέμβει με πολλούς κακόβουλους τρόπους (να χρεώσει δικές του κλήσεις στους λογαριασμούς αυτούς, να προωθεί τις κλήσεις σε άλλο αριθμό, να αλλάξει το μήνυμα του τηλεφωνητή κ.λπ.

Ποιότητα κλήσεων και ακεραιότητα (integrity): Η ποιότητα των κλήσεων μπορεί εύκολα να δεχθεί επίθεση, αν δε χρησιμοποιούνται μηχανισμοί ταυτοποίησης των πακέτων φωνής (όπως και συνήθως συμβαίνει). Για παράδειγμα, οι επιτιθέμενοι μπορούν να διακόψουν τις συνομιλίες σταματώντας τα RTP πακέτα, αλλάζοντας το περιεχόμενό τους και προωθώντας τα αλλοιωμένα στον παραλήπτη τους. Άλλα παρόμοια “man-in-the-middle” είδη επιθέσεων γίνονται σε wireless LANs, όταν για παράδειγμα ο επιτιθέμενος εισάγει θόρυβο ή «καθυστέρηση» (σιωπηλά κενά) στις ενεργές κλήσεις από ένα

παράνομο access point. Ένα βήμα παραπέρα βρίσκονται οι επιθέσεις άρνησης εξυπηρέτησης (Denial of Service - DoS). Τέτοιες επιθέσεις πλημμυρίζουν έναν voice agent με αιτήσεις εγκαθίδρυσης 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 τον λογαριασμό του.

Authentication: Η ταυτοποίηση 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 ταυτοποίηση των χρηστών. Οι συμμετρικές και ασύμμετρες μέθοδοι κρυπτογράφησης, οι οποίες εμπεριέχουν την ανταλλαγή μυστικών και ιδιωτικών κλειδιών, μπορούν να εξασφαλίσουν την ταυτοποίηση. 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 ταυτοποιούν τους χρήστες και εγκαθιστούν τις κλήσεις, μπορούν να βρίσκονται σε οποιονδήποτε server του δικτύου. Αυτό στην πραγματικότητα είναι δίκοπο μαχαίρι: οι καταγραμμένες πληροφορίες σχετικά με τις κλήσεις των χρηστών ίσως να είναι χρήσιμες για τη χρέωση και τον εντοπισμό τους, αλλά αυτές οι καταγραφές μπορούν να γίνουν στόχος πειρατείας. Επομένως, οι servers που φιλοξενούν τέτοιες ευαίσθητες πληροφορίες πρέπει να θωρακίζονται ακόμα πιο ισχυρά.

Non-Repudiation: Όταν έχουμε να κάνουμε με νομικά ζητήματα, όπως για παράδειγμα την ανάγκη να αποδείξουμε αν κάποιος εκπόνησε ή δέχτηκε μια κλήση, η μόνη πηγή πληροφόρησης στο παρελθόν ήταν οι λογαριασμοί των τηλεφωνικών εταιριών. Με το VoIP υπάρχει επιπλέον μέθοδος απόδειξης, και αυτή δεν είναι άλλη από το γεγονός ότι κανενός άλλου χρήστη τα πακέτα φωνής δε θα μπορούσαν να έχουν κρυπτογραφηθεί και αποκρυπτογραφηθεί με τη βοήθεια του ζεύγους του δημοσίου και ιδιωτικού κλειδιού του .

Πρόσθετα ζητήματα ασφάλειας: Άλλα ζητήματα ασφαλείας για ένα VoIP σύστημα αποτελεί η ανάγκη για την διασφαλίσει των βάσεων δεδομένων των servers που χρησιμοποιεί, οι υπηρεσίες που παρέχει καθώς επίσης και η αδιάλειπτη παροχή ηλεκτρικού ρεύματος. Στην κλασική τηλεφωνία το δίκτυο παραμένει λειτουργικό ακόμα και όταν υπάρχει διακοπή της ηλεκτροδότησης, Στην IP τηλεφωνία, αντίθετα, μια διακοπή στο δίκτυο παροχής ηλεκτρικού ρεύματος έχει ως αποτέλεσμα τον τερματισμό του τηλεφωνικού μας δικτύου. Είναι σαφές λοιπόν ότι ένας διαχωριστής δικτύου οφείλει να προστατέψει το δίκτυο του τόσο από ηλεκτρονικές απειλές όσο και από αιτίες όπως: διακοπή ρεύματος, φωτιά, κλοπή κ.τ.λ. Είναι κατανοητό πως δεν μπορούμε να προστατευτούμε ενάντια απ

όλες τις απειλές αλλά μπορούμε να προνοήσουμε έτσι ώστε να έχουμε την ελάχιστη διακοπή των παρεχόμενων υπηρεσιών μας σε περίπτωση που κάτι πάει στραβά.

Ανεξάρτητες μελέτες σε VoIP[45] εξοπλισμούς αρκετών κατασκευαστών έχουν δείξει ότι υπάρχουν σε αυτούς πολλές τρύπες ασφαλείας, τις οποίες μπορούν να εκμεταλλευτούν επιτήδειοι. Με τόσες διαφορετικές υλοποιήσεις του VoIP, η αποτελεσματική και συγχρόνως cost-effective θωράκισή του είναι μία πρόκληση για τους ειδήμονες.

Η ιδανική λύση για την ασφάλεια του VoIP είναι να προσαρμόζεται η ασφάλεια δυναμικά με βάση τις τρέχουσες απαιτήσεις και συνθήκες που επικρατούν, ανεξάρτητα από το πρωτόκολλο σηματοδοσίας και τη μέθοδο κρυπτογράφησης που έχει επιλεχθεί. Αυτό επιτρέπει στο επίπεδο ασφάλειας να «εξατομικευτεί» σε επίπεδο κλήσης (Dynamic per-call firewall control), όπως ακριβώς γίνεται και με την κατανομή των πόρων. Η προσέγγιση αυτή επιχειρεί επιπλέον να από-συσχετίσει την ασφάλεια από τα ειδικά χαρακτηριστικά της εκάστοτε υλοποίησης συσκευών από τους κατασκευαστές. Έτσι, η ιδανική λύση για την ασφάλεια δε θα χρειάζεται να μεταφράζει πρωτόκολλα σηματοδοσίας και να ερμηνεύει τα σήματα ελέγχου. Αντί αυτού, ένα πρωτόκολλο καθορισμένο από την IETF (RFCs 3303 και 3304) θα χρησιμοποιείται προκειμένου να επιτευχθεί ασφαλής επικοινωνία μεταξύ του Call Controller (softswitch ή IP-PBX) και των VoIP συσκευών ασφάλειας. Μια τέτοια προσέγγιση παρέχει υψηλή ασφάλεια και απόδοση, είναι συμβατή με κάθε πρωτόκολλο σηματοδοσίας, χειρίζεται σωστά τα κρυπτογραφημένα δεδομένα και αποφεύγει αρκετά από τα προβλήματα και τις παγίδες που αναφέρθηκαν προηγουμένως.

Ως ανακεφαλαίωση όλων των παραπάνω, η μελέτη ασφαλείας ενός VoIP συστήματος είναι σωστότερο και αποτελεσματικότερο να μην έρχεται «επικουρικά», μετά το σχεδιασμό του δικτύου, αλλά να θεωρείται μέρος της μελέτης και της σχεδίασης του δικτύου. Έτσι, κατά την εκπόνηση μελέτης ανάλυσης κινδύνων (risk analysis), φανερώνονται όλα τα τρωτά σημεία του δικτύου και, στη συνέχεια, αναπτύσσονται και προσαρμόζονται οι πολιτικές ασφαλείας στις συγκεκριμένες προδιαγραφές και αδυναμίες του δικτύου. Επιτυχής θεωρείται εκείνη η μελέτη που φέρνει την ισορροπία ανάμεσα στα επιθυμητά επίπεδα ασφάλειας, ποιότητας και κόστους των προσφερόμενων υπηρεσιών.

5.2 Απειλές κατά του VoIP

Τα συστήματα VoIP είναι επιρρεπή στους ίδιους τύπους επιθέσεων στους οποίους εκτίθενται όλα τα δικτυακά συστήματα. Security groups αναφέρουν ότι τα VoIP συστήματα αποτελούν στόχους και συνεχώς προκύπτουν νέες επιθέσεις κατά των συστημάτων παροχής υπηρεσιών VoIP.

Αλληλογραφία spam. Η υπηρεσία VoIP υπόκειται στο δικό της τύπο ανεπιθύμητου μάρκετινγκ, γνωστού ως «Spam over Internet Telephony» (Spam μέσω τηλεφωνίας Internet) ή SPIT.

- **Διακοπές.** Επιθέσεις διαδικτύου όπως οι ιοί και ιοί τύπου worm μπορεί να διαταράξουν την υπηρεσία ή ακόμη και να θέσουν την υπηρεσία VoIP εκτός λειτουργίας.

- **Ηλεκτρονικό «ψάρεμα» (phishing) μέσω φωνής** Γνωστό και ως «phishing», αυτό συμβαίνει όταν ένας επιτιθέμενος έλθει σε επαφή χρησιμοποιώντας τη γραμμή VoIP και επιχειρεί να σας ξεγελάσει ώστε να αποκαλύψετε πολύτιμα προσωπικά δεδομένα, όπως στοιχεία πιστωτικής κάρτας ή τραπεζικού λογαριασμού.

- **Απώλεια ιδιωτικού απορρήτου.** Το μεγαλύτερο μέρος της κυκλοφορίας VoIP δεν είναι κρυπτογραφημένο, καθιστώντας εύκολο για τους εισβολείς να παρακολουθούν τις συνομιλίες μέσω VoIP.

- **Παράνομη πρόσβαση (Hacking).** Οι hacker μπορούν να αποκτήσουν πρόσβαση στη σύνδεση VoIP και να χρησιμοποιήσουν τη γραμμή σας για να πραγματοποιούν κλήσεις. Σε ορισμένες περιπτώσεις, μπορεί ακόμη και να πουλήσουν τα στοιχεία της σύνδεσής σας στη μαύρη αγορά. Μόλις βρεθούν εντός του οικιακού δικτύου σας, οι hacker μπορούν να ψάξουν για ευαίσθητα στοιχεία που ενδέχεται να έχουν αποθηκευτεί στον υπολογιστή σας.

- **Εξάρτηση από το διαδίκτυο και το ηλεκτρικό δίκτυο.** Οποιαδήποτε στιγμή ο πάροχος της υπηρεσίας Internet ή το ηλεκτρικό δίκτυο τεθεί εκτός λειτουργίας, το ίδιο θα συμβεί και στην υπηρεσία VoIP. Η αδυναμία πραγματοποίησης εξερχόμενων κλήσεων από το οικιακό τηλέφωνό σας σε περίπτωση έκτακτης ανάγκης αποτελεί κίνδυνο, οπότε βεβαιωθείτε ότι έχετε πάντα φορτισμένο ένα κινητό τηλέφωνο ως εφεδρική συσκευή.

5.3 Περιορίζοντας τους κινδύνους

Η επικοινωνία μέσω τηλεφωνικών υπηρεσιών μέσω Internet (VoIP) είναι πολύ οικονομική και παρέχει πολλές συναρπαστικές λειτουργίες--απλά βεβαιωθείτε ότι την εγκαθιστάτε με ασφάλεια λαμβάνοντας τις εξής προφυλάξεις:

- **Ασφάλεια του εξοπλισμού.** Επιλέξτε εξοπλισμό VoIP που χρησιμοποιεί τα τρέχοντα πρότυπα RTCP, TLS, IPsec

- **Πιστοποίηση γνησιότητας και κρυπτογράφηση** Ενεργοποιήστε οποιεσδήποτε λειτουργίες πιστοποίησης γνησιότητας και κρυπτογράφησης που είναι διαθέσιμες στο σύστημα VoIP σας. Με τον τρόπο αυτό δεν θα επιτρέψετε σε μη εξουσιοδοτημένα άτομα να εισέλθουν στο δίκτυό σας και θα διασφαλίσετε το ιδιωτικό απόρρητο για τις κλήσεις σας.

- **Τείχος ασφαλείας (firewall) VoIP.** Χρησιμοποιήστε firewall ειδικά σχεδιασμένο για κυκλοφορία VoIP. Το firewall θα εντοπίσει ασυνήθιστα[23] πρότυπα κλήσεων και θα παρακολουθεί για ενδείξεις επίθεσης.

- **Ενημερωμένη προστασία από ιούς.** Χρησιμοποιήστε ενημερωμένη προστασία από ιούς και τεχνολογία προστασίας από αλληλογραφία spam στις συσκευές σας.

- **Δικαιώματα πρόσβασης.** Περιορίστε τα δικαιώματα πρόσβασης μόνο στον χρήστη που λειτουργεί το pbx και αν είναι δυνατό αφαιρέστε το δικαίωμα εγγραφής.

- **Απενεργοποίηση guest λογαριασμού:** Απενεργοποιήστε κάθε λογαριασμό χωρίς στοιχεία πρόσβασης καθώς επίσης και τις κλήσεις από ανώνυμους χρήστες. Με τον τρόπο αυτόν μπορείτε να αποφύγετε ανεπιθύμητες χρεώσεις

- **Κωδικοί χρήσης:** Χρησιμοποιείτε σύνθετους κωδικούς πρόσβασης που δεν βασίζονται σε λέξεις και περιέχουν σύμβολα. Μια καλή πρακτική ασφάλειας είναι να χρησιμοποιείται κάποια διαδικτυακή γεννήτρια κωδικών για κωδικούς που δεν χρειάζεται να θυμάστε.

- **Layer 2 security:** Χρησιμοποιήστε τις διευθύνσεις MAC των συσκευών σας έτσι ώστε να επιτρέπονται μόνο αυτές στο δίκτυο. Δεν αποτελεί πλήρες μέτρο προστασίας αλλά ενισχύει σημαντικά την ασφάλεια του δικτύου.

- **Επίγνωση.** Μπορείτε να ενεργήσετε ως μια συμπαγής γραμμή άμυνας, προσέχοντας για περίεργες δραστηριότητες στη γραμμή σας VoIP και αποκτώντας εξοικείωση με τις τεχνικές που χρησιμοποιούν οι επιτιθέμενοι.

Κεφάλαιο 6

IPv6

6 Internet Protocol version 6

6.1 Εισαγωγή

Το πρωτόκολλο TCP/IP είναι ένα σύνολο από πρωτόκολλα επικοινωνίας, δηλαδή πρότυπα κωδικοποιημένης ψηφιακής επικοινωνίας, που δημιουργήθηκαν από τους Vinton Cerf και Jon Postel στις Η.Π.Α. με σκοπό την ανάπτυξη αξιόπιστων στρατιωτικών δικτύων μεταφοράς πακέτων δεδομένων, με δυνατότητες αυτόματης εναλλακτικής δρομολόγησης, σε περίπτωση επίθεσης και καταστροφής μεμονωμένων κόμβων του δικτύου ή τμημάτων αυτού. Το 1994, το Υπουργείο Άμυνας της χώρας όρισε το TCP/IP ως πρότυπο για την ανάπτυξη των στρατιωτικών δικτύων, εξασφαλίζοντας συνεχή χρηματοδότηση της έρευνας, και το 1995 ο Dan Lynch και η Επιτροπή Αρχιτεκτονικής του Διαδικτύου (Internet Architecture Board) πραγματοποίησαν ένα τριήμερο event με θέμα τη χρήση του TCP στην βιομηχανία συστημάτων πληροφορικής. Στόχος αυτού του event ήταν η προβολή του προτύπου με σκοπό την ανάπτυξη εμπορικών προϊόντων. Τον Σεπτέμβριο του 1998, ο Lynch οργάνωσε την έκθεση «Interop Trade Show» στην οποία εταιρίες παρουσίασαν συμβατά με το TCP/IP εμπορικά προϊόντα, δίνοντας εκρηκτικές διαστάσεις στην εξέλιξη του Διαδικτύου, καθιστώντας το TCP/IP ως το κυρίαρχο πρωτόκολλο στο Διαδίκτυο.

