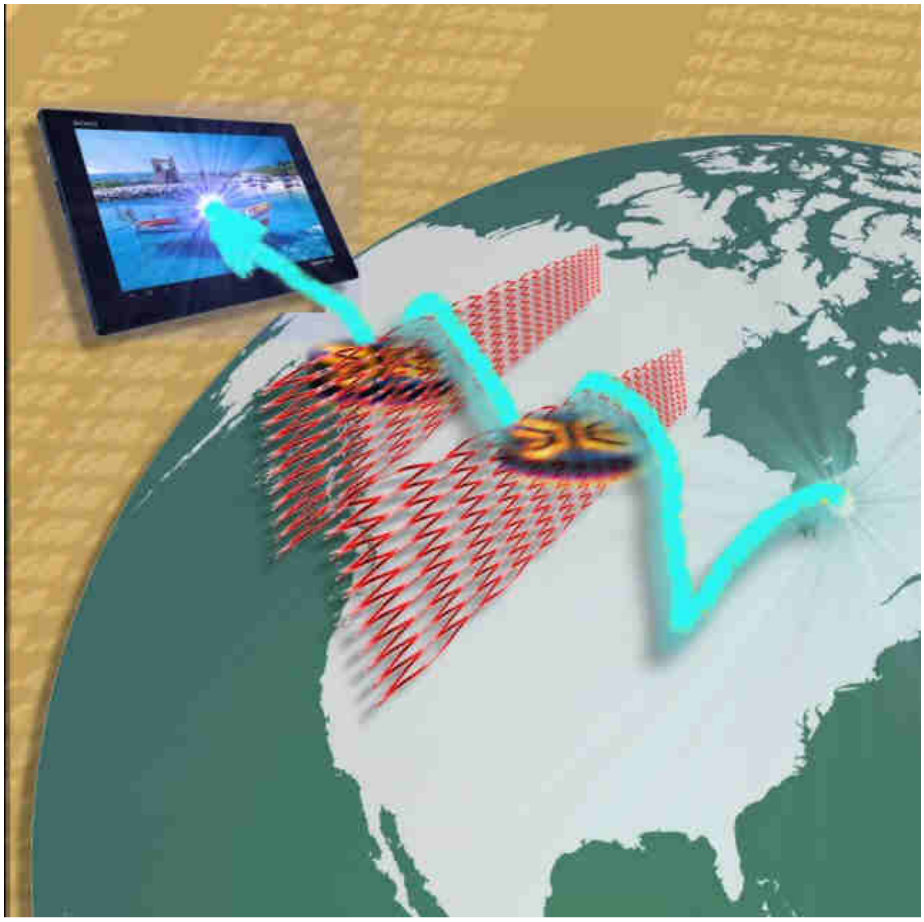
ΥΠΟΥΡΓΕΙΟ ΠΟΛΙΤΙΣΜΟΥ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ

Κωνσταντοπούλου Μ., Ξεφτεράκης Ν., Παπαδέας Μ., Χρυσοστόμου Γ.

ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Γ΄ Τάξη ΤΟΜΕΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΕΠΑ.Λ.

ΣΗΜΕΙΩΣΕΙΣ ΜΑΘΗΤΗ



ΙΝΣΤΙΤΟΥΤΟ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ & ΕΚΔΟΣΕΩΝ
«ΔΙΟΦΑΝΤΟΣ»

ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ
Πρόεδρος: **Γκλαβάς Σωτήριος**

ΓΡΑΦΕΙΟ ΕΡΕΥΝΑΣ, ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ Β΄
Προϊστάμενος: **Μάραντος Παύλος**
Επιστημονικά Υπεύθυνος: **Δρ. Τσαπέλας Θεοδόσιος,** Σύμβουλος Β΄ Πληροφορικής ΙΕΠ

ΣΥΓΓΡΑΦΙΚΗ ΟΜΑΔΑ:
Κωνσταντοπούλου Μαρία-Δήμητρα, Εκπαιδευτικός Πληροφορικής
Ξεφτεράκης Νικόλαος, Εκπαιδευτικός Πληροφορικής
Παπαδέας Μιχαήλ, Εκπαιδευτικός Πληροφορικής
Χρυσοστόμου Γεώργιος, Εκπαιδευτικός Πληροφορικής

ΕΠΙΜΕΛΕΙΑ - ΣΥΝΤΟΝΙΣΜΟΣ ΟΜΑΔΑΣ:
Κωτσάκης Σταύρος, Σχολικός Σύμβουλος Πληροφορικής

ΕΠΙΤΡΟΠΗ ΚΡΙΣΗΣ:
Αποστολάκης Ιωάννης, Εκπαιδευτικός Πληροφορικής
Μπόγρης Αντώνιος, Αναπληρωτής Καθηγητής Τ.Ε.Ι. Αθηνών
Μωράκης Διονύσιος, Εκπαιδευτικός Πληροφορικής

ΦΙΛΟΛΟΓΙΚΗ ΕΠΙΜΕΛΕΙΑ:
Μπουμπάρης Νικόλαος, Εκπαιδευτικός Φιλόλογος
Χρηστάκου Ζηνοβία, Εκπαιδευτικός Φιλόλογος

ΠΡΟΕΚΤΥΠΩΤΙΚΕΣ ΕΡΓΑΣΙΕΣ: ΔΙΕΥΘΥΝΣΗ ΕΚΔΟΣΕΩΝ/Ι.Τ.Υ.Ε. «ΔΙΟΦΑΝΤΟΣ»

Περιεχόμενα

Πρόλογος

Οι παρούσες σημειώσεις καλύπτουν σε σημαντικό βαθμό θέματα που άπτονται της τεχνολογίας των δικτύων υπολογιστών. Ο τρόπος παρουσίασης των σχετικών πληροφοριών βασίζεται στην ιστορική εξέλιξη της διασύνδεσης των δικτύων ευρείας περιοχής, όπως προέκυψε ως ανάγκη για το διαμοιρασμό πόρων και τελικά χρησιμοποιείται στη σημερινή δομή του Διαδικτύου. Η ανάγκη αυτή και το γενικό πρόβλημα της διασύνδεσης οδηγούν σε μια λογική διαίρεση σε ανεξάρτητα αλληλοτροφοδοτούμενα επίπεδα, γνωστά και ως μοντέλα TCP/IP και OSI. Η αλληλουχία των ενοτήτων δομείται με βασικό κορμό τη διαστρωμάτωση των μοντέλων αυτών καλύπτοντας τα βασικά θέματα της τεχνολογίας δικτύων που αντιμετωπίζονται σε κάθε επίπεδο. Αντίστοιχα τα περιεχόμενα των ενοτήτων πραγματεύονται τεχνολογικά προβλήματα που αντιμετωπίστηκαν κατά την εξελικτική πορεία των δικτύων σε τοπικό και ευρύτερο επίπεδο, επιτρέποντας την προσέγγιση κάθε θεματικής ενότητας με διάφορες διδακτικές μεθόδους. Στόχος είναι να δοθεί μια βασική και ολοκληρωμένη εικόνα στο μαθητή για τη δομή και λειτουργία των δικτύων έτσι ώστε να τον προετοιμάσει επαγγελματικά, συνδέοντας το γνωστικό αντικείμενο με την αγορά εργασίας, καθώς και με τις εξελίξεις στις σύγχρονες τεχνολογίες επικοινωνιών. Οι ενότητες καλύπτουν το θεωρητικό μέρος του κάθε επιπέδου και προτείνονται θεωρητικές και εργαστηριακές δραστηριότητες, που μπορεί ο εκπαιδευτικός να υλοποιήσει στα πλαίσια του μαθήματος. Αυτές οι δραστηριότητες μπορούν να αποτελέσουν έναυσμα για μελέτη βαθύτερων εννοιών και υλοποίηση πραγματικών σεναρίων στα ζητήματα λειτουργίας των δικτύων υπολογιστών, όσο εξελίσσεται η διερευνητική διαδικασία.

Από τους Συγγραφείς

Κεφάλαιο 1ο

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ ΚΑΙ ΔΙΑΣΥΝΔΕΣΗΣ ΔΙΚΤΥΩΝ

Εισαγωγή

Τα προϊόντα της σύγχρονης τεχνολογίας, ολοένα και περισσότερο ενσωματώνουν λειτουργίες που απαιτούν την αλληλοσύνδεσή τους. Η χρήση υπολογιστικών συστημάτων, ακόμη και σε συγκαλυμμένη μορφή, όπως “έξυπνες” συσκευές, έχει γενικευθεί και προσφέρει πολλές δυνατότητες διασύνδεσης. Ταυτόχρονα εξαρτάται από τις δυνατότητες διασύνδεσης των συσκευών. Ακόμη, η χρήση του Διαδικτύου έχει εισχωρήσει σε μεγάλο βαθμό στην καθημερινότητα των ατόμων. Η κατανόηση των αρχών λειτουργίας των δικτύων αποτελεί θεμελιώδη γνώση για την ενασχόληση, ιδιαίτερα, με αντικείμενα του χώρου της πληροφορικής.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 1ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- διακρίνουν τη διαστρωματωμένη αρχιτεκτονική ενός Δικτύου Υπολογιστών και να περιγράφουν συνοπτικά τη λειτουργία κάθε επιπέδου
- κατατάσσουν κάθε υλικό ή λογισμικό του δικτύου στο αντίστοιχο επίπεδο στο οποίο λειτουργούν
- διατυπώνουν την έννοια της ενθυλάκωσης

Διδακτικές Ενότητες

1.1 Ορισμός δικτύου.
1.2 Επίπεδα μοντέλου αναφοράς OSI (ISO), επίπεδα μοντέλου TCP/IP (DARPA) και η αντιστοιχία τους.
1.3 Ενθυλάκωση.

1.1 Ορισμός δικτύου

δίκτυο το [δίktio] Ο40 **: 1. πολύπλοκο συνήθ. σύμπλεγμα από γραμμές ή αγωγούς που διασταυρώνονται με τρόπο που μοιάζει με δίχτυ:** *Συγκοινωνιακό ~ / οδικό, σιδηροδρομικό, ακτοπλοϊκό, αεροπορικό ~,* το σύνολο των δρόμων, των σιδηροδρομικών γραμμών και των θαλάσσιων και εναέριων οδών που συνδέουν τους διάφορους τόπους μεταξύ τους. *~ ύδρευσης / αρδευτικό / αποχετευτικό / ηλεκτρικό / τηλεφωνικό ~,* το σύνολο των σωληνώσεων και των αγωγών που ξεκινούν από μια κεντρική μονάδα και με διακλαδώσεις φτάνουν στους καταναλωτές. *Ραδιοφωνικό / τηλεοπτικό ~,* σύστημα από ραδιοφωνικούς ή τηλεοπτικούς σταθμούς που συνδέονται μεταξύ τους, ώστε να εκπέμπουν ταυτόχρονα το ίδιο πρόγραμμα. || (πληροφ.) ***~ (ηλεκτρονικών υπολογιστών),* τρόπος σύνδεσης υπολογιστών, ώστε να επικοινωνούν μεταξύ τους.** || (πληροφ.) το ίντερνετ. **2.** σύνολο από

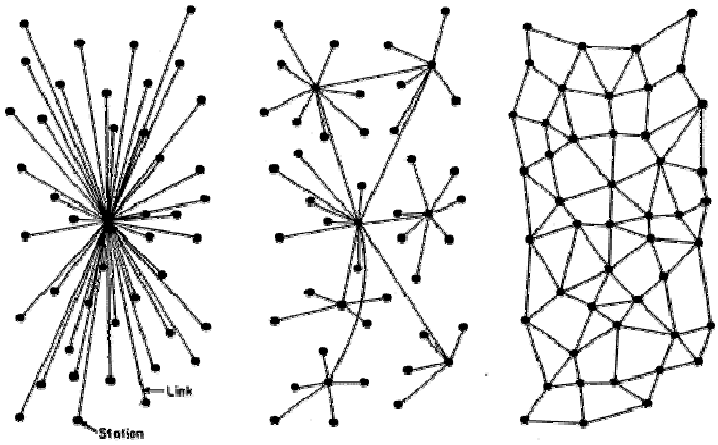
Εικόνα 1.1.α: Δίκτυ(ο)

πρόσωπα ή από επιχειρήσεις που συνεργάζονται με μια σχέση αλληλεξάρτησης: *Η επιχείρησή μας έχει ~ εμπορικών αντιπροσώπων. Εμπορικό ~*. || σύνολο από πρόσωπα με μεγάλες διασυνδέσεις, που δρουν παράνομα ή μυστικά: *Εξαρθρώθηκε ~ κακοποιών / εμπόρων ναρκωτικών / κατασκόπων.* [Λεξικό Τριανταφυλλίδη]

[λόγ. < αρχ. *δίκτυον* (δες στο *δίχτυ*) σημδ. γαλλ. réseau & αγγλ. net]

Πηγή: http://www.greek-language.gr/greekLang/modern_greek/tools/lexica/search.html?lq=δίκτυο&dq=

Συνεπώς, ένα δίκτυο οποιουδήποτε τύπου απαρτίζεται από δυο βασικά δομικά στοιχεία, τους **κόμβους** και τις **γραμμές** που ενώνουν τους κόμβους και προσδιορίζεται από το είδος τους. Έτσι όταν οι κόμβοι είναι **υπολογιστές** και οι γραμμές είναι **φυσικά μέσα μετάδοσης** όπως καλώδια, χαρακτηρίζεται ως **δίκτυο υπολογιστών**. Με τον όρο "υπολογιστής" εννοείται κάθε ψηφιακός ηλεκτρονικός υπολογιστής γενικής χρήσης, περιφερειακή συσκευή υπολογιστή ή συσκευή διακίνησης δεδομένων / πληροφοριών η οποία έχει τη δυνατότητα διασύνδεσης σε δίκτυο.



Εικόνα 1.1.β: Τοπολογίες δικτύων

Γενικά ένα δίκτυο υπολογιστών ή τηλεπληροφορικής είναι ένα σύστημα επικοινωνιών το οποίο διαθέτει συσκευές τηλεπικοινωνιών, τηλεπικοινωνιακούς κόμβους καθώς και φυσικά μέσα διέλευσης της πληροφορίας.

Η μορφή σύνδεσης μεταξύ των κόμβων ενός δικτύου ονομάζεται **τοπολογία δικτύου**.

Σε ένα δίκτυο τηλεπληροφορικής συναντάμε αυστηρούς κανόνες και πρότυπα που διέπουν το τηλεπικοινωνιακό τμήμα και την υλοποίηση του υλικού μέρους καθώς επίσης και κανόνες συνομιλίας μεταξύ των υπολογιστών οι οποίοι ονομάζονται **πρωτόκολλα επικοινωνίας**.

Πρωτόκολλο επικοινωνίας είναι ένα σύνολο κανόνων, που έχουν συμφωνηθεί από τα δυο επικοινωνούντα μέρη και εξυπηρετούν τη μεταξύ τους ανταλλαγή πληροφοριών..

1.2 Επίπεδα μοντέλου αναφοράς OSI (ISO), επίπεδα μοντέλου TCP/IP (DARPA) και η αντιστοιχία τους

Η δικτύωση, από **το μέσο μετάδοσης (καλώδιο) και την δικτυακή διασύνδεση** μέχρι **το πρόγραμμα-εφαρμογή,** είναι μια αρκετά **πολύπλοκη διαδικασία.**

Για την **υλοποίηση μιας δικτυακής εφαρμογής** η οποία παρέχεται από έναν υπολογιστή σε έναν άλλον, ξεκινώντας από το μηδέν, πρέπει

- να επινοηθεί ένας **τρόπος αναπαράστασης των δεδομένων/πληροφοριών** με τη μορφή, συνήθως, **ηλεκτρικών ή οπτικών σημάτων**,
- να κατασκευαστούν ιδιαίτερες **δικτυακές διασυνδέσεις** και **καλώδια**, τα οποία θα **συνδέσουν** τους υπολογιστές μεταξύ τους

- να επινοηθεί και να υλοποιηθεί ο **τρόπος εύρεσης μιας διαδρομής** μέσω της οποίας θα ταξιδέψουν οι πληροφορίες μέχρι τον τελικό προορισμό και να **αποκατασταθεί η επικοινωνία** από άκρο σε άκρο.

Έτσι, το έργο της δικτύωσης **διασπάστηκε σε επιμέρους λειτουργίε**ς οι οποίες μπορούν να υλοποιηθούν ανεξάρτητα, παρέχοντας και εναλλακτικές επιλογές ανάλογα με τις ανάγκες.

Με τη στρωματοποιημένη αρχιτεκτονική πετυχαίνουμε

- Διαχωρισμό του προβλήματος της επικοινωνίας σε μικρότερα και πιο εύκολα διαχειρίσιμα προβλήματα
- Εύκολη προσθήκη, αλλαγή ή βελτίωση υπηρεσιών, αφού οι απαιτούμενες αλλαγές περιορίζονται σε ένα συγκεκριμένο επίπεδο.

Ο στόχος είναι η απόκρυψη των λεπτομερειών του υλικού του δικτύου δίνοντας τη δυνατότητα στους υπολογιστές και στις εφαρμογές τους να επικοινωνούν μεταξύ τους ανεξάρτητα από τις φυσικές δικτυακές τους συνδέσεις.

Έτσι διαμορφώθηκε το μοντέλο αναφοράς (*Reference Model*) για τη Διασύνδεση Ανοικτών Συστημάτων (*Open Systems Interconnection* - **OSI**) από τον Διεθνή Οργανισμό Τυποποίησης (*International Organization for Standardization* - **ISO**) που προδιαγράφει **επτά (7) στρώματα-επίπεδα** (*seven layers*) τα οποία υλοποιούν συγκεκριμένες λειτουργίες ώστε να **είναι εφικτή η διασύνδεση διαφορετικών υπολογιστικών συστημάτων εφόσον στα αντίστοιχα επίπεδα χρησιμοποιούν συμβατές ή ίδιες τεχνικές και κανόνες *(πρωτόκολλα)***.

Ένα υπολογιστικό **σύστημα** είναι ένας υπολογιστής (πολλές φορές και ομάδα υπολογιστών) με το συνοδευτικό λογισμικό, τις περιφερειακές συσκευές και τα μέσα επικοινωνίας ο οποίος μπορεί να χρησιμοποιηθεί αυτόνομα για την επεξεργασία και διακίνηση πληροφοριών.

Όταν το σύστημα αυτό, για την επικοινωνία του με άλλα συστήματα, χρησιμοποιεί πρότυπα και πρωτόκολλα διεθνών οργανισμών όπως ISO/IEC, IEEE, ITU(πρώην CCITT) κ.λπ. και όχι ιδιόκτητα πρότυπα εταιρειών, τότε χαρακτηρίζεται **ανοιχτό σύστημα**

Αρχιτεκτονική δικτύου είναι τα διάφορα τμήματα υλικού και λογισμικού από τα οποία είναι κατασκευασμένο, ο ρόλος που παίζουν στην επικοινωνία, η μεταξύ τους σχέση - οι διεπαφές και τα πρωτόκολλα που ακολουθούνται.

1.2.1 Το μοντέλο αναφοράς για τη Διασύνδεση Ανοικτών Συστημάτων (OSI)

Τα επτά (7) επίπεδα του μοντέλου αναφοράς για τη Διασύνδεση Ανοικτών Συστημάτων, ξεκινώντας από το χαμηλότερο 1ο το οποίο είναι το **φυσικό** και προς το ανώτερο, έχουν ως εξής:

1. Το **Φυσικό** Επίπεδο ή στρώμα (Physical layer) ασχολείται με τη μετάδοση των bit (1|0) που απαρτίζουν την ομαδοποιημένη πληροφορία (πλαίσιο δεδομένων), μέσω του φυσικού μέσου το οποίο μπορεί να είναι καλώδιο, οπτική ίνα ή ασύρματη ζεύξη. Τα bit κωδικοποιούνται ως ηλεκτρικά, οπτικά ή ηλεκτρομαγνητικά σήματα. Ασχολείται επίσης με τα ηλεκτρικά, μηχανικά και λειτουργικά χαρακτηριστικά των διεπαφών (interfaces), το είδος και τα χαρακτηριστικά του φυσικού μέσου, τον τύπο του συνδετήρα (connector), ποιο σήμα αναπαριστά το 1 και ποιο το 0 καθώς και με το συγχρονισμό των συσκευών. Γενικά μιλώντας, αναφέρεται σε χειροπιαστά-φυσικά πράγματα.

Εικόνα 1.2.1.α: Το μοντέλο αναφοράς για τη Διασύνδεση Ανοικτών Συστημάτων (OSI)

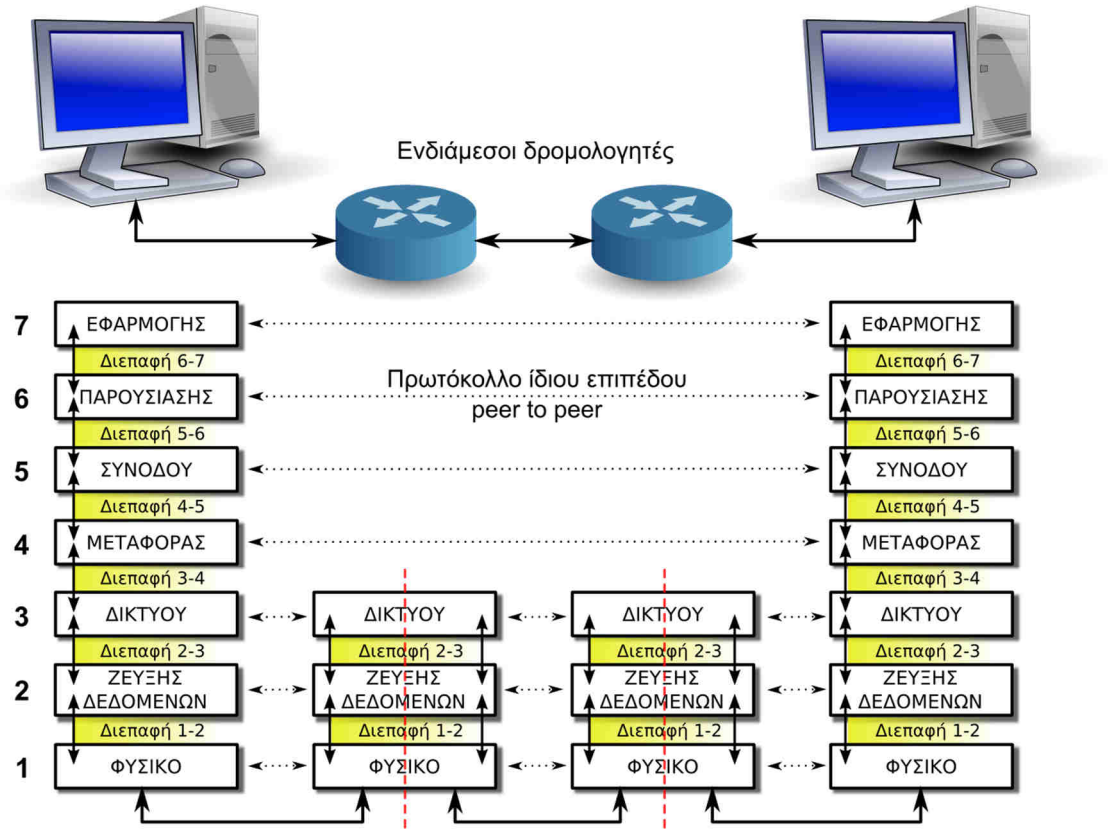
2. Το Επίπεδο **Ζεύξης** ή **Σύνδεσης Δεδομένων** (Data Link layer) παρέχει τη **φυσική διευθυνσιοδότηση** (MAC Addresses) και είναι υπεύθυνο για τον έλεγχο του μέσου μετάδοσης και του πότε μπορούν να εκπεμφθούν δεδομένα σε αυτό. Η λειτουργία αυτή παρέχεται από το υποεπίπεδο **Ελέγχου Πρόσβασης** στο **Μέσο** (Media Access Control).Το υποεπίπεδο **Λογικού Ελέγχου** της **Ζεύξης** (Logical Link Control) εξασφαλίζει την **αξιόπιστη** επικοινωνία μεταξύ δυο **άμεσα συνδεδεμένων** γειτονικών κόμβων (βρίσκονται στο ίδιο φυσικό/τοπικό δίκτυο). Εκτελεί βασικές λειτουργίες ανίχνευσης/διόρθωσης σφαλμάτων, ελέγχου ροής των πληροφοριών και συγχρονισμού πλαισίων. Η ομάδα των bit που συνθέτουν την μονάδα πληροφορίας αυτού του επιπέδου ονομάζεται **πλαίσιο** (frame). Η αρχή και το τέλος του πλαισίου σηματοδοτούνται κατάλληλα ώστε να μπορεί να συγχρονιστεί ο άλλος κόμβος.
3. Το επίπεδο **Δικτύου** (Network layer) παρέχει τη **λογική διευθυνσιοδότηση** με ενιαίο και μοναδικό τρόπο για όλη την έκταση των διασυνδεμένων μεταξύ τους δικτύων. Φροντίζει ώστε πακέτα διαφόρων μεγεθών να μπορούν να παραδοθούν από τον αποστολέα στον τελικό κόμβο του παραλήπτη **διασχίζοντας όλους τους ενδιάμεσους κόμβους** και **δίκτυα,** που ενδεχομένως μεσολαβούν μέχρι τον τελικό προορισμό. Έργο του είναι η εύρεση της κατάλληλης διαδρομής και παράδοση του πακέτου δεδομένων στον **τελικό κόμβο** η οποία χαρακτηρίζεται ως **δρομολόγηση** (routing). Στην προσπάθεια αυτή το πακέτο μπορεί να χρειαστεί να διασπαστεί σε διάφορα τμήματα τα οποία μπορεί να φτάσουν από άλλες διαδρομές και με διαφορετική σειρά, όμως το επίπεδο δικτύου θα τα επανασυνθέσει και θα

αναφέρει οποιαδήποτε προβλήματα παράδοσης προκύψουν. Το επίπεδο δικτύου στο μοντέλο OSI παρέχει υπηρεσίες με σύνδεση και χωρίς σύνδεση.

4. Το επίπεδο **Μεταφοράς** (Transport layer) παρέχει όλες τις λειτουργίες και τα μέσα που απαιτούνται ώστε να επιτευχθεί μια **από άκρο σε άκρο επικοινωνία μεταξύ προγραμμάτων ή διεργασιών**, εξασφαλίζοντας το επιθυμητό επίπεδο **ποιότητας υπηρεσίας** (quality of service, QoS). Η ποιότητα της υπηρεσίας περιλαμβάνει τις απαιτήσεις για την καθυστέρηση αποκατάστασης επικοινωνίας, την πιθανότητα απώλειας της σύνδεσης, τον επιτυγχανόμενο ρυθμό διακίνηση (throughput), το βαθμό προτεραιότητας και την ασφάλεια. Το επίπεδο μεταφοράς, στο OSI παρέχει υπηρεσίες **προσανατολισμένες σε σύνδεση** (connection oriented) και **υπηρεσίες χωρίς σύνδεση** (connectionless). Οι **υπηρεσίες με σύνδεση** βασίζονται σε λογικές συνδέσεις οι οποίες αποκαθίστανται, διατηρούνται μεταφέροντας δεδομένα και τερματίζονται. Σε αυτές τις συνδέσεις παρέχεται **αξιοπιστία** στην επικοινωνία με τον έλεγχο ροής, τον τεμαχισμό, την αρίθμηση και την επανασύνθεση των μηνυμάτων με τη σωστή σειρά και τον έλεγχο/διόρθωση των σφαλμάτων. Το επίπεδο αυτό έχει να διαχειριστεί τις επιβεβαιώσεις λήψης των πακέτων, τις επανεκπομπές, τους χρονιστές αναμονής και μετρητές προσπαθειών και το σημαντικότερο να τα κρύψει όλα αυτά από τα ανώτερα στρώματα. Είναι το χαμηλότερο επίπεδο που παρέχει από άκρο σε άκρο επικοινωνία και είναι υπό τον έλεγχο του χρήστη.
5. Το επίπεδο **Συνόδου** (Session layer) παρέχει τα αναγκαία μέσα για την οργάνωση και το συγχρονισμό των διαλόγων μεταξύ των ανωτέρων επιπέδων. Επιτρέπει ή απαγορεύει την παροχή συγκεκριμένης υπηρεσίας, αποκαθιστά τη σύνδεση εάν για κάποιο λόγο διακοπεί και περιλαμβάνει λειτουργίες όπως η εξακρίβωση του χρήστη, η χρέωση κ.λπ. Η διαδικασία απομακρυσμένης εισόδου (log-in) σε έναν υπολογιστή και ο έλεγχος του συνθηματικού (password) αφορούν το επίπεδο συνόδου. Το επίπεδο αυτό είναι υπεύθυνο για τον ομαλό τερματισμό της αντίστοιχης σύνδεσης του 4ου επιπέδου.
6. Το επίπεδο **Παρουσίασης** (Presentation layer) ασχολείται με την αναπαράσταση της πληροφορίας που μεταφέρεται από εφαρμογή σε εφαρμογή καθώς επίσης και με τη δομή των δεδομένων. Τροποποιεί κατάλληλα τα δεδομένα ώστε να είναι κατανοητά από την εφαρμογή όποτε χρησιμοποιείται διαφορετικός κώδικας από την άλλη μεριά. Είναι δηλαδή ο μεταφραστής του δικτύου όταν αυτό απαιτείται. Στο επίπεδο αυτό γίνεται η συμπίεση των δεδομένων για καλύτερη εκμετάλλευση της χωρητικότητας του καναλιού επικοινωνίας και η κρυπτογράφηση.
7. Το επίπεδο **Εφαρμογής** (Application layer) είναι το ανώτερο και τελευταίο επίπεδο προς τον χρήστη και παρέχει τον τρόπο για να μπορεί μια εφαρμογή να “συνομιλεί” με μια άλλη. Ειδικότερα επιτρέπει την εξακρίβωση της ταυτότητας των εφαρμογών που θέλουν να επικοινωνήσουν, επιβεβαιώνει την διαθεσιμότητα των εφαρμογών και του δικαιώματος για “συνομιλία”. Επίσης προσδιορίζει το πρωτόκολλο στο οποίο αναφέρονται οι εφαρμογές και με βάση το οποίο διεξάγεται η “συνομιλία”. Για παράδειγμα στην υπηρεσία του παγκόσμιου ιστού (WEB), ο φυλλομετρητής (web browser) και ο αντίστοιχος διακομιστής (web server) είναι εφαρμογές του επιπέδου εφαρμογής και το αντίστοιχο πρωτόκολλο εφαρμογής είναι το HTTP.

Το μοντέλο αναφοράς διασύνδεσης ανοιχτών συστημάτων (OSI) αποτελεί μια πρόταση του ISO προς τους κατασκευαστές υλικού και λογισμικού δικτύων, χωρίς να είναι δεσμευτική. Ο βαθμός υλοποίησής του επαφίεται σε αυτούς.

Στο μοντέλο της διαστρωματωμένης αρχιτεκτονικής ενός δικτύου, το **κάθε επίπεδο N "συνομιλεί" με το αντίστοιχο ομότιμό του στην απέναντι πλευρά**, χρησιμοποιώντας ένα **πρωτόκολλο** του ίδιου επιπέδου το οποίο καθορίζει τη συμπεριφορά και τους διαλόγους μεταξύ τους. Η λειτουργία αυτή όμως, εκτελείται **έμμεσα** καθώς κάθε επίπεδο έχει δυνατότητα άμεσης επικοινωνίας μόνο με τα γειτονικά του, το ανώτερο (επίπεδο N+1) απ' αυτό και το κατώτερο (επίπεδο N-1) το οποίο βρίσκεται χαμηλότερά του. Ο μηχανισμός επικοινωνίας μεταξύ γειτονικών επιπέδων χαρακτηρίζεται ως **διεπαφή** (interface). Κάθε επίπεδο παρέχει **υπηρεσία** στο ανώτερό του.



Εικόνα 1.2.1.β: Διαστρωματωμένη αρχιτεκτονική, διεπαφές και ομότιμα επίπεδα

Πριν την πρόταση του μοντέλου OSI, η δικτύωση ήταν μια υπόθεση που υποστηριζόταν είτε από κυβερνητικούς οργανισμούς (όπως το αμερικανικό ARPANET) είτε από ιδιόκτητες τεχνολογίες εταιρειών (όπως το SNA της IBM ή το DECnet της Digital Equipment Corporation) με αποτέλεσμα να μη μπορούν να επικοινωνήσουν συστήματα διαφορετικών κατασκευαστών μεταξύ τους. Το μοντέλο OSI αποτέλεσε την πρώτη προσπάθεια της βιομηχανίας υπολογιστών να συμφωνήσει σε κοινά πρότυπα δικτύωσης τη δεκαετία του '70 (1978) καταλήγοντας στη δημοσίευση του προτύπου το 1984. Το πρότυπο είναι το EN ISO/IEC 7498 ή ITU-T Recommendation X.200

1.2.2 Το μοντέλο δικτύωσης TCP/IP

Το δίκτυο ARPANET ήταν ένα δίκτυο μεταγωγής πακέτων που χρηματοδοτήθηκε από το υπουργείο άμυνας των Η.Π.Α. στα τέλη της δεκαετίας του '60. Από την αρχή κύριος στόχος του ήταν η **δυνατότητα να συνδέονται μαζί πολλαπλά διαφορετικά συστήματα και δίκτυα** με διαφανή τρόπο. Έμφαση επίσης δόθηκε στη δυνατότητα του δικτύου **να παραμένει λειτουργικό ακόμη κι αν μεγάλα τμήματά του έβγαιναν εκτός λειτουργίας**. Το 1983

χρησιμοποίησε τα πρωτόκολλα TCP/IP ως βασικά και σταδιακά εξελίχθηκε στο γνωστό μας **Internet**.

Χρησιμοποίησε διαστρωματωμένη αρχιτεκτονική καθορίζοντας μόνο **τέσσερα (4) επίπεδα-στρώματα** περιγράφοντας με λεπτομέρεια και αναπτύσσοντας πρωτόκολλα για τα τρία ανώτερα, τα οποία ονομάζει

- **Εφαρμογής** (αντιστοιχεί στα Εφαρμογής, Παρουσίασης και Συνόδου του OSI),
- **Μεταφοράς** (αντιστοιχεί στο Μεταφοράς του OSI),
- **Διαδικτύου** (αντιστοιχεί στο Δικτύου του OSI) και
- Ζεύξης ή **πρόσβασης δικτύου** ή διεπαφή δικτύου.

Θα πρέπει να σημειωθεί ότι η προαναφερθείσα αντιστοίχιση των επίπεδων του TCP/IP με αυτά του μοντέλου OSI ισχύει σε γενικές γραμμές και όχι απολύτως.

Κάτω από το επίπεδο διαδικτύου δεν προκαθορίζει κάτι παρά μόνο υποδεικνύει ότι θα πρέπει να χρησιμοποιηθεί κάποιο πρωτόκολλο, ώστε ο υπολογιστής να μπορεί να στέλνει πακέτα **IP** στο δίκτυο. Επειδή τα σημαντικότερα πρωτόκολλα είναι το TCP στο επίπεδο Μεταφοράς και το IP στο επίπεδο διαδικτύου, το μοντέλο ονομάστηκε **TCP/IP** και περιγράφεται στο έγγραφο RFC1122 και RFC1123. Μερικές φορές αναφέρεται και ως μοντέλο DoD (Department of Defence).

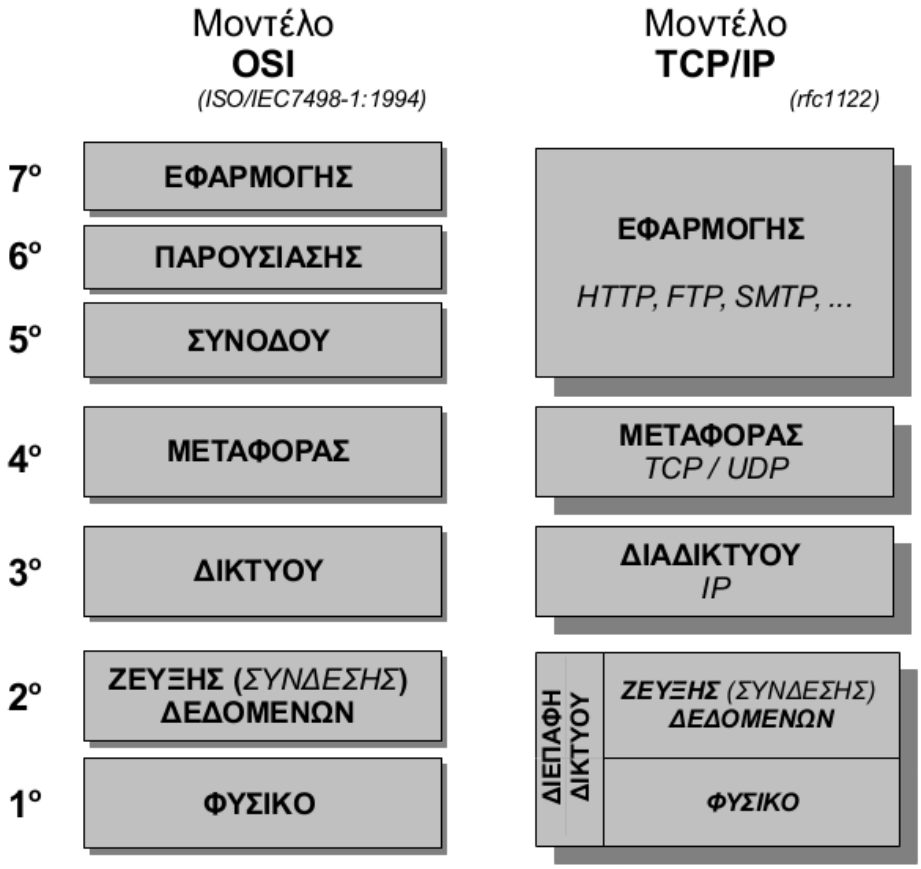
RFC (**Request For Comments**) είναι έγγραφα του IETF (Internet Engineering Task Force) που περιγράφουν (συνήθως προτείνουν) μεθόδους, συμπεριφορές, αποτελέσματα έρευνας ή καινοτομίες με εφαρμογή στο Διαδίκτυο και στα διασυνδεδεμένα με αυτό συστήματα. Τα περισσότερα υιοθετούνται ως πρότυπα και τυποποιήσεις του Διαδικτύου.

Παρότι το έγγραφο RFC1122 προδιαγράφει τέσσερα (4) επίπεδα-στρώματα, στη βιβλιογραφία χρησιμοποιούνται, από τους περισσότερους ειδικούς, πέντε (4+1) στρώματα. Στη θέση του στρώματος Διεπαφής Δικτύου του TCP/IP χρησιμοποιούνται τα δύο πρώτα στρώματα όπως περιγράφονται στο μοντέλο του OSI,το επίπεδο Ζεύξης Δεδομένων και το Φυσικό.

1. **Επίπεδο Πρόσβασης (Διεπαφής) Δικτύου** (Network Access ή link layer). Το μοντέλο TCP/IP δεν αναφέρει πολλά για το τι συμβαίνει εδώ, εκτός από το ότι ο υπολογιστής (host) πρέπει να συνδεθεί με το δίκτυο χρησιμοποιώντας κάποιο πρωτόκολλο ώστε **να μπορεί να στέλνει πακέτα IP** σε αυτό. Έτσι συνηθίζεται στη θέση του να χρησιμοποιούνται τα δυο κατώτερα επίπεδα του μοντέλου OSI, το
    a) **Φυσικό** και το
    b) **Ζεύξης Δεδομένων**.
2. **Επίπεδο Διαδικτύου**. Ισχύει ό,τι και στο 3ο επίπεδο του OSI (Δικτύου) με τη διαφορά ότι το επίπεδο Διαδικτύου του TCP/IP παρέχει μόνο **υπηρεσία χωρίς σύνδεση**. Έτσι δρομολογεί ανεξάρτητα πακέτα στον προορισμό τους και **η παράδοση των πακέτων στο επίπεδο Διαδικτύου δεν είναι εγγυημένα αξιόπιστη**. Μπορεί να φτάσουν στον προορισμό με διαφορετική σειρά, με λάθη, ή το ίδιο πακέτο περισσότερες φορές. Είναι δουλειά των ανώτερων επιπέδων να μεριμνήσουν για αυτά τα ζητήματα. Το βασικό πρωτόκολλο αυτού του επιπέδου είναι το **πρωτόκολλο Διαδικτύου** (Internet Protocol) **IP**.
3. **Επίπεδο Μεταφοράς** (Transport layer). Ισχύει γενικά ό,τι και στο 4ο επίπεδο του OSI (Μεταφοράς). Το επίπεδο μεταφοράς του **TCP/IP** μπορεί να παρέχει, μέσω διαφορετικών πρωτοκόλλων, υπηρεσίες **προσανατολισμένες σε σύνδεση** (connection oriented) ή **χωρίς σύνδεση** (connectionless). Οι **υπηρεσίες με σύνδεση** βασίζονται σε λογικές συνδέσεις οι οποίες αποκαθίστανται, διατηρούνται μεταφέροντας δεδομένα και τερματίζονται. Σε αυτές τις συνδέσεις παρέχεται

αξιοπιστία στην επικοινωνία με τον έλεγχο ροής, τον τεμαχισμό, αρίθμηση και την επανασύνθεση των μηνυμάτων με τη σωστή σειρά και τον έλεγχο/διόρθωση των σφαλμάτων. Υπηρεσίες με σύνδεση παρέχει το **πρωτόκολλο ελέγχου μετάδοσης** (Transmission Control Protocol) **TCP**. Στις **υπηρεσίες χωρίς σύνδεση** ή ασυνδεσμικές, δεν υπάρχει η έννοια της λογικής σύνδεσης ούτε παρέχεται αξιοπιστία. Είναι όμως απλούστερες και χωρίς πολλές καθυστερήσεις. Τέτοιες υπηρεσίες παρέχει το **πρωτόκολλο αυτοδύναμων πακέτων χρήστη** (User Datagram Protocol) UDP.

4. **Επίπεδο Εφαρμογής** (Application layer). Περιλαμβάνει όλα τα πρωτόκολλα των γνωστών υπηρεσιών του Διαδικτύου όπως απομακρυσμένη σύνδεση τερματικού (TELNET), μεταφορά αρχείων (FTP), ηλεκτρονικό ταχυδρομείο (SMTP/ POP3/ IMAP), τα νεώτερα DNS για την αντιστοίχηση ονομάτων υπολογιστών με τις διευθύνσεις τους στο δίκτυο, HTTP, το πρωτόκολλο μεταφοράς ιστοσελίδων του World Wide Web και πολλά άλλα.



Εικόνα 1.2.2.α: Αντιπαραβολή μοντέλων δικτύωσης OSI και TCP/IP

Δραστηριότητα 1η (Στην αίθουσα διδασκαλίας)

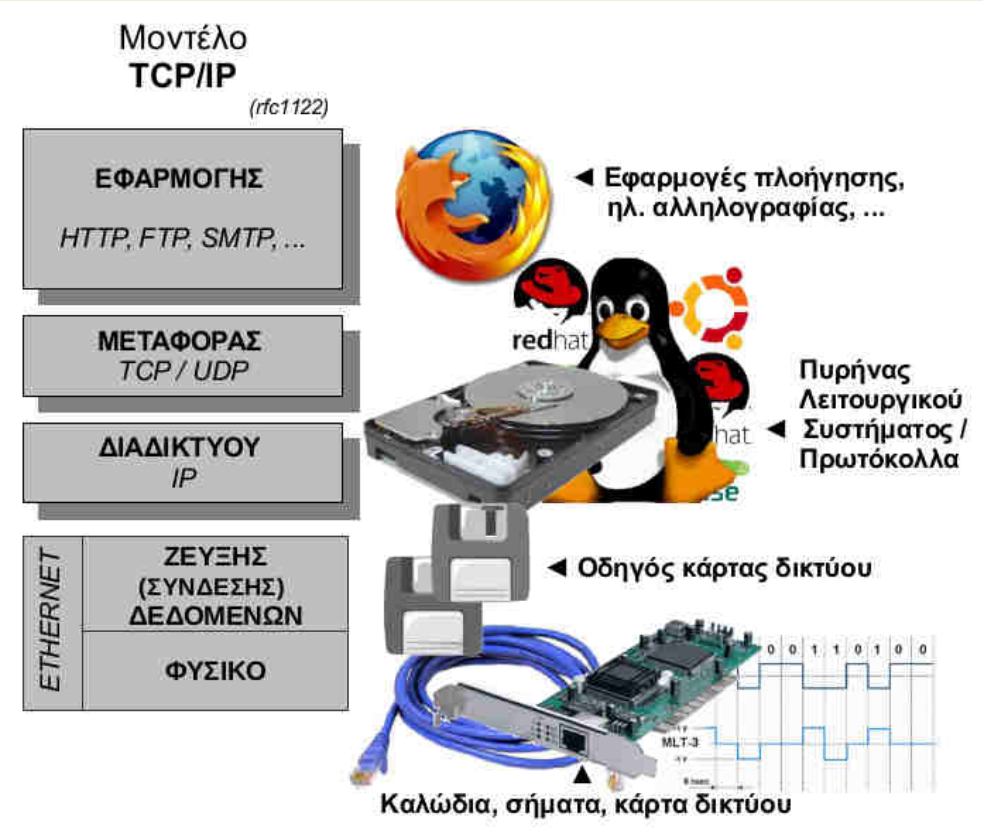
Στην παρακάτω εικόνα 1.2.2.β φαίνεται σχηματικά το μοντέλο δικτύωσης του TCP/IP σε ένα τοπικό δίκτυο τεχνολογίας Ethernet και δίπλα υλικό και λογισμικό δικτύων σε σχετική αντιστοιχία με το επίπεδο που ανήκει.

Ό,τι έχει να κάνει με σήματα, καλώδια, συνδετήρες (connectors) ανήκει σαφώς στο φυσικό επίπεδο.

Η κάρτα δικτύου, επειδή είναι σύνθετο υλικό και ενσωματώνει κυκλώματα με “στοιχειώδη εξυπνάδα”, μπορεί να δημιουργεί και να αντιλαμβάνεται πλαίσια, λειτουργεί καλύπτοντας περισσότερο από το φυσικό επίπεδο. Μαζί με τον οδηγό της (οδηγός συσκευής) καλύπτει το φυσικό και το επίπεδο ζεύξης δεδομένων του OSI.

Από εκεί και πάνω όλα υλοποιούνται με λογισμικό. Τα επίπεδα Διαδικτύου και Μεταφοράς αποτελούν μέρος του λειτουργικού συστήματος, κυρίως του πυρήνα.

Όλες οι δικτυακές εφαρμογές οι οποίες χρησιμοποιούν το δίκτυο για την αποθήκευση, ανάκτηση ή διακίνηση δεδομένων όπως τα προγράμματα ηλεκτρονικού ταχυδρομείου, πλοήγησης ιστοτόπων, μεταφοράς αρχείων κ.λπ. ανήκουν στο επίπεδο εφαρμογής.



Εικόνα 1.2.2.β: Επίπεδα TCP/IP και αντίστοιχο Υλικό - Λογισμικό

Σε ένα τοπικό δίκτυο τεχνολογίας **Ethernet - TCP/IP** το επίπεδο **πρόσβασης δικτύου** περιλαμβάνει:

- τα καλώδια διασύνδεσης, τους συνδετήρες (connectors), υποδοχές (πρίζες δικτύου),
- κάρτες δικτύου,
- παθητικό δικτυακό εξοπλισμό όπως υλικό διαχείρισης και συγκέντρωσης καλωδίων,
- επαναλήπτες (repeater hubs),
- μεταγωγείς (switching hubs) κτλ, **όχι** όμως δρομολογητές (routers).

Επιπλέον, και οι οδηγοί (drivers) των καρτών/ελεγκτών δικτύου εντάσσονται στο ίδιο επίπεδο, το 2ο του OSI.

Προσπαθήστε να απαντήσετε στα παρακάτω ερωτήματα:

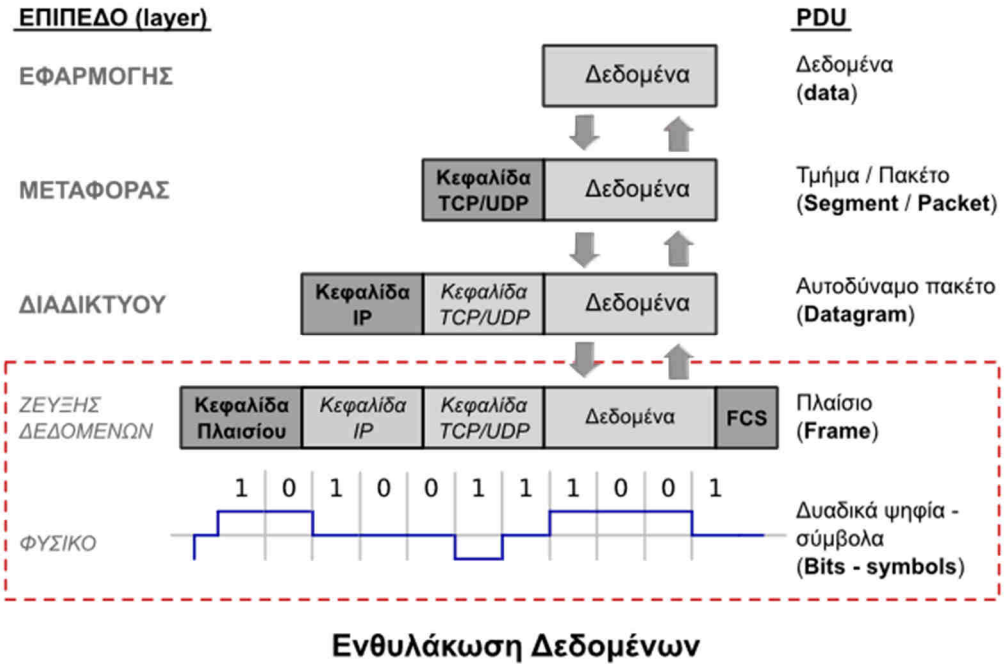
- Σε ποιο επίπεδο του OSI λειτουργεί η κάρτα δικτύου;
- Σε ποιο επίπεδο του OSI ανήκουν οι πρίζες δικτύου στις οποίες συνδέονται οι υπολογιστές;
- Ο Mozilla Firefox και το πρόγραμμα Skype ανήκουν στο ίδιο επίπεδο;
- Σε ποιο επίπεδο λειτουργεί μια ασύρματη κάρτα δικτύου;
- Μια κάρτα δικτύου Ethernet με υποδοχή για καλώδιο συνεστραμμένων ζευγών και μια για καλώδιο οπτικής ίνας, σε ποιο επίπεδο διαφέρουν;
- Αναζητήστε την ουσιαστική διαφορά ενός επαναλήπτη (repeater hub) από έναν μεταγωγέα (switching hub).

1.3 Ενθυλάκωση

Όπως προαναφέρθηκε, στη διαστρωματωμένη αρχιτεκτονική ενός δικτύου, κάθε επίπεδο επικοινωνεί με το αντίστοιχο ομότιμό του, χρησιμοποιώντας ένα **πρωτόκολλο** του ίδιου επιπέδου. Η λειτουργία αυτή όμως, εκτελείται **έμμεσα** καθώς κάθε επίπεδο έχει δυνατότητα άμεσης επικοινωνίας μόνο με τα γειτονικά του, μέσω της **διεπαφής** τους.

Έτσι **κατά την αποστολή δεδομένων** από τη μια εφαρμογή στην απομακρυσμένη, τα δεδομένα προωθούνται από το κάθε επίπεδο προς τα κάτω, στο αμέσως κατώτερο. **Κάθε επίπεδο προσθέτει στα δεδομένα πληροφορίες ελέγχου** για το αντίστοιχο, απέναντι, επίπεδο ώστε να εξασφαλίσει την επιτυχή παράδοσή τους. Οι πληροφορίες ελέγχου προστίθενται μπροστά από τα δεδομένα που πρόκειται να αποσταλούν και ονομάζονται **επικεφαλίδα**. Ορισμένα επίπεδα προσθέτουν πληροφορίες και στο τέλος των δεδομένων (όπως το 2ο επίπεδο του OSI) με σκοπό να εξασφαλίστει η αναγνώριση σφαλμάτων κατά τη μετάδοση στο φυσικό μέσο.

Κάθε επίπεδο χειρίζεται την πληροφορία που λαμβάνει από το ανώτερό του ως δεδομένα και προσθέτει μπροστά τους τη δική του επικεφαλίδα. Η προσθήκη σαν περίβλημα των πληροφοριών ελέγχου στα δεδομένα ονομάζεται **ενθυλάκωση (encapsulation)**.



Ενθυλάκωση Δεδομένων

Εικόνα 1.3.α: Ενθυλάκωση

Παρατηρώντας τη συγκεκριμένη διαδικασία στη διεπαφή του επιπέδου διαδικτύου με το ζεύξης δεδομένων, **ένα αυτοδύναμο πακέτο** του επιπέδου διαδικτύου τοποθετείται μέσα, δηλαδή **ενθυλακώνεται σε ένα πλαίσιο** του επιπέδου ζεύξης δεδομένων καθώς περικλείεται ανάμεσα στην επικεφαλίδα και στην ακολουθία ελέγχου του πλαισίου (Frame Check Sequence). Με απλά λόγια ένα "πακέτο" ανωτέρου επιπέδου τοποθετείται, ως δεδομένα, μέσα σε ένα "πακέτο" του αμέσως κατωτέρου επιπέδου.

Οι πληροφορίες ελέγχου που προστίθενται κατά τη διαδικασία ελέγχου είναι κυρίως **διευθύνσεις**, **χαρακτήρες ελέγχου σφαλμάτων** ή **άλλοι χαρακτήρες ελέγχου και συγχρονισμού**.

Στο φυσικό επίπεδο, οι άσοι και τα μηδενικά που απαρτίζουν το πλαίσιο, μετατρέπονται σε σήματα κατάλληλα για το φυσικό μέσο.

Κατά τη λήψη των δεδομένων συμβαίνει η αντίστροφη διαδικασία. Κάθε επίπεδο, αφαιρεί τις πληροφορίες ελέγχου που αφορούν το ίδιο και προωθεί τα δεδομένα στο ανώτερό του. Στην εικόνα φαίνεται η διαδικασία της ενθυλάκωσης στο μοντέλο του TCP/IP καθώς και η ονομασία της βασικής μονάδας πληροφορίας του πρωτοκόλλου κάθε επιπέδου (Protocol Data Unit).

Δραστηριότητα 2η (Στην αίθουσα διδασκαλίας)

Για να γίνει κατανοητή η διαδικασία της ενθυλάκωσης μπορούμε να δούμε το ανάλογο της αλληλογραφίας μέσω ταχυδρομείου.

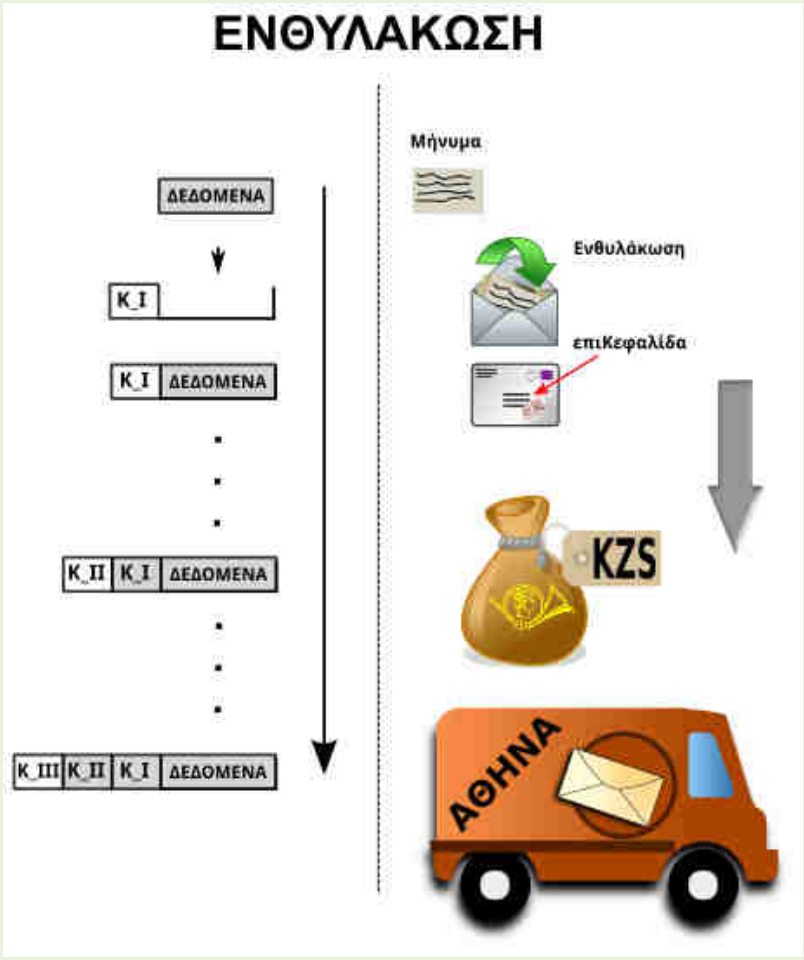
- Τα δεδομένα είναι το **μήνυμα**-γράμμα που γράφουμε απευθυνόμενοι στον απομακρυσμένο παραλήπτη.
- Στη συνέχεια τοποθετείται μέσα σε **φάκελο** (ενθυλακώνεται), γράφονται σ' αυτόν οι διευθύνσεις αποστολέα και παραλήπτη (επικεφαλίδα) και παραδίδεται στο ταχυδρομικό γραφείο (κατώτερο επίπεδο).
- Ακολούθως με διαδοχικές ενθυλακώσεις τοποθετείται σε **ταχυδρομικό σάκο** και παραδίδεται στο **ταχυδρομικό φορτηγό** για να προωθηθεί στο κεντρικό τμήμα διαλογής αλληλογραφίας.

Από εκεί και πέρα ακολουθείται η αντίστροφη διαδικασία. Ένας ταχυδρομικός σάκος παραδίδεται στο τοπικό ταχυδρομικό γραφείο του παραλήπτη και ο τοπικός διανομέας αφαιρεί τον φάκελο και τον παραδίδει στον τελικό παραλήπτη.

Ο τελικός παραλήπτης θα αφαιρέσει από τον φάκελο το γράμμα και θα το διαβάσει.

Με βάση το παράδειγμα της αλληλογραφίας μέσω ταχυδρομείου προσπαθήστε να απαντήσετε, αιτιολογημένα, στα παρακάτω ερωτήματα:

- Εάν ο χρήστης ο οποίος έγραψε τα στοιχεία στο φάκελο και τον έκλεισε είναι ένα επίπεδο (N) στη διαστρωματωμένη αρχιτεκτονική της ταχυδρομικής υπηρεσίας, ποιο είναι το αμέσως κατώτερο επίπεδο (N-1); *(Υπόδειξη: Το ταχυδρομικό γραφείο που παραλαμβάνει το φάκελο προς αποστολή)*
- Το ταχυδρομικό γραμματοκιβώτιο έξω από το ταχυδρομικό γραφείο στο οποίο οι ενδιαφερόμενοι ρίχνουν τα γράμματα που θέλουν να στείλουν, σε ποιο στοιχείο ενός διαστρωματωμένου μοντέλου αντιστοιχεί; *(Υπόδειξη: Διεπαφή μεταξύ δυο επιπέδων)*
- Τι προσφέρει ο ταχυδρομικός διανομέας στον παραλήπτη; *(Υπόδειξη: Υπηρεσία)*



Εικόνα 1.3.β: Ενθυλάκωση, το παράδειγμα του ταχυδρομείου

Δραστηριότητα 2η (Στην αίθουσα διδασκαλίας)

Ένας τουρίστας από τη Θεσσαλονίκη επισκέπτεται το Παρίσι για δει τα εκθέματα του Μουσείου του Λούβρου.

- Για το σκοπό αυτό επισκέφτηκε αρχικά ένα τουριστικό γραφείο το οποίο σχεδίασε την εκδρομή-διαδρομή του.
- Μεταφέρθηκε με μίνι λεωφορείο στο αεροδρόμιο της πόλης του και στη συνέχεια επιβιβάστηκε σε αεροπλάνο με προορισμό το Παρίσι.
- Αποβιβάστηκε από το αεροπλάνο και με λεωφορείο οδηγήθηκε στο ξενοδοχείο του και στη συνέχεια στο Μουσείο.

Βρείτε αντιστοιχίες του ταξιδιού του τουρίστα με τη διαδικασία ενθυλάκωσης/ αποθυλάκωσης της στρωματοποιημένης αρχιτεκτονικής των δικτύων.

Ερωτήσεις - Ασκήσεις Κεφαλαίου

1. Σχεδιάστε το μοντέλο της στρωματοποιημένης αρχιτεκτονικής δικτύου του OSI και του TCP/IP δείχνοντας την αντιστοιχία των στρωμάτων-επιπέδων τους.
2. Αναφέρετε δυο πλεονεκτήματα της στρωματοποιημένης αρχιτεκτονικής και σχολιάστε ένα από αυτά.
3. Απαντήστε μονολεκτικά ή με λίγες λέξεις στα παρακάτω:
    i. Τι προσφέρει ένα επίπεδο στο ανώτερό του και μέσω ποιού μηχανισμού; Πώς "συνομιλεί" με το απέναντι ομότιμό του επίπεδο;
    ii. Ποιο επίπεδο είναι υπεύθυνο για τη δρομολόγηση των δεδομένων και την επικοινωνία από υπολογιστή σε υπολογιστή;
    iii. Ποιο επίπεδο παρέχει από άκρο σε άκρο επικοινωνία μεταξύ προγραμμάτων ή διεργασιών;
4. Περιγράψτε τη διαδικασία της ενθυλάκωσης.
5. Απαντήστε μονολεκτικά ή με λίγες λέξεις στα παρακάτω:
    i. Σε ποιο επίπεδο, κατά τη διαδικασία της ενθυλάκωσης, προστίθεται πληροφορία στο τέλος του πακέτου εκτός από την επικεφαλίδα στην αρχή;
    ii. Η επικεφαλίδα του πακέτου του επιπέδου δικτύου συμπεριλαμβάνεται στην επικεφαλίδα ή στα δεδομένα-φορτίο του πλαισίου (του επιπέδου ζεύξης δεδομένων);
6. Τι είναι αρχιτεκτονική ενός δικτύου;
7. Το επίπεδο διαδικτύου είναι πολύ σημαντικό για τη διασύνδεση δικτύων. Αναπτύξτε σε λίγες γραμμές τα επιχειρήματά σας ώστε να υποστηρίξετε την άποψη αυτή.

Άσκηση (Σε Εργαστηριακό Περιβάλλον)

Για να μπορούν να **συνδεθούν** δυο ή περισσότεροι υπολογιστές σε δίκτυο ώστε να είναι δυνατόν να ανταλλάσσουν δεδομένα και να προσφέρουν ή να δέχονται διάφορες υπηρεσίες (κοινόχρηστο αποθηκευτικό χώρο, πρόσβαση στο Διαδίκτυο κτλ) θα πρέπει να είναι εξοπλισμένοι:

- με τον κατάλληλο **προσαρμογέα - ελεγκτή (κάρτα) δικτύου** (NIC-Network Interface Controller) συνοδευόμενο από **οδηγό** (πρόγραμμα οδήγησης συσκευής) για το χρησιμοποιούμενο λειτουργικό σύστημα. Κάθε θύρα εισόδου/εξόδου η οποία δίνει σ' έναν υπολογιστή τη δυνατότητα διασύνδεσης σε δίκτυο χαρακτηρίζεται ως δικτυακή διεπαφή (Network Interface).
- το κατάλληλο ***λογισμικό δικτύου*** που θα επιτρέψει την **δρομολόγηση** των δεδομένων και **αποκατάσταση της επικοινωνίας** μεταξύ των εμπλεκομένων ανταποκριτών
- τα κατάλληλα **προγράμματα-εφαρμογές** που θα προσφέρουν από τη μια μεριά και θα δεχθούν από την άλλη την παρεχόμενη υπηρεσία. *π.χ. ένας εξυπηρετητής του* παγκόσμιου *ιστού (web server) όπως ο Apache και ένας φυλλομετρητής/πλοηγός (web browser) όπως ο Mozilla Firefox από την άλλη*.

Επιπλέον, για την υλοποίηση του δικτύου απαιτούνται καλώδια, σύνδεσμοι (connectors), συσκευές ένωσης, τερματισμού και διασύνδεσης των καλωδίων και άλλο συναφές υλικό.

Με βάση τη Δραστηριότητα 1-i στην τάξη, στο εργαστήριο πληροφορικής, εντοπίστε και κατονομάσετε υλικό και λογισμικό σχετικό με τα δίκτυα.

Κατόπιν, προσπαθήστε να το κατατάξετε στο επίπεδο που ανήκει, αναφερόμενοι είτε στο μοντέλο του OSI είτε σε αυτό του TCP/IP.

Αιτιολογήστε την απόφασή σας με βάση αυτά που γνωρίζετε.

Βιβλιογραφία

Αλεξόπουλος, Α., & Λαγογιάννης, Γ. (2012). *Τηλεπικοινωνίες και Δίκτυα Υπολογιστών,* (8η έκδ.). Αθήνα.

Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). *Τεχνολογία Δικτύων Επικοινωνιών* (1η έκδ.). Αθήνα: ΟΕΔΒ.

Comer, D. E. (2001). *Διαδίκτυα με TCP/IP αρχές, πρωτόκολλα και αρχιτεντονικές,* (4η έκδ., Τ. 1). Αθήνα: Κλειδάριθμος.

Hunt, C. (1998). *TCP/IP Network Administration* (2nd έκδ.). Sebastopol, CA: O'Reilly & Associates.

Tanenbaum, A. S. (2000). *Δίκτυα Υπολογιστών* (3η έκδ.). Αθήνα: Εκδόσεις Παπασωτηρίου.

Κεφάλαιο 2ο

ΤΟΠΙΚΑ ΔΙΚΤΥΑ - ΕΠΙΠΕΔΟ ΠΡΟΣΒΑΣΗΣ ΔΙΚΤΥΟΥ (TCP/IP)

Εισαγωγή

Το επίπεδο πρόσβασης δικτύου για την τεχνολογία TCP/IP, καθώς και το φυσικό επίπεδο και επίπεδο σύνδεσης δεδομένων για το μοντέλο OSI, είναι τα κατώτερα επίπεδα στην δικτυακή επικοινωνία. Σε αυτό το κεφάλαιο θα μελετηθούν οι τρόποι πρόσβασης στο φυσικό μέσο, οι τοπολογίες δικτύων, τα φυσικά μέσα μετάδοσης που χρησιμοποιούνται, οι τρόποι μετάδοσης δεδομένων, καθώς και τεχνολογίες και πρότυπα που βασίζονται στα προαναφερόμενα κατώτερα επίπεδα επικοινωνίας.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 2ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- περιγράφουν την έννοια του τοπικού δικτύου
- κατατάσσουν ένα δίκτυο ως τοπικό, με κριτήριο τον στενό γεωγραφικό χώρο, ή το ενιαίο πεδίο συγκρούσεων (collision domain) - κοινό χώρο εκπομπής (broadcast)
- διακρίνουν τις διάφορες τεχνικές προσπέλασης στο μέσο και πότε η μετάδοση είναι βασικής ή ευρείας ζώνης
- απαριθμούν τις βασικές τεχνικές προσπέλασης στο μέσο
- απαριθμούν τα διαφορετικά μέσα μετάδοσης και να μπορούν να επιλέγουν το εκάστοτε διαθέσιμο και κατάλληλο για την εφαρμογή που χρησιμοποιούν
- περιγράφουν τα βασικά χαρακτηριστικά των διαφόρων φυσικών μέσων, υλικού τερματισμού (καλώδια - συνδετήρες) και τις βασικές απαιτήσεις χειρισμού τους
- μπορούν να επιλέγουν, αιτιολογημένα, τον καταλληλότερο για την εφαρμογή που χρησιμοποιούν, ελεγκτή (κάρτα) δικτύου (NIC) με βάση τα χαρακτηριστικά του από το φύλλο δεδομένων του (datasheet)
- εντοπίζουν μια διεύθυνση MAC και να προσδιορίζουν τον κατασκευαστή του υλικού απ' αυτήν
- εντοπίζουν τα πλαίσια Ethernet και τα διάφορα πεδία τους σε έναν αναλυτή πρωτοκόλλου ή σε ένα λογισμικό καταγραφής δικτυακής κίνησης

Διδακτικές Ενότητες

2.1 Φυσικό επίπεδο - Επίπεδο Σύνδεσης (ζεύξης) Δεδομένων (μοντέλο OSI).
2.2 Η πρόσβαση στο μέσο.
2.3 Μετάδοση Βασικής και Ευρείας ζώνης.
2.4 Δίκτυα ETHERNET (10/100/1000Mbps).
2.5 Ασύρματα Δίκτυα.
2.6 Τεχνολογία Ασύγχρονου Τρόπου Μεταφοράς Δεδομένων (Asynchronous Transfer Mode, ATM).
2.7 Πρωτόκολλο Σύνδεσης Σημείου προς Σημείο (PPP).

