

---

ΑΝΑΛΥΣΗ & ΑΞΙΟΛΟΓΗΣΗ ΜΗΧΑΝΙΣΜΩΝ ΕΠΙΚΟΙΝΩΝΙΑΣ  
VOIP ΠΑΝΩ ΣΕ ΥΠΟΔΟΜΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ  
ΤΕΧΝΟΛΟΓΙΑΣ WI-FI

---

**ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ**

*Ονοματεπώνυμο: Ασημίνα Πολέμη*

*Επιβλέπων Καθηγητής: Τσαρούχας Ανδρέας*

Η παρούσα πτυχιακή εργασία είναι οργανωμένη σε 6 κεφάλαια.

Στο κεφάλαιο 1 αναλύουμε την τεχνολογία VoIP. Συγκεκριμένα, αναλύουμε τον τρόπο λειτουργίας του, τα πλεονεκτήματα και τα μειονεκτήματα του, διάφορα χαρακτηριστικά του καθώς και σε ποιες υπηρεσίες εφαρμόζεται σήμερα.

Στο κεφάλαιο 2 παρουσιάζουμε τα βασικά μοντέλα των δικτύων υπολογιστών, το μοντέλο OSI και το TCP/IP. Αναλύουμε τις ομοιότητες και τις διαφορές ανάμεσα στα δύο μοντέλα. Επίσης, περιγράφουμε όλα τα επιμέρους επίπεδα που περιλαμβάνονται στα παραπάνω αυτά επίπεδα. Επιπλέον, γίνεται αναφορά στα πρωτόκολλα μεταφοράς του Internet.

Στο κεφάλαιο 3 παρουσιάζουμε αναλυτικά τα βήματα για να μετατρέψουμε ένα συνεχές σήμα σε διακριτό, καθώς επίσης περιγράφουμε κάποιες βασικές τεχνικές κωδικοποίησης που έχουν αναπτυχθεί μέχρι τώρα.

Στο κεφάλαιο 4 μελετάμε τα δίκτυα μεταγωγής κυκλώματος, μηνύματος και πακέτου. Έπειτα, αναλύουμε τις βασικότερες τεχνολογίες μετάδοσης φωνής (*Frame Relay, ATM, και VoIP*).

Στο κεφάλαιο 5 γίνεται αναφορά στα πιο σημαντικά πρωτόκολλα που χρησιμοποιούνται από την τεχνολογία του VoIP, αυτά είναι το SIP, το H.323, το MGCP καθώς και το Megaco.

Στο κεφάλαιο 6 αναλύουμε τα ασύρματα δίκτυα. Συγκεκριμένα, αναλύουμε τα είδη των ασυρμάτων δικτύων, όπως επίσης τις χρήσεις και τις εφαρμογές τους. Επίσης, αναλύουμε τα πιο σημαντικά πρωτόκολλα των ασύρματων δικτύων.

Ακολουθεί το πρακτικό μέρος.

<b>ΠΕΡΙΕΧΟΜΕΝΑ</b>	<b>σελ.</b>
<b>ΠΡΟΛΟΓΟΣ</b> .....	<b>2</b>
<b>ΠΕΡΙΕΧΟΜΕΝΑ</b> .....	<b>3-4</b>
<b>ΕΙΣΑΓΩΓΗ</b> .....	<b>5</b>
<b>ΚΕΦΑΛΑΙΟ 1</b> .....	<b>6</b>
<b>ΒΑΣΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΟ VOIP</b> .....	<b>6</b>
1.1 Τι είναι το VoIP (Voice over IP); .....	<b>6</b>
1.2 Τρόπος λειτουργίας του VoIP .....	<b>7</b>
1.3 Πλεονεκτήματα και μειονεκτήματα του VoIP .....	<b>8-9</b>
1.4 Εφαρμογές του VoIP .....	<b>9</b>
<b>ΚΕΦΑΛΑΙΟ 2</b> .....	<b>10</b>
<b>ΜΟΝΤΕΛΑ ΑΝΑΦΟΡΑΣ ΣΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ</b> .....	<b>10</b>
2.1 Το μοντέλο OSI .....	<b>10-17</b>
2.2 Το μοντέλο TCP/IP .....	<b>16-17</b>
2.2.1 Επίπεδο Διασύνδεσης μεταξύ υπολογιστή υπηρεσίας & δικτύου .....	<b>17</b>
2.2.2 Επίπεδο Διαδικτύου .....	<b>18-19</b>
2.2.3 Επίπεδο Μεταφοράς .....	<b>19</b>
2.2.4 Επίπεδο Εφαρμογών .....	<b>19</b>
2.3 Ομοιότητες Μοντέλου OSI και TCP/IP .....	<b>20</b>
2.4 Διαφορές Μοντέλου OSI και TCP/IP .....	<b>20</b>
2.5 Τα πρωτόκολλα μεταφοράς του Internet .....	<b>20</b>
2.5.1 Το πρωτόκολλο TCP .....	<b>20-21</b>
2.5.1.1 Έλεγχος συμφόρησης στο TCP .....	<b>21-22</b>
2.5.2 Το πρωτόκολλο UDP .....	<b>23</b>
<b>ΚΕΦΑΛΑΙΟ 3</b> .....	<b>24</b>
<b>ΔΕΙΓΜΑΤΟΛΗΨΙΑ, ΚΒΑΝΤΙΣΗ ΚΑΙ ΚΩΔΙΚΟΠΟΙΗΣΗ ΣΗΜΑΤΩΝ</b> .....	<b>24</b>
3.1 Δειγματοληψία .....	<b>24-25</b>
3.2 Κβαντισμός – Κωδικοποίηση .....	<b>25</b>
3.3 Τεχνικές Κωδικοποίησης .....	<b>25</b>
3.3.1 Παλμοκωδική Διαμόρφωση (PCM) .....	<b>25-27</b>
3.3.2 Αποδιαμόρφωση PCM .....	<b>27</b>
3.3.3 Ομοιόμορφο PCM .....	<b>27-29</b>
3.3.4 Μη ομοιόμορφο PCM .....	<b>29-32</b>
3.3.5 Δέλτα Διαμόρφωση (DM - Delta Modulation) .....	<b>32-34</b>
3.3.6 Διαφορική Παλμοκωδική Διαμόρφωση (DPCM) .....	<b>34-35</b>
3.3.7 Προσαρμοστική ΔΜ .....	<b>35</b>
<b>ΚΕΦΑΛΑΙΟ 4</b> .....	<b>36</b>
<b>ΔΙΚΤΥΑ ΜΕΤΑΓΩΓΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΜΕΤΑΔΟΣΗΣ ΦΩΝΗΣ</b> .....	<b>36</b>
4.1 Δίκτυα Μεταγωγής Κυκλώματος .....	<b>36-37</b>
4.2 Δίκτυα Μεταγωγής Μηνύματος .....	<b>37</b>
4.3 Δίκτυα Μεταγωγής Πακέτου .....	<b>38-39</b>
4.4 Τεχνολογίες Μετάδοσης Φωνής .....	<b>39</b>
4.4.1 Τεχνολογία Frame Relay .....	<b>39-40</b>
4.4.2 Τεχνολογία ATM .....	<b>40</b>

4.4.2.1 Η Δομή του ATM cell.....	41-42
4.4.2.2 Αρχιτεκτονική Πρωτοκόλλων ATM .....	42-43
4.4.3 Τεχνολογία Voice over Internet Protocol (VoIP).....	43
<b>ΚΕΦΑΛΑΙΟ 5 .....</b>	<b>44</b>
<b>ΠΡΩΤΟΚΟΛΛΑ ΣΗΜΑΤΟΔΟΣΙΑΣ ΤΗΛΕΦΩΝΙΑΣ IP .....</b>	<b>44</b>
5.1 Session Initiation Protocol (SIP).....	45-47
5.1.1 Οι οντότητες του SIP.....	47-48
5.1.2 Ασφάλεια SIP .....	48-49
5.2 H.323.....	49-50
5.2.1 Αρχιτεκτονική H.323 .....	50-52
5.2.2 Πρωτόκολλα H.323.....	53-57
5.3 MGCP (Media Gateway Control Protocol) .....	57
5.4 Megaco (Gateway Control Protocol) .....	57
<b>ΚΕΦΑΛΑΙΟ 6 .....</b>	<b>58</b>
<b>ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ .....</b>	<b>58</b>
6.1 Εισαγωγή στα Ασύρματα Δίκτυα.....	58-59
6.2 Είδη Ασύρματων Δικτύων .....	60-62
6.3 Χρήσεις και Εφαρμογές Ασύρματων Δικτύων .....	62
6.4 Τοπολογίες Ασύρματων Δικτύων .....	62-64
6.5 Συστατικά στοιχεία των ασύρματων δικτύων .....	65-66
6.6 Πρωτόκολλα στα Ασύρματα Δίκτυα .....	66-67
6.6.1 Το πρότυπο IEEE 802.11 .....	68
6.6.2 Το πρότυπο IEEE 802.11a .....	68
6.6.3 Το πρότυπο IEEE 802.11b .....	68
6.6.4 Το πρότυπο IEEE 802.11g .....	68-69
6.6.5 Το πρότυπο IEEE 802.11n .....	69
<b>ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ.....</b>	<b>70-89</b>
<b>ΑΝΑΦΟΡΕΣ (ΒΙΒΛΙΟΓΡΑΦΙΑ - ΔΙΑΔΙΚΥΑΚΕΣ ΠΗΓΕΣ).....</b>	<b>90</b>

Στη Δεκαετία του 1990, ένας σημαντικός αριθμός ερευνητών που προερχόταν τόσο από τον εκπαιδευτικό χώρο όσο και από τον επιχειρησιακό τομέα, έδειξε ενδιαφέρον σχετικά με τον τρόπο με τον οποίο θα μπορούσαν να μεταδοθούν η φωνή και το βίντεο μέσω IP δικτύων, ιδιαίτερα όσον αφορά τα εταιρικά Intranets και το Διαδίκτυο. Αυτή η τεχνολογία είναι γνωστή στις μέρες μας με την ονομασία VoIP.

Με άλλα λόγια, πρόκειται για την διαδικασία της διάσπασης της φωνής ή του βίντεο σε πακέτα, της μετάδοσης των πακέτων αυτών μέσω ενός δικτύου IP, και της αναδιάταξης τους όταν φτάνουν στον προορισμό τους, έτσι ώστε δύο χρήστες να μπορούν να επικοινωνούν χρησιμοποιώντας ήχο και εικόνα. Παραδοσιακά, η επικοινωνία μεταξύ δύο χρηστών γινόταν μέσω των κλασικών δικτύων τηλεφωνίας PSTN, τα οποία δέσμευαν μια γραμμή αποκλειστικά και μόνο για αυτόν τον σκοπό. Αντίθετα, η τεχνολογία VoIP, που στηρίζεται στη μεταγωγή πακέτων, δίνει την δυνατότητα μέσα από την γραμμή να μεταδίδονται εκτός από φωνητικές πληροφορίες και άλλοι τύποι δεδομένων, όπως είναι τα αρχεία.

Ο κυριότερος λόγος που προτιμάται η υπηρεσία VoIP είναι η σημαντική μείωση του κόστους που προσφέρει για την πραγματοποίηση τηλεφωνικών κλήσεων έναντι του παραδοσιακού φορέα τηλεπικοινωνιών.

# ΒΑΣΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΟ VOIP

Τα τελευταία χρόνια παρατηρήθηκαν σημαντικές αλλαγές στη δομή και λειτουργία των τηλεπικοινωνιακών δικτύων που οφείλονται στη ραγδαία εξέλιξη του Internet και των εφαρμογών που βασίζονται στο **Πρωτόκολλο Διαδικτύου (Internet Protocol – IP)**. Η υπηρεσία **Voice over IP (VoIP)** χρησιμοποιεί το **Πρωτόκολλο Διαδικτύου (Internet Protocol – IP)** για να μεταφέρει τηλεφωνικές συνομιλίες, μετατρέποντας τη φωνή σε πακέτα δεδομένων. Από τη μία, το χαμηλότερο κόστος των δικτύων μεταγωγής πακέτων και από την άλλη, η βελτίωση ποιότητας και η αξιοπιστία της φωνής πέρα από αυτά τα δίκτυα επιτάχυναν την ολοκλήρωση των υπηρεσιών φωνής και δεδομένων. Η ενοποίηση των ξεχωριστών δικτύων μετάδοσης φωνής δεδομένων συνέβαλε στην ελάττωση του κόστους επικοινωνίας.

Έτσι, το γνωστό τηλεφωνικό δίκτυο που σκοπό είχε τη μεταφορά ακουστικού σήματος άρχισε να εμπλουτίζεται με νέες υπηρεσίες όπως διακίνηση δεδομένων και εικόνων ενώ εμφανίστηκαν ταυτόχρονα καινούρια δίκτυα κατάλληλα για την ανταλλαγή των πληροφοριών. Η συχνότητα που απαιτεί η τεχνολογία **IP** για τη μετάδοση των δεδομένων είναι τουλάχιστον 6 φορές μικρότερη από την αντίστοιχη των παραδοσιακών τηλεπικοινωνιακών δικτύων.

### 1.1 Τι είναι το VoIP (Voice over IP);

Ο όρος **Voice Over IP (VoIP)** είναι μια τεχνολογία υλικού και λογισμικού, η οποία επιτρέπει την πραγματοποίηση τηλεφωνικών κλήσεων μέσω υπολογιστικών δικτύων, όπως το Internet. Το **VoIP** χρησιμοποιεί το **Internet Protocol (IP)** για να μεταδώσει τη φωνή σε μορφή πακέτου πάνω από το **IP** δίκτυο. Το **VoIP** άλλαξε και αλλάζει τον τρόπο με τον οποίο επικοινωνούμε, αντικαθιστώντας σταδιακά την παραδοσιακή τηλεφωνία

Έτσι το **VoIP** μπορεί να επιτευχθεί σε οποιοδήποτε δίκτυο δεδομένων που χρησιμοποιεί **IP**, όπως είναι το Internet, τα Intranets και τα τοπικά δίκτυα (*LAN*).

Το σήμα φωνής: α) ψηφιοποιείται, β) συμπιέζεται, γ) μετατρέπεται σε **IP** πακέτα και στη συνέχεια δ) διαβιβάζεται μέσω του **IP** δικτύου. Πρωτόκολλα σηματοδότησης (*Signaling protocols*) χρησιμοποιούνται για να δημιουργήσουν, να τερματίσουν κλήσεις, να μεταφέρουν τις απαιτούμενες πληροφορίες, για να εντοπίσουν τους χρήστες και να διαπραγματευτούν τα χαρακτηριστικά της κλήσεως. Ένα από τα βασικά κίνητρα χρήσης της τηλεφωνίας μέσω Internet (*Internet Telephony*) είναι το πολύ χαμηλό κόστος που συνεπάγεται. Ο στόχος της δημιουργίας της υπηρεσίας **VoIP** είναι να δοθεί η δυνατότητα στο χρήστη να πραγματοποιεί δωρεάν τηλεφωνικές κλήσεις μέσω του Internet, παρακάμπτοντας εντελώς τα τέλη των τηλεφωνικών εταιριών.

Άλλοι όροι οι οποίοι χρησιμοποιούνται συχνά ως συνώνυμο της **VoIP** είναι οι εξής: τηλεφωνία **IP (IP telephony)**, τηλεφωνία μέσω του Διαδικτύου (*Internet telephony*), φωνή μέσω ευρυζωνικών δικτύων (*voice over broadband*), ευρυζωνική τηλεφωνία (*broadband telephony*) και ευρυζωνικό τηλέφωνο (*broadband phone*).

## 1.2 Τρόπος λειτουργίας του VoIP

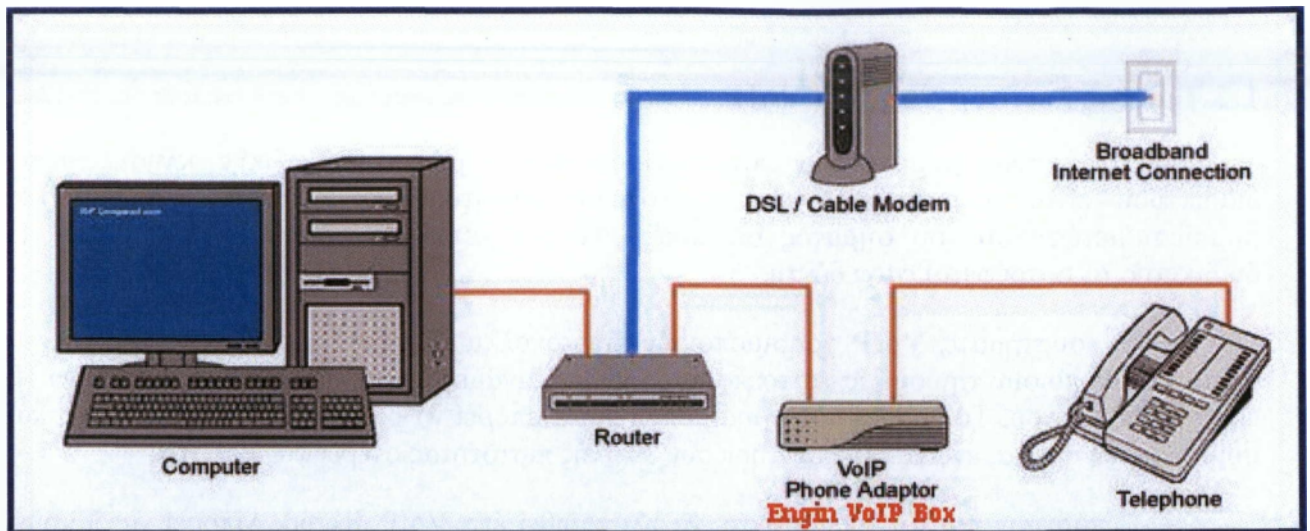
Τα βασικά βήματα για την πραγματοποίηση μιας τηλεφωνικής κλήσης μέσω διαδικτύου είναι η μετατροπή του αναλογικού φωνητικού σήματος σε ψηφιακό και συμπίεση/μετάφραση του σήματος σε πακέτα **IP** για μετάδοση μέσω του διαδικτύου. Η διαδικασία αντιστρέφεται στον δέκτη.

Τα συστήματα **VoIP** χρησιμοποιούν πρωτόκολλα ελέγχου για και codecs ήχου, τα οποία κωδικοποιούν την ομιλία επιτρέποντας έτσι την αναμεταδοσή της μέσω ενός δικτύου **IP** ως ψηφιακού ήχου. Τα codecs που χρησιμοποιούνται μπορεί να βασίζονται σε στενή ζώνη και συμπιεσμένη ομιλία, ενώ άλλα υποστηρίζουν υψηλής πιστότητας στερεοφωνικό ήχο.

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. Ένα VoIP δίκτυο μπορεί επίσης να διασυνδεθεί με τα **PSTN** (Public Switched Telephone Network) δίκτυα.

Τα στοιχεία και ο εξοπλισμός που μπορούν να χρησιμοποιηθούν σε ένα δίκτυο VoIP είναι ποικίλα, όπως: συμβατικά τηλέφωνα, **ATA**, **Gateways**, **Gatekeepers**, **PBX**, **VoIP phones**:

- **ATA (Analog Telephony Adapters)**: είναι συσκευές οι οποίες δίνουν την δυνατότητα να συνδεθεί ένα αναλογικό τηλέφωνο σε ένα VoIP δίκτυο. Μετατρέπουν το αναλογικό σήμα του τηλεφώνου σε μορφή κατάλληλη για χρήση σε VoIP δίκτυα και αντίστροφα. Κωδικοποιούν και αποκωδικοποιούν σήματα φωνής χρησιμοποιώντας codec φωνής, όπως είναι τα G711, G729, GSM κ.λ.π. Η κύρια αρμοδιότητά τους είναι η πραγματοποίηση VoIP κλήσεων χωρίς να απαιτείται η αγορά νέων τηλεφώνων.
- **VoIP Gateway**: είναι συσκευή ανάλογη με τους IP Gateways που συνδέει συμβατικά τηλεφωνικά δίκτυα (π.χ 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 καθώς και πλάνα κλήσεων (dial plans). Οι gatekeepers είναι διαχωρισμένοι από τα τερματικά, τα οποία επιβάλλεται να χρησιμοποιούν τις υπηρεσίες τους, εάν αυτοί υπάρχουν.



### 1.3 Πλεονεκτήματα και Μειονεκτήματα του VoIP

Η υπηρεσία **VoIP** προσφέρει πληθώρα πλεονεκτημάτων στα άτομα που την χρησιμοποιούν. Μερικά από τα οφέλη είναι τα παρακάτω:

- Ευκολότερη και ταχύτερη δρομολόγηση και επαναδρομολόγηση των τηλεφωνικών κλήσεων μέσω των υφισταμένων δικτύων δεδομένων χωρίς να απαιτείται η χρήση διαφορετικών δικτύων κίνησης φωνής και κίνησης δεδομένων.
- Ασφαλείς κλήσεις με τη χρήση τυποποιημένων πρωτοκόλλων, όπως το *Πρωτόκολλο Πραγματικού Χρόνου (Real Time Protocol-RTP)*. Το πρωτόκολλο αυτό υποστηρίζει την κρυπτογράφηση των μέσων. Το *Πρωτόκολλο Έναρξης Συνόδου (Session Initiation Protocol-SIP)* μπορεί να κρυπτογραφήσει και να κρίνει την αυθεντικότητα των μηνυμάτων σηματοδότησης. Αυτά τα πρωτόκολλα μαζί παρέχουν κρυπτογραφημένες και ασφαλείς επικοινωνίες.
- Δυνατότητα σύνδεσης στον πάροχο υπηρεσιών **VoIP** από οπουδήποτε με μια γρήγορη σύνδεση στο Internet.
- Δυνατότητα μετάδοσης περισσότερων από ένα τηλεφωνημάτων σε μια μόνο ευρυζωνική σύνδεση.
- Μειωμένο κόστος για απομακρυσμένες κλήσεις.
- Μειωμένο συνολικό κόστος λόγω απουσίας παγίων τελών.
- Δωρεάν παροχή υπηρεσιών, οι οποίες χρεώνονται έξτρα από τις τηλεφωνικές εταιρίες, όπως είναι η αναγνώριση κλήσης, η προώθηση κλήσης, η αυτόματη επανάκληση, οι κλήσεις σύσκεψης κ.λ.π



- Νέες υπηρεσίες, όπως η συνδιάσκεψη μέσω βίντεο, η ανταλλαγή αρχείων και μηνυμάτων, η μετάδοση πληροφοριών στους διαθέσιμους χρήστες κ.λπ.

Παρόλα αυτά τα σημαντικά οφέλη που προαναφέρθηκαν, η μετάδοση φωνής μέσω του πρωτοκόλλου **IP** παρουσιάζει και μειονεκτήματα.

Ορισμένα από αυτά είναι τα εξής:

- Απαιτείται υψηλή ταχύτητα Internet για να πραγματοποιηθεί μια τηλεφωνική κλήση.
- Η ποιότητα της φωνής είναι χαμηλότερη από ότι στα παραδοσιακά τηλέφωνα.
- Η υπηρεσία δεν λειτουργεί όταν υπάρχει διακοπή ρεύματος.
- Δεν υπάρχει άμεση σύνδεση με τους αριθμούς έκτακτης ανάγκης.
- Υπάρχει πιθανότητα κλοπής των αποθηκευμένων φωνητικών δεδομένων από hackers.
- Η υπηρεσία **VoIP** είναι επιρρεπής στους ιούς.

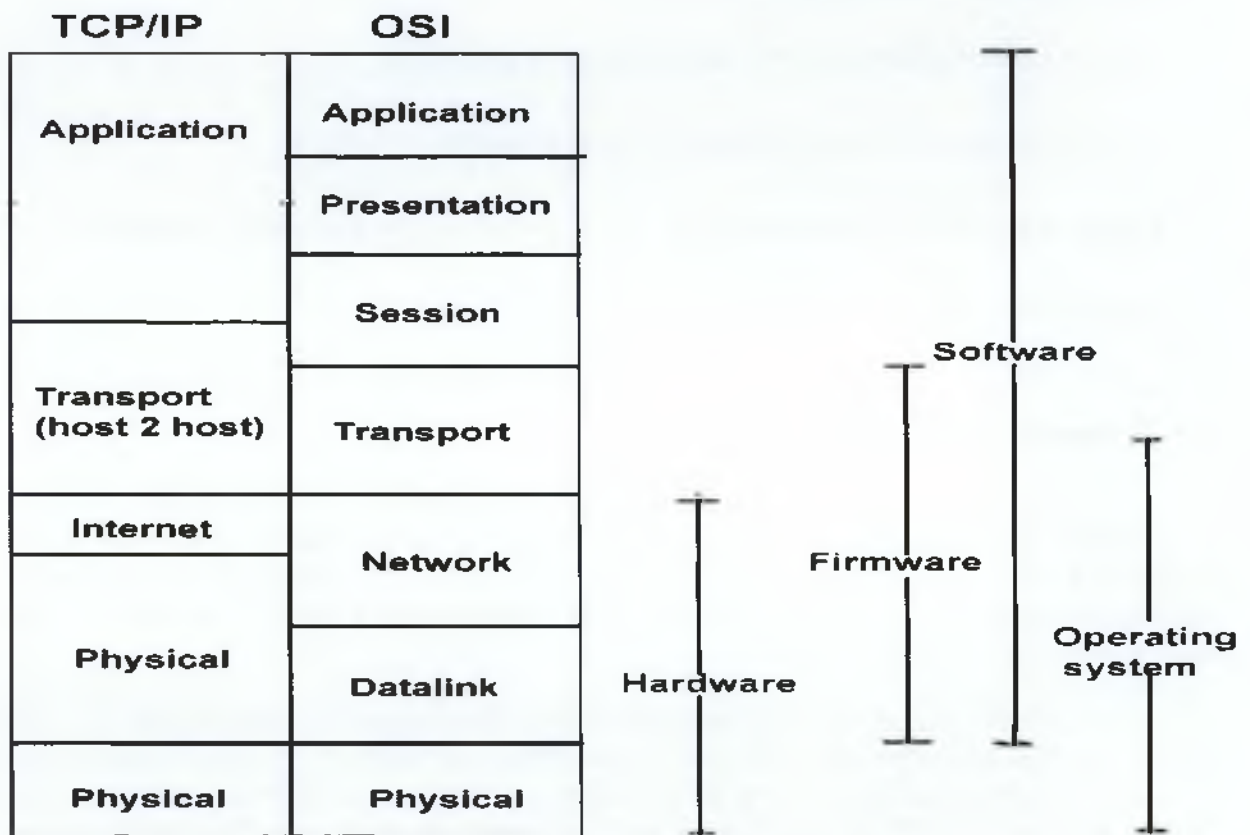
#### **1.4 Εφαρμογές του VoIP**

Σήμερα, υπάρχει πληθώρα εφαρμογών, συμπεριλαμβανομένων των *Voipbuster*, *ICQ*, *MSN Messenger*, *Skype*, *NetMeeting*, *Firefly*, *Asterisk* κ.α, οι οποίες προσφέρουν ιντερνετική τηλεφωνία. Η πιο δημοφιλής από αυτές είναι το *Skype*. Το *Skype* είναι μια εξαιρετικά δημοφιλής εφαρμογή λογισμικού που επιτρέπει στους χρήστες να πραγματοποιούν φωνητικές κλήσεις μέσω του Διαδικτύου.

Επίσης, οι κλήσεις στο εσωτερικό δίκτυο των εφαρμογών είναι δωρεάν. Οι κλήσεις που χρεώνονται είναι αυτές που γίνονται προς δίκτυα άλλων φορέων. Το *Skype* υποστηρίζει την ανταλλαγή άμεσων μηνυμάτων, την αποστολή αρχείων και τη δυνατότητα συνδιάσκεψης. Το *Msn Messenger* είναι επίσης ευρέως διαδεδομένο. Προσφέρει υπηρεσίες συνδιάσκεψης με φωνή και βίντεο σε πολλούς χρήστες ταυτόχρονα.

## ΜΟΝΤΕΛΑ ΑΝΑΦΟΡΑΣ ΣΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Με τον όρο πρωτόκολλο αναφερόμαστε σε ένα σύνολο συμφωνημένων κανόνων, απαραίτητων για την ανταλλαγή δεδομένων μεταξύ δύο συνδεδεμένων κόμβων. Ένα σύνολο πρωτοκόλλων ονομάζεται αρχιτεκτονική πρωτοκόλλου (protocol architecture). Σήμερα χρησιμοποιούνται ευρέως δύο αρχιτεκτονικές (TCP/IP και OSI) που θα περιγράψουν παρακάτω.



Τα μοντέλα TCP/IP και OSI

### 2.1 Το μοντέλο OSI (OPEN SYSTEM INTERCONNECTION)

Το μοντέλο OSI υποδιαιρεί τις λειτουργίες ενός τηλεπικοινωνιακού δικτύου σε μια «κατακόρυφη» στοίβα από επίπεδα, για το καθένα από τα οποία μπορεί να οριστεί κάποιο πρωτόκολλο σε μία συγκεκριμένη υλοποίηση. Κάθε επίπεδο αξιοποιεί τις λειτουργίες του κατώτερου του στη στοίβα επιπέδου, ενώ στόχος του είναι να παρέχει λειτουργικότητα στο αμέσως ανώτερο επίπεδό του. Μία συγκεκριμένη υλοποίηση του μοντέλου, με καθορισμένα

πρωτόκολλα για κάθε επίπεδο, ονομάζεται στοίβα πρωτοκόλλων ή απλά στοίβα. Το κάθε πρωτόκολλο υλοποιείται είτε σε υλικό είτε σε λογισμικό. Συνήθως τα κατώτερα επίπεδα υλοποιούνται στο υλικό ενώ τα ανώτερα σε λογισμικό.

Το μοντέλο OSI είναι στενά συσχετισμένο με τον κλάδο της επιστήμης υπολογιστών και τη δικτύωση υπολογιστών. Το βασικό χαρακτηριστικό του είναι η διασύνδεση μεταξύ των επιπέδων, η οποία υπαγορεύει τις προδιαγραφές της αλληλεπίδρασής τους. Αυτό σημαίνει ότι ένα επίπεδο υλοποιημένο με κάποιο συγκεκριμένο πρωτόκολλο μπορεί να συνεργαστεί με το γειτονικό του στη στοίβα επίπεδο, το οποίο υλοποιείται με κάποιο άλλο πρωτόκολλο, υπό την προϋπόθεση ότι οι προδιαγραφές του καθενός έχουν δημοσιευθεί και έχουν γίνει αντιληπτές σωστά. Αυτές οι προδιαγραφές είναι τυπικά γνωστές ως RFC (Requests for Comments) και αποτελούν πρότυπα του Διεθνούς Οργανισμού Τυποποίησης ISO.

Συνήθως τα επίπεδα είναι αυστηρά διαχωρισμένα μεταξύ τους: αξιοποιούν τις υπηρεσίες του κατώτερου επιπέδου τους και προσφέρουν υπηρεσίες στο ανώτερό τους, αλλά το καθένα δεν παρεμβαίνει στις λειτουργίες του άλλου· πιθανόν να μη γνωρίζει καν γι' αυτές. Αυτός ο λογικός διαχωρισμός των επιπέδων διευκολύνει πολύ τη μελέτη της συμπεριφοράς των πρωτοκόλλων και επιτρέπει τη σχεδίαση πολύπλοκων και αξιόπιστων στοιβών πρωτοκόλλων. Ορισμένες φορές όμως αυτή η αρχή ανεξαρτησίας των επιπέδων παραβιάζεται, για λόγους βελτιστοποίησης της απόδοσης ή αύξησης της λειτουργικότητας, με πρωτόκολλα διαφορετικών επιπέδων να συγχωνεύονται ή να παρεμβαίνουν το ένα στη λειτουργία του άλλου.

Το μοντέλο ISO/OSI είναι μία δομή επτά επιπέδων η οποία διευκρινίζει τις απαιτήσεις για την επικοινωνία μεταξύ δύο υπολογιστών. Το μοντέλο ορίζεται από το στάνταρντ 7498-1 του οργανισμού ISO. Επιτρέπει τη συνεργασία των στοιχείων ενός δικτύου ανεξάρτητα με το ποια πρωτόκολλα χρησιμοποιούνται και από ποιους κατασκευαστές υπολογιστών υποστηρίζονται.

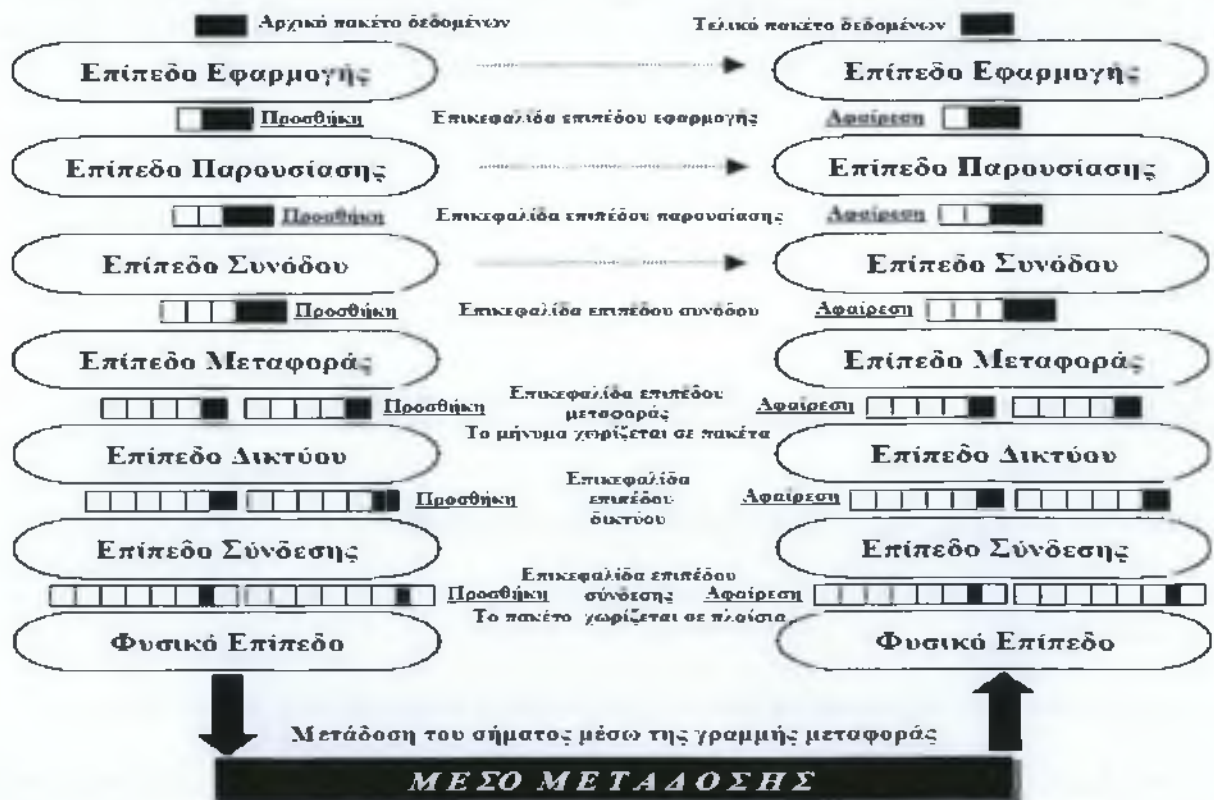
### **Τα κύρια πλεονεκτήματα του μοντέλου OSI περιλαμβάνουν τα ακόλουθα:**

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

Ο διαχωρισμός του μοντέλου OSI σε στρώματα βοήθησε πάρα πολύ στην ανάπτυξη συμβάσεων και πρωτοκόλλων αναφορικά με το κάθε στρώμα. Βέβαια, τα στρώματα αυτά

διέπονται από κάποιες αρχές. Σύμφωνα με τον Andrew S. Tanenbaum, οι αρχές αυτές συνοψίζονται παρακάτω:

- Ένα στρώμα πρέπει να δημιουργηθεί οπουδήποτε χρειάζεται ένα διαφορετικό επίπεδο αφαίρεσης.
- Κάθε στρώμα πρέπει να εκτελεί μια καλά προσδιορισμένη λειτουργία.
- Τα όρια των στρωμάτων πρέπει να επιλέγονται έτσι ώστε να ελαχιστοποιείται η ροή της πληροφορίας μέσω των διεπαφών.
- Η λειτουργία του καθενός στρώματος πρέπει να επιλέγεται με προοπτική τον καθορισμό διεθνών τροποποιημένων πρωτοκόλλων.
- Ο αριθμός των στρωμάτων πρέπει να είναι αρκετά μεγάλος, ώστε να μη στριμώχονται, αναγκαστικά, διακεκριμένες λειτουργίες στο ίδιο στρώμα και αρκετά μικρός, ώστε να μη γίνεται η αρχιτεκτονική δύσχρηστη.



Σχήμα 24 : Μετάδοση δεδομένων στο μοντέλο αναφοράς OSI

## Περιγραφή των επιπέδων OSI

### Επίπεδο 1: Φυσικό Επίπεδο (Physical Layer)

Το φυσικό επίπεδο (*physical layer*) ασχολείται με τη μετάδοση “ακατέργαστων” bit σε ένα κανάλι επικοινωνίας. Πιο συγκεκριμένα, εξασφαλίζει το όριο της τάσης πάνω από την οποία το αντίστοιχο bit θεωρείται “1” και κάτω από την οποία θεωρείται “0”, τη χρονική διάρκεια ενός bit κ.λ.π. Τα θέματα σχεδίασης ασχολούνται με τη διασφάλιση της σωστής λήψης των μεταδιδόμενων bits. Δηλαδή ενδιαφερόμαστε για μηχανικές, ηλεκτρικές συνδέσεις και διασυνδέσεις καθώς και για το φυσικό μέσο μετάδοσης το οποίο βρίσκεται από κάτω. Το φυσικό μέσο μετάδοσης παρουσιάζει ατέλειες που οδηγούν σε σφάλματα (π.χ αλλαγές τιμών ή απώλειες), με αποτέλεσμα να απαιτούνται μέθοδοι διασφάλισης της ορθής λήψης της πληροφορίας.

Γενικά το φυσικό στρώμα ασχολείται με τη λειτουργία των ηλεκτρικών κυκλωμάτων που σχηματίζονται κατά την επικοινωνία των υπολογιστών, καθώς και των λοιπών παραμέτρων που αυτά περιλαμβάνουν όπως τάσεις και ρεύματα.

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

Η βασική αποστολή του επιπέδου ελέγχου γραμμής δεδομένων (*data link layer*) είναι ο μετασχηματισμός του ακατέργαστου μέσου μετάδοσης σε μια γραμμή που εμφανίζεται ελεύθερη από σφάλματα μετάδοσης στο επίπεδο δικτύου. Ο σκοπός αυτός επιτυγχάνεται: α) με την διάσπαση των δεδομένων (πακέτων) εισόδου του αποστολέα σε πλαίσια δεδομένων (*data frames*, με μέγεθος συνήθως μερικές εκατοντάδες ή χιλιάδες bit), β) μετάδοση αυτών με τη σειρά και επεξεργασία των πλαισίων επιβεβαίωσης λήψης (*acknowledgement frames*), που επιστρέφονται από τον δέκτη. Εφόσον το φυσικό επίπεδο απλώς αποδέχεται και μεταδίδει ένα συρμό από bits χωρίς να νοιάζεται για το νόημα και τη δομή του, η δημιουργία και η αναγνώριση των ορίων των πλαισίων εξαρτάται πλέον από το επίπεδο ζεύξης δεδομένων. Εάν αυτές οι ακολουθίες μπορούν κατά σύμπτωση να παρουσιαστούν στα δεδομένα, πρέπει να ληφθεί ειδική μέριμνα για να αποφευχθεί η σύγχυση.

Η εμφάνιση θορύβου στη γραμμή μπορεί να καταστρέψει ολοκληρωτικά το πλαίσιο. Στην περίπτωση αυτή το λογισμικό του επιπέδου ζεύξης δεδομένων του πομπού πρέπει να αναμεταδώσει το πλαίσιο. Ωστόσο οι πολλαπλές μεταδόσεις του ίδιου πλαισίου δημιουργούν τη δυνατότητα ύπαρξης αντιγράφων πλαισίων. Ένα αντίγραφο πλαισίου, θα μπορούσε για παράδειγμα, να σταλεί, εάν καταστραφεί ένα πλαίσιο επιβεβαίωσης λήψης που επιστρέφει ο δέκτης στον πομπό. Από αυτό το επίπεδο εξαρτάται η λύση των προβλημάτων που δημιουργούνται από καταστροφές, απώλειες και αντίγραφα πλαισίων. Το επίπεδο ελέγχου γραμμής δεδομένων μπορεί να προσφέρει πολλές διαφορετικές κατηγορίες υπηρεσιών στο επίπεδο δικτύου.

Ένα άλλο θέμα που εμφανίζεται στο επίπεδο αυτό (καθώς και στα υψηλότερα επίπεδα) είναι η ανάγκη συγκράτησης του πομπού, ώστε ένας αργός δέκτης να μην πλημμυρίζει

από δεδομένα. Αυτή η διαδικασία καλείται επίσημα *έλεγχος ροής*. Πρέπει να εφαρμοστεί ένας ρυθμιστικός μηχανισμός ανάδρασης για να μπορεί να γνωρίζει αν ο δέκτης έχει χώρο στην ενδιάμεση μνήμη (buffer) του.

Η χρήση της γραμμής για αμφίδρομη μετάδοση δεδομένων, δημιουργεί ένα νέο πρόβλημα με το οποίο πρέπει να ασχοληθεί το λογισμικό του επιπέδου ελέγχου γραμμής δεδομένων. Το πρόβλημα είναι ότι τα πλαίσια επιβεβαίωσης λήψης για την κυκλοφορία από τη μηχανή A στη μηχανή B ανταγωνίζονται με τα πλαίσια δεδομένων της κίνησης από τη μηχανή B στη μηχανή A, για το ποιος θα χρησιμοποιήσει τη γραμμή. Μια έξυπνη κίνηση είναι η εμβόλιμη επιβεβαίωση λήψης (piggyback acknowledgement) κατά την οποία η επιβεβαίωση λήψης έχει ενσωματωθεί σε ένα πλαίσιο μετάδοσης δεδομένων που μεταδίδεται με τη φορά της επιβεβαίωσης (B-A).

Σε γενικές γραμμές, το επίπεδο ελέγχου γραμμής δεδομένων αναλαμβάνει τη μορφοποίηση και την ορθή μετάδοση των δεδομένων, με ταυτόχρονο εντοπισμό και επιδιόρθωση των σφαλμάτων. Η στατιστική συγκυρία του δικτύου καθορίζει το χρόνο που μεσολαβεί ανάμεσα σε δύο εκπομπές διαδοχικών πλαισίων, ενώ ταυτόχρονα, το επίπεδο αυτό αναλαμβάνει την εξασφάλιση της ομαλής συνεργασίας μεταξύ του φυσικού επιπέδου και των ανωτέρων.

### **Επίπεδο 3: Επίπεδο Δικτύου (Network Layer)**

Το επίπεδο δικτύου (*network layer*) ασχολείται με τον έλεγχο της λειτουργίας του υποδικτύου. Ένα βασικό θέμα της σχεδίασης είναι ο καθορισμός του τρόπου δρομολόγησης των πακέτων από την αφετηρία στον προορισμό τους. Οι διαδρομές θα μπορούσαν να βασιστούν σε στατικούς πίνακες, οι οποίοι θα ήταν καλωδιωμένοι (wired into) και σπάνια θα τροποποιούνταν. Θα μπορούσαν επίσης να οριστούν στην αρχή κάθε συνομιλίας, για παράδειγμα ενός συνόλου τερματικών. Τέλος, πρέπει να είναι πολύ δυναμικές και να μεταβάλλονται κατά τη διάρκεια της λειτουργίας ώστε να απεικονίζουν το τρέχον φορτίο του δικτύου.