Η στοίβα πρωτοκόλλων TCP/IP, που χρησιμοποιείται σήμερα στο διαδίκτυο, βασίζεται στην τέταρτη έκδοση του πρωτοκόλλου επικοινωνίας IP (Internet Protocol). Όπως αναφέρεται και στο δεύτερο κεφάλαιο κάθε συσκευή στο Διαδίκτυο λαμβάνει και χρησιμοποιεί μια μοναδική δημόσια διεύθυνση IPv4, με την οποία αναγνωρίζεται από τις άλλες συσκευές. Η εκρηκτική αύξηση των χρηστών και των συσκευών στο Διαδίκτυο καθώς και η χρήση ευρυζωνικών συνδέσεων, οδήγησε σε ταχεία εξάντληση των διαθέσιμων διευθύνσεων του IP. Για την αντιμετώπιση του προβλήματος, έχουν υιοθετηθεί διάφορες τεχνικές οι οποίες επιλύουν προσωρινά το πρόβλημα αλλά παράλληλα δημιουργούν πολλά περισσότερα. Το πρόβλημα αναγνωρίστηκε στις αρχές τις δεκαετίας του ενενήντα όπου ξεκίνησαν να αναζητούνται μέθοδοι επίλυσης. Κρίθηκε αναγκαίος ο εκσυγχρονισμός του πρωτοκόλλου. Την διαδικασία αυτή την ανέλαβε η Internet Engineering Task Force η οποία ανέπτυξε το IPv6. Το καινούργιο πρωτόκολλο περιγράφεται στο RFC1883 και δημοσιεύτηκε τον Δεκέμβρη του 1995.

6.2 Δομή και αρχιτεκτονική κεφαλίδας IPv6

Το πρωτόκολλο IPv6 έχει σχεδιαστεί με σκοπό να αντικαταστήσει το πρωτόκολλο IPv4, το οποίο χρησιμοποιείται εδώ και τριάντα χρόνια. Το IPv6 προσφέρει κάποια παραπάνω χαρακτηριστικά από το IPv4. Τα κύρια από αυτά είναι ο διευρυμένος χώρος διευθύνσεων από 32 bit σε 128 bit, η απλοποίηση της κεφαλίδας, καθώς και η υποστήριξη επιλογών και επεκτάσεων. Τέλος προσφέρει δυνατότητα μαρκαρίσματος των ροών κίνησης και δυνατότητα ασφαλείας. Το IPv6 πέρα από την πληθώρα διευθύνσεων που προσφέρει σε σχέση με το IPv4, προσφέρει επίσης και αυτόματη ρύθμιση των διευθύνσεων (auto-configuration). Η απλοποίηση της κεφαλίδας βοηθά στη μείωση του κόστους

δρομολόγησης για κάθε πακέτο αλλά και του κόστους εύρους ζώνης. Η επικεφαλίδα έχει σταθερό μέγεθος και οι δρομολογητές κάνουν καλύτερη επεξεργασία. Οι επιλογές και οι επεκτάσεις μπορούν να ενσωματωθούν σε διαφορετικές κεφαλίδες, δίνοντας στον δρομολογητή μεγαλύτερη ευκολία επεξεργασίας. Το μαρκάρισμα των ροών κίνησης κατηγοριοποιεί τα πακέτα ενός αποστολέα, προσφέροντας έτσι πιο σωστή λειτουργία. Τέλος η ασφάλεια που προσφέρει, δίνει τη δυνατότητα της πιστοποίησης του αποστολέα, αλλά και την κρυπτογράφηση των δεδομένων.

6.2.1 Η δομή της βασικής επικεφαλίδας στο IPv6

Η βασική επικεφαλίδα στο IPv6[7] έχει μέγεθος 320 bits(40bytes) και αποτελείται από τα εξής πεδία:

- Έκδοση (Version)
- Τάξη Κυκλοφορίας (Traffic Class)
- Ετικέτα Ροής (Flow Label)
- Μήκος Πακέτου (Payload Length)
- Επόμενη Κεφαλίδα (Next Header)
- Όριο Βημάτων (Hop Limit)
- Διεύθυνση Αφετηρίας (Source Address)
- Διεύθυνση Προορισμού (Destination Address)

Το πεδίο «Version» του IPv6 είναι ίσο με 6 και έχει μέγεθος 4 bits. Το πεδίο «Traffic Class» προσδιορίζει εάν το συγκεκριμένο πακέτο παρέχει μια υπηρεσία. Εάν δεν παρέχει κάποια υπηρεσία, η τιμή του είναι ίση με μηδέν. Το μέγεθος του πεδίου αυτού είναι 8 bits. Το πεδίο «Flow Label» χρησιμοποιείται για να αναγνωρίζεται ποιά πακέτα ανήκουν σε ποιά ροή. Το μέγεθος του πεδίου αυτού είναι 20 bits. Το πεδίο «μήκος πακέτου» περιέχει μια δυαδική τιμή, η οποία είναι ίση με το μέγεθος του πακέτου. Στην τιμή αυτή συνυπολογίζεται και το μέγεθος της κεφαλίδας. Το μέγεθος αυτού του πεδίου είναι 16 bits. Το πεδίο «επόμενη επικεφαλίδα» δείχνει το είδος της επικεφαλίδας που ακολουθεί, δηλαδή αν είναι επικεφαλίδα επιπέδου μεταφοράς ή επικεφαλίδα επέκτασης. Το μέγεθος αυτού του πεδίου είναι 8 bits. Το πεδίο «όριο βημάτων» είναι αντίστοιχο με το πεδίο time-to-live του IPv4 με μόνη διαφορά ότι το ένα πακέτο δεν έχει χρόνο ζωής, αλλά ένα όριο βημάτων. Το μέγεθος του πεδίου αυτού είναι 8 bits. Τα πεδία «διεύθυνση αφετηρίας» και «διεύθυνση προορισμού» εμπεριέχουν τις διευθύνσεις του αποστολέα και του παραλήπτη. Το μέγεθος για κάθε ένα από αυτά τα δυο πεδία είναι 128 bits.

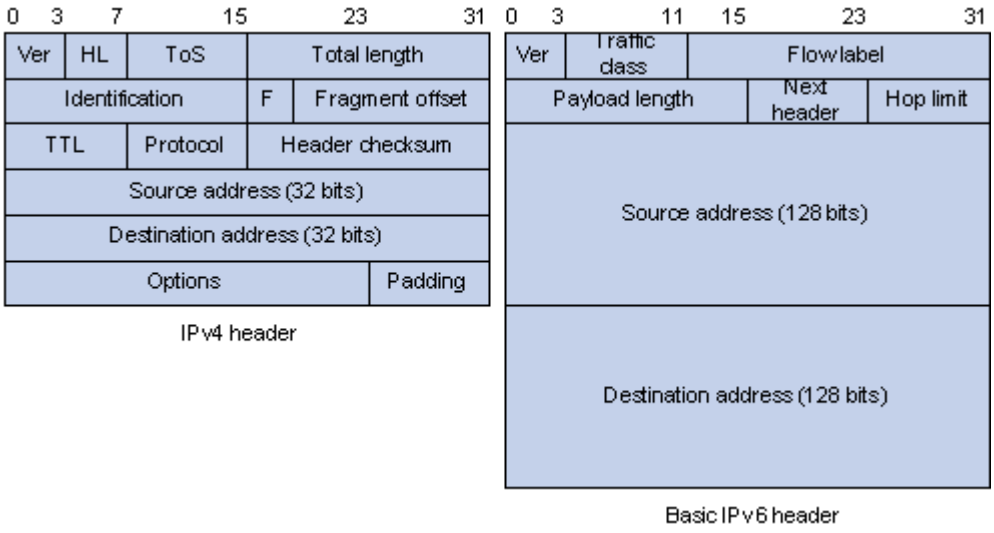
[7] (Cisco, 2006)

6.2.2 Προαιρετικές επικεφαλίδες του IPv6

Στην προηγούμενη ενότητα αναφερθήκαμε στην αρχιτεκτονική της βασικής επικεφαλίδας του IPv6. Το IPv6 προσφέρει τη δυνατότητα προσθήκης επικεφαλίδων επέκτασης, δίνοντας επιπλέον πληροφορίες για το πακέτο στο επίπεδο δικτύου. Στην περίπτωση χρήσης τέτοιων επικεφαλίδων στα πακέτα μας, οι επικεφαλίδες τοποθετούνται μεταξύ της βασικής επικεφαλίδας του IPv6 και της επικεφαλίδας του επιπέδου μεταφοράς. Ανάλογα με το περιεχόμενο και τα πεδία της κάθε επικεφαλίδας καθορίζεται αν πρέπει να προχωρήσουμε στην επόμενη κεφαλίδα. Αυτό γίνεται γιατί με εξαίρεση την επικεφαλίδα «Hop-by-Hop», οι επικεφαλίδες επέκτασης δεν εξετάζονται και δεν επεξεργάζονται από τους ενδιάμεσους κόμβους, που βρίσκονται πάνω στην διαδρομή του πακέτου. Ένα πακέτο μπορεί να έχει καμία, μία, ή περισσότερες επικεφαλίδες επέκτασης. Όταν χρησιμοποιούνται περισσότερες από μία επικεφαλίδες επέκτασης στο ίδιο πακέτο προτείνει να ακολουθούν και να εμφανίζονται με την εξής σειρά:

- Επικεφαλίδα IPv6 (IPv6 Header)
- Βήμα-προς-Βήμα Επικεφαλίδα (Hop-by-Hop Header)
- Επικεφαλίδα Επιλογών Προορισμού (Destination Option Header)
- Επικεφαλίδα Δρομολόγησης (Routing Header-RH)
- Επικεφαλίδα Διάσπασης (Fragmentation Header-FH)
- Επικεφαλίδα Πιστοποίησης (Authentication Header-AH)
- Επικεφαλίδα Ενσωματωμένης Ασφάλειας (Encapsulated Security Payload-ESP)
- Επικεφαλίδα Επιλογών Προορισμού (Destination Option Header)
- Επικεφαλίδα Ανώτερου Επιπέδου

Όπως φαίνεται παραπάνω στην περίπτωση που χρησιμοποιείται η επικεφαλίδα δρομολόγησης, η επικεφαλίδα επιλογών προορισμού, μπορεί να εμφανίζεται δυο φορές σε ένα πακέτο.



Εικόνα 17: Σύγκριση της επικεφαλίδας του IPv4 και του IPv6

6.2.3 Ανάλυση επικεφαλίδων επέκτασης

Hop by Hop Header: Χρησιμοποιείται για να μεταφέρει προαιρετικές πληροφορίες, οι οποίες πρέπει να εξεταστούν από κάθε κόμβο της διαδρομής. Αυτού του τύπου η επικεφαλίδα αναγνωρίζεται με κωδικό "0" από το πεδίο Next Header. Τα πεδία από τα οποία αποτελείται η επικεφαλίδα Βήμα-προς-Βήμα μπορούν να συνοψιστούν στα εξής:

- Επόμενη Επικεφαλίδα (Next Header)
- Μήκος Επικεφαλίδας (Hdr Ext Len)
- Επιλογές (Options)

Μια από τις βασικές επιλογές που έχουν οριστεί για την επικεφαλίδα Βήμα-προς-Βήμα είναι η επιλογή Μεγάλου Πακέτου (Jumbo Payload Option), η οποία χρησιμοποιείται για να αποστείλει πακέτα IPv6 με μέγεθος μεγαλύτερο των 65.535 bytes.

Επικεφαλίδα Δρομολόγησης (Routing Header): Χρησιμοποιείται στην περίπτωση που η πηγή θέλει να καθορίσει έναν ή περισσότερους ενδιάμεσους κόμβους μέχρι τον προορισμό. Η επικεφαλίδα δρομολόγησης αποτελείται από τα εξής πεδία:

- Είδος Δρομολόγησης (Routing Type)
- Εναπομείναντες Κόμβοι (Segments Left)
- Δεδομένα Δρομολόγησης (Type-Specific Data)

Επικεφαλίδα Διάσπασης (Fragment Header): Στην περίπτωση που θέλουμε να αποστείλουμε πακέτα, μεγαλύτερα από το MTU που έχει η διαδρομή σε μέγεθος, χρησιμοποιούμε την επικεφαλίδα διάσπασης. Το MTU (Maximum Transmition Unit) είναι το μέγιστο μήκος του πακέτου που υποστηρίζεται από όλους τους συνδέσμους της διαδρομής. Αντίθετα με το IPv4 η διάσπαση γίνεται μόνο από την πηγή. Τα πεδία από τα οποία αποτελείται η επικεφαλίδα είναι τα εξείς:

- Δεσμευμένο (Reserved)
- Μετατόπιση Διασποράς (Fragment Offset)
- Res
- M Flag
- Αναγνωριστικό (Identification)

Επικεφαλίδα Επιλογών Προορισμού (Destination Option Header): Η επικεφαλίδα επιλογών προορισμού χρησιμοποιείται για να μεταφέρει προαιρετικές πληροφορίες που χρειάζεται να εξεταστούν μόνο από τους κόμβους προορισμού.

Επικεφαλίδα Πιστοποίησης (Authentication Header): Η επικεφαλίδα πιστοποίησης προσφέρει ένα μηχανισμό υπολογισμού ενός κρυπτογραφικού αθροίσματος βάση κάποιων πεδίων της βασικής επικεφαλίδας του IPv6, των επικεφαλίδων επέκτασης και των δεδομένων. Εκτενέστερη περιγραφή γίνεται στην ενότητα 6.6.2

Επικεφαλίδα Ενσωματωμένης Ασφάλειας (Encapsulation Security Payloads):Αυτή η επικεφαλίδα είναι πάντα η τελευταία επικεφαλίδα (μη κρυπτογραφημένη) σε οποιοδήποτε πακέτο. Δείχνει ότι το υπόλοιπο μέρος, δηλαδή από αυτήν την κεφαλίδα του πακέτου και μετά, είναι κρυπτογραφημένο και προσφέρει αρκετές πληροφορίες για τον παραλήπτη, ώστε να το αποκρυπτογραφήσει. Αναλυτικότερα περιγράφεται στο κεφάλαιο της ασφάλειας αυτής της εργασίας.

6.3 Διευθυνσιοδότηση

Είναι γνωστό πως κάθε συσκευή η οποία θέλει να έχει επικοινωνία με το διαδίκτυο, στο interface το οποίο κάνει εφικτή αυτήν την επικοινωνία ανατίθεται μια μοναδική διεύθυνση IP ως όρισμα/αναγνωριστικό του συνόλου από interfaces. Η ανάθεση αυτή γίνεται ανεξάρτητα από το αν χρησιμοποιούμε IPv4 ή IPv6. Η διαφορά όμως, όπως προείπαμε, είναι πως στο IPv6 οι διευθύνσεις είναι 128 bit σε αντίθεση με το IPv4, όπου είναι 32 bit. Γι' αυτό το λόγο με το IPv6 αυξάνεται κατά πολύ το εύρος των διευθύνσεων στον κόσμο.