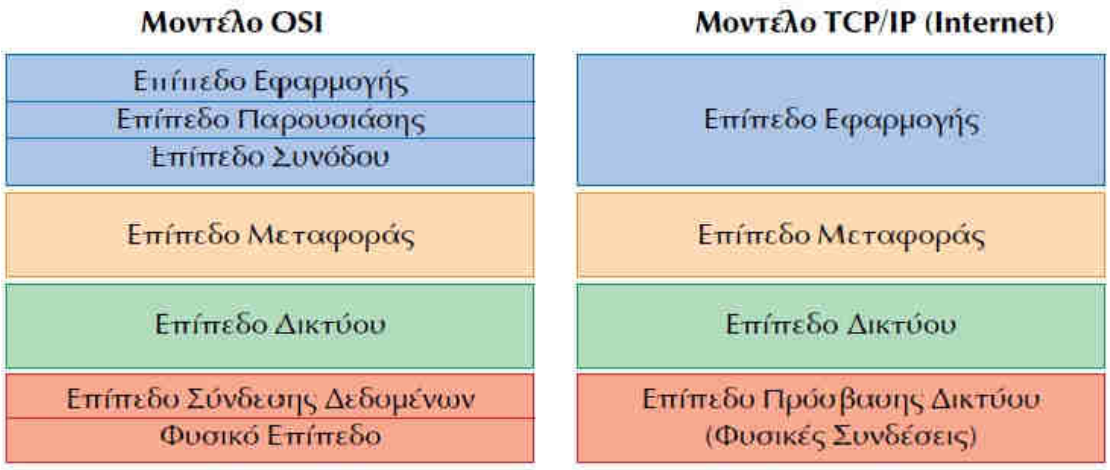
2.1 Φυσικό επίπεδο - Επίπεδο Σύνδεσης (ζεύξης) Δεδομένων (μοντέλο OSI)

Όπως έχουμε ήδη αναφέρει, το χαμηλότερο επίπεδο του μοντέλου OSI είναι το **φυσικό επίπεδο**. Αυτό το επίπεδο είναι υπεύθυνο για τη μετάδοση bits μέσα από το τηλεπικοινωνιακό κανάλι, το οποίο μπορεί να είναι ένα ενσύρματο μέσο ή και μία

ασύρματη ζεύξη. Έτσι, το φυσικό επίπεδο καθορίζει τα ηλεκτρικά και μηχανικά χαρακτηριστικά της σύνδεσης του σταθμού με το μέσο μετάδοσης. Αν, για παράδειγμα, χρησιμοποιείται καλώδιο ως μέσο μετάδοσης, οι προδιαγραφές του φυσικού επιπέδου καθορίζουν πόσους ακροδέκτες έχει ο συνδετήρας, το ρόλο του κάθε ακροδέκτη, τις διαστάσεις του, τις ανοχές κάθε διάστασης κ.ά. Στο επίπεδο αυτό καθορίζεται ο τρόπος αναπαράστασης των bits, 0 και 1, η διάρκεια κάθε bit, η αρχή και το τέλος της μετάδοσης, καθώς και το αν η μετάδοση μπορεί να γίνεται προς τη μία κατεύθυνση ή και τις δύο κατευθύνσεις ταυτόχρονα. Το φυσικό επίπεδο δεν το απασχολεί καθόλου αν μεταφέρει bytes των 8 bits ή χαρακτήρες ASCII των 7 bits.

Το δεύτερο επίπεδο του μοντέλου OSI είναι το **επίπεδο σύνδεσης (ζεύξης) δεδομένων (Data link layer)**. Το επίπεδο αυτό έχει σκοπό να κάνει αξιόπιστη τη φυσική γραμμή σύνδεσης μεταξύ δύο σταθμών. Από τα πακέτα του παραπάνω επιπέδου (επιπέδου δικτύου του μοντέλου OSI) φτιάχνει πλαίσια δεδομένων (data frames). Ορίζει που αρχίζει και που τελειώνει κάθε πλαίσιο, προσθέτοντας την κατάλληλη επικεφαλίδα (header) και ουρά (trailer), ανιχνεύει τα σφάλματα μετάδοσης, επιδιορθώνει τα αλλοιωμένα δεδομένα ή ζητά την επανεκπομπή τους. Ακόμα, ελέγχει το πότε μπορεί να δεσμεύσει το φυσικό μέσο για την αποστολή των πλαισίων, ώστε να μη γίνει ταυτόχρονη εκπομπή με άλλο σταθμό και τέλος, μεταβάλλει κατά περίπτωση τη ροή των πλαισίων ανάλογα με τους ρυθμούς που μπορεί να δεχτεί ο σταθμός παραλήπτης.

Όπως γνωρίζουμε, τα δύο χαμηλότερα επίπεδα στο μοντέλο OSI, δηλαδή το φυσικό επίπεδο και το επίπεδο σύνδεσης (ζεύξης) δεδομένων, αντιστοιχούν στο 1^{ο} επίπεδο του προτύπου TCP/IP, δηλαδή στο επίπεδο πρόσβασης δικτύου.



Σχήμα 2.1.α: Μοντέλα OSI και TCP/IP.

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Το **επίπεδο πρόσβασης δικτύου** του προτύπου **TCP/IP**, παρέχει την πρόσβαση στο φυσικό μέσο, στο οποίο μεταδίδεται η πληροφορία με τη μορφή πακέτων και αντιπροσωπεύει το χαμηλότερο λογικό επίπεδο λειτουργικότητας, που απαιτείται από ένα δίκτυο. Το επίπεδο αυτό περιλαμβάνει τα στοιχεία των φυσικών συνδέσεων, όπως: καλώδια, αναμεταδότες, κάρτες δικτύου, πρωτόκολλα πρόσβασης τοπικών δικτύων και προσφέρει τις υπηρεσίες του στο ανώτερο επίπεδο, το επίπεδο δικτύου. Στην τεχνολογία TCP/IP, τα χαμηλότερα επίπεδα του επιπέδου δικτύου δεν προδιαγράφονται και έτσι αυτά μπορούν να ακολουθούν τελείως διαφορετικές τεχνολογίες.

2.2 Η πρόσβαση στο μέσο

Σε όλα τα δίκτυα υπάρχουν περισσότεροι από έναν υπολογιστές, οι οποίοι αναγκάζονται να μοιράζονται το ίδιο μέσο μεταφοράς δεδομένων (π.χ. καλώδιο). Έτσι, αν δυο υπολογιστές προσπαθούσαν ταυτόχρονα να εισάγουν δεδομένα στο καλώδιο, τα πακέτα του ενός υπολογιστή θα συγκρούονταν με τα πακέτα του άλλου, με αποτέλεσμα την καταστροφή του συνόλου των πακέτων που προέρχονται και από τους δυο υπολογιστές. Συμπερασματικά, αν πρόκειται να γίνει αποστολή δεδομένων μέσω του δικτύου, πρέπει να βρεθεί ένας τρόπος ώστε να πληρούνται οι παρακάτω προϋποθέσεις:

- Εισαγωγή των δεδομένων στο καλώδιο χωρίς να γίνει σύγκρουση με άλλα δεδομένα.
- Να λάβει τα δεδομένα ο αποδέκτης με σχετική εγγύηση ότι αυτά δεν έχουν καταστραφεί σε σύγκρουση δεδομένων (data collision) κατά τη μετάδοση.

Το σύνολο των κανόνων που καθορίζουν τον τρόπο με τον οποίο τα δεδομένα εισάγονται στο καλώδιο, ονομάζεται **μέθοδος προσπέλασης (access method)**. Οι μέθοδοι προσπέλασης πρέπει να είναι σύμφωνες ως προς τον τρόπο με τον οποίο χειρίζονται τα δεδομένα. Αν διαφορετικοί υπολογιστές χρησιμοποιούν διαφορετικές μεθόδους προσπέλασης, τότε το δίκτυο θα αποτύχει, γιατί κάποιες μέθοδοι θα κυριαρχήσουν στο καλώδιο. Γενικά, οι μέθοδοι προσπέλασης εμποδίζουν την ταυτόχρονη εισαγωγή δεδομένων στο μέσο μεταφοράς. Έτσι, εξασφαλίζοντας το γεγονός ότι μόνο ένας υπολογιστής τη φορά θα μπορεί να στείλει δεδομένα, οι μέθοδοι προσπέλασης κρατούν οργανωμένες τις διαδικασίες αποστολής και λήψης δεδομένων δικτύου.

Υπάρχουν τρείς τρόποι για την αποφυγή ταυτόχρονης χρήσης του μέσου μεταφοράς:

- Μέθοδοι Carrier-sense multiple access (ακρόαση φέροντος πολλαπλής πρόσβασης)
  - Με ανίχνευση σύγκρουσης (collision detection)
  - Με αποφυγή σύγκρουσης (collision avoidance)
- Μέθοδος token passing (πέρασμα κουπονιού) που δίνει δυνατότητα για μεμονωμένη αποστολή δεδομένων
- Μέθοδος απαίτησης προτεραιότητας

(Πηγή: users.auth.gr/~spetrido/CSMACD.doc)

Πρότυπα Τοπικών Δικτύων

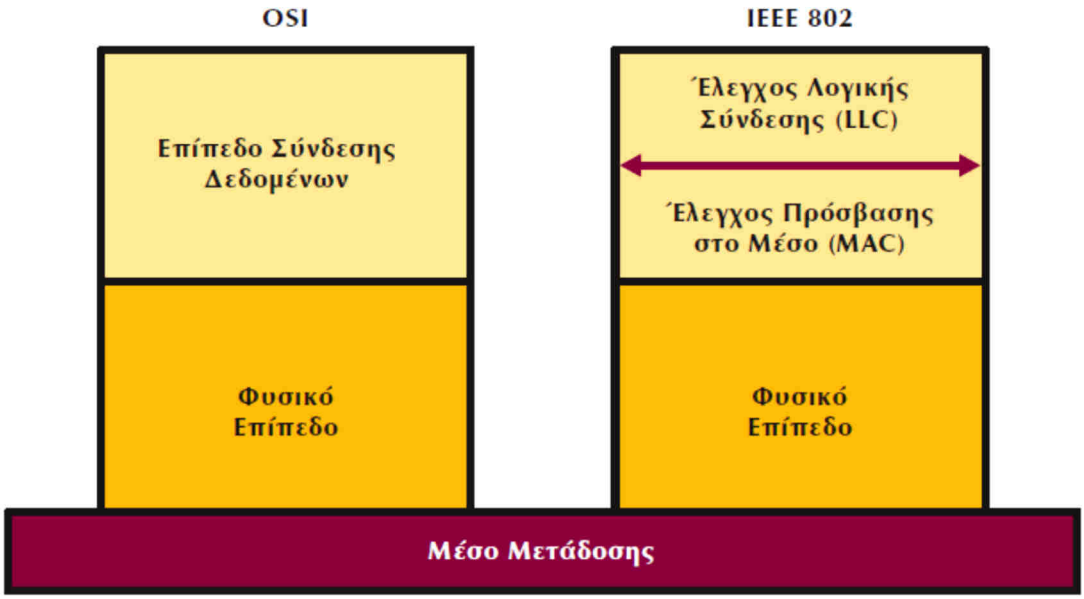
Διάφορες εταιρείες είχαν αναπτύξει τις σημαντικότερες τοπολογίες τοπικών δικτύων. Επίσης, είχαν αναπτύξει και τα πρωτόκολλα, που θα χρησιμοποιούσαν οι σταθμοί εργασίας, προκειμένου να συμμετάσχουν σε τοπικό δίκτυο. Ήταν, όμως, εμφανής η έλλειψη τυποποίησης, προκειμένου να μπορούν να επικοινωνήσουν σταθμοί εργασίας από διαφορετικούς κατασκευαστές. Η τυποποίηση των τοπικών δικτύων άρχισε με τη συνδρομή τόσο του **Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronic Engineers, IEEE)** όσο και της **Ευρωπαϊκής Ένωσης Κατασκευαστών Υπολογιστών (European Computer Manufacturing Association, ECMA)** οι οποίοι συμφώνησαν να ακολουθήσουν το μοντέλο OSI.

Όπως έχουμε ήδη αναφέρει, η ανταλλαγή μηνυμάτων και η επικοινωνία των σταθμών εργασίας μέσω δικτύου έχει αναλυθεί σε επτά επίπεδα με βάση το μοντέλο OSI. Τα δύο κατώτερα επίπεδα είναι το **επίπεδο σύνδεσης δεδομένων** και το **φυσικό επίπεδο**. Τα δύο αυτά επίπεδα καθορίζουν τον τύπο του δικτύου και το πρωτόκολλο επικοινωνίας. Η υλοποίηση των δύο αυτών επιπέδων γίνεται από συνδυασμό υλικού και λογισμικού.

Ο οργανισμός IEEE δημιούργησε επιτροπή, που είναι γνωστή σαν επιτροπή 802, με έργο τον καθορισμό προτύπων για τα τοπικά (LAN) και μητροπολιτικά (MAN) δίκτυα υπολογιστών. Τα μητροπολιτικά δίκτυα υπολογιστών έχουν χαρακτηριστικά, που βρίσκονται μεταξύ των

χαρακτηριστικών των τοπικών και των ευρέων δικτύων (παραδείγματα MAN είναι δίκτυα, που καλύπτουν μια πόλη). Το έργο της επιτροπής χωρίσθηκε αρχικά σε 6 υποεπιτροπές και η καθεμία εστιάσθηκε στην ανάπτυξη επιμέρους προτύπων για τους διαφορετικούς τύπους δικτύων. Στη συνέχεια, δημιουργήθηκαν και άλλες υποεπιτροπές. Τα αποτελέσματα της κάθε υποεπιτροπής είναι γνωστά ως IEEE 802.χ όπου χ ο αριθμός της υποεπιτροπής που έβγαλε το αποτέλεσμα.

Με βάση το έργο της επιτροπής 802, το δεύτερο επίπεδο του μοντέλου OSI χωρίσθηκε σε δύο υποεπίπεδα: στο υποεπίπεδο Ελέγχου Λογικής Σύνδεσης της γραμμής (Logical Link Control, LLC) και στο υποεπίπεδο Ελέγχου Πρόσβασης στο Μέσο (Medium Access Control, MAC).



Σχήμα 2.2.α: Σχέση μοντέλων αναφοράς OSI και IEEE 8.

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Το υποεπίπεδο Ελέγχου Λογικής Σύνδεσης περιγράφεται από το πρότυπο IEEE 802.2. Τα πρότυπα IEEE 802.3,4 και 5 περιγράφουν τους διαφορετικούς τρόπους πρόσβασης στο μέσο.

2.2.1 Έλεγχος Λογικής Σύνδεσης (LLC - IEEE 802.2)

Το πρότυπο IEEE 802.2 περιγράφει τις λειτουργίες του υποεπιπέδου LLC. Όπως έχουμε ήδη αναφέρει, το LLC είναι το ανώτερο υποεπίπεδο του επιπέδου σύνδεσης δεδομένων και είναι κοινό για τις διάφορες μεθόδους πρόσβασης στο μέσο, όπως αυτές ορίζονται από τα πρότυπα IEEE 802.3,4 και 5. Ο κύριος σκοπός του LLC είναι η παροχή υπηρεσιών στο επίπεδο δικτύου. Το επίπεδο δικτύου υποστηρίζεται από τα "Σημεία Πρόσβασης για Εξυπηρέτηση" (SAPs - Service Access Points), που παρέχει το υποεπίπεδο LLC. Το υποεπίπεδο LLC με τη σειρά του δέχεται υπηρεσίες από το κατώτερο του υποεπίπεδο ελέγχου πρόσβασης στο μέσο.

Το υποεπίπεδο LLC μπορεί να παρέχει τις παρακάτω υπηρεσίες:

- **Υπηρεσία χωρίς επιβεβαίωση και χωρίς σύνδεση (UnAcknowledged connectionless service)**

  Στην περίπτωση αυτή ένας σταθμός εργασίας στέλνει πλαίσια στο σταθμό εργασίας του προορισμού χωρίς να περιμένει επιβεβαίωση λήψης. Επίσης δεν εγκαθίσταται προκαταβολικά σύνδεση μεταξύ των δύο σταθμών και ούτε, φυσικά, τερματίζεται η

σύνδεση στο τέλος της επικοινωνίας. Εάν για διάφορους λόγους, όπως εξαιτίας θορύβου στο κανάλι επικοινωνίας, χαθεί κάποιο πλαίσιο, δεν γίνεται προσπάθεια επανάκτησής του. Η υπηρεσία αυτή προσφέρει τη μικρότερη καθυστέρηση στην επικοινωνία των σταθμών εργασίας και είναι κατάλληλη για επικοινωνία σε μέσα, που παρουσιάζουν χαμηλό ποσοστό λαθών και η επανάκτηση λανθασμένων δεδομένων γίνεται από υψηλότερα επίπεδα.

- **Υπηρεσία με επιβεβαίωση λήψης χωρίς σύνδεση (Acknowledged connectionless service)**

  Σε αυτή την υπηρεσία όπως και προηγουμένως, δεν εγκαθίσταται σύνδεση μεταξύ των σταθμών εργασίας πριν την έναρξη ανταλλαγής δεδομένων, αλλά για κάθε πλαίσιο που στέλνεται επιβεβαιώνεται η λήψη του από το σταθμό εργασίας του προορισμού. Η υπηρεσία αυτού του είδους κυρίως εφαρμόζεται, σε συνδέσεις τύπου σημείο προς σημείο (point to point).

- **Υπηρεσία με σύνδεση (Connection oriented service)**

  Είναι η πιο περίπλοκη υπηρεσία που μπορεί να παρέχει το υποεπίπεδο LLC. Ένας σταθμός εργασίας πριν αρχίσει την επικοινωνία με τον σταθμό εργασίας του προορισμού, πρέπει πρώτα να εγκαταστήσει με αυτόν ένα νοητό κύκλωμα. Επίσης γίνεται και επιβεβαίωση λήψης του κάθε πλαισίου που μεταδόθηκε. Στην υπηρεσία αυτή γίνεται επίσης και έλεγχος ροής των δεδομένων. Ο έλεγχος ροής αναφέρεται στο επίπεδο δικτύου. Η διαδικασία εγκατάστασης ενός νοητού κυκλώματος περιλαμβάνει τρία στάδια: την εγκατάσταση σύνδεσης, την μεταφορά δεδομένων και τον τερματισμό της σύνδεσης. Στην εγκατάσταση σύνδεσης οι δύο σταθμοί που πρόκειται να επικοινωνήσουν, ανταλλάσσουν κάποιες αρχικές τιμές για μεταβλητές και μετρητές που χρειάζονται για να παρακολουθήσουν την μετάδοση των πλαισίων. Στη φάση μεταφοράς δεδομένων μεταδίδονται τα πλαίσια και επιβεβαιώνεται η λήψη τους. Στη φάση τερματισμού της σύνδεσης απελευθερώνονται οι μεταβλητές και μετρητές και γενικά ότι μέσα χρησιμοποιήθηκαν για τη επίτευξη της επικοινωνίας.

(Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών)

2.2.2 Πρωτόκολλο CSMA/CD (IEEE802.3)

Πρότυπο πρόσβασης στο μέσο IEEE 802.3

Το πρότυπο IEEE 802.3 περιγράφει το πρωτόκολλο ελέγχου πρόσβασης στο φυσικό μέσο, για τοπικό δίκτυο υπολογιστών τοπολογίας αρτηρίας.

Το πρότυπο IEEE 802.3 καλύπτει τα πρωτόκολλα του φυσικού επιπέδου και του υποεπιπέδου MAC. Έτσι με το πρότυπο IEEE 802.3 καθορίζονται οι υπηρεσίες που προσφέρει το υποεπίπεδο MAC προς το υποεπίπεδο LLC που είδαμε στην προηγούμενη παράγραφο. Επίσης καθορίζεται ο τρόπος πρόσβασης του υποεπιπέδου MAC στο φυσικό μέσο. Ο τρόπος πρόσβασης στο μέσο, που χρησιμοποιείται στο πρότυπο **IEEE 802.3,** είναι γνωστός ως μέθοδος **"Πολλαπλής Προσπέλασης με Ακρόαση Φέροντος και Ανίχνευση Συγκρούσεων" (Carrier Sense Multiple Access with Collision Detection - CSMA/CD).** Τέλος καθορίζονται τα σήματα σηματοδοσίας και οι τρόποι σύνδεσης στο φυσικό μέσο. Επειδή οι τρόποι σύνδεσης με το φυσικό μέσο ποικίλουν αναλόγως με την επιλογή του φυσικού μέσου, υπάρχουν εναλλακτικά πρότυπα που θα τα παρουσιάσουμε παρακάτω. Στη συνέχεια θα περιγράψουμε τα χαρακτηριστικά της μεθόδου CSMA/CD.

Μέθοδος πρόσβασης στο μέσο CSMA/CD

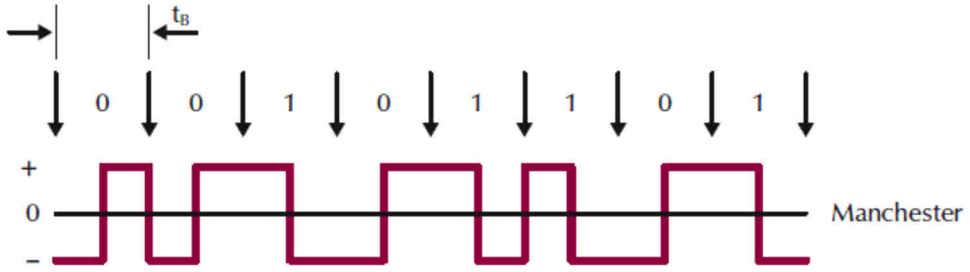
Ο συνδυασμός της μεθόδου CSMA/CD και της τοπολογίας αρτηρίας συχνά αναφέρεται ως Ethernet. Το Ethernet αναπτύχθηκε από την εταιρεία Xerox στις αρχές του 1970 και υπήρξε η βάση για την ανάπτυξη του πρωτοτύπου IEEE 802.3. Υπάρχουν δύο εκδόσεις του Ethernet (η I και η II). Η αρχική έκδοση του Ethernet (η I) δεν ήταν συμβατή με το IEEE 802.3, αλλά η έκδοση II είναι βασικά η ίδια με το IEEE 802.3. Σήμερα, ο όρος Ethernet συχνά αναφέρεται σε όλα τα δίκτυα, που χρησιμοποιούν τη μέθοδο CSMA/CD και γενικά συμμορφώνονται με το πρότυπο Ethernet ή τις διάφορες εκδοχές του IEEE 802.3.

Ο αλγόριθμος πρόσβασης στο μέσο έχει ως εξής:

Όλοι οι σταθμοί εργασίας, που συνδέονται στο ίδιο φυσικό μέσο και είναι ενεργοί, πρέπει να ακούσουν το μέσο (καλώδιο). Εάν το μέσο μετάδοσης είναι απασχολημένο, ο σταθμός εργασίας που θέλει να μεταδώσει δεδομένα, θα πρέπει να περιμένει έως ότου ελευθερωθεί. Όταν το μέσο είναι ελεύθερο, ο σταθμός εργασίας ξεκινά αμέσως τη μετάδοση των πλαισίων του. Εάν την ίδια χρονική στιγμή, που το μέσο ελευθερώνεται, υπάρξουν και άλλοι σταθμοί εργασίας, που θέλουν να μεταδώσουν στο μέσο, θα δημιουργηθεί το φαινόμενο της σύγκρουσης (collision). Στην περίπτωση αυτή, οι σταθμοί, που προσπάθησαν ταυτόχρονα να εκπέμψουν, θα αντιληφθούν το φαινόμενο και θα μεταδώσουν σύντομο σήμα, που θα αναφέρει την ύπαρξη σύγκρουσης και θα σταματήσουν την εκπομπή των υπόλοιπων πλαισίων τους, εάν βέβαια έχουν απομείνει και άλλα προς μετάδοση. Μετά το σήμα γνωστοποίησης της σύγκρουσης, οι σταθμοί που συμμετείχαν στη σύγκρουση θα περιμένουν κάποιο τυχαίο χρονικό διάστημα πριν επιχειρήσουν ξανά τη μετάδοση.

Μια πολύ κρίσιμη παράμετρος, η οποία επηρεάζει και την απόδοση της μεθόδου, είναι ο χρόνος, που απαιτείται για την ανίχνευση σύγκρουσης. Όπως έχουμε αναφέρει, όλοι οι σταθμοί εργασίας, που συνδέονται στο φυσικό μέσο με την μέθοδο CSMA/CD, πρέπει να παρατηρούν συνέχεια το μέσο. Επομένως, όταν ένας σταθμός αρχίσει να μεταδίδει πλαίσια στο μέσο και συμβεί σύγκρουση, ο σταθμός θα την αντιληφθεί, επειδή και ο ίδιος θα αντιληφθεί ότι τα πλαίσια, που έχει μεταδώσει στο μέσο, είναι αλλοιωμένα, λόγω του θορύβου, που θα προκληθεί, από την ταυτόχρονη εκπομπή πλαισίων (στην ουσία ηλεκτρικών σημάτων) από τους άλλους σταθμούς. Πρέπει, επομένως, η ανίχνευση της σύγκρουσης από το σταθμό εργασίας να γίνει σε χρόνο μικρότερο από τη διάρκεια μετάδοσης του συνόλου των πλαισίων. Αυτή η παρατήρηση δημιουργεί αυτόματα περιορισμούς στο μέγιστο μήκος του καλωδίου, καθώς και στους ρυθμούς μετάδοσης των σταθμών εργασίας. Ας πάρουμε την περίπτωση σταθμού εργασίας Α, που αρχίζει να μεταδίδει τη χρονική στιγμή t_0. Ας υποθέσουμε, επίσης, ότι ο σταθμός Α, που ξεκινά τη μετάδοση στη χρονική στιγμή to, βρίσκεται στη μια άκρη του καλωδίου και ότι ο χρόνος μετάδοσης του σήματος από τη μια άκρη στη άλλη είναι τ. Στην αντίθετη άκρη του καλωδίου υπάρχει σταθμός Β, που ξεκινά τη μετάδοση τη στιγμή t_0 + τ-χ. Όπως είναι φυσικό, ο Β θα αντιληφθεί τη σύγκρουση μετά από χρόνο χ και θα σταματήσει τη μετάδοση. Ο σταθμός Α, όμως, θα χρειαστεί χρόνο 2τ-χ, για να αντιληφθεί τη σύγκρουση, γιατί τόσο χρόνο χρειάζονται τα αλλοιωμένα πλέον πλαίσια να φθάσουν σ'αυτόν. Επομένως, ένας σταθμός δεν μπορεί να είναι σίγουρος, ότι βρήκε το μέσο ελεύθερο, παρά μόνο όταν περάσει χρόνος 2τ χωρίς να γίνει σύγκρουση. Κατά συνέπεια, το μήκος των πλαισίων, θα πρέπει να είναι τέτοιο, ώστε να επιτρέπει την ανίχνευση των συγκρούσεων πριν από το τέλος της μετάδοσης. Η υλοποίηση του μηχανισμού CSMA/CD καθορίζει, ότι το μέγιστο μήκος πλαισίου δεν πρέπει να είναι μεγαλύτερο από 1518 οκτάδες (bytes), ενώ το ελάχιστο κάτω από 64 οκτάδες. Επίσης, εάν το μήκος του καλωδίου είναι πολύ μεγάλο, οι συγκρούσεις ποτέ δεν θα ανιχνεύονται έγκαιρα. Ακόμα γίνεται αντιληπτό, ότι τα σήματα δεν θα πρέπει να έχουν στάθμη 0 Volt, γιατί σύγκρουση δύο σημάτων, που αντιστοιχούν σε μηδενική στάθμη δεν θα ανιχνευθεί. Για το λόγο αυτό, η μετάδοση των σημάτων γίνεται με βάση την ευρέως

χρησιμοποιούμενη κωδικοποίηση Manchester. Στην κωδικοποίηση Manchester, το καλώδιο μπορεί να βρίσκεται σε μία από τις τρεις καταστάσεις: η μετάδοση ενός bit 0 γίνεται με μετάβαση από χαμηλή σε υψηλή στάθμη, η μετάδοση ενός bit 1 γίνεται με μετάβαση από υψηλή σε χαμηλή στάθμη, ενώ τέλος κατάσταση χωρίς σήμα (αδρανές) ισοδυναμεί σε 0 Volts. Η υψηλή στάθμη σήματος είναι +0,85 Volts, ενώ η χαμηλή -0,85 Volts.



Σχήμα 2.2.1.α: Κωδικοποίηση Manchester.
(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Ένα θέμα, που πρέπει επίσης να εξετασθεί, είναι για πόσο χρόνο ένας σταθμός εργασίας, αφού ανιχνεύσει τη σύγκρουση, θα απέχει από τη μετάδοση. Είναι προφανές, ότι ο χρόνος δεν θα πρέπει να είναι σταθερός και ίδιος για όλους τους σταθμούς εργασίας, γιατί έτσι θα οδηγηθούμε σε διαδοχικές και συνεχείς συγκρούσεις. Για το λόγο αυτό χρησιμοποιείται αλγόριθμος για τον υπολογισμό της καθυστέρησης επαναμετάδοσης για κάθε σταθμό χωριστά, εξασφαλίζοντάς τους τυχαίο χρόνο επανεκπομπής.

Σημείωση: Στα δίκτυα Ethernet 10 Mbps γίνεται χρήση της κωδικοποίησης Manchester. Στα δίκτυα Ethernet 100 Mbps (Fast Ethernet) υπάρχουν πολλά διαφορετικά διαθέσιμα συστήματα κωδικοποίησης, τα οποία εξαρτόνται από τη συγκεκριμένη τεχνική που υλοποιείται. Τέτοια πρότυπα κωδικοποίησης είναι τα **MLT-3 (MultiLevel Transition)**, **NRZI (Non-Return to Zero, Inverted)**, **T4 Multiplexing**, **4B/5B και 8B/6T**. Αντίστοιχα, σε δίκτυα Ethernet 1000 Mbps (Gigabit Ethernet) χρησιμοποιείται η κωδικοποίηση 8B/10B.

Σε αυτό το σημείο θα αναφέρουμε ότι παλαιότερα υπήρχαν στο επίπεδο πρόσβασης στο μέσο επίσης τα πρότυπα IEEE 802.4-Αρτηρία με Κουπόνι (Token Bus) και IEEE 802.5-Δακτύλιος με Κουπόνι (Token Ring), τα οποία θεωρούνται πλέον παρωχημένα και αναφέρονται αναλυτικά στην ενότητα Π.1 του Παραρτήματος.

2.3 Μετάδοση Βασικής και Ευρείας ζώνης

Η πιο απλή μορφή σήματος είναι το απλό ημιτονικό σήμα το οποίο έχει μόνο μια συχνότητα. Όλα τα άλλα όμως, σύνθετα σήματα, περιλαμβάνουν μια μικρή ως μεγάλη περιοχή συχνοτήτων ανάλογα με τη μορφή τους.

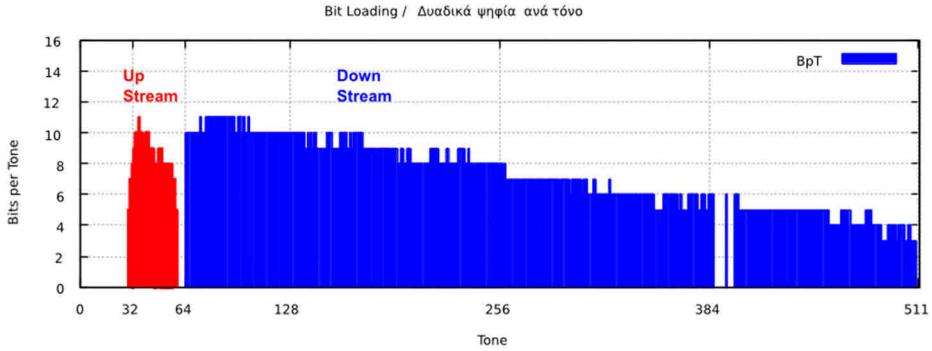
Ως **Βασική Ζώνη (Baseband)** αναφέρεται η περιοχή συχνοτήτων που περιλαμβάνει ένα σήμα, στην αρχική του μορφή, πριν μεταφερθεί σε άλλη περιοχή συχνοτήτων με κάποια διαδικασία μετατροπής ή διαμόρφωσης. Για παράδειγμα ένα ακουστικό σήμα, στη βασική του ζώνη είναι από 20Hz, σχεδόν συνεχές (D.C. - “0” Hz) μέχρι 20kHz. Το ακουστικό σήμα ομιλίας, για τις τηλεπικοινωνιακές ανάγκες, περιορίζεται μέχρι τα 3,4kHz περίπου, επειδή η χρήσιμη πληροφορία που μεταφέρει (κατανόηση του τι λέει κάποιος και αναγνώριση ποιος είναι) βρίσκεται μέχρι αυτή τη συχνότητα. Η βασική του ζώνη είναι περίπου 4kHz. Για τις ανάγκες των διαφόρων τηλεπικοινωνιακών συστημάτων, αυτή η βασική ζώνη μεταφέρεται σε υψηλότερες συχνότητες με κάποια διαδικασία διαμόρφωσης ώστε να εκπεμφθεί προς τον προορισμό. Εκεί με τη διαδικασία της αποδιαμόρφωσης αποκαθίσταται στην βασική

του ζώνη ώστε να μπορεί να χρησιμοποιηθεί. Έτσι λειτουργούν τα συστήματα κλασικής τηλεφωνίας με πολυπλεξία συχνότητας και οι ραδιοφωνικές μεταδόσεις.

Σχήμα 2.3.α: Βασική ζώνη (Low Pass).

Τα ψηφιακά σήματα, συνήθως έχουν μεγαλύτερη περιοχή συχνοτήτων η οποία μεγαλώνει όσο αυξάνεται η ταχύτητα μετάδοσης. Η βασική τους ζώνη εκτείνεται σε μεγαλύτερη περιοχή. Όταν μεταδίδονται χωρίς καμιά άλλη επεξεργασία (π.χ. διαμόρφωση), όπως είναι από τη δημιουργία τους, στη βασική τους ζώνη τότε λέμε ότι η **μετάδοση** είναι **βασικής ζώνης**. Στο φυσικό μέσο ταξιδεύει αποκλειστικά μόνο ένα σήμα. Ο όρος μετάδοση βασικής ζώνης καθιερώθηκε με το Ethernet καθώς κατά τη μετάδοση δεν χρησιμοποίησε καμιά επεξεργασία παρά μόνο κατάλληλη κωδικοποίηση, Manchester στην αρχή και διαφορετικές στις επόμενες εκδόσεις.

Ο όρος “Broadband” είναι συνώνυμος με τον όρο “wide band” ο οποίος αποδίδεται ως **ευρεία ζώνη**. Στις τηλεπικοινωνίες αναφέρεται στη δυνατότητα της **μετάδοσης ευρείας ζώνης** να μεταφέρει ταυτόχρονα πολλά σήματα ή κίνηση διαφορετικής μορφής και περιεχομένου όπως βίντεο, φωνή και δεδομένα. Για το χαρακτηρισμό ενός σήματος ή μιας μετάδοσης ως “broadband” ισχύουν διαφορετικά κριτήρια ανάλογα με τα συμφραζόμενα. Στη φυσική, την ακουστική και την ηλεκτρονική, η σημασία του όρου είναι απλώς ευρεία ζώνη. Στις ψηφιακές μεταδόσεις όμως χρησιμοποιείται για να προσδιορίσει την ταυτόχρονη μετάδοση δεδομένων από περισσότερα στενότερα μη επικαλυπτόμενα κανάλια. Για παράδειγμα στο ADSL, το εύρος ζώνης της αφόρτιστης τηλεφωνικής γραμμής χωρίζεται σε 256 ή 512 κανάλια (τα ονομάζει “τόνους”) των 4,3125kHz και από καθένα απ' αυτά διέρχονται από 2 ως 15 bit ταυτόχρονα ώστε να επιτευχθούν μεγάλες ταχύτητες. Στην εικόνα 2.3.β φαίνεται η χρήση του εύρους ζώνης της γραμμής ενός συνδρομητή το οποίο μοιράζεται μεταξύ τηλεφωνίας ISDN και μετάδοσης ADSL2+. Τα πρώτα 32 κανάλια (0-31, 138kHz) έχουν αφεθεί ελεύθερα για χρήση τηλεφωνίας ISDN και τα υπόλοιπα (32-511, έως 2208kHz) για χρήση μετάδοσης δεδομένων. Παρατηρήστε ότι καθώς αυξάνει η συχνότητα, προς τα δεξιά, όλο και λιγότερα ψηφία μπορούν να μεταφερθούν στα αντίστοιχα κανάλια. Η ταχύτητα που μετρήθηκε, στη συγκεκριμένη γραμμή, ήταν Max: Upstream rate = 948 Kbps, Downstream rate = 12356 Kbps.



Εικόνα 2.3.β: Μετάδοση σε γραμμή ADSL (over ISDN) - 512 τόνοι/κανάλια των 4,3125kHz.

2.4 Δίκτυα ETHERNET (10/100/1000Mbps)

Βασικά Πρότυπα του IEEE 802.3. Προκειμένου να καλυφθούν οι διάφοροι συνδυασμοί φυσικών μέσων μεταφοράς και ρυθμοί δεδομένων, το πρότυπο IEEE 802.3 έχει προβεί στην έκδοση κάποιων παραλλαγών. Με την πάροδο του χρόνου ολοένα και περισσότερες παραλλαγές προστίθενται στα βασικά πρότυπα του IEEE 802.3.

Η κωδικοποίηση των βασικών προτύπων γίνεται ως εξής:

XBase/BroadbandY

όπου: **X** η ταχύτητα μετάδοσης των δεδομένων σε Mbps

Base/Broadband ο τύπος σηματοδοσίας, που χρησιμοποιείται

Y αντιστοιχεί στο μέγιστο μήκος του τμήματος (segment)

Στον πίνακα 2.4.α αναφέρονται τα βασικά πρότυπα του IEEE 802.3 και τα χαρακτηριστικά τους.

Τύπος Δικτύου	Μέσο Μετάδοσης	Μέθοδος Σηματοδοσίας	Ρυθμός Δεδομένων	Μέγιστο μήκος τμήματος	Τοπολογία
10Base5	Ομοαξονικό 50 Ohm thick	Βασικής ζώνης	10 Mbps	500 m	Αρτηρίας
10Base2	Ομοαξονικό 50 Ohm thin (RG-58)	Βασικής ζώνης	10 Mbps	185 m	Αρτηρίας
1Base5	Αθωράκιστο συνεστραμμένο (UTP)	Βασικής ζώνης	1 Mbps	250 m	Αστέρα
10BaseT	Αθωράκιστο συνεστραμμένο (UTP)	Βασικής ζώνης	10 Mbps	100 m	Αστέρα
10Broad36	Ομοαξονικό 75 Ohm	Ευρυζωνική	10 Mbps	3600 m	Αρτηρίας

Πίνακας 2.4.α: Βασικά πρότυπα του IEEE 802.3 και τα χαρακτηριστικά τους.

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Το Ethernet II είναι παρόμοιο με το 10base5.

Πέρα από τις βασικές εκδόσεις του IEEE 802.3 που αναφέρονται στον παραπάνω πίνακα, έχουν παρουσιαστεί και άλλες εκδόσεις, όπως οι εκδόσεις για οπτική ίνα ως φυσικό μέσο μετάδοσης (Fiber Ethernet). Η κωδικοποίηση που χρησιμοποιείται είναι: 10Base-F.

10Base -F: Fiber Ethernet. Το 10Base-F βασίζεται στην προδιαγραφή FOIRL (Fiber Optic Inter-Repeater Link), που δημιουργήθηκε για τη διασύνδεση επαναληπτών με οπτικές ίνες. Η πιο συχνά χρησιμοποιούμενη οπτική ίνα είναι η διπλή πολύτροπη 62.5/125 μm για τη μεταφορά υπέρυθρης ακτινοβολίας φωτός από LEDs. Η πιο γνωστή έκδοση είναι η 10Base-FL και χρησιμοποιείται στη διασύνδεση κυρίως επαναληπτών (repeaters) σε απόσταση μέχρι και 2Km.

Η χρήση οπτική ίνας χρησιμοποιείται όταν θέλουμε να συνδέσουμε σημεία, που απέχουν αρκετά μεταξύ τους (μέχρι 2Km), και όταν υπάρχει αυξημένος ηλεκτρομαγνητικός θόρυβος (π.χ. βιομηχανίες). Το μειονέκτημα, όμως, της οπτικής ίνας είναι το αυξημένο κόστος και η

δυσκολία, που παρουσιάζει στην εγκατάσταση και το χειρισμό της (π.χ. δεν μπορούμε να την τσακίσουμε για το σχηματισμό γωνίας).

Ethernet υψηλών ταχυτήτων. Στην προηγούμενη παράγραφο παρουσιάσαμε τα βασικά πρότυπα του IEEE 802.3. Όπως έχουμε, ήδη, αναφέρει νέες εκδόσεις του IEEE 802.3 αναπτύσσονται και γίνονται πρότυπα με την πάροδο του χρόνου. Στη συνέχεια, θα παρουσιάσουμε δύο νέα πρότυπα: το IEEE 802.3u (Fast Ethernet) και το IEEE 802.3z (Gigabit Ethernet)

Fast Ethernet. Το Fast Ethernet παρέχει εύρος ζώνης 100Mbps. Εκτός από το δεκαπλασιασμό της ταχύτητας, που παρέχει το Fast Ethernet, δόθηκε ιδιαίτερη προσοχή στο να μην διαταραχθεί κατά το δυνατόν η υπάρχουσα καλωδιακή υποδομή. Έτσι ανάλογα με το χρησιμοποιούμενο φυσικό μέσο, δημιουργήθηκαν διάφορα επιμέρους πρότυπα: το 100Base-TX, 100Base-FX και 100Base-T4.

- **100Base-TX:** Ως φυσικό μέσο μπορεί να χρησιμοποιηθεί καλώδιο UTP (αθωράκιστο) κατηγορίας 5, ή καλώδιο STP (θωρακισμένο). Η απόσταση του τμήματος μπορεί να φθάσει μέχρι τα 100 μέτρα. Για τη μετάδοση των δεδομένων χρησιμοποιούνται τα δύο από τα τέσσερα ζεύγη του καλωδίου, ένα ζεύγος για κάθε κατεύθυνση. Επίσης, για λόγους χρονισμού κυκλοφορούν πάντα σύμβολα και στα δύο ζεύγη, είτε αυτά είναι πραγματικά δεδομένα είτε ειδικά σύμβολα στην περίπτωση, που δεν υπάρχει δραστηριότητα στο δίκτυο. Τα ζεύγη, που δεν χρησιμοποιούνται, συνήθως τερματίζονται.
- **100Base-T4:** Το φυσικό μέσο μπορεί να είναι καλώδιο UTP κατηγορίας 3 και πάνω. Στο πρότυπο αυτό γίνεται χρήση και των τεσσάρων ζευγών του καλωδίου και αυτό αποτελεί μειονέκτημα στην περίπτωση, που υπάρχουν παλαιότερες εγκαταστάσεις και χρησιμοποιούν μόνο τα δύο ζεύγη. Στα ζεύγη υπάρχει σήμα μόνο, όταν έχουμε μεταφορά δεδομένων. Η μέγιστη απόσταση ενός τμήματος είναι τα 100 μέτρα. Τα τρία ζεύγη χρησιμοποιούνται για μετάδοση δεδομένων, ενώ το τέταρτο για αναγνώριση (λήψη) των συγκρούσεων. Το 100- BaseT4, αντίθετα με το 100BaseTX, δεν χρησιμοποιεί ξεχωριστά κανάλια για εκπομπή και λήψη και για τον λόγο αυτό δεν είναι δυνατή η αμφίδρομη μετάδοση δεδομένων.
- **100Base-FX:** Μπορούμε να χρησιμοποιήσουμε διπλή πολύτροπη (62.5/125μm) ή μονότροπη οπτική ίνα. Το μήκος τμήματος για την περίπτωση χρήσης πολύτροπης ίνας είναι 412 μέτρα σε επικοινωνία half-dublex και 2 χιλιόμετρα σε επικοινωνία full-dublex. Για μονότροπη ίνα η απόσταση τμήματος μπορεί να φθάσει τα 25 χιλιόμετρα.

Gigabit Ethernet. Το gigabit Ethernet IEEE 802.3z είναι το νεώτερο πρότυπο του IEEE 802.3. Προσφέρει επικοινωνία στο δίκτυο με εύρος ζώνης τα 1000 Mbps. Υπάρχει συμβατότητα στην καλωδίωση και κυρίως για χρήση καλωδίων βελτιωμένων κατηγορίας 5 (cat 5 enhance). Το 1000BaseT είναι πρότυπο για καλώδια τύπου cat 5e. Το gigabit Ethernet έχει πρότυπα στην περίπτωση χρήσης οπτικών ινών. Ετσι για πολύτροπη οπτική ίνα 62.5 μm στο πρότυπο 1000BaseSX το μέγιστο μήκος μπορεί να φθάσει τα 275 μέτρα, ενώ για ίνα 50 μm τα 550 μέτρα. Στο πρότυπο 1000BaseLX για πολύτροπη ίνα 62.5 ή 50 microns το μέγιστο μήκος φθάνει τα 550 μέτρα και με μονότροπη ίνα των 9 μm μπορεί να φθάσει τα 5km (πίνακας 2.4.β).

ΟΝΟΜΑ	ΜΕΣΟ ΜΕΤΑΔΟΣΗΣ	ΜΕΓΙΣΤΟ ΜΗΚΟΣ ΤΜΗΜΑΤΟΣ	ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ
1000Base-SX	ΟΠΤΙΚΗ ΙΝΑ	550 m	Πολύτροπη (50 μm)
1000Base-LX	ΟΠΤΙΚΗ ΙΝΑ	5000 m	Μονότροπη (9 μm)
1000Base-CX	ΧΑΛΚΙΝΟ ΚΑΛΩΔΙΟ - 2 ΖΕΥΓΗ STP (Θωρακισμένο συνεστραμμένο)	25 m	STP
1000Base-T	ΧΑΛΚΙΝΟ ΚΑΛΩΔΙΟ - 4 ΖΕΥΓΗ UTP (Αθωράκιστο συνεστραμμένο)	100 m	Cat. 5 UTP

Πίνακας 2.4.β. Βασικά πρότυπα του IEEE 802.3z και τα χαρακτηριστικά τους.

(*Προσαρμογή από πηγή: http://web.cs.wpi.edu/~rek/Undergrad_Nets/B06/Fast_Ethernet.pdf*)

Επισήμανση: Θα λέγαμε ότι το gigabit Ethernet δημιουργεί νέες δυνατότητες στο χώρο των τοπικών δικτύων με την πραγματικά τεράστια ταχύτητα, που μπορεί να προσφέρει. Ειδικά με την τυποποίηση του 1000BaseT γίνεται πολύ ελκυστικό, γιατί μπορεί να εκμεταλλευθεί την υπάρχουσα καλωδιακή υποδομή που στην πλειοψηφία της είναι τύπου cat 5.

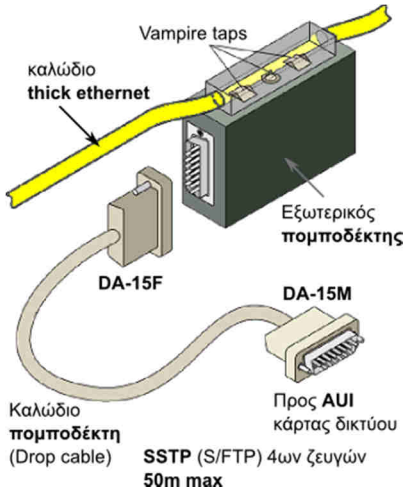
Ήδη όλοι οι κατασκευαστές δικτυακού εξοπλισμού έχουν να επιδείξουν αρκετά μεγάλη γκάμα από gigabit switches και σε πολύ ανταγωνιστικότερες τιμές από άλλες τεχνολογίες με μικρότερο προσφερόμενο εύρος ζώνης.

Οι νεότερες εκδόσεις των Gigabit Ethernet δικτύων μεταφέρουν τα δεδομένα σε 10 gigabits ανά δευτερόλεπτο, 40 gigabits ανά δευτερόλεπτο και 100 gigabits ανά δευτερόλεπτο. Τα δίκτυα αυτά είναι γνωστά ως δίκτυα των 10Gb, των 40Gb και των 100Gb Ethernet, ενώ υπό ανάπτυξη βρίσκονται τα δίκτυα των 400Gb.

2.4.1 Τα φυσικά μέσα – κωδικοποίηση

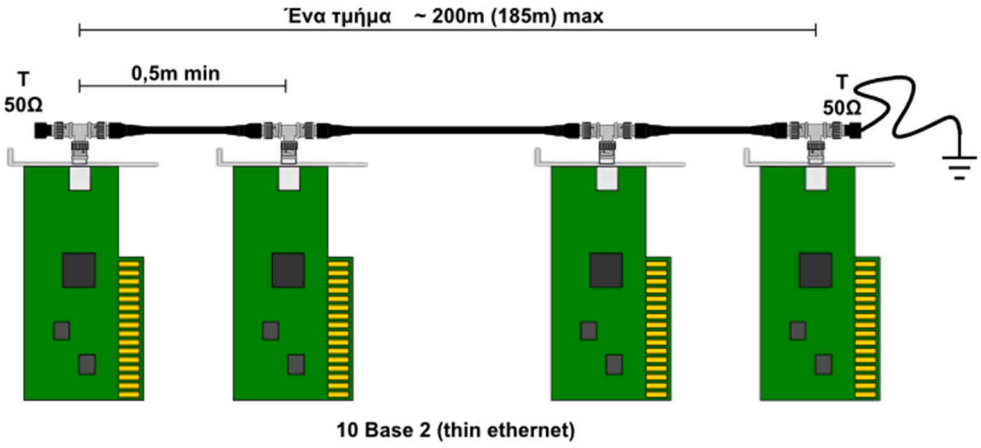
Το δίκτυο **Ethernet** προτυποποιήθηκε από την ομάδα εργασίας 802.3 του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών ως **IEEE802.3**, το 1983, μετά τη δημοσίευση του προτύπου Ethernet II από τη σύμπραξη των εταιρειών DEC, Intel και Xerox (DIX - 1982). Επιτύγχανε ονομαστική ταχύτητα ημιαμφίδρομης (half duplex) μεταφοράς δεδομένων **10Mbps**. Αρχικά προέβλεπε χρήση **διαμοιραζόμενου μέσου** (shared medium) και ως τέτοιο χρησιμοποιούσε **ομοαξονικό καλώδιο** διαμέτρου περίπου 10mm με διπλή θωράκιση, μονόκλωνο κεντρικό αγωγό και χαρακτηριστική σύνθετη αντίσταση (εμπέδηση) **50Ω**. Είχε χαρακτηριστικό κίτρινο χρώμα και έμοιαζε, μηχανικά και ηλεκτρικά με το καλώδιο τύπου **RG-8**. Κατάλληλο καλώδιο για τέτοια χρήση είναι το 9880 της Belden.

Εικόνα 2.4.1.α: Καλώδιο Thick Ethernet και συνδετήρας τύπου Ν.



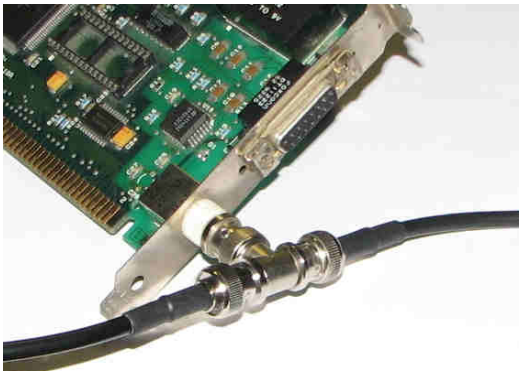
Εικόνα2.4.1.β: Εξ. πομποδέκτης Thick Ethernet.

Γρήγορα όμως (1986), εξαιτίας της δυσκαμψίας του καλωδίου και της σχετικής δυσκολίας στον χειρισμό και τον τερματισμό του σε συνδετήρες (connectors) **τύπου Ν**, αντικαταστάθηκε σε χρήση από το λεπτότερο (5mm), πιο εύκαμπτο (πολύκλωνος κεντρικός αγωγός) και πιο εύκολα διαχειρίσιμο επίσης **ομοαξονικό καλώδιο RG-58**. Και το καλώδιο αυτό έχει χαρακτηριστική εμπέδηση 50Ω αλλά χρησιμοποιεί συνδετήρες (connectors) **τύπου BNC**. Με τη χρήση του λεπτότερου καλωδίου, το δίκτυο απέκτησε το προσωνύμιο **thin Ethernet** και κατ' αναλογία το δίκτυο με χρήση του καλωδίου των 10mm χαρακτηρίστηκε **thick Ethernet**. Το thin Ethernet επικράτησε σε περιβάλλοντα γραφείων στα τέλη της δεκαετίας του 1980 και στις αρχές της δεκαετίας του 1990.



Εικόνα 2.4.1.γ: Δίκτυο Thin Ethernet (10Base2).

Και στις δυο περιπτώσεις, thick και thin Ethernet, τα καλώδια συνθέτουν μια επιμήκη **αρτηρία** η οποία τερματίζεται στα δυο άκρα σε **τερματικές αντιστάσεις των 50Ω** ενώ το ένα μόνο άκρο γειώνεται. Ενδιάμεσα, για τη σύνδεση των σταθμών παρεμβάλλονται για το thin Ethernet **συνδετήρες Τ** (T connectors) απευθείας πάνω στην κάρτα δικτύου ενώ στο thick Ethernet χρησιμοποιούνται **εξωτερικοί πομποδέκτες** πάνω στο καλώδιο οι οποίοι συνδέονται στη κάρτα δικτύου μέσω ειδικού καλωδίου 4ων ζευγών με συνδετήρες DA-15.



Εικόνα 2.4.1.δ: Σύνδεση Thin Ethernet σε κάρτα δικτύου.

Εικόνα 2.4.1.ε Τερματική αντίσταση τύπου Ν, τύπου BNC και Τ τύπου BNC.

Λίγο αργότερα (1987), προδιαγράφηκε και η χρήση **οπτικής ίνας**, αρχικά για τη διασύνδεση απομακρυσμένων επαναληπτών (FOIRL - Fiber Optic Inter Reteater Linking) σε αποστάσεις 1km. Τελικά, μετά την εισαγωγή σε χρήση των συνεστραμμένων καλωδίων (10BaseT), τυποποιήθηκε το 1993, στο πρότυπο 10BaseFL με μέγιστη απόσταση 2km και στη συνέχεια υποστήριξε πλήρως αμφίδρομη (full duplex) επικοινωνία.

Στον πίνακα 2.4.1.α φαίνονται συγκεντρωτικά τα χαρακτηριστικά των δικτύων Ethernet, 10Base5, 10Base2 και 10BaseFL.

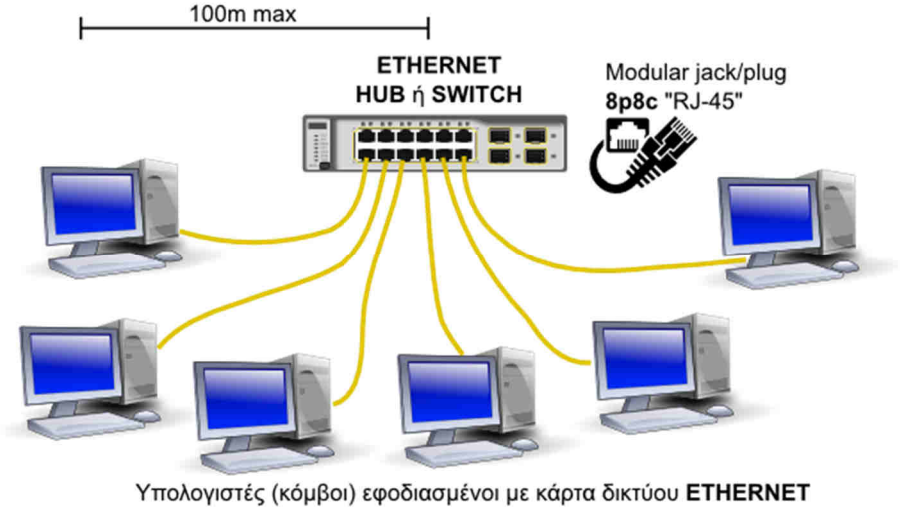
	Thick Ethernet [1983] (10Base5)	**Thin Ethernet [1986] (10Base2)**	**10BaseFL [1993] / (FOIRL - [1987])**
Μετάδοση / ταχύτητα Πρόσβαση στο μέσο	Βασικής ζώνης / 10 Mbps, Half Duplex IEEE802.3 (CSMA/CD)	Βασικής ζώνης / 10 Mbps, Half Duplex IEEE802.3 (CSMA/CD)	Βασικής ζώνης / 10 Mbps, Half Duplex (και αργότερα FDX) IEEE802.3 (CSMA/CD)
Τοπολογία/Μέγιστο μήκος τμήματος	Αρτηρία, 500m	Αρτηρία, 185m	Σημείο προς σημείο
Μέγ. αριθμός τμημάτων (με Η/Υ)	5 (3)	5 (3)	1
Μέγ. αριθμός κόμβων ανά τμήμα	100	30	2
Συνολικό μέγ. μήκος καλωδίωσης	2,5km	925m	2km (FOIRL: 1km)
Είδος καλωδίου (Zo)	τύπου RG-8 (50Ω)	RG-58 (50Ω)	850nm - Διπλή πολύτροπη οπτική ίνα 62,5/125 μm
Είδος συνδετήρων	τύπου **N**	τύπου **BNC**	τύπου **ST**
Πομποδέκτης	Εξωτερικός	Ενσωματωμένος (ή εξωτερικός)	Ενσωματωμένος (ή εξωτερικός)
Καλώδιο πομποδέκτη	SSTP (S/FTP) 4x2, 50m max	- (<<--)	- (<<--)

Επεκτασιμότητα	5 τμήματα (segments), 4 επαναλήπτες (repeaters), 3 τμήματα με κόμβους (populated)	-

Πίνακας 2.4.1.α: Χαρακτηριστικά δικτύων Ethernet 10Mbps με χρήση ομοαξονικών καλωδίων και οπτικών ινών.

Παρότι η χρήση του καλωδίου RG-58 (thin Ethernet) επέτρεψε τη φτηνότερη και ευκολότερη εγκατάσταση τοπικών δικτύων Ethernet, με την υιοθέτηση των κατά πολύ φτηνότερων καλωδίων συνεστραμμένων ζευγών (10BaseT), η χρήση ομοαξονικών καλωδίων εγκαταλείφθηκε οριστικά. Τα ομοαξονικά καλώδια δεν εγκαταλείφθηκαν λόγω επιδόσεων. Είναι εξαιρετικά ως προς τα ηλεκτρικά τους χαρακτηριστικά, είναι θωρακισμένα και έχουν ιδιαίτερα χαμηλή εξασθένηση. Όμως είναι σημαντικά ακριβότερα και απαιτούν ιδιαίτερες δεξιότητες στον χειρισμό και τον τερματισμό τους σε συνδετήρες (connectors). Η χρήση τους επανήλθε στο χώρο των ασύρματων δικτύων για τη διασύνδεση του ασύρματου εξοπλισμού με τις κεραίες και για τη δουλειά αυτή, στις περιοχές συχνοτήτων των 2,4 και 5,8GHz, αποτελούν μοναδική λύση.

Τα καλώδια συνεστραμμένων ζευγών χρησιμοποιούνταν στη βιομηχανία των τηλεπικοινωνιών για πολλά χρόνια και υπήρχε ευρεία τεχνογνωσία γύρω από αυτά και τα εξαρτήματά τους. Έτσι προς το τέλος της δεκαετίας του 1980 προτάθηκε η χρήση τους για την υλοποίηση δικτύων Ethernet και ακολούθησε η τυποποίηση από το IEEE το 1990 ως IEEE802.3i γνωστότερο ως **10BaseT**. Το δίκτυο Ethernet 10BaseT χρησιμοποιεί κεντρικό **Διανομέα (HUB)** ο οποίος είναι ουσιαστικά ένας **επαναλήπτης πολλών θυρών** με θύρες τύπου RJ-45 στις οποίες συνδέονται οι κόμβοι σε μια φυσική **τοπολογία αστέρα** (ένας κόμβος σε κάθε θύρα) με μέγιστη απόσταση κόμβου - Hub τα **100m**. Το καλώδιο που χρησιμοποιείται είναι τεσσάρων **αθωράκιστων συνεστραμμένων ζευγών** (**UTP** - Unshielded Twisted Pair) **κατηγορίας 3** (Cat3) από τα οποία χρησιμοποιούνται μόνο τα δύο ζεύγη.

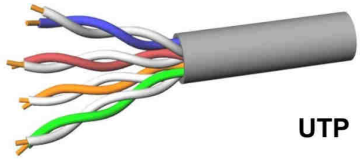


Εικόνα 2.4.1.στ: Δίκτυο Ethernet με χρήση καλωδίων συνεστραμμένων ζευγών.

Το δίκτυο Ethernet συνεχίζει την εξέλιξή του και από το 1995 υποστηρίζει ταχύτητα μετάδοσης **100 Mbps** (100Base-TX) ενώ από το 1998 έφτασε τα **1000 Mbps** ή **1 Gbps** (1000Base-T) αρχικά με χρήση οπτικής ίνας (IEEE802.3z) αλλά στη συνέχεια με χρήση καλωδίου UTP (IEEE802.3ab). Από το 1997 υποστηρίζει **πλήρως αμφίδρομη επικοινωνία**. Το σημαντικό για την επικράτηση και εξάπλωση του Ethernet είναι η προς τα πίσω συμβατότητα με τις παλαιότερες εκδόσεις του η οποία διευκολύνεται από τη χρήση ίδιων

φυσικών μέσων (αθωράκιστα συνεστραμμένα ζεύγη, κατηγορίας CAT 5/5e και καλύτερης). Έτσι κυκλοφορούν κάρτες δικτύου Ethernet **10/100/1000Mbps** που υποστηρίζουν οποιαδήποτε από τις τρεις ταχύτητες. Η **αυτόματη διαπραγμάτευση** είναι απαίτηση του προτύπου για τα 1000Mbps. Η μέγιστη απόσταση που καλύπτουν οι κάρτες δικτύου Ethernet 10/100/1000Mbps με χρήση συνεστραμμένων ζευγών UTP Cat 5e και καλύτερης, είναι **100m**. Παράλληλα υπάρχουν κάρτες οι οποίες υποστηρίζονται από διπλές πολύτροπες ή μονότροπες οπτικές ίνες και καλύπτουν αποστάσεις από 220m μέχρι περίπου 70km (1000Base-SX έως 1000Base-ZX). Πολλές από αυτές δεν συμμορφώνονται με τυποποιήσεις του IEEE αλλά αποτελούν τεχνολογική καινοτομία που υιοθετείται από διάφορους κατασκευαστές.

Τα **καλώδια συνεστραμμένων ζευγών** κατασκευάζονται σε διάφορες παραλλαγές και κατηγορίες ώστε να ανταποκρίνονται σε διαφορετικές απαιτήσεις εφαρμογών και χρήσης. Τα πιο συνηθισμένα έχουν μονόκλωνους αγωγούς διατομής **22 AWG** (Φ 0,644mm) έως **24 AWG** (Φ 0,511mm) με θερμοπλαστική μόνωση, σε τέσσερα ανεξάρτητα συνεστραμμένα ζεύγη. Όλα μαζί περικλείονται από εξωτερικό πλαστικό περίβλημα.



Εικόνα 2.4.1.ζ: Αθωράκιστο καλώδιο συνεστραμμένων ζευγών.

Από πλευράς **θωράκισης** μπορεί να είναι ή όχι θωρακισμένο συνολικά το καλώδιο ή και κάθε ζεύγος χωριστά. Η θωράκιση είναι φύλλο αλουμινίου το οποίο περιβάλλει το ζεύγος ή το καλώδιο συνολικά και χάλκινο πλέγμα (μπλεντάζ) με αραιή έως εξαιρετικά πυκνή πλέξη το οποίο περιβάλλει συνολικά το καλώδιο. Στον πίνακα 2.4.1.β. φαίνονται διάφοροι τύποι καλωδίων συνεστραμμένων ζευγών και ο χαρακτηρισμός με τον οποίο είναι γνωστοί και είναι δηλωτικός του τρόπου κατασκευής ως προς την θωράκιση.

Ακρωνύμιο Βιομηχανίας	**Όνομα κατά το πρότυπο ISO/IEC11801**	**Θωράκιση καλωδίου**	**Θωράκιση ζεύγους**
UTP	**U/UTP**	**καμία**	**καμία**
STP, ScTP, PiMF	U/FTP	καμία	μεταλλικό φύλλο
FTP, STP, ScTP	**F/UTP**	**μεταλλικό φύλλο**	**καμία**
STP, ScTP	S/UTP	μεταλλικό πλέγμα	καμία
SFTP, S-FTP, STP	SF/UTP	μεταλλικό πλέγμα, μεταλλικό φύλλο	καμία
FFTP	F/FTP	μεταλλικό φύλλο	μεταλλικό φύλλο
SSTP, SFTP, STP PiMF	**S/FTP**	**μεταλλικό πλέγμα**	**μεταλλικό φύλλο**

Πίνακας 2.4.1.β: Καλώδια συνεστραμμένων ζευγών (ως προς τη θωράκιση).

Η θωράκιση επιτρέπει σε ένα σωστά εγκατεστημένο καλώδιο να έχει **καλύτερη συμπεριφορά ως προς τον ηλεκτρομαγνητικό θόρυβο και τις παρεμβολές**. Επηρεάζεται λιγότερο από εξωτερικούς θορύβους που μπορεί να παράγουνται από εξωτερικές συσκευές, ηλεκτροκινητήρες, διατάξεις φωτισμού κ.λπ. Επίσης τα σήματα που μεταφέρει επιδρούν ασθενέστερα σε συσκευές του άμεσου εξωτερικού περιβάλλοντος διέλευσης των

καλωδίων. Τέτοια θέματα καλύπτονται από τις οδηγίες περί ηλεκτρομαγνητικής συμβατότητας (ElectroMagnetic Compatibility - EMC).

Εικόνα 2.4.1.η: Θωρακισμένα καλώδια συνεστραμμένων ζευγών.

Μια σημαντική παράμετρος για τα καλώδια μεταφοράς δεδομένων είναι το **αναλογικό εύρος ζώνης** τους (bandwidth) το οποίο όταν είναι μεγάλο επιτρέπει σε ένα καλώδιο να επιτύχει αντίστοιχα υψηλό **ρυθμό μεταφοράς δεδομένων** (ταχύτητα). Το εύρος ζώνης μετράται σε **Hz** και τα πολλαπλάσιά του ενώ ο ρυθμός μεταφοράς δεδομένων σε **Bps** (bits per second) και τα πολλαπλάσιά του. Τα πρότυπα δεν προδιαγράφουν σαφώς το εύρος ζώνης αλλά τις επιδόσεις και τα χαρακτηριστικά του καλωδίου μέχρι κάποια συγκεκριμένη συχνότητα για κάθε τύπο. Ως προς τη συχνότητα μέχρι την οποία προδιαγράφονται τα χαρακτηριστικά τους, τα καλώδια συνεστραμμένων ζευγών κατατάσσονται σε κλάσεις ή κατηγορίες.

Κλάση (Class) EN 50173-1 ISO/IEC11801	**Κατηγορία (Category) EIA/TIA-568-C.2**	**Συχνότητα (όριο προδιαγραφών)**	**Ταχύτητα**	**Συνδετήρας**	**Παρατηρήσεις**
A		100 kHz			Μη χρήση για δεδομένα
B		1 MHz			-”-
C	Cat 3	16 MHz	**10Mbps**, 10BaseT	8p8c, RJ45	Το αναγνωρίζει το πρότυπο - C.2
	Cat 5	100 MHz			TIA/EIA-568-A αντικατάσταση από Cat 5e
D	**Cat 5e**	100 MHz	**100Mbps**, **1Gbps**, 100BaseTX, 1000BaseT	8p8c, RJ45	
E	**Cat 6**	250 MHz	**1Gbps**, 1000BaseT	8p8c, RJ45	
EA	**Cat 6A**	500 MHz	**10Gbps**, 10GBaseT	8p8c, RJ45	Μέχρι Cat 6A θωράκιση προαιρετική
F	Cat 7	600 MHz	-”-	GG45, TERA	S/FTP
FA	Cat 7A	1000 MHz	**40GBps?**	GG45, TERA	S/FTP

Πίνακας 2.4.1.γ: Κατηγορίες καλωδίων συνεστραμμένων ζευγών.

Τα καλώδια συνεστραμμένων ζευγών έχουν μια τυπική τιμή χαρακτηριστικής εμπέδησης **100Ω** ανά ζεύγος. Η τιμή αυτή μπορεί να φτάνει τα 150Ω σε ορισμένους τύπους καλωδίων και είναι αποδεκτή μόνο από τα πρότυπα της σειράς EIA/TIA.

Τα πρότυπα μπορεί να είναι διεθνή (όπως ISO), ευρωπαϊκά (σειρές EN) ή και κρατικής εμβέλειας (π.χ. ANSI, DIN) τα οποία μπορεί να προτείνονται από επαγγελματικές (π.χ. EIA/TIA) ή επιστημονικές ενώσεις (όπως το IEEE).

Τα σημαντικότερα χαρακτηριστικά μεγέθη για ένα καλώδιο είναι η **εξασθένηση** (attenuation ή insertion loss) που εισάγει στη διαδρομή του σήματος, η **παραδιαφωνία** (cross talk) στο άκρο που γίνεται η εκπομπή (**NEXT** - Near End X-talk), η παραδιαφωνία στο απομακρυσμένο άκρο (**FEXT** - Far End X-talk) και ο **λόγος εξασθένησης προς παραδιαφωνία** (**ACR** - Attenuation to Cross-talk Ratio). Η εξασθένηση αναφέρεται ανά μονάδα μήκους του καλωδίου και συνήθως ανά 100m. Η παραδιαφωνία είναι το ποσοστό του εκπεμπόμενου σήματος από ένα ζεύγος το οποίο παρεμβάλλεται στο γειτονικό του ζεύγος ως ανεπιθύμητο σήμα. Υπάρχουν και άλλα χαρακτηριστικά μεγέθη τα οποία προδιαγράφονται αναλυτικά στα πρότυπα και αποτελούν αντικείμενο μέτρησης για την **πιστοποίηση** των καλωδιώσεων ως προς το αντίστοιχο πρότυπο. **Πιστοποίηση** σημαίνει ότι τα μεγέθη μετρήθηκαν με τον συνιστώμενο τρόπο και οι τιμές βρέθηκαν μέσα στα όρια που προσδιορίζει το πρότυπο.