Εάν στα υποδίκτυα μεταδίδονται πολλά πακέτα την ίδια χρονική στιγμή, θα εμπλακεί το ένα στη διαδρομή του άλλου δημιουργώντας *συμφόρηση* (*congestion*). Ο έλεγχος μιας τέτοιας συμφόρησης ανήκει επίσης στις αρμοδιότητες του επιπέδου αυτού.

Στο επίπεδο δικτύου υπάρχει και μια λειτουργία χρέωσης. Στο τέλος μιας σύνδεσης, το λογισμικό πρέπει να υπολογίζει πόσα πακέτα, χαρακτήρες ή bits στάλθηκαν από κάθε πελάτη για την ανάλογη έκδοση του λογαριασμού. Όταν ένα πακέτο διασχίσει τα εθνικά σύνορα και δεδομένων των διαφορετικών τιμών που υπάρχουν σε κάθε πλευρά, η διαδικασία χρέωσης μπορεί να γίνει πολύπλοκη. Όταν το πακέτο πρέπει να μεταδοθεί από ένα δίκτυο σε ένα άλλο για να φθάσει στον προορισμό του, εμφανίζονται πολλά προβλήματα. Η διευθυνσιοδότηση που χρησιμοποιείται από το δεύτερο δίκτυο μπορεί να είναι διαφορετική. Το δεύτερο μπορεί να μη δέχεται καθόλου το πακέτο διότι ίσως να είναι πολύ μεγάλο. Τα πρωτόκολλα των δύο δικτύων μπορεί να διαφέρουν. Το επίπεδο δικτύου πρέπει να υπερπηδήσει όλα αυτά τα προβλήματα και να επιτρέψει την διασύνδεση ετερογενών δικτύων (διαδικτύωση).

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

Η βασική λειτουργία του επιπέδου μεταφοράς (*transport layer*) είναι η αποδοχή δεδομένων από το επίπεδο συνόδου, διάσπαση αυτών σε μικρότερες μονάδες αν απαιτείται, η μεταφορά τους στο επίπεδο δικτύου και η διασφάλιση ότι όλα τα τμήματα φθάνουν σωστά στην άλλη πλευρά. Επιπλέον όλα αυτά πρέπει να γίνουν αποδοτικά και με τέτοιο τρόπο, που να απομονώνουν το επίπεδο συνόδου από τις αναπόφευκτες αλλαγές στην τεχνολογία του υλικού.

Υπό κανονικές συνθήκες, το επίπεδο μεταφοράς δημιουργεί μια ξεχωριστή σύνδεση δικτύου, για κάθε σύνδεση μεταφοράς που απαιτείται από το επίπεδο συνόδου. Εάν ωστόσο, η σύνδεση μεταφοράς απαιτεί υψηλό ρυθμό εξυπηρέτησης (*throughput*), το επίπεδο μεταφοράς μπορεί να δημιουργήσει πολλαπλές συνδέσεις δικτύου μοιράζοντας τα δεδομένα ανάμεσα στις συνδέσεις του δικτύου για να μεγαλώσει τον βαθμό εξυπηρέτησης. Από την άλλη πλευρά εάν η δημιουργία ή η συντήρηση μιας σύνδεσης δικτύου είναι ακριβή, το επίπεδο μεταφοράς μπορεί να πολυπλέκει πολλές συνδέσεις μεταφοράς στην ίδια σύνδεση δικτύου για να ελαττώσει το κόστος. Σε όλες τις περιπτώσεις το επίπεδο αυτό είναι απαραίτητο, για να κάνει την πολυπλεξία “διαφανή” (δηλαδή ανεπαίσθητη) στο επίπεδο συνόδου.

Το επίπεδο μεταφοράς καθορίζει επίσης το είδος των υπηρεσιών που θα παρέχει το επίπεδο συνόδου. Ο πιο γνωστός τύπος σύνδεσης μεταφοράς είναι ένα αλάνθαστο κανάλι **από σημείο σε σημείο** (*point-to-point*), το οποίο παραδίδει μηνύματα με τη σειρά που έχουν σταλεί. Ωστόσο άλλα πιθανά είδη υπηρεσιών μεταφοράς είναι η μεταφορά απομονωμένων μηνυμάτων χωρίς εγγυήσεις σχετικά με τη σειρά παράδοσης και η εκπομπή μηνυμάτων σε πολλούς αποδέκτες. Ο τύπος της υπηρεσίας καθορίζεται με την εγκατάσταση της σύνδεσης.

Το επίπεδο μεταφοράς ενδιαφέρεται για την επικοινωνία από την αφετηρία στον προορισμό ή από άκρο σε άκρο (*end-to-end*), σε αντίθεση με το επίπεδο ελέγχου γραμμής δεδομένων (που ενδιαφέρεται για την επικοινωνία μεταξύ δύο γειτονικών κόμβων). Με άλλα λόγια, ένα πρόγραμμα του Η/Υ-πομπού συνομιλεί με ένα παρόμοιο πρόγραμμα του Η/Υ-δέκτη, χρησιμοποιώντας τις επικεφαλίδες του μηνύματος και τα μηνύματα ελέγχου. Στα κατώτερα επίπεδα, τα πρωτόκολλα ρυθμίζουν την συνομιλία διεργασιών μεταξύ γειτονικών Η/Υ, και όχι μεταξύ των τελικών Η/Υ αφετηρίας και προορισμού, ανάμεσα στους οποίους μπορεί να παρεμβάλλονται πολλοί κόμβοι. Πολλοί κόμβοι πολυπρογραμματίζονται, πράγμα που σημαίνει ότι κάθε κόμβος θα έχει πολλαπλές εισερχόμενες και εξερχόμενες συνδέσεις. Εκεί δημιουργείται η ανάγκη ύπαρξης κάποιας θέσης, η οποία θα δηλώνει τα μηνύματα που ανήκουν σε κάθε σύνδεση. Η επικεφαλίδα μεταφοράς είναι μια θέση που μπορεί να τοποθετηθεί η πληροφορία αυτή.

Πέραν της πολύπλεξης πολλών συρμών μηνυμάτων σε ένα κανάλι, το επίπεδο μεταφοράς πρέπει να φροντίζει για την εγκατάσταση και διαγραφή των συνδέσεων μέσω του δικτύου. Αυτό απαιτεί κάποιο είδος μηχανισμού για καθορισμό ονομάτων, έτσι ώστε η διεργασία ενός μηχανήματος να διαθέτει ένα τρόπο για να ορίζει με ποιον θέλει να επικοινωνήσει. Πρέπει επίσης να υπάρχει ένας μηχανισμός ρύθμισης της ροής των πληροφοριών, έτσι ώστε ένας γρήγορος κόμβος να μην υπερφορτώνει έναν αργό.

## **Επίπεδο 5: Επίπεδο Συνόδου (Session Layer)**

Το επίπεδο συνόδου (*session layer*) επιτρέπει στους χρήστες διαφορετικών μηχανημάτων να εγκαθιστούν συνόδους (*sessions*) μεταξύ τους. Μία σύνοδος επιτρέπει μια συνήθη μεταφορά δεδομένων, όπως και το επίπεδο μεταφοράς, με τη διαφορά ότι παρέχει και μερικές πρόσθετες υπηρεσίες που είναι χρήσιμες σε πολλές εφαρμογές. Μία σύνοδος μπορεί να χρησιμοποιηθεί για να επιτρέψει τη σύνδεση ενός χρήστη σε ένα απομακρυσμένο σύστημα καταμερισμού χρόνου (*time-sharing*) ή για να μεταφέρει ένα αρχείο μεταξύ δύο μηχανών.

Μία από τις υπηρεσίες που παρέχει το επίπεδο συνόδου είναι η δυνατότητα δειξίρισης ελέγχου ενός διαλόγου. Οι σύνοδοι μπορούν να επιτρέψουν την κυκλοφορία προς τη μία κατεύθυνση ή και προς τις δύο κατευθύνσεις την ίδια χρονική στιγμή. Εάν η κυκλοφορία σε μια δεδομένη χρονική στιγμή μπορεί να κινηθεί μόνο προς την μία κατεύθυνση (μονόδρομο *simplex*) ή ημι-αμφίδρομο (*half duplex* κανάλι), το επίπεδο συνόδου παρακολουθεί ποιος έχει σειρά.

Μία άλλη υπηρεσία συνόδου είναι ο **συγχρονισμός** (*synchronization*). Μπορούν να δημιουργηθούν προβλήματα κατά την ανταλλαγή δεδομένων μεταξύ δύο μηχανών, καθώς μπορεί να διαρκέσει αρκετές ώρες, όταν υπάρχει συγκεκριμένος μέσος χρόνος κατάρρευσης του δικτύου. Όταν μια μεταφορά διακοπεί, πρέπει να ξαναρχίσει ολόκληρη από την αρχή και είναι δυνατό να υπάρξουν και νέες αποτυχίες. Για την εξάλειψη αυτού του προβλήματος, το επίπεδο συνόδου παρέχει ένα τρόπο για την εισαγωγή σημείων ελέγχου, έτσι ώστε μετά την κατάρρευση μόνο τα δεδομένα που ακολουθούν το τελευταίο σημείο ελέγχου να μεταδοθούν.

## **Επίπεδο 6: Επίπεδο Παρουσίασης (Presentation Layer)**

Το επίπεδο παρουσίασης (*presentation layer*) εκτελεί συγκεκριμένες λειτουργίες οι οποίες ζητούνται αρκετά συχνά από τους χρήστες, για να εξασφαλίσουν την εύρεση μιας γενικής λύσης γι'αυτούς, έτσι ώστε να μην αφήνεται κάθε χρήστης να λύνει τα προβλήματα του μόνος του. Συγκεκριμένα όλα τα κατώτερα επίπεδα ενδιαφέρονται μόνο για την αξιόπιστη μετακίνηση bits από το ένα στο άλλο, το επίπεδο παρουσίασης ενδιαφέρεται για τη σύνταξη και τη σημασιολογία των πληροφοριών που μεταδίδονται. Παραδείγματα τέτοιων τύπων πληροφορίας είναι ακολουθίες χαρακτήρων με διαφορετικές κωδικοποιήσεις (ASCII, Unicode κ.λ.π), αριθμοί σταθερής ή κινητής υποδιαστολής, δομές δεδομένων κ.λ.π.

Το επίπεδο παρουσίασης ενδιαφέρεται και για άλλα θέματα αναπαράστασης πληροφοριών. Για παράδειγμα η συμπίεση των δεδομένων μπορεί να χρησιμοποιηθεί για να ελαττώσει τον αριθμό των bits που πρόκειται να μεταδοθούν και συχνά απαιτείται κρυπτογράφηση για να εξασφαλιστεί η **μυστικότητα** (*privacy*) και η **γνησιότητα** (*authentication*) της πληροφορίας.



## Επίπεδο 7: Επίπεδο Εφαρμογών (Application Layer)

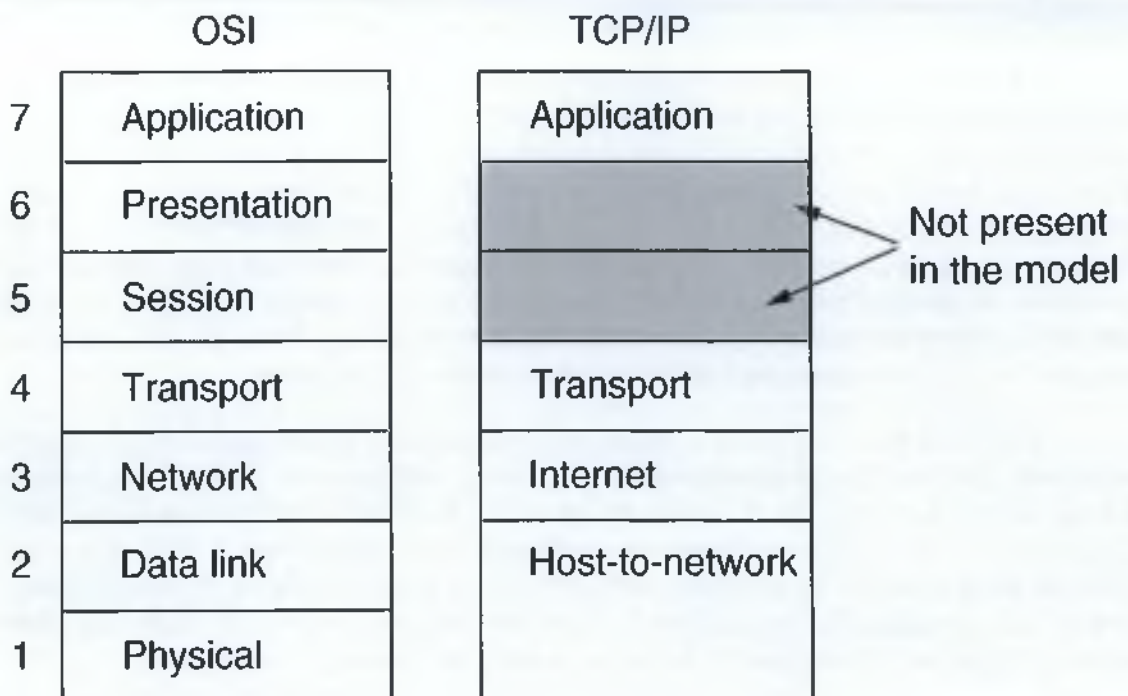
Το επίπεδο εφαρμογής (*application layer*) περιέχει μια ποικιλία πρωτοκόλλων που χρειάζονται συχνά. Καθορίζει ένα δικτυακό νοητό τερματικό (*network virtual terminal*) για την επίτευξη της συμβατότητας μεταξύ των διάφορων υπάρχοντων τερματικών σε ολόκληρο τον κόσμο. Για τον χειρισμό κάθε τύπου τερματικού, πρέπει να γραφεί ένα πρόγραμμα αντιστοίχισης των λειτουργιών του νοητού τερματικού του δικτύου πάνω το πραγματικό τερματικό. Για παράδειγμα όταν ο κειμενογράφος μετακινεί τον δρομέα του νοητού τερματικού στην επάνω αριστερή γωνία της οθόνης, το λογισμικό αυτό πρέπει να δώσει την κατάλληλη σειρά εντολών στο πραγματικό τερματικό για την κίνηση και του δικού του δρομέα εκεί. Όλο το λογισμικό του νοητού τερματικού βρίσκεται στο επίπεδο εφαρμογής.

Μία άλλη λειτουργία του επιπέδου εφαρμογής είναι η μεταφορά αρχείων. Διαφορετικά συστήματα αρχείων έχουν διαφορετικές μεθόδους καθορισμού ονομασίας, διαφορετικούς τρόπους αναπαράστασης των γραμμών κειμένου κ.λ.π. Η μεταφορά ενός αρχείου μεταξύ δύο διαφορετικών συστημάτων απαιτεί αντιμετώπιση των παραπάνω, καθώς και άλλων μη συμβατών καταστάσεων. Η εργασία αυτή ανήκει στο επίπεδο εφαρμογής όπως επίσης και το ηλεκτρονικό ταχυδρομείο, η εισαγωγή εργασιών από απόσταση, η εμφάνιση καταλόγων (*directory*) αρχείων και διάφορες άλλες ειδικού και γενικού σκοπού ευκολίες.

### 2.2 Το μοντέλο TCP/IP

Το μοντέλο OSI, λόγω του μεγάλου αριθμού επιπέδων που έχει και άλλων παραγόντων, παρέμεινε θεωρητικό αλλά έθεσε τις βάσεις ανάπτυξης άλλων μοντέλων τα οποία έχουν ευρεία εφαρμογή στις μέρες μας. Ιστορικά η πρώτη στοιβάδα πρωτοκόλλων που εμφανίστηκε ήταν το πασίγνωστο σήμερα ζεύγος πρωτοκόλλων **TCP/IP**. Η βάση για την ανάπτυξη αυτού του μοντέλου αναφοράς πραγματοποιήθηκε όταν το αμερικάνικο δίκτυο ARPAnet άρχισε να συνδέεται με ασύρματα και δορυφορικά δίκτυα. Γι'αυτό είχε από την αρχή την προοπτική της διαδικτύωσης. Το Υπουργείο Εθνικής Άμυνας των ΗΠΑ ήθελε το δίκτυο ARPAnet να παραμένει σε λειτουργία κάτω από δύσκολες συνθήκες, όταν ένα μέρος του δικτύου έχει καταρρεύσει. Μετά από μελέτες που έγιναν δημιουργήθηκε το μοντέλο αναφοράς TCP/IP (*TCP/IP Reference Model*) το οποίο πήρε το όνομα του από τα δύο κυριότερα πρωτόκολλα που χρησιμοποιεί (**TCP** και **IP**). Βασικός σκοπός του μοντέλου αυτού ήταν η εξασφάλιση της αξιοπιστίας του δικτύου σε περίπτωση βλαβών κάποιων τμημάτων του υποδικτύου. Δηλαδή, το δίκτυο έπρεπε να παραμένει σε κατάσταση λειτουργίας, ακόμη και αν διαπιστωνόταν βλάβη σε κάποιο σημείο του.

Επίσης, οι αυξημένες απαιτήσεις σε καινούργιες εφαρμογές, όπως η ανταλλαγή αρχείων ή η μετάδοση ομιλίας σε πραγματικό χρόνο απαιτούσαν μια νέα αρκετά ευέλικτη αρχιτεκτονική, την οποία μπορούσε να προσφέρει το μοντέλο TCP/IP. Αποτελείται από 4 επίπεδα σε αντίθεση με το μοντέλο OSI που αποτελείται από 7, όπως βλέπουμε στο παρακάτω σχήμα:



### Τα επίπεδα του μοντέλου TCP/IP

#### 2.2.1 Επίπεδο Διασύνδεσης μεταξύ υπολογιστή υπηρεσίας & δικτύου

Το επίπεδο αυτό είναι σε αντιστοιχία με το φυσικό επίπεδο και το επίπεδο ελέγχου γραμμής δεδομένων του μοντέλου OSI. Δεν καθορίζεται σαφώς και μπορεί να διαφέρει από υπολογιστή (κόμβο) σε υπολογιστή (κόμβο) και από δίκτυο σε δίκτυο. Το μόνο που καθορίζεται είναι η σύνδεση που δημιουργείται μεταξύ του υπολογιστή (κόμβου) και του δρομολογητή.

#### 2.2.2 Επίπεδο Διαδικτύου (Internet Layer)

Ο όρος “διαδίκτυο” αναφέρεται σε ένα σύνολο διασυνδεδεμένων μεταξύ τους δικτύων. Το επίπεδο αυτό, που ονομάστηκε επίπεδο διαδικτύου, είναι ο συνδυασμός του μοντέλου και είναι σε αντιστοιχία με το επίπεδο δικτύου του μοντέλου OSI. Η κύρια εργασία του είναι να επιτρέπει στους κόμβους να στέλνουν πακέτα σε οποιοδήποτε δίκτυο, που θα ταξιδεύουν ανεξάρτητα το ένα από το άλλο στον προορισμό τους, πιθανώς ακολουθώντας διαφορετική διαδρομή. Επίσης, ίσως να φθάσουν με διαφορετική σειρά από την σειρά αναχώρησης από τον πομπό. Σ’ αυτήν την περίπτωση, στόχος αυτού του επιπέδου είναι να τα επαναδιατάξει στη σωστή σειρά.

Το επίπεδο Διαδικτύου καθορίζει μία τυπική μορφή πακέτου και το πρωτόκολλο αυτό ονομάζεται IP (Internet Protocol). Στο επίπεδο αυτό στέλνονται πακέτα IP στον προορισμό τους. Κύρια αποστολή του επιπέδου είναι η δρομολόγηση των πακέτων με ταυτόχρονη αποφυγή

της συμφόρησης. Για όλους τους παραπάνω λόγους συμπεραίνουμε ότι το επίπεδο διαδικτύου του TCP/IP παρουσιάζει πολλές ομοιότητες με το επίπεδο του δικτύου του μοντέλου OSI.

### 2.2.3 Επίπεδο Μεταφοράς (Transport Layer)

Το επίπεδο μεταφοράς του μοντέλου TCP/IP είναι αντίστοιχο με το πρωτόκολλο μεταφοράς του μοντέλου OSI. Δύο βασικά πρωτόκολλα έχουν αναπτυχθεί στο επίπεδο αυτό. Το πρώτο ονομάζεται *πρωτόκολλο έλεγχου μετάδοσης TCP (Transmission Control Protocol)* και είναι ένα αξιόπιστο πρωτόκολλο με σύνδεση, το οποίο επιτρέπει τη μετάδοση δεδομένων χωρίς σφάλματα από ένα σύστημα σε ένα άλλο μέσω του δικτύου του Internet. Τεμαχίζει τα bytes της προς μετάδοση πληροφορίας και τα περνάει μέσω του επιπέδου διαδικτύου. Στον προορισμό το επίπεδο μεταφοράς του δέκτη επανασυνδέει τα δεδομένα ώστε να αναπαραχθεί η αρχική πληροφορία.

Το πρωτόκολλο TCP/IP διαχειρίζεται επίσης τον έλεγχο ροής, ώστε να υπάρχει απόλυτη βεβαιότητα ότι ένας γρήγορος πομπός δε θα υπερφορτώσει ένα αργό δέκτη. Το δεύτερο πρωτόκολλο αυτού του επιπέδου ονομάζεται *πρωτόκολλο δεδομενογραφημάτων χρήση UDP (User Datagram Protocol)*. Το πρωτόκολλο αυτό είναι χωρίς σύνδεση πρωτόκολλο, δεν είναι τόσο αξιόπιστο με εφαρμογές που δεν επιτρέπουν έλεγχο ροής με το TCP. Επίσης, δεν διορθώνει σφάλματα που μπορεί να προκύψουν. Ωστόσο, χρησιμοποιείται ευρέως για εφαρμογές και αναζητήσεις ερώτησης - απάντησης τύπου πελάτη - εξυπηρετητή, στις οποίες η γρήγορη παράδοση είναι περισσότερο επιθυμητή από την ακριβή παράδοση, όπως σε μετάδοση ήχου και εικόνας.

### 2.2.4 Επίπεδο Εφαρμογών ( Application Layer)

Το μοντέλο TCP/IP δεν έχει επίπεδα παρουσίασης και συνόδου, επειδή δεν υπήρχε κανένας λόγος χρησιμοποίησης τους και έτσι δεν συμπεριλήφθηκαν. Η εμπειρία από το μοντέλο OSI οδήγησε στη χρήση του ελάχιστου δυνατού αριθμού επιπέδων. Έτσι, το επίπεδο εφαρμογής είναι το μόνο ανώτερο επίπεδο που συμπεριλαμβάνει τα πρωτόκολλα των ανώτερων στρωμάτων. Τα καινούργια πρωτόκολλα περιλαμβάνουν: εικονικά τερματικά (*Telnet*), μεταφορά αρχείων (*FTP*) και ηλεκτρονικό ταχυδρομείο (*SMTP*). Το εικονικό τερματικό πρωτόκολλο επιτρέπει σε ένα χρήστη να συνδεθεί με μία απομακρυσμένη μηχανή και να εργαστεί σε αυτή. Το πρωτόκολλο μεταφοράς αρχείων παρέχει έναν αποδοτικό τρόπο για μεταφορά αρχείων από μία μηχανή σε μία άλλη. Η υπηρεσία ηλεκτρονικού ταχυδρομείου αρχικά έκανε μεταφορά αρχείων, αλλά αργότερα αναπτύχθηκε ένα νέο πρωτόκολλο ηλεκτρονικού ταχυδρομείου. Πολλά άλλα πρωτόκολλα έχουν προστεθεί σε αυτό τα τελευταία χρόνια όπως το *DNS (Domain Name Service)* για απεικόνιση ονομάτων κόμβων στις διευθύνσεις δικτύων, το *NTTP* για μεταφορά αρχείων και το *HTTP* για σχεδίαση ιστοσελίδων στο Internet.

Συγκρίνοντας τα δύο μοντέλα αναφοράς OSI και TCP/IP, είναι απαραίτητο να διευκρινιστεί ότι δε συγκρίνονται τα πρωτόκολλα που λειτουργούν στα διάφορα επίπεδα των μοντέλων. Βεβαία η ονομασία του μοντέλου TCP/IP παραπέμπει στα δύο κυριότερα πρωτόκολλα που βρίσκονται στο επίπεδο μεταφοράς και στο επίπεδο Διαδικτύου. Οι ομοιότητες αλλά και οι διαφορές των δύο μοντέλων παρουσιάζονται παρακάτω.

## 2.3 Ομοιότητες Μοντέλου OSI και TCP/IP

Η βασική ομοιότητα που χαρακτηρίζει τα μοντέλα αναφοράς **OSI** και **TCP/IP**, είναι πως και τα δύο μοντέλα, είναι δομημένα ως **σύνολα επιπέδων**, με το κάθε επίπεδο να αντιστοιχεί σε ένα ή περισσότερα **πρωτόκολλα**, τα οποία πραγματοποιούν μια εντελώς συγκεκριμένη μορφή επεξεργασίας, πάνω στα μεταδιδόμενα πακέτα δεδομένων. Το πιο πρωτόκολλο θα χρησιμοποιηθεί εξαρτάται **από τις απαιτήσεις των χρηστών και τις εφαρμογές οι οποίες θέλουν να επικοινωνήσουν**, ενώ είναι σημαντικό να αναφέρουμε, πως τα πρωτόκολλα των ανωτέρων επιπέδων, είναι **ανεξάρτητα** από το δίκτυο δια μέσου του οποίου θα πραγματοποιηθεί η επικοινωνία.

## 2.4 Διαφορές Μοντέλου OSI και TCP/IP

Από την άλλη πλευρά, η βασική διαφορά ανάμεσα στα δύο μοντέλα, είναι ο **διαφορετικός αριθμός των επιπέδων τους (επτά επίπεδα στο OSI και μόνο τέσσερα στο TCP/IP)**. Από εκεί και πέρα άλλες διαφορές εμφανίζονται στον τρόπο λειτουργίας του κάθε επιπέδου ξεχωριστά. Για παράδειγμα, το **επίπεδο συνόδου (session layer)** στο μοντέλο του **OSI** χρησιμοποιείται ελάχιστα, ενώ το **επίπεδο παρουσίασης (presentation layer)** δε χρησιμοποιείται σχεδόν καθόλου. Επίσης, στο **επίπεδο δικτύου (network layer)** το **OSI** υποστηρίζει και τις δύο μορφές υπηρεσιών (προσανατολισμένες στη σύνδεση και μη προσανατολισμένες στη σύνδεση), ενώ στο **επίπεδο μεταφοράς (transport layer)**, υποστηρίζει μόνο την επικοινωνία την προσανατολισμένη στη σύνδεση. Αντίθετα, το **TCP/IP** υποστηρίζει στο **επίπεδο διαδικτύου (internet layer)** μόνο τη μη προσανατολισμένη στη σύνδεση επικοινωνία, ενώ υποστηρίζει και τους δύο τρόπους επικοινωνίας στο επίπεδο μεταφοράς.

Τέλος, λόγω της διαφορετικής φιλοσοφίας με βάση την οποία σχεδιάστηκαν και υλοποιήθηκαν αυτά τα δύο μοντέλα αναφοράς, υπάρχουν και άλλες διαφορές όπως είναι η **έλλειψη σαφούς διαχωρισμού ανάμεσα στις έννοιες της υπηρεσίας (service), της διεπαφής (interface) και του πρωτοκόλλου (protocol)** που παρατηρείται στο μοντέλο του **OSI** αλλά όχι και στο μοντέλο του **TCP/IP** όπως επίσης και η **ασυμφωνία** ανάμεσα στα πρωτόκολλα και στα μοντέλα, που δεν υφίσταται στο **TCP/IP** αλλά εμφανίζεται εντονότερη στο μοντέλο του **OSI**.

## 2.5 Τα πρωτόκολλα μεταφοράς του Internet

Το Internet έχει δύο βασικά πρωτόκολλα στο επίπεδο μεταφοράς. Αυτά είναι το **TCP** και το **UDP**. Το συνδεσμωτικό πρωτόκολλο είναι το **TCP**, ενώ το **UDP** είναι ασυνδεσμικό πρωτόκολλο.

### 2.5.1 Το Πρωτόκολλο Ελέγχου Μετάδοσης (Transmission Control Protocol - TCP)

Το Πρωτόκολλο Ελέγχου Μετάδοσης (Transmission Control Protocol - TCP) σχεδιάστηκε για την παροχή μιας από άκρου σε άκρο αξιόπιστης ροής byte μέσω ενός

αξιόπιστου διαδικτύου. Το διαδίκτυο διαφέρει από ένα μοναδικό δίκτυο επειδή τα διάφορα μέρη του μπορεί να έχουν εντελώς διαφορετική τοπολογία, εύρος ζώνης, μέγεθος πακέτων καθώς και άλλες παραμέτρους. Το TCP σχεδιάστηκε για να προσαρμόζεται δυναμικά στις ιδιότητες ενός διαδικτύου.

Στην υπηρεσία του TCP, τόσο ο αποστολέας όσο και ο παραλήπτης δημιουργούν τερματικά σημεία, που ονομάζονται υποδοχές. Κάθε υποδοχή έχει έναν αριθμό υποδοχής (διεύθυνση), η οποία αποτελείται από τη διεύθυνση IP του υπολογιστή υπηρεσίας και ένα 16μπιτο αριθμό με τοπική σημασία για τον υπολογιστή υπηρεσίας, ο οποίος λέγεται θύρα (port). Μία υποδοχή μπορεί να χρησιμοποιείται για περισσότερες από μία συνδέσεις ταυτόχρονα. Οι αριθμοί των θυρών κάτω από το 1024 ονομάζονται ευρέως γνωστές θύρες (well-known ports) και χρησιμοποιούνται για τις τυποποιημένες υπηρεσίες.

Όλες οι συνδέσεις TCP είναι “πλήρως” αμφίδρομες και “από σημείο σε σημείο”. “Πλήρως” αμφίδρομες σημαίνει ότι η κίνηση μπορεί να ρέει και προς τις δύο κατευθύνσεις την ίδια χρονική στιγμή. “Από σημείο σε σημείο” σημαίνει ότι κάθε σύνδεση έχει ακριβώς 2 τερματικά σημεία, χωρίς πολυδιανομή (πολλαπλή διανομή) ή εκπομπή. Μία σύνδεση TCP είναι μία ροή byte, όχι μια ροή δεδομένων, καθώς και τα όρια των μηνυμάτων δεν διατηρούνται από άκρο σε άκρο. Οι οντότητες αποστολής και λήψης TCP ανταλλάσσουν δεδομένα με τη μορφή τμημάτων. Το τμήμα TCP (TCP segment) αποτελείται από μία σταθερή κεφαλίδα των 20 byte, η οποία ακολουθείται από 0 ή από περισσότερα byte δεδομένων. Το λογισμικό του TCP αποφασίζει πόσο μεγάλα πρέπει να είναι τα τμήματα. Μπορεί να συσσωρεύσει δεδομένα από πολλαπλές εγγραφές σε ένα τμήμα, ή να διασπάσει τα δεδομένα μίας εγγραφής σε πολλά τμήματα. Το μέγεθος των τμημάτων περιορίζεται από δύο λόγους. Πρώτον, κάθε τμήμα μαζί με την κεφαλίδα του TCP θα πρέπει να χωράει στο ωφέλιμο φορτίο των 65.515 byte του IP. Δεύτερον, κάθε δίκτυο έχει μια *Μέγιστη Μονάδα Μεταφοράς* (Maximum Transfer Unit – MTU), και κάθε τμήμα θα πρέπει να χωράει σε μία MTU το μέγεθος της οποίας είναι 1500 byte, γεγονός που προσδιορίζει το όριο ως προς το μέγεθος των τμημάτων.

Το βασικό πρωτόκολλο που χρησιμοποιείται από το TCP είναι το πρωτόκολλο του κυλιόμενου παραθύρου. Όταν ένας αποστολέας μεταδίδει ένα τμήμα, ξεκινά και να λειτουργεί και ένα χρονόμετρο. Όταν το τμήμα φτάσει στον προορισμό του, επιστρέφεται ένα τμήμα (με δεδομένα αν υπάρχουν, διαφορετικά χωρίς δεδομένα) το οποίο φέρει ένα αριθμό επιβεβαίωσης ίσο με τον επόμενο αριθμό ακολουθίας που περιμένει να λάβει. Αν ο χρόνος αναμονής του αποστολέα λήξει πριν λάβει την επιβεβαίωση, ο αποστολέας μεταδίδει ξανά το τμήμα. Τα τμήματα μπορεί επίσης να καθυστερήσουν τόσο πολύ στη διαδρομή με αποτέλεσμα να λήξει ο χρόνος αναμονής του αποστολέα και να αναμεταδοθούν. Αυτές οι αναμεταδόσεις μπορεί να περιέχουν διαφορετικές περιοχές byte από την αρχική μετάδοση, γεγονός που απαιτεί προσεκτική διαχείριση ώστε να μπορούν να παρακολουθούνται τα byte που έχουν ληφθεί σωστά μέχρι στιγμής. Το TCP πρέπει να μπορεί να αντιμετωπίσει αυτά τα προβλήματα ( π.χ ζητήματα συμφόρησης) και να τα λύσει με αποδοτικό τρόπο.

### 2.5.1.1 Έλεγχος Συμφόρησης

Ένα από τα πιο ενδιαφέροντα στοιχεία του TCP είναι ένας μηχανισμός για τον έλεγχο της συμφόρησης (congestion control). Στα περισσότερα διαδίκτυα, η απώλεια πακέτων ή η εξαιρετικά μεγάλη καθυστέρηση είναι πιο πιθανό να προκληθεί από συμφόρηση παρά από μια βλάβη υλικού. Το ενδιαφέρον είναι ότι τα πρωτόκολλα μεταφοράς που χρησιμοποιούν επαναμετάδοση μπορεί να επιτείνουν το πρόβλημα της συμφόρησης, εισάγοντας πρόσθετα

αντίγραφο ενός μηνύματος. Αν η συμφόρηση προκαλέσει πολλές επαναμεταδόσεις, ολόκληρο το σύστημα μπορεί να φτάσει σε μια κατάσταση *συμφορητικής κατάρρευσης* (*congestion collapse*). Για να αποφευχθεί αυτό το πρόβλημα, το TCP χρησιμοποιεί πάντα ως μέτρο της συμφόρησης την απώλεια πακέτων, και αποκρίνεται μειώνοντας το ρυθμό με τον οποίο επαναμεταδίδει δεδομένα.

Η ιδανικότερη αντιμετώπιση μιας συμφόρησης συνήθως είναι η μείωση του ρυθμού μετάδοσης. Ωστόσο το TCP δεν υπολογίζει κάποιον ακριβή ρυθμό μετάδοσης, αλλά βασίζεται τη μετάδοση σε χώρους προσωρινής αποθήκευσης. Δηλαδή, ο παραλήπτης αναγγέλει ένα μέγεθος παραθύρου, και ο αποστολέας μπορεί να μεταδίδει δεδομένα ώστε να συμπληρώσει το παράθυρο του παραλήπτη μέχρι να λάβει μια επιβεβαίωση. Το TCP για να ελέγξει το ρυθμό μετάδοσης δεδομένων, επιβάλλει έναν περιορισμό στο μέγεθος του παραθύρου, μειώνοντας προσωρινά το μέγεθος του παραθύρου, το TCP του αποστολέα στην ουσία μειώνει το ρυθμό μεταφοράς δεδομένων.

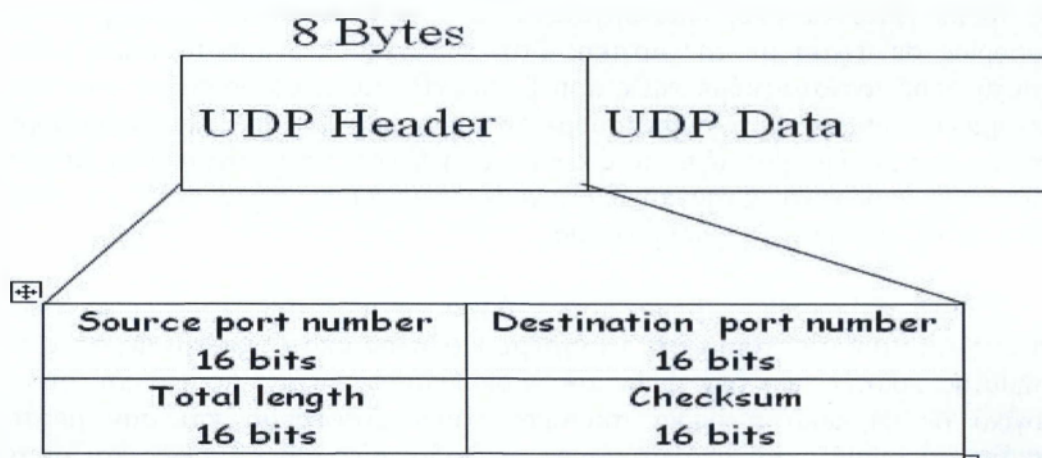
Όποτε χάνεται ένα μήνυμα, το TCP ξεκινάει τον έλεγχο της συμφόρησης. Αντί να επαναμεταδίδει όσα δεδομένα χρειάζονται για να γεμίσει ο χώρος προσωρινής αποθήκευσης του παραλήπτη, το TCP στέλνει πρώτα ένα μόνο μήνυμα που περιέχει δεδομένα. Αν έρθει η επιβεβαίωση χωρίς απώλεια, το TCP διπλασιάζει την ποσότητα των δεδομένων, και στέλνει δύο μηνύματα ακόμα. Αν έρθουν επιβεβαιώσεις για αυτά τα δύο μηνύματα, το TCP στέλνει άλλα τέσσερα, και ούτω καθεξής. Η εκθετική αύξηση συνεχίζεται, μέχρι το TCP να στείλει τα μισά από όσα χωρούν στο παράθυρο του παραλήπτη, οπότε επιβραδύνει το ρυθμό αύξησης. Μετά από αυτό, το TCP αυξάνει το μέγεθος του παραθύρου γραμμικά (για όσο δεν παρουσιάζεται συμφόρηση). Ο μηχανισμός ελέγχου συμφόρησης του TCP ανταποκρίνεται καλά στην αυξημένη κυκλοφορία σε ένα διαδίκτυο. Με τη γρήγορη υποχώρηση, το TCP μπορεί να μετριάξει τη συμφόρηση. Επίσης, επειδή αποφεύγει να προσθέτει επαναμεταδόσεις σε ένα υπερφορτωμένο διαδίκτυο, ο μηχανισμός ελέγχου συμφόρησης του TCP βοηθά να αποφευχθεί η συμφορητική κατάρρευση. Αυτός ο εκθετικός αλγόριθμος ονομάζεται αργή εκκίνηση (*slow start*), στην πραγματικότητα δεν είναι καθόλου αργός και σύμφωνα με αυτόν το αρχικό μέγεθος του παραθύρου τίθεται ίσο με το μέγεθος του μεγαλύτερου τεμαχίου που εφαρμόζεται στη σύνδεση.

Δύο προβλήματα που υπάρχουν είναι: η *χωρητικότητα του δικτύου* και η *χωρητικότητα του παραλήπτη*. Για να αντιμετωπιστούν αυτά, ο κάθε αποστολέας διατηρεί δύο παράθυρα: το παράθυρο που έχει παραχωρήσει ο παραλήπτης και το *παράθυρο συμφόρησης* (*congestion window*). Κάθε παράθυρο αντικατοπτρίζει το πλήθος των byte που μπορεί να μεταδώσει ο αποστολέας. Το πλήθος των byte που μπορεί να σταλεί είναι η ελάχιστη τιμή των δύο παραθύρων.

Ο αλγόριθμος ελέγχου συμφόρησης του Internet εκτός από τα παράθυρα παραλήπτη και συμφόρησης, χρησιμοποιεί και μια τρίτη παράμετρο, το κατώφλιο (*threshold*), η οποία αρχικά είναι ίση με 64 KB. Όταν συμβεί μια λήξη χρόνου αναμονής, το κατώφλιο παίρνει τιμή ίση με το μισό του παραθύρου συμφόρησης, ενώ το παράθυρο συμφόρησης τίθεται ίσο με ένα τμήμα μέγιστου μεγέθους. Στη συνέχεια χρησιμοποιείται η αργή εκκίνηση για να καταλάβουμε τι μπορεί να αντέξει το δίκτυο, με τη διαφορά ότι η εκθετική αύξηση σταματά όταν φτάσουμε στο κατώφλιο. Από αυτό το σημείο και μετά, οι επιτυχημένες μεταδόσεις αυξάνουν το παράθυρο συμφόρησης γραμμικά αντί να το διπλασιάζουν μία φορά ανά τμήμα.

## 2.5.2 Το πρωτόκολλο UDP

Το πακέτο πρωτοκόλλων του Internet υποστηρίζει ένα ασυνδεδεμένο πρωτόκολλο μεταφοράς, το *Πρωτόκολλο Αυτοδύναμων Πακέτων Χρήστη ή UDP (User Datagram Protocol)*. Το UDP παρέχει στις εφαρμογές μια μέθοδο για την αποστολή ενθυλακωμένων αυτοδύναμων πακέτων IP χωρίς απαραίτητα να εγκαθιδρύσουν μια σύνδεση. Κάθε μήνυμα UDP ονομάζεται αυτοδύναμο πακέτο χρήστη (user datagram) και αποτελείται από δύο μέρη: μια μικρή κεφαλίδα των οκτώ οκτάδων που καθορίζει τις εφαρμογές αποστολής και λήψης και ένα ωφέλιμο φορτίο το οποίο φιλοξενεί τα δεδομένα προς αποστολή. Η μορφή του αυτοδύναμου πακέτου φαίνεται στην παρακάτω εικόνα:



Τα δύο πρώτα πεδία της κεφαλίδας του UDP περιέχουν αριθμούς θυρών πρωτοκόλλου. Το πεδίο *Θύρα Αφειτηρίας UDP* περιέχει τον αριθμό θύρας της εφαρμογής – αποστολέα και το πεδίο *Θύρα Προορισμού UDP* περιέχει τον αριθμό θύρας της εφαρμογής – παραλήπτη. Το πεδίο *Μήκος Μηνύματος UDP* καθορίζει το συνολικό μέγεθος του μηνύματος UDP σε οκτάδες.

Το UDP δεν παρέχει έλεγχο ροής σφαλμάτων, ή αναμεταδόσεις μετά την λήψη ενός εσφαλμένου τμήματος. Όλα αυτά είναι θέμα των διεργασιών του χρήστη. Αυτό που κάνει είναι να παρέχει μια διασύνδεση με το πρωτόκολλο IP, με την πρόσθετη ευκολία της αποπολύπλεξης πολλαπλών διεργασιών μέσω των θυρών. Αυτό είναι το μόνο που κάνει. Για εφαρμογές που θέλουν αυτές τον ακριβή έλεγχο ως προς τη ροή των πακέτων, τον έλεγχο σφαλμάτων, ή το χρονισμό, το UDP παρέχει ακριβώς αυτό που χρειάζονται.