Άλλη μια βασική διαφορά μεταξύ του IPv4 και του IPv6 είναι πως πλέον στο IPv6 δεν υπάρχουν διευθύνσεις broadcast, καθώς η λειτουργία αυτή μπορεί να επιτευχθεί μέσω multicast διευθύνσεων. Υπάρχουν τρείς τύποι διευθύνσεων στο IPv6. Η πρώτη είναι η Unicast, στην οποία αν αποστέλλεται

ένα πακέτο, παραδίδεται στο interface που προσδιορίζεται απο τη διεύθυνση αυτή. Οι διευθύνσεις του Unicast είναι όρισμα μεμονωμένου interface. Η δεύτερη είναι η Anycast, στην οποία όταν αποστέλλεται ένα πακέτο, παραδίδεται στο interface, που προσδιορίζεται απο τη διεύθυνση αυτή (το πλησιέστερο, σύμφωνα με τον υπολογισμό απόστασης των πρωτοκόλλων δρομολόγησης). Οι διευθύνσεις anycast είναι όρισμα συνόλου από interfaces που ανήκουν συνήθως σε διαφορετικούς κόμβους. Τέλος υπάρχουν οι διευθύνσεις Multicast, στις οποίες όταν αποστέλλεται ένα πακέτο, παραδίδεται σε όλα τα interfaces, που προσδιορίζονται απο τη διεύθυνση αυτή. Οι διευθύνσεις τύπου Multicast είναι όρισμα συνόλου απο interfaces, που ανήκουν συνήθως σε διαφορετικούς κόμβους.

6.3.1 Απεικόνιση των διευθύνσεων

Στο IPv6 υπάρχουν τρείς συμβατικές φόρμες απεικόνισης διευθύνσεων.

Η προτιμώμενη φόρμα είναι X:X:X:X:X:X:X:X, όπου τα X αντιστοιχούν σε δακαεξαδικές τιμές των 16-bit το κάθε ένα. Στον παρακάτω παρουσιάζονται οι διευθύνσεις IPv6 δημοφιλών προορισμών.

Domain	Διεύθυνση IPv6
Facebook	2620:0:1cfe:face:b00c::3
Google	2001:4860:b002::68
OTE	2a02:580:200::200:
PirateBay	2002:c247:6b96::1
markoulidakis.eu	2001:648:2ffc:111b:a80c:f7ff:fe3d:121c

Πίνακας 3 Διευθύνσεις IPv6 δημοφιλών προορισμών

Στις διευθύνσεις IPv6 είναι σύνηθες να περιέχονται μεγάλες συμβολοσειρές μηδενικών bits. Για τις περιπτώσεις αυτές μπορούμε να χρησιμοποιήσουμε το «::» που προσδιορίζει πολλαπλές ομάδες μηδενικών 16-bits πεδίων. Χρησιμοποιώντας δηλαδή το «::» αυτό που κάνουμε είναι συμπίεση των μηδενικών, τα οποία βρίσκονται μέσα σε μια διεύθυνση. Το «::» μπορεί να εμφανιστεί μέσα σε **μια** διεύθυνση σε οποιοδήποτε σημείο και **μόνο μια φορά**. Ο παρακάτω πίνακας δείχνει τους διαφορετικούς τύπους IPv6 διευθύνσεων.

Τύπος	Κανονική μορφή	Μπορεί να αποδοθεί ως
Διεύθυνση unicast	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
Διεύθυνση multicast	FF01:0:0:0:0:0:0:101	FF01::101
Διεύθυνση loopback	0:0:0:0:0:0:0:1	::1
Απροσδιόριστη διεύθυνση	0:0:0:0:0:0:0:0	::

Πίνακας 4 Διαφορετικές μορφές IPv6 διευθύνσεων

6.3.2 Η διεύθυνση loopback

Η διεύθυνση loopback ή αλλιώς η διεύθυνση ανατροφοδότησης που αναφέρεται παραπάνω είναι τύπου unicast και έχει την μορφή 0:0:0:0:0:0:0:1. Η συγκεκριμένη διεύθυνση χρησιμοποιείται στην

περίπτωση που κάποιος κόμβος θέλει να αποστείλει ένα πακέτο τύπου IPv6 στον εαυτό του (αντίστοιχη της 127.0.0.1). Ποτέ δεν αποδίδεται αυτή η διεύθυνση σε φυσικό interface. Η διεύθυνση αυτή ανατίθεται σε ένα εικονικό interface κάποιου κόμβου και δεν πρέπει ποτέ να χρησιμοποιείται ως διεύθυνση αποστολέα που στέλνει πακέτα έξω από τον κόμβο.

6.3.3 Η απροσδιόριστη διεύθυνση

Η απροσδιόριστη διεύθυνση έχει την μορφή 0:0:0:0:0:0:0:0 και καλείται απροσδιόριστη γιατί μας δείχνει ότι υπάρχει απουσία διεύθυνσης. Όταν εμπεριέχεται στο πεδίο διεύθυνσης του αποστολέα κάθε πακέτου που αποστέλλεται από κάποιο κόμβο δείχνει ότι βρίσκετε σε φάση αρχικοποίησης προτού ο αποστολέας ενημερωθεί για την διεύθυνση του. Δεν μπορεί να χρησιμοποιηθεί ως διεύθυνση παραλήπτη ή για δρομολόγηση.

6.4 Δρομολόγηση

Σε αυτό το κεφάλαιο θα θίξουμε τα θέματα δρομολόγησης πακέτων στο IPv6. Θα αναλύσουμε την αρχιτεκτονική ενός IPv6 δικτύου, τους βασικούς αλγόριθμους υπολογισμού πινάκων δρομολόγηση και θα ολοκληρώσουμε μετα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται. Τα router ασχέτως αν είναι εσωτερικά ή εξωτερικά βασίζουν την λειτουργία τους σε πίνακες δρομολόγησης. Οι πίνακες δρομολόγησης μπορούν να δημιουργηθούν στατικά από τον διαχειριστή δικτύου είτε δυναμικά (αυτόματα) με την χρήση κάποιου αλγόριθμου. Οι αλγόριθμοι αυτοί λειτουργούν με ανταλλαγή πληροφοριών ανάμεσα στους δρομολογητές. Σήμερα οι πιο διαδεδομένοι αλγόριθμοι δρομολόγησης είναι οι κατανεμημένοι, δεν έχουν κάποιο κεντρικό σημείο όπου υπολογίζονται αλλά κάθε δρομολογητής υπολογίζει τον πίνακα του σε σχέση με τους υπόλοιπους. Από τις πιο μεγάλες οικογένειες κατανεμημένων αλγόριθμων δρομολόγησης είναι οι distance vector και οι link state. Για την υλοποίηση δυναμικής δρομολόγησης σε ένα δίκτυο είναι απαραίτητη η αναφορά στην μετρική η μετρική αναφέρεται σε δύο παράγοντες τον αριθμό των βημάτων από έναν κόμβο σε έναν άλλον και το κόστος (συχνά αναφέρεται ως βάρος) που είναι το άθροισμα του κόστους κάθε μονοπατιού από έναν κόμβο σε έναν άλλον. Τα κύρια πρωτόκολλα που χρησιμοποιεί το IPv6 για τον υπολογισμό των πινάκων δρομολόγησης είναι το RIPv6 το OSPFv6 το IDPR και πιθανώς το EIGPR. Πολλά από τα πρωτόκολλα υπήρχαν και σε παλαιότερες εκδόσεις του πρωτοκόλλου αλλά δεν μπορούν να χρησιμοποιηθούν χωρίς αλλαγές λόγω του διαφορετικού μεγέθους διευθύνσεων(128bits).

6.4.1 RIPv6

Το RIP(Routing information protocol) είναι τύπου IGP και σχεδιάστηκε από την Xerox το 1988. Χρησιμοποιείται ευρέως σε οικιακά δίκτυα και σε δίκτυα μικρών εταιρειών. Πάνω στο RIP έχουν βασιστεί πολλά πρωτόκολλα όπως το AppleTalk και το Banyan. Το RIP είναι ένα distance vector πρωτόκολλο στο οποίο κάθε δρομολογητής στέλνει τον πίνακα αποστάσεων του ανά τριάντα

δευτερόλεπτα. Σε κάθε πίνακα δρομολόγησης αποθηκεύεται μόνο ο καλύτερος επόμενος προορισμός για κάθε προορισμό. Ο βασικός περιορισμός του RIP είναι ότι επιτρέπει το πολύ 15hops. Εκτός αυτού το RIP αγνοεί την ταχύτητα των γραμμών απαγορεύοντας έτσι τον καθορισμό βάρους ή άλλων μετρικών.

Στο RIPv6 οι αλλαγές που έγιναν ήταν μόνο στο χειρισμό του νέου εύρους διευθύνσεων ώστε να μπορεί να χρησιμοποιηθεί το RIP με το IPv6. Ο σκοπός που δεν προστέθηκαν νέα χαρακτηριστικά είναι η διατήρηση της απλότητας υλοποίησης του πρωτοκόλλου ώστε να μπορεί να χρησιμοποιηθεί σε απλές συσκευές όπου δεν μπορούν να χρησιμοποιηθούν άλλα πρωτόκολλα. Το RIPv6 έχει μόνο δυο τύπους μηνυμάτων: Request και Respond και μεταφέρονται με UDP. Στο RIPv6 ένας περιορισμένος αριθμός προορισμών επιτρέπεται ανά πακέτο ώστε το συνολικό μέγεθος του IPv6 πακέτου να μην ξεπερνάει το MTU της σύνδεσης.

6.4.2 OSPFv6

Το OSPF(Open Shortest Path First) είναι ένα IGP πρωτόκολλο που σχεδιάστηκε το 1988 ειδικά για το IP και βασίζεται στον αλγόριθμο του Dijkstra. Το OSPF βασίζεται στην ιδέα της ιεραρχίας. Αρχή της ιεραρχίας είναι ένα σύστημα πρόσβασης το οποίο υποδιαιρείται σε δύο περιοχές, που κάθε μία περιλαμβάνει μια ομάδα διασυνδεδεμένων δικτύων. Η δρομολόγηση σε μια περιοχή ονομάζεται «intra-area» ενώ η δρομολόγηση ανάμεσα σε διαφορετικές περιοχές καλείται «inter-area». Οι δρομολογητές που χρησιμοποιούν το πρωτόκολλο χωρίζονται στις εξής κατηγορίες:

- Εσωτερικός δρομολογητής(internal router): Είναι οι δρομολογητές που συνδέουν υποδίκτυα που ανήκουν στην ίδια περιοχή. Οι δρομολογητές αυτοί χρησιμοποιούν μια μόνο οντότητα του αλγόριθμου. Σε αυτή την κατηγορία ανήκουν δρομολογητές που συνδέονται μόνο στο δίκτυο κορμού.

- Συνοριακός δρομολογητής περιοχής(area border router): Είναι οι δρομολογητές που συνδέονται στο δίκτυο κορμού και σε ακόμη μία ή περισσότερες περιοχές. Οι δρομολογητές αυτοί εκτελούν περισσότερες από μια οντότητες του αλγόριθμου. Οι δρομολογητές αυτοί προωθούν τις πληροφορίες που συλλέγουν από τις περιοχές στο δίκτυο κορμού.

- Δρομολογητής περιοχής κορμού(backbone router): Είναι δρομολογητές που συνδέονται μόνο στο δίκτυο κορμού ενώ για να συνδεθούν σε άλλες περιοχές χρησιμοποιούν τους συνοριακούς δρομολογητές. Οι δρομολογητές περιοχής κορμού είναι μια υποκατηγορία των εσωτερικών δρομολογητών.

- Συνοριακός δρομολογητής AS(Autonomous System boundary router): Είναι δρομολογητές που ανταλλάσουν πληροφορίες με άλλους δρομολογητές που ανήκουν σε διαφορετικά αυτόνομα συστήματα.

Οι αλλαγές που έγιναν στο πρωτόκολλο για να λειτουργήσει στο IPv6 έχουν σχέση με την διαφορετική σημειολογία που υπάρχει μεταξύ του IPv4 και του IPv6 καθώς και του τρόπου χειρισμού των διευθύνσεων. Οι βασικές αλλαγές που έγιναν στην έκδοση OSPFv6 είναι οι ακόλουθες:

- Το πρωτόκολλο OSPFv6 λειτουργεί με την λογική των συνδέσεων και όχι των υποδικτύων. Μια σύνδεση μπορεί να περιλαμβάνει περισσότερα του ενός υποδικτύου και δύο κόμβοι να επικοινωνούν απευθείας αν βρίσκονται στην ίδια σύνδεση και ας ανήκουν σε διαφορετικά υποδίκτυα.

- Προστέθηκε η δυνατότητα χρήσης παραπάνω από μια οντοτήτων του αλγόριθμου στην ίδια σύνδεση επιτρέποντας έτσι σε διαφορετικές περιοχές που μοιράζονται μια σύνδεση να παραμένουν ανεξάρτητες.

- Στο OSPFv6 χρησιμοποιείται η εξής παραδοχή: Κάθε δρομολογητής έχει μια link local unicast διεύθυνση για κάθε φυσική του σύνδεση. Τα πακέτα δρομολόγησης στέλνονται σε αυτή την διεύθυνση σύνδεσης ως πηγή. Οι δρομολογητές μαθαίνουν αυτές τις διευθύνσεις και τις χρησιμοποιούν στην πληροφορία για τον επόμενο κόμβο.

- Καταργήθηκε η πιστοποίηση από το OSPF αφού το IPv6 διαθέτει εγγενώς μηχανισμούς για προστασία αλλοίωσης των δεδομένων. Έτσι το OSPF χρησιμοποιεί το checksum του IPv6 το οποίο καλύπτει όλο το OSPF πακέτο αλλά και την κεφαλίδα IPv6.

- Στο OSPFv6 οι γειτονικοί σταθμοί αναγνωρίζονται μόνο από το Router ID τους.

6.4.3 BGP

Πρόκειται για το πιο διαδεδομένο EGP πρωτόκολλο, το οποίο χρησιμοποιεί TCP για μεγαλύτερη αξιοπιστία κατά την επικοινωνία μεταξύ διαφορετικών αυτόνομων συστημάτων. Η βασική λειτουργία του BGP είναι η ανταλλαγή πληροφοριών μεταξύ αυτόνομων πληροφοριακών συστημάτων με σκοπό την δημιουργία ενός γράφου που αναπαριστά όλα τα δυνατά μονοπάτια. Για την ανταλλαγή πληροφοριών το BGP χρησιμοποιεί τέσσερα μηνύματα.

- **UPDATE:** Χρησιμοποιείται για τη μεταφορά πληροφορίας σχετικά με τη δρομολόγηση.
- **KEEPALIVE:** Χρησιμοποιείται για τον έλεγχο μιας σύνδεσης.
- **NOTIFICATION:** Στέλνεται όταν γίνει διακοπή της BGP σύνδεσης.

Το πρωτόκολλο BGP-4 αλλά και γενικότερα τα πρωτόκολλα της κατηγορίας του είναι ανεξάρτητα του πρωτοκόλλου δικτύου, για τον λόγω αυτό το πρωτόκολλο BGP-4 είναι κατάλληλο για το IPv6, χωρίς την ανάγκη ιδιαίτερων μετατροπών. Η μόνη εξαίρεση είναι ότι το IPv6 ορίζει την εμβέλεια των unicast διευθύνσεων και το πότε πρέπει καθεμιά να χρησιμοποιείται. Αν και οι διευθύνσεις link-local χρησιμοποιούνται για να προσδιοριστεί το επόμενο βήμα κατά τη δρομολόγηση δεν είναι κατάλληλες

να χρησιμοποιηθούν από το πρωτόκολλο BGP λόγω της φύσης του πρωτοκόλλου BGP ως EGP πρωτόκολλο. Έτσι είναι ορισμένες φορές απαραίτητο να προσδιορίζεται το επόμενο βήμα από ένα πεδίο που περιέχει μία οικουμενική και μία διεύθυνση link-local.