	ΕΞΑΣΘΕΝΗΣΗ			**ΠΑΡΑΔΙΑΦΩΝΙΑ (NEXT)**		
Συχνότητα (MHz)	**Cat 5e** (dB)	**Cat 6** (dB)	**Cat 6A** (dB)	**Cat 5e** (dB)	**Cat 6** (dB)	**Cat 6A** (dB)
1,00	2,1	1,9	1,9	60,0	65,0	65,0
4,00	3,9	3,5	3,5	54,8	64,1	64,1
8,00	5,5	5,0	5,0	50,0	59,4	59,4
10,00	6,2	5,5	5,5	48,5	57,8	57,8
16,00	7,9	7,0	7,0	45,2	54,6	54,6
20,00	8,9	7,9	7,8	43,7	53,1	53,1
25,00	10,0	8,9	8,8	42,1	51,5	51,5
31,25	11,2	10,0	9,8	40,5	50,0	50,0
62,50	16,2	14,4	14,1	35,7	45,1	45,1
100,00	21,0	18,6	18,0	32,3	41,8	41,8
200,00	-	27,4	26,1	-	36,9	36,9
250,00	-	31,1	29,5	-	35,3	35,3
300,00	-	-	32,7	-	-	34,0
400,00	-	-	38,5	-	-	29,9
500,00	-	-	43,8	-	-	26,7

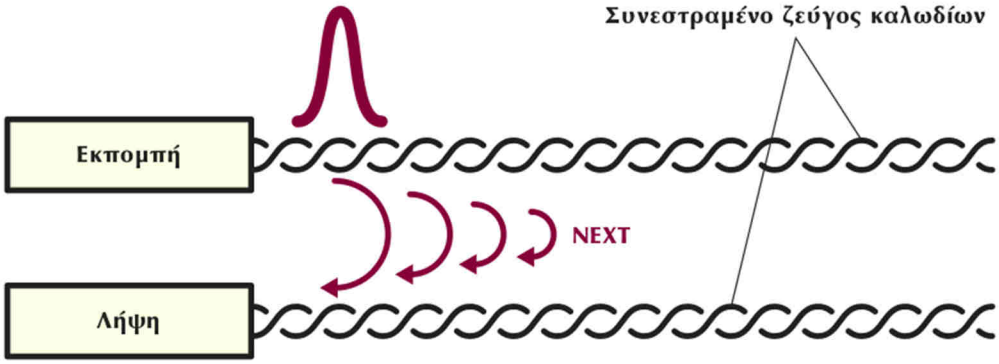
Πίνακας 2.4.1.δ: Επιδόσεις καλωδίων (TP) σύμφωνα με το ANSI/TIA-568-C.2

Στην Εικόνα 2.4.1.θ φαίνεται παραστατικά η έννοια της εξασθένησης. Το σήμα ξεκινά από το άκρο εκπομπής με δεδομένο πλάτος και φτάνει στο άλλο άκρο, λήψης, εξασθενημένο, με μικρότερο πλάτος. Εάν το σήμα είναι συχνότητας 25 Mhz και διέρχεται από καλώδιο UTP Cat 5e, θα φτάσει στο άλλο άκρο 10dB ασθενέστερο (το 1/10 ή 10% του αρχικού σήματος).

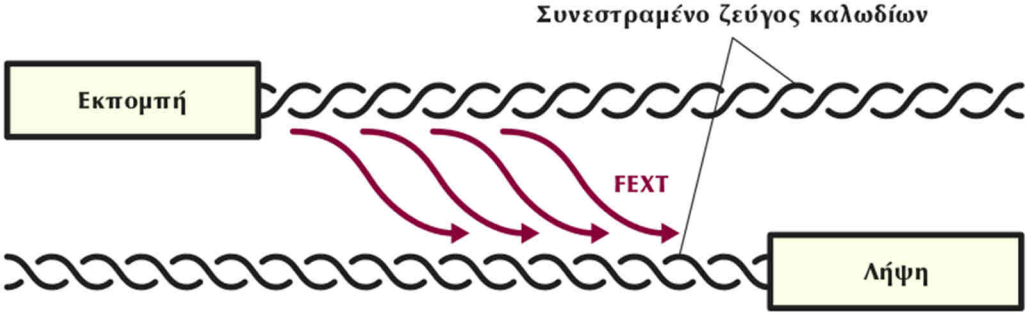
Εάν διέρχεται από καλώδιο UTP Cat 6, θα φτάσει στο άλλο άκρο 8,9dB ασθενέστερο (περίπου το 1/8 ή 12,5% του αρχικού σήματος).

Εικόνα 2.4.1.θ: Εξασθένηση (Attenuation, Insertion Loss).

Στις παρακάτω εικόνες, Εικόνα 2.4.1.ι και Εικόνα 2.4.1.κ, φαίνεται η έννοια της παραδιαφωνίας στο κοντινό και στο απομακρυσμένο άκρο.



Εικόνα 2.4.1.ι: Παραδιαφωνία NEXT (Near End CrossTalk)



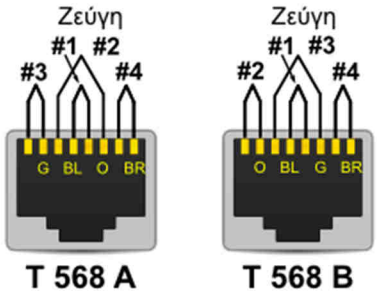
Εικόνα 2.4.1.κ: Παραδιαφωνία FEXT (Far End CrossTalk).

Τα καλώδια συνεστραμμένων ζευγών έχουν συγκεκριμένα χρώματα ανά ζεύγος και τερματίζονται σε συνδετήρες τύπου “RJ-45” (modular jack/plug 8p8c) οκτώ θέσεων και οκτώ επαφών. Τα χρώματα των ζευγών είναι **Μπλέ (ζεύγος 1)**, **Πορτοκαλί (ζεύγος 2)**, **Πράσινο (ζεύγος 3)**, και **Καφέ (ζεύγος 4)**. Για κάθε χρώμα, το ζευγάρι του είναι άσπρο με λωρίδα ή δακτυλίους ίδιου χρώματος. Στους ζυγούς αριθμούς ακροδεκτών τοποθετούνται τα καλώδια με χρώματα και στους μονούς τα άσπρα. Ο Πίνακας 2.4.1.δ δίνει την αντιστοιχία ακροδεκτών, σημάτων και χρωμάτων ζευγών καλωδίων ώστε να μπορέσει κάποιος, με τη χρήση κατάλληλων εργαλείων και υλικών, να κατασκευάσει ένα καλώδιο δικτύου Ethernet.

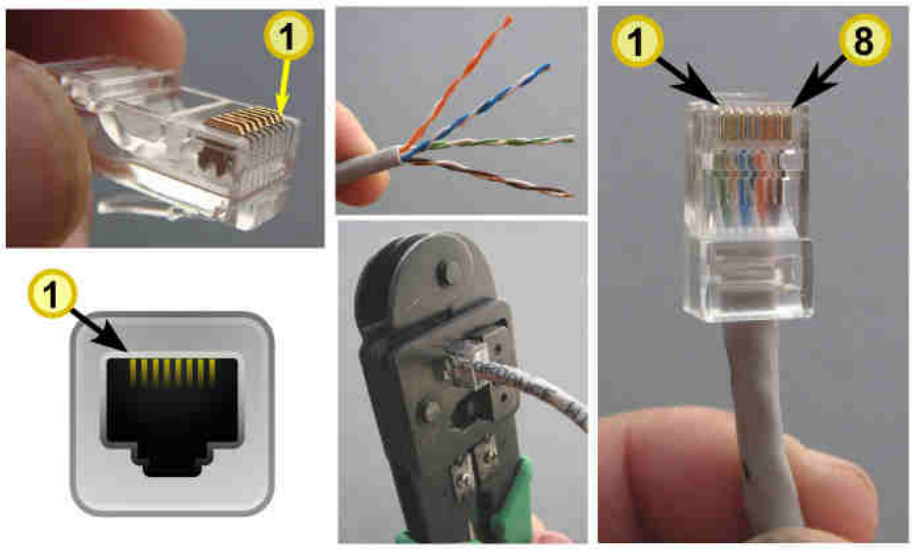
Υπάρχουν δυο είδη καλωδίων Ethernet ανάλογα με τη χρήση,

- για σύνδεση διαφορετικών συσκευών μεταξύ τους όπως κάρτας δικτύου Η/Υ σε HUB/Switch. Η αντιστοιχία ακροδεκτών είναι “ένα προς ένα” μεταξύ των δυο άκρων (straight through cable), και
- για σύνδεση ομοειδών συσκευών μεταξύ τους, όπως Η/Υ με Η/Υ ή HUB/Switch με άλλο HUB/Switch. Οι ακροδέκτες εκπομπής της μιας μεριάς οδηγούνται στους ακροδέκτες λήψης της άλλης (crossover cable) και το αντίστροφο.

Οι συνδετήρες (connectors) πάνω στις κάρτες δικτύου χαρακτηρίζονται **MDI** (Medium Dependent Interface) και έχουν σε συγκεκριμένους ακροδέκτες την έξοδο εκπομπής (1,2 στο 10/100Mbps Ethernet) και σε άλλους την είσοδο για λήψη (3,6). Οι συσκευές διασύνδεσης (HUB/Switches) έχουν στις ίδιες θέσεις την αντίθετη λειτουργία δηλαδή στο (1, 2) είσοδο λήψης και στο (3, 6) έξοδο εκπομπής. Τότε χαρακτηρίζονται ως **MDI-X** (MDI crossed). Αυτό επιτρέπει στους υπολογιστές να συνδέονται σε HUB/Switches με καλώδιο με “ένα προς ένα” αντιστοιχία (straight through cable).



Εικόνα 2.4.1.κα: Συρμάτωση



Εικόνα 2.4.1.κβ: Καλώδιο UTP, ζεύγη, συνδετήρες και αρίθμηση ακροδεκτών

	Ethernet		Τρόπος συρμάτωσης		
	10BaseT, 100Base-TX	**1000BaseT, 10GBaseT**	**T 568 A**	**T 568 B** *(AT&T 258 A)*	
Αριθμός ακροδέκτη	***Σήμα / λειτουργία***	***Σήμα / λειτουργία***	***Χρώμα καλωδίου***	***Χρώμα καλωδίου***	***Παρατηρήσεις***
1	**TX +**	**BI_DA +**	άσπρο/πράσινο	άσπρο/πορτοκαλί	για 10/100 /1000 MBps χρήση εξαρτημάτων Cat 5e και καλύτερα. Για 10GBps χρήση Cat6A και καλύτερα
2	**TX -**	**BI_DA -**	πράσινο	πορτοκαλί	
3	**RX +**	**BI_DB +**	άσπρο/πορτοκαλί	άσπρο/πράσινο	
4	-	**BI_DC +**	μπλε	μπλε	
5	-	**BI_DC -**	άσπρο/μπλε	άσπρο/μπλε	
6	**RX -**	**BI_DB -**	πορτοκαλί	πράσινο	
7	-	**BI_DD +**	άσπρο/καφέ	άσπρο/καφέ	
8	-	**BI_DD -**	καφέ	καφέ	

Πίνακας 2.4.1.ε: Αντιστοιχία ακροδεκτών, σημάτων και χρωμάτων ζευγών καλωδίων

Εκτός από τα χάλκινα καλώδια συνεστραμμένων ζευγών, τα διάφορα πρότυπα του Ethernet ήδη από την εισαγωγή του 10BaseFL προδιαγράφουν και τη χρήση οπτικών ινών. **Οπτικές ίνες** υπάρχουν **πολύτροπες** με πυρήνα μεγαλύτερης διατομής, πιο εύκαμπτες για καθημερινή χρήση ως καλώδια σύνδεσης εξοπλισμού (συνήθως με εξωτερικό περίβλημα πορτοκαλί χρώματος) ή **μονότροπες** με πιο λεπτό πυρήνα μικρότερη εξασθένηση για χρήση σε μακρινές αποστάσεις (συνήθως με εξωτερικό περίβλημα κίτρινου χρώματος).

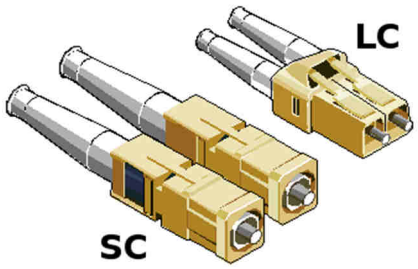
Τύποι οπτικών ινών που χρησιμοποιούνται στο Ethernet			
Τύπος	**Εφαρμογή**	**Γινόμενο εύρους ζώνης επί την απόσταση (GHz*m)**	**Διάμετρος πυρήνα / επίστρωσης (μm)**
OM1	Απαρχαιωμένος. Χρήση σε FDDI	160 - 200	62,5/125
OM2	100Base-FX έως 1000Base-SX	500	50/125
OM3	10GBase-SR και υψηλότερες ταχύτητες	2000	50/125
OM4	10GBase-SR και υψηλότερες ταχύτητες	4700	50/125
OS1	Τυποποιημένη μονότροπη οπτική ίνα	Πρακτικά άπειρο	9/125
OS2	Οπτική ίνα μειωμένης εξασθένησης. Συνήθως δεν χρησιμοποιείται για Ethernet	Πρακτικά άπειρο	9/125

Πίνακας 2.4.1.στ: "Κατηγορίες καλωδίων οπτικών ινών"

Για τις οπτικές ίνες υπάρχουν αντίστοιχα διάφορα είδη συνδετήρων και εξαρτημάτων αλλά ο τερματισμός των οπτικών ινών απαιτεί ιδιαίτερη δεξιοτεχνία και εξοπλισμό.

Εικόνα 2.4.1.κδ: Μονότροπη οπτική ίνα

Εικόνα 2.4.1.κε: Συνδετήρες οπτικών ινών (SC, ST)



Εικόνα 2.4.1.κστ: Διπλοί συνδετήρες SC, LC

Επισημαίνεται ότι με την υποστήριξη **πλήρως αμφίδρομης επικοινωνίας** saa(**Full Duplex**) πάνω από ζεύξεις **σημείο προς σημείο** όπως είναι η σύνδεση της κάρτας δικτύου ενός υπολογιστή στη θύρα ενός μεταγωγέα/διανομέα (switching hub), **παύει να ισχύει το CSMA/CD** και οι χρονικοί περιορισμοί των χρόνων πλήρους περιφοράς (Round Trip Time). Έτσι, στις συνδέσεις αυτές, οι επιτυγχανόμενες αποστάσεις επικοινωνίας περιορίζονται μόνο από τις επιδόσεις των φυσικών μέσων. Στην περίπτωση χρήσης χάλκινων καλωδίων, η εξασθένηση που εισάγει το καλώδιο αποτελεί σημαντικό περιοριστικό παράγοντα. Οι οπτικές ίνες όμως, ειδικά οι μονότροπες, με την εξαιρετικά χαμηλή εξασθένησή τους, επιτρέπουν την επίτευξη αποστάσεων επικοινωνίας της τάξης των δεκάδων χιλιομέτρων.

Στις εκδόσεις του Ethernet που χρησιμοποιούνται **ομοαξονικά καλώδια** ή **καλώδια συνεστραμμένων ζευγών με επαναλήπτες (Repeaters)** όλο το δίκτυο αποτελεί ένα **ενιαίο πεδίο συγκρούσεων** (collision domain) στο οποίο μόνο ένας κόμβος μπορεί να εκπέμπει κάθε στιγμή. Όταν χρησιμοποιείται γέφυρα ή μεταγωγέας τότε **κάθε τμήμα** (segment) αποτελεί **ανεξάρτητο πεδίο συγκρούσεων** ενώ όταν χρησιμοποιείται αποκλειστικά μεταγωγέας/διανομέας (switching hub) δεν υπάρχουν συγκρούσεις, αυξάνοντας τον ρυθμό διακίνησης (throughput) σε ένα προσεκτικά σχεδιασμένο δίκτυο. Ωστόσο, **ένα τοπικό δίκτυο** αποτελεί **ένα ενιαίο πεδίο εκπομπής** ή πολυδιανομής (broadcast/multicast domain) και το χαρακτηριστικό αυτό ίσως αποτελεί και το κριτήριο ορισμού ενός δικτύου ως τοπικού (LAN). Η έννοια του τμήματος (segment) δικτύου είναι διαφορετική ανάλογα με το επίπεδο στο οποίο γίνεται αναφορά. Στο φυσικό επίπεδο αφορά στο ενιαίο φυσικό μέσο (π.χ. καλώδιο ή επέκταση αυτού με επαναλήπτες) και ισοδυναμεί με το **πεδίο συγκρούσεων** ενώ στο επίπεδο ζεύξης δεδομένων ισοδυναμεί με το **πεδίο εκπομπής** ή πολυδιανομής.

Η τεχνολογία τοπικών δικτύων Ethernet δεν έχει παραμείνει στατική ούτε έχει εγκαταλειφθεί. Η προς τα πίσω συμβατότητα με τα παλαιότερα πρότυπα, της δίνει τη

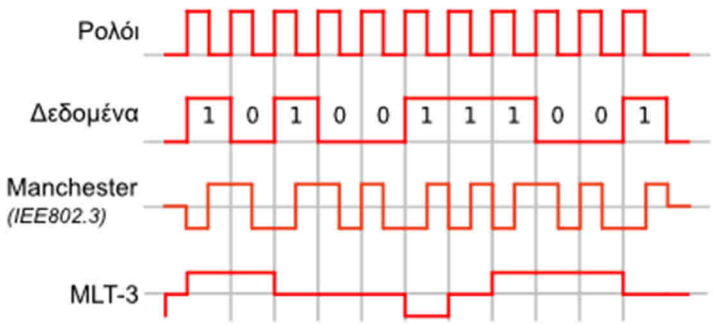
δυνατότητα να εξελίσσεται και να εισέρχεται σιγά - σιγά σε χρήση παράλληλα με τον ήδη εγκατεστημένο εξοπλισμό και σταδιακά να τον αντικαθιστά. Έτσι εγκαταστάσεις τεχνολογίας 10BaseT (10MBps) σταδιακά πέρασαν στα 100MBps και στη συνέχεια στα 1000MBps. Ήδη κυκλοφορεί εξοπλισμός για 10GBps και υπάρχουν πρότυπα για τα 40 και 100GBps. Στον ειδικό τύπο γίνεται συζήτηση για τα 400GBps.

Κωδικοποίηση και ηλεκτρική σηματοδοσία

Κατά τη διεξαγωγή οποιασδήποτε επικοινωνίας μέσω ενός φυσικού μέσου το οποίο έχει περιορισμένο εύρος ζώνης υπάρχουν δυο βασικά ζητούμενα, αντικειμενικοί στόχοι από τους ανταποκριτές:

- Να μπορεί **ο δέκτης να συγχρονίζεται με τον πομπό** ώστε να "διαβάζει" σωστά το ψηφίο που του στέλνει ο πομπός. Σωστά ως προς την τιμή (1 ή 0;) και σωστά ως προς τη θέση (το 5ο, 6ο ή 7ο;)
- Το **εύρος ζώνης του σήματος να είναι μικρότερο από του φυσικού μέσου** για την επιθυμητή ταχύτητα ώστε να "χωράει" να περάσει από το φυσικό μέσο, χωρίς σφάλματα ή με τα δυνατόν λιγότερα.

Στο 10MBps Ethernet, αυτό επιτυγχάνεται με την **κωδικοποίηση φάσης Manchester** (Manchester Phase Encoding), κατά την οποία υπάρχει μια εναλλαγή κατάστασης για κάθε bit ώστε να υπάρχει τρόπος συγχρονισμού του δέκτη. Στο 100MBps Ethernet έπρεπε να μειωθεί και το εύρος ζώνης του σήματος ώστε να επιτευχθεί δεκαπλάσια ταχύτητα από μόλις λίγο καλύτερα καλώδια με ελαφρώς μεγαλύτερο εύρος ζώνης. Το εύρος ζώνης που θα απαιτούνταν για τα 100Mbps με κωδικοποίηση Manchester έφτανε τα 200MHz ενώ τα συνεστραμμένα ζεύγη διέθεταν εύρος ζώνης της τάξης των 30MHz. Έτσι τα ψηφία πριν την αποστολή ομαδοποιήθηκαν σε τετράδες, κωδικοποιήθηκαν σε πεντάδες (**4B/5B**) και ακολούθως κωδικοποιήθηκαν σε σήμα πλάτους τριών επιπέδων (PAM3) με τη χαρακτηριστική ονομασία **MLT-3** (Multi Level Transmit). Στο Gigabit Ethernet, εφαρμόστηκαν αντίστοιχες τεχνικές. Κωδικοποίηση **8B/10B** για χρήση σε οπτικές ίνες και **4D-PAM5** για χρήση σε καλώδια συνεστραμμένων ζευγών. Με όλες τις νεότερες και ταχύτερες εκδόσεις του Ethernet οι μηχανικοί βρίσκονται πάντα αντιμέτωποι με τα δυο βασικά ζητούμενα που προαναφέρθηκαν. Και πάντα αναζητούν τις κατάλληλες τεχνικές λύσεις που παρέχονται με τις διάφορες κωδικοποιήσεις πρώτα των αριθμητικών ψηφίων και στη συνέχεια του ηλεκτρικού σήματος στο καλώδιο.



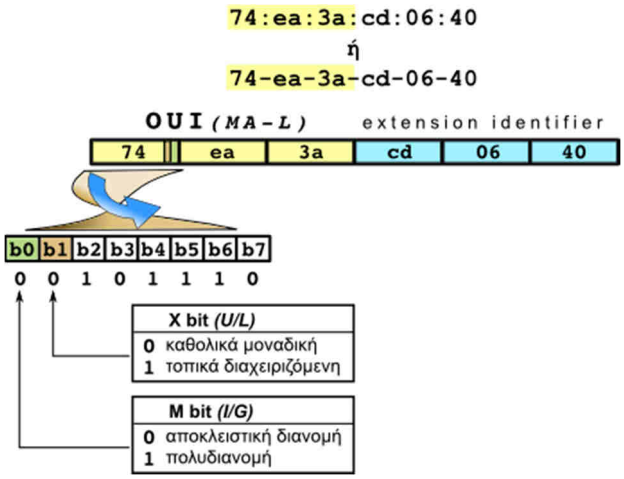
Εικόνα 2.4.1.κζ: Κωδικοποίηση Manchester, MLT-3

2.4.2 Διευθύνσεις Ελέγχου πρόσβασης στο Μέσο (MAC) - Δομή πλαισίου Ethernet - Πλαίσια Ethernet μεγάλου μεγέθους (Jumbo frames)

Κάθε κόμβος σε ένα δίκτυο Ethernet έχει μια **φυσική διεύθυνση** ή **διεύθυνση υλικού**, όπως αλλιώς χαρακτηρίζεται (Hardware Address) ώστε να αναγνωρίζεται μοναδικά σε όλο το δίκτυο. Αναφέρεται και ως διεύθυνση ελέγχου προσπέλασης στο μέσο (**MAC Address**, Media Access Control). Είναι ένας δυαδικός αριθμός των **48 bit** (MAC-48, EUI-48) ή έξι

οκτάδων και γράφεται στο δεκαεξαδικό αριθμητικό σύστημα ως **έξι διψήφιοι δεκαεξαδικοί αριθμοί** χωρισμένοι με παύλες (στα windows) ή με άνω-κάτω τελείες (στο unix/linux). Μια τέτοια διεύθυνση είναι η **74:ea:3a:cd:06:40**. Σε υπολογιστή εξοπλισμένο με προσαρμογέα/κάρτα δικτύου, η διεύθυνση MAC είναι χαρακτηριστικό της κάρτας δικτύου και πολλές φορές αναγράφεται πάνω σε αυτήν από τον κατασκευαστή της. Μπορεί να αναγνωσθεί ηλεκτρονικά με την κατάλληλη εντολή του λειτουργικού συστήματος (ipconfig/all, ifconfig κλπ).

Οι κόμβοι ενός δικτύου Ethernet ανταλλάσσουν δεδομένα-πληροφορίες τις οποίες ενθυλακώνουν σε πακέτα τα οποία ονομάζονται **πλαίσια**. Στην επικεφαλίδα του πλαισίου τοποθετούνται διαχειριστικές πληροφορίες από τις οποίες οι σημαντικότερες είναι οι διευθύνσεις αποστολέα (προέλευσης) και παραλήπτη (προορισμού).

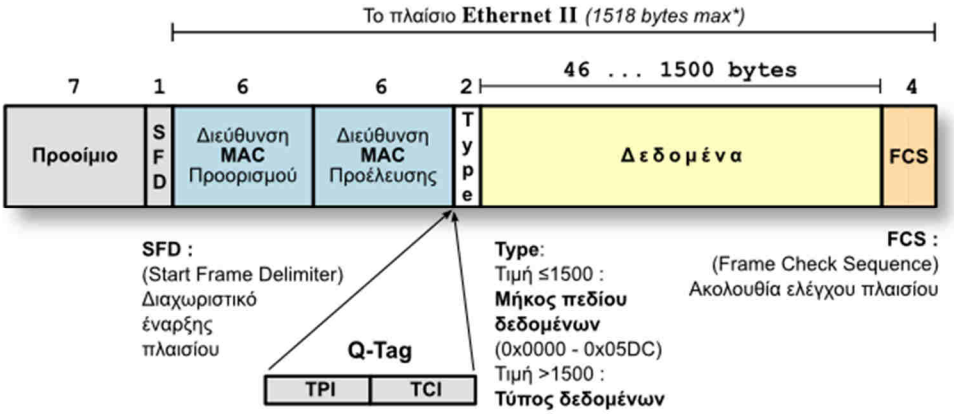


Εικόνα 2.4.2.α: Δομή διεύθυνσης MAC στο Ethernet

Οι διευθύνσεις MAC απαρτίζονται από δυο μέρη των 24ων δυαδικών ψηφίων. Το πρώτο μέρος το οποίο ονομάζεται (μοναδική) **Ταυτότητα του Οργανισμού** (**OUI** - Organizational Unique Identifier), χορηγείται από Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών και διατίθεται αποκλειστικά στον κατασκευαστή υλικού. Το δεύτερο μέρος το προσδιορίζει ο κατασκευαστής υλικού με δική του ευθύνη. Από το πρώτο μέρος τα δυο ψηφία έχουν ειδική σημασία.

Στην Εικόνα 2.4.2.α φαίνεται η δομή μιας διεύθυνσης MAC στο Ethernet. Ας σημειωθεί ότι στο Ethernet αποστέλλεται το πιο σημαντικό byte (MSB) πρώτα αλλά για κάθε byte, πρώτα το λιγότερο σημαντικό bit (LSB). Ο τρόπος αποστολής, αυτός, χαρακτηρίζεται Little Endian σε επίπεδο byte. Έτσι κατά την εκπομπή των ψηφίων μιας διεύθυνσης Ethernet θα αποσταλούν, σε επίπεδο byte, πρώτα το MSB, για το παράδειγμά μας το 74 (0111 0100) αλλά με την αντίστροφη σειρά (0010 1110), πρώτα το b0, μετά το b1 κ.ο.κ.

Αυτά τα δύο πρώτα bit, τα οποία είναι ουσιαστικά το b0 και b1 του MSB της διεύθυνσης έχουν ειδική σημασία. Το πρώτο (b0) είναι το **M bit** ή **I/G** (Individual/Group). Όταν είναι 1 σημαίνει ότι η διεύθυνση αφορά πολλούς αποδέκτες, είναι πολυδιανομής (Multicast), αλλιώς αφορά συγκεκριμένο αποδέκτη. Το δεύτερο (b1) είναι το X **bit** ή **U/L** (Universal/Local). Όταν είναι 1 σημαίνει ότι η διεύθυνση είναι τοπικά διαχειριζόμενη αλλιώς είναι καθολικά μοναδική. Ειδική περίπτωση είναι η διεύθυνση με όλα τα ψηφία 1, η **ff-ff-ff-ff-ff-ff** η οποία είναι **διεύθυνση εκπομπής**. Πλαίσιο με διεύθυνση προορισμού την ff-ff-ff-ff-ff-ff αφορά όλους τους κόμβους και παραλαμβάνεται από όλους όσους μοιράζονται το κοινά διαμοιραζόμενο μέσο, ανήκουν δηλαδή στο ίδιο τοπικό δίκτυο. Στην περίπτωση μεταγωγέα με συνδέσεις σημείο προς σημείο, αυτός προωθεί το πλαίσιο σε όλες τις θύρες του.



Εικόνα 2.4.2.β: Δομή πλαισίου Ethernet

Το πλαίσιο στο Ethernet έχει συγκεκριμένη δομή όπως φαίνεται στην Εικόνα 2.4.2.β. Για να διευκολυνθεί ο δέκτης ώστε να συγχρονιστεί με τον πομπό, ξεκινά με ένα **προοίμιο** (preamble) επτά οκτάδων (byte) εναλλασσόμενων άσων και μηδενικών (0x55) και μια οκτάδα 0xD5 η οποία σηματοδοτεί την **έναρξη του πλαισίου** (**SFD** - Start Frame Delimiter). Ακολουθούν οι **διευθύνσεις** των έξι οκτάδων η καθεμιά, πρώτα **προορισμού** ώστε να ενεργοποιηθεί έγκαιρα ο παραλήπτης και κατόπιν του αποστολέα (**προέλευσης**). Στη συνέχεια το πεδίο δυο οκτάδων "Τύπος**/Μήκος δεδομένων**" προσδιορίζει το είδος των δεδομένων που μεταφέρει το πλαίσιο ή πιο πρωτόκολλο ανωτέρου επιπέδου αφορούν. Άν έχει τιμή μικρότερη του 1500 (0x5DC) τότε δηλώνει το μήκος των δεδομένων που μεταφέρει. Στο τέλος περιλαμβάνει σε τέσσερις οκτάδες την **ακολουθία ελέγχου πλαισίου** (**FCS** - Frame Check Sequence) σύμφωνα με τον αλγόριθμο CRC-32 ώστε να είναι εφικτό να αναγνωριστεί από τον παραλήπτη οποιοδήποτε σφάλμα συμβεί κατά τη μετάδοση. Μετά το τέλος του πλαισίου ακολουθεί μια παύση διάρκειας 96bit ώστε να επιτραπεί στα κυκλώματα του δέκτη να επεξεργαστούν το ληφθέν πλαίσιο και να είναι αυτός έτοιμος για τη λήψη επόμενου πλαισίου. Αυτό λέγεται **InterPacketGap** (**IPG**).

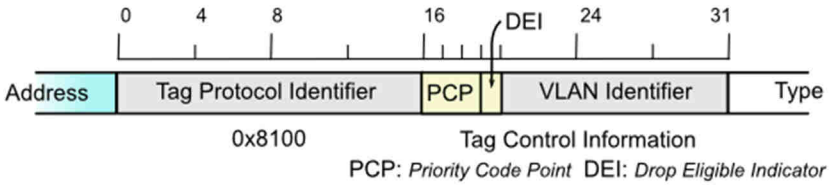
Το μήκος των δεδομένων του ωφέλιμου φορτίου του πλαισίου μπορεί να φτάσει από 46 μέχρι 1500 οκτάδες και ονομάζεται Μέγιστη μονάδα εκπομπής **MTU** (Maximum Transmission Unit). Είναι απαίτηση του προτύπου το συνολικό μέγεθος του πλαισίου να μην είναι μικρότερο των 64 οκτάδων (18 επικεφαλίδα και 46 φορτίο). Αν συμβαίνει να είναι μικρότερο τότε συμπληρώνεται συνήθως με μηδενικά (padding) για να φτάσει στο ελάχιστο μήκος.

Νοητά τοπικά δίκτυα (Virtual LAN - VLAN)

Όταν στο πεδίο "Τύπος δεδομένων" υπάρχει η τιμή **0x8100** τότε το δίκτυο υποστηρίζει **νοητά τοπικά δίκτυα** (**VLAN** - Virtual LAN). Από πλευράς πλαισίου αυτό σημαίνει ότι ακολουθούν επιπλέον δυο οκτάδες με σχετικές πληροφορίες (PCP, DEI, VLAN ID) και στη συνέχεια ένα πεδίο δυο οκτάδων που αφορούν τον τύπο των δεδομένων. Τα τέσσερα συνολικά byte μετά την διεύθυνση προέλευσης ονομάζονται Q-Tag, Q επειδή περιγράφονται στο πρότυπο IEEE802.1Q. Η επικεφαλίδα του πλαισίου από 14 byte φτάνει στα 18, το ωφέλιμο φορτίο από 42 έως 1500 και το συνολικό μήκος του πλαισίου από 64 έως 1522 byte.

Η υποστήριξη, από πλευράς εξοπλισμού (κάρτες δικτύου και μεταγωγείς), νοητών LAN, επιτρέπει σε ομάδες υπολογιστών οι οποίοι συνδέονται στον ίδιο μεταγωγέα/διανομέα (switching hub) να λειτουργούν ως ανεξάρτητα τοπικά δίκτυα χωρίς καμιά δυνατότητα επικοινωνίας (στο 2ο επίπεδο OSI) μεταξύ υπολογιστών οι οποίοι έχουν διαφορετικό

αναγνωριστικό VLAN. Δηλασή, σαν να συνδέονται σε διαφορετικούς μεταγωγείς, χωρίς καμιά σύνδεση μεταξύ των μεταγωγέων. Κόμβοι με ίδιο VLAN ID ανήκουν στο ίδιο VLAN.



Εικόνα 2.4.2.γ: VLAN Q-Tag

Με 12bit μήκος πεδίου VLAN ID, υποστηρίζονται θεωρητικά 2^{12} νοητά δίκτυα και πρακτικά 4094 καθώς εξαιρούνται οι τιμές 0x000 και 0xFFF. Η τεχνική VLAN επιτρέπει τον χωρισμό ενός δικτύου σε ανεξάρτητα υποδίκτυα στο 2ο επίπεδο του OSI. Κάθε VLAN αποτελεί ανεξάρτητο πεδίο εκπομπής ή πολυδιανομής (broadcast ή multicast domain).

Ένα **νοητό τοπικό δίκτυο VLAN** (Virtual LAN) είναι η λογική ομαδοποίηση δυο ή περισσότερων συσκευών ενός τοπικού δικτύου και μπορεί να εκτείνεται σε περισσότερους από έναν μεταγωγείς (switches). Μια ή περισσότερες θύρες ενός μεταγωγέα/διανομέα (switching hub) λειτουργούν ξεχωριστά και ανεξάρτητα ως ένα διαφορετικό σύστημα Ethernet. Δικτυακή κίνηση σε ένα συγκεκριμένο VLAN εκπέμπεται και λαμβάνεται μόνο στις θύρες του μεταγωγέα που έχουν οριστεί ως μέλη του συγκεκριμένου VLAN.

Σε έναν μεταγωγέα/διανομέα (switching hub) ο οποίος υποστηρίζει VLAN οι θύρες μπορούν να ρυθμιστούν σε δυο κατηγορίες. Θύρες για σύνδεση υπολογιστών οι οποίες χαρακτηρίζονται **access ports** ή **untagged** και θύρες οι οποίες χαρακτηρίζονται **trunk ports** ή **tagged**, επιτρέπουν την κίνηση πλαισίων με VLAN-tags που αφορούν διάφορα VLAN και χρησιμοποιούνται για την διασύνδεση μεταγωγέων μεταξύ τους.

Πλεονεκτήματα από τη χρήση νοητών τοπικών δικτύων VLANs

- Έλεγχος δικτυακής κίνησης Εκπομπής (Broadcasts)

  Όσο μεγαλώνει ο αριθμός συσκευών σε ένα δίκτυο τόσο αυξάνεται και η δικτυακή κίνηση εκπομπής με αρνητικά αποτελέσματα στην απόδοση του δικτύου. Με τη χρήση της τεχνικής χωρισμού ενός δικτύου σε περισσότερα VLAN, η κίνηση αυτή περιορίζεται μόνο μέσα στα όρια του συγκεκριμένου VLAN, καθώς αυτό αποτελεί αυτόνομο πεδίο εκπομπής.

- Ασφάλεια

  Με το διαχωρισμό ενός τοπικού δικτύου σε περισσότερα VLAN μπορεί κόμβοι οι οποίοι ανήκουν σε τμήμα με αυξημένες ανάγκες ασφάλειας να αποτελέσουν ξεχωριστό VLAN και να αποτραπεί η εύκολη πρόσβαση από τους κόμβους όλων των άλλων χρηστών.

- Ενοποίηση πόρων

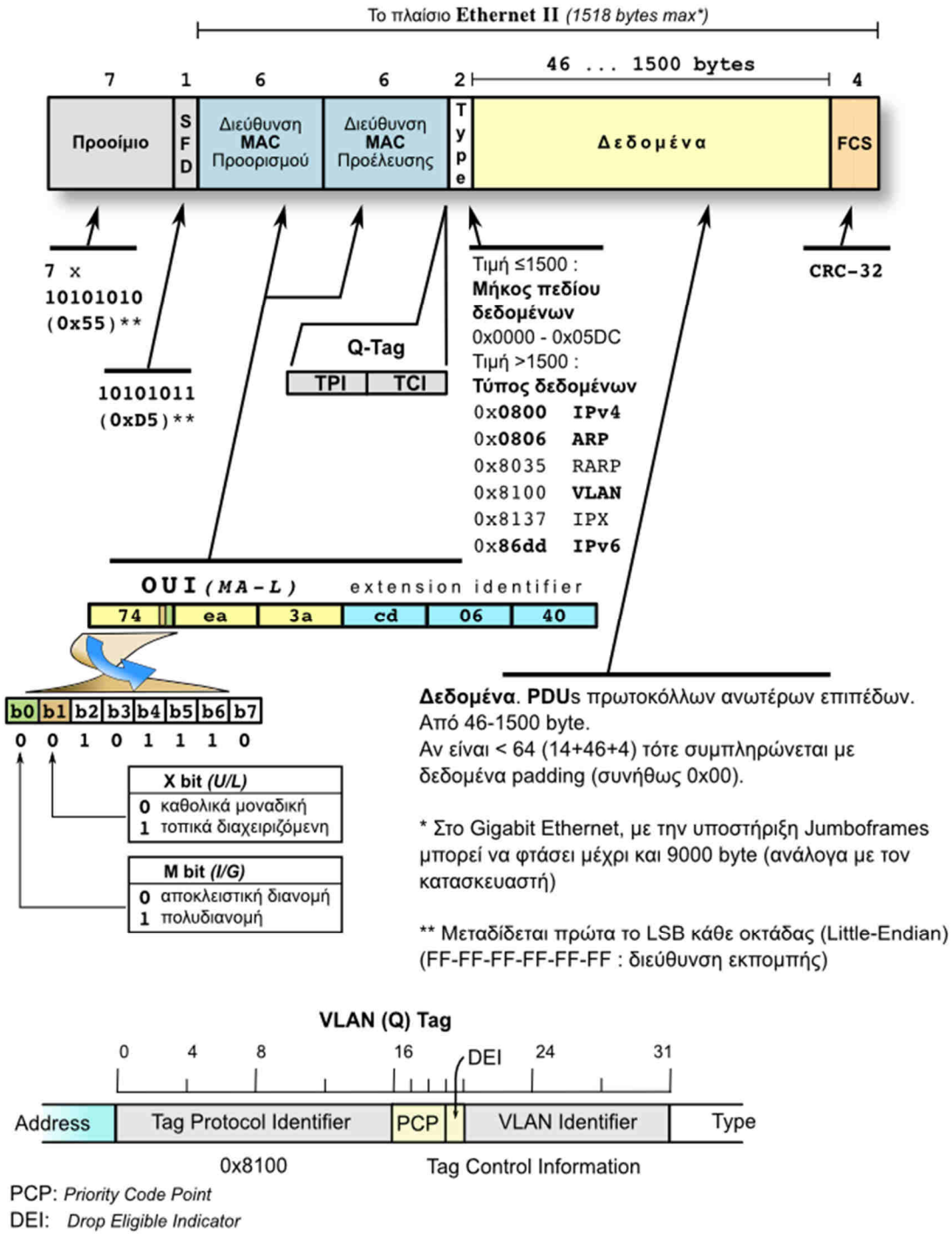
  Πόροι και συσκευές που έχουν παρόμοιες ανάγκες εξυπηρέτησης από το δίκτυο μπορούν να ομαδοποιηθούν σε ξεχωριστό VLAN για την αποδοτικότερη εξυπηρέτησή τους. Παράδειγμα η ενοποίηση όλων των κόμβων τηλεφωνίας VoIP (Voice over Internet Protocol) σε ένα VLAN ώστε να απολαμβάνουν μικρότερες καθυστερήσεις στη διεκπεραίωση των πλαισίων/πακέτων τους.

- Ευκολία διαχείρισης δικτύου

  Η ομαδοποίηση στο 2ο επίπεδο, κεντρικά, είναι πιο εύκολη και αποτελεσματική από την υποδικτύωση στο 3ο επίπεδο και την εξυπηρέτηση από δρομολογητές.

Το μόνο **μειονέκτημα**, σε μια καλοσχεδιασμένη υλοποίηση με VLAN στην οποία αποφεύγεται η επέκταση του ίδιου VLAN πέραν του ενός κτιρίου, είναι η τεκμηρίωση που απαιτείται ώστε ο διαχειριστής να έχει σαφή εικόνα του δικτύου και να γνωρίζει τι ρυθμίσεις έγιναν και σε ποιες συσκευές.

Στην Εικόνα 2.4.2 δ φαίνεται εποπτικά η δομή του πλαισίου και των διευθύνσεων Ethernet ενώ ο Πίνακας 2.4.2.α δίνει συγκεντρωτικά επεξηγήσεις για τα διάφορα πεδία.



Εικόνα 2.4.2.δ: Δομή πλαισίου και διεύθυνσης MAC στο Ethernet

Το πλαίσιο (frame) Ethernet II	
Προοίμιο (Preamble) 7 byte	56 bits εναλλασσόμενοι άσοι-μηδενικά (**10101010, 0x55**)** για να συγχρονιστεί ο δέκτης της κάρτας Ethernet
Start Frame Delimiter (Διαχωριστής Έναρξης Πλαισίου) 1 byte	η ακολουθία **10101011 (0xD5)****, η οποία σημαίνει την έναρξη του πλαισίου Το πλαίσιο Ethernet II (DIX) το θεωρεί ενιαίο με το προοίμιο (ως προοίμιο των 8 byte)
Διεύθυνση MAC Προορισμού (Destination) 6 byte	Η φυσική διεύθυνση (MAC) παραλήπτη είναι 6 byte ** *Μεταδίδεται πρώτα το LSB κάθε οκτάδας (Little-Endian)* (**FF-FF-FF-FF-FF-FF** : διεύθυνση ακρόασης)
Διεύθυνση MAC Προέλευσης (Source) 6 byte	Η φυσική διεύθυνση (MAC) αποστολέα είναι 6 byte, 3 byte OUI + 3 byte κατ' επιλογήν του κατασκευαστή του υλικού (συνήθως, βρίσκεται γραμμένη στη ROM της κάρτας)
Type (Τύπος) ή μήκος πλαισίου (802.3 LLC/SNAP, “raw”) 2 byte	Τιμή ≤1500 : Μήκος πεδίου δεδομένων 0x0000 - 0x05DC Τιμή >1500 : Τύπος δεδομένων 0x0800 **IPv4** 0x8100 **VLAN** 0x86DD Ipv6 0x0806 **ARP** 0x8137 IPX (old)
Δεδομένα (Data-payload) 46-1500 byte	Δεδομένα. PDUs πρωτοκόλλων ανωτέρων επιπέδων. Από 46-1500 byte. Αν είναι < 64 (14+46+4) τότε συμπληρώνεται με δεδομένα padding (συνήθως 0x00). ** Στο Gigabit Ethernet, με την υποστήριξη Jumboframes μπορεί να φτάσει μέχρι και 9000 byte (ανάλογα με τον κατασκευαστή)*
FCS (Frame Checksum Sequence) 4 byte	Ακολουθία ελέγχου σφάλματος (CRC-32) κατά τη μετάδοση του πλαισίου
IPG (InterPacketGap) (96bit) 12 byte	Παύση διάρκειας 96bit ώστε να επιτραπεί στα κυκλώματα του δέκτη να επεξεργαστούν το ληφθέν πλαίσιο και να είναι έτοιμος για τη λήψη επόμενου πλαισίου

Πίνακας 2.4.2.α: Επεξηγήσεις των πεδίων του πλαισίου Ethernet

Jumbo frames

Με την αύξηση των ταχυτήτων στο Ethernet, θεωρήθηκε ότι η δυνατότητα μεταφοράς ωφέλιμου φορτίου μήκους 1500 bytes (MTU=1500) αποτελεί περιοριστικό παράγοντα ειδικά στις εφαρμογές οι οποίες περιλαμβάνουν μαζική μεταφορά μεγάλου όγκου δεδομένων όπως η ανάγνωση και εγγραφή αρχείων σε δικτυακά αποθηκευτικά μέσα.

Εδώ πρέπει να αναφερθεί ότι υπήρξαν αρκετές περιπτώσεις για τις οποίες απαιτήθηκε επέκταση, σε μέγεθος, του πλαισίου Ethernet, όπως για την προσθήκη του VLAN tag. Έτσι έφτασε το IEEE802.3as να αναγνωρίσει μέγιστο μέγεθος πλαισίου τα 2000 bytes αλλά το MTU να παραμείνει στα 1500 bytes.

Διάφοροι κατασκευαστές δικτυακού εξοπλισμού Ethernet άρχισαν να υποστηρίζουν πλαίσια μεγέθους μεγαλύτερου από τα 1500 bytes του προτύπου. Σε ορισμένες περιπτώσεις φτάνουν μέχρι και τα 9000 bytes.

Jumbo frames χαρακτηρίζονται όλα τα πλαίσια Ethernet τα οποία έχουν MTU μεγαλύτερη από την τιμή των 1500 bytes που καθορίζει το πρότυπο ως μέγιστο ωφέλιμο φορτίο.

Δεν υπάρχει βιομηχανικό πρότυπο το οποίο να καθορίζει το μέγεθος ενός jumbo frame. Επιπλέον το IEEE δεν διατίθεται να υποστηρίξει τα jumbo frames εξαιτίας ενστάσεων σχετικά με την διαλειτουργικότητα μεταξύ εξοπλισμού διαφορετικών κατασκευαστών. Παρόλα αυτά διάφοροι κατασκευαστές τα υποστηρίζουν.
Τα πλεονεκτήματα χρήσης Jumbo frames προέρχονται από το γεγονός ότι μεγαλύτερες MTU κάνουν **την επικοινωνία πιο αποδοτική** καθώς οι σταθερές επικεφαλίδες των πρωτοκόλλων ποσοστιαία είναι μικρότερες επί ενός μεγαλύτερου συνόλου απ' ό,τι σε ένα μικρότερο. Έτσι η χρήση jumbo frames αποτελεί **πλεονέκτημα** σε εφαρμογές όπως:

- Συστοιχίες διακομιστών (server clustering)
- Αντίγραφα ασφαλείας σε διακομιστές (πιο γρήγορη λήψη αντιγράφων)
- Δικτυακά συστήματα αρχείων (NFS)
- Δικτυακά συστήματα αποθήκευσης NAS (Network Attached Storage) και SAN (Storage Area Network) π.χ. iSCSI

Αντιθέτως, μεγαλύτερα πλαίσια σημαίνει μεγαλύτερος χρόνος απασχόλησης του μέσου ή της ζεύξης και συνεπώς μεγαλύτερη **υστέρηση ανταπόκρισης και καθυστέρηση** για αυτούς που περιμένουν να χρησιμοποιήσουν το μέσο. Αυτό αποτελεί **μειονέκτημα** σε εφαρμογές όπως:

- Εφαρμογές πραγματικού χρόνου
- Μεταφορά video ή ήχου όπως τηλεφωνία VoIP
- Επικοινωνία διεργασιών (Inter-Process Communication - IPC)

2.4.3 Αυτόματη διαπραγμάτευση, Τύποι σύνδεσης Auto MDI/MDI-X

Με την ύπαρξη εξοπλισμού Ethernet σε υπηρεσία, ο οποίος υποστηρίζει διαφορετικές ταχύτητες επικοινωνίας είναι σημαντικό όλος αυτός ο ανομοιογενής εξοπλισμός να μπορεί να συνεργάζεται και να επικοινωνεί απροβλημάτιστα και μάλιστα με όσο το δυνατόν πιο διαφανή τρόπο για τους χρήστες, δηλαδή με αυτόματο τρόπο χωρίς την ανάγκη ρυθμίσεων από την πλευρά του χρήστη. Αυτό άλλωστε ήταν και σχεδιαστικός στόχος του Ethernet από την αρχή των αναβαθμίσεων σε ταχύτητα, η διαλειτουργικότητα εξοπλισμού διαφορετικών ταχυτήτων και άλλων δυνατοτήτων όπως η υποστήριξη πλήρως αμφίδρομης επικοινωνίας. Ένας από τους μηχανισμούς που συνετέλεσαν στην επίτευξη του στόχου αυτού είναι η **αυτόματη διαπραγμάτευση** (Auto-Negotiation) που πρωτοεμφανίστηκε με το 802.3u το "100BASE-T Fast Ethernet and Auto-Negotiation" το 1995. Με την εμφάνιση των νεότερων εκδόσεων του Ethernet ο μηχανισμός κάλυψε όλα τα πρότυπα που λειτουργούν με καλώδια συνεστραμμένων ζευγών συμπεριλαμβανομένων των 10BASE-T, 100BASE-TX, 1000BASE-T, και 10GBASE-T

Η αυτόματη διαπραγμάτευση δίνει τη δυνατότητα σε σταθμούς Ethernet συνδεδεμένους στο ίδιο τμήμα (segment) δικτύου να ανταλλάξουν στην αρχή της ζεύξης πληροφορίες για τις δυνατότητές τους. Αυτό επιτρέπει στους σταθμούς να ρυθμίσουν στη συνέχεια αυτόματα τις παραμέτρους επικοινωνίας για το καλύτερο δυνατό αποτέλεσμα. Κατ' ελάχιστο, η αυτόματη διαπραγμάτευση μπορεί να ρυθμίσει την **ταχύτητα**, στη μέγιστη κοινά υποστηριζόμενη ταχύτητα, από τους δυο σταθμούς στα άκρα ενός τμήματος. Επίσης ένας μεταγωγέας μπορεί να ανακοινώσει την υποστήριξη **πλήρως αμφίδρομης** (**full duplex**)

επικοινωνίας ώστε ένας σταθμός που συνδέεται σε μια θύρα του και την υποστηρίζει, να ρυθμιστεί σε πλήρως αμφίδρομη επικοινωνία. Η αυτόματη διαπραγμάτευση σχεδιάστηκε να είναι επεκτάσιμη και να μπορεί να υποστηρίξει τη διαπραγμάτευση και ρύθμιση πολλών τρόπων λειτουργίας και χαρακτηριστικών του Ethernet. Τυπικές ταχύτητες που υποστηρίζονται είναι 10/100Mbps, 10/100/1000Mbps και στα 10Gbps είναι αναμενόμενο να υποστηρίζονται 100/1000/10000Mbps.

Η αυτόματη διαπραγμάτευση :

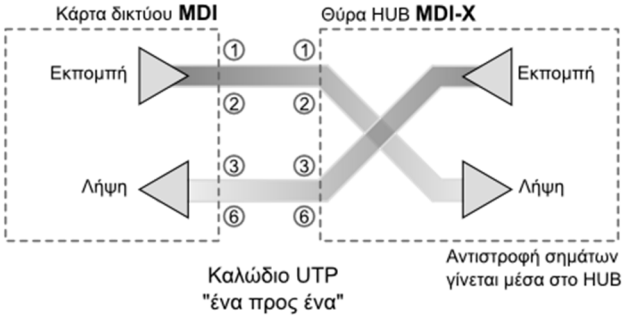
- λειτουργεί πάνω σε ένα τμήμα σύνδεσης ή ζεύξης (link segment), δηλαδή ένα καλώδιο συνεστραμμένων ζευγών με δυο συσκευές, μια σε κάθε άκρο.
- συμβαίνει μια φορά κατά την έναρξη της σύνδεσης και χρησιμοποιεί τη δική της σηματοδοσία ανεξάρτητα από τις ταχύτητες των κόμβων στα δυο άκρα.
- εάν δεν καταλήξει σε έναν κοινά αποδεκτό τρόπο λειτουργίας και ταχύτητα, τότε η ζεύξη δεν μπορεί να αποκατασταθεί.

Ο Πίνακας 2.4.3.α δίνει τη σειρά προτεραιότητας των τρόπων λειτουργίας κατά την αυτόματη διαπραγμάτευση

Τρόπος λειτουργίας	**Μέγιστη ταχύτητα (συνολικά)**
Full-duplex 10GBASE-T	20 Gb/s
Full-duplex1000BASE-T	2 Gb/s
1000BASE-T	1 Gb/s
Full-duplex 100BASE-T2	200 Mb/s
Full-duplex 100BASE-TX	200 Mb/s
100BASE-T2	100 Mb/s
100BASE-T4	100 Mb/s
100BASE-TX	100 Mb/s
Full-duplex 10BASE-T	20 Mb/s
10BASE-T	10 Mb/s

Πίνακας 2.4.3.α: Σειρά προτεραιότητας κατά την αυτόματη διαπραγμάτευση

Όπως προαναφέρθηκε, οι συνδετήρες (connectors) πάνω στις κάρτες δικτύου χαρακτηρίζονται **MDI** (Medium Dependent Interface) και έχουν την έξοδο εκπομπής στους ακροδέκτες 1, 2 (στο 10/100Mbps Ethernet) και την είσοδο για λήψη στους 3, 6. Οι συσκευές διασύνδεσης (HUB/Switches) έχουν στις ίδιες θέσεις την αντίθετη λειτουργία δηλαδή στο (1, 2) είσοδο λήψης και στο (3, 6) έξοδο εκπομπής. Τότε χαρακτηρίζονται ως **MDI-X** (MDI crossed). Αυτό επιτρέπει στους υπολογιστές να συνδέονται σε HUB/Switches με καλώδιο με αντιστοιχία “ένα προς ένα” (straight through cable).



Εικόνα 2.4.3.α: MDI/MDI-X

Η τυποποίηση 1000Base-T συνοδεύτηκε από την προαιρετική δυνατότητα των διασυνδέσεων Ethernet να κατευθύνουν αυτόματα, στο εσωτερικό τους, το σήμα της απομακρυσμένης εκπομπής στην είσοδο του δέκτη τους και την έξοδο εκπομπής τους στην είσοδο του απομακρυσμένου δέκτη. Η δυνατότητα αυτόματης εναλλαγής

σημάτων “auto crossover” επινοήθηκε για να μην είναι αναγκαία η χρήση καλωδίων “crossover” για τη σύνδεση ίδιων συσκευών. Σήμερα οι περισσότερες συσκευές και θύρες μεταγωγέων υποστηρίζουν τη λειτουργία “**auto MDI/MDI-X**” όπως λέγεται.

Η αυτόματη διαπραγμάτευση δεν γνωρίζει τίποτα για τις επιδόσεις και την κατάσταση των φυσικών μέσων. Ελάχιστη απαίτηση, για να λειτουργήσει αποτελεσματικά, είναι **η καλωδίωση να μπορεί να υποστηρίξει απροβλημάτιστα την μεγαλύτερη κοινή ταχύτητα** που μπορούν να υποστηρίξουν οι δυό σταθμοί της ζεύξης. Εάν η θύρα Ethernet του υπολογιστή και η θύρα του μεταγωγέα στον οποίο είναι συνδεδεμένη, υποστηρίζουν από κοινού ως μεγαλύτερη ταχύτητα το 1Gbps τότε η καλωδίωση που τους συνδέει θα πρέπει να είναι κατ' ελάχιστον UTP Cat 5e και καλύτερη και **να έχουν τηρηθεί όλες οι προδιαγραφές και καλές πρακτικές** κατά την εγκατάστασή της. Αν η καλωδίωση είναι κατώτερης κατηγορίας ή εξαιτίας κακών χειρισμών κατά την εγκατάσταση ή λόγω έκθεσης σε αντίξοους παράγοντες με τον καιρό βγήκε εκτός προδιαγραφών, τότε υπάρχει πρόβλημα.

Η αυτόματη διαπραγμάτευση εκτελείται με τη δική της σηματοδοσία στο φυσικό μέσο, χωρίς υψηλές απαιτήσεις εύρους ζώνης ή εξασθένησης απ' αυτό. Έτσι οι δυο σταθμοί, στην αρχή της εγκατάστασης της ζεύξης διαπραγματεύονται επιτυχώς και συμφωνούν την αποκατάστασή της στο 1Gbps. Ξεκινούν την ζεύξη στο 1Gbps, αλλά το φυσικό μέσο δε μπορεί να την υποστηρίξει - είτε καθόλου είτε εμφανίζονται πάρα πολλά πακέτα εσφαλμένα - με αποτέλεσμα εξαιρετικά χαμηλούς ρυθμούς διαμεταγωγής. Η αυτόματη διαπραγμάτευση δεν έχει τη δυνατότητα επαναδιαπραγμάτευσης και ανάνηψης από την προβληματική κατάσταση. Στην περίπτωση αυτή θα πρέπει ο διαχειριστής να επέμβει και να ρυθμίσει χειροκίνητα την κάρτα δικτύου σε χαμηλότερη ταχύτητα (1Gbps -> 100 Mbps) ώστε με την αυτόματη διαπραγμάτευση από την πλευρά του μεταγωγέα να συμφωνήσουν στη χαμηλότερη ταχύτητα η οποία μπορεί να υποστηριχθεί επιτυχώς.

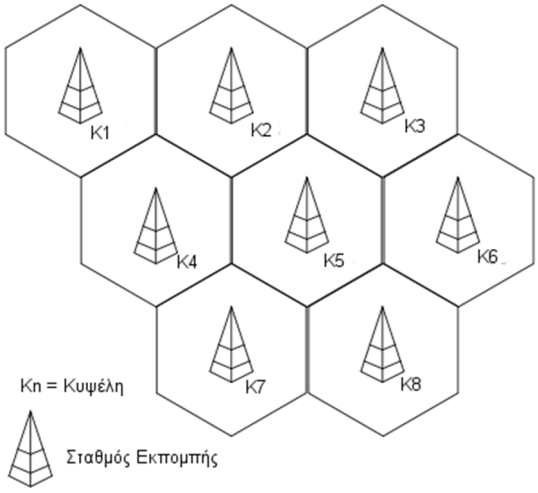
2.5 Ασύρματα Δίκτυα

Ένα **ασύρματο δίκτυο** είναι ένα δίκτυο το οποίο δεν χρησιμοποιεί καλώδια για τις συνδέσεις των διαφόρων συσκευών που δικτυώνονται σε αυτό. Αντί του καλωδίου χρησιμοποιείται η μετάδοση ειδικά διαμορφωμένων οπτικών, υπέρυθρων ή ακόμα και ραδιοκυματικών σημάτων μέσω του αέρα.

Σήμερα τα ασύρματα δίκτυα με την μεγαλύτερη εξάπλωση και εφαρμογή είναι τα κυψελοειδή, καθώς πολλά από τα ασύρματα συστήματα μπορούν να καταταχθούν ως ιδιαίτερες εφαρμογές ή απλές γενικεύσεις των κυψελοειδών δικτύων. Κάθε δίκτυο καλύπτει μια περιοχή που ονομάζεται **κυψέλη** (cell) χρησιμοποιώντας ένα **σταθμό βάσης** (Base Station) και **πολλούς ασύρματους χρήστες-δέκτες**.

Αντίστοιχα, κάθε κυψέλη καλύπτει με ασύρματο σήμα μια περίπου εξαγωνική ή κυκλική περιοχή και πολλές κυψέλες μαζί καλύπτουν μεγάλες εκτάσεις με ασύρματο σήμα, όπως φαίνεται στο σχήμα 2.5.α. Στο συγκεκριμένο σχήμα υπεραίρουν 8 σταθμοί βάσης/εκπομπής σήματος, οι οποίοι σχηματίζουν αντίστοιχα 8 κυψέλες με κάλυψη εμβέλειας ασύρματου σήματος. Οι σταθμοί εκπομπής έχουν συνήθως τη μορφή της εικόνας 2.5.α.

Προϋπόθεση για τη σύνδεση των μεταξύ τους συσκευών είναι να έχουν εξοπλιστεί με το κατάλληλο υλικό διεπαφής που επιτρέπει τη σύνδεσή τους μέσω ασύρματης τεχνολογίας.



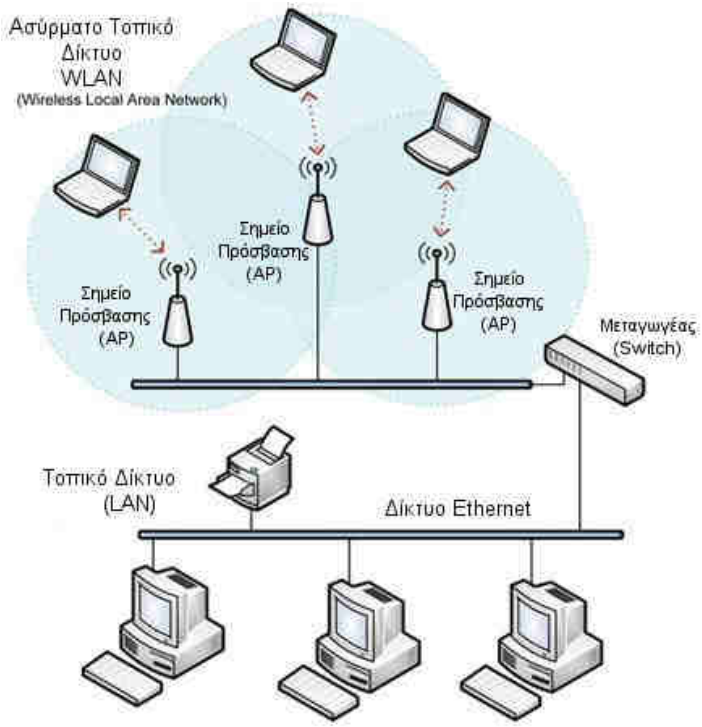
Σχήμα 2.5.α: Δίκτυο με κυψέλες

(*Προσαρμοσμένη από Πηγή: http://en.wikipedia.org/wiki/Cellular_network*)

Εικόνα 2.5.β: Κεραία-σταθμός εκπομπής ασύρματου σήματος

Ασύρματο τοπικό δίκτυο. Τα ασύρματα τοπικά δίκτυα (WLAN, Wireless Local Area Network) είναι τα δίκτυα που επιτρέπουν σε ένα χρήστη κινητής συσκευής, όπως είναι ένας φορητός υπολογιστής, ένα έξυπνο τηλέφωνο ή ένα tablet, να συνδέονται σε ένα τοπικό δίκτυο (LAN) μέσω μιας ασύρματης σύνδεσης που χρησιμοποιεί υψηλής συχνότητας ραδιοκύματα.

Όπως φαίνεται στο Σχήμα 2.5.β, ένα σύστημα από τρία (3) σημεία πρόσβασης (APs) σχηματίζουν ένα WLAN και επιτρέπουν σε φορητές συσκευές, εντός εμβέλειας του σήματος, να συνδεθούν με αυτά. Τα σημεία πρόσβασης συνδέονται ενσύρματα με έναν μεταγωγέα (switch) και στη συνέχεια με το ενσύρματο τοπικό δίκτυο (LAN). Με αυτόν τον τρόπο δίνεται η δυνατότητα επέκτασης του τοπικού δικτύου και παροχής δικτυακών υπηρεσιών σε ένα μεγαλύτερο αριθμό συσκευών.



Σχήμα 2.5.β: Ασύρματο τοπικό δίκτυο συνδεόμενο με ενσύρματο τοπικό δίκτυο
(*Προσαρμοσμένη από Πηγή: http://bb-smartworx.com/make-tablets-smart-phones-smarter-add-serial-capability-seriously-remote-data/*)

Πρωτόκολλο IEEE 802.11. Το πρωτόκολλο που υλοποιεί τα ασύρματα τοπικά δίκτυα είναι το IEEE 802.11. Το πρωτόκολλο IEEE 802.11 διαιρείται σε μια ομάδα προτύπων ασύρματης δικτύωσης (εκδόσεις "a" έως "n"), τα οποία αποτελούν τα επικρατέστερα πρότυπα αυτής παγκοσμίως.

Στο πρωτόκολλο αυτό περιγράφονται τα δύο κατώτερα επίπεδα του OSI, δηλαδή το φυσικό επίπεδο και το επίπεδο σύνδεσης δεδομένων, επιτρέποντας τη συνεργασία των συσκευών και εφαρμογών που ακολουθούν το πρότυπο αυτό. Ουσιαστικά, οι συσκευές που υποστηρίζουν το πρωτόκολλο IEEE802.11 μεταφέρουν την πληροφορία από και προς τα ανωτέρα επίπεδα του OSI. Χρησιμοποιεί το πρωτόκολλο Ethernet και το CSMA/CA (carrier sense multiple access with collision avoidance) για διαμοιρασμό του καναλιού και για κρυπτογράφηση τους αλγορίθμους WEP, WPA και WPA2.

Τα πιο γνωστά πρότυπα αυτού του πρωτοκόλλου, οι ρυθμοί μετάδοσής τους και οι συχνότητες που υποστηρίζει το κάθε ένα από αυτά φαίνονται στον πίνακα 2.5.α.

Πρότυπο IEEE	Μέγιστος ρυθμός μετάδοσης	Συχνότητες
802.11	1 Mbps/2 Mbps	2.4 GHz
802.11a	11 Mbps	5 GHz
802.11b	5.5 Mbps/11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	600 Mbps	2.4 GHz & 5 GHz

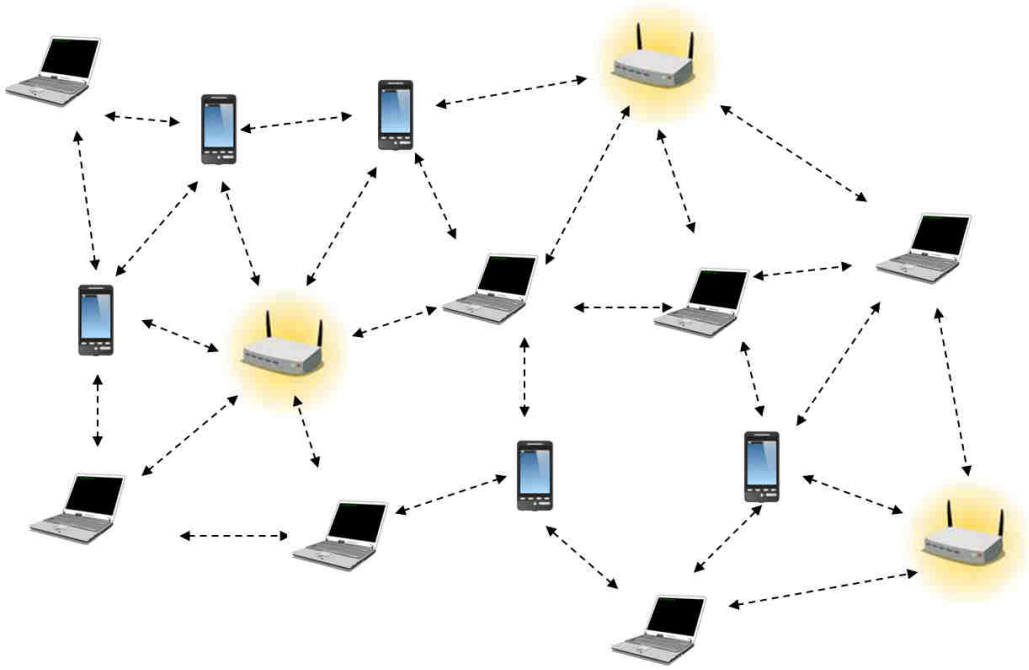
Πίνακας 2.5.α: Συγκριτικός πίνακας βασικών προτύπων του IEEE 802.11

Ένα **Ασύρματο Σημείο Πρόσβασης (Access Point, AP)** είναι μια **συσκευή** που αναλαμβάνει τη λειτουργία της ραδιοεπικοινωνίας με τους ασύρματους σταθμούς σε μια κυψέλη. Η συσκευή αυτή μπορεί να είναι εξωτερική συνδεόμενη ενσύρματα με ένα δρομολογητή, εσωτερική μονάδα σε ένα δρομολογητή ή υλοποιείται με χρήση λογισμικού και μιας κάρτας PCI σε ένα Η/Υ.

Το σημείο πρόσβασης λειτουργεί σαν σταθμός βάσης συγκεντρώνοντας την κίνηση από τους ασύρματους σταθμούς και κατευθύνοντας την προς το υπόλοιπο δίκτυο. Άλλες λειτουργίες που αναλαμβάνει, είναι η αυθεντικοποίηση ενός καινούργιου σταθμού που ζητά πρόσβαση στο ασύρματο δίκτυο και η συσχέτιση μαζί του.

2.5.1 Τοπολογία Ασύρματου δικτύου Ad-Hoc

Ένα **ασύρματο ad hoc δίκτυο (αυτοοργανωμένο ή κατ' απαίτηση)**, είναι ένας αποκεντρωμένος τύπος ασύρματου δικτύου και δεν βασίζεται σε κάποια προϋπάρχουσα υποδομή, όπως είναι η χρήση ασύρματων σημείων πρόσβασης (AP) στα προκαθορισμένα ασύρματα δίκτυα ή δρομολογητές στα ενσύρματα δίκτυα. Αντίθετα, κάθε κόμβος λαμβάνει μέρος στη δρομολόγηση προωθώντας τα δεδομένα προς τους άλλους κόμβους και η δρομολόγηση, καθώς και η επιλογή των κόμβων που προωθούν δεδομένα γίνεται δυναμικά, με βάση τη συνδεσιμότητα του δικτύου.

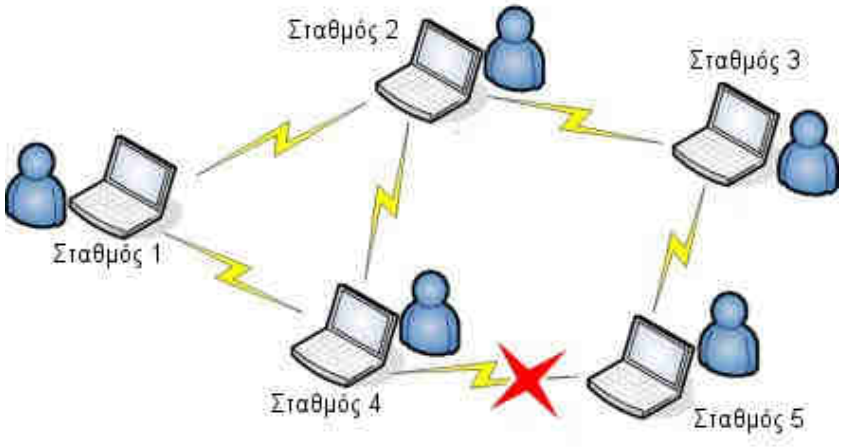


Σχήμα 2.5.1.α: Μετάδοση δεδομένων με χρήση τοπολογίας ad-hoc

(*Πηγή: http://www.thelifenetwork.org/about.html*)

Πλεονεκτήματα. Ο αποκεντρωμένος χαρακτήρας των ασύρματων ad hoc δικτύων τα καθιστά κατάλληλα για ποικίλες εφαρμογές, οι οποίες δε μπορούν να βασίζονται σε κεντρικούς κόμβους και προκαθορισμένα ασύρματα δίκτυα. Η γρήγορη εγκατάσταση και η ελάχιστη απαιτούμενη διαμόρφωση τα καθιστούν κατάλληλα για **καταστάσεις έκτακτης ανάγκης**, όπου απαιτείται η άμεση εγκατάσταση δικτύου με κατεστραμμένη προϋπάρχουσα υποδομή, πχ. σε περίπτωση καταστροφικού σεισμού. Επίσης επιτρέπουν τη γρήγορη αποκατάσταση της δικτύωσης σε **περίπτωση βλάβης** ενός κόμβου, αφού επιλέγεται εύκολα μια εναλλακτική διαδρομή δρομολόγησης.