## ΔΕΙΓΜΑΤΟΛΗΨΙΑ, ΚΒΑΝΤΙΣΗ ΚΑΙ ΚΩΔΙΚΟΠΟΙΗΣΗ ΣΗΜΑΤΩΝ

Για να εκμεταλευτούμε τα πλεονεκτήματα της ψηφιακής μετάδοσης σημάτων πρέπει να μετατρέψουμε το αναλογικό σήμα σε ψηφιακό. Για να επιτευχθεί αυτός ο σκοπός χρειαζόμαστε έναν δειγματολήπτη, που θα παίρνει τιμές (δείγματα) από το αναλογικό σήμα με τέτοιο τρόπο ώστε να μπορούμε αργότερα να το επεξεργαστούμε χωρίς μεγάλη απώλεια πληροφορίας σε σχέση με την αρχική. Στην συνέχεια, περνάμε το σήμα μέσα από έναν κβαντιστή όπου αντιστοιχούμε τιμές που βρίσκονται μέσα σε ορισμένα διαστήματα σε μια συγκεκριμένη τιμή ώστε να συμπίεσουμε το σήμα μας (με απώλεια πληροφορίας). Τέλος, κωδικοποιούμε το σήμα μας μέσω ενός κωδικοποιητή ώστε στην συνέχεια να μπορέσουμε να το μεταδώσουμε αποδοτικά. Στην πηγή αποκωδικοποιείται το σήμα ώστε να μπορέσουμε να διαβάσουμε την μεταδιδόμενη πληροφορία.

Ένα επιπρόσθετο βήμα που υπάρχει σε αρκετές περιπτώσεις είναι η χρήση συμπίεστη πριν την κβάντιση ώστε να έχουμε καλύτερα αποτελέσματα ως προς την ποιότητα του σήματος. Αποτέλεσμα των τριών αυτών διαδικασιών είναι η μετατροπή του σήματος από αναλογικό σε ψηφιακό η οποία συντομογραφικά αναφέρεται και σαν μετατροπή A/D. Παρακάτω παρουσιάζονται αναλυτικότερα οι διαδικασίες αυτές, καθώς και οι τεχνικές που χρησιμοποιούνται.

### 3.1 Δειγματοληψία

Στην επιστήμη της επεξεργασίας σήματος, **δειγματοληψία** είναι η μετατροπή ενός συνεχούς σήματος σε διακριτό. Ένα συνηθισμένο παράδειγμα δειγματοληψίας είναι η μετατροπή ενός ηχητικού σήματος (συνεχές σήμα) σε μια σειρά από δείγματα (που ονομάζεται σήμα διακριτού χρόνου). Το **δείγμα** συνήθως αναφέρεται σε μια τιμή του συνεχούς σήματος σε μια συγκεκριμένη χρονική στιγμή. Ο **δειγματολήπτης** είναι ένα σύστημα το οποίο εξάγει δείγματα (σε ίσα χρονικά διαστήματα) από ένα συνεχές σήμα. Ένας θεωρητικός ιδανικός δειγματολήπτης δημιουργεί δείγματα τα οποία αντιστοιχούν στην στιγμιαία τιμή του συνεχές σήματος στα επιθυμητά χρονικά σημεία. Η **συχνότητα δειγματοληψίας** ή **ρυθμός δειγματοληψίας** μετριέται σε  $H_z$  και μας δείχνει πόσα δείγματα έχουν ληφθεί από τον δειγματολήπτη σε διάρκεια ενός δευτερολέπτου. Εάν η συχνότητα δειγματοληψίας  $f_s$  (ο συμβολισμός  $f_s$  προκύπτει από τα αρχικά *sampling frequency* - συχνότητα δειγματοληψίας) είναι  $1000 H_z$ , σημαίνει ότι ο δειγματολήπτης δημιουργεί 1000 δείγματα σε κάθε δευτερόλεπτο σήματος.

Η διαδικασία της δειγματοληψίας βασίζεται στο θεώρημα δειγματοληψίας για σήματα περιορισμένου εύρους ζώνης. Το θεώρημα δειγματοληψίας του **Nyquist** έχει ως εξής: Έστω το σήμα  $m(t)$  περιορισμένου εύρους ζώνης το οποίο δειγματοληπτείται κάθε  $T$  sec όπου  $T=1/2 \cdot f_m$  και  $f_m$  η μέγιστη συχνότητά του. Κατά την διαδικασία λοιπόν της δειγματοληψίας, λαμβάνονται δείγματα της εισερχόμενης κυματομορφής πληροφορίας με μια ακολουθία στενών ορθογώνιων παλμών.



Για να εξασφαλιστεί η τέλεια ανακατασκευή της πληροφορίας στο δέκτη, ο ρυθμός της δειγματοληψίας πρέπει να είναι μεγαλύτερος από το διπλάσιο της υψηλότερης συνιστώσας συχνότητας  $W$  της κυματομορφής πληροφορίας σύμφωνα με το θεώρημα δειγματοληψίας. Στην πράξη, πριν να εισάγουμε το σήμα στο δειγματολήπτη χρησιμοποιείται ένα βαθυτερατό φίλτρο έτσι ώστε να απορρίπτονται συχνότητες μεγαλύτερες από  $W$  πριν από την δειγματοληψία.

### 3.2 Κβαντισμός – Κωδικοποίηση

Μετά τη φάση της δειγματοληψίας τα δείγματα αυτά υφίστανται μια διαδικασία που ονομάζεται κβάντιση. Είναι μια διαδικασία αντιστοίχισης των συνεχών τιμών που έχουν τα δείγματα που παίρνουμε σε κάποια επίπεδα σήματος, σε μια προσπάθεια να κάνουμε τα συνεχή μεγέθη να πάρουν πεπερασμένο πλήθος τιμών. Κατόπιν αυτά τα επίπεδα αριθμούνται κι αυτό που μεταδίδεται για κάθε δείγμα είναι ο αύξων αριθμός του επιπέδου στο οποίο είναι πιο κοντά στην τιμή του δείγματος μας. Αυτός ο αύξοντας αριθμός μεταδίδεται στο δυαδικό σύστημα κι έτσι έχουμε την ψηφιακή μετάδοση του σήματος μας. Σημαντικό είναι να τον τονίσουμε ότι η δειγματοληψία και η κβάντιση είναι συμπληρωματικές διαδικασίες και ο συνδυασμός αυτών των δύο διαδικασιών, καλείται ψηφιοποίηση. Η κβάντιση παίζει καθοριστικό ρόλο στο σχεδιασμό του συστήματος του ψηφιακού ήχου, ενώ ανάλογα με τις στάθμες κβάντισης διαμορφώνεται και το format του ψηφιακού ήχου. Βασική παράμετρος της φάσης αυτής είναι το μέγεθος του δείγματος, με επακόλουθο όσα περισσότερα bits χρησιμοποιούνται με μεγαλύτερη ακρίβεια περιγραφής. Για παράδειγμα, αν έχουμε 8 bit, τότε μπορούν χρησιμοποιηθούν  $2^8=256$  διαφορετικές τιμές, ενώ για 16bit μπορούν να χρησιμοποιηθούν  $2^{16}=65.536$  διαφορετικές τιμές, άρα μεγαλύτερη πιστότητα και ακρίβεια.

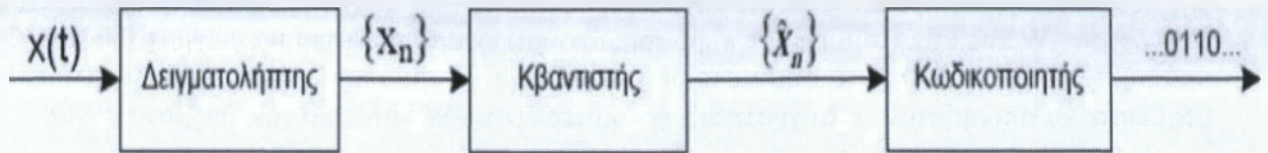
### 3.3 Τεχνικές Κωδικοποίησης

Σ'αυτήν την παράγραφο θα περιγράψουμε μερικές από τις βασικότερες τεχνικές κωδικοποίησης που χρησιμοποιούνται σήμερα στη μετάδοση σημάτων. Αυτές είναι: *ομοιόμορφο PCM, μη ομοιόμορφο PCM, παλμοκωδική διαμόρφωση αποδιαμόρφωση PCM, διαμόρφωση δέλτα, διαφορική παλμοκωδική διαμόρφωση και προσαρμοζόμενη διαφορική παλμοκωδική διαμόρφωση.*

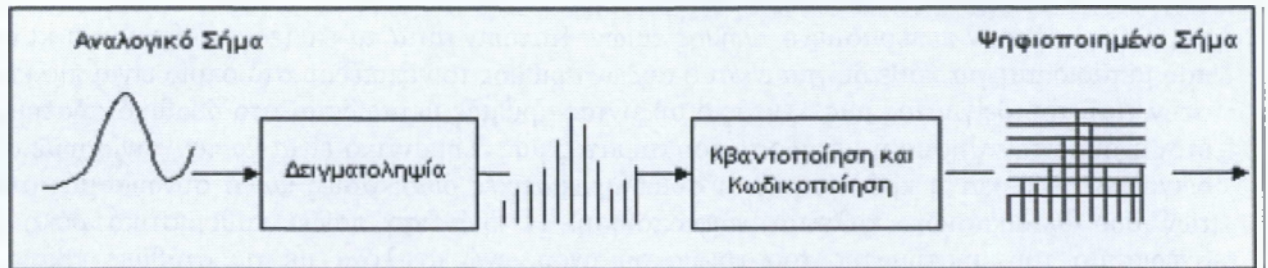
#### 3.3.1 Παλμοκωδική Διαμόρφωση (PCM)

Η *παλμοκωδική διαμόρφωση Pulse Code Modulation (PCM)* είναι το παλιότερο και απλούστερο σχήμα κωδικοποίησης κυματομορφής. Ένας παλμοκωδικός διαμορφωτής παλμών αποτελείται από τρία βασικά μέρη:

- Τον δειγματολήπτη
- Τον κβαντιστή
- Τον κωδικοποιητή



**Διάγραμμα Βαθμίδων ενός συστήματος PCM**



Πριν την εισαγωγή στο δειγματολήπτη ενός σήματος, αυτό έχει περάσει συνήθως από ένα προδειγματοληπτικό φίλτρο που εμποδίζει την είσοδο συνιστωσών του σήματος πέρα από το εύρος ζώνης  $W$  που μας ενδιαφέρει. Αφού το σήμα περάσει από τον δειγματολήπτη όπου συνήθως δειγματοληπτείται με συχνότητα μεγαλύτερη από αυτή του Nyquist, έτσι ώστε να δημιουργηθεί μια ζώνη προστασίας (υπερδειγματολήπτηση), εισέρχεται σε έναν βαθμωτό κβαντιστή. Ο κβαντιστής αυτός μπορεί να είναι είτε ομοιόμορφος είτε μη ομοιόμορφος ανάλογα με τα στατιστικά χαρακτηριστικά της εξόδου της πηγής. Μετά την κβάντισή του το σήμα κωδικοποιείται από τον κωδικοποιητή με μια δυαδική ακολουθία μήκους  $N=2^y$  είναι ο αριθμός των σταθμών κβάντισης. Η PCM διευκολύνει τη ψηφιακή μετάδοση από σημείο σε σημείο (σε σειρά ζεύξεων).

Στο σημείο αυτό, θα πρέπει να ορίσουμε ένα μέγεθος που λέγεται λόγος σήματος προς θόρυβο κβάντισης (SQNR). Αν λοιπόν μια τυχαία μεταβλητή  $X$  κβαντιστεί σε  $Q(X)$ , ο λόγος αυτός ορίζεται ως:

$$SQNR = \frac{P_x}{P_{\tilde{x}}}$$

Όταν εξετάζουμε χρονικά σήματα, η ισχύς του θορύβου κβάντισης είναι :

$$P_{\tilde{x}} = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} E \left[ \left( X(t) - Q(X(t)) \right)^2 \right] dt$$

Και η ισχύς του σήματος είναι:

$$P_x = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} E [ X(t)^2 ] dt$$

Επομένως, το SQNR είναι :

$$SQNR = \frac{P_x}{P_{\tilde{x}}}$$

### 3.3.2 ΑΠΟΔΙΑΜΟΡΦΩΣΗ PCM

Μετά τη μετάδοση του σήματος PCM μέσω ενός καναλιού, το λαμβανόμενο σήμα αποκωδικοποιείται για να αναπαράγει τα σύμβολα, για παράδειγμα τα bits εάν επρόκειτο για δυαδική διαμόρφωση. Στον αποκωδικοποιητή τα σύμβολα ομαδοποιούνται σε κωδικές λέξεις και αποκωδικοποιούνται σε αναλογικά σήματα.

### 3.3.3 Ομοιόμορφο PCM

Στις εφαρμογές ομοιόμορφου PCM υποθέτουμε ότι οι τιμές των δειγμάτων της εισόδου βρίσκονται στο διάστημα  $[-x_{max}, +x_{max}]$  και το πλήθος των σταθμών κβάντισης  $N$  του 2,  $N=2^v$ . Έτσι το εύρος κάθε περιοχής δίνεται από τη σχέση:

$$\Delta = \frac{2 x_{max}}{N} = \frac{2 x_{max}}{2^v} = \frac{x_{max}}{2^{v-1}}$$

Στο ομοιόμορφο PCM ως τιμές κβάντισης επιλέγονται τα μέσα των περιοχών κβάντισης και επομένως το σφάλμα  $\tilde{x} = x - Q(x)$  είναι μια τυχαία μεταβλητή που παίρνει τιμές στο διάστημα  $(-\frac{\Delta}{2}, \frac{\Delta}{2}]$ . Το σφάλμα  $\tilde{x} = x - Q(x)$  μπορεί να προσεγγίσει καλά μια τυχαία μεταβλητή, ομοιόμορφα κατανομημένη στο παραπάνω διάστημα. Η παραμόρφωση που παρουσιάζεται λόγω της κβάντισης (θόρυβος κβάντισης) είναι :

$$E[\tilde{X}^2] = \int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} \frac{1}{\Delta} \tilde{x}^2 d\tilde{x} = \frac{\Delta^2}{12} = \frac{x_{\max}^2}{3N^2} = \frac{x_{\max}^2}{3 \times 4^v}$$

Όπου  $v$  είναι ο αριθμός των bits/δείγμα πηγής. Ο λόγος SQNR λοιπόν γίνεται:

$$SQNR = \frac{E(X^2)}{E(\tilde{X}^2)} = \frac{E(X^2)}{\frac{x_{\max}^2}{3 \times 4^v}} = \frac{3 \times 4^v \times E(X^2)}{x_{\max}^2}$$

Αν συμβολίσουμε την κανονικοποιημένη τυχαία μεταβλητή  $X$  με  $\tilde{X}$  δηλαδή

$$\tilde{X} = \frac{X}{x_{\max}}, \text{ τότε:}$$

$$SQNR = 3 \times N^2 \times E(\tilde{X}^2)$$

Εκφράζοντας το SQNR σε Db προκύπτει:

$$SQNR_{dB} \approx P_{\tilde{x}}_{dB} + 6v + 4.8$$

Όπως φαίνεται, κάθε επιπλέον bit (δηλαδή αύξηση του  $v$  κατά 1) αυξάνει το SQNR κατά 6dB.

Συνοψίζοντας τα αποτελέσματα που αφορούν τις απαιτήσεις σε εύρος ζώνης ενός συστήματος PCM, αν ένα σήμα έχει εύρος ζώνης  $W$ , τότε ο ελάχιστος αριθμός των δειγμάτων για τέλεια αναπαραγωγή του σήματος δίνεται από το θεώρημα δειγματοληψίας και είναι ίσος με  $2W$  δείγματα/sec. Αν χρειαστεί κάποια ζώνη ασφαλείας, τότε ο αριθμός των δειγμάτων/sec που απαιτείται γίνεται  $f_s$ , μεγαλύτερος από  $2W$ .

Για κάθε δείγμα χρησιμοποιούνται  $v$  bits, άρα χρειάζονται συνολικά  $nf_s$  bits/sec για τη διαβίβαση ενός σήματος PCM. Στην περίπτωση δειγματοληψίας με το ρυθμό Nyquist, αυτό είναι ίσο με  $2Nw$  bits/sec. Η ελάχιστη απαίτηση εύρους ζώνης για τη διαβίβαση  $R$  bits/sec (ή

ακριβέστερα,  $R$  παλμών το δευτερόλεπτο) είναι  $\frac{R}{2}$ . Άρα η ελάχιστη απαίτηση εύρους ζώνης,  $BW$ , ενός συστήματος PCM είναι:

$$B W = \frac{v f_s}{2}$$

το οποίο, στην περίπτωση δειγματοληψίας με ρυθμό Nyquist, μας δίνει την απόλυτα ελάχιστη απαίτηση εύρους ζώνης:

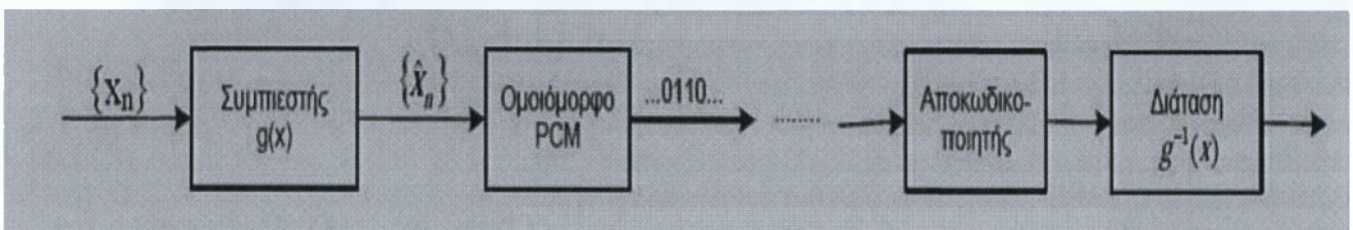
$$B W = v W$$

Αυτό σημαίνει ότι ένα σύστημα PCM διευρύνει το εύρος ζώνης του αρχικού σήματος κατά έναν παράγοντα τουλάχιστον  $v$ .

### 3.3.4 Μη ομοιόμορφο PCM

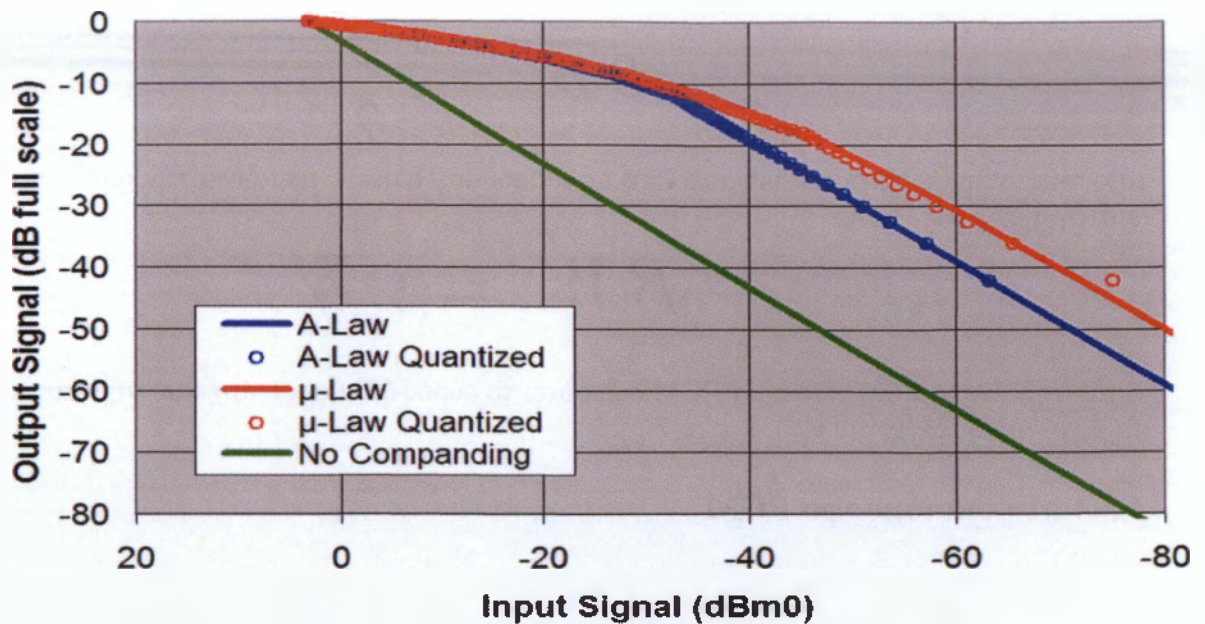
Κατά την κωδικοποίηση ορισμένων σημάτων όπως η ομιλία, η κατανομή της εισόδου απέχει πολύ από την ομοιόμορφη, σε αυτές τις περιπτώσεις προτιμούμε το μη ομοιόμορφο PCM. Η συνηθέστερη μέθοδος για την υλοποίηση της μη ομοιόμορφης κβάντισης είναι τα δείγματα να διέλθουν πρώτα από ένα μη γραμμικό στοιχείο προκειμένου να συμπιεστούν τα μεγάλα πλάτη (μείωση δυναμικής περιοχής του σήματος) και στην συνέχεια η έξοδος του μη γραμμικού σημείου να κβαντιστεί ομοιόμορφα. Στη λήψη εφαρμόζεται η αντίστροφη λειτουργία της συμπίεσης (διάταση) για να ανακτήσουμε τις τιμές των δειγμάτων. Η τεχνική αυτή ονομάζεται **companding** και περιγράφεται από το ακόλουθο σχήμα:

**Διάγραμμα Βαθμίδων Ενός Συστήματος Μη Ομοιόμορφου PCM**



Οι αλγόριθμοι συμπίεσης έχουν την ιδιότητα να μειώνουν δυναμικό εύρος ενός σήματος ήχου. Στα ψηφιακά συστήματα μπορούν να αυξήσουν το SQNR μειώνοντας το σφάλμα κβάντισης.

Για την κωδικοποίηση ομιλίας, δύο τύποι συμπεστών χρησιμοποιούνται ευρέως. Ο συμπεστής τύπου-μ ο οποίος χρησιμοποιείται στις Η.Π.Α και στην Ιαπωνία και ο συμπεστής τύπου-Α που χρησιμοποιείται κυρίως στην Ευρώπη. Ο συμπεστής τύπου-μ παρέχει ένα ελαφρώς δυναμικό εύρος σε σχέση με τον συμπεστή τύπου-Α με το κόστος χειρότερης αναλογικής παραμόρφωσης για μικρά σήματα. Συνήθως, ο συμπεστής τύπου-Α χρησιμοποιείται για διεθνής επικοινωνίες όταν τουλάχιστον μια χώρα τον χρησιμοποιεί. Στο γράφημα συγκρίνονται ο συμπεστής τύπου-μ με τον συμπεστή τύπου-Α.



Γράφημα Συμπεσστή Τύπου-μ και Συμπεσστή Τύπου-A

Οι χαρακτηριστικές που αποτελούν τον μ-κανόνα κωδικοποίησης ορίζονται ως εξής:

#### Συμπεσστής Τύπου-μ

Συμπίεση:

$$f(x) = \text{sgn}(x) \frac{\ln(1 + \mu|x|)}{\ln(1 + \mu)}, -1 \leq x \leq 1$$

Αποσυμπίεση:

$$f^{-1}(x) = \text{sgn}(x) \frac{1}{\mu} ((1 + \mu)^{|x|} - 1), 1 \leq x \leq 1$$

Όπου  $x$  το σήμα εισόδου ( $-1 \leq x \leq 1$ ),  $\text{sgn}(x)$  η συνάρτηση προσήμου του και  $\mu$  η παράμετρος που καθορίζει τη συμπίεση. Για  $\mu=0$  έχουμε γραμμικές κβαντοποιήσεις. Όσο αυξάνει η τιμή του  $\mu$  αυξάνει η συμπίεση. Αρχικά είχε επιλεγεί η τιμή  $\mu=100$  αλλά σήμερα χρησιμοποιείται αποκλειστικά η τιμή  $\mu=255$  (8 bits). Οι χαρακτηριστικές που αποτελούν τον A-κανόνα κωδικοποίησης ορίζονται ως εξής:

## Συμπιεστής Τύπου A

### Συμπίεση:

$$g(x) = \begin{cases} \text{sign}(x) \frac{A |x|}{1 + \ln A}, & |x| \leq \frac{1}{A} \\ \text{sign}(x) \frac{1 + \ln(A |x|)}{1 + \ln A}, & \frac{1}{A} \leq |x| \leq 1 \end{cases}$$

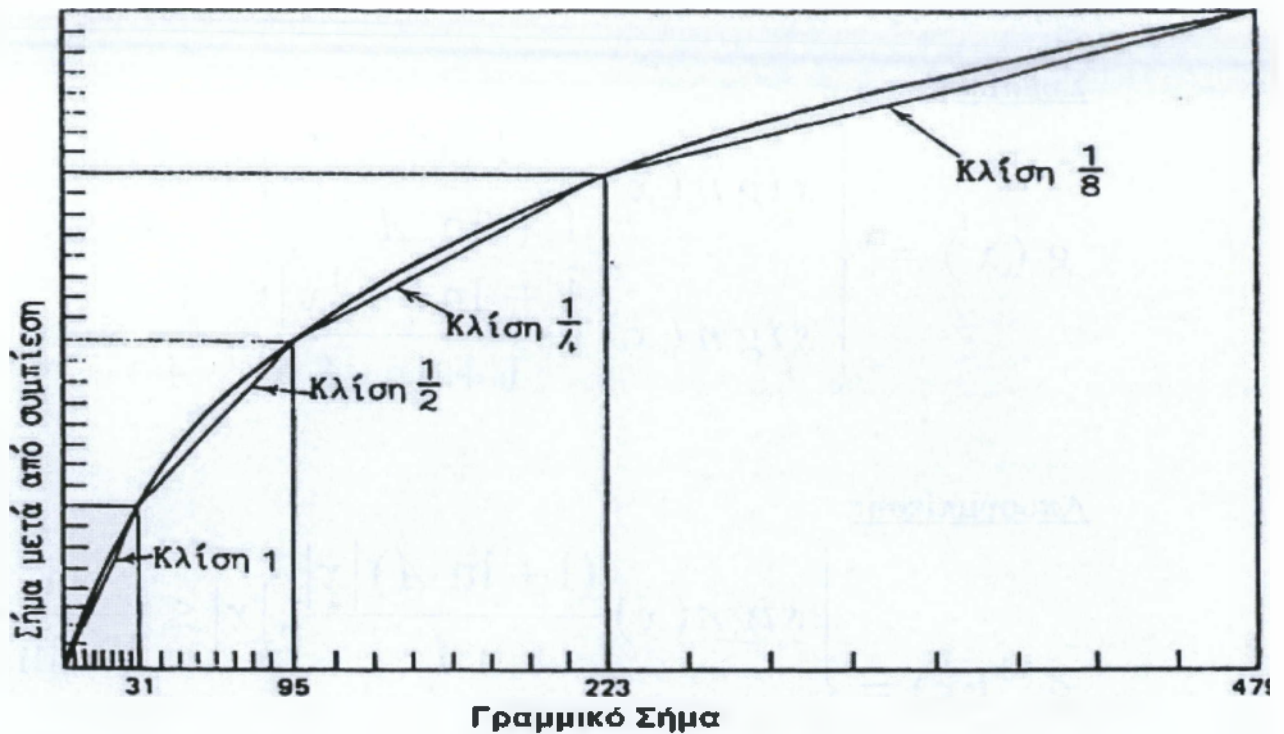
### Αποσυμπίεση:

$$g^{-1}(x) = \begin{cases} \text{sign}(x) \frac{(1 + \ln A) |x|}{A}, & |x| \leq \frac{1}{1 + \ln A} \\ \text{sign}(x) \frac{e^{|x(1 + \ln A) - 1|}}{A}, & \frac{1}{1 + \ln A} < |x| \leq 1 \end{cases}$$

Όπου η τιμή A εκλέγεται συνήθως ίση με 100.

Σήμερα τα συστήματα κωδικοποίησης χρησιμοποιούν γενικά λέξεις 8 bits σύμφωνα με τη δομή των υπολογιστικών συστημάτων και χρησιμοποιούνται επίσης αλγόριθμοι που υλοποιούν τη διαδικασία συμπίεσης-κωδικοποίησης αμέσως χωρίς την ανάγκη χρήσης μη γραμμικού στοιχείου, έχουν δηλαδή ενσωματωμένες τις παραπάνω χαρακτηριστικές συναρτήσεις. Όσο το τηλεπικοινωνιακό σύστημα γίνεται ολοένα και πιο ψηφιακό, τόσο εντονότερη γίνεται η αναγκαιότητα επεξεργασίας των σημάτων στη ψηφιακή τους μορφή έστω και συμπερισμένη χωρίς τη μετατροπή τους στα πραγματικά αναλογικά σήματα. Πολλές όμως τεχνικές επεξεργασίας ψηφιακών σημάτων (όπως απόσβεση ή πρόσθεση σημάτων) είναι γραμμικές διαδικασίες.

Επομένως, ορθότερο είναι το συμπερισμένο σήμα να μετατραπεί στην αρχική του μορφή πριν υποστεί τις διεργασίες αυτές. Έπρεπε λοιπόν να εκλεγεί μια χαρακτηριστική  $\mu$  (ή A) τέτοια ώστε η μετατροπή από αναλογικό σε ψηφιακό σήμα είναι εύκολη και αξιόπιστη. Αυτός ήταν ο λόγος επιλογής της παραμέτρου  $\mu$  που παρουσιάζει το χαρακτηριστικό ότι μπορεί να προσεγγισθεί πολύ ικανοποιητικά από 8 γραμμικά τμήματα. Η κλίση κάθε τμήματος είναι ακριβώς το μισό της κλίσης του προηγούμενου τμήματος και το πλάτος κάθε διαστήματος κβάντισης δυαδικό πολλαπλάσιο των προηγούμενων διαστημάτων. Όπως φαίνεται και στο επόμενο σχήμα:



Κανόνας  $\mu$

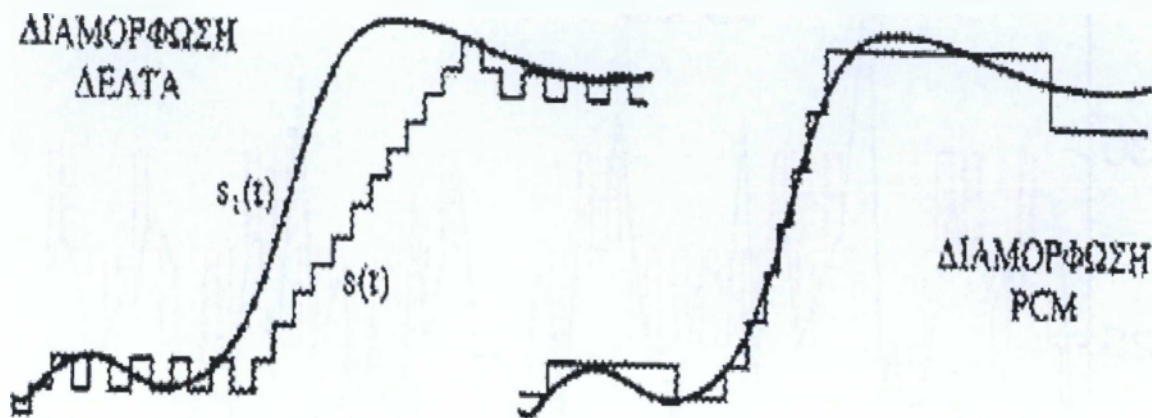
Οι παραπάνω κανόνες έχουν την δυνατότητα να μειώνουν το εύρος ζώνης, κρατώντας παράλληλα την ποιότητα της επικοινωνίας υψηλή.

### 3.3.5 Δέλτα Διαμόρφωση (DM - Delta Modulation)

Ενώ στη διαμόρφωση PCM κάθε κβαντισμένο πλάτος του σήματος κωδικοποιείται με  $n$  δυαδικά στοιχεία (bits), στη διαμόρφωση δέλτα χρησιμοποιείται 1 μόνο bit για να χαρακτηρίσει τη μεταβολή της απόκλισης του σήματος τη στιγμή της δειγματοληψίας. Σε κάθε στιγμή δειγματοληψίας συγκρίνεται το πλάτος του δείγματος με το πλάτος που λαμβάνεται από την ολοκλήρωση των παλμών που έχουν σταλεί προηγουμένως. Αν το πλάτος του δείγματος είναι μεγαλύτερο, τότε αποστέλλεται ένας θετικός παλμός 1, αν είναι μικρότερο ένας αρνητικός παλμός 0. Ο αποδιαμορφωτής είναι ένας ολοκληρωτής που αυξάνει ή μειώνει την έξοδό του ανάλογα με το λαμβανόμενο παλμό. Το αποδιαμορφωμένο σήμα παρουσιάζει ορισμένη απόκλιση από το αρχικό σήμα που οφείλεται στο ότι ο ολοκληρωτής δεν μπορεί να παρακολουθήσει ακριβώς τη μεταβολή του σήματος πληροφορίας. Η απόκλιση αυτή χαρακτηρίζει το *θόρυβο κβαντοποίησης της διαμόρφωσης Δέλτα*.

Γενικά, η παραμόρφωση αυξάνεται με τη συχνότητα και το πλάτος του σήματος εισόδου, ενώ μειώνεται με αύξηση της συχνότητας δειγματοληψίας. Έτσι σήματα με ομοιόμορφη κατανομή της ενέργειας στο φάσμα τους εμφανίζονται παραμορφωμένα στις υψηλές τους συχνότητες και για τέτοια σήματα είναι ακατάλληλη η διαμόρφωση Δέλτα. Αντίθετα είναι κατάλληλη για σήματα ομιλίας που έχουν συγκεντρωμένη την ενέργειά τους στις χαμηλές συχνότητες. Το σχήμα που ακολουθεί δίνει μια σύγκριση μεταξύ της διαμόρφωσης  $\Delta$  και της διαμόρφωσης PCM.





Φυσικά, η κβάντιση που επιτελείται εδώ είναι στην ουσία 2 επιπέδων και δεν επιτρέπει φυσικά πολύ μεγάλη ποιότητα στη μετάδοση του ήχου. Για να βελτιωθούν τα πράγματα λίγο έχει προταθεί και εφαρμόζεται υπερδειγματοληψία της εισόδου, δηλαδή παίρνουμε περισσότερα δείγματα ανά δευτερόλεπτο της εισόδου έτσι ώστε να μπορεί το σύστημα να προλαβαίνει να αντιδρά στις γρήγορες μεταβολές του σήματος. Αυτή η υπερδειγματοληψία έχει όμως σαν αποτέλεσμα στην έξοδο του αποκωδικοποιητή να εμφανίζονται στο σήμα συντελεστές φάσματος εκτός της μπάνας του σήματος μας λόγω *θορύβου κβάντισης* ή *παραμόρφωσης*, οι οποίοι όμως δεν πρέπει να μείνουν στην έξοδο. Αυτός ακριβώς είναι κι ο ρόλος του LPF που βλέπουμε στην έξοδο στο σχήμα.

Ένας παράγοντας που χαρακτηρίζει τα DM συστήματα είναι ο λόγος F:

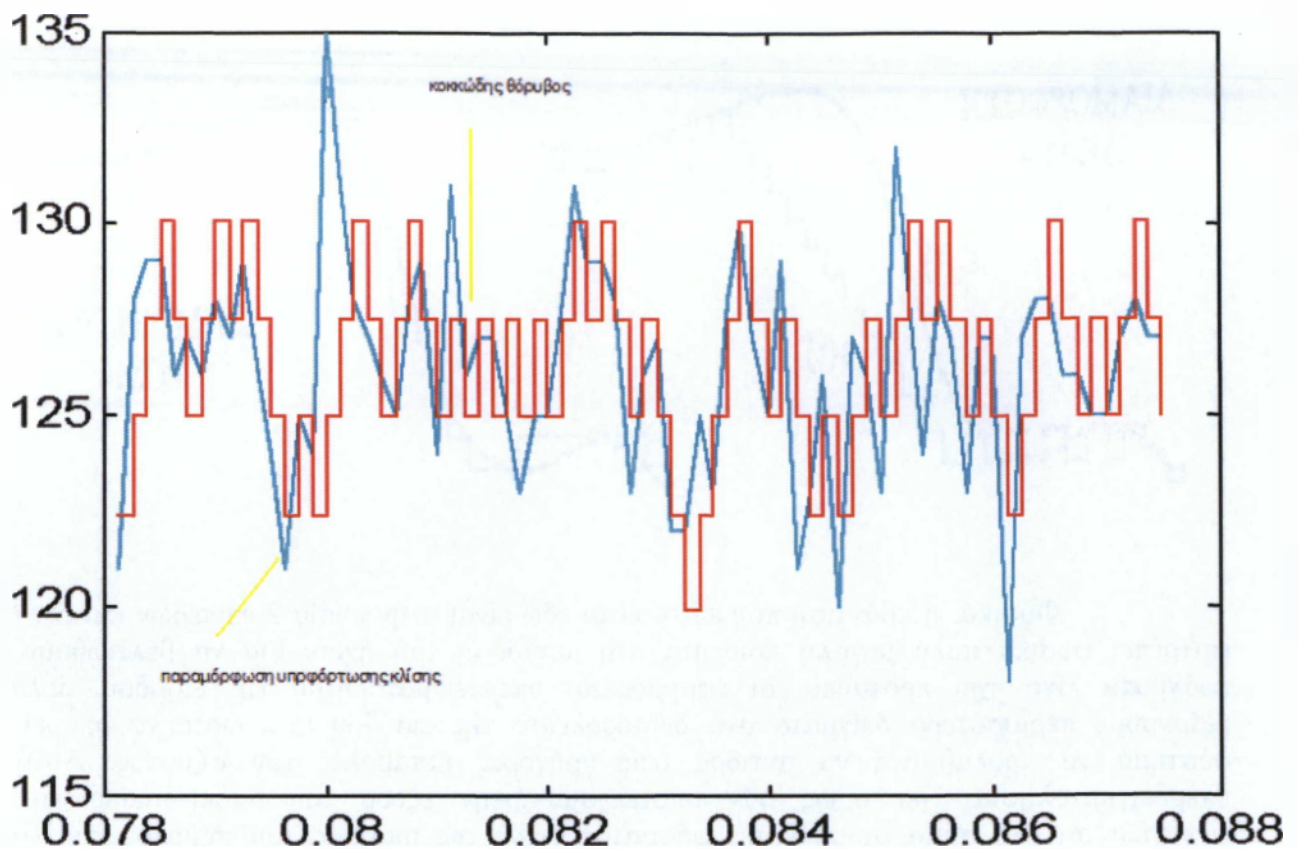
$$F = \text{Συχνότητα Δειγματοληψίας} / 2 * \text{φάσμα σήματος} \Rightarrow \mathbf{F = fs/2W}$$

Ο ρυθμός μετάδοσης I σε ένα σύστημα DM είναι:

$$\mathbf{I = fs R = fs bps}$$

Με άλλα λόγια η συχνότητα δειγματοληψίας καθορίζει το ρυθμό μετάδοσης στο DM. Ένα άλλο σημαντικό θέμα στην DM διαμόρφωση είναι η εκλογή του βήματος με το οποίο κάνει άλματα ο αποκωδικοποιητής κατά την υπόδειξη του μεταδιδόμενου bit. Όταν το βήμα είναι πολύ μικρό για την είσοδο που βάζουμε, τότε ο αποκωδικοποιητής θα αδυνατεί να παρακολουθήσει τις αλλαγές που κάνει το σήμα μας κι η έξοδος του θα είναι πολύ διαφορετική από το σήμα που βάλουμε εμείς. Το ίδιο θα συμβεί στην περίπτωση που το βήμα είναι πολύ μεγάλο. Γι' αυτό πρέπει οπωσδήποτε να χρησιμοποιηθεί το κατάλληλο βήμα δ.

Όταν αυτή μεταβάλλεται γρήγορα η έξοδος χρειάζεται αρκετά μεγάλο χρόνο για να φτάσει την είσοδο και σ' αυτή τη χρονική περίοδο δημιουργείται μια έντονη παραμόρφωση. Αυτός ο τύπος της παραμόρφωσης, ο οποίος προκαλείται από μεγάλη κλίση της κυματομορφής εισόδου, ονομάζεται *παραμόρφωση υπερφόρτωσης κλίσης (slope-overload distortion)*.

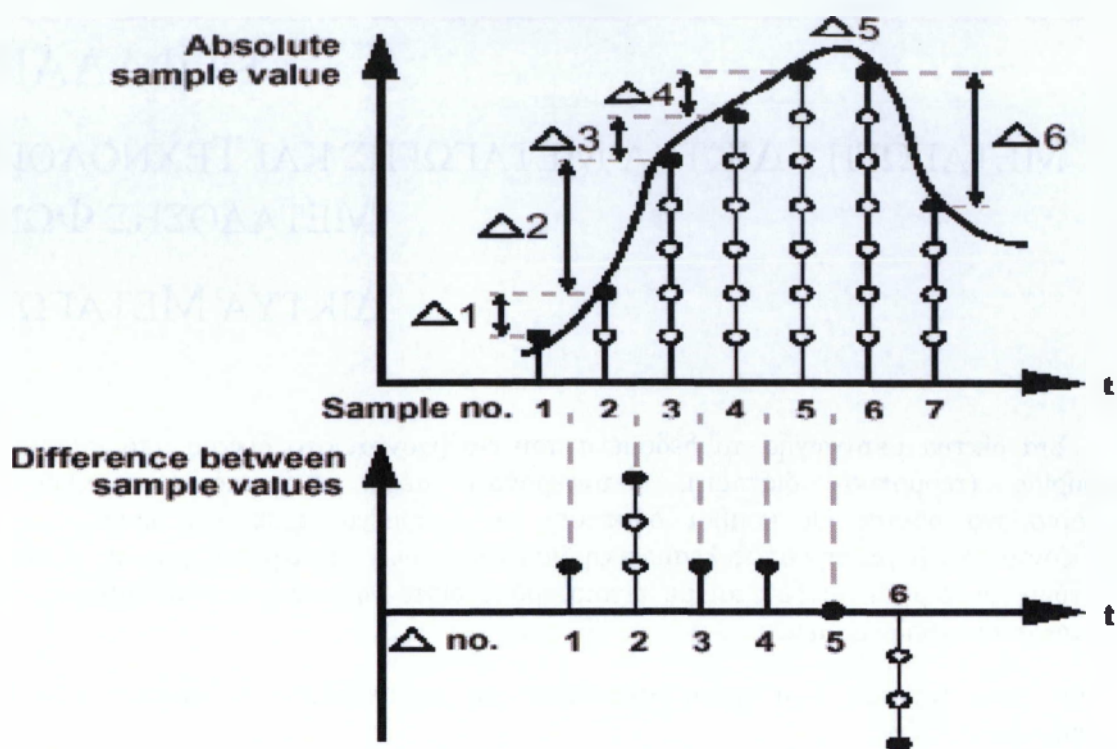


### Κοκκώδης Θόρυβος και Παραμόρφωση Υπερφόρτωσης Κλίσης

#### 3.3.6 Διαφορική Παλμοκωδική Διαμόρφωση (DPCM)

Η παλμοκωδική διαμόρφωση δεν εκμεταλλεύεται τη συσχέτιση που πιθανώς να υπάρχει ανάμεσα σε διαδοχικά δείγματα ενός συνεχούς χρονικού σήματος. Εάν το σήμα που πρόκειται να κβαντισθεί έχει μεγάλη δυναμική περιοχή, για να εξασφαλίσουμε χαμηλό θόρυβο κβάντισης, απαιτείται μεγάλος αριθμός σταθμών κβάντισης και ισοδύναμα μεγάλος αριθμός bits/δείγμα, το οποίο έχει ως αποτέλεσμα μεγάλες απαιτήσεις σε εύρος ζώνης. Με άλλα λόγια το PCM χαρακτηρίζεται από άσκοπη κατανάλωση εύρους ζώνης.