6.4.4 ICMPv6

Το πρωτόκολλο ICMPv6 (Internet Control Message Protocol) αποτελεί ένα εγγενή μηχανισμό του IPv6 και πρέπει να υποστηρίζεται από όλες τις υλοποιήσεις του πρωτοκόλλου. Το πρωτόκολλο ICMPv6 συγκεντρώνει λειτουργίες που ήταν μοιρασμένες σε διαφορετικά πρωτόκολλα στο IPv4. Αναλυτικότερα, το ICMPv6 παρέχει τα χαρακτηριστικά των πρωτοκόλλων ICMP, IGMP (Internet Group Membership Protocol) και ARP (Address Resolution Protocol). Στο ICMP6 καταργούνται τα μηνύματα που δεν χρησιμοποιούνταν έτσι αποφεύγεται η υπερφόρτωση του δικτύου. Το ICMPv6 είναι ένα πρωτόκολλο με πολλαπλό σκοπό. Χρησιμοποιείται για διάγνωση προβλημάτων την εύρεση γειτόνων και τη διαχείριση multicast ομάδων. Τα μηνύματα που χρησιμοποιεί χωρίζονται σε δύο κατηγορίες: τα μηνύματα λάθους (error messages) και τα μηνύματα πληροφοριών (information messages).

- **«Παραλήπτης Μη Προσβάσιμος»** (Destination Unreachable): Το μήνυμα αυτό δημιουργείται όταν δεν μπορεί να παραδοθεί ένα μήνυμα/πακέτο, με αποτέλεσμα το πακέτο να απορρίπτεται. Ένα πακέτο απορρίπτεται χωρίς να δημιουργηθεί μήνυμα «παραλήπτης μη προσβάσιμος» μόνο στην περίπτωση που υπάρχει συμφόρηση στο δίκτυο, ώστε να μην επιδεινωθεί η κατάσταση.

- **«Πακέτο Πολύ Μεγάλο»** (Packet Too Big): Το μήνυμα αυτό δημιουργείται όταν το δίκτυο αναγκάζεται να απορρίψει ένα πακέτο που μέγεθος του ξεπερνά το MTU της σύνδεσης. Οι πληροφορίες που περιέχονται στο πακέτο μπορούν να χρησιμοποιηθούν στη διαδικασία υπολογισμού του MTU μιας σύνδεσης.

- **«Λήξη Χρόνου»** (Time Exceeded): Το μήνυμα αυτό δημιουργείται όταν ένας δρομολογητής αναγκάζεται να απορρίψει ένα πακέτο επειδή το Hop Limit (Όριο Βημάτων) είναι μηδέν ή έχει μειωθεί στο μηδέν. Το μήνυμα αυτό υποδεικνύει, για παράδειγμα, είτε ότι η αρχική τιμή του «ορίου Βημάτων» είναι πολύ μικρή είτε ότι η επαναδημιουργία (reassemble) ενός τεμαχισμένου (fragmented) πακέτου δεν μπορεί να ολοκληρωθεί μέσα στο διαθέσιμο χρονικό διάστημα.

- **«Πρόβλημα Παραμέτρου»** (Parameter Problems): Το μήνυμα αυτό δημιουργείται όταν ένα IPv6 πακέτο απορρίπτεται επειδή υπάρχουν προβλήματα στα πεδία της επικεφαλίδας IPv6.

Τα μηνύματα πληροφοριών του lCMPv6 χωρίζονται σε τρεις ομάδες; διαγνωστικά, διαχείρισης multicast ομάδων και αναζήτησης γειτόνων.

Διαγνωστικά μηνύματα

- «Αίτηση Ηχους» και «Απάντηση Ηχους» (Echo Request - Echo Reply) (διαγνωστικά μηνύματα):

- Τα μηνύματα αυτά υλοποιούν τη διαγνωστική εφαρμογή ping, με την οποία μπορεί κάποιος να διαπιστώσει εάν ένας προορισμός είναι προσβάσιμος.

Διαχείρισης Ομάδων

- Τα μηνύματα αυτά χρησιμοποιούνται για τη μεταβίβαση πληροφοριών σχετικά με τη διαχείριση multicast ομάδων από τους κόμβους στους δρομολογητές στους οποίους συνδέονται.

Μηνύματα εύρεσης Γειτόνων

- **«Διαφήμιση Δρομολογητή»** (Router Advertisement): Οι IPv6 δρομολογητές αποστέλλουν περιοδικά μηνύματα «Διαφήμισης Δρομολογητή» ως απόκριση στα μηνύματα «Παρακίνησης Δρομολογητή».

- **«Παρακίνηση Δρομολογητή»** (Neighbor Solicitation):

Τα μηνύματα «Παρακίνηση Δρομολογητή» μεταδίδονται σε multicast διευθύνσεις όταν ένας κόμβος θέλει να αναλύσει μια διεύθυνση από IPv6 σε επιπέδου σύνδεσης (link layer) ή όταν ένας κόμβος αναζητά εάν ένας γειτονικός κόμβος είναι προσπελάσιμος.

«Διαφήμιση Γείτονα» (Neighbor Advertisement): Όταν η κατάσταση ενός κόμβου μεταβάλλεται, ο κόμβος μεταδίδει ένα μήνυμα «Διαφήμιση Γείτονα» ώστε να μεταδώσει γρήγορα τις αλλαγές που πραγματοποιήθηκαν στην κατάσταση του.

«Ανακατεύθυνση» (Redirect): Το μήνυμα αυτό χρησιμοποιείται για να ενημερωθούν άλλοι κόμβοι για ένα καλύτερο πρώτο hop προς μια κατεύθυνση.

6.5 Πρωτόκολλο Εύρεσης Γειτόνων (Neighbor Discovery)

Ένα βασικό πρωτόκολλο για τη δρομολόγηση στο IPv6 είναι η λειτουργία εύρεσης γειτόνων. Το πρωτόκολλο αυτό στηρίζει την λειτουργία του στο ARP και το ICMP ενώ για την υλοποίηση του απαιτείται η αποστολή πέντε ειδικών μηνυμάτων ICMPv6. Με το πρωτόκολλο αυτό ένας σταθμός μπορεί να ανακαλύψει τους κόμβους και τους δρομολογητές που βρίσκονται συνδεδεμένοι στο ίδιο φυσικό μέσο. Με την χρήση του πρωτοκόλλου μπορεί να υπολογίσει το MTU της σύνδεσης να εντοπίσει προβλήματα με διπλές διευθύνσεις και να ανιχνεύσει απροσπέλαστους κόμβους λόγω

αλλαγών στα μονοπάτια. Τέλος το πρωτόκολλο αυτό επιτρέπει στους σταθμούς να αποδώσουν μόνοι τους διεύθυνση.

6.6 Ασφάλεια στο IPv6

Ως γνωστόν το διαδίκτυο δημιουργήθηκε και χρησιμοποιήθηκε για πρώτη φορά από τον αμερικανικό στρατό τη δεκαετία του 60. Η ανάγκη για την ένωση συσκευών μέσα στο διαδίκτυο έφερε στο φως το πρωτόκολλο IPv4. Τον καιρό εκείνο όταν δημιούργησαν το IPv4, δεν είχαν λάβει υπ' όψη κανένα θέμα ασφαλείας λόγω της φύσης του δικτύου. Ακόμα και όταν αναπτύχθηκε έξω από το στρατό που ήταν περιορισμένο στο να συνδέει ακαδημαϊκά ιδρύματα. Μετά την εξάπλωσή του στον υπόλοιπο κόσμο, η ασφάλεια ήταν ένα βασικό στοιχείο το οποίο έπρεπε να ενσωματωθεί, ώστε να μπορέσει να υπάρξει προστασία προσωπικών δεδομένων. Για να καλυφθεί αυτή η ανάγκη, η IETF δημιούργησε το IP Security Working Group, το οποίο είχε ως στόχο να σχεδιάσει μια αρχιτεκτονική ασφαλείας και αντίστοιχα πρωτόκολλα , τα οποία θα ήταν βασισμένα στο IPv6 πρωτόκολλο. Κατά τη διάρκεια αυτών των διεργασιών παρατηρήθηκε, πως η ασφάλεια η οποία ξεκίνησε να δημιουργείται για το IPv6, μπορούσε να ενσωματωθεί και στο IPv4. Η δημιουργία του IPv6 όμως εξ' αρχής είχε ως επιλογή την ασφάλεια και αυτή είναι μια σημαντική διαφορά στην ασφάλεια μεταξύ των πρωτοκόλλων IPv4 και IPv6. Δηλαδή με πιο απλά λόγια, η ασφάλεια στο IPv6 μπορεί να ενσωματωθεί πολύ πιο εύκολα σε σχέση με το IPv4, λόγω της αρχιτεκτονικής που έχει το πρωτόκολλο IPv6.

6.6.1 Το πρότυπο IPsec

Η ασφάλεια έχει στόχο, όπως προαναφέρθηκε, την προστασία προσωπικών δεδομένων. Αυτό μπορεί να επιτευχθεί με τρεις βασικούς τρόπους . Αρχικά πρέπει να υπάρχει πιστοποίηση (authentication) παραλήπτη. Δηλαδή να γίνεται πιστοποίηση στο αντίστοιχο πεδίο του πεκέτου, πως ο αποστολέας είναι αυτός που «αναγράφεται». Η ακεραιότητα δεδομένων (data integrity) έρχεται δεύτερη στον έλεγχο. Αυτό που κάνει είναι να ελέγχει μετά την πιστοποίηση, πως τα δεδομένα δεν έχουν αλλαχθεί κατά τη μετάδοσή τους απο τον αποστολέα στον παραλήπτη. Τέλος πρέπει να υπάρχει δυνατότητα απορρήτου (confidentiality), δηλαδή η μετάδοση να γίνεται με τετοιο τρόπο, ώστε τα δεδομένα να μπορούν να διαβαστούν μόνο απο τον παραλήπτη.

Το IPsec πρότυπο χρησιμοποιείται από το IP πρωτόκολλο ανεξαρτήτως έκδοσης. Το πρότυπο αυτό επιτυγχάνει ασφάλεια στο επίπεδο δικτύου. Στη χρήση αυτού του προτύπου εισάγονται και κάποιες βασικές υπηρεσίες. Ο έλεγχος πρόσβασης, δηλαδή η πρόσβαση σε μια υπηρεσία με χρήση κωδικού, η ακεραιότητα δεδομένων, η πιστοποίηση του αποστολέα, η προστασία ενάντια σε επιθέσεις τύπου επανάληψης πακέτου (packet replay), δηλαδή προστασία από επιθέσεις DOS (Denial of Service) με σκοπό τη μείωση διαθέσιμων πόρων, η κωδικοποίηση δεδομένων και η εξασφάλιση απορρήτου της ροής των δεδομένων είναι κάποιες από τις βασικές υπηρεσίες του προτύπου IPsec. Τα πρωτόκολλα του IPsec λειτουργούν κυρίως σε ένα δρομολογητή (router) ή σε κάποια πύλη ασφαλείας (Security

Association – SA). Μια τέτοιου είδους σύνδεση παρέχει υπηρεσίες ασφαλείας στη ροή των δεδομένων. Μια σύνδεση σχέσης ασφαλείας μπορεί να επιτευχθεί με την χρήση των πρωτοκόλλων Authentication Header (AH) και Encapsulating Security Payload (ESP). Η λειτουργία των επικεφαλίδων AH και ESP υποστηρίζονται πλήρως από το IPv6 και είναι υποχρεωτική η ύπαρξή τους σε αντίθεση με το IPv4. Το πρωτόκολλο AH παρέχει στον αποστολέα την δυνατότητα να δώσει μια ψηφιακή υπογραφή στα πακέτα που αποστέλλει. Αυτό γίνεται για να επιτευχθεί η ακεραιότητα και η πιστοποίηση των πακέτων που αποστέλλονται. Αντίθετα το πρωτόκολλο ESP παρέχει τη δυνατότητα κωδικοποίησης και ενθυλάκωσης των δεδομένων για κάθε ένα απο τα πακέτα τα οποία αποστέλλονται. Ανάλογα την περίπτωση το κάθε ένα απο αυτά τα δυο πρωτόκολλα μπορούν να λειτουργήσουν μαζί ή και χωριστά. Για παράδειγμα αν δεν απαιτείται το απόρρητο των δεδομένων και η πιστοποίηση αποστολέα, μπορεί να χρησιμοποιηθεί μόνο το AH πρωτόκολλο. Τα πρωτόκολλα AH και ESP μπορούν να χρησιμοποιηθούν με δυο διαφορετικούς τρόπους: στην απευθείας μετάδοση προστατεύοντας τα πρωτόκολλα των ανώτερων επιπέδων και στη μετάδοση με χρήση σηράγγων, προστατεύοντας ολόκληρο το πακέτο που αποστέλλεται.

6.6.2 Η επικεφαλίδα πιστοποίησης AH

Στο IPv6 η επικεφαλίδα πιστοποίησης προστίθεται μετά από τις επικεφαλίδες που επεξεργάζονται από τους ενδιάμεσους κόμβους και πριν από τις επικεφαλίδες που επεξεργάζεται ο παραλήπτης. Για τον υπολογισμό και την πιστοποίηση των δεδομένων πιστοποίησης, χρησιμοποιείται μια keyed one-way hash λειτουργία, όπως η keyed-MDS ή η keyed SHA. Ανάλογα με τον τρόπο με τον οποίο δημιουργήθηκε η σχέση ασφαλείας, δημιουργείται και η ακρίβεια της πιστοποίησης. Η επικεφαλίδα πιστοποίησης αποτελείται από τα εξής πεδία:

- Δείκτης παραμέτρων ασφαλείας (Security Parameters Index – SPI)
- Αριθμός ακολουθίας (Sequence Number)
- Δεδομένα πιστοποίησης (Authentication Data)

6.6.3 Η επικεφαλίδα ESP

Η επικεφαλίδα ESP δίνει τη δυνατότητα ανταλλαγής δεδομένων με χρήση κωδικοποίησης. Η επικεφαλίδα ESP έχει σχεδιαστεί με σκοπό να παρέχει μετάδοση πακέτων με χρήση κωδικοποίησης, πιστοποίηση του αποστολέα με χρήση κωδικοποιήσεων δημοσίου κλειδιού, προστασία από επιθέσεις τύπου επανάληψης και προστασία μέχρι ένα βαθμό από επιθέσεις τύπου ανάλυσης. Μπορεί να χρησιμοποιηθεί είτε για απ' ευθείας μετάδοση δεδομένων, είτε για τη μετάδοση με χρήση καναλιών (tunnel mode). Στην πρώτη περίπτωση μπορεί να μην επιτυγχάνεται η ασφάλεια των δεδομένων, αλλά μπορεί να γίνει μελέτη της κυκλοφορίας μεταξύ του αποστολέα και του παραλήπτη. Αντίθετα στην δεύτερη περίπτωση ένας μη εξουσιοδοτημένος κόμβος δεν μπορεί να βγάλει κανένα συμπέρασμα για την κυκλοφορία. Τα πεδία της επικεφαλίδας ESP είναι τα εξής:

- Δείκτης Παραμέτρου Ασφαλείας (Security Parameters Index – SPI)
- Αριθμός Ακολουθίας (Sequence Number)
- Δεδομένα Φορτίου (Payload Data)
- Συμπλήρωμα (Padding)
- Μήκος Συμπληρώματος (Padding Length)
- Επόμενη Επικεφαλίδα (Next Header)
- Δεδομένα Πιστοποίησης (Authentication Data)

6.7 Μεταβαίνοντας στο IPv6

Το μεγαλύτερο πρόβλημα που αντιμετωπίζουν οι μηχανικοί δικτύων σήμερα είναι η μετάβαση στο IPv6 αλλά κυρίως η επικοινωνία δικτύων που χρησιμοποιούν διαφορετικές εκδόσεις του πρωτοκόλλου. Για να επιτευχθεί επικοινωνία μεταξύ τέτοιων δικτύων έχουν υιοθετηθεί διάφοροι μηχανισμοί μετάβασης.