Για παράδειγμα στο σχήμα 2.5.1.β, η βλάβη που παρουσιάζεται στη σύνδεσης μεταξύ των σταθμών 4 και 5 δεν συνεπάγεται την διακοπή της επικοινωνίας του σταθμού 5 με το υπόλοιπο δίκτυο, αφού υπάρχει η δυνατότητα επιλογής εναλλακτικής διαδρομής μέσω των σταθμών 2 και 3.



Σχήμα 2.5.1.β: Ασύρματο δίκτυο τοπολογίας ad-hoc με παρουσία βλάβης

Τέλος τα ad hoc δίκτυα είναι ευέλικτα και κατάλληλα για την **απευθείας σύνδεση δύο συσκευών**, χωρίς τη χρήση ενός κεντρικού σημείου πρόσβασης.

Μειονεκτήματα. Ωστόσο, απαιτεί **περισσότερους πόρους** από τις συσκευές για τη διατήρηση της σύνδεσης, αν αυτές μετακινούνται και παράλληλα η **εμβέλεια** των συστημάτων σύνδεσής του είναι **μικρότερη** σε σχέση με ένα σταθερό σημείο πρόσβασης. Τέλος βασικό μειονέκτημα τους είναι **αδυναμία πρόβλεψης** της ποικιλίας των **πιθανών καταστάσεων** που μπορεί να προκύψουν, λόγω του δυναμικού χαρακτήρα εδραίωσης της επικοινωνίας.

2.5.2 Τοπολογία Ασύρματου δικτύου υποδομής (Infrastructure)

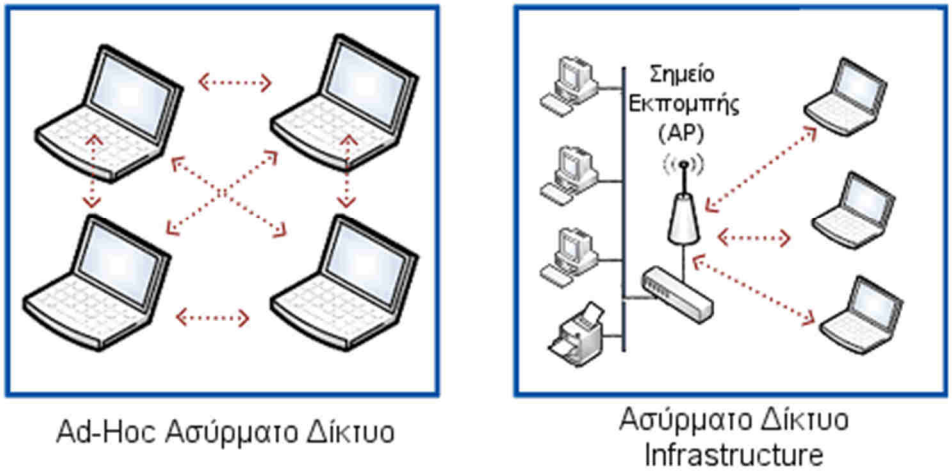
Τα **ασύρματα δίκτυα υποδομής (Infrastructure Wireless Networks)** είναι μια πιο σύνθετη τοπολογία ασύρματης δικτύωσης. Σε αυτή το ασύρματο δίκτυο έχει την κυψελοειδή μορφή ασύρματων δικτύων που προαναφέραμε, αποτελούμενο από έναν αριθμό από κυψέλες. Η κυψέλη είναι το βασικό δομικό στοιχείο αυτής της τοπολογίας ασύρματου δικτύου.

Σε κάθε κυψέλη υπάρχει ένας **σημείο πρόσβασης (AP, Access Point)** και ένας αριθμός από **ασύρματους σταθμούς**, οι οποίοι εξυπηρετούνται από το σημείο πρόσβασης. Κάθε σταθμός που θέλει να συνδεθεί στο ασύρματο δίκτυο πρέπει να κάνει αίτημα σύνδεσης σε ένα σημείο πρόσβασης και ξεκινά τη **διαδικασία συσχετισμού (Association Process),** όπου στο τέλος της το σημείο πρόσβασης κάνει δεκτό το αίτημα ή το απορρίπτει.

Πλεονεκτήματα. Η τρόπος αυτός ασύρματης σύνδεσης είναι **ιδανικός για την εγκατάσταση ενός μόνιμου δικτύου,** όπου γνωρίζουμε εκ των προτέρων ποιες είναι οι περιοχές οι οποίες πρέπει να έχουν κάλυψη δικτυακού σήματος. Επίσης οι ασύρματοι δρομολογητές που χρησιμοποιούνται ως σημεία πρόσβασης έχουν συνήθως **μεγαλύτερη εμβέλεια κάλυψης** και **διευκολύνουν την κινητικότητα** των ασυρμάτων συσκευών εντός της κυψελοειδούς περιοχής.

Μειονεκτήματα. Ο **σχεδιασμός** αυτής της τοπολογίας ασύρματου δικτύου είναι σαφώς πιο **περίπλοκος** και κατά τον οποίο πρέπει να ληφθούν υπόψη πολλές παράμετροι για την επιλογή της κατάλληλης τοποθεσίας του σταθμού εκπομπής. Αυτό γιατί ο σταθμός

εκπομπής είναι ο **μόνος διαθέσιμος πόρος δικτύου** σε αυτή την περιοχή και πρέπει να έχει τη μέγιστη δυνατή κάλυψη, ανεμπόδιστα από φυσικά εμπόδια που εξασθενούν το σήμα.



Εικόνα 2.5.2.α: Διαφορά ασύρματων τοπολογιών Ad-Hoc και Infrastructure

(*Προσαρμοσμένη από Πηγή: http://www.bb-elec.com/Learning-Center/All-White-Papers/Wireless-Cellular/How-to-Make-Devices-Communicate-in-a-Wireless-Worl.aspx*)

Τέλος υπάρχουν και υβριδικές τοπολογίες, οι οποίες συνδυάζουν και τις δύο προαναφερόμενες τοπολογίες, ad-hoc και Infrastructure, για καλύτερη κάλυψη περιοχών με ασύρματο σήμα.

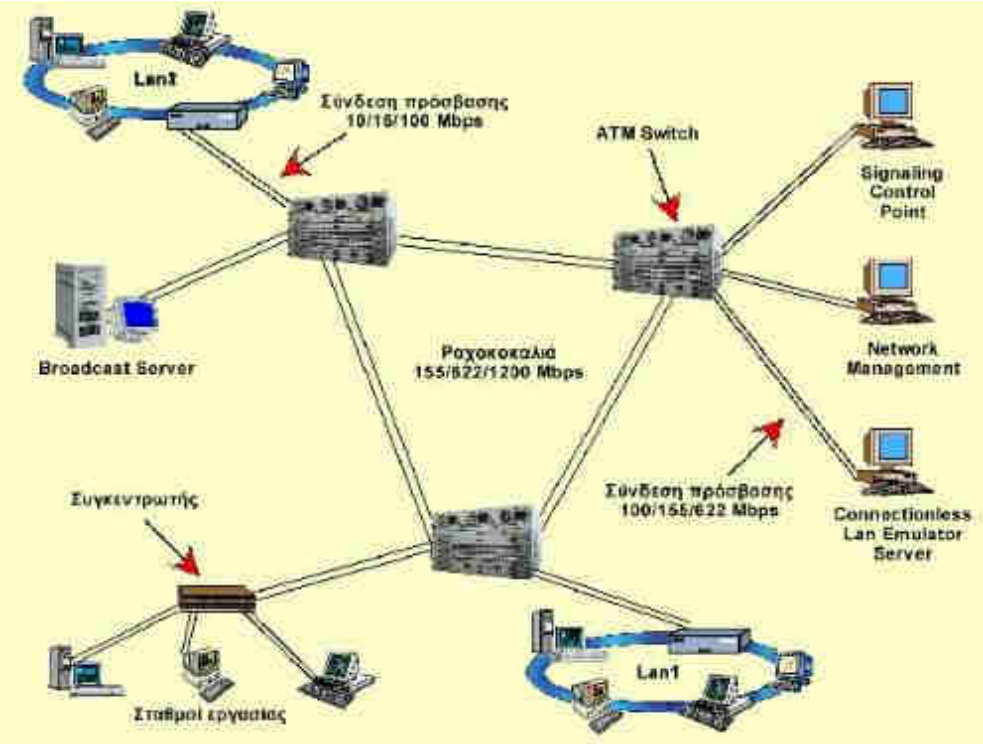
2.6 Τεχνολογία Ασύγχρονου Τρόπου Μεταφοράς Δεδομένων (Asynchronous Transfer Mode, ATM)

Σε συντομία, το ATM είναι μία τεχνολογία μεταγωγής και πολυπλεξίας, σε επίπεδο κυψελίδων (cells). ATM σημαίνει “Asynchronous Transfer Mode” δηλαδή “Ασύγχρονος Τρόπος Μεταφοράς” δεδομένων λόγω του τρόπου μεταφοράς των κυψελίδων. Ο τρόπος μεταφοράς λειτουργεί με τρόπο ώστε οι κυψελίδες να αναγνωρίζονται με προθεματικές ετικέτες και όχι από τη χρονική θέση, όπως γίνεται στο Σύγχρονο Τρόπο Μεταφοράς (STM - Synchronous Transfer Mode).

Η τεχνολογία ATM προδιαγράφτηκε αρχικά για τη δημιουργία του ISDN ευρείας ζώνης (Broadband ISDN). Συνδυάζει την αποδοτικότητα της μεταγωγής πακέτων με την αξιοπιστία της μεταγωγής κυκλώματος. Για τη μετάδοση των δεδομένων, χρησιμοποιεί σταθερού μεγέθους πακέτα των 53 bytes, τις κυψέλες (cells). Το γεγονός, ότι χρησιμοποιούνται κυψέλες σταθερού μεγέθους, επιβαρύνει πολύ λιγότερο τις διεργασίες μεταγωγής και δρομολόγησης, που εκτελούνται σε κάθε κόμβο του δικτύου ATM. Έτσι, μπορούν να επιτευχθούν πολύ υψηλές ταχύτητες μεταγωγής των δεδομένων.

Το ATM προσφέρει τα εξής πλεονεκτήματα:

- Ταχύτητα: υποστηρίζει ρυθμούς μεταφοράς μέχρι και 622 Mbps.
- Επεκτασιμότητα: επιτρέπει το αυξημένο εύρος ζώνης μέσα στις ήδη υπάρχουσες αρχιτεκτονικές.
- Αποκλειστικό εύρος ζώνης: εγγυάται το ρυθμό μεταφοράς γία μία υπηρεσία.
- Παγκόσμια εφαρμογή: προσφέρει τη δυνατότητα μίας λύσης από άκρο-σε-άκρο, από τοπικό επίπεδο μέχρι δίκτυο ευρείας περιοχής (WAN).



Σχήμα 2.6.α: Δίκτυο ATM

(*Πηγή: http://ebooks.edu.gr/modules/ebook/show.php/DSGL-C104/423/2835,10774/*)

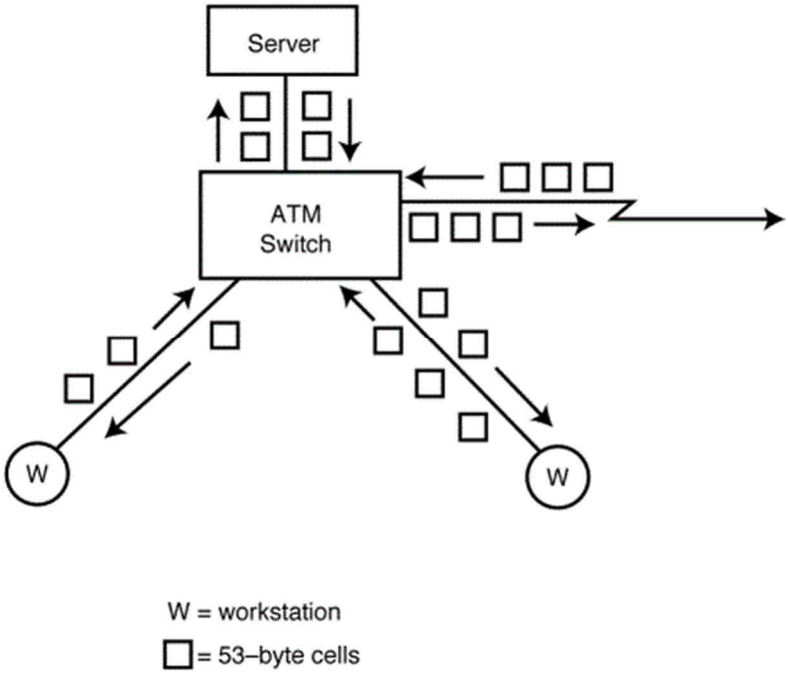
Κυψελίδα ATM (cell). Μία στοιχειώδης κυψελίδα ATM αποτελείται από 53 οκτάδες (octets/ bytes) εκ των οποίων:

- Οι 5 πρώτες αποτελούν την επικεφαλίδα (header), η οποία περιέχει σε 3 οκτάδες το μοναδικό αναγνωριστικό σύνδεσης VCI ή VPI, μία οκτάδα ελέγχου και μία οκτάδα με κώδικα ανίχνευσης λάθους για την επικεφαλίδα.
- Οι υπόλοιπες 48 οκτάδες είναι δεδομένα του χρήστη (payload), με προαιρετικά 4 από αυτές να χρησιμοποιούνται σαν αναγνωριστικά για την ανασυγκρότηση μεγαλύτερων πακέτων για ανώτερα στάδια από το ATM σύμφωνα με το μοντέλο OSI.

Η ιδέα του ATM είναι η εξής:

Αντί να αναγνωρίζει το σύστημα τον αριθμό της σύνδεσης από τη θέση του πακέτου όπως στο STM, απλώς φέρει το πακέτο τον αριθμό της σύνδεσης μαζί με τα δεδομένα, και ταυτόχρονα κρατά μικρό τον συνολικό αριθμό των bytes σε ένα πακέτο, έτσι ώστε, αν χαθεί κάποιο λόγω συμφόρησης, αυτό να έχει ελάχιστη επιρροή στην ροή των δεδομένων και ίσως να μπορεί να ανακτηθεί με ειδικούς αλγόριθμους.

Το ATM παρέχει είτε μόνιμα (PVCs) είτε επιλεγόμενα (SVCs) **νοητά κανάλια**. Τα νοητά αυτά κανάλια μπορούν να υποστηρίξουν ”σταθερό αριθμό δυαδικών ψηφίων” (CBR - Constant Bit Rate) ή “μεταβλητό αριθμό δυαδικών ψηφίων” (VBR - Variable Bit Rate). Κάθε κυψελίδα ATM που στέλνεται στο δίκτυο περιέχει πληροφορίες διευθυνσιοδότησης που επιτρέπουν την εγκατάσταση ενός νοητού καναλιού μεταξύ των σημείων αποστολής και λήψης. Στη συνέχεια όλες οι κυψελίδες μεταφέρονται μέσω του νοητού καναλιού με τη σειρά αποστολής τους.



Σχήμα 2.6.β: Μεταφορά κυψελίδων ATM (cells)

(*Πηγή*: *https://technet.microsoft.com/en-us/library/bb962019.aspx*)

Ένα δίκτυο ATM αποτελείται από **μεταγωγείς ATM** (ATM switches) υψηλής ταχύτητας, οι οποίοι δρομολογούν χωρίς καθόλου καθυστέρηση τις εισερχόμενες κυψέλες. Έτσι, η τεχνολογία ATM προσφέρει πολύ υψηλές ταχύτητες ακόμη και κάτω από συνθήκες ιδιαίτερα αυξημένης κίνησης στο δίκτυο.

Εικόνα 2.6.α: Μεταγωγείς ATM

Σαν μέσο μετάδοσης μπορεί να χρησιμοποιηθεί οποιοδήποτε από τα διαθέσιμα μέσα, όπως συνεστραμμένο ζεύγος καλωδίων, ομοαξονικό καλώδιο, οπτική ίνα. Η μετατροπή της υπάρχουσας δικτυακής υποδομής σε καθαρά ATM περιβάλλον απαιτεί σε μεγάλο βαθμό αντικατάσταση του εξοπλισμού, κάτι που αποτελεί ανασταλτικό παράγοντα στην ταχεία και σε μεγάλη κλίμακα εξάπλωση της τεχνολογίας ATM. Έχει όμως ήδη αρχίσει να αποτελεί κύρια επιλογή στην ανάπτυξη δικτύων κορμού (backbone).

Στόχος του ATM είναι η δημιουργία ενός ενιαίου δικτύου το οποίο θα υποστηρίζει:

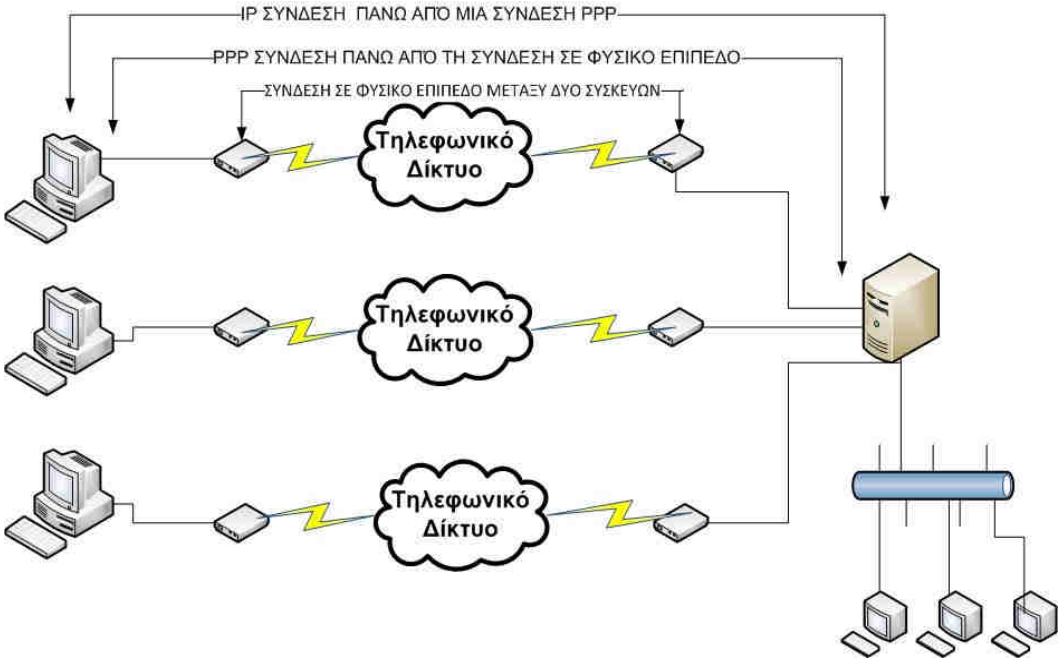
- Τηλεδιάσκεψη (Video Conferencing)
- Διάσκεψη από γραφείο σε γραφείο (Desktop Conferencing)
- Εικονοτηλέφωνο (Videophone)
- Εικόνα/Ηχος κατά παραγγελία (Audio/Video On Demand)

- Εικονικά τοπικά δίκτυα (VLANs: Virtual LANs)
- Επικοινωνίες ATM μεγάλης χωρητικότητας με κινητούς κόμβους (συνήθως με δορυφορικές ζεύξεις)

2.7 Πρωτόκολλο Σύνδεσης Σημείου προς Σημείο (PPP)

Το επίπεδο ζεύξης (σύνδεσης) δεδομένων που βρίσκεται κάτω από το επίπεδο δικτύου είναι υπεύθυνο για την αποδοτική επικοινωνία μεταξύ των γειτονικών κόμβων ενός δικτύου. Οι γειτονικοί κόμβοι μπορεί να είναι μέλη ενός τοπικού δικτύου σε ένα δίκτυο πολλαπλής πρόσβασης ή δύο κόμβοι σε απευθείας σύνδεση σε ένα δίκτυο σημείο προς σημείο. Αρχικά τον τρόπο επικοινωνίας στις συνδέσεις σημείο προς σημείο καθόριζε ένα μη τυποποιημένο πρωτόκολλο χωρίς ιδιαίτερες δυνατότητες το SLIP.

Το πρωτόκολλο Σύνδεσης Σημείου προς Σημείο (Point to Point Protocol, PPP) πρωτοεμφανίστηκε στα τέλη της δεκαετίας το '80 για να καλύψει το κενό της ύπαρξης ενός ολοκληρωμένου πρωτοκόλλου στο επίπεδο ζεύξης δεδομένων που διασυνδέει το επίπεδο δικτύου IP του TCP/IP με το φυσικό επίπεδο σε σειριακές συνδέσεις μεταξύ δύο συσκευών. Σήμερα το PPP είναι μια ολοκληρωμένη οικογένεια από πρωτόκολλα που συνεχώς εξελίσσονται και ενσωματώνουν δυνατότητες ώστε να καλύπτουν νέες ανάγκες. Συχνά αναφέρεται το βασικό PPP ως ένα πρωτόκολλο και τα επιπλέον πρωτόκολλα που ενσωματώνει αναφέρονται ως υποπρωτόκολλα του PPP.



Εικόνα 2.7.α: Εγκατάσταση σύνδεσης με πρωτόκολλο Σύνδεσης Σημείου προς Σημείο (PPP)

Το πρωτόκολλο επιπέδου ζεύξης δεδομένων PPP παρέχει τις διαδικασίες μεταφοράς πληροφοριών πάνω σε συγχρονισμένα και ασυγχρόνιστα κανάλια επικοινωνίας επιτρέποντας ημιαμφίδρομη και πλήρη αμφίδρομη επικοινωνία μεταξύ **δύο** συσκευών, μεταφέροντας σε μορφή πλαισίων (frames) πακέτα από οποιοδήποτε πρωτόκολλο του επίπεδου δικτύου (IP, IPX κ.α) στο φυσικό μέσο.

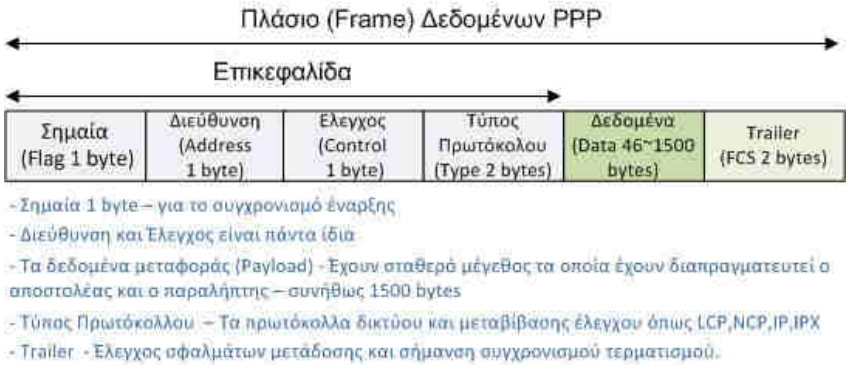
Δυνατότητες και πλεονεκτήματα του PPP. Το πρωτόκολλο PPP είναι πρωτόκολλο προσανατολισμένο σε σύνδεση (Connection Oriented Protocol) δηλαδή παρέχει υπηρεσίες

αξιόπιστης σύνδεσης πάνω σε μια εγκατεστημένη σύνδεση μεταξύ δύο άκρων υποστηρίζοντας πλαισίωση των πακέτων και επιπλέον ένα σύνολο από ελέγχους και δυνατότητες για την εξασφάλιση της μεταφοράς των πληροφοριών όπως:

- Την πολυπλεξία πακέτων από διαφορετικά πρωτόκολλα του επιπέδου δικτύου σε μια σύνδεση.
- Τον έλεγχο σφαλμάτων μετάδοσης μέσω του πεδίου CRC στην επικεφαλίδα κάθε πλαισίου.
- Παρέχει μηχανισμό διαπραγμάτευσης των παραμέτρων της σύνδεσης, όπως το μέγιστο επιτρεπόμενο μέγεθος πλαισίου
- Παρέχει τεχνικές ελέγχου την ποιότητας της σύνδεσης πριν την μετάδοση και επίβλεψης κατά την διάρκεια μετάδοση των πλαισίων.
- Υποστηρίζει έλεγχο πιστοποίησης ταυτότητας υποστηρίζοντας πολλά διαφορετικά πρωτόκολλα όπως (PAP, CHAP κ.α.) πριν την εγκατάσταση της σύνδεσης.
- Υποστηρίζει επιπλέον δυνατότητες όπως συμπίεση, κρυπτογράφηση, και εκμετάλλευση πολλών διαφορετικών συνδέσεων σε φυσικό επίπεδο υλοποιώντας ένα ιδεατό κανάλι αυξημένων επιδόσεων.

Η λειτουργία εγκατάστασης της σύνδεσης και της μετάδοσης δεδομένων του PPP στηρίζεται σε τρία βασικά μέρη:

- **Η ενθυλάκωση PPP:** Η πρωταρχική δουλεία του PPP είναι να παραλάβει τα πακέτα από το επίπεδο δικτύου και να τα ενθυλακώσει σε πλαίσια (frames), τη μονάδα μεταφοράς του επίπεδου ζεύξης δεδομένων. Τα πλαίσια δημιουργούνται ενσωματώνοντας τα δεδομένα μαζί με απλές πληροφορίες έλεγχου της μεταφοράς εξασφαλίζοντας μικρό μέγεθος πλαισίου για την μεγιστοποίηση της αποδοτικότητας της μετάδοσης και της ταχύτητας επεξεργασίας.



Εικόνα 2.7.β: Πλαίσιο PPP

- **Το Πρωτόκολλο Ελέγχου Σύνδεσης (LCP):** Το πρωτόκολλο LCP είναι υπεύθυνο για την εγκατάσταση, διατήρηση και τερματισμό της σύνδεσης μεταξύ των δυο γειτονικών διεπαφών των συσκευών. Είναι ένα εκτεταμένο πρωτόκολλο που επιτρέπει μεγάλο αριθμό ρυθμίσεων και ανταλλαγής παραμέτρων που εξασφαλίζουν τον χρησιμοποίηση της σύνδεσης με τον τρόπο που συμφωνήθηκε. Επίσης στο πρωτόκολλο ελέγχου υποστηρίζεται ένα σύνολο από διαφορετικά πρωτόκολλα πιστοποίησης ταυτότητας (authentication) πριν την εγκατάσταση της σύνδεσης. Επιπλέον προστέθηκαν με την πάροδο του χρόνου αρκετά προαιρετικά πρωτόκολλα που υποστηρίζουν συμπίεση, κρυπτογράφηση και άλλα.
- **Τα πρωτόκολλα Ελέγχου Δικτύου (NCPs):** Επειδή το πρωτόκολλο PPP υποστηρίζει την ενθυλάκωση στο πλαίσιο διαφορετικούς τύπους πακέτων που

χρησιμοποιούνται στο επίπεδο δικτύου η διαχείριση τους στην εγκατάσταση της σύνδεσης διαφέρει σε κάθε περίπτωση στο επίπεδο ζεύξης. Μετά τον καθορισμό των γενικών ρυθμίσεων σύνδεσης από το LCP ο έλεγχος μεταβιβάζεται στο NCP πρωτόκολλο που αντιστοιχεί στον τύπο των πακέτων του πρωτοκόλλου που χρησιμοποιείται στο επίπεδο δίκτυο και απαιτεί επιπλέον ειδικότερες ρυθμίσεις για την εγκατάσταση της σύνδεσης. Τέτοια πρωτόκολλα είναι το IPCP για το IP, NBF για το IPX και NetBIOS κ.α.

Η λειτουργία μετάδοσης δεδομένων με τη χρήση του PPP διακρίνεται σε τρεις βασικές φάσεις:

- **1η Φάση - Η εγκατάσταση της σύνδεσης:** Πριν οι δυο συσκευές αρχίσουν να ανταλλάσσουν δεδομένα διαπραγματεύονται τις παραμέτρους σύνδεσης που πρόκειται να εγκατασταθεί. Σ' αυτή τη φάση το βασικό πρωτόκολλο αφού ολοκληρώσει τις γενικές ρυθμίσεις μεταβιβάζει την διαδικασία έλεγχου ρυθμίσεων της εγκατάστασης σύνδεσης σε επιπλέον πρωτόκολλα για εκτέλεση πρόσθετων διαδικασιών, όπως πιστοποίηση ταυτότητας, συμπίεση, κρυπτογράφηση και ειδικές διεργασίες που απαιτούνται από το συγκεκριμένο πρωτόκολλο του επιπέδου δικτύου.
- **2η Φάση – Λειτουργία σε σύνδεση.** Σ' αυτή τη φάση οι συσκευές παραλαμβάνει πακέτα από το επίπεδο δικτύου τα ενθυλακώνει σε πλαίσια και τα μεταφέρει στο φυσικό επίπεδο. Η συσκευή παραλήπτης λαμβάνει το πλαίσιο όπου εφαρμόζοντας την αντίστροφη διαδικασία παράγει το αρχικό πακέτο και το μεταφέρει στο επίπεδο δικτύου.
- **3η Φάση – Τερματισμός σύνδεσης.** Όταν ολοκληρωθεί η μεταφορά - ή για οποιοδήποτε άλλο λόγο - κάθε συσκευή έχει την δυνατότητα σύμφωνα με το πρωτόκολλο ελέγχου σύνδεσης να τερματίσει τη σύνδεση.

Επεκτασιμότητα του πρωτοκόλλου PPP

Ένα από τα σημαντικότερα πλεονεκτήματα του πρωτοκόλλου PPP είναι η επέκταση των δυνατοτήτων του. Αρχικά ξεκίνησε να διαδίδεται ως βασική μέθοδος σειριακής σύνδεσης στο επίπεδο ζεύξης δεδομένων μεταξύ δύο κόμβων και ιδιαίτερα στην πρόσβαση στο Διαδίκτυο με Dialup συνδέσεις και τη χρήση modem. Σήμερα η διάδοση του PPP έχει οδηγήσει στην ανάπτυξη νέων προεκτάσεων του πρωτοκόλλου PPP όπως το πρωτόκολλο PPP επάνω σε Ethernet (PPPoE) και του PPP επάνω σε ATM (PPPoA) που χρησιμοποιούνται για τη σύνδεση στο Διαδίκτυο με τη χρήση τεχνολογίας xDSL.

Ερωτήσεις - Ασκήσεις Κεφαλαίου

1. Ποιες οι βασικές λειτουργίας του φυσικού επιπέδου και του επιπέδου σύνδεσης δεδομένων στο μοντέλο αναφοράς OSI;
2. Ποιες οι βασικές λειτουργίας του επιπέδου πρόσβασης δικτύου του προτύπου TCP/IP;
3. Τι ονομάζεται μέθοδος προσπέλασης (access method) στο μέσο μετάδοσης;
4. Ποιοι είναι οι τρόποι για την αποφυγή ταυτόχρονης χρήσης του μέσου μεταφοράς;
5. Ποιους τρόπους υπηρεσιών παρέχει το υποεπίπεδο LLC με βάση το πρότυπο IEEE 802.2;
6. Στην περίπτωση που γνωρίζατε ότι το κανάλι επικοινωνίας, που είχατε στη διάθεση σας,εξασφαλίζει πολύ μικρό ποσοστό λαθών, ποιου είδους υπηρεσία για τον Ελεγχο Λογικής Σύνδεσης θα προτιμούσατε, εάν μπορούσατε να επιλέξετε και γιατί:
    α. Υπηρεσία χωρίς επιβεβαίωση και χωρίς σύνδεση.
    β. Υπηρεσία με επιβεβαίωση λήψης χωρίς σύνδεση.
    γ. Υπηρεσία με σύνδεση.
7. Τι εννοούμε με τον όρο «σύγκρουση» (collision) στη μέθοδο πρόσβασης στο μέσο CSMA/CD;
8. Εξηγείστε τους λόγους, που θέτουν περιορισμούς στο μήκος των μεταδιδόμενων πακέτων από τους σταθμούς εργασίας, καθώς και στο μήκος των καλωδίων που χρησιμοποιούνται, στο πρότυπο IEEE 802.3.
9. Ο χρόνος επανεκπομπής των σταθμών εργασίας σε δίκτυο IEEE 802.3, σε περίπτωση σύγκρουσης είναι :
    α. Καθορισμένος.
    β. Τυχαίος.
    γ. Ρυθμιζόμενος.
10. Σε τι διαφέρει η μετάδοση βασικής ζώνης (Baseband) από τη μετάδοση ευρείας ζώνης (broadband);
11. Περιγράψτε πως είναι κατασκευασμένο ένα καλώδιο F/UTP (FTP).
12. Περιγράψτε πως είναι κατασκευασμένο ένα καλώδιο S/FTP (SSTP).
13. Πόσα ζεύγη έχει ένα καλώδιο UTP που χρησιμοποιείται στο Ethernet και ποια είναι η μέγιστη απόσταση που καλύπτει σύμφωνα με το πρότυπο; Αναφέρετε τα χρώματα των ζευγών;
14. Ποιο πλεονέκτημα δίνει η θωράκιση σε ένα καλώδιο;
15. Αναφέρετε τη σειρά τερματισμού των ζευγών ενός καλωδίου UTP σε συνδετήρα 8p8c τύπου “RJ-45”. Δώστε την αντιστοιχία χρωμάτων - ακροδεκτών σύμφωνα με το πρότυπο συρμάτωσης T568A.
16. Δυο οπτικές ίνες έχουν διαστάσεις πυρήνα/επικάλυψης (core/cladding) η A: 50/125μm και η B: 9/125μm. Ποια από τις δυο είναι πολύτροπη και ποια μονότροπη; Ποια έχει χαμηλότερη εξασθένηση και καλύπτει μεγαλύτερες αποστάσεις;
17. Αναφέρετε δυο αντικειμενικούς στόχους της κωδικοποίησης και ηλεκτρικής σηματοδότησης σε μια επικοινωνία μέσα από ένα φυσικό μέσο-κανάλι.
18. Περιγράψτε τη δομή μιας φυσικής διεύθυνσης MAC Ethernet και εξηγήστε ποια είναι η λειτουργία των ψηφίων M-bit (I/G) και X-bit (U/L).
19. Για τη διεύθυνση MAC 88-c9-d0-12-34-56 βρείτε τις τιμές των M-bit (I/G) και X-bit (U/L). Ακολούθως αναζητήστε στο Διαδίκτυο τον κατασκευαστή του υλικού αυτού με βάση το OUI.
20. Μεταγράψτε τη διεύθυνση 00-d0-63-56-78-90 έτσι ώστε να είναι ενεργοποιημένο (1) το M-bit (I/G).
21. Πόσα VLAN υποστηρίζει το πεδίο VLAN Identifier στην ετικέτα Q-tag ενός πλαισίου Ethernet;
22. Ποιο είναι το μέγιστο μήκος της μονάδας εκπομπής (MTU) και ποιο το μέγιστο μέγεθος πλαισίου που αναγνωρίζει το πρότυπο του Ethernet (IEEE802.3);

23. Ποιος είναι ο ρόλος του πεδίου της ακολουθίας ελέγχου πλαισίου FCS (Frame Check Sequence);
24. Τί είναι το Jumbo frame και σε ποιες εφαρμογές η χρήση του έχει πλεονεκτήματα;
25. Σε ποιες εφαρμογές η χρήση Jumbo frame παρουσιάζει μειονέκτημα. Αιτιολογήστε το.
26. Βάλτε με σειρά προτεραιότητας τους παρακάτω τρόπους λειτουργίας κατά την αυτόματη διαπραγμάτευση.

Σειρά προτεραιότητας	**Τρόπος λειτουργίας**
1	100BASE-TX
2	Full-duplex 10BASE-T
3	1000BASE-T
4	Full-duplex 100BASE-TX
5	Full-duplex1000BASE-T
6	100BASE-T2
7	100BASE-T4

27. Τι αντιπροσωπεύουν οι όροι MDI, MDI-X και τι είναι η λειτουργία “Auto MDI/MDI-X” που αναφέρει ότι υποστηρίζει ένας προσαρμογέας δικτύου Ethernet;
28. Ποια είναι τα βασικά στοιχεία από τα οποία αποτελείται ένα κυψελοειδές ασύρματο δίκτυο;
29. Τι είναι ένα ασύρματο σημείο πρόσβασης (Access Point, AP);
30. Ποια είναι τα πλεονεκτήματα και ποια τα μειονεκτήματα ενός ad-hoc ασύρματου δικτύου;
31. Περιγράψτε τα βασικά στοιχεία από τα οποία αποτελείτε ένα ασύρματο δίκτυο με κυψέλες και το βασικό τρόπο λειτουργίας του.
32. Ποια επίπεδα του μοντέλου OSI περιγράφονται στην ομάδα προτύπων του IEEE802.11;
33. Τι είναι ένα Ασύρματο Σημείο Πρόσβασης (Access Point, AP);
34. Ποια τα πλεονεκτήματα και ποια τα μειονεκτήματα της ασύρματης τοπολογίας δικτύου ad hoc;
35. Ποια τα πλεονεκτήματα και ποια τα μειονεκτήματα της ασύρματης τοπολογίας δικτύου Infrastructure;
36. Ποιο πιστεύετε ότι είναι το βασικότερο πλεονέκτημα της τεχνολογίας ATM, που την κάνει να είναι η κύρια τεχνολογία στο χώρο των δικτύων κορμού (backbone);
37. Στην τεχνολογία ATM τα δεδομένα χωρίζονται σε:
    α. Πλαίσια
    β. Πακέτα των 43 bytes
    γ. Κυψέλες (cells)
38. Στην τεχνολογία ATM, σαν μέσο μετάδοσης, μπορεί να χρησιμοποιηθεί μόνο η οπτική ίνα;
39. Πόσος χρόνος χρειάζεται για να μεταδοθεί το περιεχόμενο ενός γεμάτου CD (640 MB) μέσα από μια σύνδεση ATM των 622 Mbps;
40. Από τι αποτελείται μια κυψελίδα ATM (cell);
41. Τι είναι οι μεταγωγείς ATM;
42. Ποιος είναι ο στόχος του ATM;
43. Δώστε ένα ορισμό για τη λειτουργία του πρωτοκόλλου PPP.
44. Εξηγείστε τι σημαίνει ότι το πρωτόκολλο PPP είναι προσανατολισμένο σε σύνδεση.
45. Αναφέρετε τα βασικά συστατικά μέρη που βασίζεται η λειτουργία του πρωτοκόλλου PPP.
46. Περιγράψτε τη λειτουργία ενθυλάκωσης του PPP

47. Ποια είναι η λειτουργία του πρωτοκόλλου έλεγχου σύνδεσης
48. Ποιος είναι ο λόγος για τη χρησιμοποίηση των πρωτοκόλλων NCP πριν την εγκατάσταση μιας σύνδεσης
49. Περιγράψτε τις τρεις φάσεις βάση των οποίων γίνεται η μετάδοση πληροφοριών στο επίπεδο ζεύξης δεδομένων μεταξύ δύο συσκευών με το πρωτόκολλο PPP
50. Γιατί είναι σημαντικό πλεονέκτημα η επεκτασιμότητα του πρωτοκόλλου PPP.

Ασκήσεις σε Εργαστηριακό Περιβάλλον

1. Στον υπολογιστή του εργαστηρίου που συνήθως εργάζεστε, εντοπίστε και καταγράψτε τη φυσική διεύθυνσή του (MAC). Στη συνέχεια με βάση το OUI αναζητήστε να βρείτε τον κατασκευαστή του υλικού της κάρτας δικτύου. *(Υπόδειξη: χρησιμοποιήστε τις εντολές ipconfig /all ή ifconfig κατά περίπτωση)*
2. Χρησιμοποιώντας τον απαραίτητο εξοπλισμό εργαλείων και τα απαραίτητα υλικά κατασκευάστε ένα καλώδιο δικτύου Ethernet UTP, μήκους 1,8μ., για σύνδεση υπολογιστή σε μεταγωγέα σύμφωνα με την τυποποίηση T568A.
3. Χρησιμοποιώντας τον απαραίτητο εξοπλισμό εργαλείων και τα απαραίτητα υλικά κατασκευάστε ένα καλώδιο δικτύου Ethernet UTP, μήκους 1,8μ., για σύνδεση υπολογιστή με υπολογιστή το οποίο να υποστηρίζει Gigabit Ethernet χωρίς τη χρήση της δυνατότητας “Auto MDI/MDI-X”
4. Εργαζόμενοι σε ομάδες, “στήστε” ένα μικρό δίκτυο Ethernet αποτελούμενο από μεταγωγέα, και τέσσερις τουλάχιστον σταθμούς. Καταγράψτε όλα τα υλικά που θα χρειαστείτε.

Βιβλιογραφία

Αλεξόπουλος, Α., & Λαγογιάννης, Γ. (2012). *Τηλεπικοινωνίες και δίκτυα υπολογιστών,* (8η έκδ.). Αθήνα.

Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). *Τεχνολογία Δικτύων Επικοινωνιών* (1η έκδ.). Αθήνα: ΟΕΔΒ.

Anixter. (χ.χ.) *European Standards Reference Guide.*

Anttalainen T. (2003), *Introduction to TelecommunicationsNetwork Engineering*, (Second Edition). ARTECH HOUSE, INC.685 Canton Street Norwood, MA 02062.

Broadband. (2015, August 18). In Wikipedia, the free encyclopedia. Retrieved from https://en.wikipedia.org/w/index.php?title=Broadband&oldid=676733079

CENELEC. (2011). *EN 50173-1:2011 Information technology. Generic cabling systems. General requirements*

Cisco Systems, Inc. (2014), *Network Basics Companion Guide*, Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA

CONTA (COmputer Networks & Telematics Applications Lab) - Πανεπιστήμιο Μακεδονίας (http://conta.uom.gr/conta/ekpaideysh/seminaria/thlematikes/atm/Intro.htm)

Ethernet alliance. (2009). *Ethernet Jumbo Frames*. Beaverton, OR 97006

EXFO. (2005). *Ethernet Reference Guide: Your Everyday Ethernet Testing Reference Tool*, 1st edition. Canada: EXFO Electro-Optical Engineering Inc.

Fluke Networks. (2004). *VLAN Best Practices*. Everett, WA USA

IEEE. (2012). *Standard for Ethernet IEEE Std 802.3TM-2012 (Revision of IEEE Std 802.3-2008) (SECTION ONE)*. New York USA

Nexans. (2014). *General Installation Guide*.

ISO/IEC. (2002-9). *ISO/IEC 11801, Information technology – Generic cabling for customer premises*, 2nd ed. Geneva, Switzerland: IEC.

Sandeep D., Renu R., (2014), *Routing base congestion control metrics in manets*, Advances in Science and Technology, Research Journal Volume 8, No. 23.

Spurgeon, C. E., & Zimmerman, J. (2012). *Ethernet The Definitive Guide* (2nd ed.). Sebastopol, CA USA: O'Reilly Media.

TIA. (2009). *TIA-568-C.0, Generic Telecommunications Cabling for Customer Premises*. Arlington USA: TIA

TIA. (2009). *TIA-568-C.2, Balanced Twisted-Pair Telecommunications Cabling and Components Standard*. Arlington USA: TIA.

TIA. (2008). *TIA-568-C.3, Optical Fiber Cabling Components Standard*. Arlington USA: TIA.

Κεφάλαιο 3ο
ΕΠΙΠΕΔΟ ΔΙΚΤΥΟΥ–ΔΙΑΔΙΚΤΥΩΣΗ

Εισαγωγή

Το επίπεδο δικτύου και το αντίστοιχο Διαδικτύου του μοντέλου TCP/IP αποτελεί τον συνδετικό κρίκο ο οποίος επιτρέπει στα τοπικά δίκτυα που χρησιμοποιούν διαφορετικές τεχνολογίες δικτύωσης να ενωθούν σε μεγαλύτερα δίκτυα - διαδίκτυα, με αποκορύφωμα το γνωστό μας Internet. Σε αυτό συμβάλλουν η διευθυνσιοδότηση και η δρομολόγηση, δυο βασικές λειτουργίες του συγκεκριμένου επιπέδου γύρω από τις οποίες περιστρέφονται οι δομές και τα πρωτόκολλα που το αφορούν.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 3ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- αναγνωρίζουν το επίπεδο δικτύου ως το κατώτερο επίπεδο του διαστρωματωμένου μοντέλου δικτύωσης που καθιστά εφικτή τη διασύνδεση δικτύων
- κατανοούν ότι το πακέτο του επιπέδου δικτύου (IP) παραμένει σχεδόν αυτούσιο στη διαδρομή που διανύει από τον Η/Υ-αποστολέα ως τον Η/Υ-παραλήπτη, με μεταβολές μόνο ορισμένων πεδίων του, σε αντίθεση με τα ηλεκτρικά σήματα και τα πλαίσια Ethernet τα οποία “επιβιώνουν” μέχρι τα όρια του τοπικού δικτύου
- περιγράφουν τη δομή μια διεύθυνσης IP και το σχήμα διευθυνσιοδότησης του IPv4.
- αναγνωρίζουν πότε μια διεύθυνση IP είναι σωστή, να την κατατάσσουν στην κλάση που ανήκει, να εντοπίζουν τη διεύθυνση δικτύου στο οποίο ανήκει και τη διεύθυνση εκπομπής
- ορίζουν την έννοια της μάσκας δικτύου, τις αταξικές διευθύνσεις (CIDR) και να προσδιορίζουν δεδομένης της μάσκας ποιες άλλες IP ανήκουν στο ίδιο δίκτυο με μια συγκεκριμένη ή δοσμένη IP
- υποδικτυώνουν ένα δίκτυο υπολογίζοντας τη νέα μάσκα για τον αριθμό των ζητούμενων υποδικτύων
- περιγράφουν τη δομή του πακέτου IP (datagram) και τη λειτουργία των διαφόρων πεδίων της επικεφαλίδας του (ttl, DF, MF, offset κτλ.)
- αντιστοιχίζουν διευθύνσεις MAC με τις ανάλογες IP
- περιγράφουν το ρόλο των πρωτοκόλλων ARP και RARP
- περιγράφουν τη διαδικασία ενθυλάκωσης πακέτων IP εντός πλαισίων Ethernet
- εντοπίζουν και να τροποποιούν τις ρυθμίσεις δικτύου σε έναν υπολογιστή με Λειτουργικό Σύστημα Windows ή Unix
- εντοπίζουν και να τροποποιούν τον πίνακα ARP
- περιγράφουν την έννοια της δρομολόγησης και να εντοπίζουν και να ρυθμίζουν τον πίνακα δρομολόγησης
- ελέγχουν το βαθμό λειτουργικότητας των τριών πρώτων επιπέδων (OSI) σε έναν Η/Υ.

Διδακτικές Ενότητες

3.1 Διευθυνσιοδότηση Internet Protocol έκδοση 4 (IPv4).
3.2 Το αυτοδύναμο πακέτο IP (datagram) – Δομή πακέτου.
3.3 Πρωτόκολλα ανεύρεσης και απόδοσης διευθύνσεων, Address Resolution Protocol (ARP) και Dynamic Host Configuration Protocol (DHCP).
3.4 Διευθύνσεις IP και Ονοματολογία.

3.5 Διευθυνσιοδότηση IPv6.
3.6 Δρομολόγηση.
3.7 Πρωτόκολλα - Αλγόριθμοι δρομολόγησης.

3.1 Διευθυνσιοδότηση Internet Protocol έκδοση 4 (IPv4)

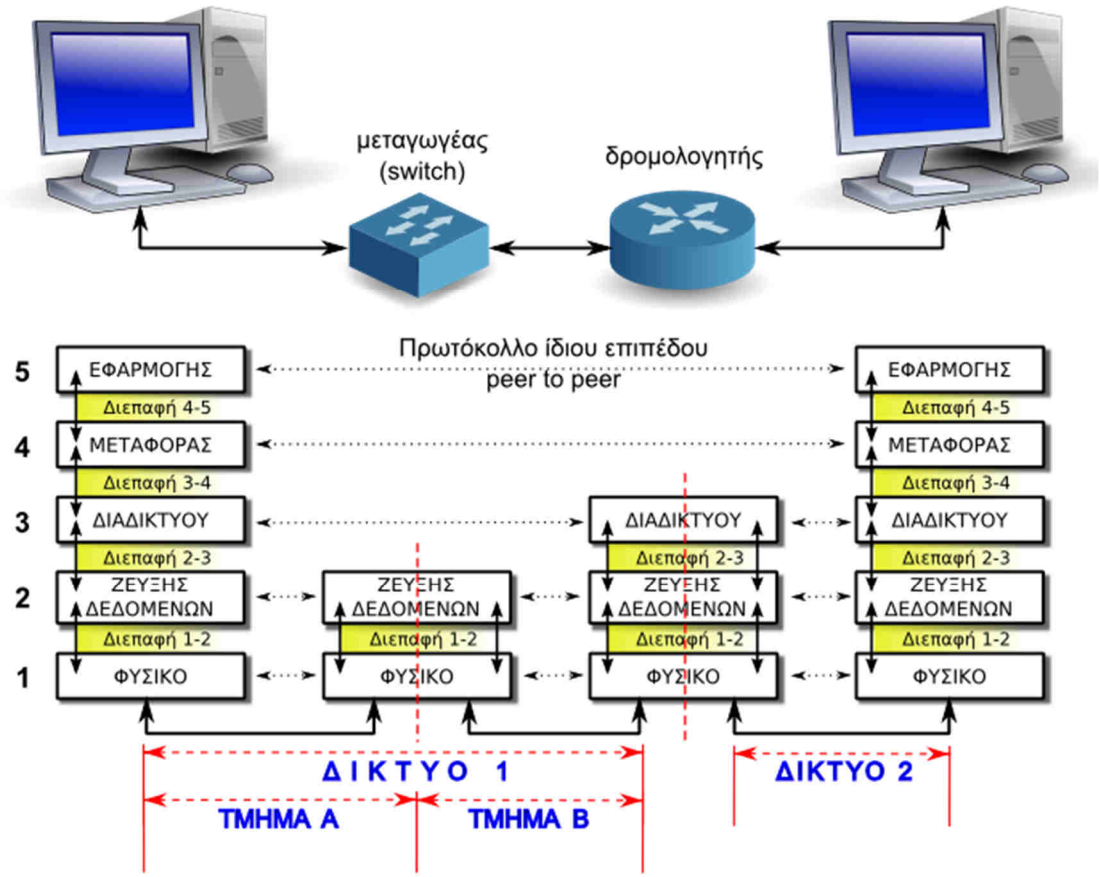
Το επίπεδο Δικτύου (Network layer) στο μοντέλο OSI ή το αντίστοιχο Διαδικτύου του TCP/IP παρέχει τη **λογική διευθυνσιοδότηση** για όλα τα διασυνδεδεμένα μεταξύ τους δίκτυα. Φροντίζει για την εύρεση της κατάλληλης διαδρομής και παράδοση του πακέτου δεδομένων στον τελικό κόμβο, έργο το οποίο χαρακτηρίζεται ως **δρομολόγηση** (routing). Στην προσπάθεια αυτή το πακέτο μπορεί να χρειαστεί να διασπαστεί σε διάφορα τμήματα τα οποία μπορεί να φτάσουν από άλλες διαδρομές και με διαφορετική σειρά, όμως το επίπεδο δικτύου θα τα επανασυνθέσει και θα αναφέρει οποιαδήποτε προβλήματα παράδοσης προκύψουν. Το επίπεδο Διαδικτύου στο μοντέλο **TCP/IP** έχει ως βασικό πρωτόκολλο το **πρωτόκολλο Διαδικτύου** (Internet Protocol - **IP**) το οποίο παρέχει υπηρεσίες αποκλειστικά χωρίς σύνδεση. Για το σκοπό αυτό χρησιμοποιεί **αυτοδύναμα πακέτα IP** τα οποία ονομάζονται **datagram** (= data + telegram).

Στο επίπεδο Διαδικτύου, εκτός από το βασικό πρωτόκολλο Διαδικτύου IP, λειτουργεί το **πρωτόκολλο μηνυμάτων ελέγχου Διαδικτύου** (Internet Control Message Protocol - **ICMP**) και το **πρωτόκολλο διαχείρισης ομάδων Διαδικτύου** (Internet Group Management Protocol - **IGMP**). Τα πρωτόκολλα ICMP και IGMP συνήθως δε χρησιμοποιούνται από τους χρήστες και τις εφαρμογές τους αλλά από δικτυακές συσκευές και λογισμικό συστημάτων. Το ICMP χρησιμοποιείται κυρίως για την αναφορά σφαλμάτων μετάδοση ερωτημάτων και αναμετάδοση (relaying) διαγνωστικών μηνυμάτων. Εξαίρεση αποτελούν οι εντολές ping και traceroute. Το IGMP χρησιμοποιείται για την ομαδοποίηση υπολογιστών και αποστολή μηνυμάτων ταυτόχρονα σε όλους τους υπολογιστές της ομάδας (streaming). Σε έναν υπολογιστή με TCP/IP η υλοποίηση και υποστήριξη του ICMP είναι υποχρεωτική ενώ του IGMP προαιρετική.

Το πακέτο IP είναι αυτό το οποίο φτάνει σχεδόν αυτούσιο από τον υπολογιστή του αποστολέα στον υπολογιστή του παραλήπτη. Οι ενδιάμεσοι κόμβοι μόνο μικρές επεμβάσεις κάνουν σε ορισμένα πεδία της επικεφαλίδας του για διαχειριστικούς λόγους. Σε όλα τα ενδιάμεσα δίκτυα ενθυλακώνεται/αποθυλακώνεται σε διάφορα πλαίσια 2ου επιπέδου τα οποία όμως ισχύουν μόνο στα όρια των ενδιάμεσων φυσικών τοπικών δικτύων κάθε φορά.

Στο Δίκτυο 1, το πακέτο IP διακινείται ενθυλακωμένο στο ίδιο πλαίσιο ακόμη κι αν κινηθεί σε διαφορετικά τμήματα (segments) του ίδιου δικτύου. Στον δρομολογητή, αποθυλακώνεται από το πλαίσιο του Δικτύου 1, ελέγχεται η διεύθυνση προορισμού και προωθείται στο Δίκτυο 2 ενθυλακώνοντάς το σε ένα νέο πλαίσιο του Δικτύου 2. Το πακέτο IP μέχρι τον υπολογιστή προορισμού παρέμεινε το ίδιο ενώ στη διαδρομή ενθυλακώθηκε σε διαφορετικά πλαίσια.

Όλη η ενδιάμεση υποδομή από γραμμές μετάδοσης (αποκαλούνται και ζεύξεις, κυκλώματα ή κανάλια) και συσκευές μεταγωγής-δρομολογητές χαρακτηρίζεται **επικοινωνιακό υποδίκτυο** και επιτρέπει σε δυο ακραίους υπολογιστές να επικοινωνήσουν μεταξύ τους. Στα δίκτυα τεχνολογίας TCP/IP, το επικοινωνιακό υποδίκτυο έχει λειτουργικότητα μέχρι και το επίπεδο διαδικτύου (3ο επίπεδο OSI). Δύο ή περισσότερα ανεξάρτητα δίκτυα διασυνδεδεμένα μεταξύ τους ώστε να λειτουργούν ως ένα μεγάλο δίκτυο συνθέτουν ένα **Διαδίκτυο** (internet - με το **i** μικρό/πεζό).



Εικόνα 3.1.α: Δίκτυα και Διαδίκτυο

Σε ένα δίκτυο υπολογιστών, για να μπορέσει η πληροφορία να φτάσει στον υπολογιστή προορισμού με τη μορφή πακέτων δεδομένων, θα πρέπει **οι υπολογιστές να προσδιορίζονται με μοναδικό τρόπο** με κάποιο σχήμα διευθυνσιοδότησης, όπως οι κατοικίες σε μια πόλη εντοπίζονται από τον αριθμό, την οδό και τον ταχυδρομικό κώδικα.

Στη συνέχεια αναφερόμαστε στο μοντέλο και στην οικογένεια ή στοίβα πρωτοκόλλων του TCP/IP.

3.1.1 Διευθύνσεις IPv4

Το πρωτόκολλο IP ορίζει ότι οι υπολογιστές που συμμετέχουν σε ένα δίκτυο, χρησιμοποιώντας το συγκεκριμένο πρωτόκολλο (την έκδοση 4 - IPv4), αναγνωρίζονται με μοναδικό τρόπο από έναν 32μπιτο δυαδικό αριθμό, την διεύθυνση IP (IP Address).

Ένας τέτοιος αριθμός είναι π.χ. ο `11000000 10101000 00000001 00010010`

Στην πραγματικότητα **ένας υπολογιστής μπορεί να έχει περισσότερες διευθύνσεις**, μια διαφορετική για κάθε διαφορετικό δίκτυο στο οποίο είναι συνδεδεμένος. Όπως μια γωνιακή οικία η οποία έχει πρόσοψη σε δυο δρόμους που διασταυρώνονται, μπορεί να προσδιοριστεί με διαφορετικές διευθύνσεις ανάλογα με το δρόμο από τον οποίο προσεγγίζεται.

Διεύθυνση IP έχει κάθε δικτυακή διεπαφή (Network Interface) ενός υπολογιστή. Έτσι ένας υπολογιστής με δυο κάρτες δικτύου Ethernet (δικτυακές διασυνδέσεις) μπορεί να έχει δυο διευθύνσεις.

Διεύθυνση που προσδιορίζει **μια** δικτυακή διασύνδεση (έναν υπολογιστή) χαρακτηρίζεται "**αποκλειστικής διανομής**" (unicast)

Τρόπος γραφής μια διεύθυνσης IPv4

Επειδή ένας αριθμός, σε μορφή όπως δίνεται στην προηγούμενη παράγραφο, είναι δυσκολομνημόνευτος έχει επικρατήσει να αναγράφεται ως εξής:

Τα ψηφία του,

- ομαδοποιούνται σε **τέσσερα τμήματα** του ενός byte και
- αναγράφονται τα αντίστοιχα **δεκαδικά** τους ισοδύναμα,
- **διαχωριζόμενα** από τα διπλανά τους **με τελείες**.

Έτσι ο προηγούμενος αριθμός **11000000 10101000 00000001 00010010** γράφεται ως **192.168.1.18** Ο συγκεκριμένος τρόπος γραφής αναφέρεται ως **δεκαδική σημειογραφία με τελείες** (*four-part dotted decimal notation)*

Σύμφωνα με αυτόν τον τρόπο γραφής **μια διεύθυνση IP για να είναι σωστή θα πρέπει:**

- να αποτελείται από **τέσσερις δεκαδικούς αριθμούς διαχωρισμένους με τελείες**
- κάθε αριθμός να είναι μεταξύ του μηδενός **0** και του **255** (αφού αυτές είναι οι τιμές που μπορεί να πάρει ένας οκταψήφιος δυαδικός αριθμός – byte, από 0 έως 2^8-1)

Παραδείγματα διευθύνσεων IP:

Α/Α	ΔΙΕΥΘΥΝΣΗ	ΣΩΣΤΗ / ΛΑΘΟΣ	ΓΙΑΤΙ;
1	**192.168.1.12**	ΣΩΣΤΗ	
2	**10.0.0.12.3**	ΛΑΘΟΣ	Έχει περισσότερα από τέσσερα τμήματα
3	**172.16.257.3**	ΛΑΘΟΣ	Ένα τμήμα (257) είναι έξω από τα όρια 0 έως 255
4	**10.146.0.1**	ΣΩΣΤΗ	
5	**194.219.227.3**	?	
6	**127.270.0.1**	?	

Μετατροπή δυαδικού αριθμού σε δεκαδικό (8 bit)

Η αξία του ψηφίου είναι ίση με τη βάση του συστήματος αρίθμησης (2 για το δυαδικό) υψωμένη σε δύναμη με εκθέτη τη θέση του ψηφίου (η αρίθμηση ξεκινά από τα δεξιά και την τιμή 0, προς τα αριστερά). Έτσι για το 5ο ψηφίο ***b_5****, η αξία είναι* ***$2^5 = 32$****.*

Αξία ψηφίου :	128	64	32	16	8	4	2	1
Ψηφίο :	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**
Θέση ψηφίου :	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0

Αθροίζοντας τις αξίες των άσσων, έχουμε 128+32+8 = 168.

Δηλαδή **$(10101000)_2 = (168)_{10}$**

Άλλα παραδείγματα:

$(1100\ 0000)_2$ = 128+64 = **$(192)_{10}$**

$(1001\ 0010)_2$ = 128+16+2 = **$(146)_{10}$**

Πίνακας 3.1.1.α: Μετατροπή δυαδικού αριθμού σε δεκαδικό (8bit)

Μετατροπή δεκαδικού αριθμού σε δυαδικό (8 bit)

Έστω ο αριθμός $(\mathbf{207})_{10}$

8. Ελέγχω εάν από το 207 αφαιρείται η μεγαλύτερη αξία ψηφίου που είναι το **128**
   a. **Εφόσον αφαιρείται, εκτελώ την αφαίρεση** 207-128 =77 **και σημειώνω 1** στη θέση $\mathbf{b_7}$
9. Ελέγχω εάν από το 77 αφαιρείται η επόμενη μεγαλύτερη αξία ψηφίου που είναι το **64**
   a. Εφόσον αφαιρείται, εκτελώ την αφαίρεση 77-64 =13 και σημειώνω **1** στη θέση $\mathbf{b_6}$
10. Ελέγχω εάν από το 13 αφαιρείται η επόμενη μεγαλύτερη αξία ψηφίου που είναι το **32**
    a. **Εφόσον δεν αφαιρείται, σημειώνω 0** στη θέση $\mathbf{b_5}$
11. Ελέγχω εάν από το 13 αφαιρείται η επόμενη μεγαλύτερη αξία ψηφίου που είναι το **16**
    a. Εφόσον δεν αφαιρείται, σημειώνω **0** στη θέση $\mathbf{b_4}$
12. Ελέγχω εάν από το 13 αφαιρείται η επόμενη μεγαλύτερη αξία ψηφίου που είναι το **8**
    a. Εφόσον αφαιρείται, εκτελώ την αφαίρεση 13-8 =5 και σημειώνω **1** στη θέση $\mathbf{b_3}$
13. Ελέγχω εάν από το 5 αφαιρείται η επόμενη μεγαλύτερη αξία ψηφίου που είναι το **4**
    a. Εφόσον αφαιρείται, εκτελώ την αφαίρεση 5-4 =1 και σημειώνω **1** στη θέση $\mathbf{b_2}$
14. Ελέγχω εάν από το 1 αφαιρείται η επόμενη μεγαλύτερη αξία ψηφίου που είναι το **2**
    a. Εφόσον δεν αφαιρείται, σημειώνω **0** στη θέση $\mathbf{b_1}$
15. Ελέγχω εάν από το 1 αφαιρείται η επόμενη μεγαλύτερη αξία ψηφίου που είναι το **1**
    a. Εφόσον αφαιρείται, εκτελώ την αφαίρεση 1-1 =0 και σημειώνω **1** στη θέση $\mathbf{b_0}$

Αξία ψηφίου :	128	64	32	16	8	4	2	1
Ψηφίο :	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**1**
Θέση ψηφίου :	$\mathbf{b_7}$	$\mathbf{b_6}$	$\mathbf{b_5}$	$\mathbf{b_4}$	$\mathbf{b_3}$	$\mathbf{b_2}$	$\mathbf{b_1}$	$\mathbf{b_0}$

Δηλαδή $(\mathbf{207})_{10}$ = 128+64+8+4+1 = $(\mathbf{11001101})_2$

Πίνακας 3.1.1.β: Μετατροπή δεκαδικού αριθμού σε δυαδικό (8 bit)

Χρήσιμες υποδείξεις για τις μετατροπές BIN ↔ DEC (8bit)

Όταν έχουμε **από δεξιά προς τα αριστερά συνεχόμενους άσους**, ο αριθμός ισούται με την αξία του επόμενου προς τα αριστερά (του τελευταίου άσου) ψηφίου μείον ένα.

Αξία ψηφίου :	128	64	32	16	8	4	2	1
Ψηφίο :	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**1**
Θέση ψηφίου :	$\mathbf{b_7}$	$\mathbf{b_6}$	$\mathbf{b_5}$	$\mathbf{b_4}$	$\mathbf{b_3}$	$\mathbf{b_2}$	$\mathbf{b_1}$	$\mathbf{b_0}$

Δηλαδή $(\mathbf{00011111})_2$ = 32-1 = $(\mathbf{31})_{10}$ κι όπως επιβεβαιώνεται $(\mathbf{00011111})_2$ = 16+8+4+2+1 = $(\mathbf{31})_{10}$

5. Όταν έχουμε **περισσότερους άσους από μηδενικά** συμφέρει να αθροίσουμε τις αξίες των θέσεων των μηδενικών (των άσων που λείπουν) και να την αφαιρέσουμε από το 255 (την αξία του αριθμού όταν έχει και τα οκτώ ψηφία άσους)

Αξία ψηφίου :	128	64	32	16	8	4	2	1
Ψηφίο :	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**
Θέση ψηφίου :	$\mathbf{b_7}$	$\mathbf{b_6}$	$\mathbf{b_5}$	$\mathbf{b_4}$	$\mathbf{b_3}$	$\mathbf{b_2}$	$\mathbf{b_1}$	$\mathbf{b_0}$

Δηλαδή $(\mathbf{11010111})_2$ = 255-(32+8) = 255-40 = $(\mathbf{215})_{10}$ κι όπως επιβεβαιώνεται $(\mathbf{11010111})_2$ = 128+64+16+4+2+1 = $(\mathbf{215})_{10}$

Πίνακας 3.1.1.γ: Χρήσιμες υποδείξεις για τις μετατροπές BIN ↔ DEC (8bit)

3.1.2 Κλάσεις (τάξεις) δικτύων - διευθύνσεων

Κάθε διεύθυνση IP αποτελείται από δυο τμήματα. Το πρώτο τμήμα είναι αναγνωριστικό του δικτύου (Network ID) ή πρόθεμα (prefix) στο οποίο ανήκει ο υπολογιστής και το δεύτερο το αναγνωριστικό του υπολογιστή (Host ID) ή επίθεμα (suffix) μέσα στο συγκεκριμένο δίκτυο. Το αναγνωριστικό του δικτύου είναι σαν την οδό στην οποία βρίσκεται μια οικία ενώ το αναγνωριστικό του υπολογιστή σαν τον αριθμό επί της οδού που βρίσκεται η οικία.

Για παράδειγμα στη διεύθυνση 192.168.1.12, οι τρεις πρώτοι αριθμοί 192.168.1 προσδιορίζουν το δίκτυο 192.168.1.0 και ο τελευταίος (12) τον υπολογιστή Νο 12 του συγκεκριμένου δικτύου.

192.	**168.**	**1.**	**12**
n	***n***	***n***	***H***

Δίκτυο *(**n**etwork)*	***Υπολογιστής*** *(**H**ost)*

Τα δυο αυτά τμήματα διαφοροποιούνται ανάλογα με το μέγεθος του δικτύου. Το συγκεκριμένο δίκτυο, εφόσον το αναγνωριστικό του υπολογιστή έχει εύρος 8bit, μπορεί να έχει μέχρι $\mathbf{2^8}$ = **256** υπολογιστές (0-255, κι αν εξαιρέσουμε τις τιμές 0 και 255 οι οποίες έχουν ειδική σημασία - *η τιμή 0 προσδιορίζει τη διεύθυνση του δικτύου και η τιμή 255 τη διεύθυνση εκπομπής* - , απομένουν μόνο οι τιμές 1 έως 254, δηλ. 254 υπολογιστές).

Εάν θέλουμε το δίκτυο να έχει περισσότερους από 254 υπολογιστές θα πρέπει να διατεθεί ακόμα μια οκτάδα (byte) για το αναγνωριστικό του υπολογιστή. Τότε το δίκτυο θα μπορεί να έχει μέχρι $\mathbf{2^{16}}$ = **65536** υπολογιστές *(στην πραγματικότητα 65536-2 = 65534, η πρώτη και η τελευταία τιμή, όπως και στην προηγούμενη περίπτωση, έχουν ειδική σημασία η οποία θα αναλυθεί παρακάτω).* Για ακόμα μεγαλύτερα δίκτυα (περισσότερους από 65534 υπολογιστές) θα πρέπει να διατεθεί ακόμα μια οκτάδα, συνολικά 24 bit για το αναγνωριστικό του υπολογιστή. Ας σημειωθεί ότι ανάλογα μειώνεται το μήκος του αναγνωριστικού του δικτύου ώστε συνολικά μαζί με το αναγνωριστικό του υπολογιστή να είναι 32 bit.

Με τον τρόπο αυτό ορίζονται οι κλάσεις-τάξεις των δικτύων ώστε να υπάρχουν δίκτυα διαφόρων μεγεθών ανάλογα με τις ανάγκες που εξυπηρετούν. Δείτε το ανάλογο μεγάλων οδών ή λεωφόρων που έχουν πολλά κτήρια-οικίες και μικρότερων οδών με λιγότερα κτήρια-οικίες.