Τη λύση στην περίπτωση αυτή αποτελεί η διαφορική παλμοκωδική διαμόρφωση, της οποίας η αρχή είναι να μην στέλνεται το κομμάτι του σήματος που μπορεί να προβλεφθεί από παρελθόντα δείγματα.



### Κωδικοποίηση DPCM

Στον απλούστερο τύπο διαφορικής παλμοκωδικής διαμόρφωσης (DPCM), η διαφορά μεταξύ του δείγματος από μια εκτιμώμενη τιμή κβαντίζεται. Επειδή δύο διαδοχικά δείγματα έχουν υψηλή συσχέτιση, η διαφορά τους παρουσιάζει μικρές διακυμάνσεις και άρα, για συγκεκριμένη τιμή παραμόρφωσης, απαιτούνται λιγότερα bits για την κβάντισή της. Αυτό σημαίνει ότι το DPCM μπορεί να πετύχει επίδοση συγκρίσιμη με αυτή του PCM με μικρότερους ρυθμούς bit ή για τους ίδιους ρυθμούς bits μπορούμε να πετύχουμε βελτιωμένο SQNR.

#### 3.3.7 Προσαρμοστική ΔΜ

Είδαμε ότι το πολύ μεγάλο εύρος βαθμίδας  $\Delta$  προκαλεί κοκκώδη θόρυβο (*granular noise*), ενώ το πολύ μικρό δημιουργεί την παραμόρφωση υπερφόρτωσης κλίσης (*slope-overload distortion*). Αυτό σημαίνει ότι μια καλή επιλογή για το  $\Delta$  είναι μια ενδιάμεση τιμή, αλλά σε μερικές περιπτώσεις η επίδοση της καλύτερης ενδιάμεσης τιμής (ακόμα και εκείνης που ελαχιστοποιεί τη μέση τετραγωνική παραμόρφωση) δεν αποδεικνύεται ικανοποιητική.

Μία προσέγγιση που λειτουργεί ικανοποιητικά στις περιπτώσεις αυτές είναι να μεταβάλλουμε το εύρος βαθμίδας σύμφωνα με τις μεταβολές στην είσοδο. Αν η είσοδος τείνει να μεταβάλλεται γρήγορα, το εύρος βαθμίδας επιλέγεται μεγάλο ώστε η έξοδος να μπορεί να ακολουθεί την είσοδο γρήγορα και να μην προκύπτει παραμόρφωση υπερφόρτωσης κλίσης. Όμως, όταν η είσοδος μεταβάλλεται αργά (είναι δηλαδή σχετικά σταθερή), το εύρος βαθμίδας γίνεται μικρό για να αποφευχθεί ο κοκκώδης θόρυβος.

---

## ΚΕΦΑΛΑΙΟ 4

# ΜΕΤΑΓΩΓΗ - ΔΙΚΤΥΑ ΜΕΤΑΓΩΓΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΜΕΤΑΔΟΣΗΣ ΦΩΝΗΣ ΔΙΚΤΥΑ ΜΕΤΑΓΩΓΗΣ

Στα δίκτυα μεταγωγής, τα δεδομένα που εισέρχονται στο δίκτυο από κάποια πηγή πληροφορίας (τερματική διάταξη), μεταφέρονται μέσω ενδιάμεσων κόμβων στον προκαθορισμένο δέκτη. Οι κόμβοι διακινούν τα δεδομένα προς τον προορισμό τους αποφασίζοντας ή όχι για την αποτελεσματική διακίνησή τους. Για την αύξηση της αξιοπιστίας του δικτύου, οι κόμβοι συνδέονται με τέτοιο τρόπο ώστε να υπάρχει εναλλακτικός δρόμος μεταξύ των τερματικών σημείων.

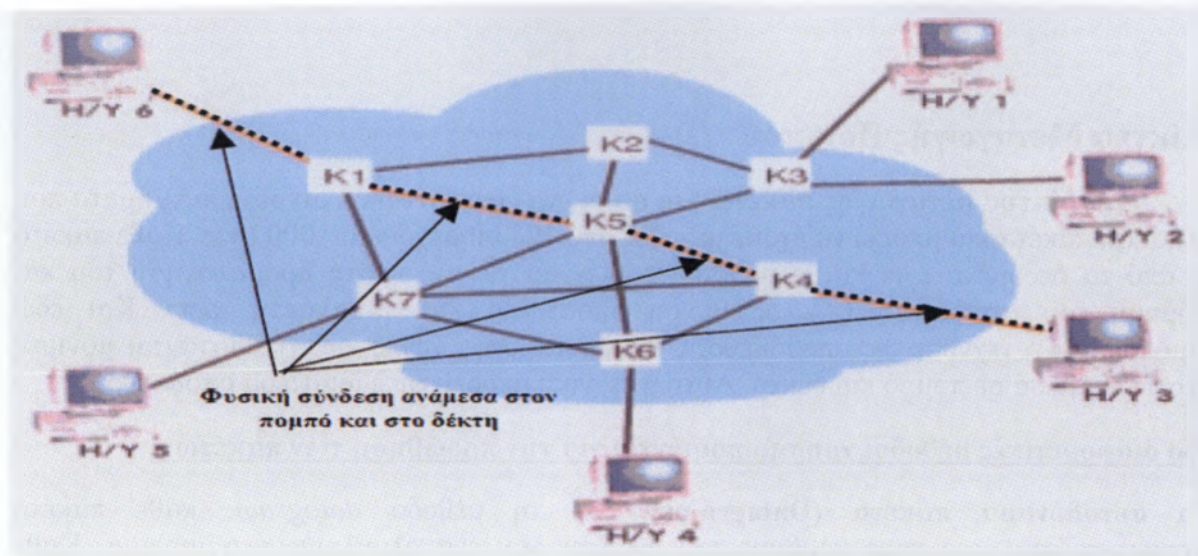
Οι τρεις τεχνικές που χρησιμοποιούνται για τη μετάδοση δεδομένων στα δίκτυα μεταγωγής είναι οι εξής:

- Μεταγωγή κυκλώματος (*Circuit switching*)
- Μεταγωγή μηνύματος (*Message switching*)
- Μεταγωγή πακέτων (*Packet switching*)

### 4.1 Δίκτυα Μεταγωγής Κυκλώματος

Στα *Δίκτυα Μεταγωγής Κυκλώματος (Circuit Switching Networks)*, η μετάδοση των πακέτων είναι εφικτή μόνο μετά την εγκατάσταση μιας φυσικής ζεύξης κυκλώματος μεταξύ δύο κόμβων. Αυτή η εγκατάσταση πραγματοποιείται όπως ακριβώς και στο τηλεφωνικό σύστημα. Όταν ένας υπολογιστής ζητά να επικοινωνήσει με κάποιο άλλο, η κλήση αυτή προωθείται τμηματικά από κόμβο σε κόμβο μέχρι να φτάσει στο δέκτη. Αν ο δέκτης θέλει να επικοινωνήσει με τον πομπό, απαντά θετικά στην πρόσκληση, οπότε και δημιουργείται μια αποκλειστική φυσική ζεύξη ανάμεσα στους δύο υπολογιστές για όλη τη διάρκεια της επικοινωνίας τους.

Η μετάδοση των δεδομένων από τον πομπό προς τον δέκτη είναι διαφανής (*transparent*), υπό την έννοια ότι τα δεδομένα δεν υποβάλλονται σε καμιά επεξεργασία κατά τη διέλευσή τους από το δίκτυο. Όσον αφορά τη ζεύξη που δημιουργείται ανάμεσα στο δέκτη και στον πομπό, αυτή παραμένει ενεργή για όλο το χρονικό διάστημα επικοινωνίας των κόμβων, ακόμη και αν αυτοί σε κάποιες χρονικές στιγμές, δεν ανταλλάσσουν δεδομένα. Αυτή η φυσική σύνδεση ανάμεσα στους δύο σταθμούς καταργείται μετά το τέλος της επικοινωνίας, και μετά από αίτηση που υποβάλλει ο ένας από τους δύο σταθμούς. Παράδειγμα δικτύου μεταγωγής κυκλώματος, παρουσιάζεται στο επόμενο σχήμα:



## Δίκτυο Μεταγωγής Κυκλώματος

Οι κυριότερες φάσεις της επικοινωνίας στα δίκτυα μεταγωγής κυκλώματος είναι:

- **Αποκατάσταση κυκλώματος:** Πριν μεταδοθεί οποιοδήποτε σήμα πρέπει να αποκατασταθεί ένα κύκλωμα από άκρο σε άκρο (από σταθμό σε σταθμό).
- **Μεταφορά δεδομένων:** Σε αυτή τη φάση μεταδίδεται η πληροφορία ανάμεσα στους σταθμούς. Γενικά, η σύνδεση είναι αμφίδρομη .
- **Αποσύνδεση κυκλώματος:** Έπειτα από κάποια περίοδο μεταφοράς δεδομένων η σύνδεση τερματίζεται με πρωτοβουλία ενός από τους 2 σταθμούς. Ελευθερώνονται οι αποκλειστικοί πόροι που χρησιμοποιούνταν.

Η μεταγωγή κυκλώματος είναι ιδανική μέθοδος για μετάδοση συνεχών σημάτων μεγάλης διάρκειας, π.χ. για μετάδοση φωνής (τηλεφωνικό δίκτυο) και εικόνας. Αυτό οφείλεται στο γεγονός ότι στην περίπτωση αυτή δεν απαιτείται καμιά επεξεργασία των σημάτων από τη στιγμή που εγκαθίσταται το κύκλωμα (φυσικό κανάλι). Τέτοιες επεξεργασίες καθυστερούν τη μετάδοση, πράγμα που δεν είναι επιθυμητό για μεγάλα και συνεχή μηνύματα. Η μεταγωγή κυκλώματος δεν είναι αποδοτική για μετάδοση μηνυμάτων μικρής διάρκειας και σποραδικής φύσεως. Στην περίπτωση αυτή, ο χρόνος που απαιτείται για να συνδεθούν οι χρήστες για κάθε σύντομη μετάδοση θα ήταν σημαντική επιβάρυνση, ενώ η διατήρηση της σύνδεσης μεταξύ διαδοχικών μεταδόσεων θα σήμαινε σπατάλη ενός μεγάλου ποσοστού της χωρητικότητας της γραμμής.

## 4.2 Δίκτυα Μεταγωγής Μηνύματος

Στα δίκτυα μεταγωγής μηνύματος η πληροφορία οργανώνεται σε ένα μήνυμα με τη διεύθυνση του παραλήπτη και περνώντας από ενδιάμεσους κόμβους μέσα στο δίκτυο, ακολουθώντας τη βέλτιστη διαδρομή ανάλογα με τις συνθήκες φόρτου, χρόνου και απόστασης, καταλήγει στον προορισμό της. Κάθε ενδιάμεσος κόμβος χρησιμοποιεί την τεχνική της αποθήκευσης και προώθησης. Έτσι η πληροφορία φτάνει στον παραλήπτη ακόμα κι αν αυτός δεν είναι άμεσα διαθέσιμος.

### 4.3 Δίκτυα Μεταγωγής Πακέτου

Στα δίκτυα μεταγωγής πακέτων τα δεδομένα χωρίζονται σε μικρότερα τμήματα που ονομάζονται πακέτα και μπορεί να έχουν μέγεθος από 128 bit μέχρι και 1000 byte. Κάθε πακέτο εκτός από τα δεδομένα έχει και πληροφορίες ελέγχου για τη σωστή δρομολόγησή του και ταξινόμησή του στο δέκτη (π.χ διεύθυνση αποστολέα και παραλήπτη κλπ). Και εδώ χρησιμοποιείται η τεχνική της αποθήκευσης και προώθησης, χωρίς να εγκαθίστανται μόνιμες συνδέσεις ανάμεσα σε πομπό και δέκτη. Αυτή η τεχνική αποδείχτηκε ιδιαίτερα αποδοτική.

#### Δύο διαφορετικές μέθοδοι χρησιμοποιούνται για την προώθηση των πακέτων:

1. Τα **αυτοδύναμα πακέτα (Datagrams)**: Με τη μέθοδο *datagram*, κάθε πακέτο αντιμετωπίζεται από τους κόμβους του δικτύου σαν ένα ολοκληρωμένο μήνυμα. Κάθε κόμβος που παραλαμβάνει το πακέτο επιλέγει ποιος θα είναι ο επόμενος έτσι ώστε το δίκτυο να λειτουργεί με τον καλύτερο δυνατό τρόπο. Για τον λόγο αυτόν οι κόμβοι οφείλουν να διαθέτουν αρκετές πληροφορίες για τη δομή και την κατάσταση του δικτύου κάθε χρονική στιγμή. Τα πακέτα πληροφορίας ενώ έχουν τον ίδιο προορισμό δεν ακολουθούν όλα τον ίδιο δρόμο γι' αυτό υπάρχει πιθανότητα να φτάσουν με διαφορετική σειρά από αυτήν που στάλθηκαν. Έτσι, θα πρέπει να υπάρχει κατάλληλη διάταξη που να τα τοποθετεί στην αρχική τους σειρά. Τυπικό παράδειγμα αυτή της λειτουργίας είναι το Διαδίκτυο.

**Πλεονέκτημα** της μεθόδου είναι η καλύτερη αξιοποίηση των φυσικών κυκλωμάτων του δικτύου και η αυξημένη αξιοπιστία, λόγω ύπαρξης εναλλακτικών δρόμων σε περίπτωση βλάβης (π.χ. καταστροφής ενός κόμβου). Επίσης, επειδή για τη μετάδοση των πακέτων δεν απαιτείται διαδικασία κλήσης, αν κάποιος σταθμός θέλει να μεταδώσει λίγα μόνο πακέτα, αυτά θα παραδοθούν συντομότερα στον προορισμό τους. Έτσι, η μεταγωγή πακέτων με τη μέθοδο αυτοδύναμων πακέτων είναι ιδανική για μεταδόσεις μικρής διάρκειας λίγων πακέτων.

**Μειονέκτημα** είναι, ότι είναι πιθανόν τα πακέτα να πρέπει να αναδιαταχθούν, γιατί μπορεί να φθάνουν στον κόμβο του παραλήπτη με διαφορετική σειρά από αυτή με την οποία στάλθηκαν.

2. Τα **εικονικά κυκλώματα (Virtual Circuit)**: Στη μέθοδο εικονικού κυκλώματος (*virtual circuit*), πριν αρχίσει η αποστολή των πακέτων αποκαθίσταται μία σταθερή νοητή σύνδεση μεταξύ των δύο συνδρομητών από όπου στη συνέχεια θα περάσουν όλα τα πακέτα του μηνύματος. Δηλαδή ο δρόμος που θα ακολουθήσουν τα πακέτα καθορίζεται μια φορά στην αρχή και παραμένει ο ίδιος μέχρι να διακοπεί η επικοινωνία των δύο συνδρομητών. Η εξασφάλιση της ύπαρξης ελεύθερου δρόμου γίνεται με την ανταλλαγή μηνυμάτων μεταξύ των δύο συνδρομητών που πρόκειται να επικοινωνήσουν. Στην τεχνική αυτή, οι ενδιάμεσοι κόμβοι δεν απαιτείται να έχουν πληροφορίες για την κατάσταση του δικτύου, γιατί δεν αποφασίζουν για τη δρομολόγηση των μηνυμάτων αλλά απλά τα διακινούν στον προορισμό τους.

**Πλεονέκτημα** της μεθόδου αυτής έναντι της μεθόδου του αυτοδύναμου πακέτου είναι η ταξινομημένη παραλαβή των πακέτων, κάτι που συνεπάγεται την εύκολη, χωρίς ελέγχους και καθυστερήσεις μετάδοση και ανασύσταση του μηνύματος. Επίσης, ο κόμβος μεταγωγής δεν χρειάζεται να παίρνει πολύπλοκες αποφάσεις δρομολόγησης για κάθε πακέτο. Οι ιδιότητες αυτές κάνουν τη μεταγωγή πακέτων με εικονικά κυκλώματα ιδανική για γρήγορες μεταδόσεις σχετικά μεγάλης διάρκειας.

**Μειονέκτημα** είναι η μειωμένη αξιοπιστία, αφού, αν χαλάσει κόμβος ή αν υπάρξει συμφόρηση σε κάποιο τμήμα του δικτύου, δεν μπορεί να γίνει εύκολα αναδρομολόγηση.

Από την άλλη πλευρά οι τεχνικές μεταγωγής μηνύματος και πακέτου, πλεονεκτούν λόγω της δυνατότητας απόδοσης προτεραιότητας στα πακέτα δεδομένων, καθώς επίσης και της ανίχνευσης και διόρθωσης σφαλμάτων, η οποία εξασφαλίζεται από το δίκτυο, και όχι από τα υπολογιστικά συστήματα που επικοινωνούν.

## 4.4 Τεχνολογίες Μετάδοσης Φωνής

Οι βασικότερες τεχνολογίες μετάδοσης φωνής είναι: οι **Frame Relay**, **ATM** και **IP**. Και οι τρεις είναι πολύ διαδεδομένες τεχνολογίες. Τα IP και ATM χρησιμοποιούνται κυρίως στη διασύνδεση πολλών δικτύων και στα δίκτυα ευρείας περιοχής (WAN), ενώ το Frame Relay χρησιμοποιείται σε μικρότερα δίκτυα.

### 4.4.1 Τεχνολογία Frame Relay

Το **Frame Relay** παρέχει υπηρεσία μεταγωγής πακέτου με τα παρακάτω χαρακτηριστικά με μεγάλες ταχύτητες προσπέλασης, αυξημένη ρυθμοαπόδοση (throughput) και αξιοπιστία, δυνατότητα διασύνδεσης με το δίκτυο ISDN, δυνατότητα δημιουργίας "*Ιδεατών Ιδιωτικών Δικτύων*" (Virtual Private Networks) με δική τους διαχείριση. Στην τεχνολογία του **Frame Relay** υπάρχει και το χαρακτηριστικό του **CIR** (Committed Information Rate), με βάση το οποίο θα πρέπει να γίνεται και ο έλεγχος της μέγιστης ή ελάχιστης χωρητικότητας της γραμμής που δίνεται στο χρήστη.

Οι μεταγωγείς πακέτων διακρίνονται στους *Κόμβους Πρόσβασης* (Access Nodes) και στους *Κόμβους Μετάβασης* (Transit Nodes). Οι *Κόμβοι Πρόσβασης* έχουν σαν σκοπό την συγκέντρωση των συνδρομητικών γραμμών και την εξυπηρέτηση της τοπικής κίνησης που αυτές δημιουργούν, ενώ οι *Κόμβοι Μετάβασης* έχουν σαν αποστολή να προωθούν την μεταξύ των κόμβων κίνηση και να εξυπηρετούν την πρόσβαση προς άλλα δημόσια δίκτυα μεταγωγής πακέτου. Σε πολλές περιπτώσεις κάποιος κόμβος πρόσβασης βρίσκεται στο ίδιο κέντρο με κόμβο μετάβασης αποτελώντας έτσι έναν πλήρη Μεταγωγέα Πακέτων.

Η τεχνολογία μετάδοσης πλαισίων (**Frame Relay - FR**) χρησιμοποιείται σήμερα ως υπηρεσία μεταφοράς στις μονάδες διασύνδεσης (Internet Working Units - **IWUs**) για την επικοινωνία τοπικών δικτύων υπολογιστών μέσω των δημόσιων δικτύων δεδομένων. Η τεχνολογία Frame Relay βασίζεται σε ένα πρωτόκολλο το οποίο υποστηρίζει πακέτα (πλαίσια) μεταβλητού μεγέθους. Το **Frame Relay** είναι πρωτόκολλο με φάση εγκατάστασης σύνδεσης, δηλαδή τα πλαίσια μεταφέρονται μέσω των μοναδικών νοητών συνδέσεων με τη βοήθεια πεδίου διεύθυνσης που περιλαμβάνεται στην *επικεφαλίδα* (header) του πλαισίου.

Επιπλέον, είναι πρωτόκολλο επιπέδου σύνδεσης δεδομένων (*data link layer*) σύμφωνα με το μοντέλο OSI, αφού προέκυψε από το πρωτόκολλο **HDLC** (High - Level Data Link Control). Τυπικό χαρακτηριστικό του **Frame Relay** είναι το γεγονός ότι η διόρθωση λαθών (*error correction*) υλοποιείται με επαναμετάδοση των λανθασμένων πλαισίων από *άκρο-σε-άκρο*. Στους ενδιάμεσους κόμβους κάθε πλαίσιο προωθείται στον επόμενο κόμβο, ακόμη και καθώς αυτό λαμβάνεται, χωρίς να δαπανάται χρόνος για έλεγχο λαθών. Το γεγονός αυτό έχει ως αποτέλεσμα τη μείωση της καθυστέρησης και της απαίτησης αποθήκευσης στους ενδιάμεσους κόμβους του δικτύου. Όταν ένα πακέτο βρεθεί λανθασμένο στέλνεται καθ'όλο το μήκος της επικοινωνιακής οδού από *άκρο-σε-άκρο*, ενώ η πιθανότητα να συμβεί κάτι τέτοιο είναι μικρή στα δίκτυα όπου τα μέσα μετάδοσης είναι χαμηλού θορύβου.

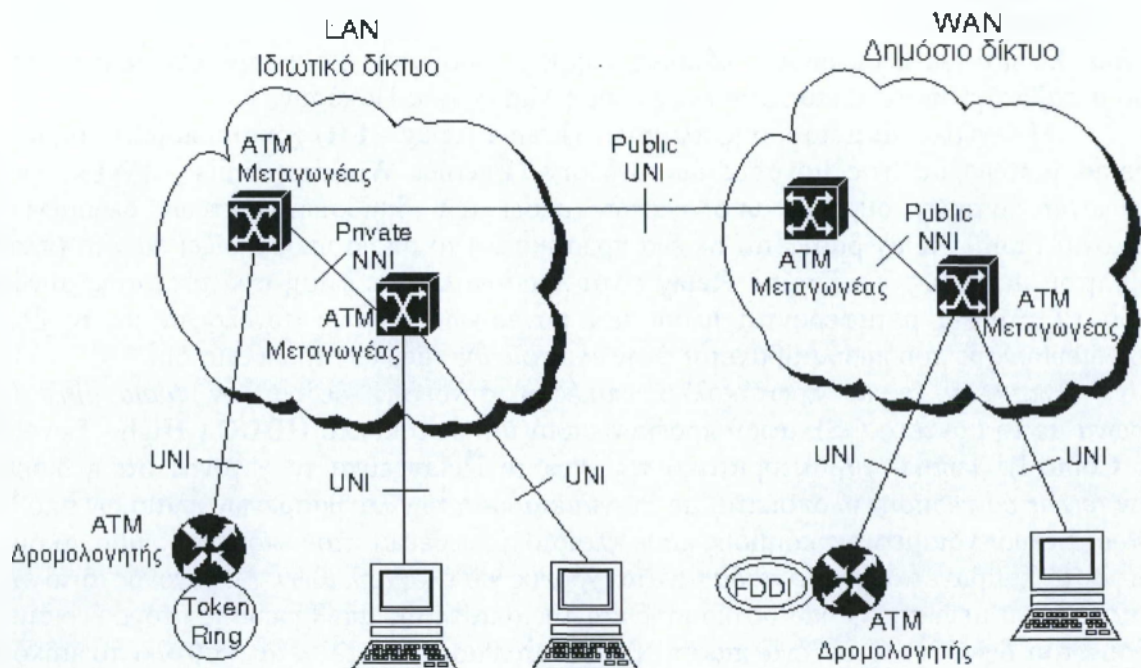
Η ταχύτητα λειτουργίας της υπηρεσίας **Frame Relay** είναι 2,048 Mbps. Η τεχνολογία Frame Relay εισήχθη ως μια πρόταση βελτίωσης και εξέλιξης της κλασικής τεχνολογίας μεταγωγής πακέτων η οποία περιγράφεται από το πρότυπο **X.25**. Η τεχνολογία αυτή προέκυψε για να ικανοποιήσει τις αυξημένες ανάγκες για δικτύωση και διασύνδεση

τοπικών δικτύων με καλή ποιότητα υπηρεσιών, χωρίς καθυστερήσεις και όσο το δυνατόν μεγαλύτερη αξιοπιστία.

#### 4.4.2 Τεχνολογία ATM

Το ATM (Asynchronous Transfer Mode) είναι μια δικτυακή τεχνολογία μετάδοσης που υποστηρίζει την μεταφορά ετερογενούς κίνησης πραγματικού χρόνου, όπως ήχου και εικόνας και μη πραγματικού χρόνου, όπως υπολογιστικών δεδομένων, με τη βοήθεια ενός μηχανισμού που διαβιβάζει μονάδες δεδομένων σταθερού μεγέθους, γνωστές ως κελιά (*cells*). Ο τρόπος μεταφοράς (*Transfer Mode*) δηλώνει ότι αυτή η τεχνολογία αφορά συγκεκριμένο τρόπο μεταφοράς και μεταγωγής στο δίκτυο. Ο όρος «ασύγχρονο» (*asynchronous*) αναφέρεται στο γεγονός ότι τα πακέτα μεταφέρονται χρησιμοποιώντας ασύγχρονες τεχνικές και τα δύο τερματικά σημεία δε χρειάζεται να έχουν συγχρονισμένα ρολόγια.

Το ATM είναι μια περίπλοκη τεχνολογία, ίσως και την περιπλοκότερη στη βιομηχανία δικτύων μέχρι τώρα. Σύμφωνα με τον επίσημο ορισμό της ITU το ATM είναι μια τεχνική πολυπλεξίας, στην οποία η ικανότητα μετάδοσης οργανώνεται με μη αφιερωμένες σχισμές (*undedicated slots*), οι οποίες γεμίζουν με κελιά (*cells*), ανάλογα με τις στιγμιαίες πραγματικές ανάγκες της κάθε εφαρμογής. Η τεχνολογία ATM είναι συνδεσμική (*connection-oriented*). Αυτό σημαίνει ότι πριν αρχίσει η μετάδοση πληροφοριών, πρέπει να επιτευχθεί η σύνδεση μεταξύ των δύο σημείων του δικτύου. Η σύνδεση μεταξύ δύο σημείων στο δίκτυο προς το παρόν είναι μόνιμη νοητή (**Permanent Virtual Circuit - PVC**). Στο παρακάτω σχήμα φαίνεται ένα τυπικό παράδειγμα δικτύου ATM.

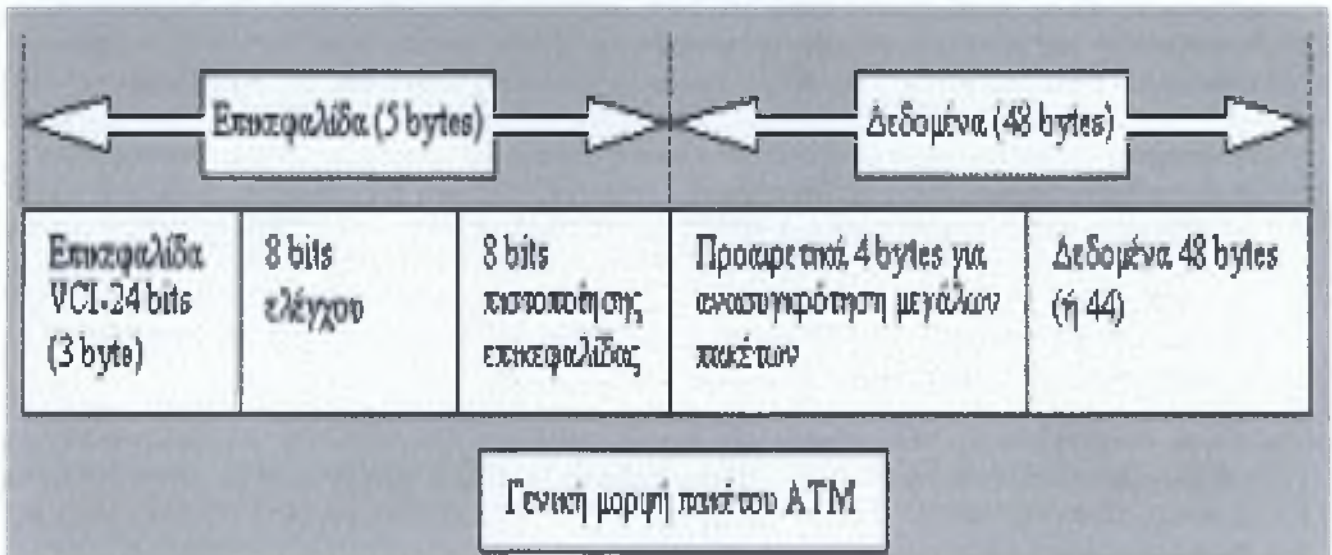


Δίκτυο ATM



#### 4.4.2.1 Η Δομή του ATM cell

Το ATM δίκτυο χρησιμοποιεί πακέτα (κελί) σταθερού μεγέθους ίσο με 53 bytes, από τα οποία επικεφαλίδα (header) είναι 5 bytes και το φορτίο (payload) είναι 48 bytes. Το μέγεθος των πακέτων ATM αποτελεί συμβιβασμό μεταξύ των απαιτήσεων που επιβάλλονται από τη μεταφορά δεδομένων και φωνής. Ο βασικός ρόλος της επικεφαλίδας είναι η ταυτοποίηση των κυττάρων που ανήκουν στο ίδιο κανάλι. Μικρού μεγέθους πακέτα είναι προτιμητέα για φωνή, ενώ μεγάλου μεγέθους πακέτα είναι προτιμητέα για δεδομένα διότι η απόδοση του δικτύου δεδομένων αυξάνει για μεγάλα μεταφερόμενα φορτία (payloads).



Το ATM, όπως και άλλες τεχνολογίες μεταγωγής πακέτων (π.χ. X.25, Frame Relay), δρομολογεί τα πακέτα μέσω της διεύθυνσης που αυτά διαθέτουν. Το ATM είναι μια τεχνολογία προσανατολισμένη σε σύνδεση, στην οποία μια λογική σύνδεση εγκαθίσταται μεταξύ δύο τερματικών σημείων πριν την έναρξη της διαδικασίας ανταλλαγής δεδομένων. Το ATM βασίζεται σε πρωτόκολλα εικονικής σύνδεσης (virtual paths, virtual circuits).

- Ένα **Virtual Channel** (Εικονικό Κανάλι) σηματοδοτεί την μεταφορά κελιών ATM τα οποία έχουν το ίδιο μοναδικό αναγνωριστικό, το οποίο και αποκαλείται **Virtual Channel Identifier (VCI)**. Το αναγνωριστικό κωδικοποιείται στην επικεφαλίδα του κελιού. Το εικονικό κανάλι αναπαριστά το βασικό μέσο επικοινωνίας μεταξύ δύο τερματικών σημείων και είναι ανάλογο σε ένα εικονικό κύκλωμα πρωτόκολλου X.25.
- Ένα **Virtual Path** (Εικονικό Μονοπάτι) σηματοδοτεί την μεταφορά των ATM κελιών τα οποία ανήκουν σε εικονικά κανάλια και μοιράζονται ένα κοινό αναγνωριστικό, το οποίο λέγεται **Virtual Path Identifier (VPI)**. Το VPI, όπως και το VCI, κωδικοποιείται στην επικεφαλίδα του κελιού. Ένα εικονικό μονοπάτι με άλλα λόγια είναι μια ομάδα εικονικών καναλιών τα οποία συνδέονται στα ίδια τερματικά. Αυτή η διεπίπεδη προσέγγιση έχει ως αποτέλεσμα την βελτιωμένη απόδοση του δικτύου. Αφού εγκατασταθεί ένα εικονικό μονοπάτι, η πρόσθεση/αφαίρεση εικονικών καναλιών είναι άμεση.

Ένα ATM δίκτυο αποτελείται από ένα σύνολο ATM μεταγωγέων διασυνδεδεμένοι με point-to-point ATM συνδέσμους ή διεπαφές. Οι μεταγωγείς των ATM υποστηρίζουν δύο ειδών διεπαφές: τη User-to-Network Interface (UNI) και τη Network-to-Network Interface

(NNI). Η πρώτη είναι η διεπαφή (*interface*) μεταξύ κάθε τερματικού συστήματος ATM (*ATM end system*) και του ATM δικτύου. Στην πράξη πρόκειται για το *interface* μεταξύ κάθε μηχανήματος (σταθμού εργασίας, *server* ή δρομολογητή), που έχει ATM κάρτα δικτύου και του ATM στοιχείου μεταγωγής στο οποίο είναι συνδεδεμένο. Η δεύτερη είναι η διεπαφή (*interface*) μεταξύ των στοιχείων μεταγωγής ATM (*ATM switches*). Είναι κάθε φυσικός ή λογικός σύνδεσμος με τον οποίο δύο ATM μεταγωγείς ανταλλάσσουν το πρωτόκολλο NNI.

Η τεχνολογία ATM συνδυάζει τα προτερήματα της μεταγωγής κυκλώματος (*circuit switching*), τα οποία είναι: *δεδομένη χωρητικότητα μιας σύνδεσης* και *σταθερή καθυστέρηση μεταφοράς*, με τα προτερήματα της μεταγωγής πακέτου (*packet switching*), τα οποία είναι: η *ελαστικότητα* και η *αποδοτικότητα* αναφορικά με κίνηση μεταβλητού ρυθμού. Ένα από τα κυριότερα χαρακτηριστικά του ATM τρόπου μεταφοράς είναι ότι το ATM είναι η πιο δημοφιλής τεχνολογία μεταγωγής στα WAN δίκτυα σκελετού (*backbone*). Επίσης, είναι συνδεσμικό (*connection-oriented*), δηλαδή επιτυγχάνεται εγκατάσταση νοητής σύνδεσης πριν την προώθηση των κελιών. Επιπλέον, γίνεται δυναμική ανάθεση εύρους ζώνης, ανάλογα με τις τρέχουσες απαιτήσεις κάθε εφαρμογής και η μεταγωγή κελιών (*cell switching*) είναι ταχεία βασισμένη σε ετικέτες. Τέλος, παρέχει διάφορα επίπεδα ποιότητας υπηρεσιών (*Quality of Service*). Έτσι, ένα δίκτυο ATM προσφέρει την αναγκαία υποδομή για την παροχή ολοκληρωμένων τηλεπικοινωνιακών υπηρεσιών μειωμένου κόστους, υψηλής ποιότητας και την προοπτική γρήγορης εξάπλωσης των δικτύων ευρείας ζώνης.

Επιπλέον, το ATM μπορεί και παρέχει ασφάλεια στις συνδέσεις ακριβώς επειδή το «κύκλωμα» που εγκαθίσταται με μία σύνδεση είναι εικονικό (*virtual circuit*) και αποσυντίθεται αμέσως μετά το τέλος της σύνδεσης. Αυτό συνδυαζόμενο με το γεγονός της μη προκαθορισμένης διαδρομής των πακέτων καθιστά σχεδόν αδύνατη την πλήρη παρακολούθηση μίας σύνδεσης ATM.

#### 4.4.2.2 Αρχιτεκτονική Πρωτοκόλλων ATM

Η αρχιτεκτονική πρωτοκόλλων του δικτύου ATM εμφανίζεται στο σχήμα. Τα τρία κατώτερα επίπεδα στην αρχιτεκτονική αυτή είναι το *φυσικό επίπεδο*, το *επίπεδο ATM* και το *ATM adaptation layer* (Επίπεδο Προσαρμογής του ATM, **AAL**). Πιο αναλυτικά για τα επίπεδα: το *φυσικό επίπεδο* περιλαμβάνει δύο υποεπίπεδα: το υποεπίπεδο φυσικού μέσου (*physical medium sublayer*) και το υποεπίπεδο σύγκλισης μετάδοσης (*transmission convergence sublayer*). Το πρώτο υποεπίπεδο εκτελεί λειτουργίες εξαρτώμενες από το φυσικό μέσο, όπως η παροχή χρονισμού σε σχέση με το ψηφιακό κανάλι και η υιοθέτηση κατάλληλης τεχνικής κωδικοποίησης γραμμής. Το δεύτερο χειρίζεται τη μεταφορά των ATM κελιών στο υποκείμενο επίπεδο της ροής bits.

Η κύρια λειτουργία του επιπέδου ATM είναι η παροχή εικονικών συνδέσεων μεταξύ δύο ή περισσότερων κόμβων του δικτύου ή μεταξύ ενός κόμβου του δικτύου και ενός τερματικού συστήματος. Οι γενικότερες λειτουργίες του αφορούν τη μετάδοση, μετατροπή και λήψη κελιών, την πολυπλεξία και αποπολυπλεξία των κελιών, όπου τα κελιά που ανήκουν σε διαφορετικά εικονικά κανάλια ή μονοπάτια πολυπλέκονται στο ίδιο «ρεύμα» από κελιά (*cell stream*) στην πλευρά του αποστολέα και αποπολυπλέκονται από το ίδιο ρεύμα από κελιά στην πλευρά του παραλήπτη. Άλλες λειτουργίες είναι ο έλεγχος συμφόρησης και διαχείριση των καταχωρητών, η παραγωγή και αφαίρεση κεφαλίδων των κελιών στην πηγή και τον προορισμό αντίστοιχα και η διαδοχική παράδοση.

Σύνηθες πρωτόκολλο του επιπέδου AAL είναι το AAL-5. Το AAL-5 εισάγει μεταβλητού μεγέθους πακέτα από τα πρωτόκολλα του ανώτερου επιπέδου και τα τεμαχίζει σε σταθερού Layer (AAL) χρησιμοποιείται ως διεπαφή μεταξύ του επιπέδου ATM με τα ανώτερα μεγέθους μονάδες των 48 bytes. Αντίστοιχα δέχεται σταθερού μεγέθους κελιά από το δίκτυο και επανασυναρμολογεί αυτά, στα αρχικά τους πακέτα. Το ATM adaptation layer είναι αυτό που παρέχει τη δυνατότητα χρήσης διαφορετικών κλάσεων υπηρεσιών. Το AAL χωρίζεται σε δύο υποεπίπεδα: *το υποεπίπεδο κατάτμησης και επανασυναρμολόγησης (Segmentation And Reassembly Sublayer, SAR)* και *το υποεπίπεδο σύγκλισης (Convergence Sublayer, CS)*. Το υποεπίπεδο SAR στην πλευρά του αποστολέα εκτελεί την κατάτμηση της πληροφορίας του χρήστη, που φθάνει με μεταβλητού μήκους πλαίσια, σε ένα σύνολο σταθερού μεγέθους ATM cell payloads προκειμένου να μεταφερθούν μέσω του ATM δικτύου. Στην πλευρά του παραλήπτη το SAR επανασυνθέτει τα μεταβλητού μεγέθους πλαίσια με τα δεδομένα του χρήστη από τα κελιά. Το Convergence Sublayer αντιστοιχεί τις απαιτήσεις του χρήστη στο ATM δίκτυο.

#### **4.4.3 Τεχνολογία Voice over Internet Protocol (VoIP)**

Την οποία έχουμε αναλύσει στο προηγούμενο κεφάλαιο.

### ΠΡΩΤΟΚΟΛΛΑ ΣΗΜΑΤΟΔΟΣΙΑΣ ΤΗΛΕΦΩΝΙΑΣ IP

Το μεγαλύτερο μέρος της πολυπλοκότητας της τηλεφωνίας IP οφείλεται στην εγκατάσταση κλήσεων (*call setup*) και τη διαχείριση κλήσεων (*call management*). Στη τηλεφωνική ορολογία, η διαδικασία εγκατάστασης και τερματισμού μιας κλήσης είναι γνωστή ως σηματοδότηση (*signaling*). Η σηματοδότηση περιλαμβάνει την αντιστοίχιση ενός τηλεφωνικού αριθμού σε μια τοποθεσία, την εύρεση μιας διαδρομής προς τον καλούμενο και τη διαχείριση διαφόρων άλλων λεπτομερειών όπως η προώθηση κλήσεων. Ο μηχανισμός που χρησιμοποιείται στο παραδοσιακό τηλεφωνικό σύστημα για τη διαχείριση κλήσεων ονομάζεται *Σύστημα Σηματοδότησης 7 (Signaling System 7, SS7)*. Ένα από τα βασικά ερωτήματα στην τηλεφωνία IP εστιάζεται στην προσέγγιση που πρέπει να ακολουθείται σχετικά με την σηματοδότηση – θα πρέπει το σύστημα σηματοδότησης να είναι κεντρικό, όπως αυτό του τρέχοντος τηλεφωνικού συστήματος, ή κατανεμημένο όπως η τρέχουσα αντιστοίχιση των ονομάτων περιοχών (*domain names*) σε διευθύνσεις IP;

Οι υπέρμαχοι της κατανεμημένης προσέγγισης υποστηρίζουν ότι δύο τηλέφωνα IP που βρίσκονται σε τυχαίες περιοχές του Internet θα πρέπει να βρίσκουν το ένα το άλλο και να επικοινωνούν όπως οι άλλες διαδικτυακές εφαρμογές (δηλαδή, ένα τηλέφωνο IP θα λειτουργεί ως διακομιστής για τη λήψη εισερχόμενων κλήσεων και ως πελάτης για την πραγματοποίηση εξερχόμενων κλήσεων). Επίσης, σε μια κατανεμημένη προσέγγιση δε χρειάζεται επιπλέον υποδομή εκτός του DNS και των υπηρεσιών προώθησης του IP που αυτή τη στιγμή είναι διαθέσιμες για την επικοινωνία δεδομένων. Η κατανεμημένη προσέγγιση είναι ιδιαίτερα κατάλληλη για τοπικά συστήματα τηλεφωνίας IP (π.χ για ένα σύστημα που επιτρέπει κλήσεις μεταξύ δύο τηλεφώνων IP στην ίδια εταιρεία).

Οι υπέρμαχοι της κεντρικής ιδέας προσέγγισης υποστηρίζουν ότι ένα συμβατικό τηλεφωνικό μοντέλο λειτουργεί καλύτερα επειδή, όταν οι τηλεφωνικές εταιρείες έχουν τον κεντρικό έλεγχο της εγκατάστασης κλήσεων μπορούν να παρέχουν εγγυήσεις για την ποιότητα των υπηρεσιών τους.