Οι μηχανισμοί που παρουσιάζονται είναι:

- Μηχανισμοί διπλής στοίβας
- Μηχανισμοί Tunneling
- 6to4
- Teredo

6.7.1 Μηχανισμοί διπλής στοίβας

Η τεχνική DSTM αναπτύχθηκε προκειμένου να επιτρέψει την επικοινωνία μεταξύ των IPv6 σταθμών και των IPv4 μόνο δικτύων. Η τεχνική βασίζεται στην χρήση ενός DHCPv6 server ο οποίος Η τεχνική Dual Stack Transition Mechanism (DSTM) έχει αναπτυχθεί προκειμένου να επιτρέψει την επικοινωνία μεταξύ των IPv6 σταθμών και των IPv4 only δικτύων (υποστηρίζουν μόνο IPv4) που υπάρχουν σήμερα. Είναι μια εναλλακτική πρόταση στις τεχνικές μετάφρασης επικεφαλίδας, που παρουσιάζονται αναλυτικότερα στη συνέχεια.

Ο DSTM ουσιαστικά αποτελεί ένα μηχανισμό, ο οποίος προκύπτει από το συνδυασμό τεχνικών απόδοσης IPv4 διευθύνσεων σε IPv6 σταθμούς και Dynamic Tunneling Interfaces (DTI).

Η τεχνική DSTM βασίζεται στη χρήση ενός DHCPv6 server, ο οποίος αποδίδει προσωρινά global IPv4 διευθύνσεις στους IPv6 σταθμούς που θέλουν να επικοινωνήσουν με κάποιον IPv4 σταθμό. Τα

IPv4 πακέτα ενθυλακώνονται σε IPv6 μέσω ενός DTI interface και μεταφέρονται μέσα στο IPv6 δίκτυο μέχρι τον συνοριακό δρομολογητή που ενώνει το IPv6 δίκτυο με το IPv4 δίκτυο. Η λειτουργία του μηχανισμού είναι αμφίδρομη, η αρχικοποίηση της επικοινωνίας μπορεί να γίνει είτε από την πλευρά του IPv6 σταθμού είτε από την πλευρά του IPv4. Αυτό αποτελεί και σημαντικό πλεονέκτημα της συγκεκριμένης μεθόδου σε σχέση με άλλες τεχνικές, οι οποίες επιτρέπουν την επικοινωνία των IPv6 σταθμών με το IPv4 δίκτυο και απαιτούν την αρχικοποίηση της επικοινωνίας μόνο από τον IPv6 σταθμό. Ο τρόπος λειτουργίας του μηχανισμού DSTM διαφέρει αν η επικοινωνία αρχικοποιείται από τον IPv6 σταθμό ή από τον IPv4 σταθμό. Ο IPv6 σταθμός στέλνει IPv4 πακέτα μέσω του DTI interface, το οποίο υλοποιεί την ενθυλάκωση σε IPv6 πακέτα και στη συνέχεια τα προωθεί προς το άλλο άκρο του Tunneling interface. Εκει τα πακέτα από-ενθυλακώνονται και προωθούνται πλέον προς τον IPv4 προορισμό.

6.7.2 Tunneling

Οι μηχανισμοί tunneling χρησιμοποιούνται για την επίτευξη IPv6 επικοινωνίας μέσω της υπάρχουσας IPv4 υποδομής, αλλά και αντίστροφα. Η κατηγοριοποίηση τους μπορεί να γίνει ανάλογα με το τμήμα της διαδρομής της επικοινωνίας στο οποίο εφαρμόζονται. Έτσι έχουμε τις παρακάτω γενικές κατηγορίες:

Router-to-Router: Στην περίπτωση αυτή το tunnel χρησιμοποιείται για να επιτευχθεί IPv6 επικοινωνία μεταξύ 2 δρομολογητών, οι οποίοι «καταλαβαίνουν» και τα δύο πρωτόκολλα (IPv4 και IPv6). Η επικοινωνία επιτυγχάνεται με ενθυλάκωση των IPv6 πακέτων σε πακέτα IPv4 και προώθηση αυτών πάνω από την IPv4 υποδομή. Άρα, σε αυτή την περίπτωση, το tunnel εξαπλώνεται πάνω σε ένα ενδιάμεσο τμήμα της συνολικής διαδρομής της επικοινωνίας.

Host-to-Host: Στην περίπτωση αυτή χρησιμοποιείται το tunnel για να επικοινωνήσουν απευθείας δυο IPv4/IPv6 σταθμοί με χρήση του του πρωτοκόλλου IPv6.

Router-to-Host: Αυτή η tunneling τεχνική χρησιμοποιείται για να προωθήσουν IPv6 πακέτα προς τον τελικό προορισμό οι ενδιάμεσοι δρομολογητές.

Στις πρώτες δύο περιπτώσεις, στο τέλος του tunnel βρίσκεται ένας δρομολογητής ο οποίος αποενθυλακώνει τοα IPv6 πακέτα και τα προωθεί στον τελικό προορισμό. Η IPv6 διεύθυνση των πακέτων δεν μπορεί να παρέχει καμία πληροφορία και σχετικά με την IPv4 διεύθυνση και συνεπώς αυτή η πληροφορία πρέπει να δοθεί μέσω ρύθμισης. Αντίθετα, στις δύο τελευταίες περιπτώσεις (host-to-host και router-to-host), τα IPv6 πακέτα ενθυλακώνονται προς ένα σταθμό, ο οποίος αποτελεί και τον τελικό αποδέκτη της μεταδιδόμενης πληροφορίας. Δηλαδή, τόσο η IPv6 διεύθυνση όσο και η IPv4 δείχνουν προς τον ίδιο σταθμό. Αυτό μπορεί να χρησιμοποιηθεί με την εφαρμογή κατάλληλων τεχνικών, έτσι ώστε η IPv4 διεύθυνση του τελικού σταθμού προορισμού να κωδικοποιείται μέσα στην

IPv6 διεύθυνση του πακέτου. Αποτέλεσμα αυτού είναι να μπορεί ο κόμβος που κάνει την ενθυλάκωση να καταλαβαίνει αυτόματα την IPv4 διεύθυνση του σταθμού προορισμού

6.7.3 6over4

Η μέθοδος 6over4 αναπτυχθήκε με κύριο σκοπό να επιτρέψει σε κάποιον απομονωμένο σταθμό IPv6, ο οποίος βρίσκεται πάνω σε φυσικό σύνδεσμο (link) χωρίς την παροχή native IPv6 υποστήριξης, να γίνει ένας πλήρως λειτουργικός IPv6 σταθμός με πρόσβαση στο IPv6 δίκτυο. Ο μηχανισμός 6over4 κάνει χρήση του IPv4 multicast διαχειριστικού τμήματος, το οποίο θεωρείται ως το επίπεδο διασύνδεσης πάνω από το οποίο δομείται η IPv6 στοίβα. Προκειμένου να χρησιμοποιηθεί η 6over4 μέθοδος, πρέπει το IPv4 διαχειριστικό τμήμα να υποστηρίζει multicast. Η 6over4 μέθοδος είναι εφαρμόσιμη στα όρια του ίδιου site και λόγω του ότι δεν χρησιμοποιεί IPv4-compatible IPv6 διευθύνσεις ή configured tunnels, παρέχει μεγάλη ανεξαρτησία, όσον αφορά την τεχνολογία των συνδέσμων που χρησιμοποιούνται αλλά και την τοπολογία του IPv6 δικτύου που επιχειρείται να εφαρμοστεί. Συχνά η μέθοδος 6over4 αναφέρεται και ως virtual Ethernet.

Ο τρόπος λειτουργίας της συγκεκριμένης τεχνικής είναι σχετικά απλός: Πα κάθε IPv6 LAN ορίζεται ένα multicast session, το οποίο «ακούν» τόσο οι σταθμοί που συμμετέχουν στο IPv6 υποδίκτυο όσο και ο δρομολογητής που δρομολογεί την κίνηση του προς τα έξω (λειτουργίες IPv6 neighbor/router discovery). Απαραίτητη προϋπόθεση: ο δρομολογητής να έχει υλοποιημένες και τις δύο στοίβες (IPv4 και IPv6) στο interface που εξυπηρετεί το virtual LAN.

Προκειμένου οι σταθμοί που χρησιμοποιούν τη συγκεκριμένη τεχνική να μπορούν να υποστηρίξουν stateless auto configuration, έχει οριστεί ότι το συμπλήρωμα του προθέματος FE80:0000/64 (χρησιμοποιείται στη stateless auto configuration διαδικασία) θα είναι η unicast IPv4 διεύθυνση του συνδέσμου, συμπληρωμένη (padded) από τα αριστερά με 32 bits, προκειμένου να συμπληρωθεί το σύνολο των 128 bits που αποτελούν την IPv6 διεύθυνση.

Ιδιαίτερη προσοχή πρέπει να δοθεί στην τιμή TTL που δίνεται στα multicast IPv4 πακέτα που μεταφέρουν την IPv6 κίνηση, έτσι ώστε η τιμή του να είναι αρκετά μικρή για να μην υπάρχουν διαρροές IPv6 κίνησης έξω από το multicast διαχειριστικό τμήμα.

6.7.4 Teredo

Ο μηχανισμός Teredo σχεδιάστηκε για τις περιπτώσεις όπου δεν μπορεί να εφαρμοστεί καμία από τις προηγούμενες μεθόδους. Η μέθοδος Teredo απευθύνεται σε κόμβους των οποίων ο πάροχος δεν είναι διατεθειμένος να παρέχει υποστηρίξει IPv6. Είναι σαφές πως με την πάροδο του χρόνου και την εξέλιξη των συσκευών και των δικτύων θα εκλείψει ή χρήση αυτής της τεχνικής. Ο μηχανισμός Teredo βασίζεται στην απόδοση διεύθυνσης και στην αυτόματη δημιουργία tunnel για την παροχή IPv6 σύνδεσης πάνω από IPv4 δίκτυα. Ο μηχανισμός αυτός δημιουργεί tunnels μέσω τον οποίον στέλνει την IPv6 κίνηση

6.8 VoIP και IPv6

Έχουμε τονίσει επανειλημμένως την αναγκαιότητα μετάβασης στο IPv6. Το VoIP είναι μια από τις υπηρεσίες που θα επωφεληθούν από την μετάβαση στο νέο πρωτόκολλο, και αποτελεί πολύ καλό παράδειγμα για τις προκλήσεις που θα πρέπει να αντιμετωπίσουν οι εταιρίες. Η ανάπτυξη νέων δικτύων στην Ασία έχει αυξηθεί και ασκεί πιέσεις στην διεθνή κοινότητα ενώ ή έλλειψη νέων block δημιουργεί προβλήματα στην IANA και δυσχεραίνει την κατάσταση. Σε έναν τέλειο κόσμο, η μετάβαση στο IPv6 θα γινόταν αυτόματα, θα ενεργοποιούσαμε το νέο πρωτόκολλο στις συσκευές μας και όλα θα δούλευαν. Δυστυχώς για όλους εμάς(ιδίως τους διαχειριστές δικτύων) κάτι τέτοιο δεν πρόκειται να συμβεί. Ένα εύλογο ερώτημα είναι λοιπόν: «γιατί δεν αλλάζουμε;». Η αλλαγή είναι τόσο μεγάλη που από μόνη της αποτελεί τροχοπέδη. Οι πάροχοι των TIER I & II δικτύων θα πρέπει να δαπανήσουν εκατομμύρια ευρώ για την αντικατάσταση του εξοπλισμού. Εκτός αυτού θα πρέπει να αλλάξουν και όλες οι υπόλοιπες δικτυακές συσκευές αλλά και οι δικτυακές εφαρμογές. Ο Geoff Johnson διευθύνων σύμβουλος της εταιρίας-ερευνητικό κέντρο Gartnet δήλωσε ότι οι εταιρείες θα αναγκαστούν να υιοθετήσουν dual-stack μηχανισμούς μέχρι ότου μεταβούμε πλήρως στο IPv6. Οι εταιρείες θα κρατήσουν το εσωτερικό IPv4 δίκτυο τους ενώ εξωτερικά θα έχουν διεύθυνση IPv6. Ο μηχανισμός NAT θα αναλάβει να μεταφράζει αυτές τις διευθύνσεις. Σύμφωνα με τον ίδιο μέχρι το 2015 οι επιχειρήσεις θα πρέπει να έχουν αντικαταστήσει το 20% του εξοπλισμού τους. Η υλοποίηση ενός τέτοιου ενδιάμεσου σταδίου θα ήταν αρκετά επίπονη και ιδίως για εφαρμογές όπως το VoIP. Στο πρώτο σημείο που δημιουργεί πρόβλημα η αλλαγή, είναι στου υλικού. Ο τηλεφωνικός εξοπλισμός θα έπρεπε να αντικατασταθεί προκειμένου να υποστηρίξει το νέο πρωτόκολλο ενώ ο server θα έπρεπε να ρυθμιστεί κατάλληλα. Ένας άλλος τομέας που χρειάζεται προσοχή είναι η ασφάλεια. Ως επί το πλείστον τα περισσότερα IPPBX βρίσκονται πίσω από μηχανισμούς NAT, αν και δεν μπορούμε να θεωρήσουμε το NAT σαν firewall (με τη στενή έννοια του όρου) το τηλεφωνικό κέντρο από απευθείας έκθεση στις διαδικτυακές απειλές. Αναφορές από διάφορες ομάδες ασφαλείας δείχνουν ότι τα δίκτυα τηλεφωνικών κέντρων στοχοποιούνται από ομάδες hacker.

Είναι μεγάλη μερίδα των ανθρώπων η οποία σαρώνει διευθύνσεις IP με σκοπό την ανεύρεση τηλεφωνικών συστημάτων. Η τεχνική είναι απλή, οι επιτιθέμενοι ψάχνουν για διευθύνσιες που ακούν στην θύρα του VoIP 5060, αν το σύστημα απαντήσει προσπαθούν να συνδεθούν με τους "εργοστασιακούς κωδικούς" ή χρησιμοποιούν εργαλεία «ωμής βίας» με την ελπίδα ότι έχουν ανακαλύψει ένα αδύναμο σύστημα. Αν η επίθεση είναι επιτυχής ο εισβολέας έχει αποκτήσει πρόσβαση και μπορεί να πραγματοποιήσει τηλεφωνικές κλήσεις οι οποίες βέβαια βαρύνουν τον ιδιοκτήτη τους συστήματος. Αν και οι επιχειρήσεις έχουν ξεκινήσει να αναπτύσσουν μηχανισμούς ασφαλείας για την προστασία των συστημάτων τους θα πρέπει να δουλέψουν σκληρά προκειμένου να διασφαλίσουν το δίκτυό αφού το νέο πρωτόκολλο ξεχωρίζει την κάθε δικτυακή συσκευή. Στην αρχή της ενότητας αναφέραμε ότι δεν υπάρχουν διαθέσιμα block διευθύνσεων για τα νέα συστήματα, αυτό

ενδέχεται να οδηγήσει τους παρόχους στην υλοποίηση NAT για να εξυπηρετήσουν τους πελάτες τους. Κάτι τέτοιο θα δημιουργούσε τεράστια προβλήματα στου πελάτες που χρησιμοποιούν VoIP δεδομένου ότι μια θύρα μπορεί να δεσμευτεί από μια εφαρμογή και επομένως έναν πελάτη. Τα πράγματα περιπλέκονται λοιπόν καθώς οι χρήστες που θα θέλουν voip θα πρέπει να έρχονταις σε συννενόηση για να ενεργοποιήσουν την υπηρεσία. Μια τεχνική που θα μπορούσε να συμβάλλει στην αντιμετώπιση του προβλήματος είναι η υλοποίηση της μεθόδου stun όπως κάνει το (skype). Το STUN είναι ένας μηχανισμός που επιτρέπει σε έναν κόμβο πίσω από NAT να βρει την εξωτερική του IP. Με την κατάλληλη εφαρμογή λοιπόν μπορούν οι πελάτες να εγγράφονται δυναμικά στο NAT του παρόχου και να τους ανατίθεται η θύρα 5060. Το μεγαλύτερο πλεονέκτημα που θα προσφέρει το IPV6 στις υπηρεσίες φωνής είναι η εξάλειψη του μηχανισμού NAT. Αυτό θα έχει σαν αποτέλεσμα mobile χρηστών. Οι εταιρίες θα μπορούν επωφεληθούν από αυτό το χαρακτηριστικό καθώς οι εξωτερικοί συνεργάτες θα μπορούν να δρομολογούν από οπουδήποτε τις κλήσεις τους και να τις χρεώνουν στην εταιρία. Η διαφορά ανάμεσα στις επικεφαλίδες κάνει το IPV6 να απαιτεί περισσότερους πόρους για την πραγματοποίηση μιας κλήσης. Αυτό θα ωθήσει τις εταιρίες να χρησιμοποιήσουν συνδέσεις μεγαλύτερης ταχύτητας. Στην παρακάτω εικόνα παρουσιάζεται το εύρος ζώνης που απαιτούν για την πραγματοποίηση κλήσεων, τα δύο πρωτόκολλα. Η σύγκριση γίνεται χρησιμοποιώντας ως δείγμα τους τρεις βασικούς κωδικοποιητές ήχου.