Έτσι ορίζονται τρεις τάξεις δικτύων ανάλογα με το μέγεθός τους οι οποίες συνοψίζονται στον παρακάτω πίνακα 3.1.2.α:

ΤΑΞΗ	**ΔΙΕΥΘΥΝΣΗ IP – 4 οκτάδες**				**Δίκτυα**	**Υπολ/στές**
A	**0** **n** *(7bit)*	**H**	**H**	**H**	2^7 = **128**	2^{24}-2 = **16 777 214**
	Δίκτυο	Υπολογιστής				
B	**1 0** **n** *(6bit)*	**n**	**H**	**H**	2^{14} = **16 384**	2^{16}-2 = **65 534**
	Δίκτυο		Υπολογιστής			

C	**11 0**	**n** *(5bit)*	**n**	**n**	**H**	2^{21} = **2 097 152**	2^8-2 = **254**
	Δίκτυο				Υπολογιστής	

Πίνακας 3.1.2.α: Κλάσεις/τάξεις διευθύνσεων IPv4

Προσδιορισμός τάξης (κλάσης) δικτύου με δοσμένη διεύθυνση IP. Βλέποντας μια διεύθυνση IP, η τάξη του δικτύου στο οποίο ανήκει, **προκαθορίζεται από την πρώτη οκτάδα (byte)** της και ειδικότερα από τη δυαδική της μορφή (2η στήλη του προηγούμενου Πίνακα), ως εξής:

ΤΑΞΗ	1η οκτάδα	Δυαδικό		Δεκαδικό		Παρατηρήσεις
		Από	έως	Από	έως	
A	**0xxx xxxx**	**0000 0000**	**0111 1111**	**0**	**127**	**x** : 0 ή 1
B	**10xx xxxx**	**1000 0000**	**1011 1111**	**128**	**191**	
C	**110x xxxx**	**1100 0000**	**1101 1111**	**192**	**223**	
D	**1110 xxxx**	**1110 0000**	**1110 1111**	**224**	**239**	Multicast (Πολυδιανομή)
E	**1111 0xxx**	**1111 0000**	**1111 0111**	**240**	**247**	Δεσμευμένες

Πίνακας 3.1.2.β: Προσδιορισμός κλάσης/τάξης διευθύνσεων

Από τις παραπάνω τάξεις, **μόνο οι A, B και C χρησιμοποιούνται για την απόδοση διευθύνσεων σε υπολογιστές δικτύων για κανονική χρήση**. Οι D και E έχουν ειδικές χρήσεις.

Παραδείγματα διευθύνσεων IP και αντιστοίχων τάξεων δικτύων στα οποία ανήκουν:

Διεύθυνση IP	Τάξη	Γιατί;
192.168.1.12	C	το 192 ανήκει στο διάστημα 192 .. 223
10.146.0.1	A	το 10 ανήκει στο διάστημα 0 .. 127
172.16.32.253	B	το 172 ανήκει στο διάστημα 128 .. 191
127.0.0.1	A	το 127 ανήκει στο διάστημα 0 .. 127
194.219.227.1	C	το 194 ανήκει στο διάστημα 192 .. 223

Σημείωση: Το κριτήριο για τον προσδιορισμό της τάξης δικτύου στην οποία ανήκει μια διεύθυνση IP είναι η μορφή της πρώτης οκτάδας της διεύθυνσης στο δυαδικό της ισοδύναμο. Για λόγους ευκολίας χρησιμοποιούμε το δεκαδικό ισοδύναμο, 1-127, 128-191,192-223, 224-239, 240-247

Προσπαθήστε να εξηγήσετε γιατί ο αριθμός των πιθανών δικτύων και υπολογιστών για κάθε τάξη είναι αυτός που φαίνεται στον αντίστοιχο πίνακα. *(υπόδειξη: λάβετε υπόψη τον αριθμό των διαθέσιμων bit)*

Διαχείριση και απόδοση διευθύνσεων IP

Οι διευθύνσεις IP είναι μοναδικές στον κόσμο και διαχειρίζονται από κεντρικό φορέα διαχείρισης, (IANA/ICANN) ο οποίος μεταβιβάζει αρμοδιότητες διαχείρισης σε περιφερειακούς καταχωρητές (RIR – Regional Internet Registry) και μέσω αυτών σε τοπικούς (LIR – Local Internet Registry) ή εθνικούς καταχωρητές (NIR – National Internet Registry). Για την Ευρώπη, Μέση Ανατολή και Κεντρική Ασία περιφερειακός καταχωρητής Internet είναι το RIPE NCC (Réseaux IP Européens Network Coordination Center).

Οι τελικοί απλοί ή και εταιρικοί χρήστες απευθύνονται στον πάροχο υπηρεσιών Διαδικτύου (Internet Service Provider, ISP) ο οποίος τους παρέχει πρόσβαση στο Διαδίκτυο μαζί με τις απαιτούμενες διευθύνσεις IP, διαφορετικές κάθε φορά (δυναμικές) ή τις ίδιες πάντα (στατικές) και κατά κανόνα είναι και τοπικός καταχωρητής.

Ιδιωτικές διευθύνσεις IP

Για την υλοποίηση ιδιωτικών δικτύων, οι υπολογιστές των οποίων δεν έχουν άμεση πρόσβαση στο Διαδίκτυο, δεν είναι ανάγκη ο διαχειριστής που υλοποιεί το δίκτυο να ζητήσει επίσημες διευθύνσεις IP από κάποιον πάροχο όπως αναφέρθηκε παραπάνω. Για το σκοπό αυτό έχουν προβλεφθεί περιοχές διευθύνσεων και των τριών τάξεων οι οποίες μπορούν να χρησιμοποιηθούν αυθαίρετα και χωρίς κανένα συντονισμό με κάποια από τις αρχές διαχείρισης διευθύνσεων IP.

Αυτές περιγράφονται στο έγγραφο RFC1918 - Address Allocation for Private Internets και είναι οι εξής:

Τάξη	Από	Έως	*Μορφή CIDR*[1]
A	10.0.0.0	10.255.255.255	10/8
B	172.16.0.0	172.31.255.255	172.16/12
C	192.168.0.0	192.168.255.255	192.168/16

Πίνακας 3.1.2.γ: Ιδιωτικές διευθύνσεις IPv4

Συνεπώς, **για την υλοποίηση ενός ιδιωτικού δικτύου IP, επιλέγονται διευθύνσεις ΜΟΝΟΝ από τον προηγούμενο πίνακα** και ανάλογα με το μέγεθος του δικτύου. Οι διευθύνσεις αυτές ΔΕΝ δρομολογούνται από τους δρομολογητές στο Διαδίκτυο.

RFC (**Request For Comments**) είναι έγγραφα του IETF (Internet Engineering Task Force) που περιγράφουν (συνήθως προτείνουν) μεθόδους, συμπεριφορές, αποτελέσματα έρευνας ή καινοτομίες με εφαρμογή στο Διαδίκτυο και στα διασυνδεδεμένα με αυτό συστήματα. Τα περισσότερα υιοθετούνται ως πρότυπα και τυποποιήσεις του διαδικτύου.

3.1.3 Σπατάλη διευθύνσεων IP

Έστω ότι ένας οργανισμός έχει 55 υπολογιστές και θέλει να τους συνδέσει σε δίκτυο χρησιμοποιώντας το TCP/IP. Για τη διευθυνσιοδότησή τους, του παραχωρείται ένα δίκτυο τάξης C, π.χ. το 194.219.227.0 το οποίο μπορεί να έχει μέχρι και 254 υπολογιστές. Όπως είναι φυσικό, χρησιμοποιώντας την περιοχή από 194.219.227.1 – 194.219.227.55 για τους υπολογιστές του, **οι υπόλοιπες διευθύνσεις παραμένουν δεσμευμένες και ανεκμετάλλευτες**.

1 Για τη μορφή αυτή γίνεται λόγος με την εισαγωγή της έννοιας της Μάσκας (υπο-)δικτύωσης

Έστω ότι ο ίδιος οργανισμός έχει 250 περίπου υπολογιστές και εκμεταλλεύεται όλο το εύρος των διευθύνσεων που του αποδίδεται. Λόγω διεύρυνσης των δραστηριοτήτων του, ο οργανισμός έχει ανάγκη επιπλέον υπολογιστών π.χ. συνολικά 300. Τότε όμως θα πρέπει να του αποδοθεί διεύθυνση δικτύου τάξης Β **με συνέπεια να δεσμευτούν και να παραμείνουν ανεκμετάλλευτες πάνω από 65000 διευθύνσεις.**

Το γεγονός αυτό οδηγεί γρήγορα στην εξάντληση των διαθέσιμων διευθύνσεων IP (ειδικά τάξης Β)

Πέρα από τη **σπατάλη και εξάντληση των διαθέσιμων διευθύνσεων**, ο τρόπος αυτός εμφανίζει και **δυσχέρειες στη δρομολόγηση των πακέτων δεδομένων και τη διαχείριση των πινάκων δρομολόγησης**. Για να ξεπεραστούν τέτοιου είδους προβλήματα, γίνεται συστηματική και εξειδικευμένη χρήση της μάσκας δικτύου. Κάθε διεύθυνση IP συνοδεύεται από την μάσκα δικτύου, καταργώντας τις τάξεις διευθύνσεων και καθιερώνοντας τον αταξικό τρόπο δρομολόγησης (CIDR) [RFC1519, RFC4632].

3.1.4 Μάσκα δικτύου

Η μάσκα δικτύου είναι ένας **δυαδικός αριθμός 32 ψηφίων**, ο οποίος συνοδεύει μια διεύθυνση IP και διευκρινίζει ποιά ψηφία της διεύθυνσης ανήκουν στο αναγνωριστικό του δικτύου (Net ID - prefix) και ποιά στο αναγνωριστικό του υπολογιστή (Host ID - suffix) μέσα στο συγκεκριμένο δίκτυο.

Η μάσκα έχει άσους (1) στις θέσεις που τα αντίστοιχα ψηφία της διεύθυνσης ανήκουν στο αναγνωριστικό του δικτύου και μηδενικά (0) στις θέσεις που τα αντίστοιχα ψηφία της διεύθυνσης ανήκουν στο αναγνωριστικό του υπολογιστή.

(δεκαδική μορφή)	192.	168.	1.	18
Διεύθυνση IP:	**1100 0000**	**1010 1000**	**0000 0001**	**0001 0010**
Μάσκα:	**1111 1111**	**1111 1111**	**1111 1111**	**0000 0000**
(δεκαδική μορφή)	255.	255.	255.	0

Παράδειγμα ζεύγους Διεύθυνσης IP - Μάσκας δικτύου

- Οι άσοι (1) βρίσκονται στο αριστερό μέρος,
- τα μηδενικά (0) στο δεξιό και
- δεν μπορεί να μπλέκονται μεταξύ τους άσοι και μηδενικά. Δηλαδή δε μπορεί ένας άσος να έχει στα αριστερά του μηδενικό ούτε ένα μηδενικό στα δεξιά του έναν άσο[2].

Η πράξη του **Λογικού ΚΑΙ** (*AND*), ψηφίο προς ψηφίο (*bitwise*), μεταξύ της διεύθυνσης IP και της μάσκας δικτύου δίνει τη διεύθυνση του δικτύου στο οποίο ανήκει ο υπολογιστής με τη συγκεκριμένη διεύθυνση IP.

Διεύθυνση IP:	**1100 0000**	**1010 1000**	**0000 0001**	**0001 0010**	**192.168. 1.18**	**Λογικό AND**
Μάσκα:	**1111 1111**	**1111 1111**	**1111 1111**	**0000 0000**	**255.255.255. 0**	
Διεύθυνση Δικτύου:	**1100 0000**	**1010 1000**	**0000 0001**	**0000 0000**	**192.168. 1. 0**	**Αποτέ-λεσμα**

Πίνακας 3.1.4.α: (Διεύθυνση IP) AND (Μάσκα δικτύου) = Διεύθυνση Δικτύου

2 RFC1812 Requirements for IP Version 4 Routers, p22

Προκαθορισμένες μάσκες δικτύων τάξης A, B, C

Με βάση τον ορισμό και την περιγραφή της μάσκας δικτύου, οι προκαθορισμένες μάσκες για τις τρεις τάξεις (κλάσεις) δικτύων με βάση τα τμήματα (Net ID και Host ID) του Πίνακα 3.1.2.β, είναι αυτές που συνοψίζονται στον Πίνακα 3.1.4.β.

ΤΑΞΗ	1η οκτάδα	Δεκαδικό		Μάσκα		Παρατηρήσεις
		Από	έως	δεκαδική με τελείες	μορφή CIDR	
A	**0xxx xxxx**	**0**	**127**	**255.0.0.0**	**/8**	**x :** 0 ή 1
B	**10xx xxxx**	**128**	**191**	**255.255.0.0**	**/16**	
C	**110x xxxx**	**192**	**223**	**255.255.255.0**	**/24**	

Πίνακας 3.1.4.β: Προκαθορισμένες μάσκες δικτύων τάξεων A, B, C

Εναλλακτικός τρόπος γραφής μιας μάσκας είναι η μορφή CIDR. Μετά τη διεύθυνση IP ακολουθεί πλάγια κάθετος και ένας αριθμός ο οποίος δηλώνει τους άσους της μάσκας ή αλλιώς τα ψηφία της διεύθυνσης που προσδιορίζουν το αναγνωριστικό δικτύου (prefix), π.χ. **192.168.1.12 / 24**

3.1.5 Ειδικές διευθύνσεις

Διεύθυνση Δικτύου: Προσδιορίζει το δίκτυο στο οποίο ανήκει μια διεύθυνση. Για μια δεδομένη διεύθυνση IP, η διεύθυνση δικτύου είναι ο αριθμός ο οποίος είναι ίδιος με τη διεύθυνση στο τμήμα που αντιπροσωπεύει το αναγνωριστικό δικτύου ενώ **στο τμήμα που προσδιορίζει τον υπολογιστή έχει μηδενικά** (στο δυαδικό του ισοδύναμο) Πρόκειται για το αποτέλεσμα του λογικού AND μεταξύ της διεύθυνσης IP και της μάσκας δικτύου.

Για την διεύθυνση IP **192.168.1.18** με μάσκα **255.255.255.0** ή **192.168.1.18/24**, η διεύθυνση δικτύου είναι **192.168.1.0** [*=(192.168.1.18) AND (255.255.255.0) Βλέπε Πίνακα 3.1.4.α*]

Διεύθυνση Εκπομπής (**Broadcast** ή Bcast): Αφορά σε όλους τους υπολογιστές που ανήκουν στο ίδιο δίκτυο. Πακέτο με διεύθυνση προορισμού τη διεύθυνση εκπομπής λαμβάνεται από όλους τους υπολογιστές που ανήκουν στο ίδιο δίκτυο ή υποδίκτυο, όπως αυτό προσδιορίζεται από την αντίστοιχη μάσκα. Για μια δεδομένη διεύθυνση IP, η διεύθυνση εκπομπής είναι ο αριθμός ο οποίος είναι ίδιος με τη διεύθυνση στο τμήμα που αντιπροσωπεύει το αναγνωριστικό δικτύου ενώ **στο τμήμα που προσδιορίζει τον υπολογιστή έχει άσους** (στο δυαδικό του ισοδύναμο).

Για την διεύθυνση IP **192.168.1.18** με μάσκα **255.255.255.0** ή **192.168.1.18/24**, η διεύθυνση εκπομπής είναι **192.168.1.255**

Διεύθυνση Πολυδιανομής (**Multicast**): Διευθύνσεις κλάσης D οι οποίες προσδιορίζουν μια ομάδα υπολογιστών/κόμβων. Για παράδειγμα στη διεύθυνση 224.0.0.2 “ακούνε” όλοι οι δρομολογητές του υποδικτύου. Η υλοποίηση των τεχνικών πολυδιανομής περιγράφεται στο RFC1112 και στην ιστοσελίδα http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml του IANA υπάρχει η επίσημη λίστα διευθύνσεων πολυδιανομής σε αντιστοιχία με τη χρήση τους.

Διεύθυνση επανατροφοδότησης (Loopback), 127.0.0.0/8 και συνήθως **127.0.0.1/32** Αναφέρεται στον ίδιο τον τοπικό υπολογιστή. Ένας υπολογιστής, ακόμη κι αν δεν έχει καμιά δικτυακή διασύνδεση στέλνοντας πακέτα με **προορισμό** (destination) τη διεύθυνση

127.0.0.1 (ή και οποιαδήποτε άλλη διεύθυνση του δικτύου 127.0.0.0/8) αυτά διεκπεραιώνονται πίσω (επανατροφοδοτούνται) στον ίδιο του τον εαυτό.

0.0.0.0/8 (Limited source): Συναντάται μόνον ως διεύθυνση **προέλευσης** (source) και δηλώνει πακέτα από υπολογιστές του "ίδιου" του δικτύου στο οποίο ανήκει και ο συγκεκριμένος υπολογιστής ενώ **0.0.0.0/32** δηλώνει πακέτα του "ίδιου" του υπολογιστή.

169.254.0.0/16 (Link local): Υπολογιστές που είναι ρυθμισμένοι να παίρνουν αυτόματες δικτυακές ρυθμίσεις από διακομιστή DHCP, όταν δεν λάβουν απόκριση, είτε επειδή δεν υπάρχει τέτοιος διακομιστής είτε επειδή υπάρχει κάποιο άλλο πρόβλημα, παίρνουν μια τυχαία διεύθυνση από αυτήν την περιοχή. Για τις διευθύνσεις αυτές γίνεται αναφορά στο RFC3927.

Άλλες **Ειδικές Διευθύνσεις IP** περιγράφονται στο RFC3330 Special-Use IPv4 Addresses.

Διεύθυνση IP υπολογιστή (Host)		**Παράδειγμα**
αποκλειστικής διανομής (unicast)	προσδιορίζει έναν (1) υπολογιστή - host (μια διασύνδεση)	**192.168.1.3** Ο υπολογιστής 192.168.1.3
πολυδιανομής (multicast)	προσδιορίζει ομάδα (group) υπολογιστών	**224.0.0.2** Οι δρομολογητές του δικτύου (κλάση D)
εκπομπής ή ακρόασης (broadcast)	προσδιορίζει όλους τους υπολογιστές ενός δικτύου ή υποδικτύου	**192.168.1.255** Όλοι οι υπολογιστές του δικτύου 192.168.1.0/24

Πίνακας 3.1.5.α: Τύποι διευθύνσεων IPv4

3.1.6 Υποδικτύωση

Πολλές φορές προκύπτει η ανάγκη ένα δίκτυο να χωριστεί σε περισσότερα, μικρότερα υποδίκτυα. Οι λόγοι μπορεί να είναι:

- **Οικονομία διευθύνσεων IP**. Π.χ. ένα δίκτυο τάξης Β το οποίο μπορεί να έχει 65534 υπολογιστές θα μπορούσε να χωριστεί σε 8 υποδίκτυα και να μοιραστεί σε ισάριθμες εταιρείες εφόσον καμιά απ' αυτές δεν πρόκειται να χρειαστεί δίκτυο με παραπάνω από 8190 υπολογιστές.
- **Διαχειριστικοί λόγοι**. Ένα δίκτυο τάξης C, μιας εταιρείας, χωρίζεται σε υποδίκτυα με βάση την οργανωτική δομή της εταιρείας. Ένα υποδίκτυο για το Τμήμα Πωλήσεων, άλλο για το Λογιστήριο και το Τμήμα Προσωπικού και άλλο για το Τεχνικό Τμήμα.

Η υποδικτύωση με δεδομένη τη **διεύθυνση δικτύου** και την **προκαθορισμένη μάσκα δικτύου** πραγματοποιείται σε δυο βήματα:

- Με βάση την απαίτηση για **n υποδίκτυα** ή **m υπολογιστές ανά υποδίκτυο**, υπολογίζεται η **νέα μάσκα δικτύου** δεσμεύοντας δυαδικά ψηφία από το αναγνωριστικό του υπολογιστή (Host ID) και παραχωρώντας τα στο αναγνωριστικό δικτύου (Net ID).
- **Υπολογίζονται οι περιοχές διευθύνσεων** καθώς και οι διευθύνσεις (υπο-)δικτύου και εκπομπής για κάθε υποδίκτυο από τις οποίες διευθυνσιοδοτούνται οι υπολογιστές του κάθε υποδικτύου.

Παράδειγμα 3.1.6.α

Δραστηριότητα 1η

Δίνεται η διεύθυνση δικτύου **192.168.3.0/24** δηλαδή με μάσκα δικτύου **255.255.255.0**

- Να χωριστεί το δίκτυο σε **έξι τουλάχιστον υποδίκτυα** και να δοθούν
- οι περιοχές διευθύνσεων καθώς και
- οι διευθύνσεις υποδικτύου και εκπομπής για κάθε υποδίκτυο.
- Πόσους υπολογιστές μπορεί να έχει το κάθε υποδίκτυο;

Η διεύθυνση ενός υπολογιστή στο δίκτυο **192.168.3.0/24** είναι της μορφής <Net_ID>,<Host_ID> με μήκη σε δυαδικά ψηφία 24,8. Μετά την υποδικτύωση θα είναι της μορφής <Net_ID>,<Subnet_ID>,<Host_ID> με το Net_ID: 24bit και Subnet_ID +Host_ID: 8bit Εφόσον το **Subnet_ID** θα πρέπει να μπορεί να απαριθμήσει **6 υποδίκτυα**, αναφερόμενοι στον επόμενο πίνακα, θα χρειαστούν **3bit**.

Ψηφία	**αριθμήσιμα αντικείμενα**	
1	2^1	2
2	2^2	4
3	2^3	8
4	2^4	16
5	2^5	32
6	2^6	64
7	2^7	128
8	2^8	256

Πίνακας 3.1.6.α

Με 2bit μπορούμε να απαριθμήσουμε 2^2=4 ενώ με 3bit, 2^3=8 διαφορετικά αντικείμενα. Συνεπώς 2bit δεν αρκούν ενώ 3bit είναι αρκετά. Έτσι τα τρία σημαντικότερα ψηφία του αρχικού Host_ID, με τη μορφή άσων, χαρακτηρίζονται ως Subnet_ID και προσαρτώνται στο Net_ID. Το **Subnet_ID** είναι **3 bit**, το Host_ID απομένει 8-3=5bit (τα λιγότερο σημαντικά ψηφία) και στη μάσκα, στις θέσεις τους, αναγράφονται μηδενικά.

Διεύθυνση Δικτύου	**192**	**168**	**3**	**0**
Μάσκα Δικτύου	**255**	**255**	**255**	**0**
	11111111	**11111111**	**11111111**	**00000000**
Μάσκα υποδικτύου	**11111111**	**11111111**	**11111111**	**11100000**
	255	**255**	**255**	**224**

Έτσι η νέα μάσκα είναι η **255.255.255.224** και το δεδομένο δίκτυο γράφεται ως **192.168.3.0/27**

Οι διευθύνσεις των υπολογιστών των υποδικτύων τώρα πια είναι της μορφής <Net_ID>,<Subnet_ID>,<Host_ID> με το Net_ID: 24bit, Subnet_ID: 3bit, Host_ID: 5bit

Το δίκτυο με τη διαδικασία αυτή χωρίστηκε τελικά σε οκτώ υποδίκτυα από τα οποία χρησιμοποιούνται τα έξι και τα υπόλοιπα παραμένουν ελεύθερα για μελλοντική χρήση. Ανεξάρτητα με τον ζητούμενο αριθμό, **ο συνολικός αριθμός των υποδικτύων είναι πάντα δύναμη του δύο (2^n)**.

Οι περιοχές διευθύνσεων για κάθε υποδίκτυο δίνονται παρακάτω:

A/A	1η οκτάδα	2η οκτάδα	3η οκτάδα	4η οκτάδα		Διεύθυνση	
0	11000000	10101000	00000011	000	00000	192.168.3.0	από
	11000000	10101000	00000011		11111	192.168.3.31	έως
1	11000000	10101000	00000011	001	00000	192.168.3.32	
	11000000	10101000	00000011		11111	192.168.3.63	
2	11000000	10101000	00000011	010	00000	192.168.3.64	
	11000000	10101000	00000011		11111	192.168.3.95	
3	11000000	10101000	00000011	011	00000	192.168.3.96	
	11000000	10101000	00000011		11111	192.168.3.127	
4	11000000	10101000	00000011	100	00000	192.168.3.128	
	11000000	10101000	00000011		11111	192.168.3.159	
5	11000000	10101000	00000011	101	00000	192.168.3.160	
	11000000	10101000	00000011		11111	192.168.3.191	
6	11000000	10101000	00000011	110	00000	192.168.3.192	
	11000000	10101000	00000011		11111	192.168.3.223	
7	11000000	10101000	00000011	111	00000	192.168.3.224	
	11000000	10101000	00000011		11111	192.168.3.255	

Πίνακας 3.1.6.β: Υποδίκτυα 192.168.3.0/27

Η στήλη A/A δίνει τον αύξοντα **αριθμό του υποδικτύου** (*η αρίθμηση αρχίζει από το 0, παρατηρήστε ότι ταυτίζεται με την τιμή των ψηφίων της τέταρτης οκτάδας που αντιστοιχούν στο Subnet_ID*). Οι υπολογιστές του κάθε υποδικτύου έχουν κοινές τις τρεις πρώτες οκτάδες (Net_ID) και τα τρία πρώτα ψηφία της τέταρτης οκτάδας (Subnet_ID).

Οι διευθύνσεις από 192.168.3.0 – 192.168.3.31 ανήκουν στο πρώτο υποδίκτυο και μάλιστα η πρώτη και τελευταία έχουν ειδική σημασία. **Η πρώτη**, 192.168.3.0, **είναι η διεύθυνση δικτύου** για το συγκεκριμένο υποδίκτυο ενώ **η τελευταία**, 192.168.3.31 **είναι η διεύθυνση εκπομπής**/μετάδοσης.

Στους υπολογιστές του πρώτου υποδικτύου μπορούν να δοθούν οι διευθύνσεις από 192.168.3.1 έως 192.168.3.30, **συνολικά τριάντα (30)**.

Αντίστοιχα προσδιορίζονται οι διευθύνσεις και για τα άλλα υποδίκτυα.

Διάγραμμα 3.1.6.α

Παρατήρηση: Ένα δίκτυο τάξης C έχει συνολικά διαθέσιμες 254 διευθύνσεις για απόδοση σε υπολογιστές. Δηλαδή μπορεί να έχει μέχρι 254 υπολογιστές. Το ίδιο δίκτυο, υποδικτυωμένο σε οκτώ (8) υποδίκτυα, μπορεί να έχει μέχρι 8 x 30 = 240 υπολογιστές, μια απώλεια συνολικά 14 υπολογιστών. Συνεπώς η υποδικτύωση έχει ως επακόλουθο τη μείωση των διαθέσιμων συνολικά διευθύνσεων υπέρ της διαχείρισης ή της αποφυγής απώλειας περισσότερων διευθύνσεων.

Παράδειγμα 3.1.6.β

Δραστηριότητα 2η

Δίνεται η διεύθυνση δικτύου **192.168.17.0/24** δηλαδή με μάσκα δικτύου **255.255.255.0**.

- Να χωριστεί το δίκτυο σε υποδίκτυα των **50 τουλάχιστον υπολογιστών** και να δοθούν:
  - οι περιοχές διευθύνσεων καθώς και
  - οι διευθύνσεις υποδικτύου και εκπομπής για κάθε υποδίκτυο.
- Πόσα υποδίκτυα μπορεί να έχει συνολικά το συγκεκριμένο δίκτυο;

Ανατρέχοντας στον Πίνακα 3.1.6.α, για να απαριθμηθούν **50 υπολογιστές**, απαιτούνται **έξι (6) bit** ($2^6 = 64$). Συνεπώς για το **Subnet_ID** διατίθενται 8-6=**2 bit**

Διεύθυνση Δικτύου	**192**	**168**	**17**	**0**
Μάσκα Δικτύου	**255**	**255**	**255**	**0**
	11111111	**11111111**	**11111111**	**00000000**
Μάσκα υποδικτύου	**11111111**	**11111111**	**11111111**	**11000000**
	255	**255**	**255**	**192**

Έτσι η νέα μάσκα είναι η **255.255.255.192** και το δεδομένο δίκτυο γράφεται ως **192.168.17.0/26**

Οι διευθύνσεις των υπολογιστών των υποδικτύων τώρα πια είναι της μορφής <Net_ID>,<Subnet_ID>,<Host_ID> με το Net_ID: 24bit, Subnet_ID: 2bit, Host_ID: 6bit

Οι περιοχές διευθύνσεων για κάθε υποδίκτυο δίνονται στον Πίνακα 3.1.6.γ

Ομοίως, όπως και στο προηγούμενο παράδειγμα, η στήλη Α/Α δίνει τον αύξοντα **αριθμό του υποδικτύου** (*η αρίθμηση αρχίζει από το 0, παρατηρήστε ότι ταυτίζεται με την τιμή των ψηφίων της τέταρτης οκτάδας που αντιστοιχούν στο Subnet_ID*). Οι υπολογιστές του κάθε υποδικτύου έχουν κοινές τις τρεις πρώτες οκτάδες (Net_ID) και τα δυο πρώτα ψηφία της τέταρτης οκτάδας (Subnet_ID).

Α/Α	1η οκτάδα	2η οκτάδα	3η οκτάδα	4η οκτάδα		Διεύθυνση	
0	11000000	10101000	00010001	00	000000	192.168.17.0	από
	11000000	10101000	00010001		111111	192.168.17.63	έως
1	11000000	10101000	00010001	01	000000	192.168.17.64	
	11000000	10101000	00010001		111111	192.168.17.127	
2	11000000	10101000	00010001	10	000000	192.168.17.128	
	11000000	10101000	00010001		111111	192.168.17.191	
3	11000000	10101000	00010001	11	000000	192.168.17.192	
	11000000	10101000	00010001		111111	192.168.17.255	

Πίνακας 3.1.6.γ: Υποδίκτυα 192.168.17.0/26

Οι διευθύνσεις από 192.168.17.0 – 192.168.17.63 ανήκουν στο πρώτο υποδίκτυο. **Η πρώτη**, 192.168.17.0, **είναι η διεύθυνση δικτύου** για το συγκεκριμένο υποδίκτυο ενώ **η τελευταία**, 192.168.17.63 **είναι η διεύθυνση εκπομπής**/μετάδοσης.

Το δίκτυο χωρίζεται σε 2^2 = **4 υποδίκτυα.**

Στους υπολογιστές του πρώτου υποδικτύου μπορούν να δοθούν οι διευθύνσεις από 192.168.3.1 έως 192.168.3.62, **συνολικά εξήντα δύο (62)**.

Αντίστοιχα προσδιορίζονται οι διευθύνσεις και για τα άλλα υποδίκτυα.

Παρατήρηση: Ένα δίκτυο τάξης C έχει συνολικά διαθέσιμες 254 διευθύνσεις για απόδοση σε υπολογιστές. Δηλαδή μπορεί να έχει μέχρι 254 υπολογιστές. Το ίδιο δίκτυο, υποδικτυωμένο σε τέσσερα (4) υποδίκτυα, μπορεί να έχει μέχρι 4 x 62 = 248 υπολογιστές, μια απώλεια συνολικά 6 υπολογιστών. Συγκρίνοντας τον αριθμό αυτό με αυτόν του προηγούμενου παραδείγματος, διαπιστώνεται ότι κατά την υποδικτύωση, όσο μικρότερος είναι ο αριθμός των υποδικτύων τόσο μικρότερη είναι η απώλεια σε διαθέσιμες διευθύνσεις.

Με βάση τα δυο προηγούμενα παραδείγματα, να υπολογιστούν τα ζητούμενα, στην επόμενη περίπτωση υποδικτύωσης, η οποία αφορά δίκτυο κλάσης Β.

Δραστηριότητα 3η

Δίνεται η διεύθυνση δικτύου **172.25.0.0/16** δηλαδή με μάσκα δικτύου **255.255.0.0**

- Να χωριστεί το δίκτυο σε **24 τουλάχιστον** υποδίκτυα και να δοθούν
- οι περιοχές διευθύνσεων καθώς και
- οι διευθύνσεις υποδικτύου και εκπομπής για τα τέσσερα (4) πρώτα υποδίκτυα.
- Πόσα υποδίκτυα μπορεί να έχει συνολικά το συγκεκριμένο δίκτυο και πόσους υπολογιστές ανά υποδίκτυο;

3.1.7 Αταξική δρομολόγηση (CIDR3), υπερδικτύωση και μάσκες μεταβλητού μήκους

Εφόσον μια διεύθυνση IP συνοδεύεται από τη μάσκα της, παύει να ισχύει η τάξη/κλάση της διεύθυνσης, όπως αυτή ορίστηκε αρχικά, και το αναγνωριστικό του δικτύου είναι αυτό που ορίζει η συνοδός μάσκα. Έτσι διευκολύνεται η διαδικασία της δρομολόγησης και της διαχείρισης πινάκων δρομολόγησης από τους δρομολογητές IPv4.

Όλος ο χώρος των διευθύνσεων IPv4 αντιμετωπίζεται από τα πρωτόκολλα δρομολόγησης ως ενιαίος χώρος, χωρίς τάξεις/κλάσεις (Classless Inter Domain Routing - CIDR).

Έτσι π.χ. σε μια εταιρεία με αυξημένες ανάγκες δικτύωσης (~1000 υπολογιστές) αντί να δοθεί ένα δίκτυο κλάσης B, με σπατάλη ~64000 διευθύνσεων, δίνονται τέσσερα διαδοχικά δίκτυα κλάσης C.

Για να αντιμετωπίζονται όμως ως ενιαίο δίκτυο, δυο ψηφία ($2^2 = 4$) από το αναγνωριστικό δικτύου (Net_ID) παραχωρούνται στο αναγνωριστικό υπολογιστή (Host_ID) και η συνοδός μάσκα γίνεται **255.255.252.0** (**11111111.11111111.111111**00.**00000000**)

Στην υποδικτύωση, από το αναγνωριστικό του υπολογιστή (Host_ID) δόθηκαν ψηφία στο αναγνωριστικό του δικτύου (Net_ID) ως Subnet_ID. Αντιθέτως, **δίνοντας ψηφία από το (Net_ID) στο αναγνωριστικό υπολογιστή (Host_ID)**, η ενέργεια αυτή χαρακτηρίζεται ως **υπερδικτύωση**. *(δημιουργούνται μεγαλύτερα δίκτυα)*

Π.χ. το δίκτυο **192.168.128.0/22** δηλαδή με μάσκα **255.255.252.0** περιλαμβάνει τις διευθύνσεις από 192.168.128.0 – 192.168.131.255

Α/Α	**1η οκτάδα**	**2η οκτάδα**	**3η οκτάδα**		**4η οκτάδα**	**Διεύθυνση**	
NA	**11000000**	**10101000**	**100000**	**00**	**00000000**	**192.168.128.0**	Από
				11	**11111111**	**192.168.131.255**	έως

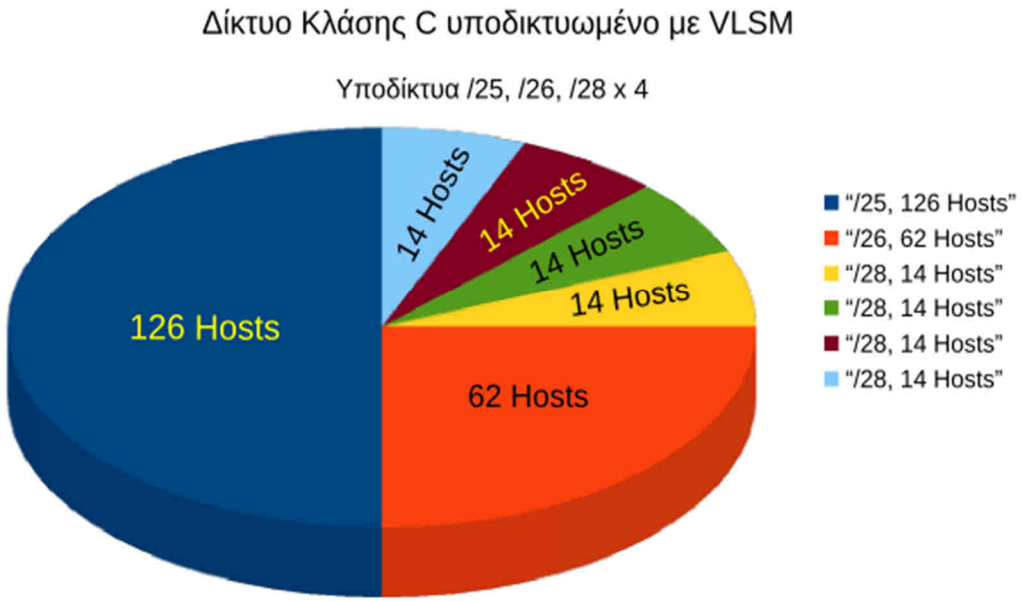
Πίνακας 3.1.7.α: Δίκτυο 192.168.128.0/22 (CIDR)

Δεν υπάρχει θέμα ορισμού υποδικτύων. Το δίκτυο είναι ενιαίο και είναι το **192.168.128.0/22**

Ποιά είναι η **διεύθυνση δικτύου** και ποιά η **διεύθυνση εκπομπής** ή μετάδοσης στην περίπτωση αυτή; *(Θυμηθείτε, η διεύθυνση δικτύου έχει στο Host_ID μηδενικά ενώ η διεύθυνση εκπομπής έχει στο Host_ID άσους. Τα υπόλοιπα ψηφία παραμένουν ίδια.)*

Εδώ πρέπει να επισημανθεί ότι και στην περίπτωση της υποδικτύωσης μπορούμε να χρησιμοποιήσουμε **μεταβλητού μήκους μάσκες υποδικτύωσης** (Variable Length Subnet Masking - **VLSM**) για διαφορετικά υποδίκτυα. Αυτό έχει ως αποτέλεσμα διαφορετικού μεγέθους υποδίκτυα. Να εφαρμόσουμε δηλαδή υποδικτύωση σε υποδίκτυο.

3 Classless Inter Domain Routing



Διάγραμμα 3.1.7.α

3.2 Το αυτοδύναμο πακέτο IP (datagram) – Δομή πακέτου

Το **πρωτόκολλο Διαδικτύου** (Internet Protocol -**IP**) ενθυλακώνει τα πακέτα δεδομένων που του προωθούνται από το ανώτερο επίπεδο σε **αυτοδύναμα πακέτα (datagrams)**. Στην επικεφαλίδα των πακέτων αυτών, σε αντίστοιχα πεδία, προσθέτει όλες τις απαραίτητες διαχειριστικές πληροφορίες ώστε να γίνει εφικτή η εύρεση του προορισμού και η επιτυχής δρομολόγηση από τα πρωτόκολλα δρομολόγησης.

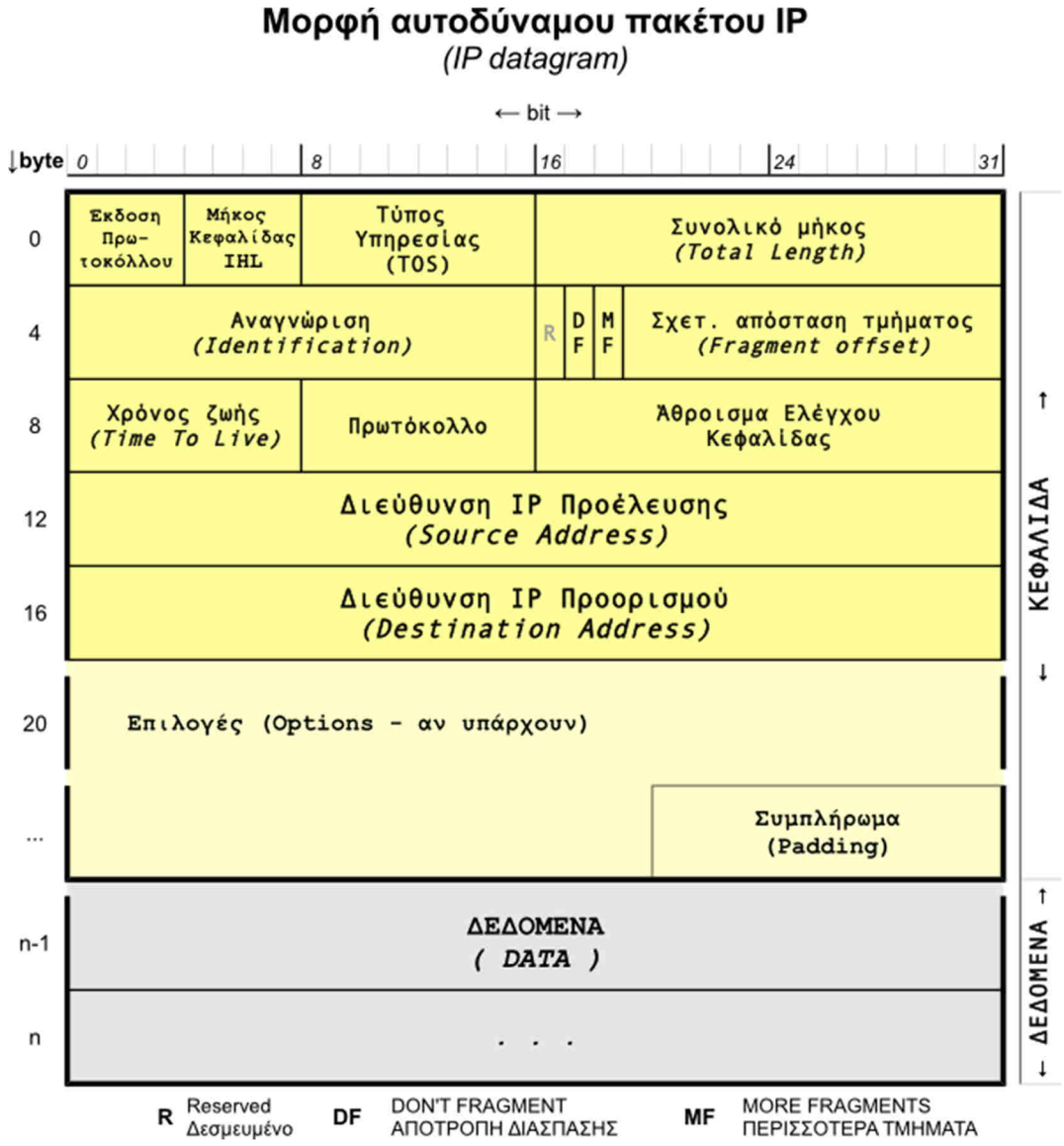
Η σημαντικότερες από αυτές είναι η **διεύθυνση IP προέλευσης** (source IP) και η **διεύθυνση IP προορισμού** (destination IP), μήκους 32bit η καθεμιά, για τις οποίες έγινε λόγος στα προηγούμενα.

Στην Εικόνα 3.2.α φαίνεται η δομή του αυτοδύναμου πακέτου IP.

Το πεδίο **Έκδοση πρωτοκόλλου** (version) μήκους 4 bit, δηλώνει την έκδοση του χρησιμοποιούμενου πρωτοκόλλου Διαδικτύου (4: IPv4, 6: IPv6). Στην περίπτωση του IPv6 η επικεφαλίδα διαφοροποιείται και έχει ελάχιστο μήκος 40 bytes.

Το πεδίο **Μήκος επικεφαλίδας** (Internet Header Length - IHL) μήκους 4 bit, εκφράζει το μήκος της επικεφαλίδας σε λέξεις των 32 bit (4άδες byte). Το ελάχιστο μήκος είναι 5 λέξεις ή 20 byte και το μέγιστο 15 λέξεις ή 60 byte (=15x4).

Ο **Τύπος της Υπηρεσίας** (Type of Service) μήκους 8 bit, περιγράφει πώς πρέπει να χειριστεί το πακέτο κάθε κόμβος δίνοντας προτεραιότητα στην ταχύτητα, εάν επιτρέπεται δηλαδή να καθυστερήσει ή όχι, στην αξιοπιστία ή στο ρυθμό διακίνησης (throughput). Σε νεώτερη αναθεώρηση, το RFC2474 αλλάζει τη σημασία του συγκεκριμένου πεδίου ώστε να υποστηρίζει ένα σύνολο διαφοροποιημένων υπηρεσιών και το ονομάζει Differentiated Services Code Point - **DSCP** (6 bit). Το RFC3168 χαρακτηρίζει τα υπόλοιπα δυο bit ως ρητή ειδοποίηση συμφόρησης, Explicit Congestion Notification - **ECN** (2 bit). Οι αλλαγές σκοπό έχουν να υποστηρίξουν υπηρεσίες με ιδιαίτερες απαιτήσεις όπως μεταφορά φωνής σε πραγματικό χρόνο (VoIP). Για να είναι όμως αυτό εφικτό πρέπει να υποστηρίζεται και από το υπόλοιπο δίκτυο.



Εικόνα 3.2.α: Το αυτοδύναμο πακέτο IP (IP datagram)

Το πεδίο **Συνολικό μήκος** (Total length) μήκους 16 bit, δίνει το συνολικό μήκος του αυτοδύναμου πακέτου (επικεφαλίδα + δεδομένα) σε byte. Μπορεί να πάρει τιμές από 20 που είναι το ελάχιστο μήκος της επικεφαλίδας χωρίς δεδομένα μέχρι 65535 (=16 άσοι). Αυτό σημαίνει ότι το **μέγιστο μέγεθος αυτοδύναμου πακέτου IP** που υποστηρίζει το πρωτόκολλο IPv4 **είναι 65535 bytes**

Τα πεδία της επόμενης, δεύτερης λέξης των 32 bit του αυτοδύναμου πακέτου, χρησιμοποιούνται για την περίπτωση που απαιτείται **διάσπαση ή κατάτμηση** (fragmentation) του πακέτου IP. Όταν το πακέτο πρόκειται να διέλθει από δίκτυο το οποίο στο δεύτερο επίπεδο (ζεύξης δεδομένων) υποστηρίζει πλαίσια μικρότερου μεγέθους από το αυτοδύναμο πακέτο, τότε μοναδικός τρόπος για να εξυπηρετηθεί είναι να διασπαστεί σε μικρότερα **τμήματα**, να περάσουν από το δίκτυο και στον προορισμό να επανασυνδεθούν στο αρχικό πακέτο IP. Τα κομμάτια αυτά του αρχικού πακέτου, τα τμήματα, αποτελούν νέα αυτοδύναμα πακέτα. Για να μπορεί το πρωτόκολλο IP να γνωρίζει σε ποιο αρχικό πακέτο ανήκουν, χρησιμοποιεί το πεδίο **Αναγνώριση** (Identification), μήκους 16 bit, το οποίο είναι η ταυτότητα του πακέτου. Το πεδίο αυτό είναι διαφορετικό σε κάθε πακέτο αλλά ίδιο στα πακέτα που είναι τμήματα του ίδιου αρχικού πακέτου. Για να μπορέσει ο υπολογιστής

προορισμού να τα βάλει με τη σωστή σειρά χρησιμοποιείται το πεδίο **Σχετική Θέση Τμήματος** (Fragment Offset), μήκους 13 bit, η οποία δείχνει τη σχετική απόσταση του τμήματος από την αρχή του αρχικού πακέτου σε **οκτάδες (8x) byte**.

Η Σχετική Θέση Τμήματος η οποία αναφέρεται και ως Δείκτης Εντοπισμού Τμήματος (ΔΕΤ), είναι ένας αριθμός ο οποίος υπολογίζεται ως εξής:

Fragment_offset = n * INT((MTU - IHL*4) / 8)

όπου INT(): η συνάρτηση ... το ακέραιο μέρος του () ...,

MTU: Maximum Transmission Unit δηλ. το μέγιστο μήκος δεδομένων του πλαισίου στο δίκτυο 2ου επιπέδου,

IHL: Internet Header Length δηλαδή το μήκος της επικεφαλίδας του πακέτου IP. Θυμηθείτε ότι εκφράζεται σε λέξεις των 32bit ή 4άδες byte. Η τιμή που μας ενδιαφέρει είναι σε byte.

n: 0 για το πρώτο τμήμα, 1 για το δεύτερο κ.ο.κ.

Για το πρώτο τμήμα η σχετική απόσταση τμήματος είναι πάντα μηδέν (0).

Στη διαδικασία της κατάτμησης σημαντικό ρόλο παίζουν και οι σημαίες MF και DF. Οι σημαίες είναι μεμονωμένα bit των οποίων η κατάσταση είναι 1 ή 0 και έχουν να δηλώσουν κάτι. Έτσι η σημαία **MF** (More Fragments), **ύπαρξη περισσότερων τμημάτων**, όταν είναι ενεργοποιημένη (1) δηλώνει ότι ακολουθούν και άλλα τμήματα ενώ όταν είναι απενεργοποιημένη (0) δηλώνει ότι είναι το τελευταίο τμήμα διασπασμένου πακέτου ή μεμονωμένο πακέτο.

Εάν για οποιοδήποτε λόγο το αυτοδύναμο πακέτο δεν πρέπει να διασπαστεί τότε η σημαία **DF** (Don't Fragment), **απαγόρευση διάσπασης**, τίθεται σε τιμή (1). Έτσι κατά τη δρομολόγηση του πακέτου θα ακολουθηθεί διαδρομή με MTU που δεν απαιτεί διάσπαση ή αν αυτό δεν είναι δυνατό, το πακέτο θα απορριφθεί και ενδεχομένως να ειδοποιηθεί ο αποστολέας για την ενέργεια αυτή του δικτύου.

Στο πρωτόκολλο IPv6 η διάσπαση των πακέτων διενεργείται μόνο από τον υπολογιστή προέλευσης με βάση το μικρότερο MTU της διαδρομής (Path MTU - PMTU) και όχι από τους ενδιάμεσους δρομολογητές.

Η διαδικασία της κατάτμησης (fragmentation) στο IPv4 περιγράφεται με περισσότερη λεπτομέρεια σε επόμενο παράδειγμα.

Το πεδίο **Χρόνος Ζωής** (Time To Live - TTL) μήκους 8 bit, ξεκινά από τον αποστολέα με μια αρχική τιμή, συνήθως 64, και κάθε δρομολογητής, από τον οποίο διέρχεται το πακέτο, μειώνει την τιμή κατά ένα. Όταν η τιμή μηδενιστεί το πακέτο απορρίπτεται και επιστρέφεται στον αποστολέα διαγνωστικό μήνυμα σφάλματος υπέρβασης χρόνου (time exceeded). Κάθε διέλευση του πακέτου από κόμβο χαρακτηρίζεται αναπήδηση (hop). Έτσι το συγκεκριμένο πεδίο μπορεί να χαρακτηριστεί και αντίστροφος μετρητής αναπηδήσεων (hops). Πρακτικά λειτουργεί ως όριο απόρριψης του πακέτου όταν αυτό έχει καθυστερήσει, έχει χαθεί στη διαδρομή ή έχει συμβεί κάποιο σφάλμα με τη διεύθυνση προορισμού και περιφέρεται άσκοπα στο δίκτυο.

Το πεδίο αυτό χρησιμοποιεί η εντολή **traceroute** ή tracert για να ιχνηλατήσει τη διαδρομή, να καταγράψει δηλαδή τους ενδιάμεσους κόμβους από τους οποίους διέρχονται τα πακέτα προς ένα προορισμό. Στέλνει διαδοχικά πακέτα με TTL αρχικά 1 και στη συνέχεια το αυξάνει κατά ένα.

Έτσι στο πρώτο πακέτο το πεδίο TTL με τιμή 1 αφού μειωθεί κατά 1 στον πρώτο κόμβο μηδενίζεται, ο κόμβος το απορρίπτει (drop), το αναφέρει και καταγράφεται ποιος είναι. Στο δεύτερο πακέτο το πεδίο TTL=2 μηδενίζεται στον δεύτερο κόμβο κ.ο.κ. μέχρι για κάποια

τιμή TTL να καταφέρει να φτάσει στον προορισμό. Εν τω μεταξύ έχουν καταγραφεί όλοι οι ενδιάμεσοι κόμβοι στη διαδρομή προς τον προορισμό.

Το πεδίο **πρωτόκολλο**, μήκους 8 bit, περιέχει μια αριθμητική τιμή η οποία δηλώνει το πρωτόκολλο του επιπέδου μεταφοράς στο οποίο ανήκουν τα δεδομένα που περιέχει το πακέτο IP. Έτσι πληροφορείται το πρωτόκολλο IP στο απέναντι άκρο σε ποιο πρωτόκολλο του επιπέδου μεταφοράς να παραδώσει τα δεδομένα, στο TCP (6), στο UDP (17) ή αλλού. Αν υπάρχει πρόσβαση σε υπολογιστή με unix/linux, στο αρχείο /etc/protocols μπορείτε να δείτε την αντιστοιχία αριθμών και πρωτοκόλλων για το πεδίο αυτό. Το ίδιο σε υπολογιστή με windows στο

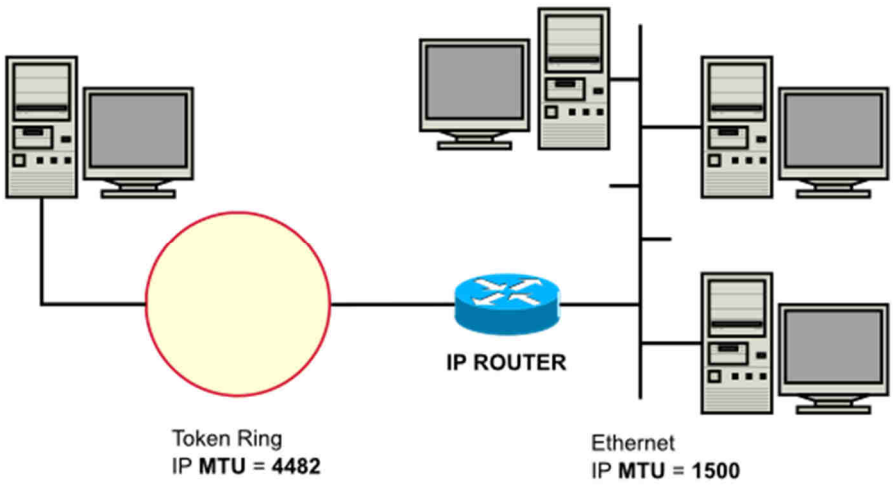
%SystemRoot%\System32\drivers\etc\protocols.

Το **Άθροισμα Ελέγχου της Επικεφαλίδας** (Header Checksum), μήκους 16 bit, διασφαλίζει την ακεραιότητα των τιμών των πεδίων της επικεφαλίδας. Εφαρμόζεται μόνο στην επικεφαλίδα του πακέτου IP ενώ το ίδιο το πεδίο δεν συμμετέχει στον υπολογισμό θεωρώντας ότι περιέχει την τιμή 0. Ο έλεγχος ακεραιότητας της επικεφαλίδας θεωρείται επιβεβλημένος καθώς κατά τη διέλευση του πακέτου από διάφορους δρομολογητές αυτοί τροποποιούν πεδία της επικεφαλίδας με αυξημένη πιθανότητα να συμβούν σφάλματα.

Το πεδίο **Επιλογές** (Options) είναι προαιρετικό και χρησιμοποιείται για ειδικές λειτουργίες όμως όχι συχνά. Όταν υπάρχει, το πεδίο **Συμπλήρωμα** (Padding) συμπληρώνει το πεδίο Επιλογές με μηδενικά ώστε η επικεφαλίδα συνολικά να είναι ακέραιος αριθμός λέξεων των 32 bit.

Παράδειγμα 3.2.1 κατάτμησης αυτοδύναμου πακέτου IP

Ένα αυτοδύναμο πακέτο IP προερχόμενο από ένα δίκτυο Token Ring πρόκειται να προωθηθεί στον υπολογιστή προορισμού ο οποίος βρίσκεται σε δίκτυο Ethernet. Τα δυο δίκτυα συνδέονται με έναν δρομολογητή IP. Στο δίκτυο Token Ring (2ο επίπεδο) το **MTU = 4482 bytes**, δηλαδή το πλαίσιο μπορεί να μεταφέρει δεδομένα μέγιστου μεγέθους 4482 byte. Από την άλλη μεριά το δίκτυο **Ethernet** έχει **MTU = 1500 bytes**, δηλαδή το πλαίσιό του μπορεί να μεταφέρει το πολύ 1500 bytes. Τα δεδομένα ενός πλαισίου Token Ring τα οποία είναι ένα πακέτο IP δεν "χωρούν" σε ένα πλαίσιο Ethernet. Συνεπώς το πακέτο IP πρέπει να διασπαστεί. Αυτό επιτρέπεται εφόσον το DF=0. Να περιγραφεί η διαδικασία κατάτμησης και επανασύνθεσης του αρχικού πακέτου.



Εικόνα 3.2.β: Δίκτυα με διαφορετικό MTU

Το αρχικό πακέτο έχει συνολικό μήκος 4482 bytes ή επικεφαλίδα 20 και 4462 δεδομένα. Κάθε τμήμα θα πρέπει να έχει συνολικό μήκος μαζί με την επικεφαλίδα Total_Length ≤1500 bytes και **το μήκος των δεδομένων να είναι ακέραιο πολλαπλάσιο του 8** για να βγαίνει ακέραια η τιμή της σχετικής θέσης του τμήματος (Offset).

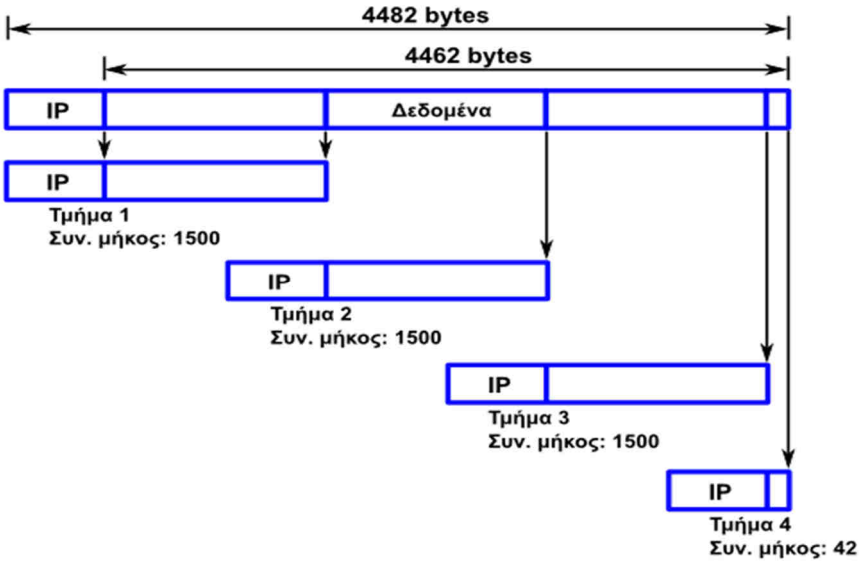
Πρέπει να είναι δηλαδή:

Payload_Length = INT((MTU - IHL*4) / 8) = INT((1500 - 20) / 8) = INT(1480/8) = 185 οκτάδες byte ή 185x8 = 1480 bytes.

Στην περίπτωσή μας συμβαίνει να είναι το 1480 και ακέραιο πολλαπλάσιο του 8.

Το αρχικό πακέτο των 4462 bytes δεδομένων θα χωριστεί σε INT(4462/1480)+1 πακέτα δηλαδή INT(3,01486)+1 = 4 πακέτα, 3 πακέτα των 1480 και ένα με τα δεδομένα που περισσεύουν δηλαδή 4462-(3x1480)= 22

Στην παρακάτω εικόνα 3.2.γ φαίνεται η διαδικασία κατάτμησης



Εικόνα 3.2.γ: Κατάτμηση αυτοδύναμου πακέτου IPv4

Η σχετική θέση του τμήματος (σε οκτάδες byte) υπολογίζεται ως εξής Fragment_offset = n * INT((MTU - IHL*4) / 8) = n *INT(1480/8) = n*185 για n = 0, 1, 2, 3

και είναι για το πρώτο τμήμα 0 με MF=1, για το δεύτερο τμήμα 1*185=185 με MF=1, για το τρίτο τμήμα 2*185=370 με MF=1 και για το τέταρτο τμήμα 3*185=555 με MF=0 γιατί είναι το τελευταίο τμήμα και δεν υπάρχει άλλο.

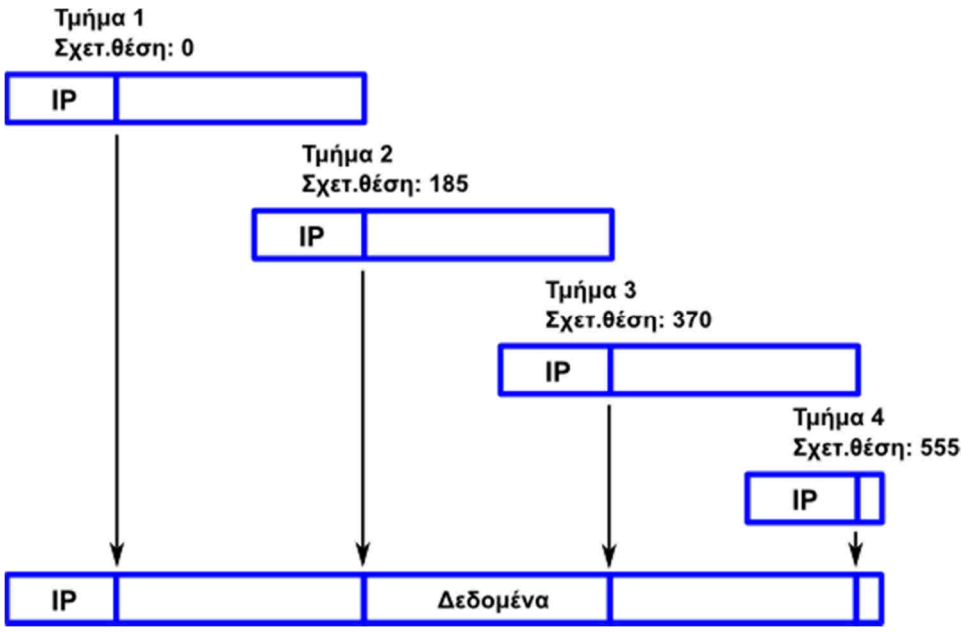
Η σχετική θέση τμήματος επιτρέπει στον υπολογιστή προορισμού να τοποθετήσει τα τμήματα με τη σωστή σειρά για τη συναρμολόγηση του αρχικού πακέτου ακόμη κι αν αυτά έχουν φτάσει στον προορισμό με διαφορετική σειρά.

Όλα τα τμήματα του ίδιου αρχικού πακέτου έχουν την ίδια τιμή στο πεδίο Αναγνώριση.

	1ο τμήμα	2ο τμήμα	3ο τμήμα	4ο τμήμα
Μήκος επικεφαλίδας (λέξεις των 32bit)	5	5	5	5
Συνολικό μήκος (bytes)	1500	1500	1500	42
Μήκος δεδομένων	1480	1480	1480	22
Αναγνώριση	0x2b41	0x2b41	0x2b41	0x2b41
DF (σημαία)	0	0	0	0
MF (σημαία)	1	1	1	0
Σχετ. θέση τμήματος (οκτάδες byte)	0	185	370	555

Πίνακας 3.2.α: Πεδία επικεφαλίδων τμημάτων κατατμημένου πακέτου IPv4

Όταν τα τμήματα φτάσουν στον υπολογιστή προορισμού συναρμολογούνται στο αρχικό διασπασθέν πακέτο IP.

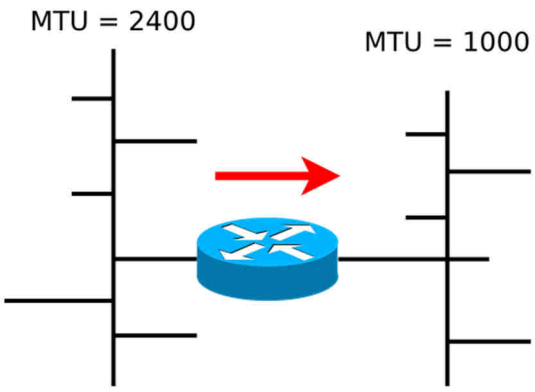


Εικόνα 3.2.δ: Επανασύνθεση κατατμημένου πακέτου IPv4

Παράδειγμα 3.2.2 κατάτμησης αυτοδύναμου πακέτου IP

Ένα αυτοδύναμο πακέτο IP (datagram) μεγέθους **2400** bytes με DF=0 και Αναγνώριση: 0x4a28 πρόκειται να διέλθει από δίκτυο το οποίο υποστηρίζει μέγιστο μήκος δεδομένων πλαισίου (MTU) **1000** bytes. Το πακέτο θα κατατμηθεί;

Σε περίπτωση κατάτμησης, υπολογίστε τον αριθμό των τμημάτων, το μήκος δεδομένων των τμημάτων και δώστε για κάθε τμήμα τα πεδία Μήκος επικεφαλίδας, Συνολικό μήκος, Αναγνώριση, DF, MF και Σχετ. θέση τμήματος (Offset).



Εικόνα 3.2.ε: Δίκτυα με διαφορετικό MTU

Επειδή MTU1=2400 > MTU2=1000 το πακέτο θα κατατμηθεί.

Ξεκινάμε αρχικά με το μήκος δεδομένων των τμημάτων το οποίο είναι Payload_Length = INT((MTU - IHL*4) / 8) = INT((1000 - 20) / 8) = INT(980/8) = 122 ή σε byte 122*8 = 976 bytes και μαζί με επικεφαλίδα 20 bytes το συνολικό μήκος είναι 996 bytes

Ο αριθμός των τμημάτων είναι (2400-20) / 976 = 2,439 δηλαδή τρία (3), δυο ολόκληρα τμήματα των 976 bytes και ένα τρίτο με τα υπόλοιπα δεδομένα, 2380 - 2*976 = 428 bytes.

Κάθε τμήμα θα έχει το ίδιο πεδίο αναγνώρισης με το αρχικό πακέτο (0x4a28) και το DF=0. Επίσης το MF=1 εκτός από το τελευταίο τμήμα στο οποίο θα είναι MF=0

Η Σχετική θέση τμήματος θα είναι n * INT((MTU - IHL*4) / 8) = n *INT(980/8) = n*122 για n=0, 1, 2 δηλαδή 0 για το πρώτο τμήμα, 122 για το δεύτερο και 244 για το τρίτο.

	1ο τμήμα	**2ο τμήμα**	**3ο τμήμα**
Μήκος επικεφαλίδας (λέξεις των 32bit)	5	5	5
Συνολικό μήκος (bytes)	996	996	448
Μήκος δεδομένων	976	976	428
Αναγνώριση	0x2a28	0x2a28	0x2a28
DF (σημαία)	0	0	0
MF (σημαία)	1	1	0
Σχετ. θέση τμήματος (οκτάδες byte)	0	122	244

Πίνακας 3.2.β: Πεδία επικεφαλίδων τμημάτων κατατμημένου πακέτου IPv4

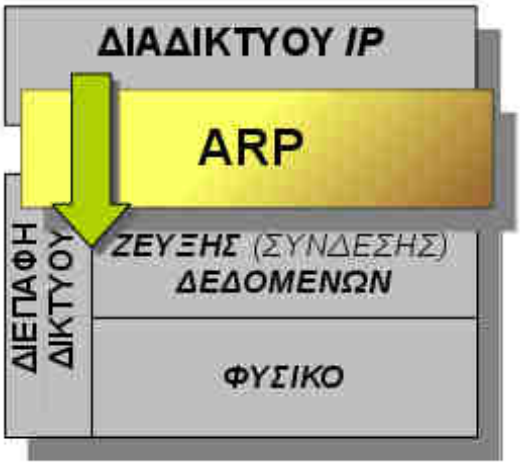
3.3 Πρωτόκολλα ανεύρεσης και απόδοσης διευθύνσεων, Address Resolution Protocol (ARP) και Dynamic Host Configuration Protocol (DHCP)

Σε έναν κόμβο ο οποίος επιθυμεί να αποστείλει δεδομένα σε κάποιον άλλο, το επίπεδο εφαρμογής ξεκινά τη διαδικασία ενθυλάκωσης και κάθε επίπεδο είναι υπεύθυνο να προσθέσει τις δικές του διαχειριστικές πληροφορίες στο πακέτο (PDU - Protocol Data Unit). Το επίπεδο διαδικτύου (3ο OSI):

- δημιουργεί ένα αυτοδύναμο πακέτο IP ενθυλακώνοντας τα δεδομένα που του παραδόθηκαν από το παραπάνω επίπεδο μεταφοράς και
- τοποθετεί στα αντίστοιχα πεδία της επικεφαλίδας τις **διευθύνσεις IP** προέλευσης και προορισμού - καθώς και ό,τι άλλο απαιτείται.
- Στη συνέχεια το παραδίδει στο αμέσως κατώτερο επίπεδο.

Το επίπεδο πρόσβασης δικτύου ή ζεύξης δεδομένων του OSI όμως δε γνωρίζει τίποτα από διευθύνσεις IP παρά μόνο για **διευθύνσεις υλικού** ή **φυσικές** ή **διευθύνσεις MAC** (Media Access Control) όπως αλλιώς λέγονται. Για να το παραδώσει στον παραλήπτη θα πρέπει να γνωρίζει σε ποια φυσική διεύθυνση βρίσκεται ο κόμβος με τη διεύθυνση IP που υπάρχει στο αντίστοιχο πεδίο του αυτοδύναμου πακέτου.

Τον συνδετικό κρίκο ανάμεσα στα δυο επίπεδα, απαντώντας στο ερώτημα "ποια είναι η φυσική διεύθυνση (MAC) του κόμβου με τη συγκεκριμένη διεύθυνση IP;" αναλαμβάνει το **πρωτόκολλο ανάλυσης διευθύνσεων ARP** (Address Resolution Protocol).



Εικόνα 3.3.α: Το πρωτόκολλο ARP

Το **ερώτημα ARP** (ARP request) απευθύνεται στο τοπικό δίκτυο Ethernet με ένα πλαίσιο εκπομπής (broadcast) με διεύθυνση Ethernet προορισμού FF-FF-FF-FF-FF-FF (48 άσοι). Αυτό σημαίνει ότι το ερώτημα φτάνει σε όλους τους κόμβους.

Οι κόμβοι οι οποίοι δεν έχουν την διεύθυνση IP η οποία περιλαμβάνεται στο ερώτημα, απλά το αγνοούν. Ο κόμβος ο οποίος αναγνωρίζει την δική του διεύθυνση IP αποστέλλει μια **απάντηση ARP** (ARP Reply) με ένα πλαίσιο με προορισμό την διεύθυνση Ethernet του ερωτούντος απευθυνόμενος μόνο σε αυτόν (unicast).

Έτσι, τώρα πια είναι γνωστή η φυσική διεύθυνση του παραλήπτη και μπορεί να ολοκληρωθεί το πλαίσιο Ethernet και να αποσταλεί στον παραλήπτη.