Καθώς, η διαμάχη για τη βασική προσέγγιση βρισκόταν σε εξέλιξη, προτάθηκαν τα εξής σύνολα πρωτοκόλλων σηματοδότησης για τη χρήση στην τηλεφωνία IP:

1. **SIP (Session Initiation Protocol)** (Πρωτόκολλο Εκκίνησης Συνόδου)
2. **H.323**
3. **MGCP (Media Gateway Control Protocol)** (Πρωτόκολλο Ελέγχου Πύλης Μέσων)
4. **Megaco (Media Gateway Control)**

## Αναλυτικά παρουσιάζεται το καθένα παρακάτω:

### 5.1 SIP (Session Initiation Protocol)

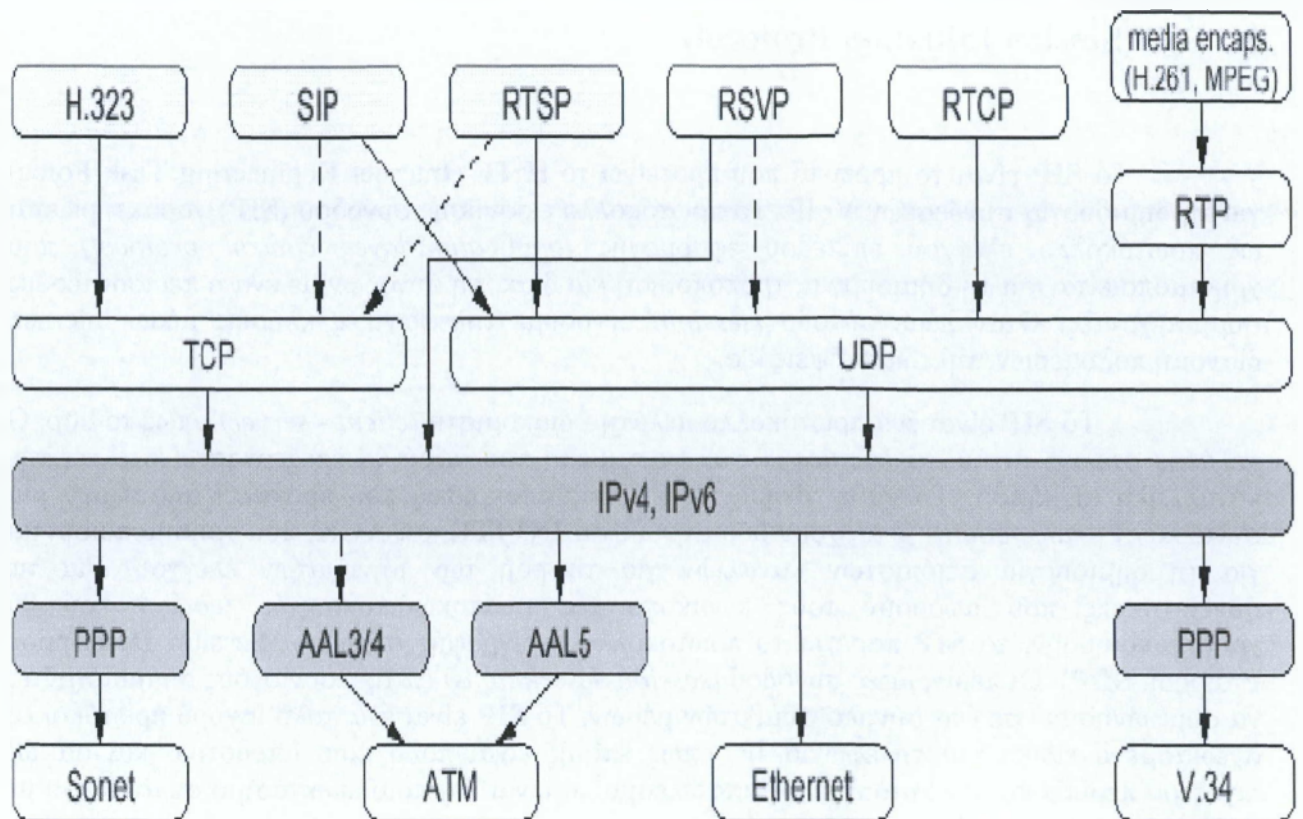
Το **SIP** είναι το πρότυπο που προτείνει το **IETF** (Internet Engineering Task Force) για τη δημιουργία συνδέσεων VoIP. Το πρωτόκολλο εκκίνησης συνόδου (**SIP**) χαρακτηρίζεται ως πρωτόκολλο ελέγχου επιπέδου εφαρμογής (*application-layer control protocol*) που χρησιμοποιείται για τη δημιουργία, τροποποίηση και διακοπή συνόδων με ένα ή περισσότερους συμμετέχοντες. Όταν λέμε σύνοδο (*session*) εννοούμε τηλεφωνικές κλήσεις μέσω internet, διανομή πολυμέσων, τηλεδιασκέψεις κ.α.

Το **SIP** είναι ένα πρωτόκολλο πελάτη - διακομιστή (*client - server*) όπως το http. Ο πελάτης στέλνει αιτήματα (*requests*) στο διακομιστή που αφού τα επεξεργαστεί στέλνει την κατάλληλη απόκριση. Το κάθε αίτημα μαζί με τις αποκρίσεις που προκαλεί αποτελούν μια συναλλαγή (*transaction*). Υπάρχουν δύο μηνύματα, **INVITE** και **ACK**, που χρησιμοποιούνται για τη δημιουργία αξιόπιστων καναλιών για τη ροή των μηνυμάτων έλεγχου. Για τις συνεννοήσεις που αφορούν τους κωδικοποιητές - αποκωδικοποιητές (*codec*) που θα χρησιμοποιηθούν, το **SIP** παρέχει το πρωτόκολλο περιγραφής συνόδου (**Session Description Protocol, SDP**). Οι περιγραφές συνόδου (*session descriptions*) επιτρέπουν στους συμμετέχοντες να συμφωνήσουν σε ένα σύνολο συμβατών μέσων. Το **SIP** είναι ένα πολύ ισχυρό πρωτόκολλο σχεδιασμένο ειδικά για τηλεφωνία IP, όπως επίσης είναι πολύ ποιο αποδοτικό και σαφώς λιγότερο περίπλοκο και αυτό έχει ως αποτέλεσμα να είναι και ποιο επεκτάσιμο σε αντίθεση με το **H.323** που θα αναλύσουμε στη συνέχεια.

Οι υπηρεσίες που παρέχει το **SIP** είναι:

- *Τοποθεσία χρήστη (User Location)*: προσδιορισμός του τέλους του συστήματος που χρησιμοποιείται για επικοινωνία.
- *Δημιουργία κλήσης (Call Setup)*: «κουδούνισμα» και εγκατάσταση των παραμέτρων κλήσης και στις δύο πλευρές, τόσο από τη μεριά του καλούντος όσο και από τη μεριά του καλούμενου.
- *Διαθεσιμότητα χρήστη (User Availability)*: καθορισμός της προθυμίας αυτού που καλεί να ασχοληθεί με την επικοινωνία.
- *Ικανότητες χρήστη (User Capabilities)*: καθορισμός του μέσου και των παραμέτρων του για να χρησιμοποιηθεί.
- *Χειρισμός κλήσης (Call handling)*: η μεταφορά και ο τερματισμός της κλήσης.

Το SIP βασίζεται στην υποστήριξη και άλλων πρωτοκόλλων από το τερματικό - πομπό.

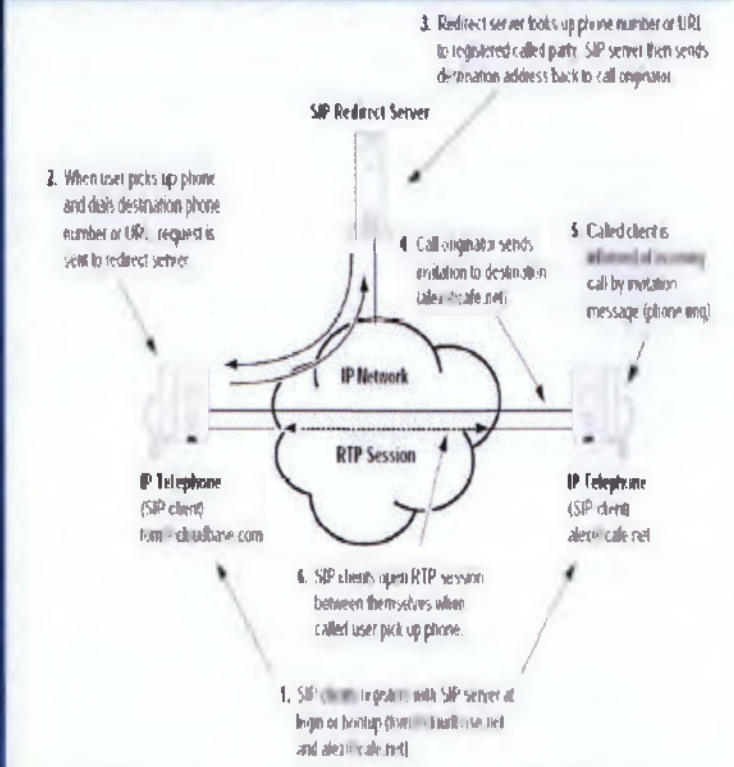
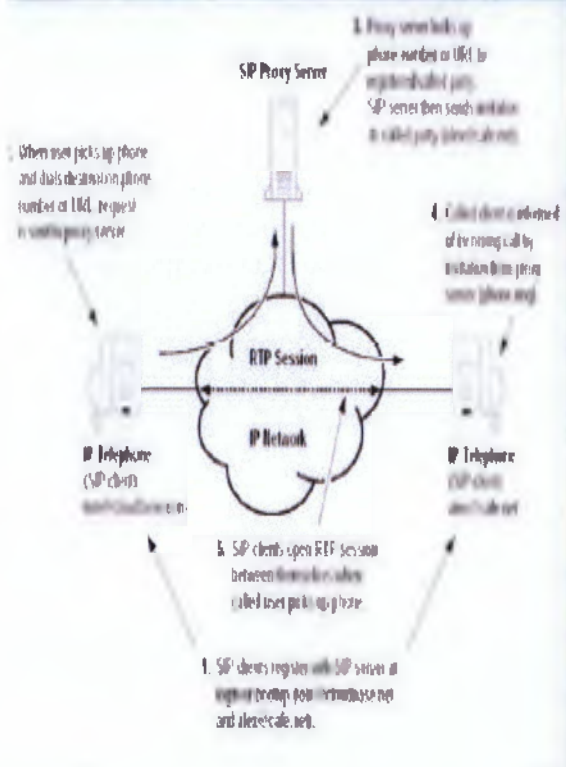


## ΟΡΙΣΜΟΙ

- **Πελάτης (Client):** Μια εφαρμογή που στέλνει αιτήματα SIP. Μπορεί να αλληλεπιδρά ή όχι με κάποιο χρήστη.
- **Διακομιστής (Server):** Μια εφαρμογή που λαμβάνει αιτήματα με σκοπό να τα εξυπηρετήσει και να στείλει πίσω τις κατάλληλες αποκρίσεις.
- **Κλήση:** Αποτελείται από όλους τους συμμετέχοντες σε μια διάσκεψη (conference) που έχουν κληθεί από την ίδια πηγή. Κάθε κλήση SIP αναγνωρίζεται από ένα μοναδικό call-id. Αυτό σημαίνει ότι αν ένας χρήστης κληθεί σε μια διάσκεψη από αρκετά άτομα, κάθε μια πρόσκληση θα έχει ξεχωριστό call-id.
- **Σκέλος κλήσης:** Αναγνωρίζεται από το συνδυασμό του call-id και των addr-spec, tag που βρίσκονται στα πεδία To και From της επικεφαλίδας. Για το ίδιο call-id, τα μηνύματα από το A στο B ανήκουν στο ίδιο σκέλος όπως και τα μηνύματα με την αντίθετη φορά.

- **Σύνοδος (Session):** Όπως περιγράφεται στην προδιαγραφή του SDP: «Μια σύνοδος πολυμέσων αποτελείται από ένα σύνολο πομπών και δεκτών πολυμέσων και των ροών πακέτων (streams) που δημιουργούν». Όπως έχει αναφερθεί μπορεί το ίδιο άτομο να κληθεί πολλές φορές, μέσω διαφορετικών κλήσεων, στην ίδια σύνοδο. Αν χρησιμοποιείται το SDP τότε η σύνοδος ορίζεται από την αλληλουχία των εξής στοιχείων : user name, session id, τύπος δικτύου, τύπος διεύθυνσης και στοιχεία διεύθυνσης στο πεδίο προέλευσης.
- **(SIP) Συναλλαγή:** Μια συναλλαγή SIP λαμβάνει χώρα μεταξύ ενός πελάτη και ενός διακομιστή και αποτελείται από όλα τα μηνύματα, από το πρώτο αίτημα που στέλνει ο πελάτης ως την απόκριση του διακομιστή. Αναγνωρίζεται από τον αριθμό ακολουθίας CSeq.

# SIP:Session Initiation Protocol



## 5.1.1 Οι οντότητες του SIP

Οι οντότητες που συνθέτουν μια SIP αρχιτεκτονική είναι οι πράκτορες χρήστη (*User Agents*) και οι εξυπηρετητές (*Servers*). Υπάρχουν 4 ειδών servers, αυτοί είναι: *location server*, *proxy server*, *redirect server* και *registrat server*, τα οποία αναλύονται παρακάτω.

**Πράκτορας Χρήστη (user agent):** Τα έγγραφα του SIP αναφέρονται σε μια συσκευή που δημιουργεί ή τερματίζει τηλεφωνικές κλήσεις με το όνομα *πράκτορας χρήστη*. Ένας πράκτορας χρήστη του SIP μπορεί να υλοποιηθεί σε ένα τηλέφωνο SIP, σε ένα φορητό υπολογιστή, ή σε

μία πύλη δικτύου PSTN η οποία επιτρέπει σε ένα τηλέφωνο SIP να πραγματοποιεί κλήσεις στο PSTN. Ο πράκτορας χρήστη αποτελείται από δύο μέρη: έναν *πελάτη πράκτορα χρήστη (user agent client)*, ο οποίος πραγματοποιεί εξερχόμενες κλήσεις και έναν *διακομιστή πράκτορα χρήστη (user agent server)*, που διαχειρίζεται εισερχόμενες κλήσεις.

**Διακομιστής Θέσης (location server):** Ένας διακομιστής θέσης SIP διαχειρίζεται τη βάση δεδομένων από πληροφορίες σχετικές με τον κάθε χρήστη, όπως ένα σύνολο από διευθύνσεις IP, υπηρεσίες στις οποίες έχει εγγραφεί ο χρήστης και οι προτιμήσεις του. Κατά τη διάρκεια της εγκατάστασης μιας κλήσης, ο διακομιστής θέσης δίνει πληροφορίες σχετικά με τη θέση ή τις θέσεις που θα δεχτούν την κλήση αυτή.

**Διαμεσολαβητής (proxy server):** Το SIP εμπεριέχει την ιδέα ενός διαμεσολαβητή (proxy) ο οποίος μπορεί να προωθεί αιτήσεις από πράκτορες χρήστη σε μια άλλη τοποθεσία. Οι διαμεσολαβητές χειρίζονται τη βέλτιστη δρομολόγηση και επιβάλλουν πολιτικές (για παράδειγμα εξασφαλίζουν ότι ο καλών είναι εξουσιοδοτημένος να κάνει τη κλήση). Ένας Proxy Server μπορεί να μεταφράζει ή ακόμα και να αναδιατυπώνει αν αυτό είναι απαραίτητο ένα αίτημα πριν το προωθήσει.

**Διακομιστής Ανακατεύθυνσης (redirect server):** Το SIP χρησιμοποιεί ένα διακομιστή ανακατεύθυνσης για να χειρίζεται λειτουργίες όπως η προώθηση κλήσεων. Ο διακομιστής ανακατεύθυνσης λαμβάνει αιτήσεις από έναν πράκτορα χρήστη και επιστρέφει στον πράκτορα χρήστη εναλλακτικές τοποθεσίες για επικοινωνία.

**Διακομιστής Καταχώρισης (registrar server):** Το SIP χρησιμοποιεί ένα διακομιστή καταχώρισης για να λαμβάνει αιτήσεις εγγραφής και να ενημερώνει τη βάση δεδομένων που μπορούν να συμβουλευτούν οι διακομιστές θέσης. Ένας διακομιστής καταχώρισης είναι υπεύθυνος για την πιστοποίηση μιας αίτησης εγγραφής και για να εξασφαλίζει ότι η υποκείμενη βάση δεδομένων παραμένει συνεπής.

## 5.1.2 Ασφάλεια SIP

### A. Εμπιστευτικότητα και κρυπτογράφηση (confidentiality & encryption)

Τα μηνύματα SIP μπορεί να περιέχουν ευαίσθητες πληροφορίες. Ακόμα στο σώμα του μηνύματος μπορεί να υπάρχει το κλειδί της κωδικοποίησης της συνόδου. Το SIP υποστηρίζει 2 συμπληρωματικές υπηρεσίες για την προστασία των δεδομένων:

1. **Κρυπτογράφηση για όλη τη διαδρομή (End-to-end encryption):** βασίζεται σε κλειδιά που έχουν οι χρήστες. Κάθε μήνυμα στέλνεται κωδικοποιημένο με το κλειδί του παραλήπτη έτσι ώστε μόνο αυτός να μπορεί να το διαβάσει. Πρέπει σημειωθεί ότι δεν κωδικοποιείται ολόκληρο το μήνυμα. Κάποια πεδία της επικεφαλίδας πρέπει να είναι «ελευθέρα» γιατί τα δεδομένα που περιέχουν είναι απαραίτητα στους ενδιάμεσους διακομιστές. Όλες οι υλοποιήσεις πρέπει να υποστηρίζουν κωδικοποίηση PGP (pretty good privacy).
2. **Κρυπτογράφηση ανά βήμα (Hop-by-hop encryption):** με τη μέθοδο αυτή μπορούμε να κωδικοποιήσουμε ολόκληρο το μήνυμα. Έτσι, κανονικά, δεν αποκαλύπτονται σε hackers οι διευθύνσεις των ατόμων που συνομιλούν. Αλλά αυτό δεν συμβαίνει. Τα δεδομένα αυτά είναι γνωστά στους ενδιάμεσους διακομιστές (για να γίνει η δρομολόγηση) και συνεπώς μπορούν βρεθούν μέσω της ανάλυσης της κίνησης που περνάει από το διακομιστή. Ακόμα και έτσι όμως η παρεχόμενη ασφάλεια είναι ικανοποιητική. Η μέθοδος αυτή μπορεί να



χρησιμοποιηθεί ακόμα και αν το μήνυμα έχει αρχικά κωδικοποιηθεί με βάση την κρυπτογράφηση για όλη τη διαδρομή (end-to-end encryption).

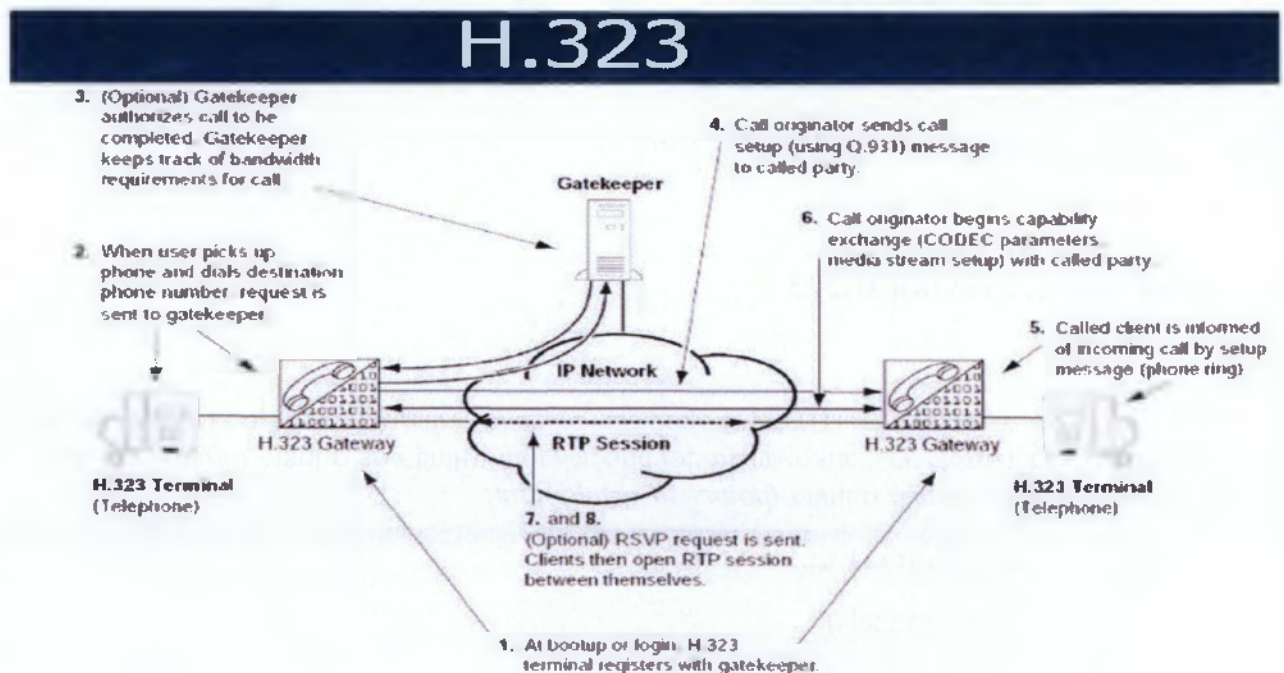
## B. Έλεγχος πρόσβασης και ακεραιότητα μηνυμάτων μέσω πιστοποίησης (authentication)

Πρέπει να ληφθούν προστατευτικά μέτρα για την αποτροπή αλλαγής ενός μηνύματος. Μπορούν να χρησιμοποιηθούν τα ίδια κρυπτογραφικά μέσα που χρησιμοποιούνται για την αυθεντικότητα των μηνυμάτων και την αυθεντικότητα της προέλευσης του μηνύματος. Όμως, ο βασικός μηχανισμός και η περίληψη προσφέρουν μόνο πιστοποίηση και όχι την ακεραιότητα (integrity) των μηνυμάτων. Το επίπεδο μεταφοράς (transport layer) και το επίπεδο δικτύου (network layer) προσφέρουν κάποιους μηχανισμούς που χρησιμοποιούνται για τη πιστοποίηση ανά βήμα (hop-by-hop authentication). Κάθε υλοποίηση πρέπει να υποστηρίζει πιστοποίηση PGP.

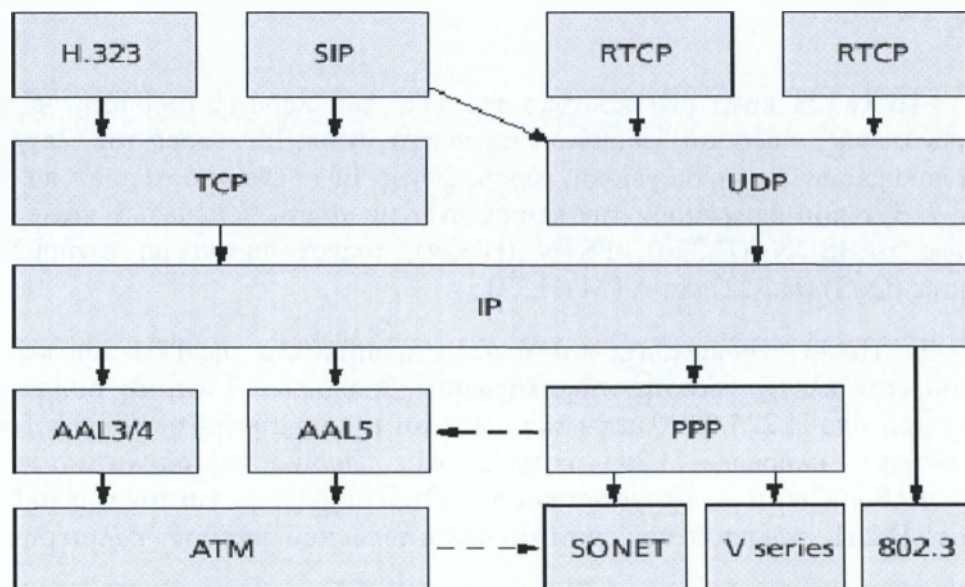
## 5.2 H.323

Το H.323 είναι ένα πρότυπο της ITU που παρέχει τη βάση για τη σύγκλιση επικοινωνιών φωνής, video και δεδομένων πάνω από δίκτυα IP. Αφορά τον έλεγχο κλήσης, τη διαχείριση πολυμέσων και τη διαχείριση εύρους ζώνης. Είναι ένα από τα πρότυπα επικοινωνιών της σειράς H.32x που επιτρέπουν την επικοινωνία με χρήση πολυμέσων πάνω από διάφορα δίκτυα όπως το ISDN (H.320), PSTN (H.324), τοπικά δίκτυα με εγγυημένη ποιότητα εξυπηρέτησης (QoS) (H.322) και ATM (H.321).

Το H.323 ενσωματώνει πολλά άλλα πρωτόκολλα της ITU που περιγράφουν τη σηματοδότηση, τον έλεγχο κλήσης, συμπληρωματικές υπηρεσίες και τη συμπίεση ήχου και εικόνας. Το πρότυπο H.225.0 καλύπτει τη μορφή και τη ροή μηνυμάτων σηματοδότησης, ενώ το πρότυπο ελέγχου κλήσεων H.245 εστιάζει στις διαδικασίες αποκατάστασης κλήσεων πολυμέσων. Καθορίζονται ως υποχρεωτικοί δυο τύποι συμπίεσης, για τον ήχο το G.711 και για την εικόνα το H.261, ενώ υποστηρίζονται και άλλοι τύποι που παρέχουν καλύτερη ποιότητα.



Το πρότυπο είναι ανεξάρτητο από λειτουργικά και μηχανικά συστήματα. Μπορεί να χρησιμοποιηθεί σε PCs, τηλεφώνια IP, καλωδιακή τηλεόραση κ.α. Το H.323 μπορεί από μόνο του να υποστηρίξει επικοινωνία μεταξύ τριών και πλέον τερματικών χωρίς τη βοήθεια του *ελεγκτή μονάδος πολλαπλών σημείων (multipoint control unit, MCU)*. Όμως η χρήση ενός τέτοιου υποσυστήματος παρέχει μια πλατφόρμα πιο ευέλικτη και με περισσότερες υπηρεσίες. Σε επικοινωνίες μεταξύ πάνω από 2 τερματικών υποστηρίζεται η μετάδοση σε πολλούς αποδέκτες (*αποστολή multicast*). Αυτό σημαίνει ότι αν κάποιο πακέτο πρέπει να σταλεί σε πολλαπλούς προορισμούς τότε στέλνεται 1 φορά. Αντίθετα σε αποστολές σε έναν μόνο αποδέκτη (*unicast*) δημιουργούνται πολλαπλές αποστολές από σημείο σε σημείο (*point-to-point*) ενώ κατά την εκπομπή στέλνεται πακέτο παντού ανεξάρτητα από το αν έχει ζητηθεί ή όχι. Συνεπώς, οι πόροι του δικτύου δεν χρησιμοποιούνται αποτελεσματικά.



AAL – ATM adaptation layer  
 ATM – Asynchronous transfer mode  
 IP – Internet protocol  
 PPP – Point-to-point protocol  
 RTCP – Real-time control protocol

RTP – Real-time protocol  
 SIP – Session initiation protocol  
 SONET – Synchronous optical network  
 TCP – Transmission control protocol  
 UDP – User datagram protocol

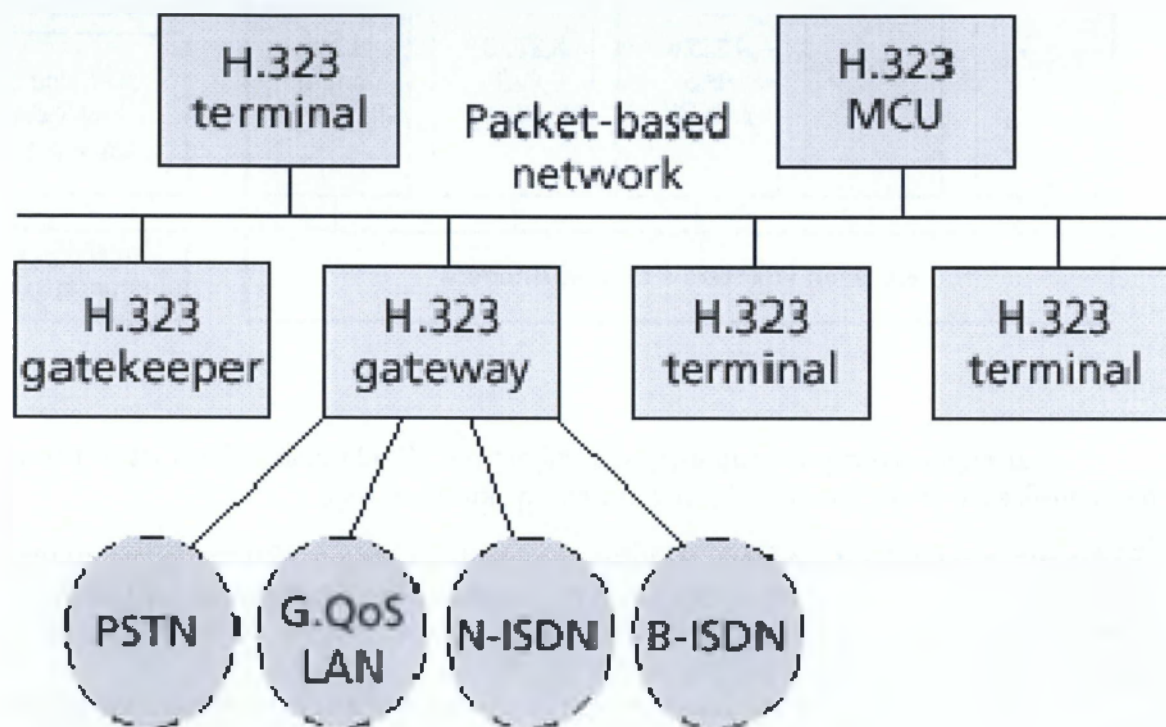
### 5.2.1 Αρχιτεκτονική H.323

Το πρωτόκολλο **H.323** καθορίζει τέσσερα «συστατικά» για το δίκτυο που αν συνδεθούν μαζί παρέχουν επικοινωνία πολυμέσων από σημείο σε σημείο (*point - to - point*) και από σημείο σε πολλαπλά σημεία (*point - to - multipoint*).

Τα βασικότερα από αυτά είναι:

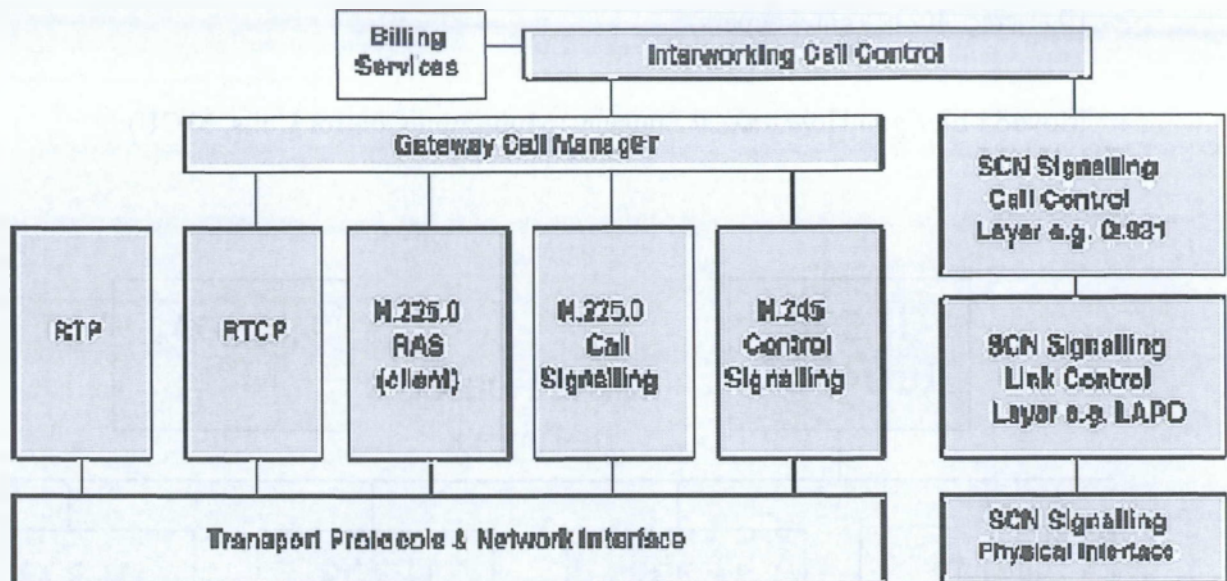
- Τερματικά (terminals)
- Πύλες (gateways)

- Ελεγκτές Πύλης (gatekeepers)
- Μονάδα Ελέγχου Πολλαπλών Σημείων (Multipoint Control Units, MCU)



### Αρχιτεκτονική H.323

- **Τερματικό (terminal):** Χρησιμοποιείται για διπλής κατεύθυνση επικοινωνία πολυμέσων πραγματικού χρόνου. Μπορεί να είναι ένα PC ή άλλη συσκευή που υποστηρίζει το H.323 και εφαρμογές πολυμέσων. Επίσης, περιέχει δυνατότητες για μεταφορά εικόνας και δεδομένων.
- **Πύλη (Gateway):** Μια πύλη συνδέει δίκτυα που δεν βασίζονται στο ίδιο πρωτόκολλο.



Για παράδειγμα μια εφαρμογή μιας πύλης του H.323 εμφανίζεται στην τηλεφωνία IP όπου συνδέει το IP δίκτυο με τα δίκτυα μεταγωγής κυκλώματος.

➤ **Ελεγκτής πύλης (Gatekeeper):** Παρέχει υπηρεσίες έλεγχου κλήσης όπως μετάφραση διευθύνσεων και διαχείριση εύρους ζώνης (bandwidth). Ο ελεγκτής πύλης δεν είναι υποχρεωτικό τμήμα του δικτύου. Αν όμως είναι παρών τότε οι πύλες και τα τερματικά πρέπει να χρησιμοποιούν τις υπηρεσίες που προσφέρουν.

Το H.323 ορίζει ότι ένας ελεγκτής πύλης (gatekeeper) πρέπει να προσφέρει υποχρεωτικά κάποιες υπηρεσίες:

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

Ο ελεγκτής πύλης δεν είναι απαραίτητο να υπάρχει ως αυτόνομη συσκευή. Μπορεί να υλοποιείται σαν μέρος της πύλης ή της **MCU (Μονάδα Ελέγχου Πολλαπλών Σημείων)**.

➤ **Μονάδα Ελέγχου Πολλαπλών Σημείων (Multipoint Control Unit- MCU):** Είναι μια προαιρετική συσκευή που όταν υπάρχει καθιστά ικανή τη διάσκεψη μεταξύ περισσότερων των τριών τερματικών. Αποτελείται από έναν υποχρεωτικό ελεγκτή πολλαπλών σημείων (**Multipoint Controller, MC**) και κάποιους, ή και κανέναν, επεξεργαστή πολλαπλών σημείων (**Multipoint Processors, MP**). Μπορεί να υλοποιηθεί σαν μέρος οποιασδήποτε από τις άλλες τρεις συσκευές του H.323.

## 5.2.2 Πρωτόκολλα H.323

Το H.323 ακριβώς επειδή αποτελεί πρωτόκολλο «ομπρέλα», περιγράφει την χρήση των H.225, H.245 αλλά και άλλων πρότυπων που αφορούν στην παράδοση των υπηρεσιών για συνόδους που είναι βασισμένα στην μεταφορά πολυμεσικών πακέτων. Δηλαδή το H.225 περιγράφει τρία πρωτόκολλα σηματοδότησης που είναι το RAS, το Call Signaling και το “Annex G”, ενώ το H.245 περιγράφει το πρωτόκολλο που αφορά τον έλεγχο των πολυμέσων και είναι παρόμοιο με τα H.323, H.310 και H.324. Πέρα όμως από τα βασικά το H.323 περιγράφει και κάποια επιπρόσθετα πρότυπα όπως είναι το H.235 που ασχολείται με την ασφάλεια μεταξύ συστημάτων βασισμένων πάνω σε H.245, το H.246 που ασχολείται με την διάδραση στο δίκτυο PSTN. Ακόμη ασχολείται με τα H.450.x πρότυπα που αναφέρονται σε επιπρόσθετες υπηρεσίες και με την σειρά των H.460.x που αποτελούν επεκτάσεις του κυρίως H.323 πρωτοκόλλου.

**Αναλυτικότερα παρουσιάζονται τα πιο γνωστά πρωτόκολλα που καθορίζει το H.323:**

- **Audio Codecs**

Ένας κωδικοποιητής - αποκωδικοποιητής (Codec) ήχου παίρνει τον ήχο από το μικρόφωνο και τον κωδικοποιεί έτσι ώστε να είναι κατάλληλο για αποστολή. Στην πλευρά του δεκτή επιτελεί την αντίστροφη λειτουργία. Επειδή η επικοινωνία με ήχο είναι η ελάχιστη επιτρεπτή λειτουργία που παρέχει το H.323, όλα τα H.323 τερματικά πρέπει να έχουν τουλάχιστον ένα κωδικοποιητή - αποκωδικοποιητή (Codec) όπως περιγράφεται στην σύσταση G.711 της ITU (κωδικοποίηση στα 64Kbps). Υπάρχουν και άλλες συστάσεις όπως G.722 (64, 56 και 48 Kbps), G.723.1 (5.3 και 6.3 Kbps), G.728 (16 Kbps) και G.729 (8 Kbps).

- **Video Codecs**

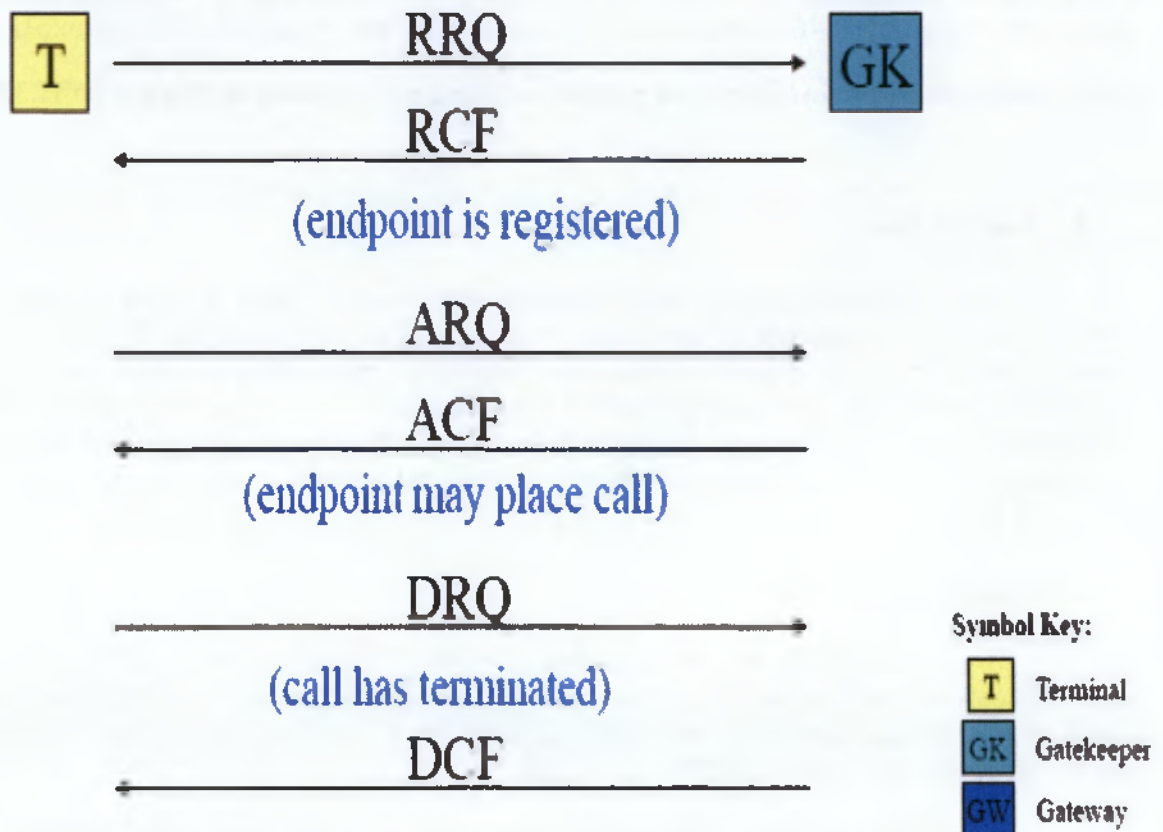
Χαρακτηριστικό της επικοινωνίας με video είναι ότι απαιτεί μεγάλο εύρος ζώνης bandwidth ενώ τα πακέτα εμφανίζονται κατά μεγάλες ομάδες (burst). Γι'αυτό είναι απαραίτητες αποδοτικές τεχνικές συμπίεσης και αποσυμπίεσης για να έχουμε ικανοποιητική απόδοση. Το H.323 καθορίζει δύο Codecs, **H.261** και **H.263**.

Το **H.261** παράγει video για κανάλια με εύρος ζώνης (bandwidth)  $k*64Kb/s$  όπου το  $k$  είναι από 1 ως 30. Χρησιμοποιείται ο μετασχηματισμός διακριτού συνημίτονου (**Discrete Cosine Transform - DCT**) για κβαντοποίηση και συμπίεση. Υποστηρίζονται δυο video format. Το **Common Intermediate Format (CIF)**, με ανάλυση 352X288, και το **Quarter Common Intermediate (QIF)**, με ανάλυση 176X144, εκ των οποίων το **CIF** είναι προαιρετικό.

Το **H.263** χρησιμοποιείται για μετάδοση χαμηλού ρυθμού αλλά χωρίς απώλεια ποιότητας. Η κβαντοποίηση και η συμπίεση γίνεται με το **DCT** αλλά για πετύχουμε το χαμηλότερο ρυθμό βασιζόμαστε σε τεχνικές εκτίμησης και πρόβλεψης κίνησης (*motion estimation and prediction*). Το αποτέλεσμα είναι να έχουμε καλύτερη ποιότητα εικόνας με πιο χαμηλό ρυθμό. Τα video formats που υποστηρίζονται είναι sub-QCIF (128X96), QCIF (276X144), DIC (352X244), 4CIF (702X576) και 16CIF (1408X576). Τα τρία πρώτα είναι απαραίτητα ενώ τα άλλα δύο προαιρετικά. Μέσω του QCIF διατηρείται η συμβατότητα μεταξύ **H.261** και **H.263**.