VoIP Packet	Packet Size	Over Ethernet	Over PPP w/RTP	Over PPP w/cRTP
IPv4 w/G.711 & G.722 at 64 kbps	20 ms/160 bytes/packet	87 kbps	82 kbps	68 kbps
IPv6 w/G.711 & G.722 at 64kbps	20 ms/160 bytes/packet	95 kbps	90 kbps	68 kbps
IPv6 + Header Extension w/G.711 & G.722 at 64kbps	20 ms/160 bytes/packet	98 kbps	94 kbps	69 kbps
IPv4 w/G.729 at 8 kbps	20 ms/20 bytes/packet	31 kbps	26 kbps	12 kbps
IPv6 w/G.729 at 8 kbps	20 ms/20 bytes/packet	39 kbps	34 kbps	12 kbps
IPv6 + Header Extension w/G.729 at 8 kbps	20 ms/20 bytes/packet	42 kbps	38 kbps	13 kbps

VoIP Bandwidth Consumption, IPv4 vs. IPv6
Calculations rounded to the nearest whole number

Εικόνα 18: Απαιτούμενο bandwidth για την SIP κλήση με χρήση IPv4&IPv6

Το μέγεθος της επικεφαλίδας του IPV6 επιφέρει μεγαλύτερη απαίτηση σε εύρος ζώνης ωστόσο αυτό δεν αποτελεί πρόβλημα εντός των τοπικών δικτύων ή σε περιπτώσεις που χρησιμοποιούμαι cRTP. Αντίθετα με την χρήση ασυμπίεστων αλγορίθμων χρειαζόμαστε 15% περισσότερο εύρος ζώνης με την χρήση μικρότερης επικεφαλίδας ενώ αυξάνεται στο 46% με την χρήση επικεφαλίδων επέκτασης. ΟΙ ειδικοί προβλέπουν ότι η μετάβαση θα πάρει 5 έως 10 χρόνια ενώ οι εταιρίες παροχής υπηρεσιών διαδικτύου θεωρούν ότι θα διακόψουν το IPV4 το 2020. Κατά τη διάρκεια αυτής της περιόδου πολλές εταιρίες θα λειτουργούν ακόμη στο παλαιό πρωτόκολλο και θα υπάρξει ανάγκη για την υλοποίηση

μηχανισμών διπλής στοίβας. Όπως δείχνουν τα πράγματα η μετάβαση για τις εταιρίες θα είναι εύκολη αναβαθμίζοντας απλώς τη σύνδεσή τους με το διαδίκτυο. Για τις μεγάλες επιχειρήσεις και τους οργανισμούς αυτό θα είναι εύκολο σε αντίθεση με τις μικρές εταιρίες και τα τηλεφωνικά κέντρα που θα επιβαρυνθούν ακόμη περισσότερο σε σχέση με τον τζίρο που παράγουν. Όλοι όμως θα πρέπει να επωμιστούν το κόστος αντικατάστασης του εξοπλισμού τους.

Κεφάλαιο 7

Asterisk

7 Asterisk PBX

7.1 Εισαγωγή

Το Asterisk είναι μια πλατφόρμα υλοποίησης IPPBX. Η πρώτη έκδοση του Asterisk αναπτύχθηκε από τον Mark Spencer το 1999. Ο Spencer δημιούργησε το Asterisk με κίνητρο την μείωση τηλεφωνικών δαπανών της επιχείρησής του. Όταν είδε τις μεγάλες δυνατότητες που προκύπτουν από την χρήση του, έκανε το Asterisk την κύρια απασχόληση της εταιρείας του. Έτσι το 2001 η εταιρεία μετονομάζετε σε Digium και από εταιρεία παροχής τεχνικής υποστήριξης χρηστών Linux μετατρέπεται σε εταιρεία ανάπτυξης τηλεφωνικών συστημάτων. Επίσημα, το Asterisk είναι ένα υβριδικό τηλεφωνικό κέντρο, μεταγωγής κυκλωμάτων και πακέτων με ενσωματωμένη λειτουργία IVR, και ACD (Automated Call Distribution). Ανεπίσημα, το Asterisk είναι το πιο ισχυρό, ευέλικτο, και εύκολα επεκτάσιμο τηλεπικοινωνιακό λογισμικό ανοιχτού κώδικα που υπάρχει σήμερα. Η ονομασία του προέκυψε από το σύμβολο του αστερίσκου (*), που χρησιμοποιείται στα Regular expressions για να αναπαραστήσει τα πάντα. Ομοίως, το Asterisk έχει σχεδιαστεί έτσι ώστε να είναι συμβατό με οποιαδήποτε συσκευή, λογισμικό και πρωτόκολλο τηλεφωνίας με σκοπό την ενσωμάτωσή του σε οποιαδήποτε τηλεφωνική εφαρμογή.

Εικόνα 19: Το λογότυπο του Asterisk

7.2 Downloading Asterisk

Το Asterisk είναι διαθέσιμο από την επίσημη ιστοσελίδα: http://www.asterisk.org και παρέχετε δωρεάν. Σήμερα το Asterik βρίσκεται στην έκδοση 11.3 L.T.S.(Long term Support). Επίσης στην ήδια σελίδα παρέχονται οι δοκιμαστικές εκδόσεις του λογισμικού, οι σημειώσεις έκδοσης καθώς επίσης και ο πηγαίος κώδικας του Asterisk.

7.3 Άδεια χρήσης

Το Asterisk διανέμεται ως ελεύθερο λογισμικό υπό την General Public License. Η άδεια αυτή επιτρέπει την ελεύθερη διανομή του Asterisk σε πηγαίο κώδικα και σε εκτελέσιμη μορφή, με ή χωρίς μετατροπές, με την προϋπόθεση όταν διανέμεται τροποποιημένο σε κάποιον τρίτο να συνοδεύεται από τον πηγαίο αρχικό κώδικα, συμπεριλαμβανομένων των αλλαγών, χωρίς κάποιο περεταίρω περιορισμό στην χρήση του (είτε για περαιτέρω τροποποιήσεις είτε για αναδιανομή). Η άδεια ελεύθερου λογισμικού (GPL) δεν επεκτείνεται απαραίτητα στο υλικό ή στο λογισμικό που πιθανώς χρησιμοποιείται σε συνδυασμό με το Asterisk, όπως για παράδειγμα τα softphones ή τα sip phones. Για εκείνες τις εφαρμογές στις οποίες η άδεια ελεύθερου λογισμικού (GNU – GPL) δεν είναι κατάλληλη και απαιτείται υποχρεωτικά κάποια μορφή άδειας για την λειτουργία τους, η εταιρεία Digium είναι αποκλειστικά αυτή που έχει το δικαίωμα να χορηγεί την άδεια για χρήση του Asterisk, έξω από την έννοια του ανοικτού λογισμικού (GPL).

7.4 Χρησιμοποιώντας το Asterisk

7.4.1 PBX

Το Asterisk μπορεί να χρησιμοποιηθεί ως αναλογικό PBX. Αυτό σημαίνει ότι μπορούμε να αναβαθμίσουμε ένα υπάρχον τηλεφωνικό κέντρο χωρίς να χρειαστεί να υποστούμε το κόστος μετάβασης σε VoIP. Για να γίνει αυτό το μόνο που χρειάζεται είναι ειδικό hardware για να συνδέσουμε τις τηλεφωνικές μας γραμμές και συσκευές. Μια άλλη δυνατότητα που μας παρέχει το Asterisk είναι η υλοποίηση ενός υβριδικού τηλεφωνικού δικτύου. Έτσι μπορούμε να χρησιμοποιήσουμε το παλαιό τηλεφωνικό μας δίκτυο σε συνδιασμό με voip συσκευές ακόμα και με ip παρόχους.

7.4.2 IP PBX

Το Asterisk πληροί όλες τις προϋποθέσεις για να χρησιμοποιηθεί ως IP PBX. Οι μόνες απαιτήσεις για να υλοποιηθεί ένα πλήρες τέτοιο τηλεφωνικό σύστημα, είναι ένας ηλεκτρονικός υπολογιστής (χωρίς αυτό να μας περιορίζει στην συσκευή) με εγκατεστημένο το Asterisk), ένα τοπικό δίκτυο και IP τηλεφωνικές συσκευές ή Softphones. Είναι ακόμη εφικτή η χρήση ασύρματων δικτύων για την ανάπτυξη ενός τηλεφωνικού δικτύου αλλά λόγω της φύσης των ασύρματων δικτύων προτείνεται η χρήση ενός ξεχωριστού wifi δικτύου. Το Asterisk είναι συμβατό με διάφορα πρωτόκολλα τηλεφωνίας που βασίζονται στο IP, όπως το SIP, MGCP, H.323, SCCP. Εντούτοις, είναι γνωστό ότι έχει μερικές ιδιαιτερότητες με ορισμένα πρωτόκολλα, και γι' αυτό συστήνεται η χρήση του πρωτοκόλλου SIP. Το Asterisk υλοποιεί το πρωτόκολλο IAX (Inter Asterisk eXchange), ένα πρωτόκολλο ανοικτού κώδικα που γράφτηκε με αφορμή το Asterisk. Το IAX πλεονεκτεί έναντι του SIP καθώς λειτουργεί καλύτερα σε περιβάλλοντα που κάνουν χρήση NAT [Βλ. ΚΕΦ 2.4.3].

7.4.3 Χαρακτηριστικά λειτουργίας

7.4.3.1 Βασικά χαρακτηριστικά

Μεταξύ πολλών άλλων χαρακτηριστικών, το Asterisk μπορεί να χρησιμοποιηθεί σε οποιαδήποτε από τις παρακάτω εφαρμογές:

- Private Branch Exchange (PBX)
- Ετερογενής πύλη Voice over IP (SIP, H.323, IAX,MGCP, SCCP)
- Συνδεσιμότητα με PSTN δίκτυα μέσω, ταυτόχρονα, ψηφιακών και αναλογικών γραμμών
- Interactive Voice Response (IVR)
- Automatic Call Distribution (ACD)
- Softswitch

- Conference server
- Number translation
- Calling card application
- Predictive dialler
- Ουρά αναμονής κλήσεων
- Απομακρυσμένα γραφεία με τα αντίστοιχα PBX τους
- Μουσική αναμονής για τους πελάτες που βρίσκονται σε ουρές κλήσεων, υποστηρίζοντας ροές πολυμέσων και αρχείων ήχου.
- Εκμετάλλευση μηχανών text-to-speach

7.4.3.2 Εσωτερικές κλήσεις

Το Asterisk μετά την εγκατάσταση του είναι έτοιμο να χρησιμοποιηθεί σαν τηλεφωνικό σύστημα. Το μόνο που απαιτείται είναι η προσθήκη των αριθμών. Η αριθμοδότηση που γίνεται καθορίζεται από τον εκάστοτε διαχειριστή δικτύου αν και συνηθίζετε για μικρές εταιρείες να χρησιμοποιούνται τριψήφιοι αριθμοί ενώ για μεγαλύτερες τετραψήφιοι.

7.4.3.3 Line trunking

Η ζεύξη γραμμών είναι το χαρακτηριστικό που επιτρέπει σε ένα ιδιωτικό τηλεφωνικό δίκτυο να επικοινωνήσει με το δημόσιο τηλεφωνικό δίκτυο. Το Asterisk υποστηρίζει μια μεγάλη ποικιλία από trunks. Μπορούμε να δημιουργήσουμε ένα IP trunk προς μια εταιρία παροχής VoIP και να δρομολογούμε τις κλήσεις μας χρησιμοποιώντας την σύνδεση του internet ή μπορούμε να χρησιμοποιήσουμε μία ή και περισσότερες γραμμές PSTN/ISDN.

7.4.3.4 Automatic Call Distribution

Το Asterisk παρέχει την δυνατότητα ελέγχου τον κλήσεων και να τις δρομολογεί βάση ενός προκαθορισμένου Dialplan. Εάν δεν παρέχονται αρκετές πληροφορίες από τον πάροχο της σύνδεσης με το εξωτερικό δίκτυο, μπορούμε να ζητήσουμε από τον καλούντα να εισάγει τις ζητούμενες πληροφορίες, χρησιμοποιώντας το πληκτρολόγιο ενός τονικού τηλεφώνου. Μόλις λάβει μια απόφαση όσον αφορά τη δρομολόγηση μιας κλήσης, μπορεί να τη στείλει σε μια επέκταση (τηλεφωνικό αριθμός), μια ομάδα επεκτάσεων, σε ένα ηχογραφημένο μήνυμα (μέσω IVR), στο φωνητικό ταχυδρομείο (voicemail), ή ακόμα και σε μια ομάδα υπαλλήλων - τηλεφωνητών που μπορούν να απαντήσουν τέτοιες κλήσεις. Επίσης μπορούμε να χρησιμοποιήσουμε ουρές αναμονής κλήσεων (call queues) για να εξυπηρετήσουμε αποτελεσματικότερα τους πελάτες μας. Αυτή η ευελιξία μας δίνει τη δυνατότητα να έχουμε ένα ισχυρό σύστημα διαχείρισης κλήσεων αυξάνοντας την ποιότητα επικοινωνίας των καλούντων, σε σχέση με μια απλή τηλεφωνική υπηρεσία. Η αυτοματοποιημένη

διανομή κλήσης (ACD – Automated Call Distribution) είναι η υπηρεσία η οποία υλοποιεί όλα τα παραπάνω, και μας δίνει την δυνατότητα να εξυπηρετούμε τους καλούντες με τον καλύτερο δυνατό τρόπο. Ένας σημαντικός παράγοντας που διαφοροποιεί το Asterisk σε σχέση με τα άλλα συστήματα PBX που υποστηρίζουν ACD, είναι ότι το Asterisk δεν απαιτεί την αγορά ειδικής άδειας χρήσης ή υλικού για την ενεργοποίηση και λειτουργία οποιουδήποτε από αυτά τα χαρακτηριστικά.