Για να αποφευχθούν τα συχνά ερωτήματα προς το τοπικό δίκτυο με πλαίσια εκπομπής (αυξημένη δικτυακή κίνηση), οι σταθμοί διατηρούν προσωρινά τις απαντήσεις που έλαβαν σε έναν πίνακα αντιστοιχίας διευθύνσεων IP σε διευθύνσεις Ethernet στην τοπική μνήμη (arp cache). Έτσι πριν υποβάλλουν νέο ερώτημα ελέγχουν τον προσωρινό πίνακα (cache) arp και υποβάλλουν ερώτημα μόνο όταν δεν υπάρχει κατάλληλη καταχώριση σε αυτόν. Υπάρχει ένας πίνακας ARP για κάθε δικτυακή διασύνδεση (κάρτα δικτύου) ενός υπολογιστή.

Παρακάτω φαίνεται ένας **πίνακας arp** (cache) ενός υπολογιστή με Λ.Σ. Windows7. Οι δυναμικές καταχωρήσεις προέρχονται από ερωτήματα arp ενώ οι στατικές είναι προκαθορισμένα ρυθμισμένες. Προσέξτε ότι η διεύθυνση IP εκπομπής αντιστοιχεί σε διεύθυνση Ethernet εκπομπής.

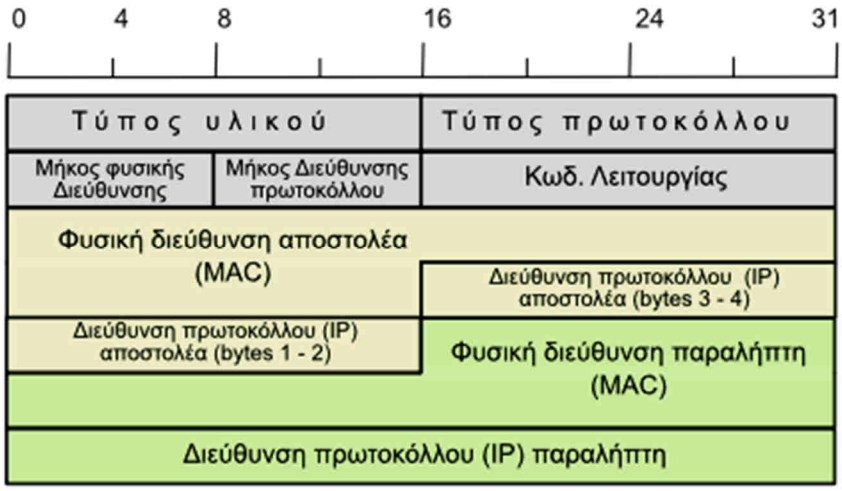
```
Διασύνδεση: 192.168.1.200 --- 0xb
  Διεύθυνση Internet    Φυσική διεύθυνση      Τύπος
  192.168.1.1           74-ea-3a-cd-06-40     δυναμικό
  192.168.1.65          00-04-00-ed-f9-68     δυναμικό
  192.168.1.110         00-19-d1-60-cb-f8     δυναμικό
  192.168.1.255         ff-ff-ff-ff-ff-ff     στατικό
  224.0.0.22            01-00-5e-00-00-16     στατικό
```

224.0.0.251	01-00-5e-00-00-fb	στατικό
224.0.0.252	01-00-5e-00-00-fc	στατικό
239.255.255.250	01-00-5e-7f-ff-fa	στατικό
255.255.255.255	ff-ff-ff-ff-ff-ff	στατικό

Πίνακας 3.3.α: ARP cache υπολογιστή με Λ.Σ. Windows

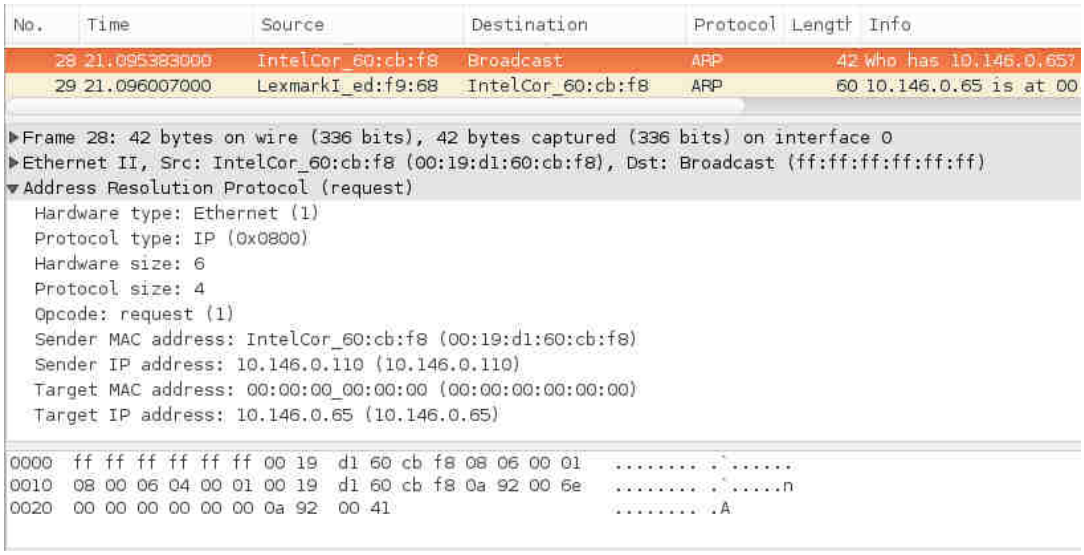
Οι δυναμικές καταχωρίσεις του πίνακα arp μετά την παρέλευση ορισμένου χρόνου χωρίς να χρησιμοποιηθούν, διαγράφονται. Ο χρόνος ποικίλει από μερικά δευτερόλεπτα μέχρι μερικά λεπτά (συνήθως 1-5 λεπτά) και μπορεί να ρυθμιστεί από τον διαχειριστή του συστήματος.

Η δομή του πακέτου ARP (είναι ενθυλακωμένο σε πλαίσιο Ethernet) έχει ως εξής:



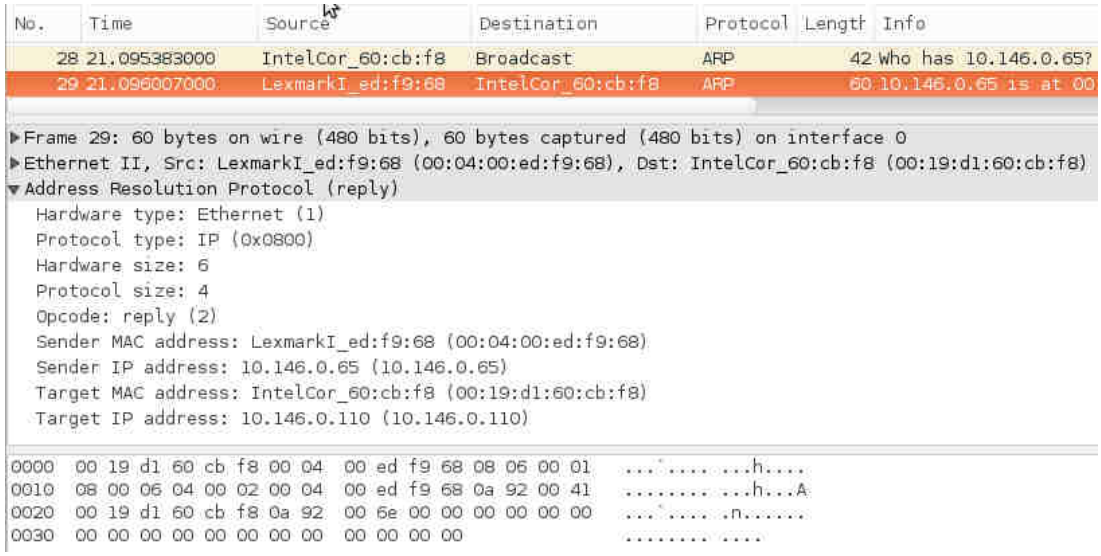
Εικόνα 3.3.β: Δομή πακέτου ARP

Στην επόμενη εικόνα 3.3.γ φαίνεται ένα **ερώτημα ARP** (ARP request, Opcode: 1) όπως υποβλήθηκε από τον υπολογιστή με διεύθυνση IP 10.146.0.110 ο οποίος ερωτά ποια είναι η διεύθυνση Ethernet του υπολογιστή με διεύθυνση IP 10.146.0.65. Συγκρίνετέ το με την δομή του πακέτου ARP και αναγνωρίστε τα διάφορα πεδία του και τις τιμές που περιέχουν. (*Η καταγραφή έγινε με τον αναλυτή πρωτοκόλλου wireshark*)



Εικόνα 3.3.γ: Ερώτημα ARP (ARP request, opcode 1)

Και η **απάντηση ARP** (ARP reply, Opcode: 2) στο ερώτημα η οποία φαίνεται στο πεδίο Sender MAC address: και είναι 00:04:00:ed:f9:68

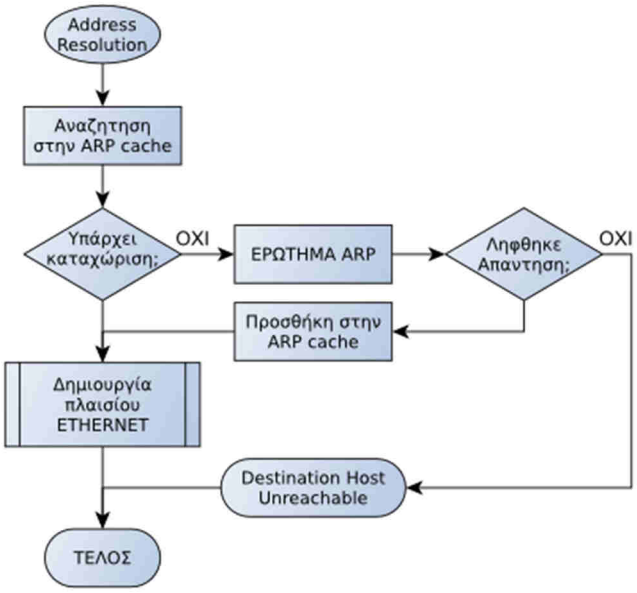


Εικόνα 3.3.δ: Απάντηση ARP (ARP reply, opcode 2)

Εάν δεν βρεθεί καταχώρηση στον πίνακα ARP και ούτε απαντηθεί το ερώτημα ARP (γιατί ίσως απλώς ο υπολογιστής με τη συγκεκριμένη IP να είναι κλειστός ή να μην υπάρχει) τότε επιστρέφεται στην εφαρμογή διαγνωστικό μήνυμα ότι ο υπολογιστής προορισμού δε μπορεί να προσεγγιστεί. Παράδειγμα εκτέλεσης ping σε ανύπαρκτο υπολογιστή:

```
From 10.146.0.110 icmp_seq=3 Destination Host Unreachable
```

Συνοψίζοντας, το πακέτο IP κρατείται σε αναμονή και εκτελείται η διεργασία αντιστοίχησης διεύθυνσης IP προορισμού σε φυσική διεύθυνση Ethernet από το πρωτόκολλο ARP όπως φαίνεται στο διάγραμμα ροής.



Εικόνα 3.3.ε: Ανάλυση διευθύνσεων ARP

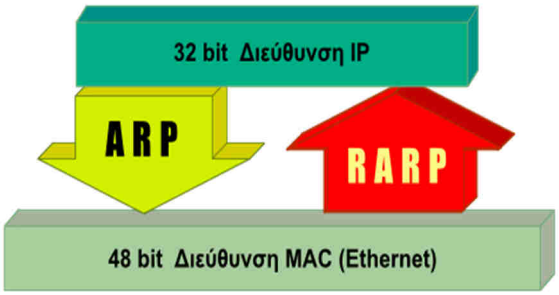
Μόλις αποκτηθεί η φυσική διεύθυνση προορισμού, δημιουργείται το πλαίσιο (frame) και αποστέλλεται στον υπολογιστή προορισμού.

Το πρωτόκολλο ARP έχει τυποποιηθεί στο RFC826.

Εάν ένας υπολογιστής δεν γνωρίζει την δική του διεύθυνση IP, επειδή ίσως να μην του έχει οριστεί, τότε μπορεί να ζητήσει να του αποδοθεί μια. Τη διαδικασία αυτή μπορεί να την αναλάβει το **πρωτόκολλο αντίστροφης ανάλυσης διευθύνσεων** (Reverse Address Resolution Protocol - **RARP**) σε

συνεργασία με έναν **εξυπηρετητή RARP,** ο οποίος είναι επιφορτισμένος με την απόδοση διευθύνσεων IP στους αιτούντες σταθμούς.

Το **πρωτόκολλο RARP** αναλαμβάνει να πληροφορήσει των ερωτώντα υπολογιστή για το ποια είναι η η δική του διεύθυνση IP, ποια διεύθυνση IP πρέπει να πάρει.



Εικόνα 3.3.στ: Σχέση ARP/RARP και διευθύνσεων

Επειδή όμως περιορίζεται μόνο στην διεύθυνση IP και ένας υπολογιστής χρειάζεται επιπλέον ρυθμίσεις όπως μάσκα δικτύου, προεπιλεγμένη πύλη, διακομιστές DNS κ.ά. το RARP χρησιμοποιείται από σπάνια έως καθόλου. Περιγράφεται στο RFC903.

Αντί αυτού χρησιμοποιείται το **πρωτόκολλο εκκίνησης BOOTP** (BOOTstrap Protocol) και το νεώτερο **πρωτόκολλο δυναμικής απόδοσης ρυθμίσεων υπολογιστή DHCP** (Dynamic Host Configuration Protocol).

Το BOOTP είναι προσανατολισμένο για χρήση από δικτυακούς υπολογιστές χωρίς δίσκο. Αυτοί οι υπολογιστές εκκινούν παίρνοντας όλες τις ρυθμίσεις τους και φορτώνουν το λειτουργικό τους σύστημα από κάποιον διακομιστή του δικτύου. Το DHCP είναι πιο ευέλικτο και έχει επικρατήσει καθώς προσφέρει συμβατότητα προς τα πίσω μπορώντας να εξυπηρετήσει και πελάτες BOOTP.

Θα πρέπει να σημειωθεί πως αντίθετα με τα πρωτόκολλα ARP/RARP τα οποία λειτουργούν ως ενδιάμεσα των επιπέδων 2 και 3 του OSI, **τα πρωτόκολλα BOOTP και DHCP καλύπτουν και το επίπεδο εφαρμογής του TCP/IP**. Είναι εφαρμογές που ακολουθούν το μοντέλο πελάτη-εξυπηρετητή (client-server). Παρόλα αυτά, επειδή ο ρόλος τους για τις ρυθμίσεις του πρωτοκόλλου IP είναι σημαντικός θα περιγραφούν μαζί του.

3.3.1 Χρήση BOOTP από σταθμό χωρίς δίσκο

Το αίτημα απευθύνεται στο δίκτυο με εκπομπή (broadcast) και η απάντηση με τις ρυθμίσεις λαμβάνεται στη φυσική διεύθυνση αποκλειστικής διανομής (unicast) του πελάτη.

- Ο υπολογιστής εκκινεί και πληροφορείται τη φυσική του διεύθυνση από τη ROM της κάρτας δικτύου του. Η ROM περιέχει και μια τελείως βασική υλοποίηση της στοίβας πρωτοκόλλων του TCP/IP
- Δημιουργεί ένα πακέτο UDP με **αίτημα BOOTP** (BOOTP Request) προς την θύρα 67.
- Ενθυλακώνεται σε πακέτο IP με διεύθυνση προέλευσης 0.0.0.0 και διεύθυνση προορισμού τη διεύθυνση εκπομπής 255.255.255.255
- Εν συνεχεία ενθυλακώνεται σε ένα πλαίσιο με διεύθυνση προέλευσης τη δική του φυσική διεύθυνση και διεύθυνση προορισμού τη διεύθυνση εκπομπής FF-FF-FF-FF-FF-FF και στέλνεται στο τοπικό δίκτυο.
- Ο διακομιστής BOOTP παραλαμβάνει το αίτημα.
- Απαντά με πλαίσιο στη φυσική διεύθυνση του αιτούντα ως διεύθυνση προορισμού.
- Το ενθυλακωμένο πακέτο IP έχει ως διεύθυνση προορισμού την διεύθυνση IP που αποδίδεται στον αιτούντα υπολογιστή.
- Το ενθυλακωμένο πακέτο UDP με προορισμό την θύρα 68 είναι **απάντηση BOOTP** (BOOTP Reply) και περιλαμβάνει το όνομα και τη θέση ενός αρχείου εκκίνησης.
- Ο υπολογιστής χρησιμοποιεί το απλό πρωτόκολλο μεταφοράς αρχείων TFTP (Trivial File Transfer Protocol) και μεταφορτώνει το αρχείο εκκίνησης.

- Με την ολοκλήρωση της μεταφόρτωσης αποσυμπιέζει το αρχείο εκκίνησης στη RAM, εκκινεί και αρχικοποιεί (ρυθμίσεις TCP/IP) το λειτουργικό σύστημα. Τέλος ξεκινά την εκτέλεση της προκαθορισμένης εφαρμογής.

Το πρωτόκολλο BOOTP λειτουργεί ακόμη κι αν παρεμβάλλονται δρομολογητές, δηλαδή ο αιτών υπολογιστής και ο διακομιστής βρίσκονται σε διαφορετικά φυσικά δίκτυα. Αυτό είναι εφικτό εφόσον οι ενδιάμεσοι δρομολογητές υποστηρίζουν την προώθηση αιτημάτων BOOTP λειτουργώντας ως **πράκτορες αναμετάδοσης** (**BOOTP Relay Agent**). Το πρωτόκολλο BOOTP περιγράφεται στο RFC951.

3.3.2 Το πρωτόκολλο δυναμικής διευθέτησης υπολογιστή DHCP

Το **πρωτόκολλο δυναμικής διευθέτησης (απόδοσης ρυθμίσεων) υπολογιστή DHCP** (Dynamic Host Configuration Protocol) λειτουργεί όπως το BOOTP το οποίο και επεκτείνει. Εξακολουθεί να λειτουργεί ως εφαρμογή πελάτη-εξυπηρετητή χρησιμοποιώντας πακέτα UDP με αριθμό θύρας προορισμού 67 για τον εξυπηρετητή και 68 για τον πελάτη.

Επιτρέπει σε έναν υπολογιστή να αποκτά τις ρυθμίσεις που χρειάζεται σε ένα μόνο μήνυμα και να λαμβάνει μια διεύθυνση γρήγορα και δυναμικά.

Καθορίζει τρεις τύπους εκχώρησης διευθύνσεων:

- μη αυτόματη ρύθμιση (manual configuration), στην οποία ο διαχειριστής ορίζει συγκεκριμένες διευθύνσεις που θα πάρουν συγκεκριμένοι υπολογιστές.
- αυτόματη ρύθμιση (automatic configuration), κατά την οποία ο διακομιστής DHCP εκχωρεί μια μόνιμη διεύθυνση σε έναν υπολογιστή ο οποίος συνδέεται πρώτη φορά, και
- δυναμική ρύθμιση (dynamic configuration) κατά την οποία ο διακομιστής δανείζει ή μισθώνει μια διεύθυνση σε έναν υπολογιστή για περιορισμένο χρόνο.

Η δυναμική ρύθμιση είναι και η πιο συχνά χρησιμοποιούμενη.

Τα πλεονεκτήματα του DHCP

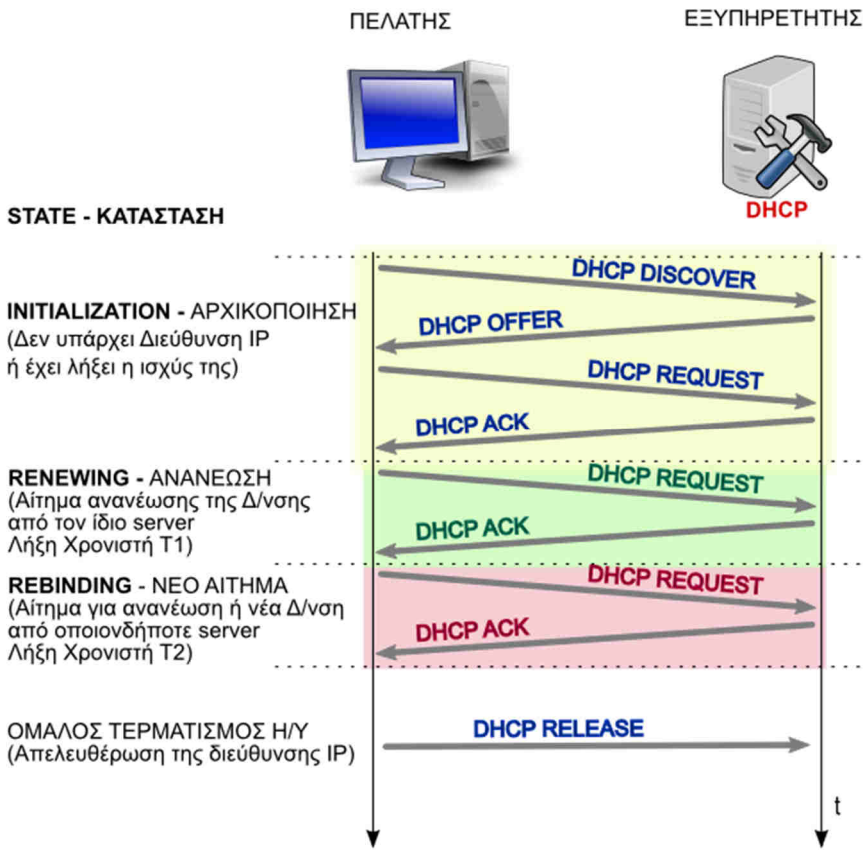
Οι περισσότεροι χρήστες δεν αντιλαμβάνονται τις τεχνικές λεπτομέρειες της δικτύωσης και οι ρυθμίσεις του TCP/IP για να συνδεθούν σε δίκτυο, τους φαίνονται πολύπλοκες. Το DHCP δίνει τη δυνατότητα σ' αυτούς τους χρήστες να συνδεθούν εύκολα στο δίκτυο και στο διαχειριστή το πλεονέκτημα της κεντρικής διαχείρισης των ρυθμίσεων και την ευκολία υποστήριξης των χρηστών και συντήρησης του δικτύου.

Το πρωτόκολλο DHCP επιτρέπει σε έναν υπολογιστή να πάρει επιπλέον ρυθμίσεις πέραν της διεύθυνσης IP όπως μάσκα δικτύου, προεπιλεγμένη πύλη, διακομιστές DNS. Μπορεί να πάρει ρυθμίσεις στο επίπεδο διαδικτύου για τον υπολογιστή ή για κάθε του δικτυακή σύνδεση ανεξάρτητα, ρυθμίσεις για το επίπεδο ζεύξης δεδομένων, για το πρωτόκολλο TCP (μεταφοράς) και για υπηρεσίες (εφαρμογής) όπως διακομιστές χρόνου (NTP), διακομιστές αλληλογραφίας κ.λπ. Όλες αυτές οι επιλογές φαίνονται στο RFC2132 και στα συμπληρωματικά του.

Ένας υπολογιστής, ρυθμισμένος να χρησιμοποιεί την υπηρεσία DHCP, αμέσως μετά την εκκίνησή του:

- Δημιουργεί ένα πακέτο UDP **DHCPDISCOVER** στη θύρα προορισμού 67.
- το ενθυλακώνει σε πακέτο IP με διεύθυνση προέλευσης 0.0.0.0 και διεύθυνση προορισμού τη διεύθυνση εκπομπής 255.255.255.255

- στη συνέχεια το ενθυλακώνει σε ένα πλαίσιο με διεύθυνση προέλευσης τη δική του φυσική διεύθυνση και διεύθυνση προορισμού τη διεύθυνση εκπομπής FF-FF-FF-FF-FF-FF και στέλνεται στο τοπικό δίκτυο.
- Εάν υπάρχουν εξυπηρετητές DHCP ανταποκρίνονται ο καθένας με ένα πακέτο **DHCPOFFER** στη θύρα 68, ενθυλακωμένο σε πακέτο IP εκπομπής και πλαίσιο εκπομπής (διευθύνσεις προορισμού 255.255.255.255, FF-FF-FF-FF-FF-FF). Όταν είναι εφικτό, αποφεύγουν να απαντούν με πλαίσια εκπομπής.
- Ο πελάτης υπολογιστής επιλέγει τις ρυθμίσεις που προσφέρονται από έναν από τους εξυπηρετητές και το δηλώνει αποστέλλοντας ένα πακέτο εκπομπής **DHCPREQUEST** στο οποίο ζητά τις προσφερόμενες ρυθμίσεις.
- Ο εξυπηρετητής DHCP που προσέφερε τις ρυθμίσεις επιβεβαιώνει την προσφορά του με ένα πακέτο DHCPACK.



Εικόνα 3.2.2.α: Λειτουργία DHCP

Από τη λήψη της επιβεβαίωσης DHCPACK και στη συνέχεια ο υπολογιστής λειτουργεί με τις δικτυακές ρυθμίσεις που πήρε (κατάσταση Δεσμευμένος - BOUND). Η διεύθυνση IP παραχωρείται στον υπολογιστή για συγκεκριμένο χρονικό διάστημα και χαρακτηρίζεται ως μίσθωση (lease).

Από τη στιγμή αυτή, ο υπολογιστής αρχίζει τη σχετική μέτρηση χρόνου ώστε να προβεί στις κατάλληλες ενέργειες παράτασης της μίσθωσης της διεύθυνσης πριν τη λήξη της. Κρατά δύο χρόνους,

- τον T1, μετά την παρέλευση του οποίου προσπαθεί να ανανεώσει τη μίσθωση (DHCPREQUEST - unicast) από τον διακομιστή ο οποίος έδωσε αρχικά τη διεύθυνση, περνά δηλαδή σε κατάσταση RENEWING και

- τον T2, μετά την παρέλευση του οποίου αναζητά ανανέωση ή νέα διεύθυνση (DHCPREQUEST - broadcast) από οποιονδήποτε διακομιστή DHCP περνά δηλαδή σε κατάσταση REBINDING.

Ο χρόνος T1 είναι περίπου (0,5*χρόνος_μίσθωσης) και ο T2 περίπου (0,875*χρόνος_μίσθωσης). Είναι δηλαδήT1 < T2.

Όταν ο υπολογιστής τερματίζει τη λειτουργία του ομαλά (shutdown) πριν λήξει η μίσθωση της διεύθυνσης, τότε απελευθερώνει την διεύθυνσή του στέλνοντας πριν τον τερματισμό, στον διακομιστή DHCP, ένα πακέτο **DHCPRELEASE**.

Το πρωτόκολλο DHCP προβλέπει επιπλέον και τα εξής μηνύματα:

- **DHCPNAK** (από τον διακομιστή προς τον πελάτη). Εάν μετά από ένα αίτημα DHCPREQUEST ο διακομιστής δεν επαληθεύσει ως σωστές τις ζητηθείσες ρυθμίσεις απαντά αρνητικά με DHCPNAK.
- **DHCPDECLINE** (από τον πελάτη προς τον διακομιστή). Εάν μετά από μια προσφορά DHCPOFFER, ο πελάτης διαπιστώσει ότι οι ρυθμίσεις που του δόθηκαν είναι σε σύγκρουση με αυτές άλλου υπολογιστή, τις απορρίπτει με DHCPDECLINE και ξεκινά τη διαδικασία από την αρχή με DHCPDISCOVER.
- **DHCPINFORM** (από τον πελάτη προς τον διακομιστή). Από τη στιγμή που ο πελάτης έχει λάβει διεύθυνση IP και θέλει πρόσθετες πληροφορίες ρυθμίσεων, δε μπορεί να στείλει νέο αίτημα DHCPREQUEST. Στην περίπτωση αυτή τις ζητά με ένα αίτημα DHCPINFORM.

Η λειτουργία του πρωτοκόλλου DHCP υποστηρίζεται και από **πράκτορες αναμετάδοσης** (DHCP Relay Agents) για την εξυπηρέτηση πελατών οι οποίοι δε βρίσκονται στο ίδιο φυσικό δίκτυο με τον διακομιστή. Ο πελάτης εφόσον δεν έχει δικτυακές ρυθμίσεις σε επίπεδο IP δεν μπορεί να επικοινωνήσει με υπολογιστές σε άλλα δίκτυα. Ένας υπολογιστής που βρίσκεται στο ίδιο φυσικό δίκτυο με τον πελάτη, προωθεί το αίτημά του πελάτη στο διακομιστή DHCP στο άλλο δίκτυο και του επιστρέφει την απάντηση.

Το πρωτόκολλο DHCP προτάθηκε ως επέκταση του BOOTP, αρχικά στα RFC1531, 1541 τα οποία έχουν αντικατασταθεί από το RFC2131. Όλες οι πληροφορίες σχετικά με αυτό βρίσκονται στο RFC2131 και στα συμπληρωματικά του.

3.4 Διευθύνσεις IP και Ονοματολογία

Η **δεκαδική σημειογραφία με τελείες** (*four-part dotted decimal notation)* είναι ένας σχετικά εύκολος τρόπος γραφής διευθύνσεων IP οι οποίες είναι δυαδικοί αριθμοί των 32 bit. Έτσι το να θυμάται ένας χρήστης έναν αριθμό όπως ο 192.168.1.2 είναι σχετικά εύκολο, όμως το να θυμάται έναν τέτοιο αριθμό για κάθε υπολογιστή στον οποίο θέλει να συνδεθεί είναι δύσκολο.

Είναι σαν να προσπαθεί να θυμάται τους αριθμούς τηλεφώνου όλων των φίλων και γνωστών του τους οποίους πρόκειται κάποια στιγμή να καλέσει από το τηλέφωνο. Θυμάται τα ονόματά τους μα όχι και τους αριθμούς τηλεφώνων τους. Όταν πρόκειται να τηλεφωνήσει σε κάποιον χρησιμοποιεί έναν τηλεφωνικό κατάλογο στον οποίο αναζητά το όνομα το οποίο γνωρίζει και χρησιμοποιεί τον τηλεφωνικό αριθμό που αντιστοιχεί στο όνομα.

Η διαδικασία της ενθυλάκωσης απαιτεί αριθμητικές διευθύνσεις. Για τους ανθρώπους είναι πιο βολικά τα ονόματα. Έτσι από την αρχή του Διαδικτύου και της ανάπτυξης της ομάδας πρωτοκόλλων του TCP/IP χρησιμοποιήθηκαν **απλά μονολεκτικά ονόματα** με τα οποία αναφέρονταν στους διασυνδεδεμένους υπολογιστές. Όμως έπρεπε να υπάρχει μια λίστα αντιστοιχίας ή μετάφρασης ονομάτων σε διευθύνσεις IP την οποία θα συμβουλεύονταν τα

πρωτόκολλα ώστε να χρησιμοποιούν την αντίστοιχη αριθμητική διεύθυνση. Το ρόλο της λίστας αυτής ανέλαβε το αρχείο HOSTS.TXT αντίγραφο του οποίου είχε στη διάθεσή του κάθε υπολογιστής του δικτύου. Το πρωτότυπο ενημερωνόταν κεντρικά από έναν διαχειριστικό κόμβο και διανέμονταν ένα αντίγραφό του σε όλους τους άλλους. Το αρχείο αυτό υπάρχει και στους σημερινούς υπολογιστές παρότι δεν ενημερώνεται και δεν χρησιμοποιείται συνήθως. Σε υπολογιστή με windows είναι το %SystemRoot%\System32\drivers\etc\hosts ενώ σε υπολογιστή με unix/linux το /etc/hosts. Για το αρχείο HOSTS.TXT και τη δομή του δείτε το RFC952.

Παράδειγμα αρχείου hosts από υπολογιστή με Λ.Σ. windows

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host
name.
# The IP address and the host name should be separated by at least
one
# space.
#
# Additionally, comments (such as these) may be inserted on
individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
# localhost name resolution is handled within DNS itself.
#     127.0.0.1       localhost
#     ::1             localhost
```

Με τον καιρό και την μεγάλη αύξηση του αριθμού των κόμβων του Διαδικτύου, τη δυναμική σύνδεση αλλά και αποσύνδεση των κόμβων, ο επίπεδος χώρος ονομάτων και το αρχείο HOSTS.TXT δεν επαρκούσαν για να δώσουν μια σαφή και προπάντων επικαιροποιημένη εικόνα των υπολογιστών του δικτύου.

Έτσι, νωρίς ακόμη (1983, RFC882,883), προτάθηκε και υλοποιήθηκε η **Υπηρεσία Ονομάτων Περιοχών** (Domain Name System - DNS). Ένα σύστημα ονομάτων το οποίο δεν είναι επίπεδο αλλά **ιεραρχικά δομημένο**, **οργανωμένο σε περιοχές και υποπεριοχές σε διάφορα επίπεδα**. Στο κατώτερο επίπεδο, στο αριστερό μέρος, βρίσκεται το όνομα του υπολογιστή. Η διαδικασία αντιστοίχισης-μετάφρασης ονομάτων σε διευθύνσεις IP ονομάζεται **ανάλυση ονομάτων** (name resolve) και το κομμάτι του λογισμικού που είναι επιφορτισμένο με αυτή name resolver.

Η μορφή ενός τέτοιου ονόματος είναι:

υπολογιστής.υποπεριοχή_n. ... .υποπεριοχή1.περιοχή.περιοχή_TLD

(TLD = Top Level Domain - περιοχή ανώτατου επιπέδου)

Το πλήρες όνομα του διακομιστή του 2ου ΕΠΑ.Λ. Κατερίνης είναι:

2epal-kater.pie.sch.gr

Από δεξιά προς αριστερά και από ανώτατο προς το κατώτερο επίπεδο η σημασία είναι η εξής:

.gr	Όνομα περιοχής ανώτατου επιπέδου (TLD), Ελλάδα.
.sch.gr	όνομα περιοχής, το σχολικό δίκτυο (.sch.)
.pie.	όνομα υποπεριοχής, Πιερία
2epal-kater.	το όνομα ή ψευδώνυμο (alias) του υπολογιστή

Η διαχείριση του συστήματος DNS είναι και αυτή ιεραρχική και **κατανεμημένη** σε διάφορους διακομιστές της υπηρεσίας για διαφορετικές περιοχές και υποπεριοχές.
Περισσότερες πληροφορίες μπορούν να βρεθούν στα RFC1034, 1035. Εκτενής λόγος για την Υπηρεσία DNS γίνεται στο 6ο κεφάλαιο το οποίο αναφέρεται στο επίπεδο Εφαρμογής.

3.5 Διευθυνσιοδότηση IPv6

Το πρωτόκολλο Διαδικτύου IPv4, από τη δεκαετία του 1980, αντιμετώπισε επιτυχώς τις ανάγκες της παγκόσμιας διαδικτύωσης. Όμως με την τεράστια αύξηση του αριθμού των διασυνδεδεμένων υπολογιστών άρχισαν να εμφανίζονται καταστάσεις οι οποίες οδηγούν το πρωτόκολλο στα όριά του. Η σημαντικότερη από αυτές είναι η **εξάντληση των διαθέσιμων διευθύνσεων**. Έτσι προέκυψε η ανάγκη επέκτασής του που οδήγησε στην έκδοση 6 (IPv6). Τα κυριότερα προβλήματα που αντιμετωπίζει το IPv4 και ήρθε να δώσει λύσεις η νέα έκδοση του πρωτοκόλλου συνοψίζονται στα εξής:

- Το IPv4 προβλέπει διευθύνσεις μήκους 32 bit και ένα χώρο διευθύνσεων θεωρητικού μεγέθους $2^{32} = 4.294.967.296$. Ο αριθμός αυτός, αν λάβουμε υπόψη τους περιορισμούς της διευθυνσιοδότησης, είναι στην πραγματικότητα πολύ μικρότερος. Ο τρόπος αύξησης των διαθέσιμων διευθύνσεων είναι να αυξηθεί ο αριθμός των ψηφίων (bit) που διατίθενται για τη διευθυνσιοδότηση. Έτσι στο νέο πρωτόκολλο το οποίο ονομάζεται **πρωτόκολλο Διαδικτύου IPv6** (έκδοση 6) οι διευθύνσεις έχουν μήκος **128 bit**. Εκτός από το πρόβλημα της εξάντλησης των διαθέσιμων διευθύνσεων το νέο πρωτόκολλο κλήθηκε να αντιμετωπίσει και άλλα προβλήματα τα οποία προέκυψαν κυρίως λόγω γιγάντωσης του Διαδικτύου.
- Οι πίνακες δρομολόγησης στους δρομολογητές του δικτύου κορμού (backbone routers) περιέχουν πληροφορίες δρομολόγησης για κάθε διασυνδεδεμένο δίκτυο στον κόσμο. Το μέγεθος των πινάκων αυτών αυξήθηκε σε ανησυχητικά όρια (σε περισσότερα από 500.000 δρομολόγια, στα μέσα του 2015) με αποτέλεσμα από πολλούς ειδικούς να θεωρείται σημαντικότερο πρόβλημα ακόμη και από την εξάντληση των διευθύνσεων. Η **βελτιστοποίηση της διαδικασίας της δρομολόγησης** είναι άμεσης προτεραιότητας.

Σε αυτό συμβάλλει η **απλοποίηση της επικεφαλίδας** του πακέτου IPv6 κι η έξυπνη χρήση των προαιρετικών επικεφαλίδων επέκτασης.

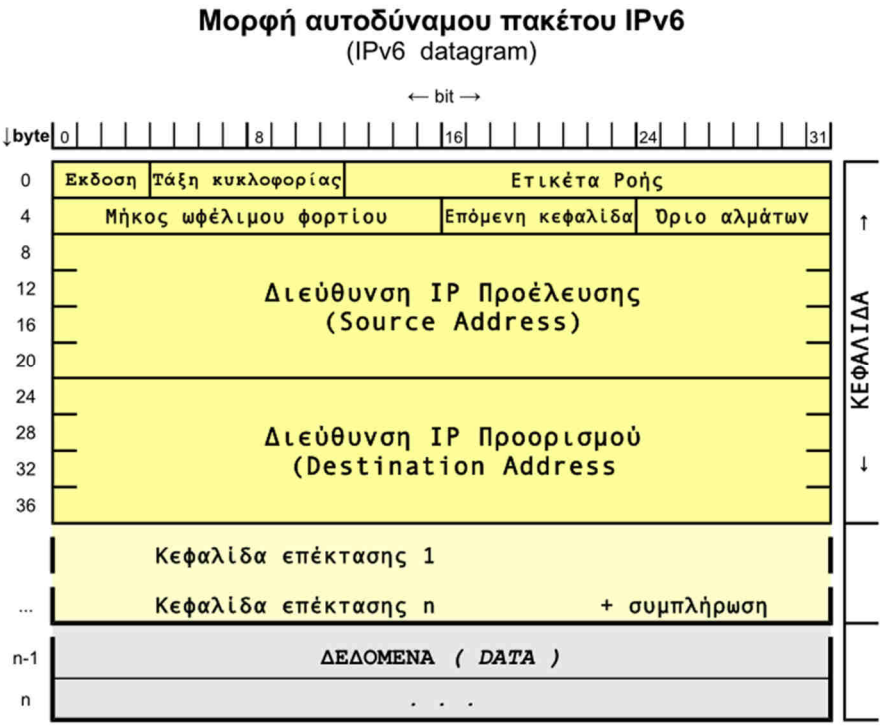
Η διαδικασία επιταχύνεται καθώς δεν χρειάζεται να υπολογίζεται **άθροισμα ελέγχου της επικεφαλίδας** (δεν υπάρχει στο IPv6) σε κάθε δρομολογητή.

Επίσης δεν επιτρέπεται η **διάσπαση-κατάτμηση πακέτων** στους ενδιάμεσους δρομολογητές.

Επιπλέον το πεδίο “Ετικέτα Ροής” επιτρέπει στο IPv6 να χειρίζεται καλύτερα **προτεραιότητες** σε υπηρεσίες πραγματικού χρόνου όπως μετάδοση φωνής και βίντεο.

Οι υπηρεσίες που παρέχει το πρωτόκολλο Διαδικτύου IPv4 (επίπεδο διαδικτύου) στους δύο τερματικούς κόμβους-υπολογιστές οφείλουν να προσφέρονται χωρίς επέμβαση των ενδιάμεσων κόμβων στη μεταξύ τους “συνομιλία”. Αυτό είναι σημαντικό από πλευράς ασφαλείας όμως δεν είναι πάντα εφικτό καθώς μεγάλο μέρος των διασυνδεδεμένων στο

Διαδίκτυο υπολογιστών χρησιμοποιούν ιδιωτικές διευθύνσεις IPv4 και βρίσκονται πίσω από δρομολογητές που εκτελούν **μετάφραση διευθύνσεων** (Network Address Translation - **NAT**). Αυτό δημιουργεί **προβλήματα στη χρήση ασφαλών πρωτοκόλλων** (IPsec) τα οποία στηρίζονται στην παγκόσμια μοναδικότητα των διευθύνσεων IP των τερματικών κόμβων. Αυτό όμως δεν ισχύει με τις ιδιωτικές διευθύνσεις IPv4. Εδώ πρέπει να σημειωθεί ότι και η λειτουργία NAT είναι ένα μέτρο για οικονομία διευθύνσεων IPv4 λόγω του κινδύνου εξαντλήσεώς τους. Το IPv6 έχει τη δυνατότητα να προσφέρει σε κάθε δικτυακή διασύνδεση σε κάθε υπολογιστή στον κόσμο **μια μοναδική διεύθυνση IPv6**.



Εικόνα 3.5.α: Μορφή αυτοδύναμου πακέτου IPv6

Με διευθύνσεις μήκους 128 bit μπορεί να διαθέσει (θεωρητικά) συνολικά $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$ ή περίπου $3{,}403\,x\,10^{34}$ διευθύνσεις (~340 εν δεκάκις εκατομμύρια)

Στο διάγραμμα με τη μορφή του πακέτου του πρωτοκόλλου Διαδικτύου IPv6 φαίνεται το μεγαλύτερο μήκος των πεδίων διεύθυνσης προέλευσης και προορισμού (16 οκτάδες ή 128 bit) και η απλούστερη δομή του, με λιγότερα πεδία τα οποία ευνοούν την αποδοτικότερη δρομολόγηση.

3.5.1 Τρόπος γραφής διεύθυνσης IPv6

Μια **διεύθυνση IPv6**, 128 bit σε δυαδική μορφή είναι η:

```
0010000000000001 0000110110111000  0000000000000000 0000000000000000
0000000000000001 0000000000000000  0000000000000000 0000000000000001
```

όπως είναι φανερό, σε αυτή τη μορφή είναι πρακτικά αδύνατο να χρησιμοποιηθεί. Στο IPv4 (32 bit) τα ψηφία ομαδοποιούνταν σε οκτάδες και γράφονταν στο δεκαδικό. Ο πιο αποδοτικός (λιγότερα ψηφία) τρόπος γραφής ενός δυαδικού αριθμού είναι η γραφή του στο δεκαεξαδικό. Τέσσερα δυαδικά ψηφία γράφονται ακριβώς με ένα δεκαεξαδικό ψηφίο. Δηλαδή 16 bit γράφονται με τέσσερα (4) δεκαεξαδικά ψηφία.

Σύμφωνα με το RFC4291 που αφορά στην αρχιτεκτονική της διευθυνσιοδότησης στο IPv6 και και το RFC5952 το οποίο υποδεικνύει τον τρόπο γραφής μιας διεύθυνσης IPv6, τα 128 bit:

- χωρίζονται σε οκτώ δεκαεξάδες,
- η κάθε μια γράφεται στο δεκαεξαδικό με τέσσερα ψηφία (τα ψηφία a,b,c,d,e,f γράφονται με πεζά-μικρά γράμματα) και
- χωρίζεται από τη διπλανή της με άνω-κάτω τελεία.

η διεύθυνση του παραδείγματος γίνεται:

2001:0db8:0000:0000:0001:0000:0000:0001

Επιπλέον, παραλείπονται τα αρχικά μηδενικά (leading zeros) σε κάθε τετράδα δεκαεξαδικών αριθμών. Έτσι η διεύθυνση γράφεται:

2001:db8:0:0:1:0:0:1

Επίσης δίνεται η δυνατότητα παράλειψης δύο ή περισσοτέρων συνεχόμενων μηδενικών δεκαεξάδων και αντικατάστασής τους με δυο συνεχόμενες άνω-κάτω τελείες **"::"** Το σύμβολο **"::"** όμως πρέπει να εμφανίζεται **μόνο μια φορά** στη διεύθυνση. Μια μόνο μηδενική δεκαεξάδα δεν αντικαθίσταται από το **"::"**. Έτσι η διεύθυνση ξαναγράφεται:

2001:db8::1:0:0:1

εάν όπως στην παραπάνω περίπτωση υπάρχουν δυο σημεία στο οποία εμφανίζονται συνεχόμενες μηδενικές δεκαεξάδες τότε η αντικατάσταση εφαρμόζεται στις περισσότερες ή αν είναι ίσες στον αριθμό, στις πρώτες (αριστερά).

~~**2001:db8:0:0:1::1**~~

Στο πρωτόκολλο Διαδικτύου IPv6 υπάρχουν τρεις τύποι διευθύνσεων:

Τύπος Διεύθυνσης IPv6	**Περιγραφή**
Αποκλειστικής διανομής (unicast)	Η διεύθυνση προσδιορίζει μια συγκεκριμένη δικτυακή διεπαφή (κάρτα δικτύου - interface) ενός υπολογιστή. Πακέτο που αποστέλλεται σε αυτή, **παραδίδεται στη συγκεκριμένη** δικτυακή διασύνδεση.
Μη αποκλειστικής διανομής (anycast)	Η διεύθυνση προσδιορίζει μια ομάδα δικτυακών διεπαφών (interfaces) οι οποίες τυπικά ανήκουν σε διαφορετικούς κόμβους. Πακέτο που αποστέλλεται σε αυτή, **παραδίδεται σε ένα από τα μέλη της ομάδας**, το "πλησιέστερο" σύμφωνα με την εκτίμηση των πρωτοκόλλων δρομολόγησης.
Πολυδιανομής (multicast)	Η διεύθυνση προσδιορίζει μια ομάδα δικτυακών διεπαφών (interfaces) οι οποίες τυπικά ανήκουν σε διαφορετικούς κόμβους. Πακέτο που αποστέλλεται σε αυτή, **παραδίδεται σε όλα τα μέλη της ομάδας**.

Πίνακας 3.5.1.α: Τύποι διευθύνσεων IPv6

Δεν υπάρχει η έννοια της εκπομπής (broadcast). Η εκπομπή αντιμετωπίζεται ως ειδική περίπτωση πολυδιανομής.

Στη γενική τους μορφή οι διευθύνσεις IPv6 μπορεί να θεωρηθεί ότι αποτελούνται από δυο τμήματα, όπως και οι διευθύνσεις IPv4. Το αναγνωριστικό δικτύου ή υποδικτύου ή πρόθεμα (prefix) και το τμήμα του υπολογιστή.

2100	:0	:0	:0	:4d	:31ac	:12	:45

Δίκτυο *(prefix)*	***Υπολογιστής*** *(interface ID)*

Χρησιμοποιείται και εδώ η σημειογραφία CIDR με τον αριθμό μετά την κάθετη "/" να δηλώνει στο δεκαδικό σύστημα τον αριθμό των ψηφίων του προθέματος τα οποία είναι σημαντικά για τη δρομολόγηση:

`2100:0:0:0:4d:31ac:12:45/64` ή **`2100::4d:31ac:12:45/64`**

με αναγνωριστικό (υπο-)δικτύου: **`2100::/64`**

Στις διευθύνσεις καθολικής αποκλειστικής διανομής (unicast) το πρόθεμα μπορεί να αναλύεται σε επιπλέον τμήματα:

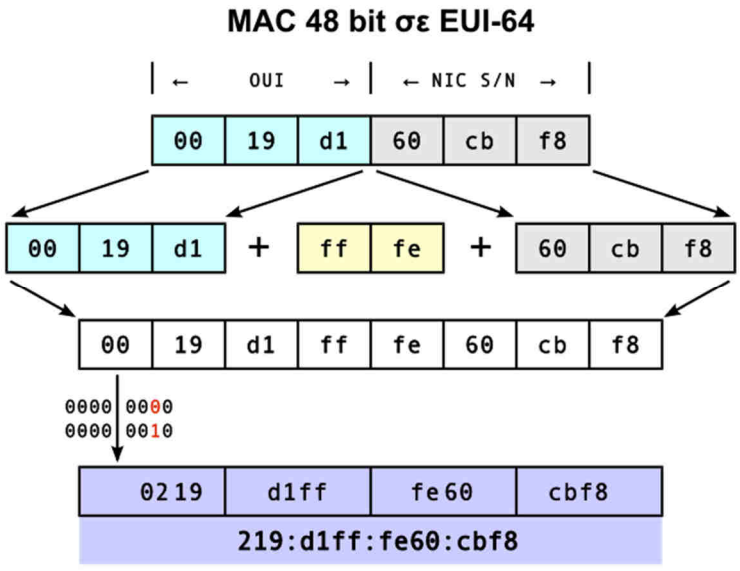
2100	:0	:0	:0	:4d	:31ac	:12	:45

prefix	***sub-net***	***interface ID***

Το αναγνωριστικό της δικτυακής διεπαφής (interface ID) προέρχεται από τη φυσική διεύθυνση της διασύνδεσης με τη μορφή EUI-64 του IEEE

Η μορφή EUI-64 δηλαδή το **εκτεταμένο μοναδικό αναγνωριστικό** των 64 bit (Extented Unique Identifier EUI-64), εφόσον δεν είναι εξαρχής 64 bit, σε μια απλή κάρτα δικτύου, προκύπτει από τη φυσική διεύθυνση (48 bit MAC address) με την εξής διαδικασία:

- Η διεύθυνση MAC χωρίζεται στο μέσον σε δυο ίσα τμήματα (24 + 24 bit ή 3 + 3 byte)
- παρεμβάλλεται η ακολουθία **`11111111 11111110`** (στο δυαδικό) ή **`fffe`** (στο δεκαεξαδικό)
- στην πρώτη οκτάδα αλλάζει το 7ο από αριστερά bit (b6) σε 1
- γράφεται ομαδοποιημένη σε τετράδες δεκαεξαδικών αριθμών χωρισμένες με **`"::"`** ακολουθώντας τους συντακτικούς κανόνες γραφής διευθύνσεων IPv6.



Εικόνα 3.5.1.α: Μεταγραφή διεύθυνσης MAC 48 bit σε EUI-64

Ο τύπος της διεύθυνσης αναγνωρίζεται από τα υψηλότερης τάξης ψηφία (αριστερά) της διεύθυνσης ως εξής:

Τύπος Διεύθυνσης	**Πρόθεμα** (δυαδικό)	**Σημειογραφία IPv6**
Ακαθόριστη (Unspecified)	**00...0 (128 bits)**	**::/128**
Επανατροφοδότησης (Loopback)	**00...1 (128 bits)**	**::1/128**
Πολυδιανομής (Multicast)	**11111111**	**ff00::/8**
Τοπικές δ/νσεις ζεύξης αποκλειστικής διανομής (Link-Local unicast)	**1111111010**	**fe80::/10**
Καθολική δ/νση αποκλειστικής διανομής (Global unicast)	οτιδήποτε άλλο	

Πίνακας 3.5.1.β: Αναγνώριση τύπων δ/νσεων IPv6

Κατά την εκκίνηση, ένας υπολογιστής ο οποίος υποστηρίζει το πρωτόκολλο IPv6 **ρυθμίζεται αυτόματα** (autoconfiguration) παίρνοντας μια Τοπική δ/νση ζεύξης αποκλειστικής διανομής (Link-Local unicast) ώστε να έχει τη δυνατότητα δικτυακής επικοινωνίας σε επίπεδο τοπικού δικτύου. Η διεύθυνση αυτή έχει τη μορφή:

1111111010 + 54 μηδενικά + EUI-64

Για παράδειγμα, για την κάρτα δικτύου με φυσική διεύθυνση **00:19:d1:60:cb:f8** η τοπική δ/νση ζεύξης αποκλειστικής διανομής (Link-Local unicast) είναι η **fe80::219:d1ff:fe60:cbf8** σημαντικά για τη δρομολόγηση

3.5.2 Ειδικές διευθύνσεις IPv6

Διεύθυνση επανατροφοδότησης (Loopback)**, ::1/128** Αναφέρεται στον ίδιο τον τοπικό υπολογιστή. Ένας υπολογιστής, ακόμη κι αν δεν έχει καμιά δικτυακή διασύνδεση στέλνοντας πακέτα με **προορισμό** (destination) τη διεύθυνση **::1** αυτά διεκπεραιώνονται πίσω (επανατροφοδοτούνται) στον ίδιο του τον εαυτό. Αντιστοιχεί στην 127.0.0.1/32 του IPv4.

0:0:0:0:0:0:0:0 ή ::/128 (unspecified): Συναντάται μόνον ως διεύθυνση **προέλευσης** (source) και δηλώνει πακέτα του "ίδιου" του υπολογιστή. Έχει την ίδια σημασία με την αντίστοιχη του IPv4, 0.0.0.0/32 (Limited source)

fe80::/64 (Link local unicast): Τοπική δ/νση ζεύξης αποκλειστικής διανομής. Ρυθμίζεται αυτόματα. Έχει σημασία αντίστοιχη της 169.254.0.0/16 (Link local) του IPv4. Σε έναν υπολογιστή είναι το πρόθεμα **fe80::/64 συνοδευόμενο από τη διεύθυνση MAC (48 bit) μεταγραμμένη σε μορφή EUI-64. Για παράδειγμα στον υπολογιστή με φυσική διεύθυνση MAC** 00-19-d1-60-cb-f8 **η οποία σε EUI-64 γίνεται** 02-19-d1-ff-fe-60-cb-f8**, η τοπική δ/νση ζεύξης αποκλειστικής διανομής είναι fe80::219:d1ff:fe60:cbf8. Τα windows δεν ακολουθούν αυτή την πρακτική. Αντί αυτής δημιουργούν, αυτόματα, ένα τυχαίο interface ID.**

ff00::/8 (Multicast): Διεύθυνση πολυδιανομής. Αντίστοιχη λειτουργία στο IPv4 έχουν οι διευθύνσεις κλάσης D, 224.0.0.0/4.

3.6 Δρομολόγηση

Το επίπεδο Διαδικτύου (στο μοντέλο TCP/IP), εκτός από τη **διευθυνσιοδότηση**, είναι επιφορτισμένο και με τη **δρομολόγηση** των αυτοδύναμων πακέτων (datagrams) ώστε να

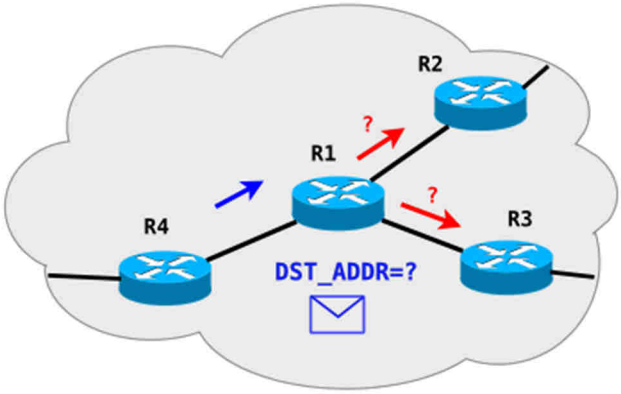
εξασφαλίσει την επικοινωνία μεταξύ των δυο ακραίων υπολογιστών του δικτύου (host to host). Να παρέχει, δηλαδή, το απαιτούμενο **επικοινωνιακό υποδίκτυο**. Η δρομολόγηση έχει έννοια όταν μεταξύ των ακραίων υπολογιστών μεσολαβεί τουλάχιστον ένας δρομολογητής. Σε αντίθετη περίπτωση είναι διαθέσιμες και άλλες τεχνικές (μεταγωγή - switching, γεφύρωση - bridging) οι οποίες μπορούν να υλοποιηθούν από το 2ο επίπεδο του OSI και αναφέρονται στο ίδιο φυσικό δίκτυο.

Δρομολόγηση είναι το έργο της μετακίνησης (προώθησης, διεκπεραίωσης) της πληροφορίας από την αφετηρία μέσω ενός διαδικτύου και παράδοσης στον προορισμό της. Η δρομολόγηση περιλαμβάνει δυο διακριτές δραστηριότητες

- τον προσδιορισμό της καλύτερης διαδρομής από την αφετηρία έως τον προορισμό και
- την μεταφορά (προώθηση - IP forwarding) της ομαδοποιημένης, σε πακέτα, πληροφορίας στον προορισμό της, διαμέσου του Διαδικτύου.

Η δεύτερη δραστηριότητα, η μεταφορά-προώθηση των πακέτων δεν είναι ιδιαίτερα πολύπλοκη και η υλοποίησή της είναι σχετικά εύκολη. Η πρώτη όμως, ο προσδιορισμός της διαδρομής, μπορεί να καταλήξει σε ιδιαίτερα σύνθετο πρόβλημα το οποίο καλούνται να αντιμετωπίσουν τα **πρωτόκολλα δρομολόγησης**.

Τα πρωτόκολλα δρομολόγησης χρησιμοποιούν μετρήσιμα χαρακτηριστικά για να εκτιμήσουν ποια διαδρομή είναι καλύτερη για ένα πακέτο. Τέτοια είναι το εύρος ζώνης (ταχύτητα) των γραμμών της διαδρομής, η σχετική απόσταση (αριθμός των αλμάτων ή κόμβων) έως τον προορισμό κ.ά. Η εκτίμηση της βέλτιστης διαδρομής προς τον προορισμό γίνεται από τους **αλγόριθμους** που χρησιμοποιούνται από τα πρωτόκολλα δρομολόγησης.



Εικόνα 3.6.α: Προώθηση πακέτων IP

Με τη βοήθεια των αλγορίθμων συντάσσουν τους **πίνακες δρομολόγησης** οι οποίοι περιέχουν πληροφορίες δρομολογίων. Οι πληροφορίες δρομολογίων ποικίλουν ανάλογα με τον χρησιμοποιούμενο αλγόριθμο.

Οι αλγόριθμοι δρομολόγησης ενημερώνουν στους πίνακες δρομολόγησης μια ποικιλία πληροφοριών. Οι βασικότερες είναι οι αντιστοιχίσεις προορισμού και **επόμενου άλματος** (next hop) οι οποίες λένε στο δρομολογητή σε ποια δικτυακή διασύνδεση να προωθήσει ένα εισερχόμενο πακέτο. Όταν ένας δρομολογητής παραλαμβάνει ένα εισερχόμενο πακέτο εξετάζει την διεύθυνση προορισμού και προσπαθεί να την ταιριάξει με μια εγγραφή επόμενου άλματος στον πίνακα δρομολόγησης. Στη συνέχεια προωθεί το πακέτο από την αντίστοιχη δικτυακή διασύνδεση.

Αυτό σημαίνει ότι η λήψη αποφάσεων για τη διαδρομή που θα ακολουθήσουν τα αυτοδύναμα πακέτα επαναλαμβάνεται για κάθε πακέτο χωριστά και υπάρχει το

ενδεχόμενο πακέτα για τον ίδιο προορισμό να ακολουθήσουν σε διαφορετικές χρονικές στιγμές διαφορετικές διαδρομές.

Οι πίνακες δρομολόγησης περιέχουν και πληροφορίες οι οποίες εκφράζουν το βαθμό προτίμησης μιας διαδρομής (του επόμενου άλματος).

Οι δρομολογητές επικοινωνούν μεταξύ τους ανταλλάσσοντας μηνύματα και ενημερώνουν τους πίνακες δρομολόγησής τους. Τα μηνύματα ενημέρωσης μπορεί να είναι μέρος του πίνακα δρομολόγησης ή ολόκληρος. Ένας δρομολογητής αναλύοντας τα μηνύματα ενημέρωσης άλλων δρομολογητών μπορεί να σχηματίσει μια λεπτομερή εικόνα της τοπολογίας και της τρέχουσας κατάστασης των συνδέσεων του Διαδικτύου. Έτσι είναι σε θέση να προσδιορίζει τις βέλτιστες διαδρομές προς διάφορους προορισμούς του Διαδικτύου.

Το πρωτόκολλο IP χρησιμοποιεί αυτοδύναμα πακέτα (datagrams) και είναι σχεδιασμένο να λειτουργεί σε όλους τους τύπους υλικού δικτύου. Αν και κάνει τη βέλτιστη προσπάθεια (best effort) για να επιδώσει το κάθε αυτοδύναμο πακέτο, το υποκείμενο υλικό δικτύου μπορεί να λειτουργήσει λανθασμένα. Έτσι δεν εγγυάται ότι μπορεί να αντιμετωπίσει τα παρακάτω προβλήματα:

- Επανάληψη αυτοδύναμου πακέτου
- Επίδοση με καθυστέρηση ή εκτός σειράς
- Αλλοίωση δεδομένων
- Απώλεια αυτοδύναμου πακέτου

Για την αντιμετώπιση τέτοιων σφαλμάτων υπεύθυνα είναι τα ανώτερα στρώματα δικτύωσης.

3.6.1 Άμεση/Έμμεση

Στη βασική της αρχή, η δρομολόγηση είναι πολύ απλή. Ο αρχικός υπολογιστής, ο αποστολέας, ο οποίος δημιουργεί τα αυτοδύναμα πακέτα (datagrams), εξετάζει την διεύθυνση IP προορισμού. Εάν δεν είναι τοπική (δεν έχει ως προορισμό υπολογιστή ο οποίος βρίσκεται στο ίδιο δίκτυο) τότε ο αποστολέας αναζητά έναν δρομολογητή ο οποίος (ελπίζει να) βρίσκεται στη σωστή κατεύθυνση προς τον προορισμό και στέλνει τα πακέτα σε αυτόν. Ο δρομολογητής ουσιαστικά εκτελεί την ίδια διαδικασία. Κάθε δρομολογητής κατά μήκος της διαδρομής επαναλαμβάνει τη διαδικασία μέχρι το πακέτο να φτάσει σε έναν δρομολογητή ο οποίος βρίσκεται στο ίδιο φυσικό δίκτυο με τον υπολογιστή στον οποίο ανήκει η διεύθυνση προορισμού. Εκεί παραδίδεται το πακέτο.

Τα πράγματα φαίνονται απλά, ωστόσο πολύ γρήγορα περιπλέκονται καθώς τα δίκτυα μεγαλώνουν σε έκταση μαζί με τις ανάγκες χωρητικότητας των γραμμών επικοινωνίας.

Αναφέρθηκε ότι ο αρχικός υπολογιστής, ο αποστολέας, εξετάζει την διεύθυνση IP προορισμού. Αυτό που κάνει, στην πραγματικότητα, είναι λογικό ΚΑΙ (AND) της διεύθυνσης IP προορισμού με τη μάσκα δικτύου για να βρει τη διεύθυνση του δικτύου προορισμού. Στη συνέχεια τη συγκρίνει με τη δική του διεύθυνση δικτύου. Αν είναι ίδιες τότε συμπεραίνει ότι ο υπολογιστής προορισμού βρίσκεται στο ίδιο δίκτυο. Στη συνέχεια καλεί το πρωτόκολλο ARP για να μάθει τη φυσική διεύθυνση που αντιστοιχεί στη διεύθυνση IP προορισμού, ενθυλακώνει το πακέτο σε ένα πλαίσιο και το στέλνει στον προορισμό του. Στην περίπτωση αυτή οι υπολογιστές προέλευσης και προορισμού βρίσκονται στο ίδιο δίκτυο, δεν μεσολαβεί δρομολογητής και η διαδικασία χαρακτηρίζεται **άμεση δρομολόγηση**

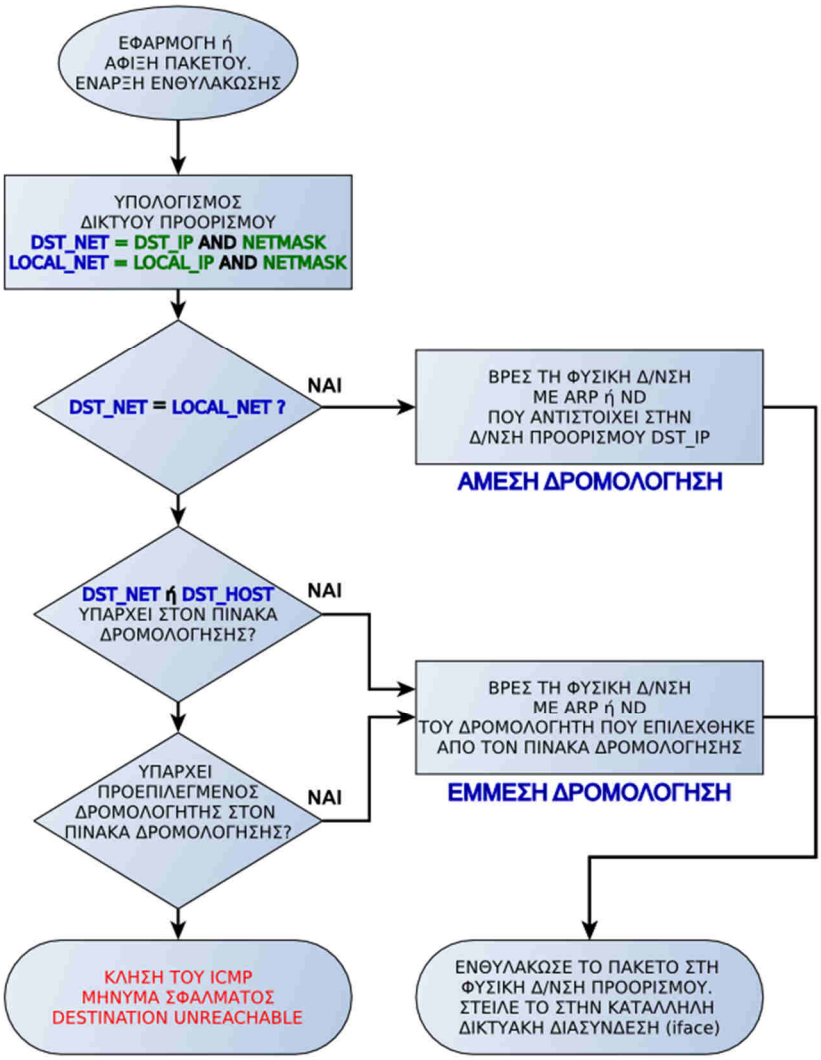
Εάν κατά την εξέταση της διεύθυνσης IP προορισμού διαπιστώσει ότι ο υπολογιστής προορισμού βρίσκεται σε διαφορετικό δίκτυο τότε αναζητά στον πίνακα δρομολόγησης μια καταχώριση η οποία να αναφέρεται είτε στη διεύθυνση είτε στη διεύθυνση δικτύου

προορισμού. Εκεί εντοπίζει τον αντίστοιχο δρομολογητή, καλεί το πρωτόκολλο ARP για να μάθει τη φυσική διεύθυνση που αντιστοιχεί στον δρομολογητή, ενθυλακώνει το πακέτο σε ένα πλαίσιο με προορισμό τη φυσική διεύθυνση του δρομολογητή και του το στέλνει για να συνεχίσει την προσπάθεια παράδοσης του πακέτου προς τον τελικό του προορισμό. Όταν οι υπολογιστές προέλευσης και προορισμού δεν βρίσκονται στο ίδιο δίκτυο και μεσολαβούν ανάμεσά τους ένας ή περισσότεροι δρομολογητές τότε η διαδικασία χαρακτηρίζεται **έμμεση δρομολόγηση**

Συνήθως υπάρχει ένας **προεπιλεγμένος δρομολογητής** (default router, default gateway) ώστε εάν δεν ταιριάζει κάποια από όλες τις άλλες καταχωρίσεις του πίνακα δρομολόγησης με το δίκτυο ή τη διεύθυνση IP προορισμού να παραδίδεται το πακέτο για διεκπεραίωση σε αυτόν.

Εάν η διεύθυνση προορισμού δεν ανήκει στο ίδιο δίκτυο με τον αποστολέα, δεν υπάρχει καταχώριση γι αυτήν και το δίκτυό της στον πίνακα δρομολόγησης και δεν έχει οριστεί προεπιλεγμένος δρομολογητής τότε το δίκτυο αδυνατεί να προχωρήσει τη διαδικασία δρομολόγησης και πληροφορεί τον αποστολέα, κάνοντας χρήση του πρωτοκόλλου ICMP, ότι ο προορισμός δεν είναι προσβάσιμος.

Το παρακάτω διάγραμμα ροής στο σχήμα 3.6.1.α εμφανίζει παραστατικά τη διαδικασία της δρομολόγησης, άμεσης ή έμμεσης.



Σχήμα 3.6.1.α: Διαδικασία δρομολόγησης αυτοδύναμου πακέτου

3.6.2 Πίνακας δρομολόγησης

Κεντρικό ρόλο στη διαδικασία της δρομολόγησης παίζει ο πίνακας δρομολόγησης. Είναι η καρδιά του αλγόριθμου δρομολόγησης. Βρίσκεται στη μνήμη του υπολογιστή ή δρομολογητή και σε κάθε γραμμή του περιλαμβάνει απαραίτητα:

- μια **διεύθυνση δικτύου προορισμού** ή υπολογιστή προορισμού (σπανιότερα) συνοδευόμενη από τη μάσκα δικτύου. Είναι το κλειδί αναζήτησης στον πίνακα,
- τη **διεύθυνση του επόμενου δρομολογητή** (επόμενο άλμα - next hop) προς αυτόν τον προορισμό και
- τη **δικτυακή διεπαφή** (interface) μέσω της οποίας είναι προσβάσιμος ο επόμενος δρομολογητής.

Συνήθως περιλαμβάνει και άλλες πληροφορίες όπως την τιμή μέτρησης (metric) για το βαθμό προτίμησης του συγκεκριμένου δρομολογητή.

Ο πίνακας δρομολόγησης αρχικοποιείται κατά την εκκίνηση του υπολογιστή ή δρομολογητή από ρυθμίσεις που είναι αποθηκευμένες σε αρχεία ρυθμίσεων. Στη συνέχεια μπορεί να παραμένει στατικός ή να μεταβάλλεται διαρκώς εφόσον έχει ρυθμιστεί να ενημερώνεται δυναμικά από τα πρωτόκολλα δρομολόγησης.

Πίνακας δρομολόγησης (το βασικό μέρος) σε υπολογιστή με windows7

```
C:\Windows\System32\drivers\etc>route -4 print

...