- **H.225 RAS (Registration Admission and Status)**

Το RAS είναι ένα πρωτόκολλο για το Registration, Admission και Status. Σε ένα H.323 σύστημα ήχου ή βίντεο, το πρωτόκολλο αυτό είναι ένα κανάλι ελέγχου πάνω από το οποίο στέλνονται τα H.225 μηνύματα σηματοδότησης και από το οποίο είναι ορισμένο. Επιτρέπει σε ένα τελικό σημείο να ζητήσει εξουσιοδότηση για να θέσει ή να δεχθεί μια κλήση. Επιτρέπει σε ένα Gatekeeper να ελέγξει την πρόσβαση από και προς τις συσκευές που είναι υπό τον έλεγχό του. Επίσης, επιτρέπει σε έναν Gatekeeper να επικοινωνήσει την διεύθυνση σε άλλα τερματικά σημεία. Τέλος, επιτρέπει σε δύο Gatekeepers να ανταλλάξουν εύκολα πληροφορίες διευθύνσεων. Ένα μήνυμα RAS περιγράφεται στο παρακάτω σχήμα:

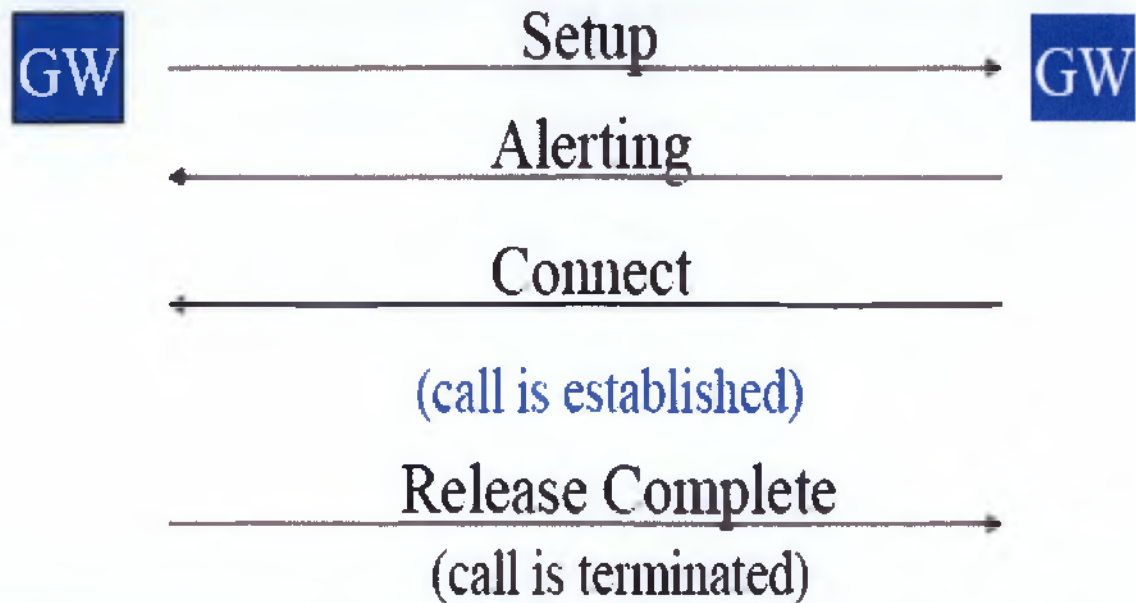


### Δομή Μηνύματος RAS

- **H.225 Σηματοδότηση Κλήσεων**

Το πρωτόκολλο αυτό χρησιμοποιείται για να περιγράψει την σηματοδότηση της κλήσης, τον ήχο και την εικόνα καθώς και την stream packetization, τον συγχρονισμό των πολυμεσικών stream και τον έλεγχο του μηνύματος. Αναλυτικότερα όσον αφορά την σηματοδότηση της κλήσης, το H.225 εγκαθιστά, ελέγχει και ολοκληρώνει μια κλήση H.323. Η σηματοδότηση της κλήσης είναι βασισμένη πάνω στις διαδικασίες για το setup μιας κλήσης για ISDN που περιγράφονται στο Q.931.

Το **H.225** είναι υπεύθυνο για την συνάρτηση σηματοδοσίας **RAS** η οποία εκτελεί την εγγραφή, την παραδοχή και τις αλλαγές στο bandwidth, την θέση και τις αλλαγές μεταξύ των τερματικών σημείων ενός **H.323** Gatekeeper. Η **RAS** συνάρτηση σηματοδοσίας χρησιμοποιεί ένα ξεχωριστό κανάλι το οποίο έχει μια συλλογή από μηνύματα, τα **Registration, Admission** και **Status**. Ένα μήνυμα **H.225** περιγράφεται στο παρακάτω σχήμα:



### Δομή Μηνύματος H.225

- **H.245 Σηματοδοσία Ελέγχου**

Είναι το πρωτόκολλο που ελέγχει την επικοινωνία των πολυμέσων, και που περιγράφει τις διαδικασίες και τα μηνύματα προκειμένου να ανοιχτούν και να κλείσουν τα λογικά κανάλια για τον ήχο, την εικόνα και τα δεδομένα. Επίσης, ελέγχει την δυνατότητα ανταλλαγής, ελέγχου και ενδείξεων. **Αναλυτικότερα**, διαχειρίζεται τις παρακάτω λειτουργίες: ανταλλαγή δυνατοτήτων όπου τα τερματικά καθορίζουν τους κωδικοποιητές που διαθέτουν και γίνεται αποστολή προς το άλλο τελικό σημείο. Το **H.245** αναλαμβάνει να ανοίξει και να κλείσει τουλάχιστον δύο ή τρία κανάλια ήχου και εικόνας **H.323** τα οποία είναι point to point και ανευ κατεύθυνσης. Επίσης, θα πρέπει να φτιάξει τον έλεγχο ροής όταν θα υπάρχει πρόβλημα.

- **H.450 Συμπληρωματικές Υπηρεσίες**

Η σύσταση **H.323** συνδέει τα παραδοσιακά τηλεφωνικά δίκτυα με τα δίκτυα που βασίζονται σε πακέτα. Υπάρχουν πολλές δυνατότητες για νέες υπηρεσίες και εφαρμογές που θα χρησιμοποιούν τα επιπλέον χαρακτηριστικά των δικτύων. Οι νέες υπηρεσίες ποικίλουν από πρόσθετες υπηρεσίες που αφορούν καθαρά τις τηλεφωνικές κλήσεις (προώθηση κλήσης, εκτροπή) ως το voice mail. Το **H.323** μέσω της σειράς συστάσεων **H.450.x** παρέχει μια επιπλέον ευέλικτη αρχιτεκτονική για βοηθητικές υπηρεσίες.

- **H.235 Ασφάλεια**

Το **H.235** ασχολείται με τέσσερα θέματα που έχουν σχέση με την ασφάλεια. Πιστοποίηση (*authentication*), ακεραιότητα (*integrity*), μυστικότητα (*privacy*), μη-αποκήρυξη (*non-repudiation*).

Η **πιστοποίηση** είναι ένας μηχανισμός που διασφαλίζει ότι οι χρήστες των τερματικών σημείων που παίρνουν μέρος σε μια συνομιλία είναι αυτοί που λένε ότι είναι. Παρέχεται μέσω του έλεγχου πρόσβασης των τερματικών σημείων. Υπεύθυνος για τον έλεγχο είναι ο ελεγκτής πύλης που ελέγχει τη ζώνη.

Η **ακεραιότητα** παρέχει τα μέσα που επιβεβαιώνουν ότι τα δεδομένα σε κάθε πακέτο δεν έχουν αλλοιωθεί.

Η **μυστικότητα** και η εμπιστευτικότητα παρέχονται μέσω κωδικοποίησης που κρύβει τα δεδομένα έτσι ώστε αν κάποιο πακέτο γίνει αντιληπτό να μην είναι δυνατή η ανάγνωσή του.

Η **μη-αποκήρυξη** είναι ένας τρόπος προστασίας έναντι κάποιου που θα ισχυριστεί ότι δεν πήρε μέρος σε μια συνομιλία, ενώ ξέρουμε ότι ήταν εκεί.

- **Πρωτόκολλα RTP και RTCP**

Το πρωτόκολλο μεταφοράς πραγματικού χρόνου (*Real-time Transport Protocol - RTP*) καθορίζει ένα τυποποιημένο σχήμα για την μεταφορά πακέτων ήχου και εικόνας πάνω από ένα δίκτυο IP. Αναπτύχθηκε από την ομάδα εργασίας μεταφοράς ήχου – βίντεο της IETF και δημοσιεύθηκε αρχικά το 1996 ως RFC 1889, ενώ αντικαταστάθηκε από το RFC 3550 το 2003.

Το RTP σχεδιάστηκε για την από άκρη σε άκρη μεταφορά στοιχείων πολυμέσων σε πραγματικό χρόνο. Το RTP ουσιαστικά αποτελείται από δύο πρωτόκολλα, το ίδιο το RTP καθώς και το πρωτόκολλο ελέγχου Real-time Transport Control Protocol (RTCP). Το RTP χρησιμοποιείται για τη μεταφορά των στοιχείων πολυμέσων, ενώ το RTCP χρησιμοποιείται για να στέλνονται περιοδικά οι πληροφορίες ελέγχου και οι παράμετροι του *QOS* (*Quality of Service*).

Οι εφαρμογές πολυμέσων για να λειτουργήσουν σωστά χρειάζονται την έγκαιρη παράδοση των πακέτων και μπορούν να ανεχτούν ορισμένη απώλεια πακέτων. Για παράδειγμα η απώλεια ενός πακέτου δεδομένων φωνής έχει ως αποτέλεσμα την απώλεια ενός κλάσματος του δευτερολέπτου του ακουστικού σήματος, το οποίο όμως διορθώνεται με κατάλληλους αλγόριθμους. Στην περίπτωση όμως που υπάρξει συνεχείς απώλεια πακέτων τότε αυτό γίνεται αντιληπτό από τον τελικό χρήστη. Στις εφαρμογές πολυμέσων είναι σημαντικότερο να επιτυγχάνεται η έγκαιρη παράδοση των πακέτων σε σχέση με την αξιοπιστία παράδοσης αυτών. Για αυτό αν και το πρωτόκολλο TCP είναι τυποποιημένο για χρήση από το RTP συνήθως προτιμάται η χρήση του UDP για την μετάδοση των πακέτων RTP, λόγω των καθυστερήσεων στην άφιξη των πακέτων που εισάγονται από το TCP για την εγκαθίδρυση συνδέσεων και τον έλεγχο των λαθών.

- **T.120**

Είναι ένα πρότυπο για συνόδους με δεδομένα και για τον έλεγχο συνόδων για πολυμεσική επικοινωνία τόσο σε multipoint όσο και σε point-to-point επίπεδο.



- **Πρωτόκολλα H.261 – H.263**

Πρόκειται για κωδικοποιητές βίντεο που ορίζει το **H.323** όμως μπορούν να χρησιμοποιηθούν και άλλοι.

### **5.3 MGCP (Media Gateway Control Protocol)**

Το Media Gateway Control Protocol (MGCP, RFC 2705) ακολουθεί την μεθοδολογία την μεταγωγής πακέτων. Στην ουσία αποτελείται από 3 μέρη: το media gateway, το media gateway controller και το signalling gateway. Έτσι διαχειρίζεται το κάθε gateway ξεχωριστά, αναφέροντας την κάθε επιμέρους επικοινωνία σαν MGCP master-slave επικοινωνία. Ο media gateway controller αναφέρεται και σαν μεσίτης κλήσεων (call agent). Ο call agent διαχειρίζεται την σηματοδότηση ελέγχου, καθώς ο media gateway πληροφορεί τον call agent για κάποιο alarm. Ο call agent υποδεικνύει στον media gateway να ξεκινήσει ή να κλείσει μια επικοινωνία. Αλλά σαν βασικό μέλημα του call agent είναι να ενημερώνει τον media gateways να ξεκινήσει, να διακόψει ή να σταματήσει ένα RTP session.

### **5.4 Megaco (Media Gateway Control)**

Το πρωτόκολλο **Megaco/H.248 (Gateway Control Protocol)** είναι ένα πρωτόκολλο ελέγχου το οποίο χρησιμοποιείται ανάμεσα σε έναν *Media Gateway* ο οποίος έχει αναλάβει να μετατρέψει την circuit-switched φωνή σε πακέτα μετάδοσης και έναν *Media Gateway Controller* ο οποίος ελέγχει αυτήν την κίνηση μετάδοσης σε ένα δίκτυο *VoIP*. Σκοπός του είναι να ορίσει όλες εκείνες τις απαραίτητες λειτουργίες και τους μηχανισμούς για να μπορέσει ο *Media Gateway Controller* να ελέγξει τα gateways προκειμένου να υποστηρίξουν τηλεφωνικές κλήσεις μεταξύ *PSTN* και *IP* δικτύων ή μεταξύ *IP* και *IP* δικτύων.

Το πρωτόκολλο αυτό προήλθε από την συνεργασία της **ITU** μαζί με την **IET**. Περιγράφεται και ορίζεται ως **RFC 3525** και το **H.248.1** από τις δύο ομάδες που το δημιούργησαν. Στην ουσία το πρωτόκολλο αυτό λειτουργεί σαν το πρωτόκολλο του *Media Gateway Controller (MGCP)*, με παρόμοια αρχιτεκτονική και ισοδύναμη λειτουργικότητα.

---

## ΚΕΦΑΛΑΙΟ 6

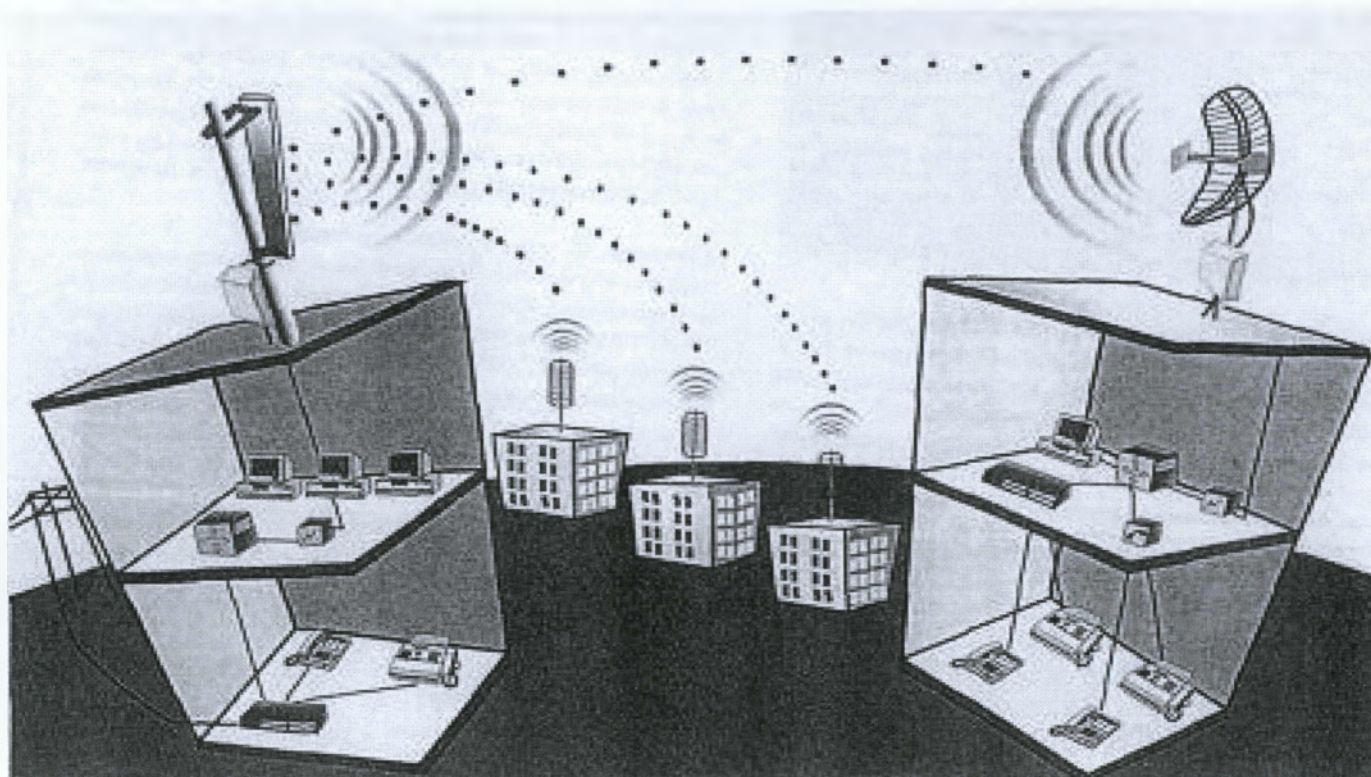
### ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

#### 6.1 Εισαγωγή στα ασύρματα δίκτυα

Τα τελευταία χρόνια παρατηρείται μεγάλη αύξηση στις πωλήσεις φορητών ηλεκτρονικών υπολογιστών. Στη ζωή μας έχει κυριαρχήσει η τάση για φορητότητα, κινητικότητα και συνεχή σμίκρυνση των συσκευών (με σκοπό την ευκολότερη μεταφορά τους). Όλα αυτά έχουν σαν αποτέλεσμα, οι παραδοσιακές ενσύρματες τεχνολογίες δικτύωσης, να αποδεικνύονται ανεπαρκείς για το νέο τρόπο ζωής του ανθρώπου.

Την λύση στο πρόβλημα της δικτύωσης, δίνουν οι τεχνολογίες ασύρματης δικτύωσης, που καταργούν τα καλώδια και δίνουν μεγάλο βαθμό ελευθερίας στους χρήστες τους. Τα ασύρματα δίκτυα, όπως και τα ενσύρματα, μεταδίδουν δεδομένα μέσα από ένα μέσο διάδοσης. Το μέσο αυτό είναι οι ραδιοσυχνότητες (RF) που μεταδίδονται μέσω του αέρα. Οι ραδιοσυχνότητες μεταδίδονται στον χώρο, άρα ένα ασύρματο δίκτυο δραστηριοποιείται σε μια συγκεκριμένη περιοχή κάλυψης, έξω από την οποία τα σήματα εξασθενούν σε βαθμό που δεν είναι αξιοποιήσιμα.

Η εγκατάσταση ενός ασύρματου δικτύου σε ένα χώρο απαιτεί την εγκατάσταση κάποιων κεντρικών ασύρματων σταθμών (στα δίκτυα 802.11 ονομάζονται *σημεία ασύρματης πρόσβασης* – *wireless Access Points*). Αντίστοιχα, κάθε χρήστης χρειάζεται μια ασύρματη συσκευή για να μπορεί να συνδεθεί σε κάποιον από τους κεντρικούς σταθμούς.

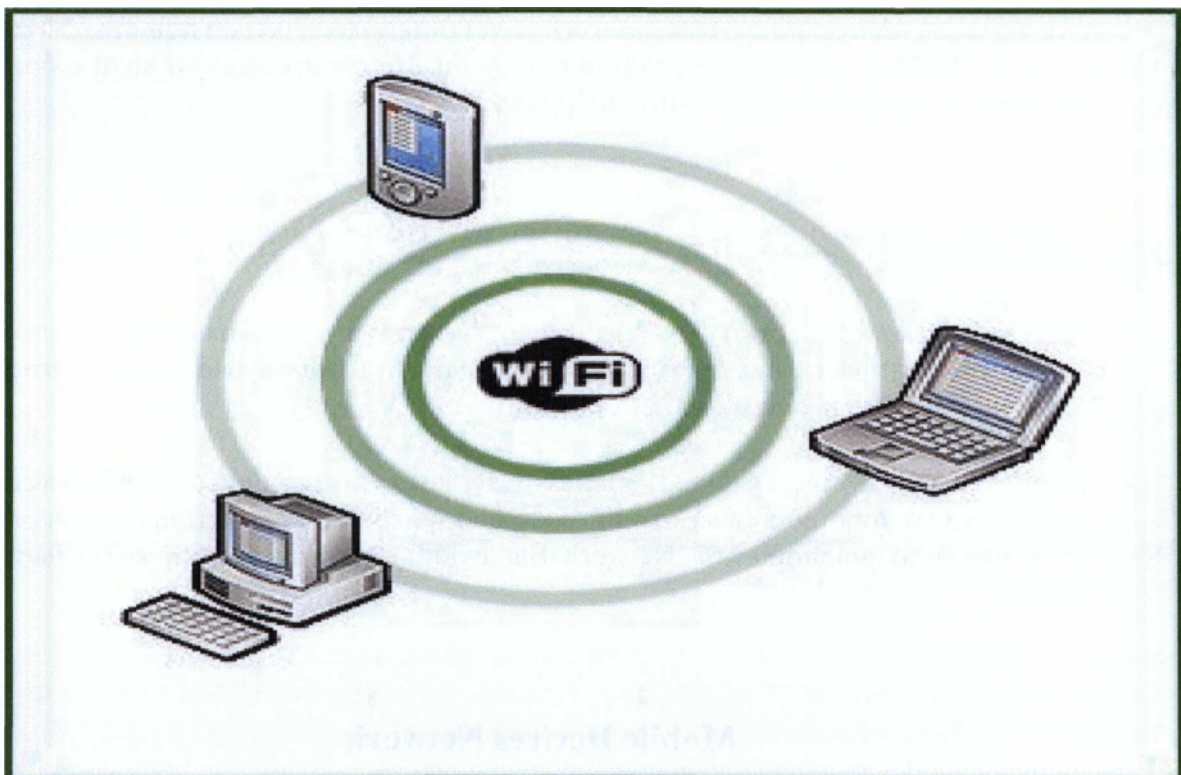


Ο τρόπος λειτουργίας των ασυρμάτων δικτύων τους δίνει τα παρακάτω πλεονεκτήματα σε σχέση με τα ενσύρματα δίκτυα:

**Φορητότητα και Κινητικότητα:** Το πλεονέκτημα αυτό είναι προφανές. Οι χρήστες ενός ασυρμάτου δικτύου μπορούν να συνδέονται στο δίκτυο από οποιοδήποτε σημείο της περιοχής κάλυψης και να μετακινούνται μέσα σε αυτή χωρίς να διακόπτεται η σύνδεση. Μπορούν ακόμα και να μεταπηδούν (*roam*) από μια περιοχή κάλυψης σε μια άλλη (εφόσον αυτές είναι διασυνδεδεμένες κατάλληλα μεταξύ τους), διατηρώντας και πάλι την σύνδεση με το δίκτυο.

**Απλότητα εγκατάστασης:** Η εγκατάσταση και η σύνδεση σε ένα ασύρματο δίκτυο είναι πολύ απλή και γρήγορη, καθώς δεν απαιτείται εγκατάσταση καλωδίων.

**Ευελιξία εγκατάστασης:** Η τεχνολογία ασύρματης δικτύωσης μας δίνει τη δυνατότητα να εγκαταστήσουμε δίκτυα σε σημεία ή περιοχές που η εγκατάσταση ενσύρματων δικτύων είναι δύσκολη ή ακόμα και αδύνατη. Για παράδειγμα η σύνδεση μεταξύ απομακρυσμένων κτηρίων ενός οργανισμού είναι μια εφαρμογή η οποία θα απαιτούσε πολύ χρόνο και υψηλό κόστος αν γινόταν με ενσύρματο δίκτυο (προφανώς με χρήση οπτικών ινών). Μια εφαρμογή των ασύρματων δικτύων πέρα από τις παραδοσιακές, είναι η δημιουργία *hot spots*, δηλαδή ασύρματη κάλυψη δημόσιων ή πολύ εκτεταμένων χώρων με μεγάλη πυκνότητα χρηστών. Τέτοιοι χώροι είναι τα αεροδρόμια, τα λιμάνια, οι καφετέριες, ακόμα και οι πλατείες των πόλεων. Σε τέτοιους χώρους η μαζική παροχή υπηρεσιών δικτύωσης με ενσύρματες τεχνολογίες θα ήταν αδύνατη.



## 6.2 Είδη Ασύρματων Δικτύων

Ο όρος ασύρματο δίκτυο αναφέρεται σε κάθε δίκτυο, το οποίο είναι υλοποιημένο χωρίς την χρήση καλωδίων. Συνήθως ένα τέτοιο τηλεπικοινωνιακό δίκτυο υλοποιείται με κάποιο είδος απομακρυσμένου συστήματος μετάδοσης πληροφοριών που χρησιμοποιεί ηλεκτρομαγνητικά κύματα, όπως ραδιοκύματα.

Υπάρχουν διάφορα είδη ασύρματων δικτύων, τα οποία είναι:

- **Wireless LAN**

Τα *Wireless Local Area Networks (WLANs)* παρέχουν ένα LAN χρησιμοποιώντας ραδιοκύματα αντί για καλώδια σε μία μικρή περιοχή όπως ένα σπίτι, ένα γραφείο ή ένα σχολείο. Τα περισσότερα WLANs βασίζονται στο IEEE 802.11. Ο όρος Wi-Fi χρησιμοποιείται όλο και περισσότερο ως συνώνυμο για τα 802.11 WLANs, αν και στην πραγματικότητα είναι μια πιστοποίηση της συνεργασίας 802.11 συσκευών.

- **Wireless PAN**

Τα *Wireless Personal Area Networks (WPANs)* συνδέουν συσκευές σε ένα σχετικά μικρό χώρο, γενικά στην εμβέλεια ενός ανθρώπου. Το Bluetooth για παράδειγμα παρέχει ένα WPAN που μπορεί να χρησιμοποιηθεί για συνδέσεις όπως ακουστικών με κινητό τηλέφωνο.

- **Wireless MAN**

Τα *Wireless Metropolitan Area Networks* είναι ένας τύπος δικτύου που συνδέει αρκετά ασύρματα LAN. *WiMAX (Worldwide Interoperability for Microwave Access)* είναι ο όρος που χρησιμοποιείται για να αναφερόμαστε στα ασύρματα MAN.

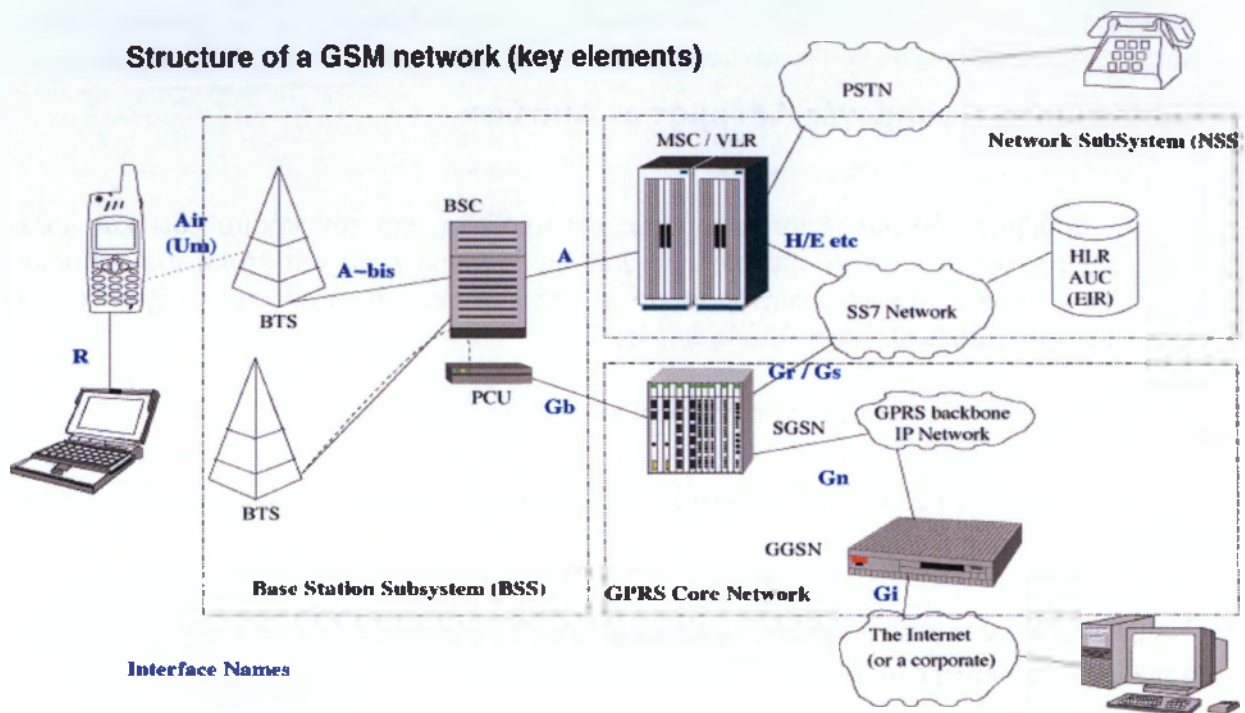
Με την ανάπτυξη των έξυπνων τηλεφώνων (*smart phones*) τα δίκτυα κινητών επικοινωνιών μεταφέρουν πολλών ειδών δεδομένα εκτός της φωνής.

- **Wi-Fi (Wireless Fidelity):** Το Wi-Fi είναι ένα συχνά χρησιμοποιούμενο ασύρματο δίκτυο στα συστήματα υπολογιστών που δίνει τη δυνατότητα σύνδεσης στο Internet ή σε άλλες μηχανές που έχουν Wi-Fi λειτουργικότητες.
- **Fixed Wireless Data:** Το Fixed Wireless Data είναι ένα ασύρματο δίκτυο δεδομένων που μπορεί να χρησιμοποιηθεί στη σύνδεση δύο ή περισσότερων κτιρίων με σκοπό την επέκταση ή το μοίρασμα του Network Bandwidth χωρίς τη φυσική καλωδίωση των κτιρίων.

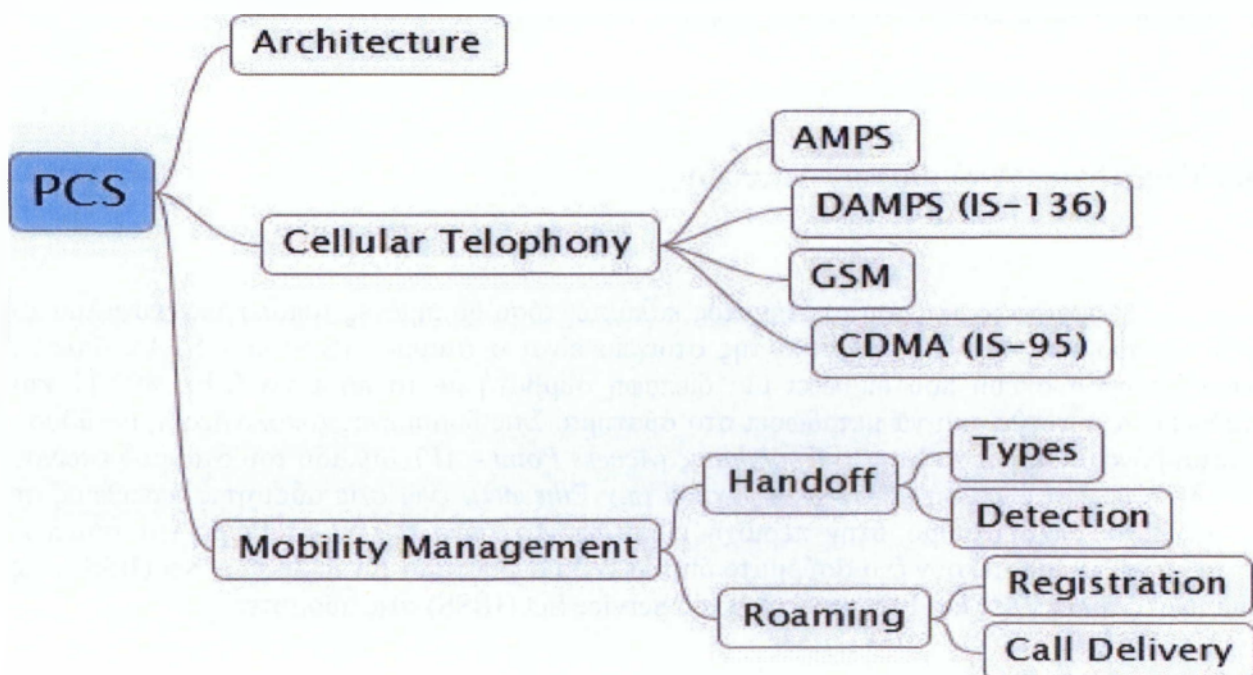
### Mobile Devices Network

- **Global System for Mobile Communications (GSM):** Το δίκτυο GSM χωρίζεται σε τρία κύρια συστήματα: το σύστημα μεταγωγής (*Switching System*), το σύστημα σταθμού βάσης (*Base Station System*) και το σύστημα λειτουργίας και υποστήριξης (*Operation and Support System*). Το κινητό τηλέφωνο συνδέεται στο σύστημα σταθμού βάσης το οποίο

στη συνέχεια συνδέεται στο σταθμό λειτουργίας και υποστήριξης. Τέλος, συνδέεται στο σταθμό μεταγωγής όπου η κλήση μεταφέρεται στον προορισμό της.



- **Personal Communication Service (PCS):** Το PCS είναι ένα είδος δικτύου που χρησιμοποιείται από κινητά τηλέφωνα στην Βόρειο Αμερική και την Νότιο Ασία.



- **D-AMPS:** Το **Digital Advanced Mobile Phone Service** είναι ένα είδος δικτύου που έχει πλέον ξεπεραστεί από την ανάπτυξη της τεχνολογίας και του GSM.

### 6.3 Χρήσεις και Εφαρμογές Ασύρματων Δικτύων

Τα ασύρματα δίκτυα είχαν εφαρμογές και αποδοχή από τον κόσμο εδώ και πολλά χρόνια. Από τον δεύτερο παγκόσμιο πόλεμο χρησιμοποιήθηκαν για αποστολή πληροφοριών. Από τότε τα ασύρματα δίκτυα αναπτύσσονται και εξελίσσονται συνεχώς και οι χρήσεις τους έχουν αυξηθεί και εξαπλωθεί σε πολλούς τομείς:

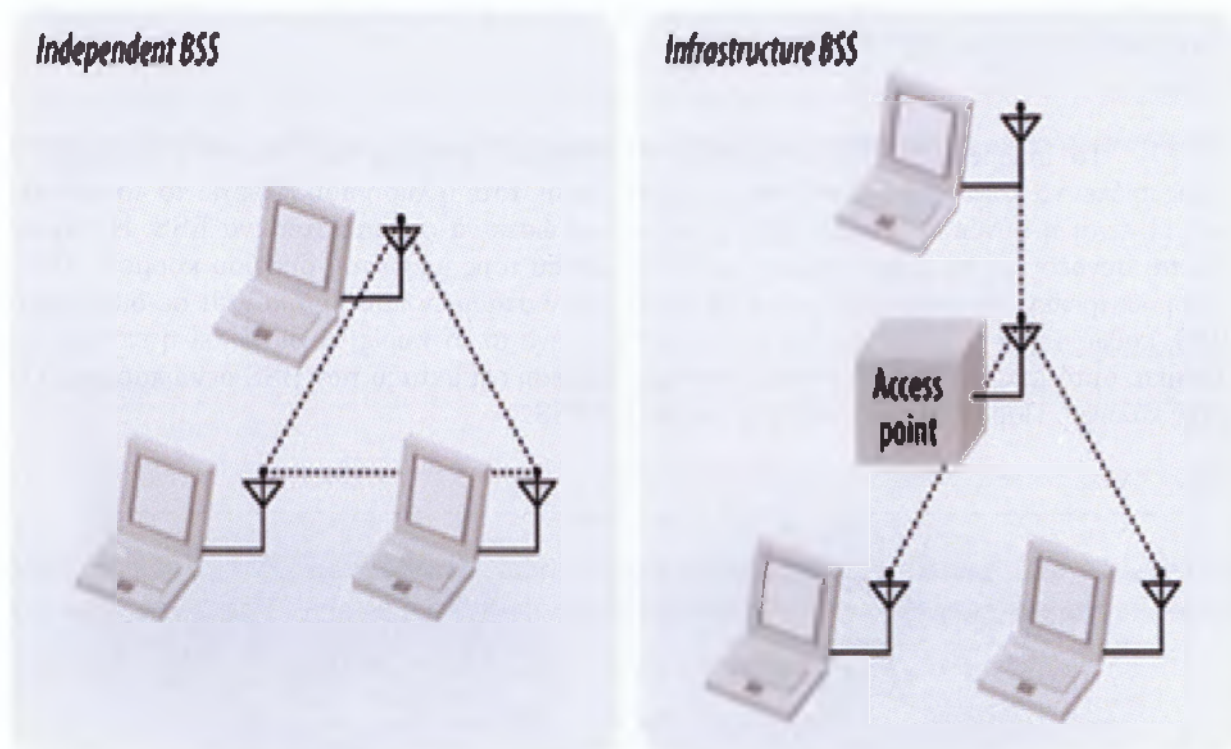
- Τα κινητά τηλέφωνα είναι μέρος τεράστιων ασύρματων δικτύων.
- Οι δορυφόροι επιτρέπουν την αποστολή πληροφοριών, εικόνων, ήχου και κάθε μορφής δεδομένων σε όλο τον κόσμο.
- Υπηρεσίες όπως η αστυνομία και η πυροσβεστική χρησιμοποιούν ασύρματη δικτύωση για γρήγορη και εύκολη επικοινωνία.
- Γραφεία, υπηρεσίες και επιχειρήσεις χρησιμοποιούν ασύρματη δικτύωση για κοινή χρήση δεδομένων.
- Το Internet στα περισσότερα σπίτια πλέον φτάνει ενσύρματα αλλά μέσα σε αυτά χρησιμοποιούνται συσκευές (*wireless routers*) που στέλνουν το σήμα στον υπολογιστή ασύρματα. Επίσης με τον ίδιο τρόπο πολλές βιβλιοθήκες, καφετέριες πανεπιστήμια κ.α παρέχουν στους παρευρισκόμενους φορητές υπολογιστές ασύρματη δικτύωση.

### 6.4 Τοπολογίες Ασύρματων Δικτύων

Η αρχιτεκτονική του συστήματος καλύπτει τόσο δομημένες τοπολογίες (κυβελωτές) όσο και αδόμητες (ad-hoc). Βασικό της στοιχείο είναι ο σταθμός (Station - STA), δηλαδή οποιαδήποτε συσκευή που διαθέτει μια διεπαφή συμβατή με το πρότυπο IEEE 802.11 και επιθυμεί να συνδεθεί και να μεταδώσει στο σύστημα. Στις δομημένες τοπολογίες, η μετάδοση γίνεται μόνο από/προς το Σημείο Πρόσβασης (*Access Point - AP*), δηλαδή του σταθμού εκείνου που διαθέτει και διεπαφή με σταθερό δίκτυο (π.χ *Ethernet*), ενώ στις αδόμητες απευθείας σε οποιοδήποτε άλλο σταθμό στην περιοχή κάλυψης. Το σύνολο των σταθμών και σημείων πρόσβασης που αποτελούν ένα ασύρματο δίκτυο WiFi ονομάζεται **Basic Service Set (BSS)** στις δομημένες τοπολογίες και **Independent Basic Service Set (IBSS)** στις αδόμητες.

- **Independent BSS ή Ad-hoc mode**

Είναι η πιο απλή περίπτωση δημιουργίας ενός ασύρματου δικτύου, όπου κάθε ασύρματος σταθμός επικοινωνεί απ' ευθείας με όλους τους άλλους σταθμούς (εφόσον βρίσκονται στην εμβέλεια του). Η δημιουργία ενός ad-hoc δικτύου είναι πολύ εύκολη και γρήγορη, γι' αυτό χρησιμοποιείται συνήθως σε περιπτώσεις που απαιτείται η δημιουργία ενός δικτύου ανταλλαγής δεδομένων για περιορισμένο χρονικό διάστημα, όπως π.χ. κατά την διάρκεια μιας σύσκεψης. Οι δυνατότητες αυτού του τύπου δικτύου όσον αφορά την ασφάλεια είναι αρκετά περιορισμένες σε σχέση με το Infrastructure BSS.



- **Infrastructure BSS**

Τα Infrastructure ασύρματα δίκτυα διαφοροποιούνται από τα ad-hoc, λόγω της χρήσης των access points. Ένα Infrastructure BSS αποτελείται από ένα access point και ένα αριθμό από ασύρματους σταθμούς. Το access point αποτελεί το κεντρικό κομβικό σημείο του Infrastructure BSS, καθώς όλη η δικτυακή κίνηση μεταξύ των σταθμών περνάει αναγκαστικά από το access point.

Η χρήση των access point παρέχει δύο σημαντικά πλεονεκτήματα:

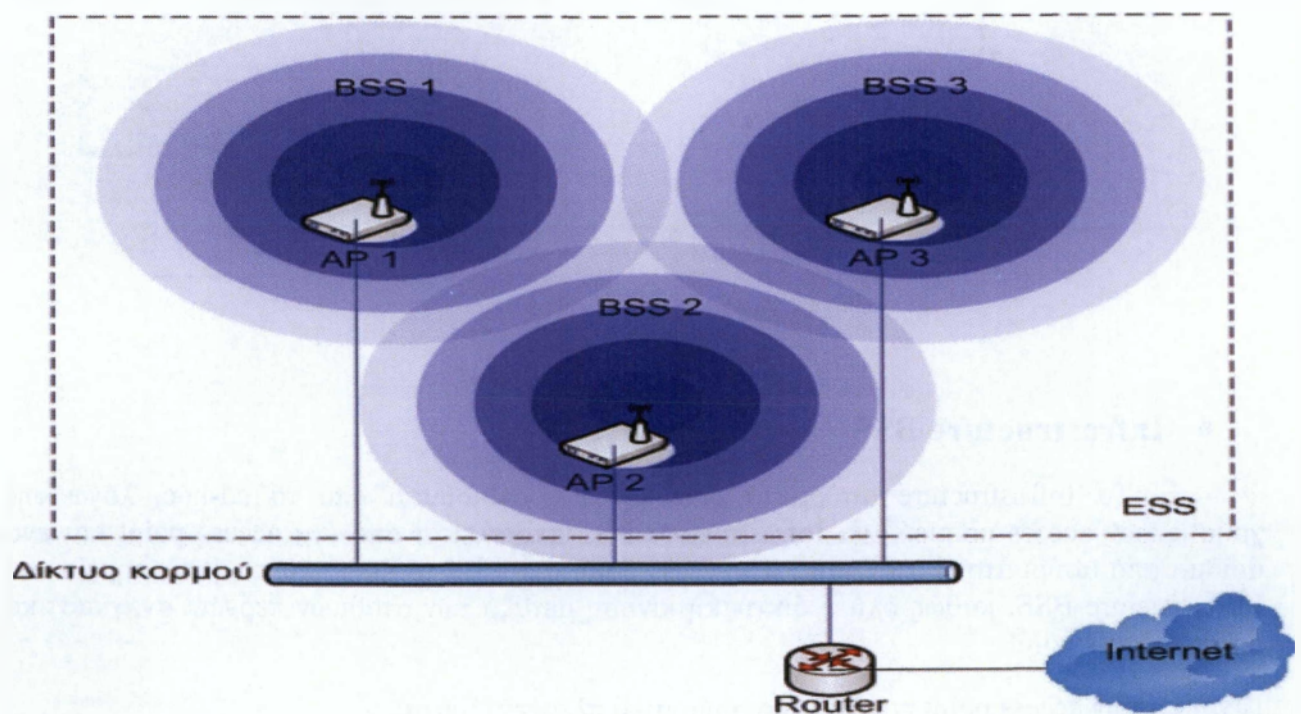
- Η ακτίνα της περιοχής κάλυψης του BSS καθορίζεται με βάση την απόσταση από το access point. Αυτό σημαίνει ότι κάθε σταθμός αρκεί να βρίσκεται στην εμβέλεια του access point, ενώ δεν υπάρχει περιορισμός στην απόσταση μεταξύ των ασύρματων σταθμών.

- Η δομή του Infrastructure BSS επιτρέπει την κεντροποιημένη διαχείριση του δικτύου, καθώς και μεγάλη ευελιξία όσον αφορά την ασφάλεια. Αυτό οφείλεται αφενός στην ύπαρξη ενός κεντρικού κόμβου στο δίκτυο και αφετέρου στον τρόπο με τον οποίο ένας ασύρματος σταθμός συσχετίζεται (associates) με το access point για να επικοινωνήσει με το υπόλοιπο δίκτυο. Η διαδικασία συσχέτισης δεν είναι συμμετρική: Ο ασύρματος σταθμός αποστέλλει μια αίτηση στο access point και αυτό επιτρέπει ή απαγορεύει την πρόσβαση στο υπόλοιπο δίκτυο, ανάλογα με το περιεχόμενο της αίτησης και την πολιτική ασφάλειας που έχει οριστεί.

Η διαφορά των δύο τοπολογιών είναι ότι στην μία περίπτωση χρησιμοποιούμε ασύρματο σημείο (access point) ενώ στην άλλη όχι για να συνδεθούμε με το υπόλοιπο δίκτυο.