7.4.3.5 Call Detail Records

Το Asterisk διατηρεί λεπτομερή αρχεία κλήσεων για τις πραγματοποιηθέντες κλήσεις. Μπορούμε να αποθηκεύσουμε τις πληροφορίες αυτές σε αρχείο δεδομένων σε βάση δεδομένων και από εκεί να χρησιμοποιήσουμε κάποιο εργαλείο(excel) προκειμένου να εξάγουμε πληροφορίες. Χρησιμοποιώντας αυτές τις πληροφορίες μπορούμε να ελέγξουμε τη χρήση του τηλεφωνικού κέντρου και να εντοπίσουμε πιθανούς καταχρηστικού χρήστες/ Μελετώντας τα αρχεία αυτά, μπορούμε να δούμε πληροφορίες σχετικά με τις εισερχόμενες, τις εξερχόμενες, και τις αναπάντητες κλήσεις, όπως ημερομηνία και ώρα κλήσης, διάρκεια κλήσης, αριθμό καλούντος και καλούμενου, κ.α. Με κατάλληλη επεξεργασία των δεδομένων που προκύπτουν, οι χρήσεις αυτού του χαρακτηριστικού είναι πολλές. Για παράδειγμα, μπορούμε να συγκρίνουμε αυτά τα αρχεία με το λογαριασμό που μας στέλνει ο πάροχος τηλεφωνίας. Μας επιτρέπει να αναλύσουμε τις διεξαχθείσες κλήσεις και να απαντήσουμε σε ερωτήματα όπως “βρες μου τους δέκα συνηθέστερα καλούμενους τηλεφωνικούς αριθμούς”, ή ‘‘πες μου πόσες κλήσεις σε κινητά τηλέφωνα έχει κάνει μια συγκεκριμένη επέκταση – χρήστης – στο σύστημα’’. Θα μπορούσαμε επίσης να καθορίσουμε κάποια τηλεφωνικά νούμερα ή προεκτάσεις περιοχής που μας καλούν πολύ συχνά, έτσι ώστε να στοχεύσουμε το marketing της επιχείρησης στη σωστή περιοχή. Επίσης μπορούμε να εξετάσουμε πόση διάρκεια έχουν τα τηλεφωνήματα, να μετρήσουμε σε πόσες κλήσεις απαντούν συγκεκριμένοι υπάλληλοι και να συγκρίνουμε τα δεδομένα αυτά με το μέσο όρο. Χρησιμοποιώντας αυτές τις πληροφορίες, μπορούμε επίσης να προσδιορίσουμε τις καταχρήσεις όσον αφορά κλήσεις σε κινητά η υπεραστικά νούμερα που κοστίζουν και περισσότερο. Οι υπάλληλοι σε όλο τον κόσμο έχουν την τάση να «κλέβουν» την επιχείρηση, κάνοντας υπεραστικές κλήσεις μεγάλων αποστάσεων (και προς το εξωτερικό) και έτσι κοστίζουν χρήμα και χρόνο στους εργοδότες. Το Asterisk μας δίνει τα απαραίτητα εργαλεία για να ανιχνεύσουμε τέτοιες πιθανές σπατάλες και καταχρήσεις. Η σημασία των αρχείων αυτών δεν πρέπει σε καμία περίπτωση να υποτιμηθεί, καθώς αυτές οι πληροφορίες είναι ανεκτίμητες για ποικίλες επιχειρησιακές λειτουργίες.

7.4.3.6 Call Recording

Το Asterisk έχει τη δυνατότητα να ηχογραφεί τις κλήσεις που γίνονται μέσω του PBX. Μπορούμε να χρησιμοποιήσουμε αυτό το χαρακτηριστικό του Asterisk για να ελέγχουμε ,για παράδειγμα, τις κλήσεις που πήγαν άσχημα ή πήγαν καλά. Αυτό μπορεί επίσης να χρησιμοποιηθεί ως απόδειξη του περιεχόμενου κάποιας κλήσης για ικανοποίηση κάποιων πελατών ή τους συνεργατών, καθώς επίσης ενδεχομένως να φανεί χρήσιμο σε μια κατάσταση νομικής φύσεως. Η χρήση αυτής της υπηρεσίας εν

τούτοις, καθορίζεται από την κρίση και την πολιτική που ακολουθεί κάθε εταιρεία, όμως σε περίπτωση που χρησιμοποιείται θα πρέπει, για νομικούς λόγους, να ενημερώνεται σχετικά ο καλούμενος. Είναι όμως σημαντικό να εξεταστεί αν η χρήση της λειτουργίας αυτής κρίνεται απαραίτητη, κατά την καταγραφή των απαιτήσεων του τηλεφωνικού συστήματος με Asterisk στην αρχή, δεδομένου ότι μπορεί να αντιμετωπίσουμε ζητήματα μη επάρκειας του υλικού, και πιο συγκεκριμένα του χώρου αποθήκευσης, ειδικά εάν το Asterisk πρέπει να χειριστεί και να καταγράψει έναν σημαντικό αριθμό κλήσεων. Σε αντίθετη περίπτωση θα πρέπει να γίνουν τροποποιήσεις υλικού για την απροβλημάτιστη και αξιόπιστη λειτουργία της υπηρεσίας αυτής.

7.4.3.7 Interactive Voice Response

Η λειτουργία αυτόματης απάντησης με φωνή, ή IVR (Interactive Voice Response), σε ένα τηλεφωνικό κέντρο είναι εντυπωσιακή για κάθε επιχείρηση, και όχι μόνο. Η δύναμη και η ευελιξία ενός τέτοιου συστήματος στο τηλεφωνικό κέντρο, μας δίνει τη δυνατότητα να αποκριθούμε στους πελάτες με τον πιο εντυπωσιακό και αποδοτικό τρόπο. Μπορούμε να χρησιμοποιήσουμε το Asterisk για να παρέχουμε εικοσιτετράωρη τηλεφωνική υπηρεσία (24 ώρες την ημέρα, 7 ημέρες την εβδομάδα) μειώνοντας έτσι το φόρτο εργασίας για τους υπαλλήλους, αλλά και συνεπώς το λειτουργικό κόστος μιας επιχείρησης. Το Asterisk μας επιτρέπει να αναπαράγουμε προεπιλεγμένα ή τα δικά μας ηχογραφημένα μηνύματα, να εκφωνήσουμε κάποιο κείμενο, ή ακόμη και να ανακτήσουμε πληροφορίες από μια βάση δεδομένων οι οποίες θα αναπαραχθούν αυτόματα με ειδικό λογισμικό. Παρόμοια τεχνολογία χρησιμοποιούν τα συστήματα αυτόματης πληρωμής λογαριασμών ή τραπεζικών κινήσεων μέσω τηλεφώνου. Όταν καλούμε την τράπεζα ακούμε συνήθως διάφορα ηχογραφημένα μηνύματα και δίνουμε εντολές ζητημάτων χρησιμοποιώντας συνήθως ένα τηλέφωνο τόνων (touch tone). Παραδείγματος χάριν, μπορούμε να ακούσουμε τους χαιρετισμούς και τα μηνύματα μας, τον τύπο του λογαριασμού μας και άλλα προσωπικά μηνύματα πληροφοριών ή επικύρωσης. Επίσης συχνά ακούμε τις προσωπικές μας πληροφορίες, οι οποίες ανακτώνται από μια βάση δεδομένων, όπως οι τελευταίες μας συναλλαγές ή το υπόλοιπο του τραπεζικού μας λογαριασμού. Τέτοια συστήματα μπορούν να υλοποιηθούν εύκολα και οικονομικά, χρησιμοποιώντας το Asterisk.

7.4.3.8 Voice-Mail

Το Asterisk περιλαμβάνει ένα πλήρως λειτουργικό σύστημα φωνητικού ταχυδρομείου. Το σύστημα φωνητικού ταχυδρομείου είναι εκπληκτικά ισχυρό. Υποστηρίζει ομάδες ρυθμίσεων φωνητικού ταχυδρομείου (voicemail contexts) έτσι ώστε πολλά διαφορετικά συστήματα φωνητικού ταχυδρομείου με διαφορετικές ρυθμίσεις να μπορούν να φιλοξενηθούν από τον ίδιο κεντρικό υπολογιστή. Υποστηρίζει διαφορετικές χρονικές ζώνες έτσι ώστε οι χρήστες να μπορούν να καταλάβουν πότε έγινε κάποια κλήση όταν παίρνουν τα μηνύματά τους. Παρέχει ακόμη την δυνατότητα ενημέρωσης κάθε χρήστη μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail) για τα

νέα μηνύματα που έχει λάβει, και στην πραγματικότητα μπορεί ακόμη και να επισυνάπτει το περιεχόμενο των μηνυμάτων, και να το αποστέλλει σε κάποιον λογαριασμό ηλεκτρονικού ταχυδρομείου.

7.4.4 Other distributions

Όπως αναφέραμε και στις προηγούμενες ενότητες το Asterisk παρέχει μια πληθώρα λειτουργιών και ευκολιών στον χρήστη. Σε αυτό που υστερούσε πραγματικά το Asterisk ήταν το γραφικό περιβάλλον. Όλη η παραμετροποίηση του Asterisk γινόταν μέσω των αρχείων ρυθμίσεων ή με χρήση εντολών. Αυτό δημιουργούσε προβλήματα στην επόπτευση της εγκατάστασης αλλά και στην χρήση του Asterisk από ανθρώπους που δεν ήταν τόσο εξοικειωμένοι με το Unix και bash. Έτσι διάφορες ανεξάρτητες από την Digium εταιρείες ξεκίνησαν να αναπτύσσουν και να πουλάνε διανομές που παρείχαν τον asterisk μαζί με το γραφικό τους περιβάλλον. Τα περισσότερα GUIS που υπάρχουν σήμερα για τον Asterisk βασίζονται στο λειτουργικό CentOS και το γραφικό περιβάλλον παρέχεται μέσα από το web. Ένα από τα πρώτα web περιβάλλοντα που αναπτύχθηκαν για τον Asterisk ήταν το "Asterisk Management Portal". Η ανάπτυξή του ξεκίνησε το 2004 ενώ λόγω πνευματικών δικαιωμάτων τον Μάιο του 2006 μετονομάστηκε σε Freepbx. Το 2007 η Digium λανσάρει το AsteriskNow το οποίο από τις αρχές του 2013[8] χρησιμοποιεί το Freepbx ως web interface.

[8] Σύμφωνα με την ιστοσελίδα asterisk.org

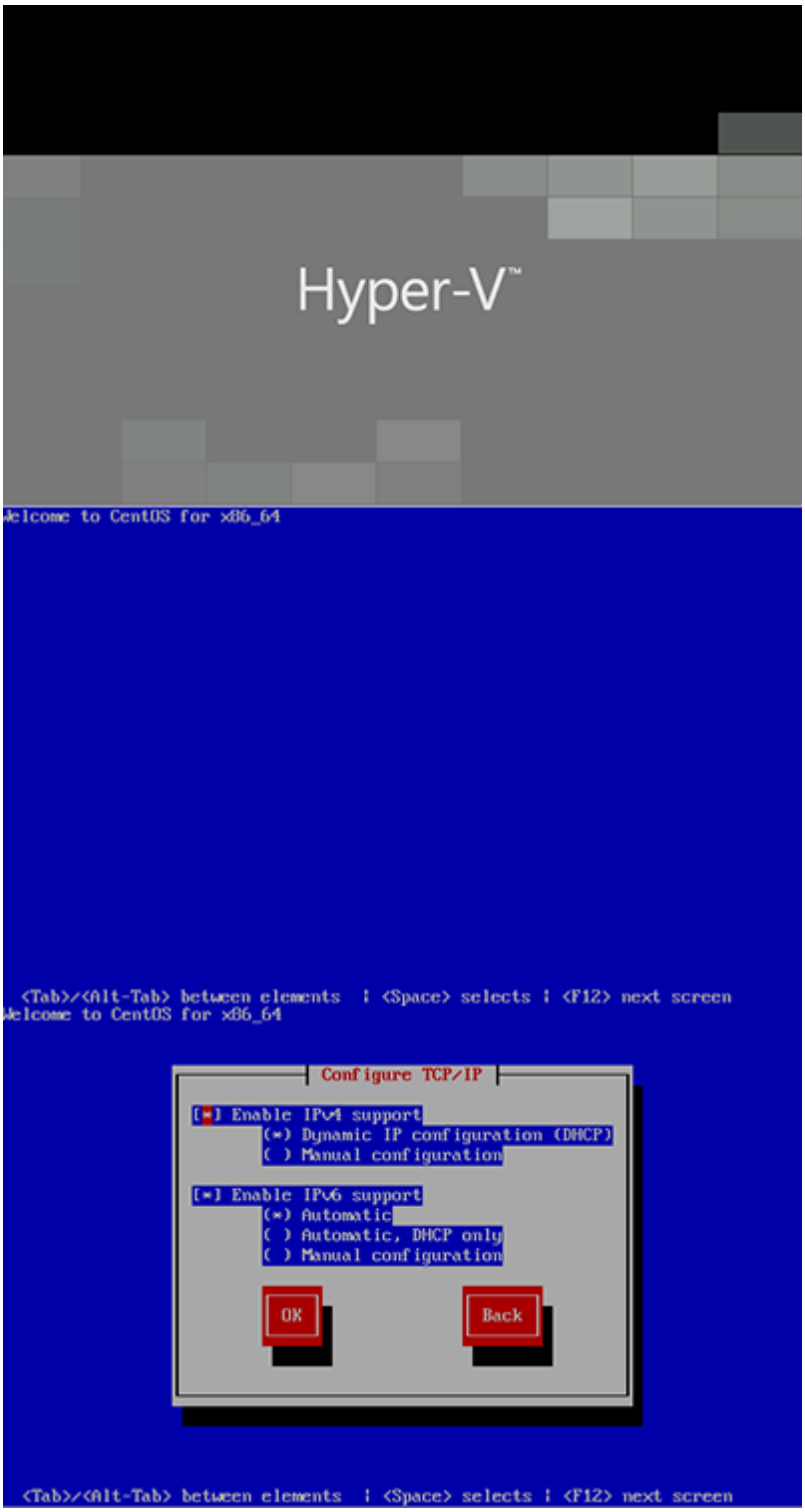
Παράρτημα Α

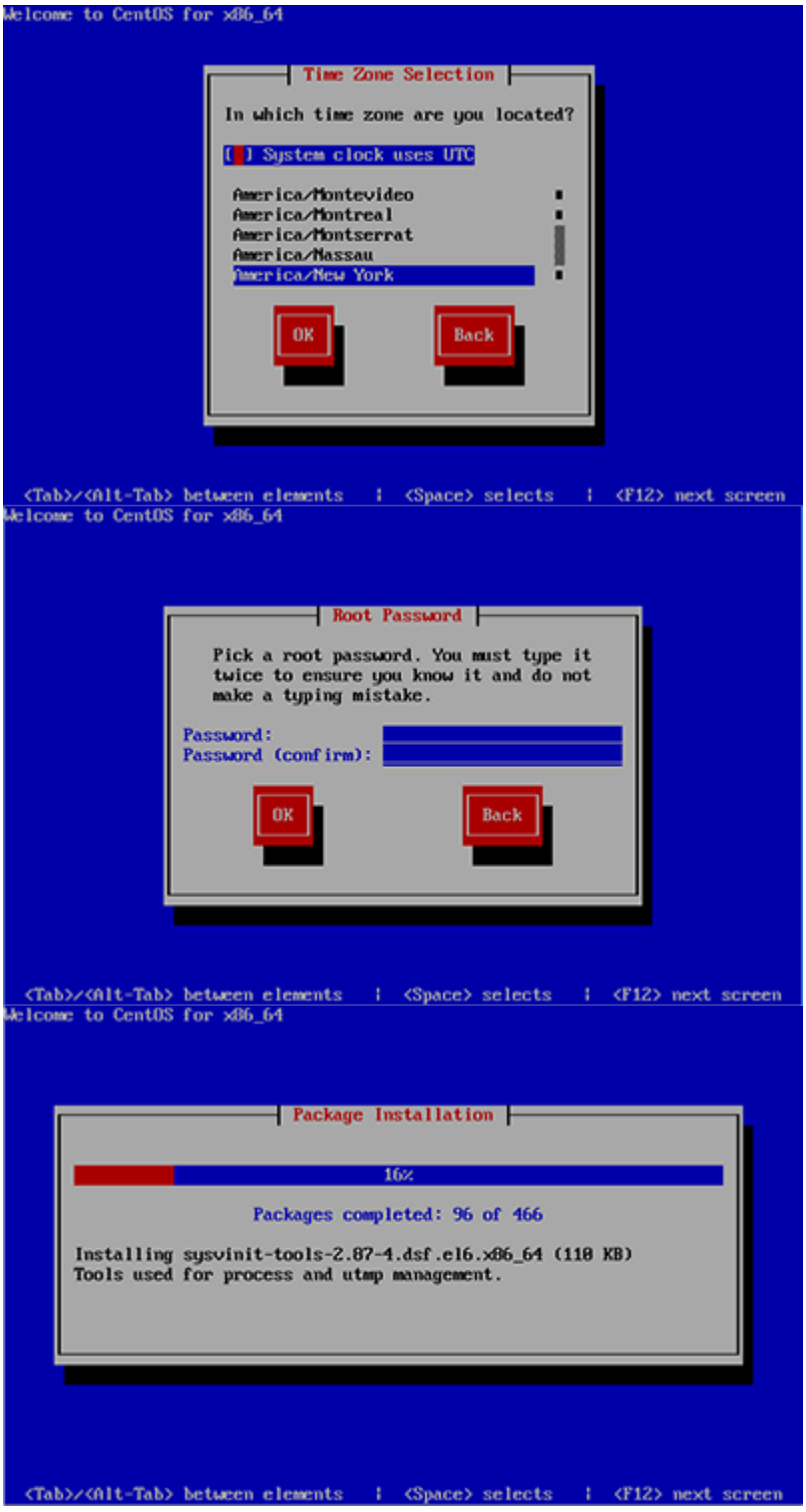
FreePBX

Παράρτημα Α: Εγκατάσταση Freepbx

Στο παράρτημα Α περιγράφεται η εγκατάσταση του Freepbx. Η λήψη του Freepbx είναι δωρεάν και μπορεί να πραγματοποιηθεί από την επίσημη ιστοσελίδα της πλατφόρμας: http://www.freepbx.org/. Το Freepbx διατίθεται σε εκδόσεις για επεξεργαστές 32 και 64bit. Χρησιμοποιεί το CentOS και παρακάτω παρουσιάζεται η διαδικασία εγκατάστασης 4.211.64-1 Beta.