IPv4 Πίνακας διαδρομών

===========================================================================

Ενεργές διαδρομές:

Διεύθυνση δικτύου    Μάσκα δικτύου            Πύλη      Διασύνδεση   Μέτρο

          0.0.0.0          0.0.0.0      192.168.1.1     192.168.1.11     30

        127.0.0.0        255.0.0.0      Με σύνδεση        127.0.0.1    306

        127.0.0.1  255.255.255.255      Με σύνδεση        127.0.0.1    306

  127.255.255.255  255.255.255.255      Με σύνδεση        127.0.0.1    306

      192.168.1.0    255.255.255.0      Με σύνδεση     192.168.1.11    286

     192.168.1.11  255.255.255.255      Με σύνδεση     192.168.1.11    286

    192.168.1.255  255.255.255.255      Με σύνδεση     192.168.1.11    286

        224.0.0.0        240.0.0.0      Με σύνδεση        127.0.0.1    306

        224.0.0.0        240.0.0.0      Με σύνδεση     192.168.1.11    286

  255.255.255.255  255.255.255.255      Με σύνδεση        127.0.0.1    306

  255.255.255.255  255.255.255.255      Με σύνδεση     192.168.1.11    286

===========================================================================
```

Πίνακας 3.6.2.α: Πίνακας δρομολόγησης IPv4 σε υπολογιστή με Λ.Σ Windows

Για παράδειγμα, με βάση τον παραπάνω πίνακα, αν η διεύθυνση προορισμού είναι 192.168.1.65 τότε:

- φτιάχνεται αυτοδύναμο πακέτο IP με διεύθυνση προέλευσης την 192.168.1.11 και διεύθυνση προορισμού την 192.168.1.65
- η διεύθυνση 192.168.1.65 με μάσκα 255.255.255.0 ανήκει στο δίκτυο 192.168.1.0
- για το δίκτυο 192.168.1.0 η πέμπτη γραμμή του πίνακα δείχνει στη στήλη "Πύλη" ότι δεν απαιτείται χρήση δρομολογητή, είναι "Με σύνδεση"
- το πακέτο θα προωθηθεί για άμεση δρομολόγηση από τη Διασύνδεση με διεύθυνση IP 192.168.1.11
- Θα κληθεί το πρωτόκολλο ARP να πληροφορήσει για τη φυσική διεύθυνση του υπολογιστή με IP 192.168.1.65
- Θα φτιαχτεί ένα πλαίσιο με διεύθυνση προέλευσης τη φυσική διεύθυνση της διασύνδεσης 192.168.1.11 και διεύθυνση προορισμού τη φυσική διεύθυνση του 192.168.1.65
- Το πλαίσιο στέλνεται στο τοπικό δίκτυο

Σε άλλη περίπτωση, έστω ότι η διεύθυνση προορισμού είναι 147.102.222.211, τότε:

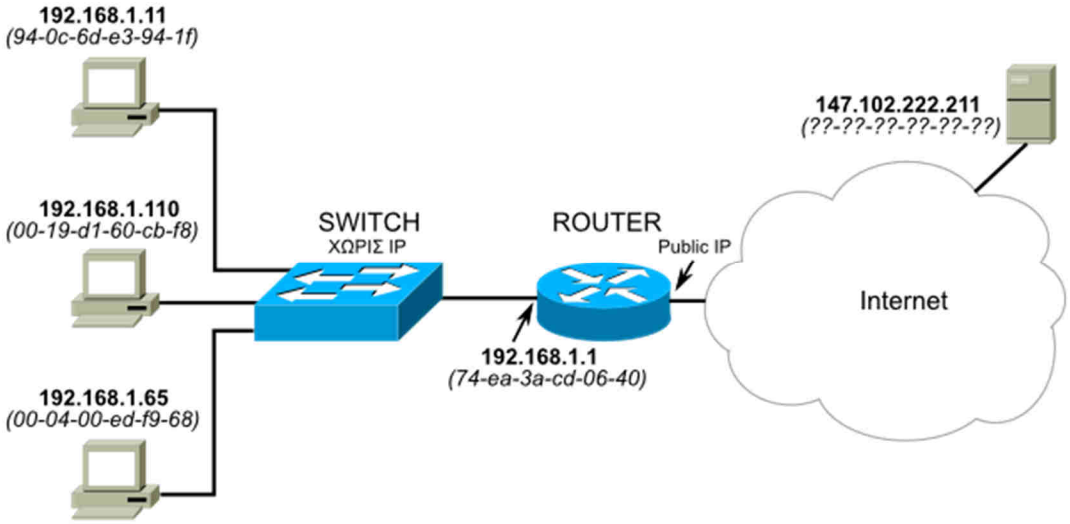
- φτιάχνεται αυτοδύναμο πακέτο IP με διεύθυνση προέλευσης την 192.168.1.11 και διεύθυνση προορισμού την 147.102.222.211
- η διεύθυνση 147.102.222.211 με μάσκα 255.255.255.0 δίνει διεύθυνση δικτύου 147.102.222.0 ≠ 192.168.1.0 δηλαδή διαφορετικό δίκτυο από το τοπικό.
- για το δίκτυο 147.102.222.0 δεν υπάρχει καταχώριση στον πίνακα δρομολόγησης
- υπάρχει όμως προεπιλεγμένη "Πύλη" (0.0.0.0) και είναι η 192.168.1.1 η οποία βρίσκεται στο ίδιο δίκτυο
- Θα κληθεί το πρωτόκολλο ARP να πληροφορήσει για τη φυσική διεύθυνση της προεπιλεγμένης πύλης με IP 192.168.1.1
- Θα φτιαχτεί ένα πλαίσιο με διεύθυνση προέλευσης τη φυσική διεύθυνση της διασύνδεσης 192.168.1.11 και διεύθυνση προορισμού τη φυσική διεύθυνση του 192.168.1.1
- Το πλαίσιο στέλνεται στο τοπικό δίκτυο

Λαμβάνοντας υπόψη τον πίνακα ARP της ενότητας 3.3 και ότι η δικτυακή διασύνδεση 192.168.11 έχει φυσική διεύθυνση την 94-0c-6d-e3-94-1f (δεν φαίνεται στον πίνακα ARP επειδή αφορά την ίδια, η ARP cache περιέχει τις φυσικές διευθύνσεις των άλλων συνδέσεων) η διαδικασία της ενθυλάκωσης για τις δυο περιπτώσεις δρομολόγησης φαίνεται συγκεντρωτικά στον παρακάτω πίνακα 3.6.2.β:

		ΔΙΕΥΘΥΝΣΕΙΣ	
Προορισμός	Ενθυλάκωση σε ...	***Προέλευσης***	***Προορισμού***
192.168.1.65 /24 **192.168.1.0**	**Αυτοδύναμο πακέτο IP**	192.168.1.11	192.168.1.65
	Πλαίσιο Ethernet	94-0c-6d-e3-94-1f	00-04-00-ed-f9-68
147.102.222.211 /24 **147.102.222.0**	**Αυτοδύναμο πακέτο IP**	192.168.1.11	147.102.222.211
	Πλαίσιο Ethernet	94-0c-6d-e3-94-1	74-ea-3a-cd-06-40 *(192.168.1.1)*

Πίνακας 3.6.2.β: Πακέτα και πλαίσια κατά τη δρομολόγηση, σύμφωνα με το παράδειγμα

Η διάταξη του δικτύου φαίνεται στο παρακάτω διάγραμμα της εικόνας 3.6.2.α.



Εικόνα 3.6.2.α: Διάταξη του δικτύου του παραδείγματος

Πίνακας δρομολόγησης σε υπολογιστή με linux

```
george@perseus:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.146.0.1      0.0.0.0         UG    0      0        0 eth0
10.146.0.0      0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.210.0.0      10.210.5.1      255.255.0.0     UG    0      0        0 eth1
10.210.5.0      0.0.0.0         255.255.255.0   U     0      0        0 eth1
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eth0
```

Πίνακας 3.6.2.γ: Πίνακας δρομολόγησης IPv4 σε υπολογιστή με Λ.Σ. linux

Ο συγκεκριμένος πίνακας δρομολόγησης ανήκει σε υπολογιστή με δυο κάρτες δικτύου (eth0, eth1) ο οποίος είναι διασυνδεδεμένος με δυο διαφορετικά δίκτυα, με το 10.146.0.0/24 και με το 10.210.5.0/24 (υποδίκτυα δικτύου κλάσης Α). Στον πίνακα δρομολόγησης υπάρχουν δύο δρομολογητές, ο 10.210.5.1 προς το δίκτυο 10.210.0.0/16 και ο 10.146.0.1 (προεπιλεγμένος - 0.0.0.0) προς όλα τα άλλα δίκτυα.

Τα δίκτυα 10.146.0.0/24 και 10.210.5.0/24 είναι άμεσα προσβάσιμα (Gateway 0.0.0.0) από τις αντίστοιχες κάρτες δικτύου eth0 και eth1.

3.7 Πρωτόκολλα Δρομολόγησης

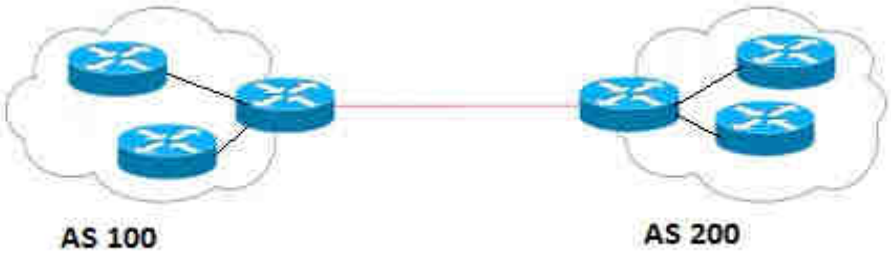
Από τη μέχρι τώρα περιγραφή της δρομολόγησης στα TCP/IP δίκτυα, βλέπουμε ότι ένα IP αυτοδύναμο πακέτο που ταξιδεύει στο Διαδίκτυο, μπορεί να περάσει από πολλούς δρομολογητές και δίκτυα μέχρι να φτάσει στον προορισμό του. Το μονοπάτι που ακολουθεί

δεν καθορίζεται από μία κεντρική αρχή, αλλά είναι αποτέλεσμα των οδηγιών που παίρνει από τους πίνακες δρομολόγησης που συναντά στο ταξίδι του. Κάθε δρομολογητής καθορίζει μόνο τον επόμενο σταθμό του αυτοδύναμου πακέτου και βασίζεται σε αυτόν, προκειμένου το αυτοδύναμο πακέτο να οδηγηθεί στον προορισμό του. Σε μικρά δίκτυα οι πίνακες δρομολόγησης γεμίζουν χειροκίνητα από τον διαχειριστή του δικτύου, ενώ σε μεγαλύτερα, το έργο αυτό έχει αυτοματοποιηθεί και πραγματοποιείται από το πρωτόκολλο δρομολόγησης, το οποίο μεταφέρει και κατανέμει την απαιτούμενη πληροφορία σε όλο το δίκτυο.

Τα **πρωτόκολλα δρομολόγησης** (routing protocols) είναι τεχνικές που χρησιμοποιούνται από τους δρομολογητές, για να επικοινωνήσουν ο ένας με τον άλλον και να ενημερώνονται για τις αλλαγές που σημειώνονται στις διαδρομές και στον τρόπο προσέγγισης των διαφόρων δικτύων. Τα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται για τον καθορισμό των διαδρομών, δηλαδή για τη συμπλήρωση των πινάκων δρομολόγησης, ποικίλουν και εξαρτώνται από τη δόμηση των δικτύων και τη σχέση που έχουν μεταξύ τους τα προς διασύνδεση δίκτυα. Επομένως, τα πρωτόκολλα δρομολόγησης είναι υπεύθυνα για:

- την επιλογή του καλύτερου δρόμου προς οποιοδήποτε δίκτυο/υποδίκτυο προορισμού
- την κατάλληλη ενημέρωση των πινάκων δρομολόγησης
- την ανταλλαγή πληροφοριών δρομολόγησης μεταξύ των δρομολογητών ενός δικτύου.

Η επικοινωνία ενός δικτύου με άλλα δίκτυα γίνεται μέσω συγκεκριμένων δρομολογητών που ονομάζονται **εξωτερικοί δρομολογητές** και χειρίζονται όλη την εισερχόμενη και εξερχόμενη κίνηση του δικτύου. Με αυτόν τον τρόπο, η εσωτερική δομή του δικτύου και των υποδικτύων του δεν είναι ορατή από τα υπόλοιπα δίκτυα που είναι συνδεδεμένα με αυτό. Τα δίκτυα, η εσωτερική δομή των οποίων δεν είναι ορατή από τον υπόλοιπο κόσμο, ονομάζονται **αυτόνομα συστήματα (AS - Autonomous Systems)**.



Σχήμα 3.7.α: Αυτόνομα Συστήματα

Οι μέθοδοι δρομολόγησης διακρίνονται σε **στατική** (static) και **δυναμική** (dynamic) δρομολόγηση.

Στατική δρομολόγηση. Οι διαδρομές που μαθαίνει ένας δρομολογητής στατικά, είναι σταθερές διαδρομές που μπορούν είτε να οριστούν άμεσα από τον διαχειριστή δικτύου, είτε να εισαχθούν αυτόματα από τον ίδιο τον δρομολογητή. Ο δρομολογητής ελέγχει τις ενεργές διεπαφές δικτύου που διαθέτει, καθορίζει τα δίκτυα που αντιστοιχούν σε κάθε διεπαφή και εισάγει τη σχετική πληροφορία στον πίνακα δρομολόγησης. Κατά τη στατική δρομολόγηση:

- Ο πίνακας δρομολόγησης δημιουργείται χειροκίνητα από τον διαχειριστή του δικτύου και αποθηκεύεται
- Ο διαχειριστής ενημερώνει τον πίνακα δρομολόγησης κάθε φορά που ενεργοποιείται μια νέα σύνδεση
- Οι δρομολογητές δεν ανταλλάσσουν πληροφορία

- Τα τερματικά συνήθως ξέρουν την IP διεύθυνση ενός προεπιλεγμένου (default) δρομολογητή
- Στα τερματικά γίνεται να δημιουργηθούν δυναμικά οι πίνακες δρομολόγησης μέσω του πρωτόκολλου ICMP (Internet Control Message Protocol)

Μειονεκτήματα στατικής δρομολόγησης:

- Για κάθε προορισμό δημιουργείται μια εγγραφή στον πίνακα δρομολόγησης του τερματικού
- Ακόμη και αν δυο τερματικά βρίσκονται στο ίδιο δίκτυο, δεν είναι δυνατόν να γίνει μια μόνο εγγραφή στον πίνακα δρομολόγησης
- Οι πίνακες που δημιουργούνται είναι μεγάλοι
  - Άσκοπη κατανάλωση μνήμης
  - Αύξηση του χρόνου αναζήτησης μιας διεύθυνσης μέσα στον πίνακα
- Η χειροκίνητη ενημέρωση πίνακα στους δρομολογητές παραμένει.

Δυναμική δρομολόγηση. Στα μεγαλύτερα δίκτυα η στατική δρομολόγηση είναι αρκετά σύνθετη και χρονοβόρα εργασία. Για το λόγο αυτό, στα μεγάλα δίκτυα χρησιμοποιείται η δυναμική μέθοδος δρομολόγησης. Με τη δυναμική μέθοδο δρομολόγησης, οι διαδρομές δημιουργούνται αυτόματα με τη χρήση διάφορων τεχνικών οι οποίες υλοποιούνται με πρωτόκολλα δρομολόγησης. Με τη χρήση δυναμικών πρωτοκόλλων, οι δρομολογητές μπορούν να ενημερώνονται αυτόματα για αλλαγές στο δίκτυο, ανταλλάσσοντας δεδομένα με γειτονικούς δρομολογητές. Κατά τη δυναμική δρομολόγηση γίνεται:

- Ανταλλαγή πληροφοριών μεταξύ γειτονικών δρομολογητών, σχετικών με τις τοπολογίες των δικτύων στα οποία οι δρομολογητές συνδέονται.
- Διαφοροποίηση ως προς την πληροφορία που εγγράφεται στους πίνακες δρομολόγησης
- Χρησιμοποίηση ενός αλγορίθμου δρομολόγησης, ο οποίος :
  - Χρησιμοποιεί πρωτόκολλα ανταλλαγής πληροφορίας δρομολόγησης:
    - Για εσωτερική δρομολόγηση (μέσα στα όρια ενός Αυτόνομου Συστήματος)
    - Για εξωτερική δρομολόγηση (μεταξύ Αυτόνομων Συστημάτων)
  - Ενημερώνει τους πίνακες με βάση την πληροφορία που λαμβάνει από πίνακες γειτονικών δρομολογητών
  - Καθορίζει την «πολιτική» δρομολόγησης (επιλέγει την καλύτερη διαδρομή προς τον προορισμό)

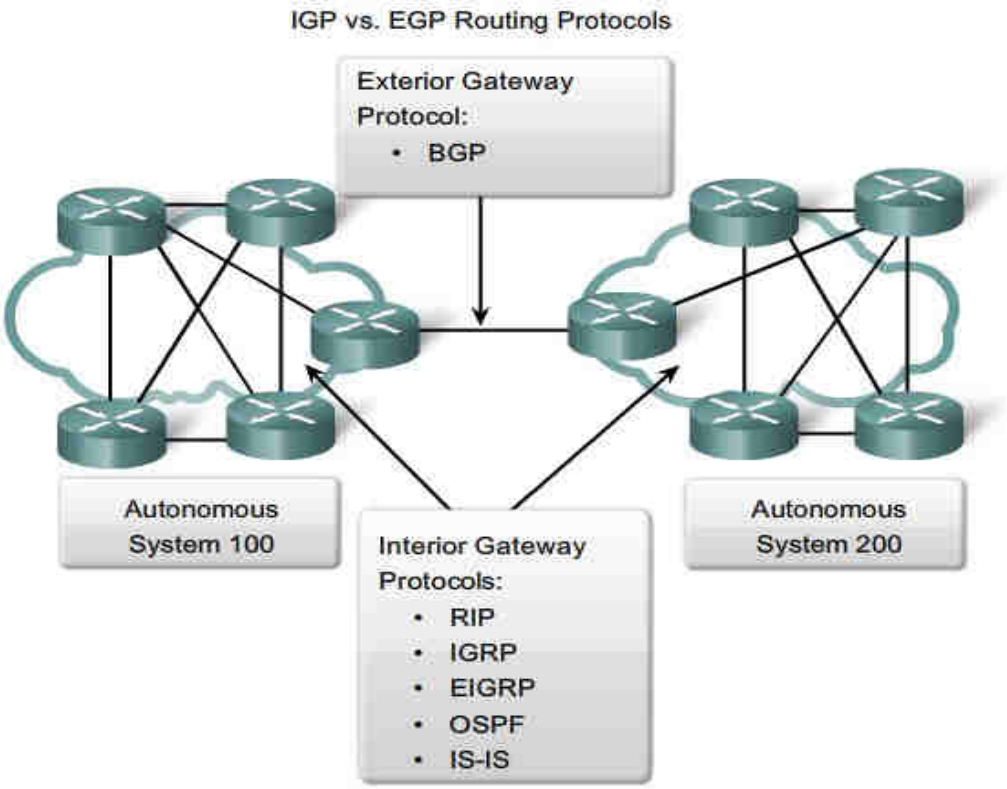
Υπάρχουν δυο βασικά είδη πρωτοκόλλων δυναμικής δρομολόγησης:

- **Τα Εσωτερικά Πρωτόκολλα Πύλης (IGP - Interior Gateway Protocols),** τα οποία χρησιμοποιούνται για την επικοινωνία των δρομολογητών και την ανταλλαγή των πινάκων δρομολόγησης τους σε ένα αυτόνομο σύστημα**.** Τυπικά πρωτόκολλα αυτής της κατηγορίας είναι το Πρωτόκολλο Πληροφορίας Δρομολόγησης **(RIP – Routing Information Protocol)** και το Πρωτόκολλο Βραχύτερου Μονοπατιού **(OSPF – Open Shortest Path First)**.
- **Τα Εξωτερικά Πρωτόκολλα Πύλης (EGP - Exterior Gateway Protocols)** τα οποία χρησιμοποιούνται για την επικοινωνία των δρομολογητών και την ανταλλαγή των πινάκων δρομολόγησης τους μεταξύ διαφορετικών αυτόνομων συστημάτων. Τυπικό πρωτόκολλο αυτής της κατηγορίας είναι το **BGP (Border Gateway Protocol)**.

Οι αλγόριθμοι στα εσωτερικά πρωτόκολλα πύλης (IGP) δυναμικής δρομολόγησης διακρίνονται σε δυο κατηγορίες:

- **Αλγόριθμοι Διανύσματος Απόστασης (Distance Vector Algorithms),** στους οποίους οι πίνακες δρομολόγησης αποτελούνται από μια σειρά από προορισμούς (vectors) και κόστη για τις αποστάσεις (distances) που διανύονται μέχρι την προσέγγιση του προορισμού (π.χ. RIP, IGRP).

- **Αλγόριθμοι Κατάστασης Σύνδεσης (Link State Algorithms)** (π.χ. OSPF).



Σχήμα 3.7.β: Χρήση πρωτοκόλλων IGP και EGP

(*Πηγή:http://mars.tekkom.dk/mediawiki/index.php/CCNA_Explorer_2_Introduction_to_Dynamic_Routing_Protocols*)

Βασική λειτουργία των πρωτοκόλλων δρομολόγησης, όπως προείπαμε, είναι η εύρεση και η επιλογή του καλύτερου δρόμου για τα δίκτυα προορισμού με τη χρήση κατάλληλων αλγορίθμων δρομολόγησης (routing algorithms). Ο αλγόριθμος δρομολόγησης δημιουργεί έναν αριθμό, τον οποίο ονομάζουμε **μετρικό (metric) κόστους,** για κάθε διαδρομή στο δίκτυο. Η διαδρομή με το μικρότερο κόστος για τον ίδιο προορισμό καταχωρείται τελικά στον πίνακα δρομολόγησης. Ανάλογα με την υλοποίηση, ως κόστος μπορεί να χρησιμοποιηθεί ο αριθμός των δρομολογητών (hop count) που περνά το μήνυμα μέχρι να φτάσει στον προορισμό του, το εύρος ζώνης της γραμμής (bandwidth), η καθυστέρηση (delay), το φορτίο της γραμμής (load) και μια σειρά άλλων παραμέτρων ή ένας συνδυασμός από αυτές.

Ερωτήσεις - Ασκήσεις Κεφαλαίου

1. Από τις παρακάτω διευθύνσεις IP σημειώστε ποιες είναι σωστές (ΣΩΣΤΗ) και ποιες λάθος (ΛΑΘΟΣ). Για τις σωστές, δώστε την κλάση (τάξη) στην οποία ανήκουν και την προκαθορισμένη μάσκα της κλάσης, για δε τις λάθος, αιτιολογήστε γιατί είναι λάθος.

α	155.54.12.17
β	10.146.0.1
γ	192.268.1.1
δ	122.122.11.53
ε	192.168.12.7.1
στ	223.54.136.133

2. Για τον υπολογιστή με διεύθυνση IP **192.168.1.18** να δώσετε:
   1) Την κλάση-τάξη δικτύου στην οποία ανήκει
   2) Την προκαθορισμένη μάσκα δικτύου
   3) Τη διεύθυνση δικτύου (network address) και τη διεύθυνση εκπομπής (broadcast address)
   4) Την περιοχή διευθύνσεων (από - έως) οι οποίες ανήκουν στο ίδιο δίκτυο με τον συγκεκριμένο υπολογιστή και τον συνολικό αριθμό υπολογιστών του συγκεκριμένου δικτύου
3. Για τον υπολογιστή με διεύθυνση IP **172.16.1.18** να δώσετε:
   1) Την κλάση-τάξη δικτύου στην οποία ανήκει
   2) Την προκαθορισμένη μάσκα δικτύου
   3) Τη διεύθυνση δικτύου (network address) και τη διεύθυνση εκπομπής (broadcast address)
   4) Την περιοχή διευθύνσεων (από - έως) οι οποίες ανήκουν στο ίδιο δίκτυο με τον συγκεκριμένο υπολογιστή και τον συνολικό αριθμό υπολογιστών του συγκεκριμένου δικτύου
4. Υπολογίστε πόσους υπολογιστές μπορεί να έχει το δίκτυο **192.168.64.0/16** (μάσκα δικτύου 255.255.0.0)
5. Οι υπολογιστές με διευθύνσεις IP **192.168.31.12/22** και **192.168.47.13/22** (η μάσκα δικτύου /22 είναι 255.255.252.0) ανήκουν στο ίδιο δίκτυο;
6. Δίνεται η διεύθυνση δικτύου **192.168.5.0/24** δηλαδή με μάσκα δικτύου **255.255.255.0**
   1) Να χωριστεί το δίκτυο σε **τρία (3) τουλάχιστον υποδίκτυα** και να δοθούν
   2) οι περιοχές διευθύνσεων καθώς και
   3) οι διευθύνσεις υποδικτύου και εκπομπής για τα δυο πρώτα υποδίκτυα.
   4) Πόσους υπολογιστές μπορεί να έχει το κάθε υποδίκτυο;
7. Ποιοί υπολογιστές (διευθύνσεις IP) ανήκουν στο ίδιο δίκτυο με τον **192.168.31.12/22** (η μάσκα δικτύου /22 είναι 255.255.252.0);
8. Πόσα ψηφία (bit) πρέπει να δώσουμε στους άσους της μάσκας για να χωριστεί ένα δίκτυο οποιασδήποτε κλάσης (A, B, C) σε τουλάχιστον έξι (6) υποδίκτυα;
9. Ένα αυτοδύναμο πακέτο IP συνολικού μήκους **2600 bytes (μαζί με την επικεφαλίδα) και με τιμή στο πεδίο αναγνώρισης 0x012d8** πρόκειται να διέλθει από δίκτυο **Ethernet** με **MTU = 1500 bytes**, δηλαδή το πλαίσιό του μπορεί να μεταφέρει το πολύ 1500 bytes. Το πακέτο IP έχει το DF=0. Να αιτιολογήσετε γιατί θα διασπαστεί το αρχικό πακέτο και να υπολογίσετε σε πόσα τμήματα θα χωριστεί. Ακολούθως να συμπληρώσετε τον παρακάτω πίνακα:

	1ο τμήμα	2ο		
Μήκος επικεφαλίδας (λέξεις των 32bit)				
Συνολικό μήκος (bytes)				
Μήκος δεδομένων				
Αναγνώριση				
DF (σημαία)				
MF (σημαία)				
Σχετ. θέση τμήματος (οκτάδες byte)				

10. Από τη διάσπαση ενός πακέτου IP προέκυψε ο πίνακας με τα στοιχεία των τμημάτων, όμως λείπουν μερικά. Συμπληρώστε τα στοιχεία που λείπουν και απαντήστε στο ερώτημα “Ποιο ήταν το συνολικό μήκος του αρχικού πακέτου;”

	1ο τμήμα	2ο		
Μήκος επικεφαλίδας (λέξεις των 32bit)		5		
Συνολικό μήκος (bytes)		844	100	
Μήκος δεδομένων				
Αναγνώριση	0x34b6			
DF (σημαία)	0			
MF (σημαία)				
Σχετ. θέση τμήματος (οκτάδες byte)			206	

11. Αφού το πεδίο MF είναι 0 και σε ένα αυτοδύναμο πακέτο που δε διασπάστηκε αλλά και στο τελευταίο τμήμα ενός διασπασμένου πακέτου, πως μπορούμε να καταλάβουμε αν πρόκειται για την πρώτη περίπτωση ή τη δεύτερη;
12. Ποιο είναι το μέγιστο μήκος του αυτοδύναμου πακέτου IPv4; (υπόδειξη: μελετήστε τα πεδία της επικεφαλίδας)
13. Οι επικεφαλίδες δυο τμημάτων του ίδιου αρχικού τεμαχισμένου πακέτου IPv4 έχουν το ίδιο άθροισμα ελέγχου;
14. Ένα αυτοδύναμο πακέτο IPv4 διέρχεται από έναν δρομολογητή. Έχει το ίδιο άθροισμα ελέγχου επικεφαλίδας όταν φεύγει με αυτό που είχε όταν ήρθε;
15. Γιατί η σχετική θέση τμήματος (το offset) σε ένα πακέτο IPv4 που διασπάστηκε μετρείται σε οκτάδες byte;(υπόδειξη: μελετήστε τα πεδία της επικεφαλίδας)
16. Ένα αυτοδύναμο πακέτο IPv4 διέρχεται από έναν δρομολογητή. Τι συμβαίνει στο πεδίο της επικεφαλίδας “Χρόνος ζωής - TTL”; Τι θα συμβεί εάν το πακέτο, στο πεδίο “TTL”, έχει την τιμή 0;

17. Ποια είναι η θέση του πρωτοκόλλου ARP (σε ποιο επίπεδο)στο διαστρωματωμένο μοντέλο δικτύωσης (OSI ή TCP/IP) και ποια λειτουργία εκτελεί; Ποια είναι η φυσική διεύθυνση στην οποία απευθύνεται ένα ερώτημα ARP;
18. Πώς σχετίζονται τα πρωτόκολλα ARP, RARP και οι διευθύνσεις, φυσικές (MAC) και λογικές (IPv4);
19. Τι κάνει το πρωτόκολλο ARP, πριν προχωρήσει στην υποβολή ενός ερωτήματος ARP;
20. Σε ποιο επίπεδο του μοντέλου TCP/IP λειτουργούν τα πρωτόκολλα BOOTP και DHCP; Δώστε δυο βασικά πλεονεκτήματα του DHCP τα οποία τελικά συνέβαλλαν στην επικράτηση της χρήσης του.
21. Ένας πελάτης DHCP, με δυναμική ρύθμιση, τι πρέπει να κάνει πριν λήξει η μίσθωση της διεύθυνσής του;
22. Πως μπορούν να εξυπηρετηθούν πελάτες DHCP από διακομιστές DHCP οι οποίοι βρίσκονται σε διαφορετικά φυσικά δίκτυα;
23. Βάλτε σε σωστή χρονική σειρά τα μηνύματα DHCP

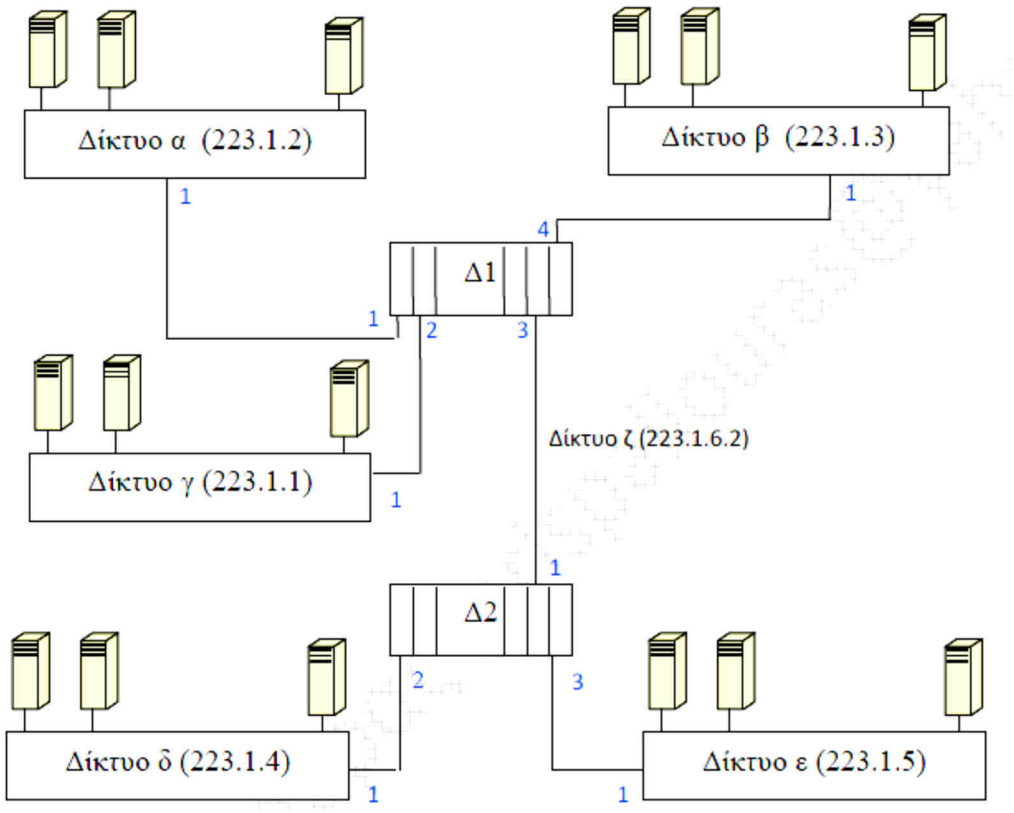
    1.DHCPACK

    2.DHCPDISCOVER

    3.DHCPREQUEST

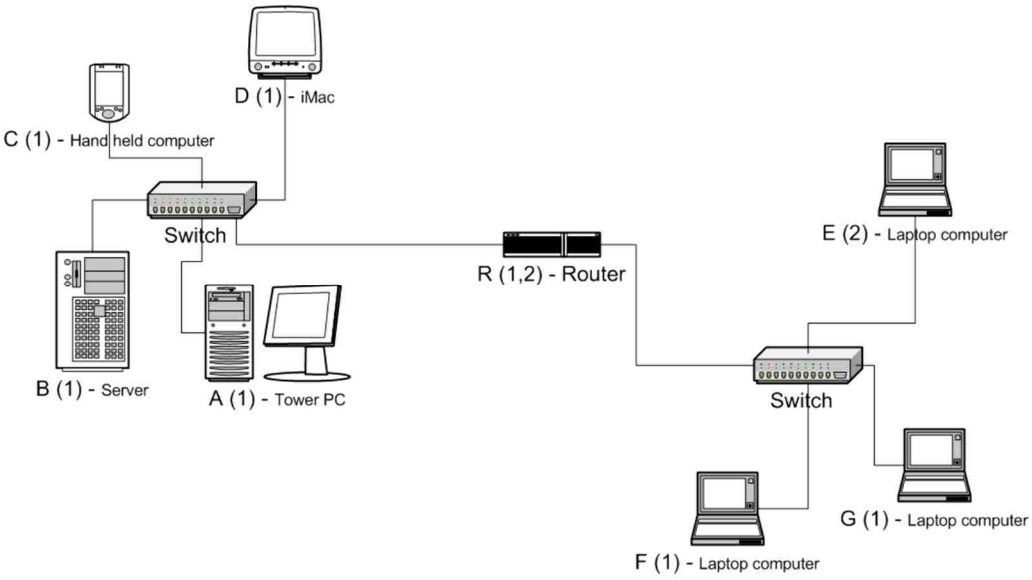
    4.DHCPOFFER
24. Πώς πληροφορείται ένας υπολογιστής τη διεύθυνση IP ενός άλλου υπολογιστή τον οποίο ο χρήστης ζητά με το όνομά του;
25. Αναφέρετε δυο βασικά προβλήματα που εμφανίστηκαν κατά τη χρήση του πρωτοκόλλου IPv4, κυρίως εξαιτίας της αύξησης του μεγέθους του Διαδικτύου, και περιγράψτε ένα από αυτά. Πώς αντιμετωπίστηκε από το πρωτόκολλο IP έκδοση 6 (IPv6);
26. Μεταγράψτε τη διεύθυνση IPv6 2001:0db8:0000:0000:0001:0000:0000:0001 με το σωστό τρόπο σύντομης γραφής για διευθύνσεις IPv6.
27. Περιγράψτε τους τρεις γενικούς τύπου διευθύνσεων που ορίζει το πρωτόκολλο IPv6.
28. Για τον υπολογιστή με φυσική διεύθυνση (MAC) 74-ea-3a-cd-06-40 να γράψετε την τοπική δ/νση ζεύξης αποκλειστικής διανομής (Link Local Unicast)
29. Τι είναι η δρομολόγηση και ποιες επιμέρους δραστηριότητες περιλαμβάνει;
30. Ποια προβλήματα (αναφέρετε τουλάχιστον τρία) δεν εγγυάται ότι μπορεί να αντιμετωπίσει το πρωτόκολλο Διαδικτύου IP; Ποιος θα πρέπει να τα αντιμετωπίσει;
31. Πότε η δρομολόγηση χαρακτηρίζεται άμεση και πότε έμμεση;
32. Υπολογιστής με διεύθυνση IPv4 192.168.1.12/24 θέλει να επικοινωνήσει με τον υπολογιστή με διεύθυνση 192.168.2.124/24. Η δρομολόγηση θα είναι άμεση ή έμμεση; Αιτιολογήστε την απάντησή σας.
33. Ένας υπολογιστής θέλει να στείλει ένα αυτοδύναμο πακέτο IP σε έναν άλλο του οποίου η διεύθυνση (και η διεύθυνση δικτύου) δεν έχει καταχωριστεί στον πίνακα δρομολόγησής του. Τι θα κάνει;
34. Τι είναι ο αλγόριθμος δρομολόγησης;
35. Ποιος ο ρόλος των πρωτοκόλλων δρομολόγησης;
36. Αναφέρετε τις κατηγορίες, στις οποίες διακρίνονται τα πρωτόκολλα δρομολόγησης.
37. Περιγράψτε εν συντομία την άμεση και την έμμεση δρομολόγηση.
38. Ποια εργασία εκτελεί ένας εξωτερικός δρομολογητής;
39. Ποια δίκτυα ονομάζονται αυτόνομα συστήματα (AS);
40. Ποια η διαφορά της στατικής από τη δυναμική δρομολόγηση;

41. Δίνεται το παρακάτω δίκτυο με αριθμημένα τα σημεία διεπαφής δικτύου. Δώστε τη δομή του πίνακα δρομολόγησης (τις βασικές στήλες από τις οποίες αποτελείται) και συμπληρώσετε τον για τον δρομολογητή Δ2.



(*Πηγή:* http://www.2epal-iliou.edu.gr/moodle/pluginfile.php/148/mod_resource/content/1/7.9.pdf)

42. Δίνεται το παρακάτω δίκτυο:



(*Πηγή:* http://petros-salavasidis.blogspot.gr/2012/11/2012-2013.html)

Οι διεπαφές και οι IP διευθύνσεις των κόμβων είναι:

Κόμβος	Διεπαφή	IP
A	1	123.43.1.7
B	1	123.43.1.2
C	1	123.43.1.11
D	1	123.43.1.23
E	2	123.43.2.4
F	1	123.43.2.5
G	1	123.43.2.6

Το δίκτυο που αποτελείται από τους κόμβους A,B,C και D, συνδέεται στην διεπαφή 1 του Δρομολογητή (R). Το δίκτυο που αποτελείται από τους κόμβους E, F και G συνδέεται στην διεπαφή 2 του Δρομολογητή (R).

Να γραφούν οι πίνακες δρομολόγησης όλων των κόμβων (A, B, C, D, E, F και G) και του Δρομολογητή (R).

Ασκήσεις σε Εργαστηριακό Περιβάλλον

Οι περισσότερες ασκήσεις αφορούν σε εμφάνιση ρυθμίσεων που σημαίνει ότι μπορούν να εκτελεστούν εύκολα σε σχολικό εργαστήριο πληροφορικής από απλούς χρήστες. Όσες απαιτούν αλλαγή ρυθμίσεων μπορούν να γίνουν υπό τη σύμφωνη γνώμη και επιτήρηση του υπευθύνου του εργαστηρίου με προϋπόθεση την επαναφορά των αρχικών ρυθμίσεων πριν την απομάκρυνση από το εργαστήριο. Επίσης, μπορούν να εκτελεστούν σε υπολογιστές παλαιότερους, αν είναι διαθέσιμοι, οι οποίοι έχουν αποσυρθεί από ενεργό εργαστήριο είναι όμως λειτουργικοί και έχουν διατεθεί για μαθήματα σχετικά με το Υλικό, τη Συντήρηση και τα Δίκτυα. Στη δεύτερη περίπτωση μπορεί να υλοποιηθεί εύκολα και η τελευταία άσκηση (8) που αφορά στην εγκατάσταση ενός μικρού τοπικού δικτύου κλάσης C και στην υποδικτύωσή του. Για βοήθεια σχετικά με τις αναφερόμενες εντολές ανατρέξτε στην ενσωματωμένη βοήθεια των εντολών, των χρησιμοποιούμενων λειτουργικών συστημάτων (help, man pages) και στον συνημμένο οδηγό.

Χρονοπρογραμματισμός

Ώρες	Άσκηση - αντικείμενο
1	1, 2 Εμφάνιση/αλλαγή δικτυακών ρυθμίσεων
1	3, 4 Έλεγχος επικοινωνίας (3ο OSI), ιχνηλάτηση διαδρομής, ονόματα περιοχών
2	5, 6, 7 Εύρεση φυσικών διευθύνσεων άλλων υπολογιστών του δικτύου, εμφάνιση πίνακα δρομολόγησης και επαναληπτικές αναφορές στις 1 – 4.
2	8 Εγκατάσταση και υποδικτύωση μικρού τοπικού δικτύου κλάσης C.

1. Στον υπολογιστή που εργάζεστε,
   i. αναγνωρίστε εάν υπάρχει εγκατεστημένη κάρτα δικτύου Ethernet, είναι συνδεδεμένη σε hub ή switch επίσης
   ii. ποια διεύθυνση IP, μάσκα δικτύου και προεπιλεγμένη πύλη έχει.

   *(**Υπόδειξη**: Εξετάστε οπτικά το πίσω μέρος του υπολογιστή και προσπαθήστε να εντοπίσετε μια υποδοχή τύπου RJ-45 (modular jack/plug 8p8c) είτε στο πίσω μέρος*

της μητρικής (ενσωματωμένη στο Μ/Β) είτε στην πίσω όψη των υποδοχών επέκτασης (πρόσθετη εκ των υστέρων). Δείτε εάν υπάρχει κατάλληλο καλώδιο τύπου UTP/FTP με τους αντίστοιχους ακροδέκτες που να καταλήγει σε hub ή switch. Ελέγξτε αν είναι σε λειτουργία.
Εάν ο υπολογιστής σας "τρέχει" windows εκτελέστε ***ipconfig /all***
Εάν "τρέχει" linux, εκτελέστε ***/sbin/ifconfig****)*
Σημειώστε τα αποτελέσματα.

2. Στον υπολογιστή που εργάζεστε,
   i. αλλάξτε τη διεύθυνση IP σε 192.168.7.12 (ή ό,τι άλλο σας ζητηθεί)
   ii. αλλάξτε τη μάσκα δικτύου σε 255.255.255.192
   iii. αλλάξτε την προεπιλεγμένη πύλη σε 192.168.1.3
   (Εργαστείτε ανάλογα με το Λ.Σ. που "τρέχει" ο υπολογιστής σας, σύμφωνα με τα προηγούμενα).
3. Ελέγξτε τη συνδεσιμότητα του υπολογιστή στον οποίο εργάζεστε με τον διακομιστή του εργαστηρίου κάνοντας χρήση της εντολής ping. Εφόσον λαμβάνονται απαντήσεις, η λειτουργικότητα του δικτύου μέχρι το επίπεδο διαδικτύου (3ο OSI) είναι εντάξει.Δοκιμάστε να στείλετε 15 πακέτα με τιμή στο πεδίο TTL=128. Μελετήστε τα συγκεντρωτικά στατιστικά που σας επιστρέφει. Δοκιμάστε να κάνετε ping σε προορισμούς έξω από το δίκτυο του σχολείου σας και συγκρίνετε τους χρόνους. Άν αυτό δεν είναι εφικτό αναζητήστε λογική εξήγηση γιατί δεν είναι εφικτό. Συζητήστε γιατί είναι κρίσιμοι οι μικροί χρόνοι ping σε online παιχνίδια και γιατί αυτό αποτελεί βασικό κριτήριο για την επιλογή παρόχου (ISP) από τους φανατικούς gamers.
4. Ιχνηλατήστε με την traceroute τη διαδρομή που ακολουθούν τα πακέτα σας προς κάποιο συγκεκριμένο προορισμό. Καταγράψτε την. Επαναλάβετε το ίδιο σε άλλη χρονική στιγμή (ακόμη και άλλη μέρα ή από το σπίτι σας). Συγκρίνετε τις διαδρομές. Δοκιμάστε να βρείτε τη διεύθυνση IPv4 του www.sch.gr και του ftp.ntua.gr. Απ' ό,τι φαίνεται το ftp είναι ψευδώνυμο. Ποιο είναι το πραγματικό όνομα του διακομιστή ftp.ntua.gr;
5. Εμφανίστε τον πίνακα ARP του υπολογιστή στον οποίο εργάζεστε. Σε ποια περίπτωση μπορεί να είναι κενός; Βρείτε τη φυσική διεύθυνση του υπολογιστή σας αλλά και του διακομιστή του εργαστηρίου. Μπορούν να βρεθούν με τον ίδιο τρόπο;
6. Εφόσον εργάζεστε σε υπολογιστή του οποίου το Λ.Σ. υποστηρίζει IPv6 βρείτε τη διεύθυνση IPv6 που έχει *(ipconfig /all, ifconfig ή οποιαδήποτε άλλη εναλλακτική μέθοδος)* και δείτε ποιοι άλλοι γειτονικοί υπολογιστές υπάρχουν. Στο IPv4 αυτό το κάνει το ARP. Στο IPv6 λέγεται "Neighbor Discovery". Ανάλογα με το Λ.Σ. του υπολογιστή σας, δοκιμάστε το netsh (windows) ή ip (linux) και συζητήστε τα αποτελέσματα. Εφόσον ο υπολογιστής σας έχει τοπική διεύθυνση ζεύξης αποκλειστικής διανομής (Link Local Unicast) επαληθεύστε τα τμήματά της (prefix fe80::/64 και interface ID EUI-64 σε linux ή τυχαίο interface ID σε windows). Εάν δεν έχει, γράψτε την εσείς πως έπρεπε να είναι ακολουθώντας την τυποποίηση EUI-64.
   (Υπόδειξη: Εμφάνιση αποτελεσμάτων "Neighbor Discovery" σε linux: ip -6 neigh show και σε windows: netsh interface ipv6 show neighbors).
7. Εμφανίστε τον πίνακα δρομολόγησης του υπολογιστή σας και εντοπίστε από τις καταχωρίσεις του ποια είναι η προεπιλεγμένη πύλη.
8. Εάν σας επιτρέπει ο υπεύθυνος εργαστηρίου, υπό την εποπτεία του, ή έχετε πρόσβαση σε παλιό λειτουργικό εξοπλισμό (4-8 υπολογιστές, hub/switch, απαραίτητα καλώδια), συνθέστε ένα μικρό τοπικό δίκτυο κλάσης C κάνοντας τις απαραίτητες συνδέσεις και ρυθμίσεις. Ελέγξτε την επικοινωνία μεταξύ των υπολογιστών με την ping. Αφού εξασφαλίσετε και επιβεβαιώσετε την επικοινωνία όλων με όλους, υποδικτυώστε το σε δύο ή τέσσερα υποδίκτυα. Με τις νέες

ρυθμίσεις, επιβεβαιώστε ότι στα ping απαντούν μόνο υπολογιστές του ίδιου υποδικτύου και είναι αδύνατον να επικοινωνήσουν με υπολογιστές άλλων υποδικτύων. *(Υπόδειξη: πρόκειται για πρακτική εφαρμογή της θεωρητικής άσκησης 6)*.

Βιβλιογραφία

Αλεξόπουλος, Α., & Λαγογιάννης, Γ. (2012). *Τηλεπικοινωνίες και Δίκτυα Υπολογιστών,* (8η έκδ.). Αθήνα.

Comer, D. E. (2001). *Διαδίκτυα με TCP/IP αρχές, πρωτόκολλα και αρχιτεκτονικές,* (4η έκδ., Τ. 1). Αθήνα: Κλειδάριθμος.

Hunt, C. (1998). *TCP/IP Network Administration* (2nd έκδ.). Sebastopol, CA: O'Reilly & Associates.

Loshin, P. (2004). *IPv6 Theory, Protocol and Practice* (2η έκδ.). San Francisco, CA., USA: Elsevier, Inc.

MANN, S., & KRELL, M. (2002). *LINUX TCP/IP Network Administration*. Upper Saddle River, NJ, USA: Prentice Hall PTR.

Routing Basics - DocWiki. (χ.χ.). Ανακτήθηκε 6 Αύγουστος 2015, από *http://docwiki.cisco.com/wiki/Routing_Basics*

Tanenbaum, A. S. (2000). *Δίκτυα Υπολογιστών* (3η έκδ.). Αθήνα: Εκδόσεις Παπασωτηρίου.

Κεφάλαιο 4ο

ΕΠΙΠΕΔΟ ΜΕΤΑΦΟΡΑΣ

Εισαγωγή

Στα προηγούμενα κεφάλαια μελετήθηκαν πώς μεταφέρονται τα δεδομένα από διεπαφή σε διεπαφή για να φτάσουν στο προορισμό τους. Επειδή το επίπεδο δικτύου από τη φύση του είναι αναξιόπιστο, τα πακέτα φθάνουν καθυστερημένα, εκτός σειράς και πολλές φορές καταστρέφονται στην διαδρομή. Επομένως χρειάζεται ένας ενδιάμεσο στρώμα μεταξύ της εφαρμογής και των κατώτερων στρωμάτων του δικτύου που να εξασφαλίζει ένα γενικό εύκολο τρόπο μεταφοράς των δεδομένων από τον αποστολέα προς τον παραλήπτη καλύπτοντας τις ανάγκες αξιοπιστίας, μεταφοράς των δεδομένων που απαιτούνται.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 4ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- απαριθμούν τις διαφορές των πρωτοκόλλων TCP/UDP
- διατυπώνουν πώς προκύπτει η αξιοπιστία του TCP και πότε αποτελεί την καταλληλότερη επιλογή
- διαπιστώνουν την έναρξη, διατήρηση και τερματισμό μιας σύνδεσης TCP
- περιγράφουν τη δομή της υποδοχής τερματισμού (socket) και να αναφέρουν τους τρόπους αξιοποίησής της προγραμματιστικά

Διδακτικές Ενότητες

4.1 Πρωτόκολλα προσανατολισμένα στη σύνδεση –χωρίς σύνδεση.
4.2 Υποδοχές (sockets).
4.3 Συνδέσεις TCP - Έναρξη/τερματισμός σύνδεσης.

4.1 Πρωτόκολλα προσανατολισμένα στη σύνδεση –χωρίς σύνδεση

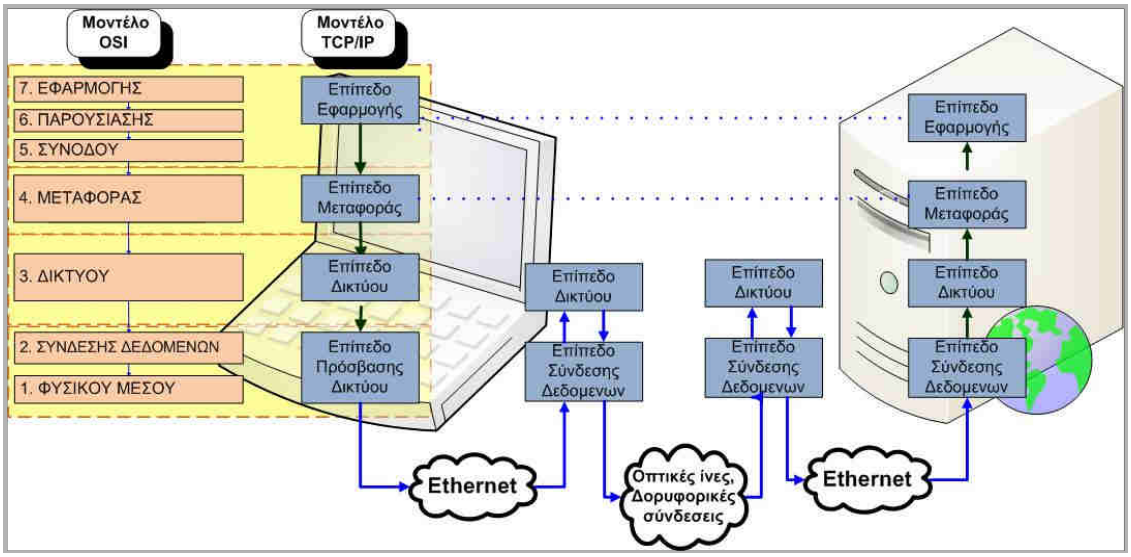
Οι δικτυακές εφαρμογές που είναι εγκατεστημένες στους κόμβους ενός δικτύου, σε ηλεκτρονικούς υπολογιστές, σε έξυπνες φορητές συσκευές κ.α., επικοινωνούν ανταλλάσσοντας μηνύματα δεδομένων. Το επίπεδο μεταφοράς παρέχει τις διαδικασίες που αναλαμβάνουν την μεταφορά μηνυμάτων με διαφανή τρόπο από τις δικτυακές εφαρμογές που παράγουν τα μηνύματα αυτά.

Το επίπεδο μεταφοράς είναι υπεύθυνο για την επικοινωνία των δεδομένων που λαμβάνονται από το επίπεδο εφαρμογής μεταξύ του υπολογιστή (κόμβου) αφετηρίας και του υπολογιστή (κόμβου) προορισμού ή αλλιώς επικοινωνία από-άκρο-σε-άκρο (end-to-end), **με ή χωρίς εγκατάσταση σύνδεσης**. Με άλλα λόγια στην πρώτη περίπτωση, αρχικά γίνεται εγκατάσταση σύνδεσης και ένα πρόγραμμα στον υπολογιστή αφετηρίας συνομιλεί με ένα παρόμοιο πρόγραμμα του υπολογιστή προορισμού, ενώ στην δεύτερη περίπτωση χωρίς να εγκατασταθεί σύνδεση μεταξύ των κόμβων, το πρόγραμμα στην αφετηρία μεταδίδει άμεσα τα δεδομένα στο πρόγραμμα προορισμού. Στην περίπτωση που αρχικά γίνεται εγκατάσταση της σύνδεσης οι πληροφορίες της εγκατεστημένης σύνδεσης αποθηκεύονται στις επικεφαλίδες του μηνύματος και στα μηνύματα ελέγχου.

Στα κατώτερα επίπεδα, τα πρωτόκολλα δημιουργούν συνδέσεις ανάμεσα σε κάθε υπολογιστή που συνδέεται με τους γειτονικές του υπολογιστές, και όχι μόνο ανάμεσα στους τερματικούς κόμβους, δηλαδή στους υπολογιστές αφετηρίας και προορισμού.

Επομένως, οι λειτουργίες που αναλαμβάνει το επίπεδο μεταφοράς είναι η εγκατάσταση και ο τερματισμός των συνδέσεων διαμέσου δικτύου έλεγχου της ροής της πληροφορίας, ώστε μια γρήγορη μηχανή να μην υπερφορτώνει μια αργή, καθώς και η επιβεβαίωση ότι η πληροφορία έφτασε στο προορισμό της.

Η οικογένεια πρωτοκόλλων TCP/IP διαθέτει στο επίπεδο μεταφοράς τα πρωτόκολλα TCP και UDP που υλοποιούν τις διαδικασίες μεταφοράς των μηνυμάτων δεδομένων.



Εικόνα 4.1.α: OSI – TCP Διαστρωμάτωση

Τα πρωτόκολλα αυτά διαχωρίζονται μεταξύ τους: στο TCP που είναι πρωτόκολλο προσανατολισμένο σε **σύνδεση (Connection oriented)** και UDP που είναι πρωτόκολλο **χωρίς σύνδεση (Connectionless).**

Πρωτόκολλο **προσανατολισμένο στη σύνδεση** είναι αυτό που αρχικά, πριν ξεκινήσει η μετάδοση των δεδομένων εγκαθιστά μια σύνδεση από άκρο σε άκρο για να εξασφαλιστεί μια διαδρομή (νοητό κύκλωμα) για τη μετάδοση των πακέτων. Όλα τα πακέτα μεταδίδονται στο ίδιο νοητό κύκλωμα. Αφού ξεκινήσει η μετάδοση εξασφαλίζει ότι τα δεδομένα θα φτάσουν στον παραλήπτη χωρίς σφάλματα.

Πρωτόκολλο **χωρίς σύνδεση** είναι αυτό στο οποίο ξεκινά η μετάδοση των δεδομένων χωρίς να έχει προηγηθεί επικοινωνία με τον παραλήπτη. Τα δεδομένα μεταδίδονται σε **αυτοδύναμα πακέτα (datagrams)** χωρίς την εγκατάσταση σύνδεσης μέσω νοητών κυκλωμάτων. Τα πρωτόκολλα αυτά θεωρούνται αναξιόπιστα επειδή δεν εξασφαλίζουν ότι τα δεδομένα θα φτάσουν στο προορισμό τους.

Η πληροφορία που μεταφέρεται από άκρο σε άκρο στο επίπεδο μεταφοράς οργανώνεται σε ακολουθία από ομάδες δεδομένων που ονομάζονται datagrams. Κάθε ένα datagram μετράται σε octets δηλαδή οκτάδες ψηφίων (byte) και αντιμετωπίζεται απολύτως ανεξάρτητα από το δίκτυο.

Octet: Το byte πρωτοεμφανίστηκε στα μέσα της δεκαετίας του '50 από την IBM με την έννοια της μικρότερης ομάδας χρησιμοποιούμενων δυαδικών ψηφίων που αντιστοιχεί σε διευθύνσεις μνήμης σε έναν ηλεκτρονικό υπολογιστή και αρχικά δεν αντιστοιχούσε σε 8 ψηφία (bit). Για το λόγο αυτό στο TCP/IP χρησιμοποιείται ο όρος που εξορισμού αντιστοιχεί σε μονάδα δεδομένων μήκους 8 bit.

4.1.1 Πρωτόκολλο TCP - Δομή πακέτου

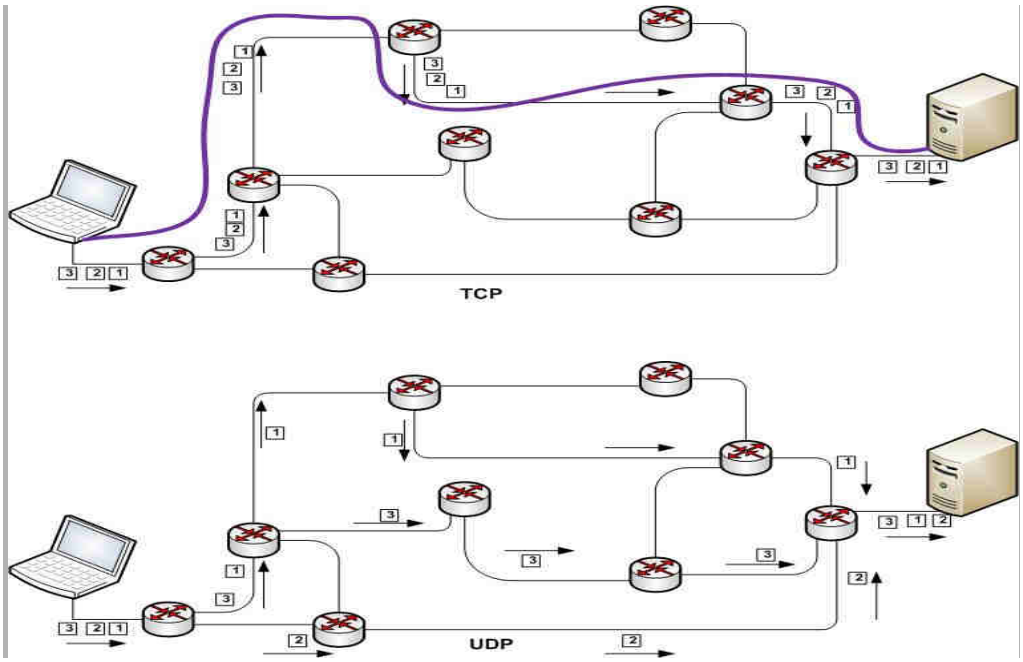
Για να κατανοηθεί η λειτουργία του πρωτοκόλλου TCP ας δούμε ένα παράδειγμα:

Έστω ότι θέλουμε να αποστείλουμε ένα μήνυμα μέσω ηλεκτρονικού ταχυδρομείου. Αρχικά η εφαρμογή χρησιμοποιώντας τα πρωτόκολλα του επιπέδου εφαρμογής παράγει μια σειρά πληροφοριών υπό μορφή δεδομένων με τις εντολές και το περιεχόμενο που ανταλλάσσουν δυο κόμβοι μέσω του δικτύου. Προϋπόθεση είναι η αξιόπιστη μετάδοση των πληροφοριών μέσω του δικτύου.

Η πληροφορία παραλαμβάνεται στο επίπεδο μεταφοράς από το πρωτόκολλο TCP που αναλαμβάνει να μεταφέρει τα δεδομένα – πληροφορίες από το ένα άκρο στο άλλο.

Έστω ότι στο παραπάνω παράδειγμα το TCP παραλαμβάνει από την εφαρμογή ηλεκτρονικού ταχυδρομείου δεδομένα μεγέθους 6000 octets. Ελέγχει το δίκτυο και διαπιστώνει ότι δεν μπορεί να διαχειριστεί datagram μεγαλύτερα από 600 octets. Στην πραγματικότητα τα δύο άκρα δηλώνουν το μεγαλύτερο μέγεθος datagram που μπορούν να διαχειριστούν. Για να αντιμετωπιστεί η κατάσταση το αρχικό datagram διασπάται σε 10 μικρότερα των 600 octets και αποστέλλονται ανεξάρτητα από το ένα άκρο στο άλλο. Τα μικρότερα αυτά datagrams συμφωνημένου μεγέθους ονομάζονται **Τμήματα (segments). Επομένως στο πρωτόκολλο TCP η μονάδα δεδομένων που διαχειρίζεται (PDU) αναφέρεται ως Τμήμα (Segment).** Βέβαια στο Τμήμα μεταξύ των δύο άκρων μπορεί να χωρά ολόκληρο το datagram, οπότε δεν θα χρειαστεί να διασπαστεί.

Το TCP/IP είναι βασισμένο στο "catenet model" (περιγράφεται με λεπτομέρεια στο IEN 48). Το μοντέλο “catenet” θεωρεί ότι υπάρχει ένας αρκετά μεγάλος αριθμός ανεξάρτητων δικτύων που διασυνδέονται με εξωτερικές πύλες δρομολόγησης (Gateways). Τα τμήματα διαπερνούν από πολλά διαφορετικά δίκτυα πριν φτάσουν στο προορισμό τους. Σε πολλές περιπτώσεις το μονοπάτι είναι διαφορετικό για κάθε τμήμα και η διαδρομή είναι αόρατη στο χρήστη.



Εικόνα 4.1.1.α: TCP – UDP Επικοινωνία

Όταν φτάσουν στο άλλο άκρο θα επανασυνδεθούν για να διαμορφώσουν το αρχικό μήνυμα των 6000 octets. Όμως τα ανεξάρτητα τμήματα είναι πολύ πιθανόν να φτάσουν με διαφορετική σειρά, για παράδειγμα το όγδοο τμήμα να φτάσει πριν το πρώτο. Επίσης λόγω

σφάλματος δικτύου σε κάποιο σημείο της διαδρομής είναι πιθανό κάποιο τμήμα να καταστραφεί. Στην περίπτωση αυτή το συγκεκριμένο τμήμα πρέπει να σταλεί ξανά.

Επιπλέον ένα θέμα που πρέπει να χειριστεί το TCP είναι σε ποια σύνδεση ανήκει ένα συγκεκριμένο τμήμα. Για να γίνει κατανοητό αυτό στο ένα άκρο, σε ένα ηλεκτρονικό υπολογιστή (κόμβο) μπορεί η ίδια ή και διαφορετική εφαρμογή να παράγει πολλά ανεξάρτητα μηνύματα που πρέπει να αποσταλούν στον ίδιο ή και σε διαφορετικό προορισμό. Επίσης στο άλλο άκρο μπορεί να παραλαμβάνονται τμήματα από πολλούς διαφορετικούς αποστολείς και να απευθύνονται σε διαφορετικές δικτυακές εφαρμογές.

Πολυπλεξία (Multiplexing) είναι η δυνατότητα πολλές διεργασίες μέσα στον ίδιο τερματικό κόμβο (host) να χρησιμοποιούν τις υπηρεσίες επικοινωνίας του TCP ταυτόχρονα.

Το TCP στην φάση της επανασύνδεσης του αρχικού μηνύματος πρέπει να γνωρίζει ποια είναι η προέλευση (source) του μηνύματος και ποιος ο προορισμός (destination).

Έτσι το TCP εξασφαλίζει την **Αξιοπιστία** της σύνδεσης με:

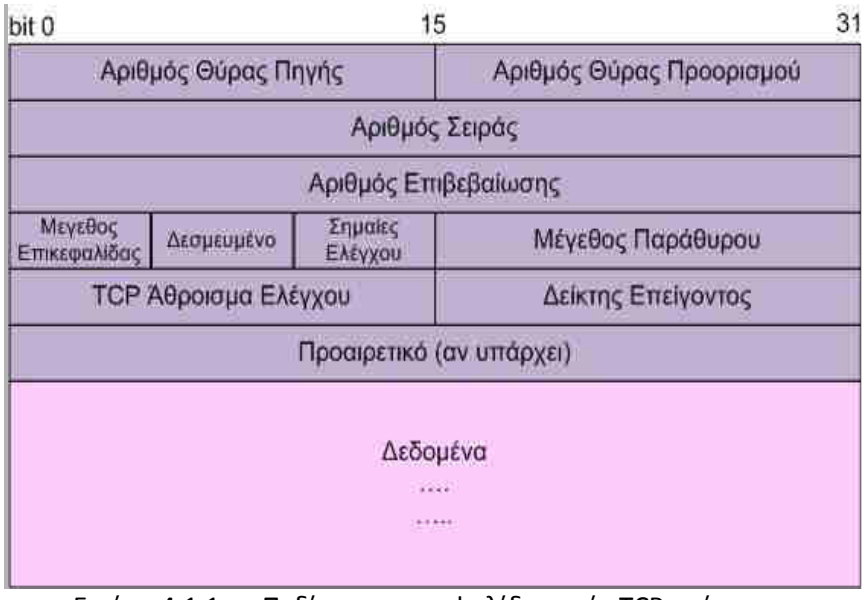
- Την Εγκατάσταση Σύνδεσης από την προέλευση στον προορισμό.
- Τεμαχίζει τα δεδομένα αν επιβάλλεται από το δίκτυο.
- Επιβεβαιώνει την παραλαβή δεδομένων.
- Τοποθετεί στη σειρά τα τμήματα κατά την παραλαβή

Όλες αυτές οι πληροφορίες που είναι απαραίτητες για τον έλεγχο και την ανασύνθεση του αρχικού μηνύματος περιέχονται στην **επικεφαλίδα (header)** που δημιουργείται κατά τον αρχικό σχηματισμό του τμήματος.

Η επικεφαλίδα είναι ένα σύνολο από octets δεδομένων πριν από τα πραγματικά δεδομένα και προστίθεται στην αρχή του τμήματος.

Εικόνα 4.1.1.β: Τμήμα TCP

Η επικεφαλίδα έχει ελάχιστο μήκος 20 octets και μέγιστο 60 octets μαζί με το προαιρετικό πεδίο options. Οι πληροφορίες που εισάγει το TCP στην επικεφαλίδα ώστε να εξασφαλίσει την αξιοπιστία της μεταφοράς του μηνύματος είναι:



Εικόνα 4.1.1.γ: Πεδία της επικεφαλίδας ενός TCP τμήματος.

- Ο **Αριθμός Θύρας Προέλευσης (source port number)** και **Αριθμός Θύρας Προορισμού (destination port number)**. Οι αριθμοί θύρας χρησιμεύουν στην ταυτοποίηση των διαφορετικών συνομιλιών μεταξύ των δύο άκρων. Έστω ότι δυο διαφορετικοί άνθρωποι στέλνουν από ένα μήνυμα ηλεκτρονικού ταχυδρομείου προς ένα τρίτο.
  Το TCP αποδίδει τις θύρες με αριθμούς 100 και 200 στις διεργασίες των εφαρμογών ηλεκτρονικού ταχυδρομείου των αποστολέων αντίστοιχα και τη θύρα 25 με την εφαρμογή που θα παραδοθεί το μήνυμα στον υπολογιστή του παραλήπτη στο άλλο άκρο. Όταν μεταδίδεται ένα τμήμα στην επικεφαλίδα των δύο τμημάτων, τα νούμερα 1024 και 2024 αποτελούν τις θύρες προέλευσης. Βέβαια το TCP πρέπει να γνωρίζει ποια είναι η θύρα προορισμού στο άλλο άκρο, και για το λόγο αυτό προσθέτει τον αριθμό 25 στην επικεφαλίδα στο αντίστοιχο πεδίο (του προορισμού). Τώρα, αν από το άλλο άκρο πρέπει να σταλεί πίσω ένα τμήμα τότε τα πεδία θύρα προέλευσης και προορισμού πρέπει να αντιστραφούν στην επικεφαλίδα του αντίστοιχου τμήματος.
- Ο **Αριθμός Σειράς (Sequence Number).** Ο αριθμός αυτός χρησιμεύει ώστε ο παραλήπτης στο άλλο άκρο να τοποθετεί τα τμήματα στη σωστή σειρά καθώς συνθέτει το αρχικό τμήμα, επειδή η σειρά που έχουν παραληφθεί μπορεί να είναι διαφορετική από τη σειρά που έχουν, αποσταλεί. Το TCP αριθμεί τα τμήματα με βάση τα octets, έτσι αν κάθε τμήμα αποτελείται από 600 octets, τότε ο αριθμός σειράς στην επικεφαλίδα του πρώτου τμήματος θα έχει τον αριθμό 0, στου δεύτερου 600, στου τρίτου 1200 κ.ο.κ.
- Ο **Αριθμός Επιβεβαίωσης (Acknowledgment).** Ο αριθμός αυτός χρησιμοποιείται για να διασφαλιστεί ότι κάθε τμήμα έχει φτάσει στον προορισμό του. Όταν ο παραλήπτης στο άλλο άκρο παραλάβει το τμήμα στέλνει ένα νέο τμήμα (ACK- επιβεβαίωσης) του οποίου το πεδίο Αριθμός επιβεβαίωσης, είναι συμπληρωμένο. Για παράδειγμα, στέλνοντας ένα τμήμα με επιβεβαίωση τον αριθμό 1201, σημαίνει ότι έχουν φτάσει όλα τα δεδομένα μέχρι και το octet με αριθμό 1200. Αν η επιβεβαίωση δεν παραληφθεί μέσα σε ένα συγκεκριμένο χρονικό διάστημα, αποστέλλονται ξανά τα δεδομένα.
- Το **Μέγεθος Παράθυρο (Window)**. Για λόγους επιτάχυνσης της επικοινωνίας το TCP δεν περιμένει την παραλαβή της επιβεβαίωσης για να στείλει το επόμενο τμήμα. Δεν γίνεται όμως να αποστέλλονται συνεχώς δεδομένα διότι ένας γρήγορος αποστολέας στο ένα άκρο θα μπορούσε να ξεπεράσει τις δυνατότητες απορρόφησης δεδομένων από ένα αργό παραλήπτη. Έτσι με το πεδίο Window κάθε άκρο δηλώνει πόσα νέα δεδομένα μπορεί να απορροφήσει τοποθετώντας σ' αυτό το πεδίο τον αριθμό από octets που διαθέτει ελεύθερα ο ενταμιευτής εισόδου (buffer). Όμως το μέγεθος του προσωρινού χώρου που μένει ελεύθερος μειώνεται όσο ο υπολογιστής λαμβάνει δεδομένα ανάλογα με τις δυνατότητες επεξεργασίας του παραλήπτη. Αν ο χώρος αυτός γεμίσει πρέπει ο αποστολέας να σταματήσει την αποστολή νέων δεδομένων επειδή σ' αυτή την περίπτωση τα δεδομένα θα απορριφθούν. Όταν ο παραλήπτης απελευθερώσει χώρο δηλώνει με το πεδίο Window ότι είναι έτοιμος να δεχτεί νέα δεδομένα.
- Το **Άθροισμα Ελέγχου (Checksum).** Ο αριθμός στο πεδίο αυτό της επικεφαλίδας τοποθετείται από τον αποστολέα αφού υπολογίσει το άθροισμα απ' όλα τα octets σε ένα datagram. Το TCP στο άλλο άκρο υπολογίζει ξανά το άθροισμα και το συγκρίνει με αυτό παρέλαβε. Αν τα δύο αποτελέσματα δεν είναι ίδια, τότε κάτι συνέβη κατά τη μεταφορά και το datagram απορρίπτεται.
- Τα πεδία **Σημαίες Ελέγχου (Flags)** χρησιμεύουν για τον χειρισμό των συνδέσεων και αντιστοιχούν σε 9 bit όπου τα σημαντικότερα από αυτά είναι:
  1. **URG (Urgent Pointer).** Το πεδίο URG επιτρέπει στο ένα άκρο να πληροφορήσει το άλλο για κάτι σημαντικό, όπως να προχωρήσει στην επεξεργασία ενός

συγκεκριμένου octet, τη διακοπή της εξόδου με την πληκτρολόγηση κάποιου χαρακτήρα ελέγχου (control character) κ.α.

2. **ACK (Acknowledgment).** Το πεδίο αυτό δηλώνει ότι ο κόμβος που στέλνει το bit με τιμή 1 (On) επιβεβαιώνει τη λήψη δεδομένων.
3. **PSH (Push).** Το πεδίο αυτό ενημερώνει το παραλήπτη ότι πρέπει όσο το δυνατό γρηγορότερα να προωθήσει τα δεδομένα στο επίπεδο εφαρμογής.
4. **RST (Reset).** Το πεδίο αυτό κάνει επισημαίνει επανεκκίνηση /καθαρισμό της σύνδεσης
5. **SYN (Synchronize).** Το πεδίο αυτό χρησιμεύει για το συγχρονισμό της εγκατάστασης μιας νέας σύνδεσης χρησιμοποιώντας τα πεδία Αριθμός Σειράς έτσι ώστε να ξεκινήσει μία σύνδεση
6. **FIN (Finalize).** Το πεδίο αυτό ενημερώνει ότι ο αποστολέας έχει τελειώσει την μεταφορά δεδομένων.

Αναλυτικότερη περιγραφή αυτών των πεδίων θα γίνει στην ενότητα 4.1.4.

Ολοκληρώνοντας, η δομή του πακέτου του πρωτοκόλλου TCP περιέχει όλες πληροφορίες που απαιτούνται σε μια επικοινωνία που παρέχει υπηρεσίες με σύνδεση και αφορούν τα εξής:

- **Την Εγκατάσταση σύνδεσης** με συμφωνημένες προδιαγραφές επικοινωνίας μεταξύ των δυο άκρων
- **Την Αξιοπιστία** στην μετάδοση των δεδομένων. Απώλεια δεδομένων μετά τον έλεγχο σφαλμάτων απαιτεί αναμετάδοση.
- **Τον Έλεγχο ροής δεδομένων** δηλαδή τον έλεγχο ώστε να μην πλημμυρίσει ο παραλήπτης με δεδομένα από το αποστολέα.
- **Τον Έλεγχο Συμφόρησης δεδομένων** δηλαδή τον έλεγχο ώστε να μην πλημμυρίσει 'ένα αργό κανάλι επικοινωνίας με δεδομένα με κίνδυνο κατάρρευσης.

4.1.2 Πρωτόκολλο UDP - Δομή πακέτου

Το πρωτόκολλο User Datagram Protocol είναι ένα σχετικά απλούστερο πρωτόκολλο σε σχέση με το TCP που χρησιμοποιείται στο επίπεδο μεταφοράς.

Για την μεταφορά των datagrams δεν γίνεται εγκατάσταση σύνδεσης μεταξύ των δύο άκρων και δεν διασπάται το μήνυμα σε μικρότερα τμήματα όταν δεν υποστηρίζεται το μέγεθος του datagram. Κάθε αυτοδύναμο πακέτο μεταφέρεται μέσω δικτύων από κόμβο σε κόμβο μέχρι να φτάσει στο προορισμό του χωρίς να εγγυάται κανείς ότι δεν θα χαθεί ή θα καταστραφεί. Από την άλλη πλευρά όμως αυτή η απλότητα της δομής του και η έλλειψη ελέγχων προσδίδει στο UDP το πλεονέκτημα της αύξησης στην ταχύτητα μετάδοσης των δεδομένων και την απώλεια σε overhead δηλαδή της μείωσης χρησιμοποίησης των πόρων του δικτύου για μη ωφέλιμες εργασίες.

Το UDP έχει μέγεθος επικεφαλίδας μόνο 8 octets αφού οι πληροφορίες από όπου αποτελείται η επικεφαλίδα ενός datagram είναι:

- Ο **αριθμός Θύρας Προέλευσης** και ο **αριθμός Θύρας Προορισμού**. (Source Port & Destination Port)
- Το **μήκος του datagram (Length).** Το ελάχιστο μήκος είναι 8 octets δηλαδή μόνο η επικεφαλίδα, και το μέγιστο μέγεθος φτάνει τα 64534 octets (64Kb) μαζί με την επικεφαλίδα.
- Το **Άθροισμα Έλεγχου (Checksum).** Είναι προαιρετικό πεδίο 16-bit το οποίο χρησιμοποιείται για επαλήθευση της ορθότητας του datagram κατά την παραλαβή

του στην πλευρά του παραλήπτη. Υπολογίζει το άθροισμα τη κεφαλίδας και των δεδομένων και η λειτουργία του είναι παρόμοια με του TCP.

Επομένως όπως έχει ήδη περιγραφεί το TCP είναι κατάλληλο για εφαρμογές που απαιτούν την αξιόπιστη μεταφορά των δεδομένων. Αντίθετα το UDP χρησιμοποιείται σε εφαρμογές όπου δεν έχει τόση σημασία η πληρότητα της μεταφοράς των δεδομένων σε σύγκριση με την ταχύτητα που θα παραληφθούν.

Εικόνα 4.1.2.α: Πεδία της επικεφαλίδας ενός UDP τμήματος.

Τέτοιες εφαρμογές είναι:

- αυτές οι οποίες μεταδίδουν σε πραγματικό χρόνο ροές video και ήχου (real-time audio/video), όπως IPTV, VoIP. Εδώ μας ενδιαφέρει τα δεδομένα να φτάνουν τη σωστή χρονική στιγμή. Οποιαδήποτε απώλειά τους μας επηρεάζει μόνο στην ποιότητα του αναπαραγόμενου σήματος.
- Servers, οι οποίοι απαντούν σε μικρά αιτήματα ενός τεράστιου αριθμού από πελάτες/clients, όπως στα δικτυακά online παιχνίδια. Οι Servers, χρησιμοποιώντας UDP, δεν απασχολούνται με το να ελέγχουν την κατάσταση της κάθε σύνδεσης και έτσι μπορούν να εξυπηρετήσουν ένα πολύ μεγαλύτερο αριθμό χρηστών σε αντίθεση με το αν χρησιμοποιούσαν TCP.

Παρόλα αυτά αν απαιτείται να λυθούν και θέματα αξιοπιστίας, ελέγχου ροής, τεμαχισμού των πακέτων κ.λπ., τότε αναλαμβάνει το επίπεδο εφαρμογής να διαχειριστεί αυτά τα ζητήματα. Επίσης πρέπει να σημειωθεί το πρόβλημα δικτυακής συμφόρησης που πρέπει να αναλάβει το επίπεδο εφαρμογής στην περίπτωση κατά την οποία ένας αποστολέας UDP πλημμυρίσει το δίκτυο με πακέτα. Επίσης είναι απαραίτητο οι συσκευές του ενδιάμεσου δικτύου (Δρομολογητές) να χρησιμοποιούν τεχνικές έλεγχου, που αποθηκεύουν προσωρινά ή απορρίπτουν τα πακέτα UDP ώστε να αποφευχθεί πιθανή κατάρρευση.

4.2 Υποδοχές (sockets)

Όπως έχει ήδη περιγραφεί το επίπεδο μεταφοράς χρησιμοποιεί τα πρωτόκολλα TCP και UDP για την μεταφορά δεδομένων πάνω από ένα επικοινωνιακό κανάλι με διαφανή τρόπο προς τις εφαρμογές που βρίσκονται στο παραπάνω επίπεδο.

Όμως, πώς υλοποιείται αυτή η σύνδεση προγραμματιστικά στους τερματικούς κόμβους των δυο άκρων, και πώς προωθούνται από τις διεργασίες τα δεδομένα στο επίπεδο μεταφοράς ανεξάρτητα με τις διαδικασίες των πρωτοκόλλων που υλοποιούνται σ' αυτό;

Την απάντηση σ' αυτό την δίνουν οι υποδοχές (sockets).

Η **υποδοχή (socket)** είναι μια οντότητα η οποία χρησιμοποιείται στην ανάπτυξη εφαρμογών για την επικοινωνία μεταξύ δύο άκρων πάνω σε ένα αμφίδρομο κανάλι και αντιπροσωπεύει το τερματικό σημείο που καταλήγει ή ξεκινά η μεταφορά των δεδομένων.

Έτσι σε κάθε επικοινωνία πρέπει να υπάρχουν δύο socket που κάθε ένα πρέπει να καθορίζεται από το πρωτόκολλο και την διεύθυνση του. Η διεύθυνση ορίζεται από την διεύθυνση IP και τον αριθμό θύρας.

Έστω για παράδειγμα ότι στο ένα άκρο έχουμε μια εφαρμογή ηλεκτρονικού ταχυδρομείου και στο άλλο άκρο έχουμε την εφαρμογή εξυπηρέτησης (server) που εξυπηρετεί χρήστες αποθηκεύοντας στο λογαριασμό τους τα μηνύματα που έρχονται γι' αυτούς.

Κάποια στιγμή αποφασίζει ένας πελάτης να στείλει μέσω αξιόπιστης σύνδεσης ένα μήνυμα ηλεκτρονικού ταχυδρομείου. Τα βήματα που ακολουθούνται για την εγκατάσταση της σύνδεσης είναι τα εξής:

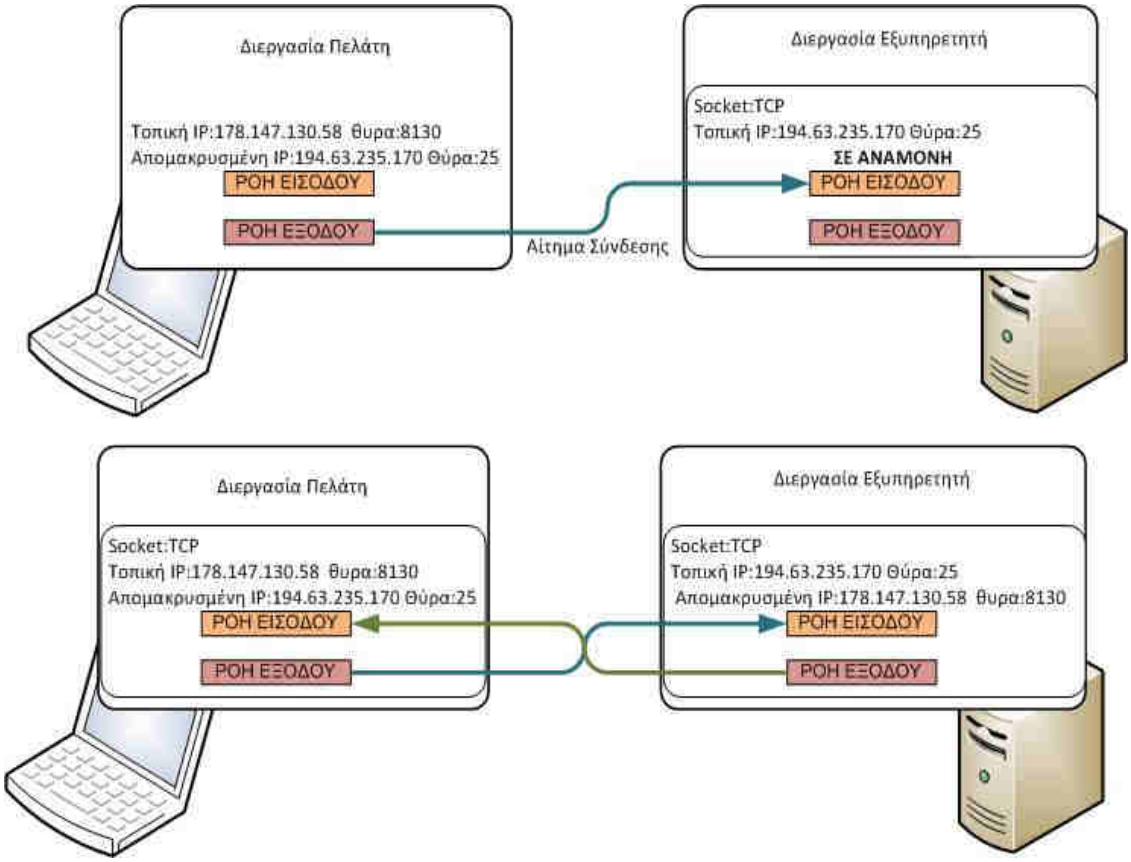
- Μέσω της εφαρμογής ηλεκτρονικού ταχυδρομείου δημιουργείται μια διεργασία στον υπολογιστή για την αποστολή ενός νέου μηνύματος.
- Στο άλλο άκρο στην εφαρμογή που δέχεται μηνύματα αλληλογραφίας έχει ήδη δημιουργηθεί μια διεργασία που δέσμευσε ένα TCP socket με την διεύθυνση IP του εξυπηρετητή (έστω η διεύθυνση **194.63.235.170**) και την θύρα (port) που αντιστοιχεί στην υπηρεσία εξυπηρέτησης ηλεκτρονικού ταχυδρομείου (θύρα **25**). Κατόπιν η διεργασία στην πλευρά του εξυπηρετητή πέρασε σε κατάσταση αναμονής, περιμένοντας το αίτημα εγκατάστασης σύνδεσης από κάποιο πελάτη.

Όπως έχει ήδη αναφερθεί οι αριθμοί θύρας (Ports) αποτελούν το όνομα της σύνδεσης σε κάθε άκρο, δηλαδή σε κάθε socket. Οι θύρες έχουν εύρος 65536 διαφορετικών τιμών. Όμως όλοι οι αριθμοί κάτω από 1023 ονομάζονται Γνωστές (Well-Known) θύρες και είναι δεσμευμένες από συγκεκριμένες τυπικές υπηρεσίες στο άκρο του εξυπηρετητή. Για παράδειγμα οι θύρες και υπηρεσίες, 21-FTP (Μεταφορά αρχείων, 23-Telnet (Απομακρυσμένη Διαχείριση), 25-E-mail κ.λπ.

- Η διεργασία του πελάτη αποστέλλει ένα αίτημα για την εγκατάσταση σύνδεσης με στοιχεία την διεύθυνση IP και τη θύρα του εξυπηρετητή.
- Ο εξυπηρετητής αποδέχεται το αίτημα του πελάτη και αποθηκεύει τη διεύθυνση και τη θύρα του. Η εφαρμογή στον εξυπηρετητή μπορεί να παρέχει υπηρεσίες μόνο σ' ένα πελάτη με το συγκεκριμένο socket. Αν ήθελε να δέχεται πολλαπλές αιτήσεις σύνδεσης, ο εξυπηρετητής θα έπρεπε να δημιουργεί ένα καινούργιο socket για κάθε νέα αίτηση πελάτη.
- Με την επιβεβαίωση της αποδοχής του αιτήματος ο πελάτης δημιουργεί το socket, για παράδειγμα με τη διεύθυνση IP 178.147.130.58 και τη θύρα **8130**.
- Το socket στο άκρο του πελάτη συνδέεται με μεθόδους (εντολές) εξόδου ροής δεδομένων προς το κανάλι, ενώ αντίστοιχα το socket στον εξυπηρετητή συνδέεται με το κανάλι επικοινωνίας με μεθόδους εισόδου ροής δεδομένων από το κανάλι.
- Όταν η επικοινωνία ολοκληρωθεί στέλνεται αίτημα τερματισμού και απελευθερώνεται το socket του χρήστη ενώ στην πλευρά του εξυπηρετητή αποδεσμεύεται το socket από τη σύνδεση και επιστρέφει σε κατάσταση αναμονής.

Έτσι με τη χρήση των TCP sockets επιτυγχάνεται η αξιόπιστη συνδιάλεξη μεταξύ εφαρμογών από άκρο σε άκρο πάνω από ένα τηλεπικοινωνιακό κανάλι.

Στην περίπτωση όμως των υποδοχών UDP - sockets δεν υπάρχει αυτή η αλληλουχία ανταλλαγής μηνυμάτων για την εγκατάσταση της σύνδεσης και μεταφοράς των δεδομένων. Η πληροφορία μεταδίδεται στο δίκτυο με βάση τη διεύθυνση και την θύρα και χρησιμεύει μόνο για τη σύνδεση της εφαρμογής με το κανάλι. Η πληροφορία αν τα καταφέρει δια μέσω των δικτύων που διαπερνά καταφθάνει σε ανεξάρτητα πακέτα στο παραλήπτη.



Εικόνα 4.2.α: Υποδοχές (Sockets) TCP

4.3 Συνδέσεις TCP - Έναρξη/τερματισμός σύνδεσης

Η μετάδοση των πληροφοριών μεταξύ των δύο άκρων με τη χρήση του πρωτοκόλλου TCP γίνεται σε τρεις φάσεις:

- Εγκατάσταση Σύνδεσης
- Μεταφορά δεδομένων
- Τερματισμός Σύνδεσης

Εγκατάσταση Σύνδεσης. Για την εγκατάσταση μίας νέας σύνδεσης σε μια αξιόπιστη συνδιάλεξη μεταξύ δύο άκρων το TCP χρησιμοποιεί την μέθοδο χειραψίας τριών βημάτων (three-way handshake).

- Ο τερματικός κόμβος (host) Α ενεργοποιεί τη σύνδεση στέλνοντας ένα **Τμήμα Συγχρονισμού** TCP με το πεδίο **SYN** σε τιμή **ON** και ένα **αρχικό τυχαίο αριθμό** στο πεδίο **Αριθμό Σειράς** (Initial Sequence Number) έστω ο **ISN A = x** στα αντίστοιχα πεδία της επικεφαλίδας.

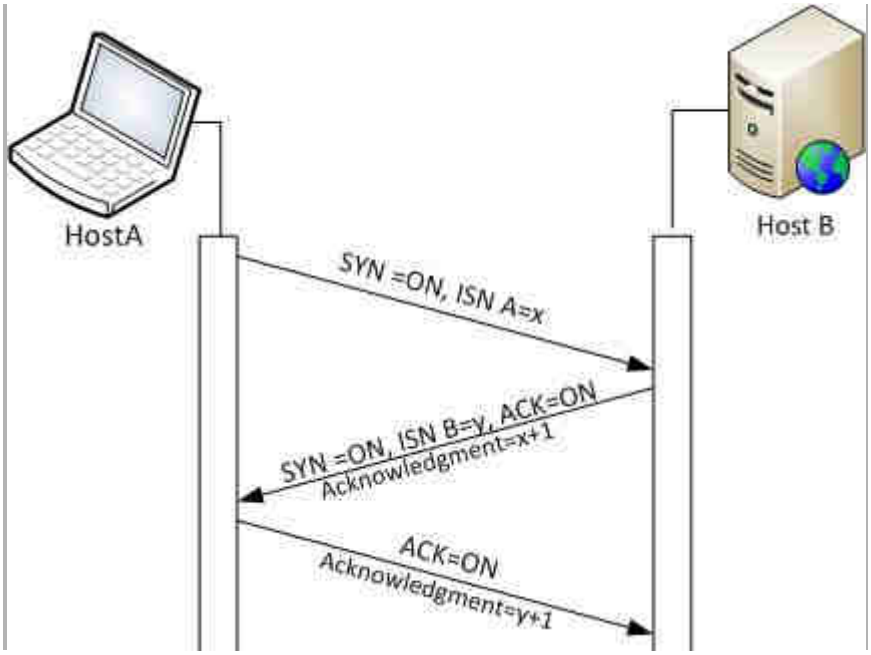
Ο αρχικός αριθμός στο πεδίο Αριθμός Σειράς είναι τυχαίος γιατί αν ήταν ίδιος στην περίπτωση δυο συνδέσεων με την ίδια θύρα και έχουν δημιουργηθεί με μικρή χρονική διαφορά, και η μια έχει ήδη τερματιστεί υπάρχει περίπτωση να εμφανιστούν τμήματα της παλαιότερης σύνδεσης στην νεότερη.

- Ο τερματικός κόμβος (host) Β παραλαμβάνει το **Τμήμα Συγχρονισμού**, το επεξεργάζεται και απαντά με ένα δικό του **Τμήμα Συγχρονισμού** TCP, όπου στο πεδίο **SYN** ορίζεται σε τιμή **ON** και ένα δικό του αρχικό Αριθμό Σειράς **ISN B=y**. Επίσης τοποθετεί την τιμή στο πεδίο **ACK=ON** και στο πεδίο στο πεδίο **Αριθμός**

Επιβεβαίωσης (Acknowledgment) την τιμή **x+1** για να δηλώσει ότι το επόμενο αναμενόμενο octet από τον κόμβο Α που θα ξεκινά να περιέχει δεδομένα.

Στο TCP ένα τμήμα επιβεβαίωσης προσδιορίζει τον επόμενο Αριθμό Σειράς που αναμένεται να λάβει με ένα τμήμα δεδομένων και με αυτό το τρόπο επιβεβαιώνονται όλοι οι προηγούμενοι Αριθμοί Σειράς που έχουν ληφθεί.

- Αφού ο κόμβος Α παραλάβει την απάντηση από τον κόμβο Β ολοκληρώνει την εγκατάστασης της σύνδεσης στέλνοντας ένα τρίτο Τμήμα Επιβεβαίωσης ACK στον κόμβο Β. Σ΄ αυτό το Τμήμα ο κόμβος Α θέτει το πεδίο ACK=ON και υποδηλώνει ότι το επόμενο αναμενόμενο octet από τον κόμβο Β με την τιμή στο πεδίο Αριθμός Επιβεβαίωσης (Acknowledgment) = y+1.



Εικόνα 4.3.α: Εγκατάσταση νέας Σύνδεσης με τριμερή χειραψία.

Το TCP όπως έχει ήδη περιγραφεί είναι πρωτόκολλο προσανατολισμένο στη σύνδεση. Δέχεται ροές (streams) από δεδομένα octets και τα περνάει από το επίπεδο της εφαρμογής στο επίπεδο δικτύου. Επίσης το TCP χρησιμοποιεί ενταμιευτές (buffers) για να αποθηκεύσει τα εισερχόμενα και εξερχόμενα δεδομένα (ροές εισόδου, και εξόδου). Οι εφαρμογές στέλνουν τις ροές δεδομένων στο TCP όπου τις αποθηκεύει στους ενταμιευτές.

Μεταφορά δεδομένων. Το TCP στηρίζεται σε τρείς παράγοντες προκειμένου να αποφασίσει κάθε φορά πόσα octets μπορεί να στείλει με ένα τμήμα δεδομένων.

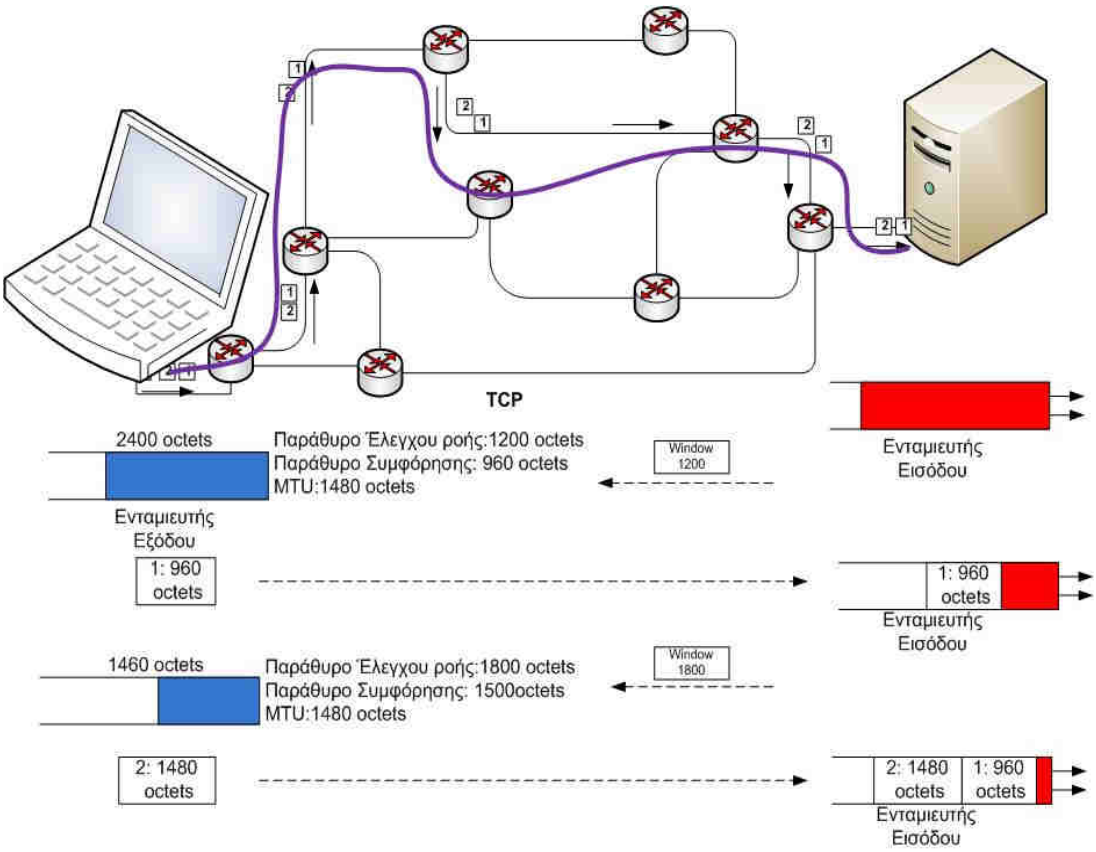
- Ο πρώτος παράγοντας είναι η τιμή του πεδίου **Παράθυρο** που ανακοινώνει το κάθε άκρο με βάση το **μηχανισμό έλεγχου ροής.** Με άλλα λόγια η τιμή του Παράθυρου (Window) έχει ανακοινωθεί σε κάποιο τμήμα του πεδίου της επικεφαλίδας από τον παραλήπτη.
- Σε επόμενο στάδιο λαμβάνει υπόψη του από το **μηχανισμό ελέγχου συμφόρησης** μια τιμή που αναφέρεται ως **Παράθυρο Συμφόρησης** ώστε να μην πλημμυρίσει ο αποστολέας με δεδομένα το δίκτυο. Για τον έλεγχο της συμφόρησης το TCP διατηρεί μια μεταβλητή όπου η τιμή της μπορεί να μεταβάλλεται, καθώς

μεταβάλλεται η ροή δεδομένων (φόρτος) μεταξύ των συσκευών(δρομολογητές) του ενδιαμέσου δικτύου.

- Ο τελευταίος παράγοντας που λαμβάνεται υπόψη στο TCP είναι το όριο που έχει τεθεί από το φυσικό επίπεδο και είναι γνωστό ως μέγιστη μονάδα εκπομπής (MTU). Στο Ethernet είναι 1500 octets ανά πακέτο.

Το TCP επιλέγει το μικρότερο μέγεθος δεδομένων από τους τρεις παράγοντες.

Για παράδειγμα όπως φαίνεται στην εικόνα 4.1.4.β έστω ότι ο ενταμιευτής εξόδου του παραλήπτη περιέχει 2400 octets που πρέπει να μεταφέρει χωρίς την επικεφαλίδα. Το παράθυρο του παραλήπτη έχει καθοριστεί σε 1200 octets, ο μηχανισμός ελέγχου συμφόρησης έχει καθορίστει στο όριο 960 octets και το φυσικό επίπεδο δικτύου έχει ορίσει την MTU σε 1460 octets. Επιλέγεται το μικρότερο μέγεθος τα 940octets +20 octets επικεφαλίδα και μεταφέρεται ένα τμήμα στο παραλήπτη.



ΕιΕικόνα 4.1.4.β: Εγκατάσταση νέας Σύνδεσης με τριμερή χειραψία.

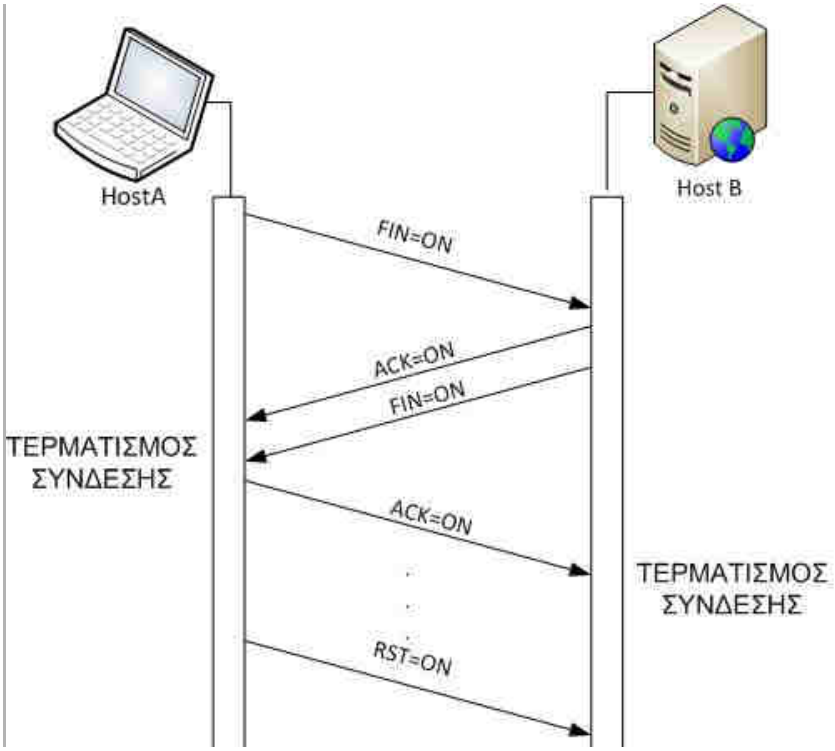
Το μέγεθος το δεδομένων που μεταφέρονται κάθε φορά μπορεί να μεταβάλλεται αφού ο παραλήπτης μπορεί να απελευθερώνει χωρητικότητα στον ενταμιευτή εισόδου όσο το TCP επεξεργάζεται τα δεδομένα που παραλαμβάνει ή το ενδιάμεσο δίκτυο μπορεί να είναι λιγότερο φορτωμένο. Οπότε ο παραλήπτης μπορεί να ανακοινώσει μια νέα τιμή στο πεδίο **Παράθυρο** της επικεφαλίδας ενός τμήματος που ελέγχει την ροή δεδομένων.

Στο παράδειγμα της εικόνας 4.1.4.β επειδή ελευθερώνεται ο χώρος στον ενταμιευτή του παραλήπτη, ανακοινώνεται στον αποστολέα νέο Παράθυρο με μέγεθος 1800 octets. Παράλληλα γίνεται επιβεβαίωση του τμήματος που έχει παραληφθεί με τμήμα ACK και ενημερώνει για το επόμενο octet δεδομένων που μπορεί να παραλάβει στο πεδίο Αριθμός Επιβεβαίωσης. Επίσης το ενδιάμεσο δίκτυο μπορεί να έχει επιλύσει προβλήματα φόρτου που πιθανόν να υπήρχαν σε κάποιο δρομολογητή και ο μηχανισμός έλεγχου φόρτου να

ενημερώσει το Παράθυρο Συμφόρησης σε 1500 octets. Έτσι το TCP στη πλευρά του αποστολέα αποφασίζει να στείλει τα υπόλοιπα δεδομένα (1460 δεδομένα+20 επικεφαλίδα) αφού σ' αυτή τη περίπτωση το όριο που αποφασίστηκε είναι η μονάδα MTU 1480 octets.

Τερματισμός Σύνδεσης

Αφού μεταδοθούν όλα τα δεδομένα για το τερματισμό της σύνδεσης αποστέλλεται από το άκρο του αποστολέα Α αποκλειστικά ένα TCP τμήμα χωρίς δεδομένα με το πεδίο (Finalize-FIN) σε τιμή ON. Όταν ο κόμβος Β παραλάβει το αρχικό **Τμήμα Τερματισμού**, αμέσως επιβεβαιώνει την παραλαβή του με ένα τμήμα ACK, και μεταφέρει στο επίπεδο εφαρμογής την αίτηση τερματισμού μεταφοράς δεδομένων. Αφού η εφαρμογή στο κόμβο Β αποφασίσει το τερματισμό της συνομιλίας ενημερώνει το TCP όπου στέλνει το δικό του τμήμα Τερματισμού στο κόμβο Α. Αφού το παραλάβει ο Α επιβεβαιώνει με ένα τμήμα ACK τη λήψη και θέτει το πεδίο RST με τιμή ON.



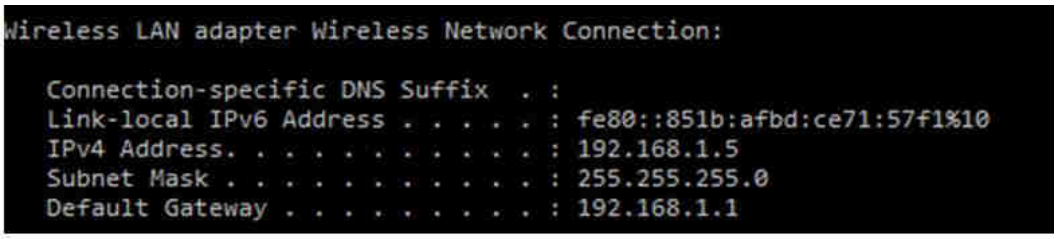
Εικόνα 4.3.γ: Τερματισμός Σύνδεσης.

Κάθε πλευρά που στέλνει ένα τμήμα FIN περιμένει να λάβει επιβεβαίωση για συγκεκριμένο χρονικό διάστημα και αν δεν το λάβει επανεκπέμπει ένα τμήμα FIN. Όμως αυτό μπορεί να οδηγήσει σε συνεχείς αναμεταδόσεις του τμήματος τερματισμού. Γι' αυτό το λόγο μετά από χρόνο που αντιστοιχεί σε διάστημα δυο εκπομπών του τμήματος τερματισμού και επιστροφής της επιβεβαίωσης, διακόπτεται η σύνδεση.

Ερωτήσεις - Ασκήσεις Κεφαλαίου

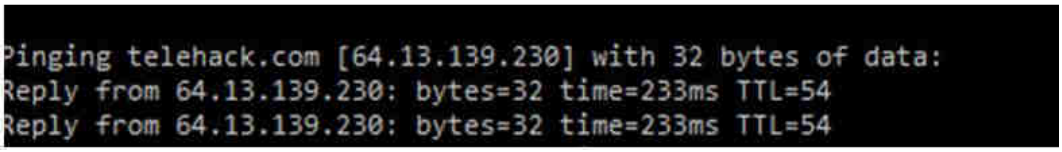
1. Ποιες υπηρεσίες παρέχει το επίπεδο μεταφοράς;
2. Γιατί είναι πιθανό ο παραλήπτης να απορρίψει ένα τμήμα TCP θεωρώντας το αναξιόπιστο;
3. Ποιους ελέγχους λαμβάνει υπόψη του το TCP για να αποφασίσει για το μέγεθος τμήματος που πρέπει να μεταδώσει;
4. Σε ποια ζητήματα διαφέρει το TCP από το UDP;
5. Σε ποιες εφαρμογές εφαρμόζεται το πρωτόκολλο UDP.
6. Ποιες είναι οι φάσεις για να ξεκινήσει την μεταφορά δεδομένων το TCP από την προέλευση στο προορισμό;
7. Ένας χρήστης ξεκινά μια εγκατάσταση σύνδεσης από το φορητό του υπολογιστή με ένα απομακρυσμένο εξυπηρετητή τον telehack.com με την υπηρεσία telnet. Για να ανακαλύψει τα socket προέλευσης και προορισμού εκτελεί τις παρακάτω τρεις εντολές.

Ipconfig



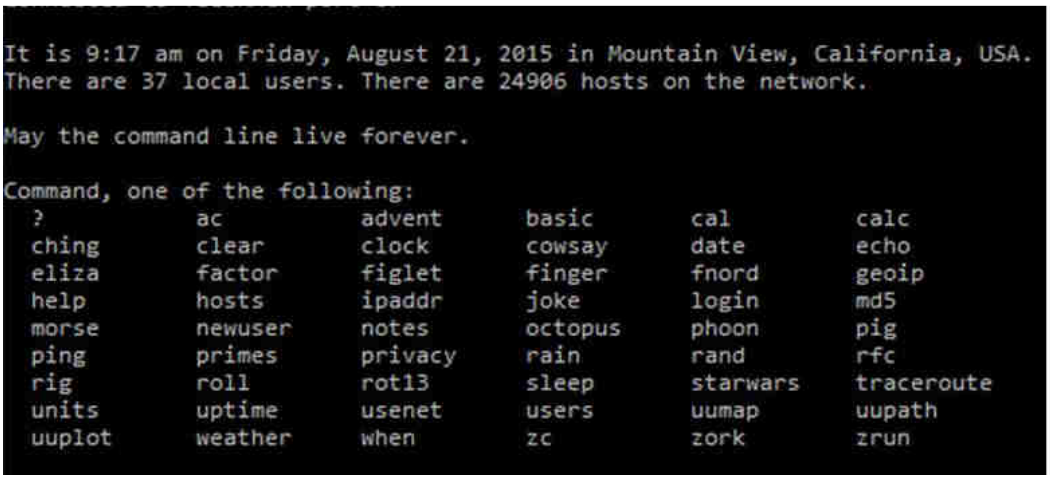
Εικόνα 1: Αποτέλεσμα εκτέλεσης εντολής ipconfig

ping telehack.com



Εικόνα 2: Αποτέλεσμα εκτέλεσης εντολής ping

telnet telehack.com



Εικόνα 3: Αποτέλεσμα εκτέλεσης εντολής telnet

Συμπληρώστε τα χαρακτηριστικά του κάθε socket.

Socket Προέλευσης: IP : ….. ….. ……. ……. : Θύρα: …….

Socket Προορισμού: IP : ….. ….. ……. ……. : Θύρα: …….

Σημείωση: Η Άσκηση μπορεί να εφαρμοστεί στο εργαστήριο.

8. Αν μια ροή δεδομένων το TCP έχει γεμίσει το ενταμιευτή εξόδου με 3600 bytes και πρέπει να μεταφερθούν μέσω μιας εγκατεστημένης σύνδεσης σε ένα εξυπηρετητή. Αν το Παράθυρο Συμφόρησης είναι 1400 bytes, το πεδίο της επικεφαλίδας Παράθυρο 1200 bytes, η MTU 1500 bytes και η επικεφαλίδα ορίζεται σε 20 bytes απαντήστε στα παρακάτω:
   - Θα χρειαστεί να τεμαχίσει τα δεδομένα το TCP; Αν ναι, ποιο είναι το μέγεθος του τμήματος που θα αποφασίσει να στείλει το TCP;
   - Αν κατά την επιβεβαίωση της λήψης του πρώτου τμήματος αλλάξει το μέγεθος του παράθυρου σε 2440 bytes και το παράθυρο συμφόρησης σε 3200 bytes, πόσα πρέπει να είναι και ποιο το μέγεθος των τμημάτων που ακολουθούν.
9. Κατά την εγκατάσταση σύνδεσης ο αποστολέας έχει δημιουργήσει ένα αρχικό Αριθμό Σειράς = 4567802006. Όταν ο αποστολέας παραλάβει το αρχικό τμήμα συγχρονισμού και επιστρέψει την επιβεβαίωση ποιες τιμές θα περιλαμβάνουν τα πεδία ACK, και Αριθμός Επιβεβαίωσης; Σχετίζεται ο Αριθμός Σειράς που στέλνει ο παραλήπτης με το δικό του τμήμα συγχρονισμού και αν ναι ποια είναι η τιμή του;
10. Πώς γίνεται ο έλεγχος ροής δεδομένων στο TCP;
11. Τι είναι το Παράθυρο Συμφόρησης και για ποιο λόγο χρησιμοποιείται;
12. Αναφέρετε τους παράγοντες με βάση τους οποίους το TCP αποφασίζει για το μέγεθος του επόμενου τμήματος δεδομένων που πρόκειται να στείλει
13. Αν κατά την εγκατάσταση μιας σύνδεσης μεταφέρονται με τα τμήματα συγχρονισμού και από τις δυο άκρες οι εξής πληροφορίες.
    Πελάτης:
    [Αριθμός Σειράς: 4567802006, Παράθυρο:65535, Μέγιστο Μήκος Τμήματος:1536]
    Εξυπηρετητής:
    [Αριθμός Σειράς: 3277203904, Παράθυρο:4580, Μέγιστο Μήκος Τμήματος:1245]
    Περιγράψτε τις επικεφαλίδες στα τμήματα επιβεβαίωσης που αποστέλλονται και από τις δυο πλευρές.
14. Πώς τερματίζεται μια σύνδεση που έχει σταλεί ένα τμήμα FIN από το πελάτη αλλά η επικοινωνία έχει διακοπεί από την πλευρά του εξυπηρετητή;

Έλεγχος και δημιουργία TCP/UDP συνδέσεων με τη χρήση εντολής netstat, τη βοήθεια της εντολής ping και εργαλείων του λειτουργικού συστήματος.

Στην άσκηση θα μελετηθούν οι βασικές έννοιες όπως:

- Τα πρωτόκολλα TCP/UDP
- Οι θύρες επικοινωνίας (Ports)
- Οι Διευθύνσεις IP
- Το πρωτόκολλο ICMP και σύστημα DNS.
- Η έννοια των υποδοχών (sockets) και η έννοια της σύνδεσης.

Στόχοι είναι

- Η αναγνώριση της σχέσης των διεργασιών που δημιουργούνται από τις εφαρμογές με τη σύνδεση τους με τα αντίστοιχα sockets.
- Η απόκτηση της ικανότητας χρησιμοποίησης εντολών σε γραμμή τερματικού του λειτουργικού συστήματος και γενικότερα εργαλείων για τον έλεγχο της δικτυακής επικοινωνίας στο επίπεδο μεταφοράς.

Περιγραφή ομαδοσυνεργατικών δραστηριοτήτων

Βήμα 1: Κατανόηση Εντολής netstat.

Ξεκινάμε την οθόνη εξομοίωσης γραμμής εντολών των Windows εκτελώντας την εντολή **cmd.exe** και μέσα από την οθόνη εκτελούμε την εντολή **netstat -o**

Η εντολή εμφανίζει σε μορφή λίστας όλες τις ενεργές συνδέσεις των πρωτοκόλλων TCP/UDP με τις αντίστοιχες πληροφορίες για τα socket προέλευσης και προορισμού.

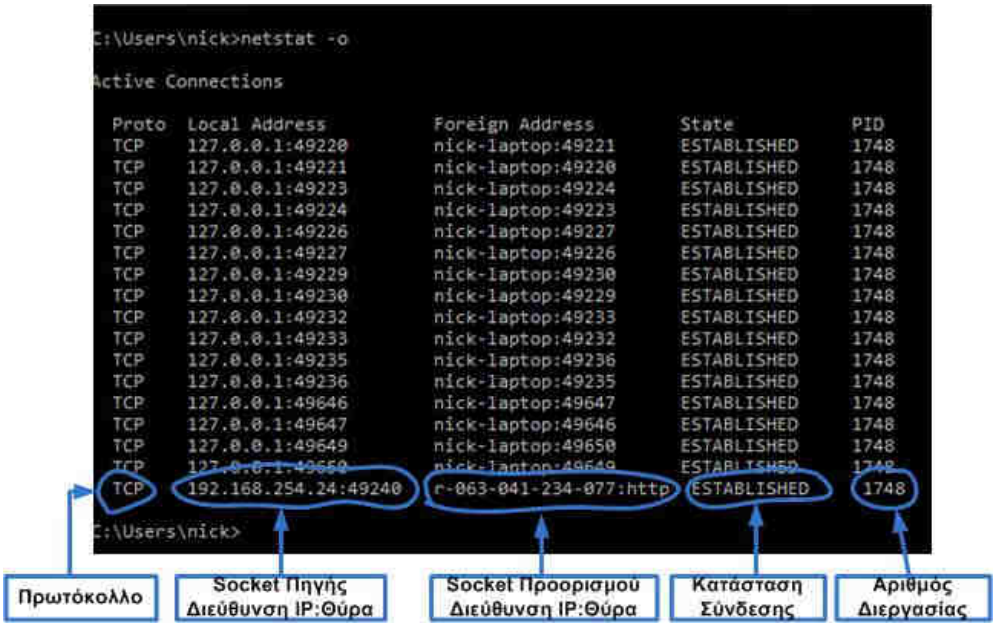
Την παράμετρο "-o" την εισάγουμε για να μας εμφανιστεί στο τέλος κάθε γραμμής της λίστας ο μοναδικός αριθμός (ProcessID-PID) που αντιστοιχεί στην διεργασία που εκτελείται αυτή τη στιγμή στην μνήμη RAM του υπολογιστή και έχει δημιουργηθεί από κάποια εφαρμογή.

Αν εξερευνήσουμε τη λίστα θα δούμε ότι στη στήλη Κατάσταση (Status) εμφανίζεται η πληροφορία Εγκατεστημένη "Established" δηλαδή έχει γίνει η σύνδεση μεταξύ των δύο άκρων.

Οι τιμές για την πληροφορία Κατάστασης (State) είναι:

- **SYN_SEND**. Σηματοδοτεί την έναρξη σύνδεσης.
- **SYN_RECEIVED**. ο Εξυπηρετητής μόλις παρέλαβε το μήνυμα έναρξης σύνδεσης
- **ESTABLISHED**. Ο πελάτης παρέλαβε από το Εξυπηρετητή το δικό του μήνυμα SYN και η σύνδεση εγκαταστάθηκε.
- **LISTEN**. Ο εξυπηρετητή είναι σε ακρόαση, έτοιμος να δεχτεί συνδέσεις.
- **FIN_WAIT_1**. Σηματοδοτεί ότι έχει γίνει αποστολή τμήματος για τερματισμό της σύνδεσης.
- **TIMED_WAIT**. Ο πελάτης μπαίνει σε κατάσταση αναμονής μετά την κατάσταση αποστολής τμήματος για τερματισμό της σύνδεσης.
- **CLOSE_WAIT**. Ο εξυπηρετητής μπαίνει σε κατάσταση αναμονής μόλις παραλάβει το μήνυμα FIN από τον πελάτη και ενημερώσει το επίπεδο εφαρμογής για τερματισμό της σύνδεσης.
- **FIN_WAIT_2**. Ο πελάτης παρέλαβε την επιβεβαίωση μετά την αποστολή του τμήματος τερματισμού FIN που είχε στείλει στον εξυπηρετητή.
- **LAST_ACK**. Ο εξυπηρετητής είναι στην κατάσταση μετά από αποστολή στο πελάτης το δικό του τμήμα τερματισμού FIN.
- **CLOSED**. Ο εξυπηρετητής παρέλαβε την επιβεβαίωση ACK από τον πελάτη και η σύνδεση έκλεισε.

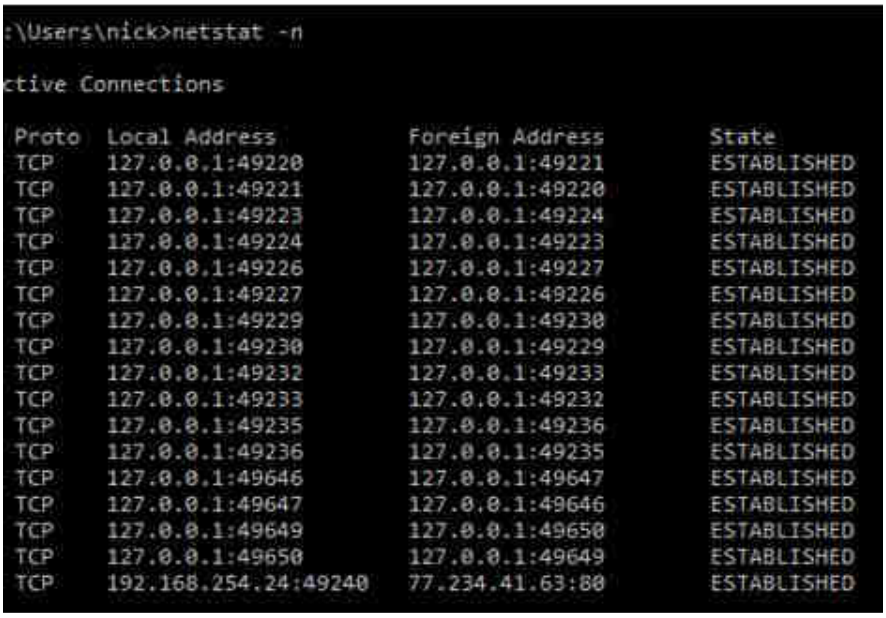
Παρατηρώντας τη λίστα διαπιστώνουμε αρκετές συνδέσεις TCP σε κατάσταση σύνδεσης αλλά είναι συνδεδεμένη μόνο με μια διαδικασία με PID:1748. Σε μια από αυτές διαπιστώνουμε ότι το socket προορισμού είναι διαφορετικό από το τοπικό τερματικό κόμβο. r-063-041-234-077:http.



Εικόνα 4: Εκτέλεση εντολής netstat -o

Αν θέλουμε να εμφανίζονται πάντα στις στήλες προέλευσης και προορισμού οι IP διευθύνσεις και οι αριθμοί πόρτας χρησιμοποιούμε την παράμετρο -n.

netstat -n



Εικόνα 5: Εκτέλεση εντολής netstat -n

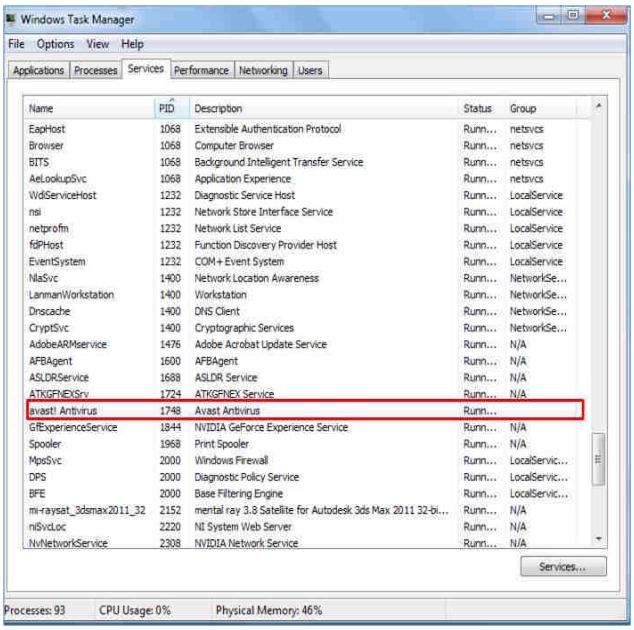
Βλέπουμε ότι η πραγματική διεύθυνση IP προορισμού είναι 77.234.41.63.88 και η θύρα προορισμού 80 που είναι δεσμευμένη για την υπηρεσία http.

Η εντολή netstat από προεπιλογή εμφανίζει μόνο τις συνδέσεις TCP. Αν θέλουμε να εμφανιστούν όλες οι συνδέσεις χρησιμοποιούμε την παράμετρο **-a** ενώ αν θέλουμε να δούμε μόνο τις UDP συνδέσεις χρησιμοποιούμε την παράμετρο **-p [πρωτόκολλο]**.