## Extended Service Set (ESS)

Το Independent BSS επιτρέπει την ασύρματη κάλυψη ενός ορισμένου χώρου. Αν όμως πρέπει να καλυφθεί μια σχετικά μεγάλη έκταση, τότε η λύση που παρέχει το πρωτόκολλο 802.11 είναι η σύνδεση πολλών BSS μεταξύ τους ώστε να σχηματιστεί ένα ESS. Η σύνδεση γίνεται συνδέοντας τα access points των BSS μεταξύ τους μέσω του δικτύου κορμού. Αυτή η λύση, επιτρέπει την επικοινωνία μεταξύ ασυρμάτων σταθμών που βρίσκονται σε διαφορετικά BSS, καθώς και την μετακίνηση από ένα BSS σε ένα άλλο χωρίς να διακοπεί η επικοινωνία. Φυσικά, αυτό μπορεί να γίνει μόνο με την προϋπόθεση ότι μεταξύ των BSS δεν υπάρχουν κενά στην κάλυψη. Παρακάτω φαίνεται μια τοπολογία ESS.

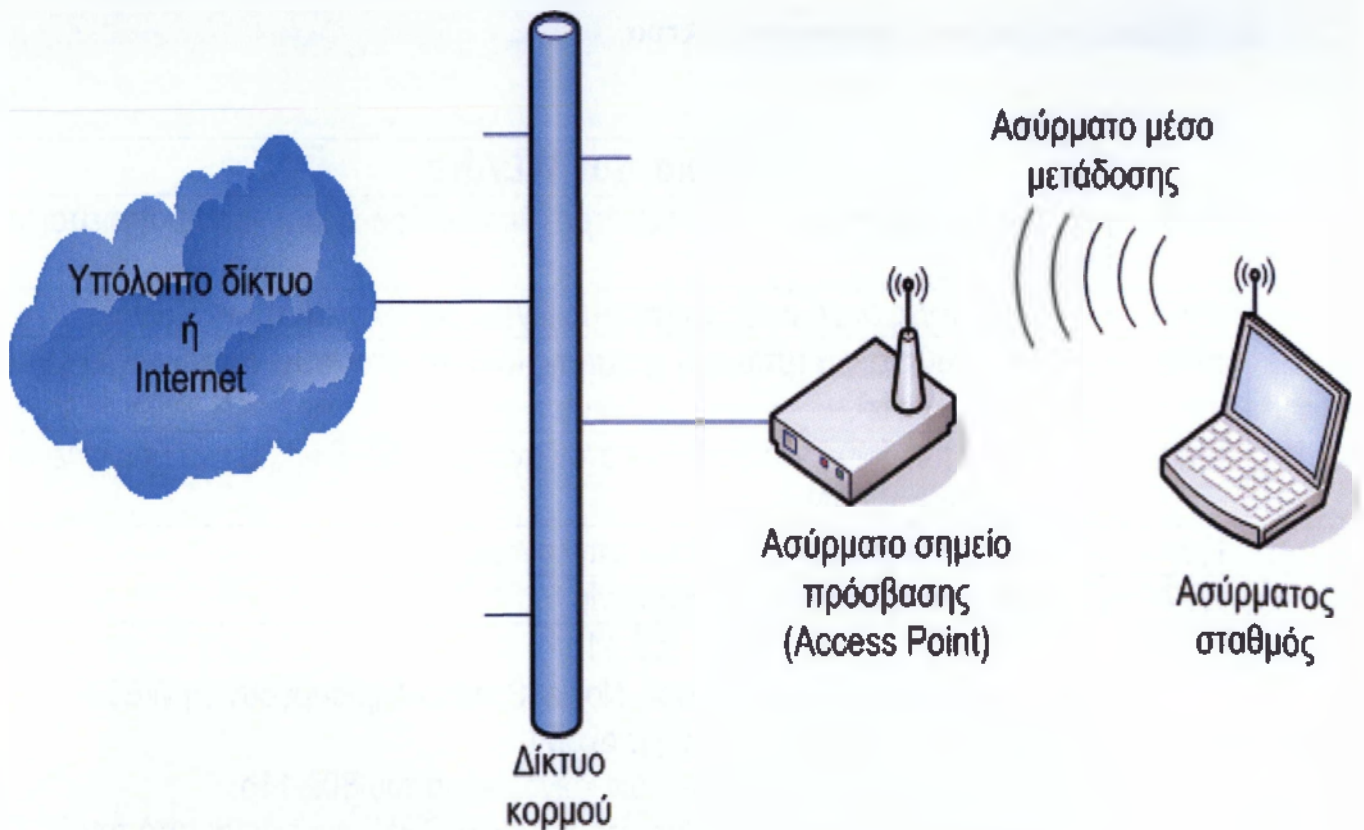


## Extended Service Set (ESS)



## 6.5 Συστατικά στοιχεία ασύρματων δικτύων

Τα ασύρματα δίκτυα αποτελούνται από τέσσερα βασικά συστατικά τα οποία περιγράφονται παρακάτω:



### Συστατικά στοιχεία ενός ασύρματου δικτύου

- **Ασύρματοι σταθμοί**

Οι ασύρματοι σταθμοί είναι συσκευές εφοδιασμένες με μια ασύρματη κάρτα δικτύου που τους επιτρέπει να επικοινωνούν μεταξύ τους. Συνήθως πρόκειται για φορητούς υπολογιστές (Laptop).

- **Ασύρματα σημεία πρόσβασης**

Τα ασύρματα σημεία πρόσβασης (*Wireless Access Points*) είναι οι συσκευές που επιτρέπουν στους ασύρματους σταθμούς που βρίσκονται μέσα στην περιοχή κάλυψης, να επικοινωνούν μεταξύ τους. Επίσης, προωθούν την δικτυακή κίνηση από το ασύρματο δίκτυο προς το δίκτυο κορμού και το αντίστροφο.

- **Δίκτυο κορμού ή δίκτυο διανομής (DS – Distribution System)**

Το δίκτυο κορμού είναι ένας γενικός όρος που περιγράφει το ενσύρματο δίκτυο που συνδέει πολλά ασύρματα σημεία πρόσβασης μεταξύ τους καθώς και με το υπόλοιπο ενσύρματο δίκτυο και το Internet.

## 6.6 Πρωτόκολλα στα Ασύρματα Δίκτυα

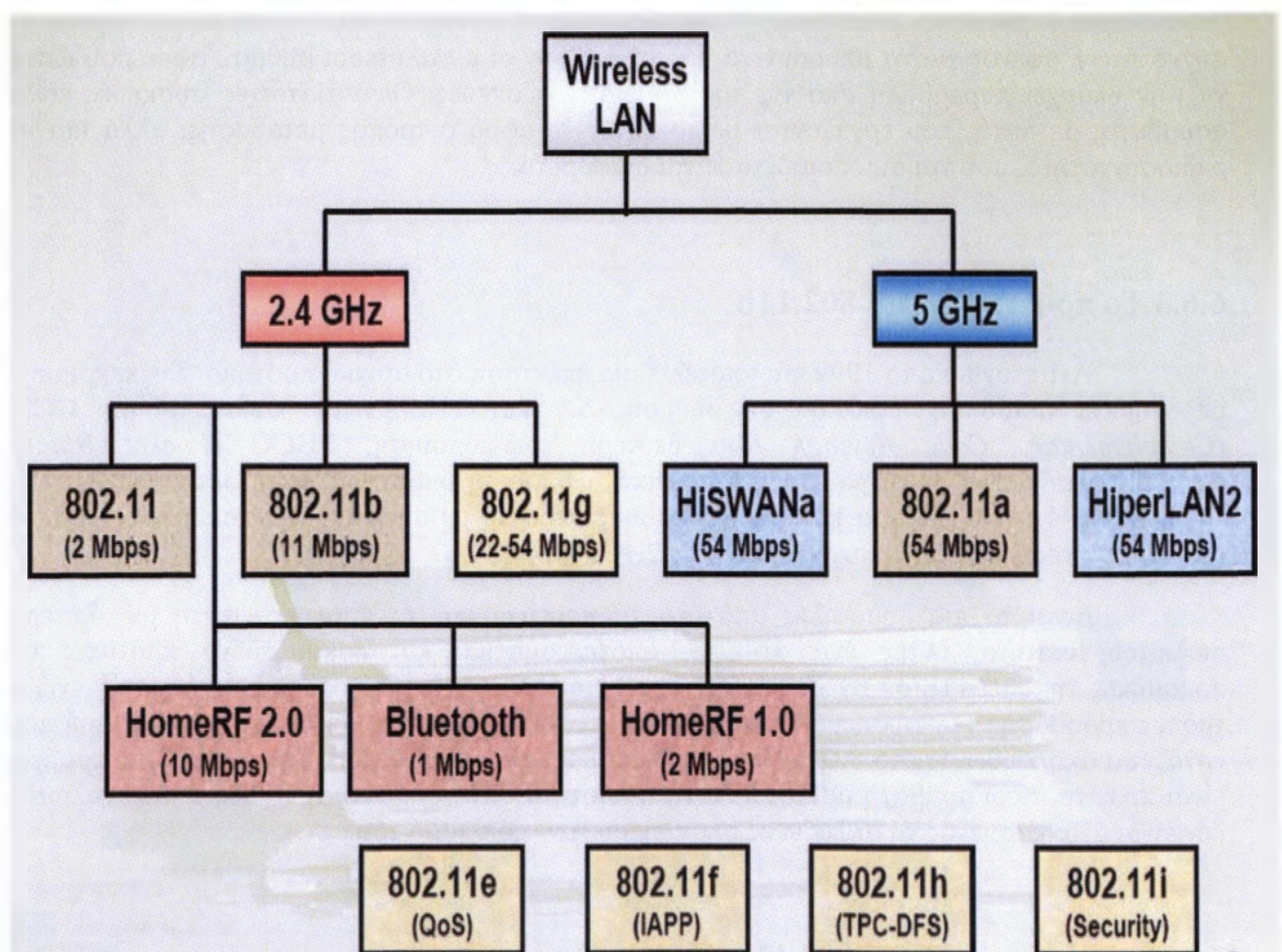
Ιστορία των WLANs	
1940	Η Τεχνολογία Διευρυμένου Φάσματος (Spread Spectrum) χρησιμοποιείται για πρώτη φορά.
1980	Περιορισμένες εφαρμογές χρησιμοποιώντας τεχνολογία στενής ζώνης
1989	Η FCC αναθέτει για εμπορική χρήση τις ISM μπάντες συχνοτήτων (900 MHz, 2.4 GHz, 5 GHz).
1990	Προϊόντα των 900 MHz βγαίνουν στην αγορά. Η IEEE αρχίζει να δουλεύει σε ένα πρότυπο WLAN.
1994	Προϊόντα των 2.4 GHz βγαίνουν στην αγορά.
1997	Το πρότυπο IEEE 802.11 εγκρίνεται.
1999	Επικύρωση των 802.11a και 802.11b. Οι Lucent, 3Com, Cisco, Intersil, Nokia, Symbol δημιουργούν τη WECA. Προϊόντα 802.11b βγαίνουν στην αγορά. 2000 - Η WECA ορίζει το Wi-Fi ως κοινό όνομα του 802.11b. Το Ευρυζωνικό Frequency Hopping WBFH (NPRM) εγκρίνεται από την FCC. Η ομάδα εργασίας του 802.11 βελτιώνει και ενισχύει το 802.11b. Η ομάδα εργασίας 802.11e δουλεύει σε θέματα ασφαλείας για τα Wi-Fi προϊόντα. Η ομάδα εργασίας 802.11f εξετάζει ενδο-AP πρωτόκολλο για τα Wi-Fi προϊόντα. Η ομάδα εργασίας 802.11e εξετάζει επεκτάσεις υψηλότερης ταχύτητας στο 802.11b. Η συμμετοχή στη WECA ξεπερνά τις 60 εταιρείες, με πάνω από 50 Wi-Fi πιστοποιημένα προϊόντα
>2000	Η ομάδα IEEE εργασίας 802.11 απελευθερώνει το πρότυπο 802.11g που πετυχαίνει ταχύτητες έως 54 Mbps στη ζώνη των 2.4 GHz.

Το Wi-Fi προέρχεται από τα αρχικά των «Wireless Fidelity» (Ασύρματη Πιστότητα) και έχει επικρατήσει σαν όρος για το υψηλής συχνότητας ασύρματο τοπικό δίκτυο (WLAN). Βασικά αποτελεί ένα ασύρματο τρόπο διασύνδεσης, ενώ δίνει την δυνατότητα σύνδεσης και με

το Internet. Οι ασύρματες τεχνολογίες πρόσβασης χρησιμοποιούνται για να αντικαταστήσουν ή να επεκτείνουν ένα κοινό ενσύρματο δίκτυο (Ethernet) και επιτρέπουν στον κινητό χρήστη την ασύρματη μετάδοση και λήψη δεδομένων.

Τα Ασύρματα Τοπικά Δίκτυα (WLANs) ακολουθούν το πρότυπο IEEE 802.11, το πρώτο πρότυπο για ασύρματη δικτύωση το οποίο αναπτύχθηκε. Τα ασύρματα τοπικά δίκτυα, τα οποία είναι συμβατά με το πρότυπο IEEE 802.11, ονομάζονται και δίκτυα Wi-Fi. Τα πρότυπα της οικογένειας 802.11 καθορίζουν τον έλεγχο πρόσβασης μέσου (MAC) και τα φυσικά στρώματα (PHY) για ένα LAN με ασύρματη σύνδεση. Ακόμη, εξετάζουν την τοπική δικτύωση όπου οι συνδεδεμένες συσκευές επικοινωνούν μέσω του αέρα με άλλες συσκευές που βρίσκονται κοντά ή μακριά. Τα πρωτόκολλα αυτά δημοσιεύονται από την IEEE γεγονός που είναι σημαντικό για την διαλειτουργικότητα, δηλαδή την ικανότητα συνεργασίας των συσκευών που το ακολουθούν. Στα πλαίσια της ανάπτυξης της οικογένειας των προτύπων IEEE 802.11, δημιουργήθηκαν διάφορες ομάδες εργασίας, που σκοπό είχαν την έρευνα και ανάπτυξη διαφορετικών χαρακτηριστικών των τεχνολογιών Wi-Fi.

Αυτές οι ομάδες είναι οι εξής:



### 6.6.1 Το πρότυπο IEEE 802.11

Το 1997, μετά από επτά χρόνια μελέτης, η IEEE δημοσίευσε το πρότυπο IEEE 802.11, το πρώτο πρότυπο για ασύρματη δικτύωση. Το πρότυπο αυτό προβλέπει ρυθμούς μετάδοσης 1 και 2 Mbps. Η μετάδοση γίνεται με ασύρματο τρόπο με χρήση διαμόρφωσης **FHSS** ή **DSSS** σε ζώνες συχνοτήτων 915MHz, 2.4GHz, 5.2GHz ή υπέρυθη μετάδοση στα 850nm ως 900nm. Υποστηρίζει δυνατότητες όπως προτεραιότητα της κίνησης, υποστήριξη εφαρμογών πραγματικού χρόνου και διαχείριση ισχύος συσκευής. Το πρότυπο γνώρισε περιορισμένη επιτυχία λόγω των πολύ χαμηλών ρυθμών μετάδοσης.

### 6.6.2 Το πρότυπο IEEE 802.11a

Το 1999 δημιουργήθηκε η επέκταση στο αρχικό πρότυπο που προβλέπει μετάδοση στη ζώνη συχνοτήτων U-NII των 5GHz με ρυθμούς μετάδοσης 1, 2, 5.5, 11, 6, 12, 24 Mbps και προαιρετικά 36, 48, 54 Mbps χρησιμοποιώντας **OFDM** (*Orthogonal Frequency Division Multiplexing*) διαμόρφωση. Η επέκταση αυτή αποσκοπούσε να καλύψει την ανάγκη για μεγαλύτερους ρυθμούς μετάδοσης. Επιλέχθηκε η λειτουργία σε μια υψηλότερη ζώνη συχνοτήτων, αφενός για να μπορούν να υποστηριχθούν οι μεγαλύτεροι ρυθμοί, αφετέρου ώστε να μην υπάρχει παρεμβολή από τις προηγούμενες συσκευές. Οι αντίστοιχες συσκευές είναι ασύμβατες με αυτές που εργάζονται με το 802.11b, αφού ο τρόπος μετάδοσης, αλλά και οι ραδιοσυχνότητες που χρησιμοποιούνται είναι διαφορετικές.

### 6.6.3 Το πρότυπο IEEE 802.11b

Αναπτύχθηκε το 1999 και αποτελεί μια επέκταση στο αρχικό πρότυπο. Συγκεκριμένα υποστηρίζει μετάδοση επιπλέον σε ρυθμούς 5.5 και 11Mbps με κωδικοποίηση **CCK** (*Complementary Code Keying*). Μια δεύτερη κωδικοποίηση, **PBCC** (*Packet Binary Convolutional Code*) ορίστηκε για προαιρετική υλοποίηση υποστηρίζοντας μετάδοση 5.5 και 11Mbps και έχοντας ελαφρά καλύτερη ευαισθησία δέκτη με αντίτιμο την πολυπλοκότητα. Η μετάδοση γίνεται στη ζώνη συχνοτήτων των 2.4GHz.

Είναι το πιο δημοφιλές από όλα τα πρότυπα και το πρότυπο με τη μεγαλύτερη διαλειτουργικότητα, όντας ένα στιβαρό, αποτελεσματικό και δοκιμασμένο πρότυπο. Οι προσθήκες της 802.11b σε σχέση με την 802.11 αφορούν μόνο τον τρόπο μετάδοσης, ενώ ο τρόπος πρόσβασης των συσκευών και οι τρόποι λειτουργίας μένουν οι ίδιοι. Μία συσκευή που εργάζεται ακολουθώντας το 802.11b, υλοποιεί και τους τρόπους μετάδοσης του 802.11 και έτσι είναι προς τα πίσω συμβατή με αυτό. Αυτή η ιδιότητα είναι σημαντική καθώς ο καταναλωτής δεν είναι αναγκασμένος να αλλάξει εξ ολοκλήρου τον εξοπλισμό του.

### 6.6.4 Το πρότυπο IEEE 802.11g

Πρόκειται για πρότυπο της οικογένειας 802.11 και έχει πρωτοτυποποιηθεί εδώ και πολλά χρόνια. Λειτουργεί στην μπάντα των 2,4GHz, όπως και το 802.11b και ουσιαστικά αποτελεί την εξέλιξή του. Χρησιμοποιεί τόσο την τεχνική διαμόρφωσης **DSSS** (*Direct Sequence Spread Spectrum*) με σκοπό να είναι συμβατό με το 802.11b, όσο και την **OFDM**

(*Orthogonal Frequency - Division Multiplexing*). Υποστηρίζονται ταχύτητες μεταφοράς δεδομένων 6, 9, 12, 18, 24, 36, 48 και 54Mbps. Πρόκειται για το πρότυπο το οποίο χρησιμοποιείται ευρέως τόσο στον εξοπλισμό των σταθμών βάσης όσο και στον καταναλωτικό εξοπλισμό. Παρέχει αυξημένη απόδοση σε σχέση με το 802.11b, υπάρχει σημαντικά μεγάλη εγκατεστημένη βάση και μπορεί να καλύψει ικανοποιητικές αποστάσεις.

Ένα σημαντικό χαρακτηριστικό είναι ότι πρόκειται για μια σχετικά οικονομική τεχνολογία, αφού υπάρχει μεγάλη εγκατεστημένη βάση και έντονος ανταγωνισμός. Επίσης, με το πέρασμα του χρόνου έχει δεχθεί μια σειρά από βελτιώσεις, ειδικά στα επίπεδα ευαισθησίας του δέκτη (-91dBm), χαρακτηριστικό εξαιρετικά σημαντικό, με αποτέλεσμα να θεωρείται μια ευσταθής (stable) και οικονομική τεχνολογία.

### 6.6.5 Το πρότυπο IEEE 802.11n

Πρόκειται για σχέδιο (draft) προτύπου της οικογένειας 802.11 και το οποίο βρίσκεται υπό εξέλιξη. Πρόκειται για εξέλιξη των υπάρχοντων προτύπων της οικογένειας 802.11 με σκοπό την αύξηση της ταχύτητας στα 540Mbps (πρακτικά περί τα 200Mbps) και της απόστασης μετάδοσης. Θα λειτουργεί στην μπάντα των 2,4GHz και θα χρησιμοποιεί την τεχνολογία MIMO (Multiple - input Multiple - output).

[www.amdpk.com](http://www.amdpk.com)

<b>802.11 Wireless Standards</b>					
<b>IEEE Standard</b>	<b>802.11a</b>	<b>802.11b</b>	<b>802.11g</b>	<b>802.11n</b>	<b>802.11ac (Draft)</b>
<b>Year Released</b>	1999	1999	2003	2009	2011 (Draft)
<b>Frequency</b>	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
<b>Max. Data Rate</b>	54 Mbps	11 Mbps	54 Mbps	600 Mbps	>1 Gbps
<b>Typical Range Indoors*</b>	100 ft.	100 ft.	125 ft.	225 ft.	TBD
<b>Typical Range Outdoors*</b>	400 ft.	450 ft.	450 ft.	825 ft.	TBD

## Πρακτικό Μέρος

Στο πρακτικό μέρος της διπλωματικής μου εργασίας, παρουσιάζουμε τα αποτελέσματα που έχουμε λάβει κάνοντας κάποια πειράματα μέσω *Ασύρματου Τοπικού Δικτύου (Wireless LAN)*. Πιο συγκεκριμένα, εξετάζουμε κάποιες παραμέτρους που συσχετίζονται με την τεχνολογία VoIP, όπως το *Jitter (τρέμουλο)* των πακέτων, *Packet Loss (Απώλεια Πακέτων)*, κλπ.

Για την επίτευξη του παραπάνω σκοπού, έχουμε πραγματοποιήσει κλήσεις VoIP χρησιμοποιώντας το πρόγραμμα **MicroSIP** για τις εξής περιπτώσεις:

- Ασύρματο τοπικό δίκτυο μεταξύ δύο υπολογιστών οι οποίοι βρίσκονται σε μικρή απόσταση μεταξύ τους (στο ίδιο δωμάτιο).
- Ασύρματο τοπικό δίκτυο μεταξύ δύο υπολογιστών οι οποίοι βρίσκονται σε σχετικά μεγάλη απόσταση μεταξύ τους (έξω από το δωμάτιο).
- Συνομιλία μεταξύ δύο υπολογιστών οι οποίοι είναι συνδεδεμένοι στο ασύρματο ιδιωτικό δίκτυο CYTA096962.

### Ο εξοπλισμός που χρειάστηκε είναι:

#### 1) Για τον πρώτο χρήστη:

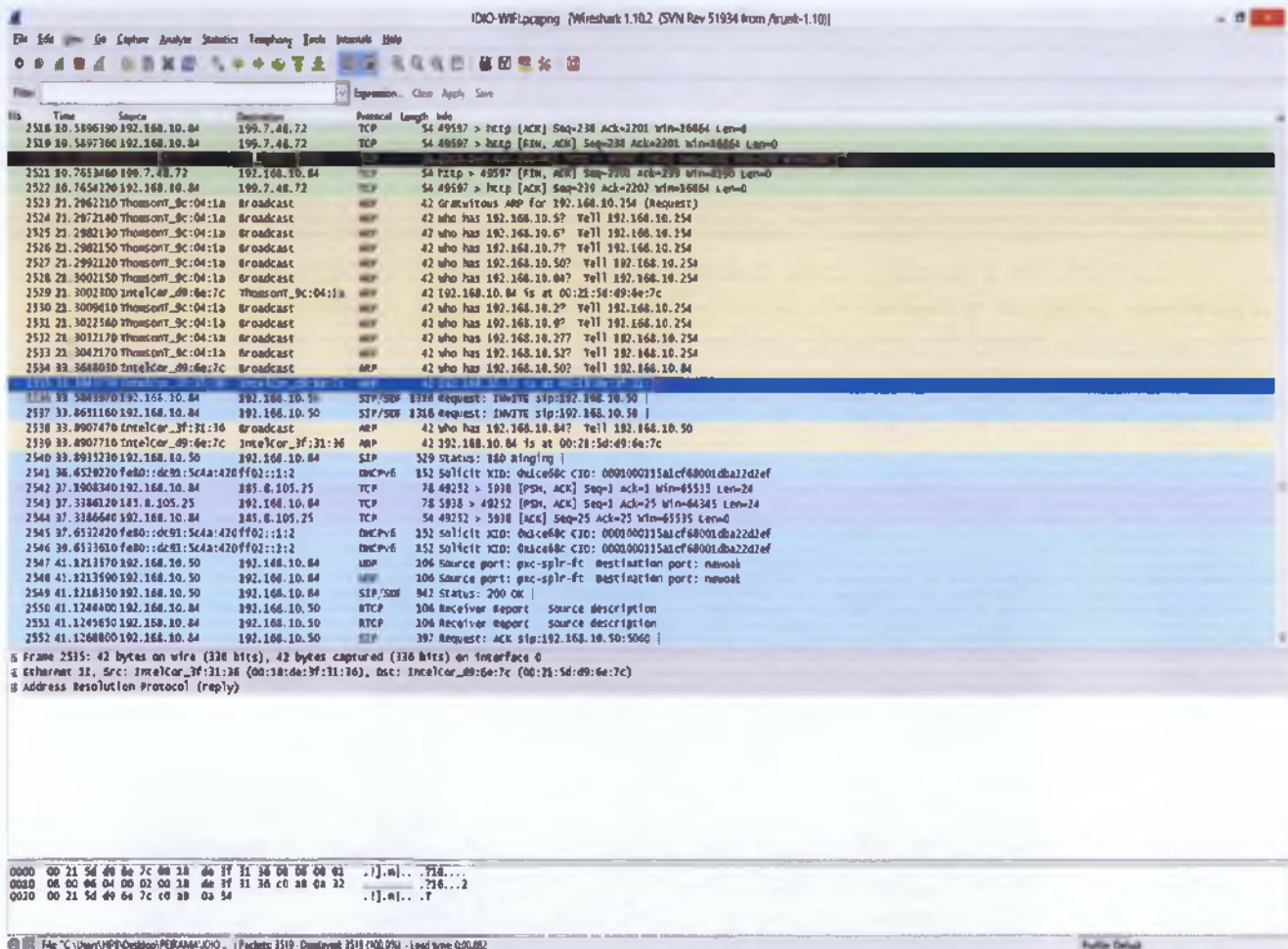
- PC Intel® Core™ 2 DUO P8600 (2.40GHz, 4096 MB)
- Realtek High Definition Audio
- Απλό μικρόφωνο
- Marvel Yukon 88E8055 PCI-E Gigabit Ethernet Controller
- Intel®WiFi Link 5100 AGN

#### 2) Για το δεύτερο χρήστη:

- PC Intel® Core™ 2 T7200 (2.00GHz, 2048 MB)
- Κάρτα ήχου
- Απλό μικρόφωνο
- Intel ® Pro Wireless 3945ABG
- Marvell Yukon 88E8036 PCI Fast Ethernet Controller

Οι μετρήσεις έχουν γίνει με το πρόγραμμα **Wireshark** το οποίο αποτελεί ένα από τα διασημότερα προγράμματα παγκοσμίως για την ανάλυση των δικτύων. Αυτό το πολύ δυνατό εργαλείο παρέχει πληροφορίες για το δίκτυο μας και των πρωτοκόλλων ανώτερου επιπέδου

σχετικά με τα δεδομένα που διακινούνται σ' αυτό. Αποτελεί τον πιο διάσημο *Packet Sniffer & Network Analyzer* που κυκλοφορεί.



## Το πρόγραμμα Wireshark

Το **Wireshark** χρησιμοποιεί τη δικτυακή βιβλιοθήκη *pcap* για την σύλληψη (ανάλυση) των πακέτων. Το εργαλείο αυτό ανήκει στη κατηγορία των *packet-sniffer*. Όπως υπονοεί και το όνομα ο *sniffer* συλλαμβάνει τα μηνύματα που στέλνονται ή λαμβάνονται από τον υπολογιστή σας. Επιτρέπει στο χρήστη να παρακολουθήσει όλη την κίνηση που γίνεται στο δίκτυο θέτοντας την κάρτα δικτύου σε λειτουργία *promiscuous* (ανάμεικτη) για να δει όλη την κίνηση που είναι ορατή σε αυτή, όχι μόνο την κίνηση που απευθύνεται σε μια από τις ρυθμισμένες διευθύνσεις της και την *broadcast/multicast* κυκλοφορία.

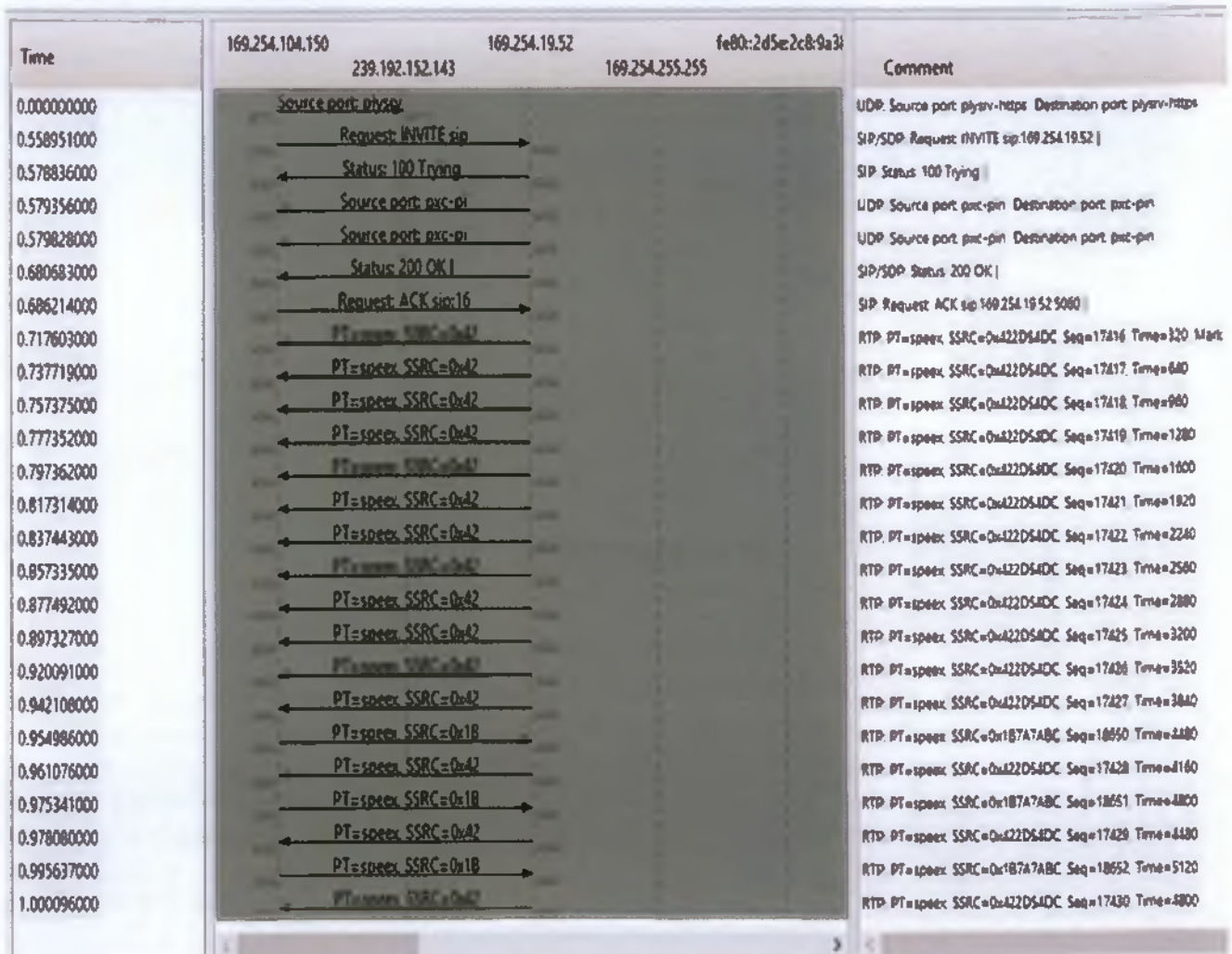
Αυτές οι πληροφορίες παρουσιάζονται στη συνέχεια σε γραφικό περιβάλλον. Στη συνέχεια, θα παρουσιάσουμε αναλυτικά τα αποτελέσματα για τις τρεις παραπάνω περιπτώσεις καθώς και συγκρίσεις μεταξύ των διάφορων παραμέτρων που μας ενδιαφέρουν. Σε όλες τις περιπτώσεις έχει χρησιμοποιηθεί η κωδικοποίηση **ITU-T G.711 PCMU**.

## Περιπτώσεις

### 1<sup>η</sup> Περίπτωση: Στο ίδιο δωμάτιο

Μετά τη δημιουργία ενός ασύρματου τοπικού δικτύου μεταξύ των δύο χρηστών (μέσω των ασύρματων καρτών των 2 LAPTOPs), χρησιμοποιούμε το πρόγραμμα MicroSIP για την πραγματοποίηση της ομιλίας και το πρόγραμμα Wireshark για την καταγραφή των απαιτούμενων μετρήσεων.

Από την VoIP ανάλυση λαμβάνουμε το παρακάτω διάγραμμα:



### VoIP Graph Analysis

Στο παραπάνω διάγραμμα παρατηρούμε τα χαρακτηριστικά της κλήσης που έχουμε



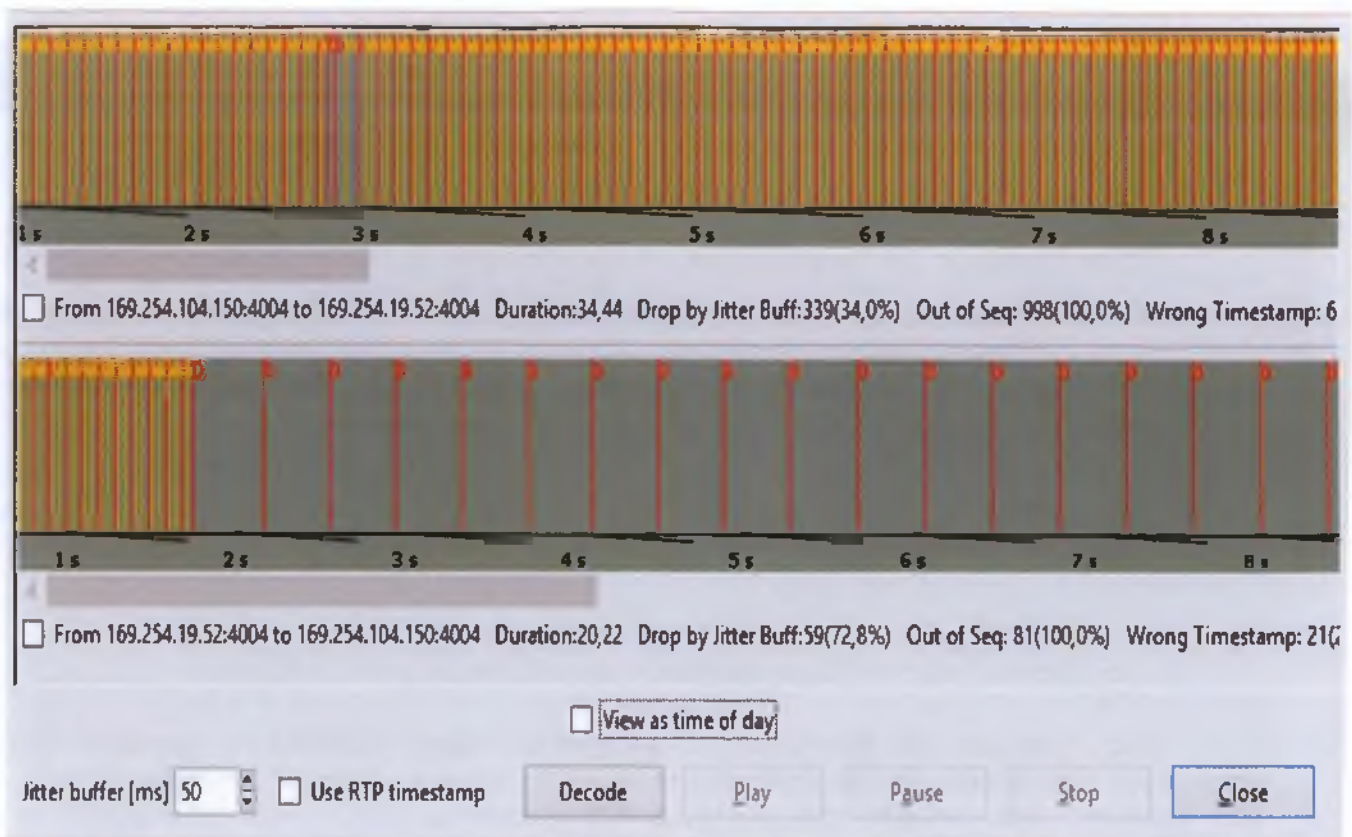
πραγματοποιήσει. Πιο συγκεκριμένα, διακρίνουμε τέσσερις στήλες.

Αυτές είναι οι:

- **Time (χρόνος):** Τα στοιχεία που περιέχονται στη στήλη αυτή είναι οι εκάστοτε χρονικές στιγμές κατά τις οποίες γίνεται αποστολή/λήψη πακέτων.
- **IP address (IP διεύθυνση -1):** Πρόκειται για την IP διεύθυνση του πρώτου υπολογιστή (στη συγκεκριμένη περίπτωση είναι η 169.254.104.150).
- **IP address (IP διεύθυνση -2):** Πρόκειται για την IP διεύθυνση του δεύτερου υπολογιστή (στη συγκεκριμένη περίπτωση είναι η 169.254.19.52).
- **Comment (Σχόλιο):** Στη στήλη αυτή αναγράφονται τα διάφορα σχόλια που αφορούν στην επικοινωνία των δύο υπολογιστών και στα πακέτα που μεταδίδονται.

Πιο συγκεκριμένα, βλέπουμε ότι τη χρονική στιγμή 0,5588, το τερματικό (1) αποστέλλει ένα πακέτο, δηλώνοντας την επιθυμία να επικοινωνήσει με το τερματικό (2). Στη συνέχεια, αφού δηλωθεί στο τερματικό (2) η επιθυμία του (1) για επικοινωνία, τη χρονική στιγμή 0,717 γίνεται η αποδοχή της κλήσης. Έτσι, στη συνέχεια ξεκινάει η συνομιλία και η ανταλλαγή των πακέτων.

Επίσης, το ίδιο το πρόγραμμα μας παρέχει τη δυνατότητα να αναπαράγουμε τη συνομιλία που έχει πραγματοποιηθεί μεταξύ των δύο χρηστών, όπως βλέπουμε στο παρακάτω σχήμα:



## RTP Player

Στη συνέχεια, αναζητούμε τα RTP Streams που έχουν προκύψει, από το μενού RTP Analysis, και επιλέγουμε Show RTP Streams, όπου και λαμβάνουμε αναλυτικά στοιχεία όσον αφορά Source και Destination IP, Ports, Κωδικοποίηση, ποσοστό χαμένων πακέτων, Delta και Jitter, σε δύο κατευθύνσεις Forward και Reversed, όπως φαίνεται παρακάτω σχήμα:

Detected 2 RTP streams. Choose one for forward and reverse direction for analysis

Src addr	Src port	Dst addr	Dst port	SSRC	Payload	Packets	Lost
169.254.104.150	4004	169.254.19.52	4004	0x1B7A7ABC	speex	998	0 (0,0%)
169.254.19.52	4004	169.254.104.150	4004	0x422D54DC	speex	81	0 (0,0%)

Select a forward stream with left mouse button, and then  
Select a reverse stream with Ctrl + left mouse button

## RTP Streams

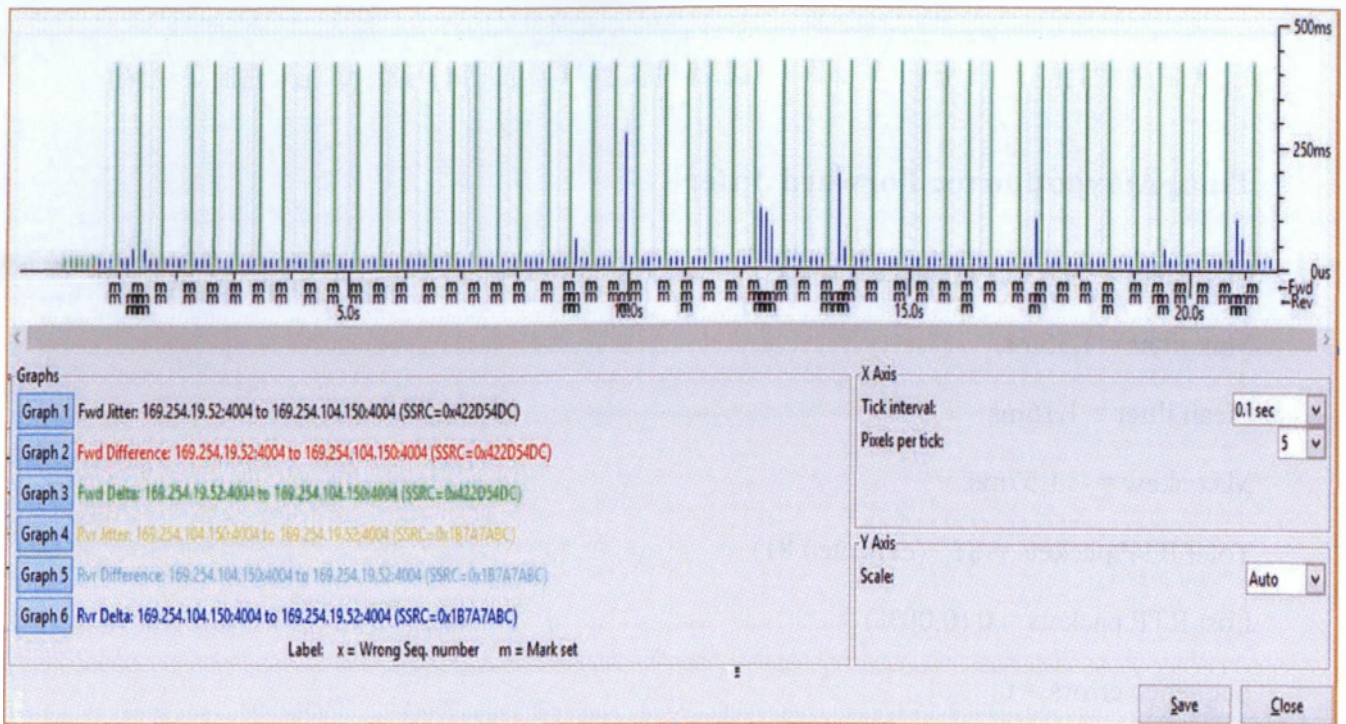
Επιλέγοντας λοιπόν, το Forward Stream και το Reversed stream και πατώντας Analyze ανοίγει καινούργιο παράθυρο RTP Stream Analysis με τις παραμέτρους: Packet, Sequence, Delta (ms), Jitter (ms), Bandwidth (kbps), marker και τέλος Status, και στις δύο κατευθύνσεις σχήμα:

Forward Direction		Reversed Direction					
Analysing stream from 169.254.19.52 port 4004 to 169.254.104.150 port 4004 SSRC = 0x422D54DC							
Packet	Sequence	Delta(ms)	Filtered Jitter(ms)	Skew(ms)	IP BW(kbps)	Marker	Status
8	17416	0,00	0,00	0,00	0,88	SET	[ Ok ]
9	17417	20,12	0,01	-0,12	1,76		[ Ok ]
10	17418	19,66	0,03	0,23	2,64		[ Ok ]
11	17419	19,98	0,03	0,25	3,52		[ Ok ]
12	17420	20,01	0,03	0,24	4,40		[ Ok ]
13	17421	19,95	0,03	0,29	5,28		[ Ok ]
14	17422	20,13	0,03	0,16	6,16		[ Ok ]
15	17423	19,89	0,04	0,27	7,04		[ Ok ]
Max delta = 29,03 ms at packet no. 61 Max jitter = 1,35 ms. Mean jitter = 1,16 ms. Max skew = -11,57 ms. Total RTP packets = 81 (expected 81) Lost RTP packets = 0 (0,00%) Sequence errors = 0 Duration 21,21 s (-36 ms clock drift, corresponding to 15973 Hz (-0,17%))							
Save payload...		Save as CSV...		Refresh		Jump to	
Graph		Player		Next non-Ok		Close	

### RTP Stream Analysis (Forward Direction)

Επίσης, η παράμετρος **Delta** παριστάνει το χρονικό διάστημα που μεσολαβεί ανάμεσα σε δύο διαδοχικές μεταδόσεις πακέτων. Η παράμετρος **Jitter** ονομάζεται «τρέμουλο» και παριστάνει τη διακύμανση του χρόνου μεταφοράς ενός πακέτου από άκρο σε άκρο. Είναι το διπλάσιο του αριθμού των msec που μπορεί να κυμανθεί η καθυστέρηση ενός πακέτου ως προς το μέσο όρο. Έτσι, η τιμή 2 msec σημαίνει ότι ένα πακέτο μπορεί να είναι μέχρι 1msec μπροστά ή πίσω από το μέσο όρο, αλλά όχι περισσότερο.