Η διαδικασία εγκατάστασης είναι αρκετά απλή και είναι όμοια με αυτή του CentOS. Αφού ο υπολογιστής φορτώσει το πρόγραμμα εγκατάστασης από το μέσο(usb disk – cdrom – PXE) μας ζητάει να ρυθμίσουμε το δίκτυο. Η πιο απλή μορφή είναι να χρησιμοποιήσουμε Αυτόματη ρύθμιση του IPv4 και να απενεργοποιήσουμε το IPv6(εκτός και αν χρησιμοποιείται από το δίκτυό μας). Στην συνέχεια μας ζητάει να ρυθμίσουμε την ζώνη ώρας στην οποία βρισκόμαστε και να διαλέξουμε την διάταξη του πληκτρολογίου (συνίσταται η επιλογή EN_US και όχι EL_GR). Η διαδικασία εγκατάστασης (από μέρους μας) ολοκληρώνεται με τον ορισμό του Root password.


Hyper-V™
Welcome to CentOS for x86_64
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen
Welcome to CentOS for x86_64
Configure TCP/IP
[*] Enable IPv4 support
(*) Dynamic IP configuration (DHCP)
( ) Manual configuration
[*] Enable IPv6 support
(*) Automatic
( ) Automatic, DHCP only
( ) Manual configuration
OK
Back
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen



Εικόνες Ι Στάδια εγκατάστασης Freepbx

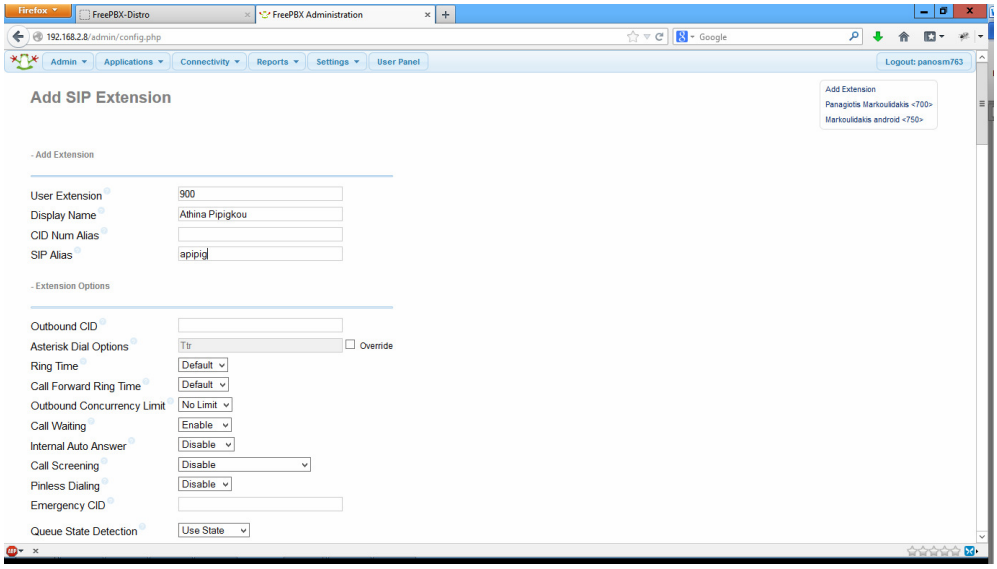
Δημιουργία Extension

Η δημιουργία extension «εσωτερικών αριθμών» είναι απλή και γρήγορη. Από το menu Applications επιλέγουμε “extension” -> “Add new” -> “Generic SIP device”.

Εικόνα 20 Add extension menu

Στην νέα σελίδα που εμφανίζεται συμπληρώνουμε τα στοιχεία του νέου μας χρήστη. Τα απαραίτητα πεδία είναι:

- User Extension: Ο αριθμός του χρήστη
- Display Name: Το όνομα που θα δείχνει όταν καλεί
- Secret: Ο κωδικός ταυτοποίησης του χρήστη



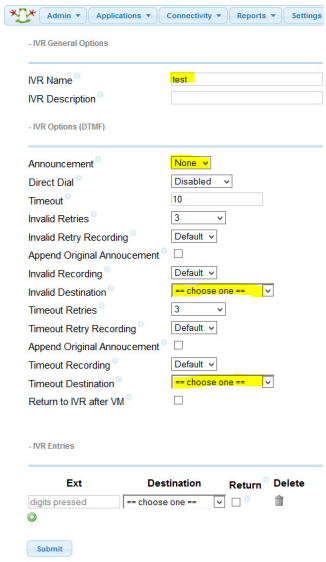
Εικόνα 21: Add Extension 2

Αφού προσθέσουμε δυο χρήστες μπορούμε να πραγματοποιήσουμε εσωτερικές κλήσεις.

Δημιουργία IVR

Ένα από τα πιο αγαπητά χαρακτηριστικά των τηλεφωνικών κέντρων είναι τα τηλεφωνικά menu «I.V.R». Για την δημιουργία ενός τηλεφωνικού μενού απαιτείται η ηχογράφηση ενός εισαγωγικού μηνύματος. Η διαχείριση των ηχογραφήσεων γίνεται από την καρτέλα “System Recordings” και μας δίνεται η δυνατότητα να ανεβάσουμε μια έτοιμη ηχογράφηση σε μορφή wav ή να ηχογραφήσουμε

μια καινούργια από κάποιο τηλέφωνο. Στην συνέχεια πηγαίνουμε στο menu “I.V.R” και πατάμε “Add New”.



Τα απαραίτητα πεδία για την δημιουργία ενός Τηλεφωνικού μενού είναι.

- IVR Name: Το όνομα του Menu
- Invalid destination: Ο προορισμός που θα προωθήσει το τηλεφωνικό κέντρο την κλήση στην περίπτωση που ο προορισμός δεν υπάρχει.
- Timeout destination: Ο προορισμός όταν λήξει το χρονικό όριο επιλογής.
- IVR entries: Αποτελούν τις επιλογές του τηλεφωνικού μενού. Δηλώνουμε τον συνδιασμό πληκτρολόγησης της επιλογής και τον προορισμό.

8 Ευρετήριο ορολογίας.

9 Βιβλιογραφία

01. Atsushi Kobayashi, K. I. (2009). *VoIP Measurement Architecture Using Data Mediation.*

02. Balliache, L. (n.d.). QoS τι είναι και πως δουλεύει.

03. Chen, J. B. (n.d.). Implementing VoIP: A Voice transmission performance progress report. *IEEE communication magazine*.

04. Cisco. (2005). *IPv6 QoS At a Glance.* Ανάκτηση από http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8026004d.pdf

05. Cisco. (2006). *IPv6 Extension Headers Review and Considerations.* Ανάκτηση από http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

06. Cisco. (2008). Ανάκτηση από RTP Header Compression and QoS: http://www.cisco.com/en/US/tech/tk543/tk762/technologies_tech_note09186a0080108e2c.shtml

07. Cisco. (2012). Ανάκτηση από Implementing VoIP for IPv6: http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-voip.html

08. David Irwin, J. S. (2011). *EXTRACTING EVIDENCE RELATED TO VoIP CALLS.*

09. Eun-Ju Ha, B.-S. Y. (2004). *End-to-End QoS Management for VoIP Using DiffServ.*

10. Filipe Neves, S. S. (2011). *Quality Evaluation Methods to Improve Enterprise VoIP Communications.*

11. Grainne Hanley, S. M. (2007). *Performance of VoIP over IEEE 802.11G DSSS-OFDM Mode with IEEE 802.11E QOS Support.*

12. Haniyeh Kazemitabar, A. M. (n.d.). *Capacity Analysis of G.711 and G.729 Codec for VoIP over 802.11b WLANs.*

13. Hayashi, M. M. (2009). *Performance Evaluation of VoIP QoE Monitoring Using RTCP XR.*

14. Hersent, O. (2011). *IP Telephony: Deploying VoIP Protocols and IMS Infrastructure.* John Wiley & Sons Ltd.

15. Hicks, J. Q. (n.d.). *Evaluating Data Networks for VoIP.* NetIQ Corporation.

16. ICANN. (2011). *IPv4 Ceremony.* Ανάκτηση από http://www.youtube.com/watch?v=orJpEJuZick

17. ICAP. (2008). Η Ελλάδα σε αριθμούς. Στο *Ελληνικός Οικονομικός Οδηγός 2008.*

18. IETF: RFC3611. (2003). *RTP Control Protocol Extended Reports.*

19. Insu Kim, K. K. (2007). *Secure Session Management Mechanism in VoIP Service.*

20. Ismail, M. N. (2011). *Analysis of VoIP softphone performance between wired and wireless in campus network environment.* International Journal of Computional cognition.

21. Ismail, M. N. (n.d.). Best VoIP Codecs Selection for VoIP Conversation over Wireless Carriers Netwoek. *Annals Computer Science Series*.

22. Jae-Won Choi, K.-H. L. (n.d.). *Implementation of a Network Simulator Supporting VoIP.*

23. (n.d.). Building A Business Case For VoIP. Στο J. T. John Q. Walker, *Taking Charge of Your VoIP Project.* Cisco press.

24. Kelly, T. V. (2005). *VoIP for Dummies.* Wiley Publishing.

25. Kim1, C.-C. (2012). A Software Implementation for Quality Management of Mobile VoIP Services. *National Information Society Agency*.

26. Lee, K.-w. (2011). Abnormal Traffic Detection System of VoIP Based on SIP. *Lee, D. Howard, and D. Ślęzak*, σσ. 496-504.

27. Leif Madsen, R. B. (2011). *Asterisk Cookbook.* O'Reilly.

28. Miller, M. A. (2005). *Implementing the VoIP Network.* Network General.

29. Minoli, D. (2006). *Voice Over IPv6: Architectures for Next Generation VoIP Networks.*

30. Miroslav Voznak, A. K. (2012). *Effective Packet Loss Estimation on VoIP Jitter Buffer.*

31. Networks, Q. A. (2009). *David Rodrigues, Eduardo Cerqueira, Edmundo Monteiro.*

32. Olejniczak, S. P. (2005). *Telecom for Dummies.* Wiley Publishing.

33. Olejniczak, S. P. (2009). *IP Deployment for Dummies.* Wiley Publishing.

34. Oussema Dabbebi, R. B. (2010). *Managing Risks at Runtime in VoIP Networks and Services.*

35. Polycom. (2008). *VoIP to 20 kHz:Codec Choices for High Definition Voice Telephony.*

36. Robar, A. (2009). *FreePBX 2.5 Powerful Telephony Solutions.* PACKT publishing.

37. Rudinsky, J. (2009). *VoIP-PSTN Interoperability by Asterisk and SS7 Signalling.*

38. SANS Institute: InfoSec Reading Room. (2004). *Latency and QoS for Voice over IP.* SANS Institute.

39. Services, E. t. (2010). *Bala Dhandayuthapani Veerasamy.*

40. Siddiqui, A. A. (2011). *VoIP Performance Management and Optimization.* Cisco Press.

41. Sinnreich, H., & Johnston, A. (2006). *Internet Communicastions Using SIP.* WILEY.

42. So-In, C. (2004). *Designing VOIP in Campus Network.*

43. spiceworks. (2013). *The day of the DoS: Are we under attack from inside the office?* Ανάκτηση από http://community.spiceworks.com/topic/299014-the-day-of-the-dos-are-we-under-attack-from-inside-the-office

44. Thomas Porter, B. B. (2004). *Practical VoIP Security.* SYNGRESS publishing.

45. Tu, X. L. (2011). *Research on Security of VoIP Network.*

46. Voznak, M. (2010). Delay Variation Model with RTP Flows Behavior in Accordance with MD1 Kendall's Notation. *Information and Communication technologies and services*.

47. Wallingford, T. (n.d.). *Switching to VoIP.* O'REILLY.

48. Wenyu Jiang, H. S. (2002). *Comparisons Of FEC and Codec Robustness on VoIP Quality and Efficiency.*

49. Whittaker, Z. (2013). *ZDNet*. Ανάκτηση από Homeland Security: Disable UPnP as tens of millions at risk: http://www.zdnet.com/homeland-security-disable-upnp-as-tens-of-millions-at-risk-7000010512/

50. XO Communications. (2011). *Making the Move to VoIP: Total Cost of Ownership.*

51. Yoo, S. N. (2002). *Allowable Propagation Delay for VoIP Calls of Acceptable Quality.* Department of Computer Communication Engineering,Ajou University, Suwon, Korea.

52. Δημήτριος, Α. (2011). *Μελέτη και υλοποίηση συστήματος τηλεφωνίας μέσω διαδικτύου.*

53. Εθνική Συνομοσπονδία Ελληνικού Εμπορίου. (2012). *Ετήσια Έκθεση Ελληνικού Εμπορίου.*

54. Εθνική Τράπεζα. (2012, Ιούλιος). Μικρομεσαίες Επιχειρήσεις Έρευνα συγκυρίας.

55. Ζήνωνος, Ζ. (2009). *Εκτίμηση παραμέτρων ποιότητας εξυπηρέτησης σε VoIP μέσω διαφορετικών τεχνολογιών ευρυζωνικής πρόσβασης.*

56. Ινστιτούτο Μικρών Επιχειρήσεων. (2012, Οκτώβριος 23). *ΙΜΕ ΓΣΕΒΕΕ*. Ανάκτηση 2013, από http://www.imegsevee.gr/statistics/555-2012-10-23-10-15-20: http://www.imegsevee.gr/statistics/555-2012-10-23-10-15-20