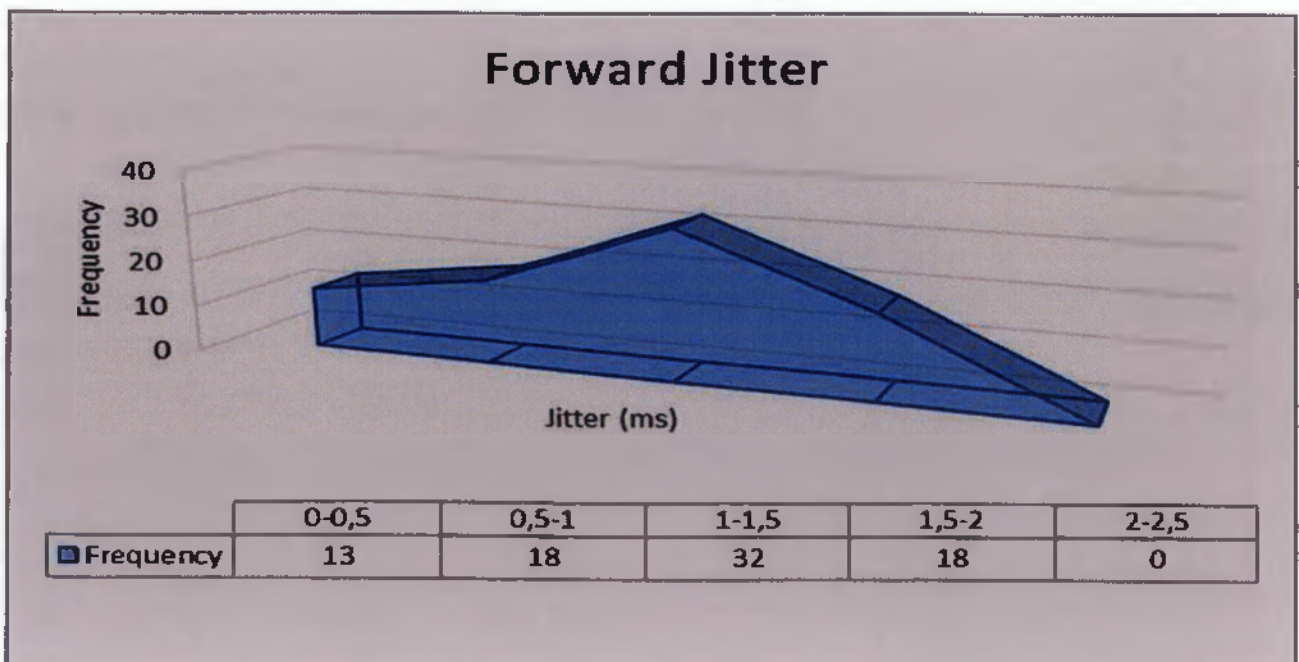
Το παράθυρο, όπως εύκολα μπορεί να διαπιστώσει κανείς, μας δίνει επιπλέον πληροφορίες για την αλληλουχία των πακέτων, το bandwidth, την επιτυχή ή μη άφιξη των πακέτων, καθώς και ορισμένα γενικά στατιστικά της επικοινωνίας. Με την κατάλληλη επεξεργασία των δεδομένων, παρουσιάζουμε γραφικά τις παραπάνω παραμέτρους, έτσι ώστε να γίνει η εστίαση σε κάποιες λεπτομέρειες που δεν φαίνονται, όπως θα δούμε στη συνέχεια:



## RTP Graph Analysis (Forward & Reversed)

Αυτό που κάνουμε είναι να εξάγουμε τα δεδομένα στο Excel και τα κατατάσσουμε σε κατάλληλες κατηγορίες όπως βλέπουμε στα παρακάτω διαγράμματα για το **Forward** και **Reversed Jitter**:

**Forward Jitter: 169.254.104.150:4004 → 169.254.19.52:4004**



## Τιμές Διαγράμματος Forward Jitter

Max delta = 29,03ms at packet no. 61

Max jitter = 1,35ms.

Mean jitter = 1,16ms.

Max skew = -11,57ms.

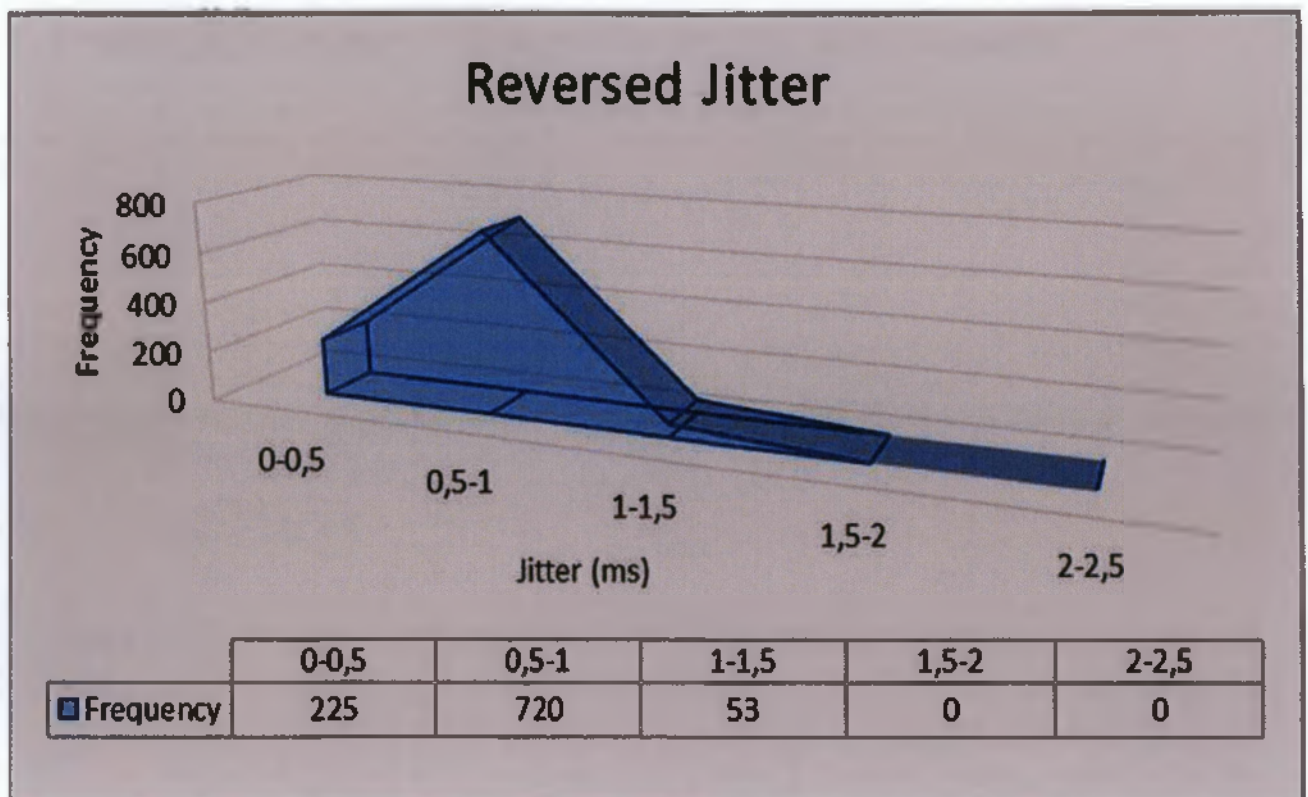
Total RTP packets = 81 (expected 81)

Lost RTP packets = 0 (0,00%)

Sequence errors = 0

Duration 21,21s (-36 ms clock drift, corresponding to 15973 Hz (-0,17%))

**Reversed Jitter: 169.254.19.52:4004 → 169.254.104.150:4004**



## Τιμές Διαγράμματος Reversed Jitter

Max delta = 21,26ms at packet no. 870

Max jitter = 1,21ms.

Mean jitter = 0,63ms.

Max skew = 9,12ms.

Total RTP packets = 998 (expected 998)

Lost RTP packets = 0 (0,00%)

Sequence errors = 0

Duration 21,35s (-6 ms clock drift, corresponding to 15995 Hz (-0,03%))

Συμπεραίνουμε ότι η κλήση ήταν πολύ καλής ποιότητας με 0% χαμένα πακέτα και στις δύο κατευθύνσεις και μέσο όρο *Jitter* 1.16 ms και 0.63 ms για την ορθή (*forward*) και ανάστροφη (*reversed*) κατεύθυνση αντίστοιχα. Παρατηρούμε ότι στην πρώτη περίπτωση, το *Jitter* είναι συνεχώς πάνω από 0,5 msec, ενώ το *Jitter* της συντριπτικής πλειοψηφίας των πακέτων είναι ανάμεσα στα 1 ms και στα 1.5 ms.

**Αντίθετα**, στη δεύτερη περίπτωση, οι τιμές του *Jitter* είναι κατανομημένες σε μεγάλη πλειοψηφία μεταξύ 0.5 - 1 ms.

## 2<sup>η</sup> Περίπτωση: Έξω από το δωμάτιο

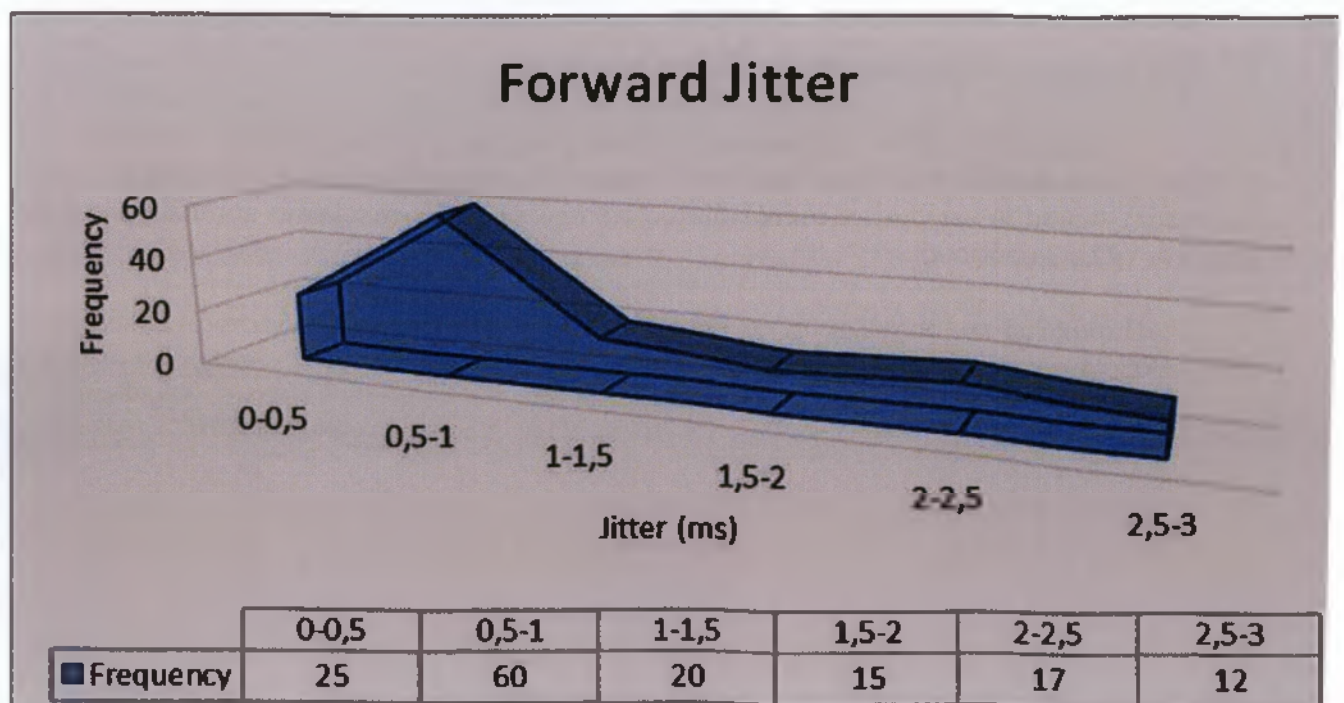
Προχωράμε στην εξέταση της δεύτερης περίπτωσης, όπου έχουμε μεταφέρει τα 2 Laptops σε διαφορετικό χώρο από αυτό, χωρίς να υπάρχει οπτική επαφή μεταξύ τους. Και πάλι στήσαμε ασύρματο τοπικό δίκτυο μεταξύ τους, σε τοποθεσία που απέχει ο ένας από τον άλλο 3 ορόφους.

Παρακάτω παρουσιάζονται τα αποτελέσματα του δεύτερου πειράματος. Η ερμηνεία του κάθε σχήματος είναι η ίδια με την προηγούμενη περίπτωση.

Time	169.254.104.150	169.254.255.255	fe80::2d5e:2c8:9a3b	#02::1:2	MonHaiPr_b9:ba:2	Comment
0.00000000	Name query NB WORKG					NBNS Name query NB WORKGROUP<1c>
0.755328000	Name query NB WORKG					NBNS Name query NB WORKGROUP<1c>
0.852136000			Source IP: 0x7b83			D=CPv6 Source XID: 0x7b83e CID: 0001000110011a330
1.507877000	Name query NB WORKG					NBNS Name query NB WORKGROUP<1c>
3.955712000	Name query NB WORKG					NBNS Name query NB WORKGROUP<1c>
4.708425000	Name query NB WORKG					NBNS Name query NB WORKGROUP<1c>
5.459558000	Name query NB WORKG					NBNS Name query NB WORKGROUP<1c>
5.767321000					Who has	ARP Who has 169.254.19.52? Tell 169.254.104.150
5.769693000						ARP 169.254.19.52 is at e84e 08 08 04 8f
5.769751000					Request: INVITE sip	SIP/SDP Request INVITE sip 169.254.19.52
5.789116000						ARP Who has 169.254.104.150? Tell 169.254.19.52
5.789151000						ARP 169.254.104.150 is at 0c ee ed b0 ba 21
5.789951000					Status: 100 Trying	SIP Status 100 Trying
5.801681000					Source port: network	UDP Source port: network Destination port: pxt-spr
5.802274000					Source port: network	UDP Source port: network Destination port: pxt-spr
6.037818000					Status: 200 OK	SIP/SDP Status 200 OK
6.046248000					Request: ACK sip:16	SIP Request ACK sip 169.254.19.52:5060
6.074610000					PT=speex SSRC=0x294823	RTP PT=speex SSRC=0x294823 Seq=8013 Time=320
6.094133000					PT=speex SSRC=0x29	RTP PT=speex SSRC=0x294823 Seq=8014 Time=640
6.114469000					PT=speex SSRC=0x29	RTP PT=speex SSRC=0x294823 Seq=8015 Time=960
6.132815000					PT=speex SSRC=0x29	RTP PT=speex SSRC=0x294823 Seq=8016 Time=1280
6.153150000					PT=speex SSRC=0x29	RTP PT=speex SSRC=0x294823 Seq=8017 Time=1600
6.172718000					PT=speex SSRC=0x29	RTP PT=speex SSRC=0x294823 Seq=8018 Time=1920

## Graph Analysis

Forward Jitter: 169.254.104.150:4002 → 169.254.19.52:4002





## Τιμές Διαγράμματος Forward Jitter

Max delta = 20,61 ms at packet no. 118

Max jitter = 2,68ms.

Mean jitter = 0,65ms.

Max skew = 10,75ms.

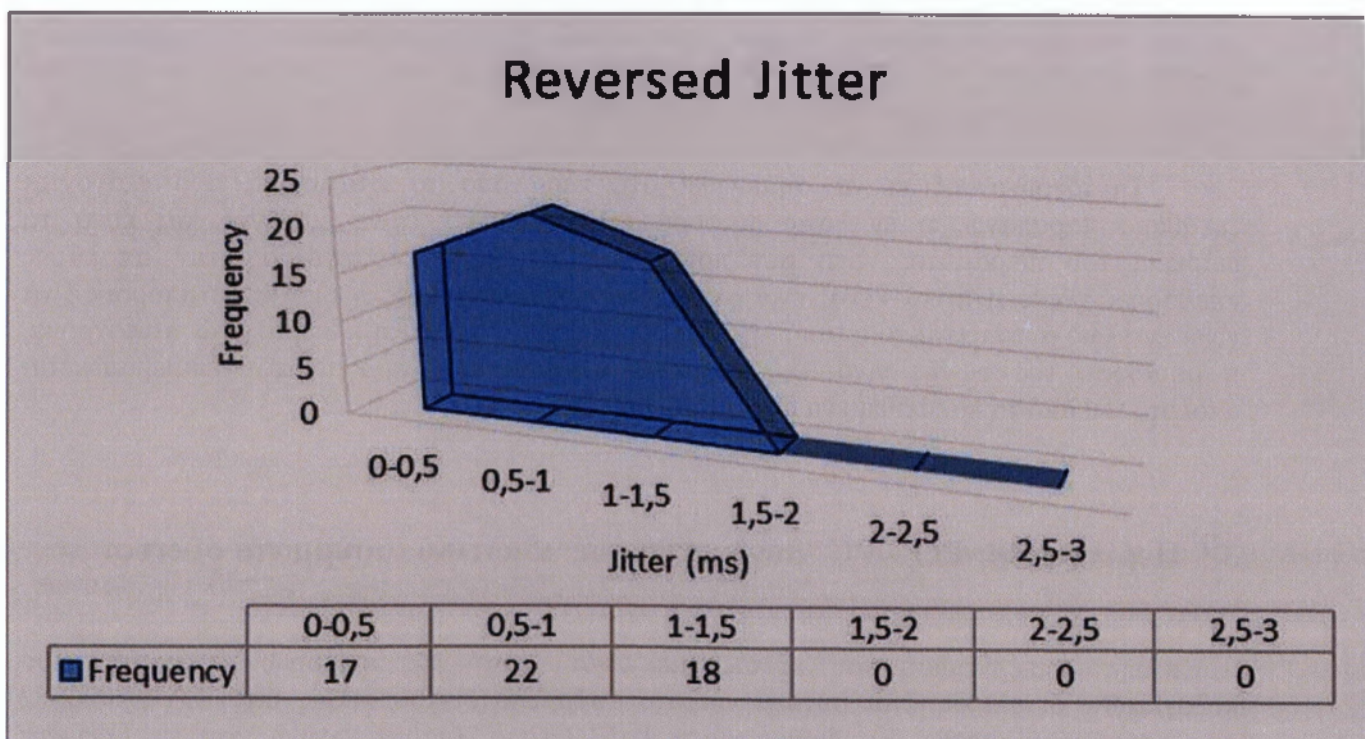
Total RTP packets = 149 (expected 149)

Lost RTP packets = 0 (0,00%)

Sequence errors = 0

Duration 10,95 s (-440 ms clock drift, corresponding to 15356 Hz (-4,02%))

**Reversed Jitter: 169.254.19.52:4002 → 169.254.104.150:4002**



## Τιμές Διαγράμματος Reversed Jitter

Max delta = 25,59 ms at packet no. 73

Max jitter = 0,76ms.

Mean jitter = 0,77ms.

Max skew = -8,15ms.

Total RTP packets = 57 (expected 57)

Lost RTP packets = 0 (0,00%)

Sequence errors = 0

Duration 11,13 s (-782 ms clock drift, corresponding to 14875 Hz (-7,03%))

Συμπεραίνουμε ότι η συνομιλία σε αυτήν την περίπτωση ήταν μέτριας ποιότητας, με 0% χαμένα πακέτα και 0,65 ms μέσο όρο *Jitter* από την πλευρά του πρώτου χρήστη, και 0% χαμένα πακέτα και 0,77 ms μέσο όρο *Jitter* από την πλευρά του δεύτερου.

Όπως και στο πρώτο πείραμα, έτσι και εδώ, παρατηρούμε ότι στην ανάστροφη φορά, το *Jitter* εμφανίζει μεγαλύτερη διακύμανση σε σχέση με την ορθή φορά. Μάλιστα, στην ανάστροφη περίπτωση, βλέπουμε ξεκάθαρα ότι το *Jitter* παίρνει τιμές που φτάνουν και τα 1,5 msec, πράγμα που δείχνει σαφώς χαμηλότερη ποιότητα επικοινωνίας.

Παρατηρώντας τα δύο πειράματα, εύκολα μπορεί να παρατηρήσει κανείς ότι στην περίπτωση που ο ένας υπολογιστής βρίσκεται απομακρυσμένος από τον άλλο, η επικοινωνία είναι σαφώς χειρότερη από αυτή που οι δύο υπολογιστές βρίσκονται δίπλα. Το συμπέρασμα αυτό είναι απολύτως λογικό, διότι η μεγάλη απόσταση των υπολογιστών, σε συνδυασμό με την ύπαρξη των δομικών υλικών που παρεμβάλλονται ανάμεσά τους, προκαλεί τη μεγάλη εξασθένιση του σήματος. Οι παραπάνω μετρήσεις μας δίνουν και μια ποσοτική εικόνα της ελάττωσης της ποιότητας της επικοινωνίας.

Ταυτόχρονα, αξίζει να σημειωθεί ότι, πέρα από τα στατιστικά που φαίνονται ξεκάθαρα παραπάνω, η εν λόγω διαφορά στην ποιότητα έγινε εμφανής και κατά τη διάρκεια του πειράματος. Στη μεν πρώτη περίπτωση, η επικοινωνία ήταν απολύτως «καθαρή», χωρίς ηχητικά κενά, ενώ στη δεύτερη, πολλές φορές η ομιλία δε μπορούσε να γίνει εντελώς αντιληπτή, τόσο από τη μία, όσο και από την άλλη πλευρά, ενώ ταυτόχρονα, η μετάδοση της φωνής γινόταν με αρκετή καθυστέρηση, πράγμα που επιβεβαιώνεται απόλυτα και από τα παρατιθέμενα διαγράμματα.

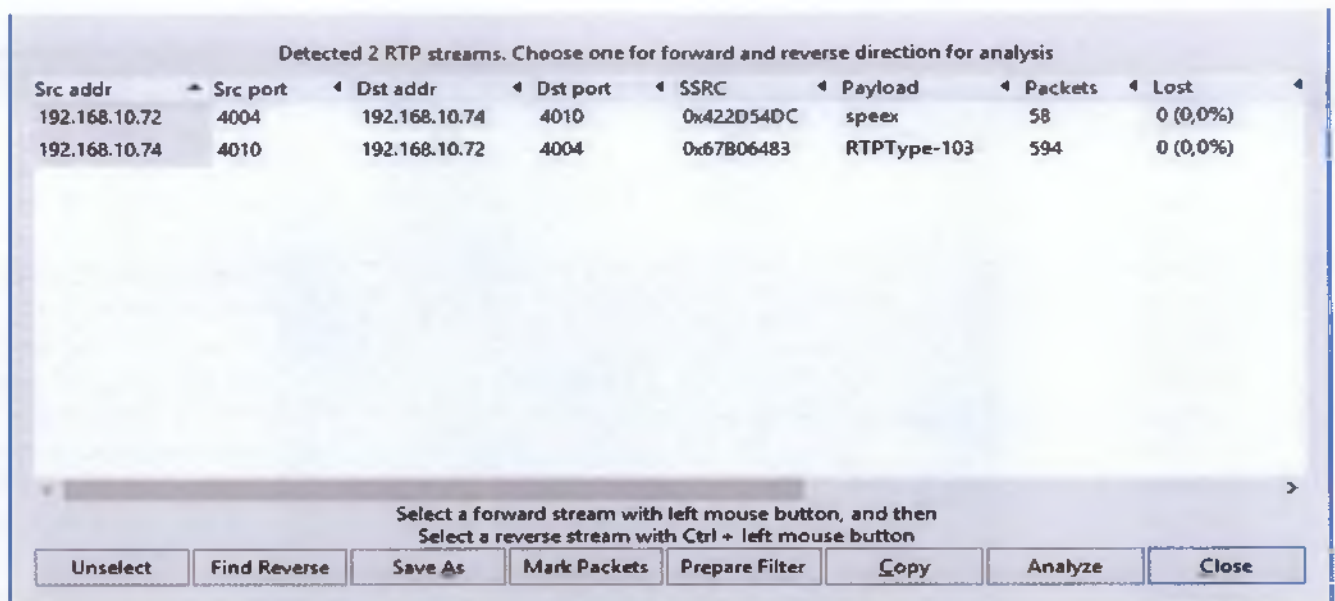
### **3<sup>η</sup> Περίπτωση: PC – PC συνδεδεμένοι σε ιδιωτικό ασύρματο δίκτυο.**

Η τελευταία περίπτωση που εξετάζουμε είναι αυτή της επικοινωνίας μεταξύ δύο υπολογιστών, οι οποίοι είναι συνδεδεμένοι στο ασύρματο δίκτυο οικίας μας CYTA096962 μέσω ασύρματων καρτών. Τα διαγράμματα *VoIP Graph Analysis*, καθώς και τα *Forward & Reversed Jitter* παρουσιάζονται παρακάτω:

Time	FujitsuS_a3:28:4b	Broadcast	54.236.217.42	192.168.10.74	192.168.10.80	Comment
0.00000000						ARP: Who has 192.168.1.10? Tell 192.168.10.72
1.228476000						ARP: Who has 192.168.1.10? Tell 192.168.10.72
1.520550000						HTTP: Continuation of non-HTTP traffic
1.520986000						HTTP: Continuation of non-HTTP traffic
1.521076000						TCP: 50827 > http [ACK] Seq=1 Ack=57 Win=62 Len=0
1.521271000						TCP: 50827 > http [FIN ACK] Seq=1 Ack=57 Win=62 Len=0
1.537128000						BROWSER: Become Backup Browser
1.689518000						TCP: http > 50827 [RST] Seq=57 Win=0 Len=0
1.982363000						TCP: 50836 > http [SYN] Seq=0 Win=8192 Len=0 MSS=14
2.150082000						ARP: Who has 192.168.1.10? Tell 192.168.10.72
2.162413000						TCP: http > 50836 [SYN ACK] Seq=0 Ack=1 Win=5840 Len=0
2.162568000						TCP: 50836 > http [ACK] Seq=1 Ack=1 Win=16384 Len=0
2.162967000						HTTP: GET /v3.1/collection/30430082/7382667857549912/?
2.359694000						TCP: http > 50836 [ACK] Seq=1 Ack=841 Win=5120 Len=0
2.361497000						TCP: [TCP segment of a reassembled PDU]
2.411503000						TCP: 50836 > http [ACK] Seq=841 Ack=495 Win=15872 Len=0
3.072975000						NBNS: Name query NB NIKOS-PC<20>
3.073986000						ARP: Who has 192.168.1.10? Tell 192.168.10.72
3.282918000						SNMP: get-request 1.3.6.1.2.1.25.3.2.1.5.1.1.3.6.1.2.1.25.3.5.1.1
3.379102000						ARP: Who has 192.168.1.20? Tell 192.168.1.254
3.686484000						NBNS: Name query NB NIKOS-PC<20>
4.301032000						ARP: Who has 192.168.1.20? Tell 192.168.1.254
4.608091000						NBNS: Name query NB NIKOS-PC<20>

## Graph Analysis

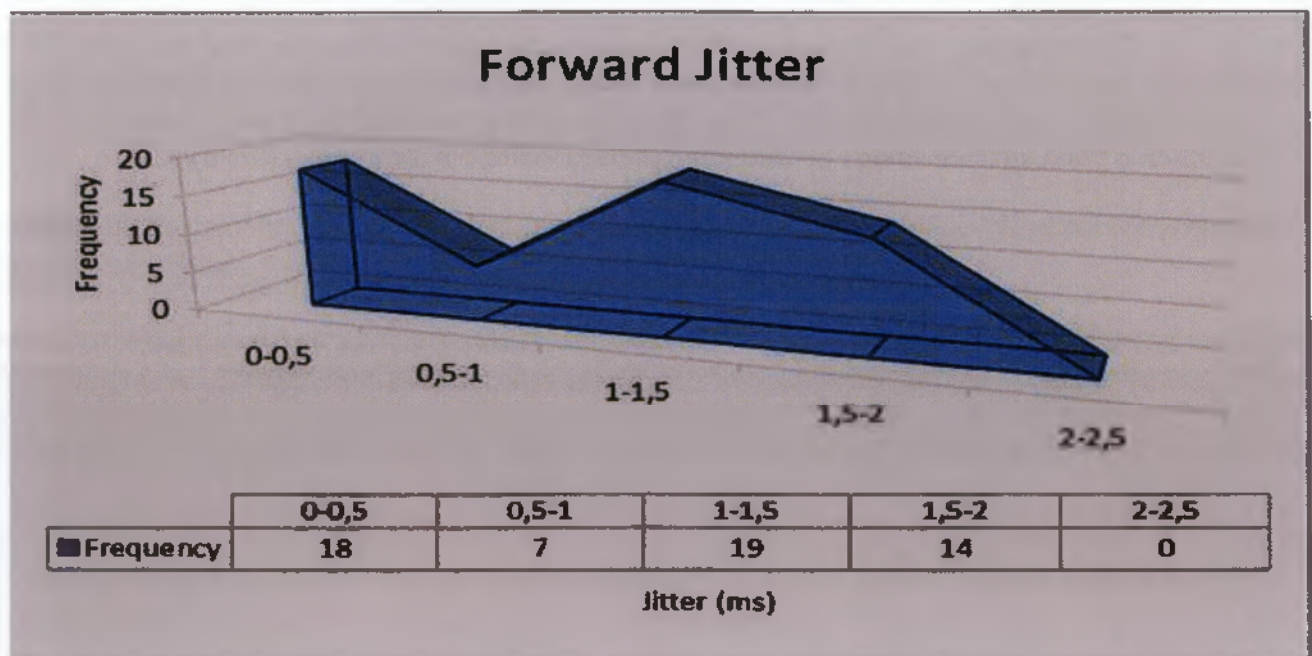
Στη συνέχεια, αναζητούμε τα RTP Streams που έχουν προκύψει, από το μενού RTP Analysis, και επιλέγουμε Show RTP Streams, όπου και λαμβάνουμε αναλυτικά στοιχεία όσον αφορά Source και Destination IP, Ports, Κωδικοποίηση, ποσοστό χαμένων πακέτων, Delta και Jitter, σε δύο κατευθύνσεις Forward και Reversed, όπως φαίνεται παρακάτω σχήμα:



## RTP Streams

Στα σχήματα φαίνεται η κατανομή του Jitter για ορθή και ανάστροφη φορά, ακριβώς όπως και στις προηγούμενες δύο περιπτώσεις.

**Forward Jitter: 192.168.10.74:4010 → 192.168.10.72:4004**



## Τιμές Διαγράμματος Forward Jitter

Max delta = 27,29ms at packet no. 105

Max jitter = 1,54ms.

Mean jitter = 1,26ms.

Max skew = -10,11ms.

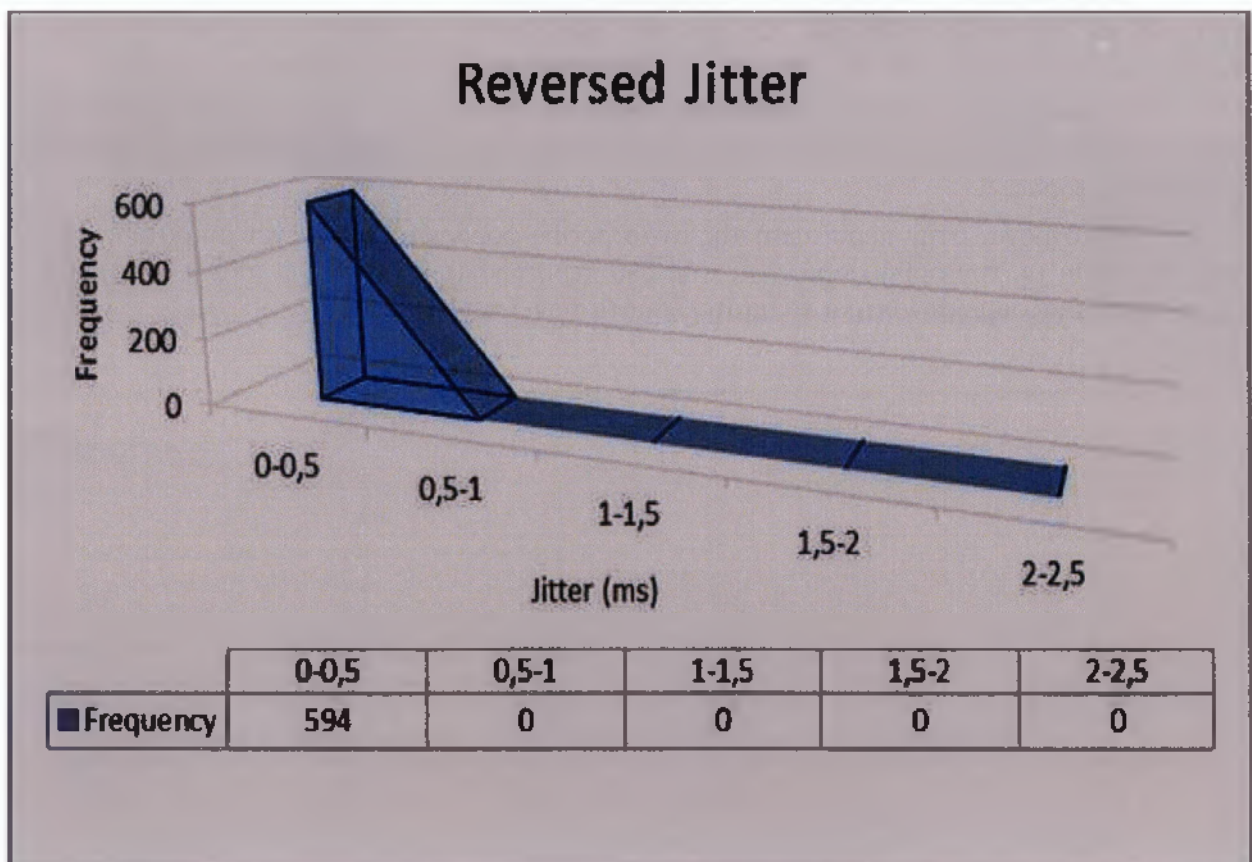
Total RTP packets = 58 (expected 58)

Lost RTP packets = 0 (0,00%)

Sequence errors = 0

Duration 11,55s (-1751 ms clock drift, corresponding to 13574 Hz (-15,16%))

### Reversed Jitter: 192.168.10.72:4004 → 192.168.10.74:4010



## Τιμές Διαγράμματος Reversed Jitter

Max delta = 0,00ms at packet no. 0

Max jitter = 0,00ms.

Mean jitter = 0,00ms.

Max skew = 0,00ms.

Total RTP packets = 594 (expected 594)

Lost RTP packets = 0 (0,00%)

Sequence errors = 0

Duration 11,97s (0 ms clock drift, corresponding to 1 Hz (+0,00%))

Η επικοινωνία στο τελευταίο πείραμα είχε πολύ καλή ποιότητα, με 0% χαμένα πακέτα και μέση τιμή για το *Jitter* ίσο με 1,26 ms στην περίπτωση της ορθής φοράς και 0% χαμένα πακέτα και μέση τιμή για το *Jitter* 0 ms στην περίπτωση της ανάστροφης φοράς.

Παρατηρούμε και πάλι λοιπόν, στο τρίτο αυτό πείραμα, ότι στην περίπτωση της ορθής φοράς, το *Jitter* παρουσιάζει σαφώς μεγαλύτερη διακύμανση από την περίπτωση της ανάστροφης φοράς.

Ταυτόχρονα, στην περίπτωση της ανάστροφης φοράς, το *Jitter* έχει μικρότερη μέση τιμή, σε σχέση με την ορθή φορά. Και στις δυο περιπτώσεις δεν υπάρχει απώλεια πακέτων. Τέλος, παρουσιάζουμε συνοπτικά τα αποτελέσματα των 3 πειραμάτων.

## ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ ΤΩΝ 3 ΠΕΙΡΑΜΑΤΩΝ

	Lost RTP Packets (%)	Sequence Errors	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)
Ίδιο Δωμάτιο (Forward)	0	0	29.03	1.35	1.16
Ίδιο Δωμάτιο (Reversed)	0	0	21.26	1.21	0.63
Έξω από το Δωμάτιο (Forward)	0	0	20.61	2.68	0.65
Έξω από το Δωμάτιο (Reversed)	0	0	25.59	0.76	0.77
PC- 7 PC Wireless Internet (Forward)	0	0	27.29	1.54	1.26
PC- 7 PC Wireless Internet (Reserved)	0	0	0	0	0

## Παρατηρήσεις

Σε κάθε σύστημα επικοινωνίας, το βασικό κριτήριο για το χαρακτηρισμό της απόδοσής του, είναι η ακρίβεια με την οποία μεταδίδει οποιαδήποτε πληροφορία από το ένα σημείο στο άλλο. Ο χαρακτηρισμός αυτός σε φυσικό επίπεδο, προϋποθέτει την απάντηση στο ερώτημα: μπορεί ο δέκτης να διακρίνει το εισερχόμενο σήμα, έτσι ώστε να είναι σε θέση να αναγνωρίζει ένα λογικό '1' από ένα λογικό '0';

Το ερώτημα αυτό, οριοθετεί την ποιότητα φυσικής μετάδοσης και για την απάντηση σε αυτό πρέπει να ληφθούν υπόψη θέματα όπως ο θόρυβος, η παραμόρφωση του σήματος κατά τη διάρκεια της μετάδοσης ή λήψης κ.τ.λ. Ένας από τους σημαντικότερους παράγοντες υποβάθμισης, σε φυσικό επίπεδο, του μεταδιδόμενου σήματος στα συστήματα επικοινωνίας, είναι το jitter (ελληνιστί: χρονική ολίσθηση).

Ως *Jitter* στις τηλεπικοινωνίες αναφέρεται η χρονική απόκλιση ενός περιοδικού σήματος, συχνά σε σχέση με μια χρονική πηγή αναφοράς. Μπορεί να παρατηρηθεί σε χαρακτηριστικά όπως η συχνότητα διαδοχικών παλμών, το πλάτος του σήματος, ή τη φάση περιοδικών σημάτων. Γενικότερα, το jitter, είναι ένας σημαντικός και, τις περισσότερες φορές, ανεπιθύμητος παράγοντας στη σχεδίαση όλων σχεδόν των επικοινωνιακών συστημάτων/ζευξέων.

Και στην περίπτωση του πειράματος μας ο όρος jitter παίζει σημαντικό ρόλο, αφού αυτός αποτελεί το κύριο παράγοντα μετρήσεων. Το πρόγραμμα Wireshark που χρησιμοποιήθηκε υπολογίζει το jitter βάσει του RFC3550 (RTP), το οποίο αποτελεί βασικό πρωτόκολλο μεταφοράς δεδομένων σε πραγματικό χρόνο.

Παρατηρούμε ότι η μικρότερη τιμή για το Jitter είναι για την τρίτη περίπτωση, όπου η επικοινωνία είναι καλύτερη. Οι τιμές *Max Jitter* και *Max Delta* αναφέρονται για μεμονωμένες περιπτώσεις πακέτων και δεν αφορούν την επικοινωνία των δύο υπολογιστών στο σύνολό της. Έτσι, καλό είναι να μη ληφθούν υπ' όψη για την εξαγωγή συμπερασμάτων.

Παρακάτω, δίνεται ένας πίνακας που ταξινομεί την ποιότητα της επικοινωνίας, ανάλογα με τις εκάστοτε τιμές του Jitter:



Περιοχή τιμών Jitter	Αξιολόγηση
0 - 20 ms	Good
20 ms – 50 ms	Acceptable
> 50 ms	Unacceptable

Εύκολα από όλα τα παραπάνω μπορεί κάποιος να συμπεράνει ότι VoIP κλήσεις μέσω ασύρματου δικτύου και καλή ακουστική ποιότητα είναι κάτι το εφικτό. Πρέπει όμως να ικανοποιηθούν πρώτα κάποιες συγκεκριμένες απαιτήσεις έτσι ώστε ο τελικός χρήστης να είναι σε θέση να απολαύσει την συγκριμένη υπηρεσία. Πρέπει να γίνουν κάποιες σωστές επιλογές από την αρχή, και έχουν να κάνουν με τον εξοπλισμό κυρίως της ασύρματης σύνδεσης, αλλά και πιθανά τη σύνδεση internet που θα χρησιμοποιηθεί. Αυτά είναι που μπορούν να επηρεάσουν αλλά με την κατάλληλη επιλογή από την πλευρά του χρήστη μπορεί να είναι σίγουρος ότι έχει κάνει τον καλύτερο δυνατό συνδυασμό.

Στη συνέχεια αυτό που πρέπει να προσεχθεί, και είναι κάτι το οποίο πρέπει να γίνεται για κάθε μία κλήση ξεχωριστά είναι η παρακολούθηση του traffic στο δίκτυο. Είναι κάτι που όσο καλά ρυθμισμένος και να είναι ο wifi και ο internet εξοπλισμός του χρήστη, δυστυχώς για αυτόν, δεν μπορεί να τον βοηθήσει στην συγκεκριμένη περίπτωση.

## Βιβλιογραφία

Κατά την συγγραφή της πτυχιακής μου έλαβα υπόψη μου αρκετά βιβλία από την σχολή μου, άρθρα και σημειώσεις από την Ελληνική και Ξένη βιβλιογραφία.

Αυτά είναι:

1. Δίκτυα Υπολογιστών - Andrew S. Tanenbaum, Εκδόσεις Κλειδάριθμος
2. Ασύρματες Επικοινωνίες - William Stallings, Εκδόσεις Τζιόλα
3. Μελέτες - Εφαρμογές & Υλοποίηση Δικτύων Η/Υ - Γ.Μπάρδης, Β.Νικολόπουλος, Γ.Μπράττος, Β.Γκούρδιας Εκδοτική
4. Δίκτυα και Διαδίκτυα Υπολογιστών και Εφαρμογές τους στο Internet - Douglas E.Comer, Εκδόσεις Κλειδάριθμος
5. Network + Certification Study System Joseph J. Byrne 2002
6. Wi-Fi Handbook: Building 802.11b Wireless Networks by Frank Ohrtman and Konrad Roeder
7. Advanced Wireless Networks by Savo Glisic and Beatriz Lorenzo
8. Porter T., "Practical VoIP Security", 2006

## Διαδικτυακές Πηγές

1. <http://el.wikipedia.org/wiki>