```
netstat -a
netstat -p udp
```

Βήμα 2: Διερεύνηση Σύνδεσης

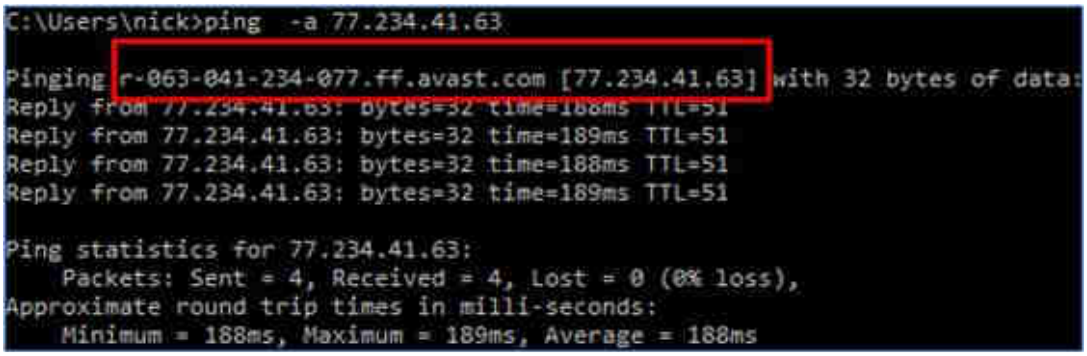
Μπορούμε να ανακαλύψουμε την εφαρμογή που δημιούργησε τη διεργασία που αντιστοιχεί στη συγκεκριμένη σύνδεση χρησιμοποιώντας τον διαχειριστή εργασιών Task Manager των Windows: στην καρτέλα υπηρεσίες (services) αναζητούμε την διεργασία με PID:1748 του συγκεκριμένου παραδείγματος. Έτσι ανακαλύπτουμε ότι η συγκεκριμένη διεργασία αντιστοιχεί στο πρόγραμμα antivirus.



Εικόνα 6: Οι υπηρεσίες (services) που εκτελούνται στα Windows

Από την άλλη πλευρά μπορούμε να ελέγξουμε την διεύθυνση IP του προορισμού χρησιμοποιώντας την εντολή ping με την παράμετρο -a, ώστε να γίνει αίτημα στην υπηρεσία ονοματοδοσίας DNS για να μας επιστρέψει το πλήρες όνομα που αντιστοιχεί στο τερματικό κόμβο που παρέχει τη συγκεκριμένη υπηρεσία.

```
Ping -a 77.234.41.63
```



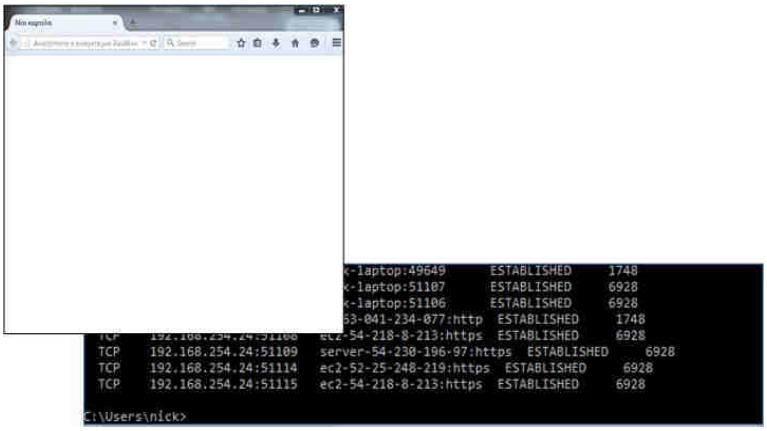
Εικόνα 7: Εκτέλεση εντολής ping -a

Εναλλακτικά μπορεί να χρησιμοποιηθεί ή η παράμετρος **-f** στην εντολή netstat.

```
netstat -f -o
```

Βήμα 3: Εκκίνηση μιας νέας σύνδεσης

Για να δημιουργήσουμε μια νέα TCP σύνδεση ξεκινάμε ένα φυλλομετρητή για παράδειγμα τον Firefox. Καλύτερα είναι να ξεκινήσουμε την εφαρμογή σε ασφαλή κατάσταση και η αρχική σελίδα να είναι κενή. Αυτό συμβαίνει επειδή συνήθως οι φυλλομετρητές φορτώνουν πρόσθετα και γραμμές εργαλείων με συνδέσεις σε διάφορους δικτυακούς τόπους και επίσης οι δημοφιλείς ιστοσελίδες περιέχουν διαφημίσεις και συνδέσμους σε τρίτους δικτυακούς τόπους.



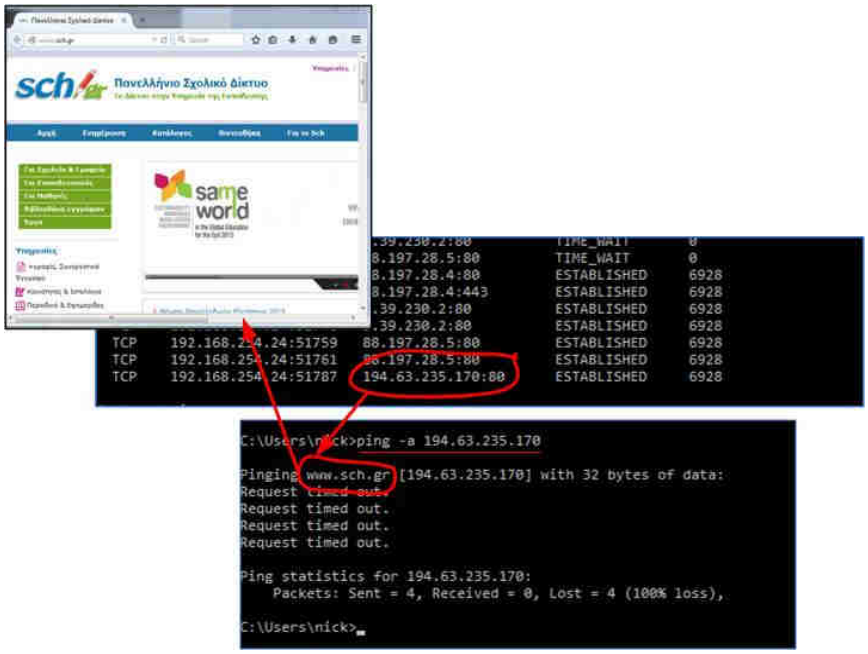
Εικόνα 8: Εγκατάσταση μιας νέας σύνδεσης

Αν εκτελέσουμε την εντολή netstat -o βλέπουμε ότι μια καινούργια διεργασία έχει δημιουργηθεί με PID:6928.

Ελέγχοντας στη διαχείριση εργασιών τη καρτέλα υπηρεσίες διαπιστώνουμε ότι η διεργασία έχει δημιουργηθεί από την εφαρμογή του firefox.

Αν τώρα στο φυλλομετρητή δώσουμε την διεύθυνση του πανελλήνιου σχολικού δικτύου www.sch.gr και εκτελέσουμε την εντολή netstat -n -o θα δούμε την νέα διεύθυνση IP στο socket προορισμού.

Χρησιμοποιώντας την εντολή ping με την διεύθυνση IP διασταυρώνουμε τη σύνδεση με το σχολικό δίκτυο.



Εικόνα 9: Διασταύρωση της σύνδεσης στη πλευρά του εξυπηρετητή

Δραστηριότητες

1. Εκτελέστε την εντολή netstat -a χωρίς να έχετε φορτώσει κάποια δικτυακή εφαρμογή στην μνήμη.
2. Διερευνήστε τις ενεργές συνδέσεις που εμφανίζονται, καταγράψτε τα socket και την κατάσταση που βρίσκονται. Προσπαθήστε να δικαιολογήσετε γιατί είναι σε αυτή την κατάσταση.
3. Διερευνήστε την περίπτωση ύποπτου λογισμικού εγκατεστημένο στον υπολογιστή σας. Για παράδειγμα ένα πρόγραμμα "Δούρειος ίππος -Trojan horse" δημιουργεί ένα socket και μπαίνει σε κατάσταση ακρόασης δεσμεύοντας μια ελεύθερη θύρα του υπολογιστή ακριβώς όπως θα έκανε ένας εξυπηρετητής. Στο άλλο άκρο μπορεί να συνδεθεί ένα πρόγραμμα πελάτης που μπορεί να δέχεται πληροφορίες και αρχεία μέσα οπό τον υπολογιστή δια μέσω της σύνδεσης.
4. Εξετάστε τι κάνουν οι υπόλοιπες παράμετροι της εντολής netstat χρησιμοποιώντας την εντολή "netstat ?"
5. Διερευνήστε και καταγράψτε τις πληροφορίες των δύο άκρων σε μια νέα σύνδεση με υπηρεσία http όπως την διεύθυνση www.ote.gr
6. Χρησιμοποιείστε κάποιο πρόγραμμα ftp client όπως το filezilla και συνδεθείτε σε ένα ftp εξυπηρετητή όπως το ftp.ntua.gr. Διερευνήστε και καταγράψτε τις πληροφορίες της σύνδεσης για τα δυο άκρα σ' αυτή την υπηρεσία.
7. Διερευνήστε και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και αν υπάρχει κάποιος τοπικός telnet server την αντίστοιχη υπηρεσία.

Βιβλιογραφία

Αλεξόπουλος, Α., & Λαγογιάννης, Γ. (2012). *Τηλεπικοινωνίες και και δίκτυα υπολογιστών,* (8η έκδ.). Αθήνα.

Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). *Τεχνολογία Δικτύων Επικοινωνιών* (1η έκδ.). Αθήνα: ΟΕΔΒ.

Cisco Networking Academy (2014). *Network Basics Companion Guide.Cisco Press*, 800 East 96th Street, Indianapolis, Indiana 46240 USA

Tanenbaum, A. S. (2000). *Δίκτυα Υπολογιστών* (3η έκδ.). Αθήνα: Εκδόσεις Παπασωτηρίου.

Κεφάλαιο 5ο

ΕΠΕΚΤΕΙΝΟΝΤΑΣ ΤΟ ΔΙΚΤΥΟ - ΔΙΚΤΥΑ ΕΥΡΕΙΑΣ ΠΕΡΙΟΧΗΣ

Εισαγωγή

Στο παρόν κεφάλαιο θα μελετηθούν τα Δίκτυα Ευρείας Περιοχής (WAN), τα οποία είναι σχεδιασμένα να καλύπτουν τις ανάγκες μετάδοσης δεδομένων σε μεγάλες γεωγραφικές αποστάσεις. Γίνεται εκτενής αναφορά στις πιο ευρέως διαδεδομένες τεχνολογίες WAN, τις συσκευές που χρησιμοποιούν και τον τρόπο εφαρμογής τους στην πράξη.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 5ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- επιλέγουν και να εφαρμόζουν την κατάλληλη κατά περίπτωση λύση διαδικτύωσης ή σύνδεσης στο Διαδίκτυο, βάσει αναγκών σύνδεσης και διαθεσιμότητας δικτύου
- εγκαθιστούν συνδέσεις και να υλοποιούν ρυθμίσεις στον τηλεπικοινωνιακό εξοπλισμό του τηλεφωνικού δικτύου (PSTN/POTS και ISDN)
- εγκαθιστούν και να ρυθμίζουν εξοπλισμό τεχνολογίας xDSL
- κάνουν στοιχειώδη εκτίμηση επιδόσεων, σαφή περιγραφή προβλημάτων και μια αρχική εκτίμηση ή υπόδειξη ενεργειών για επίλυση προβλημάτων συνδεσιμότητας

Διδακτικές Ενότητες

5. Εισαγωγή στα Δίκτυα Ευρείας περιοχής
5.1 Εγκατεστημένο Τηλεφωνικό Δίκτυο
5.2 Τεχνολογίες FTTH και Metro Ethernet
5.3 Ασύρματες ζεύξεις

5. Εισαγωγή στα Δίκτυα Ευρείας περιοχής

Τα τοπικά δίκτυα αποτελούν πολύ καλή λύση για επικοινωνία με περιορισμένη, όμως, απόσταση κάλυψης. Για να ικανοποιηθεί η διαρκώς αυξανόμενη ανάγκη για επικοινωνία σε ευρύτερες γεωγραφικές εκτάσεις, αναπτύσσονται τα δίκτυα ευρείας περιοχής (Wide Area Networks, WAN). Η επέκταση των τοπικών δικτύων και ο σχηματισμός δικτύων WAN επιτυγχάνεται με τη χρήση κατάλληλων γραμμών σύνδεσης και στοιχείων, όπως modem, γέφυρες, δρομολογητές, κ.α.

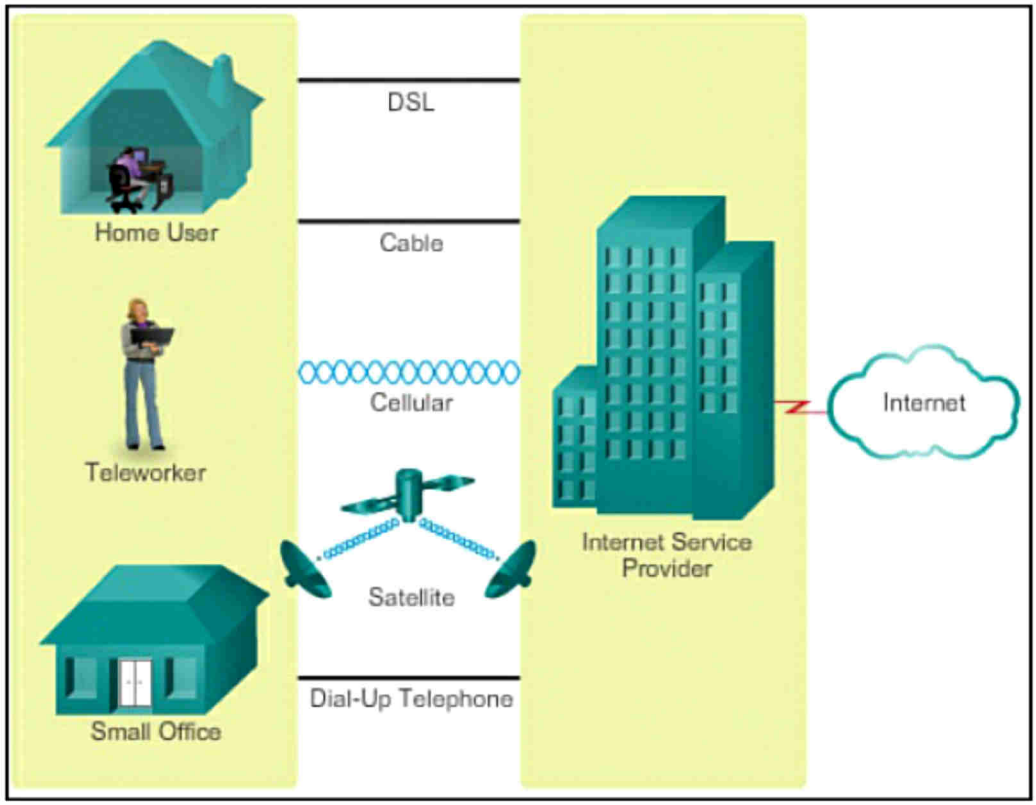
Για την ανάπτυξη γραμμών WAN μπορεί να χρησιμοποιούνται δίκτυα μεταγωγής (κυκλώματος, πακέτου), δορυφορικές συνδέσεις, μικροκυματικές συνδέσεις, οπτικές ίνες, ακόμα και συστήματα καλωδιακής τηλεόρασης.

Ως προς το χρήστη, το WAN εμφανίζεται να λειτουργεί κατά τον ίδιο ακριβώς τρόπο με το LAN. Πραγματικά, αν το WAN έχει υλοποιηθεί με τις κατάλληλες τεχνικές, δεν θα πρέπει να υπάρχει καμία διαφορά στη συμπεριφορά ως προς το LAN.

Επειδή είναι αρκετά δύσκολο π.χ. για μια εταιρεία να εγκαταστήσει και να διαχειριστεί από μόνη της τις γραμμές WAN, συνήθως τις νοικιάζει από τηλεπικοινωνιακό φορέα, ο οποίος μπορεί να έχει αναπτύξει την απαραίτητη σε εξοπλισμό αλλά και γεωγραφική εξάπλωση υποδομή. Οι τεχνολογίες, που χρησιμοποιούνται στις **υπηρεσίες δικτύων ευρείας περιοχής**

(υπηρεσίες WAN) που παρέχονται ως υπηρεσίες από τους διάφορους τηλεπικοινωνιακούς φορείς, είναι:

- Επιλεγόμενες τηλεφωνικές γραμμές
- Μόνιμες ή μισθωμένες γραμμές
- X.25
- Frame Relay
- ISDN
- ATM
- xDSL
- Τεχνολογίες FTTH και Metro Ethernet
- Ασύρματες και δορυφορικές ζεύξεις



Σχήμα 5.α: Επιλογές σύνδεσης σε WAN

(*Πηγή:* http://www.ciscopress.com/articles/article.asp?p=2158215&seqNum=6)

Από τις παραπάνω, οι X.25 και Frame relay έχουν ουσιαστικά καταργηθεί, η ATM έχει αναφερθεί στο κεφάλαιο 2 των παρόντων σημειώσεων, γι' αυτό και θα ασχοληθούμε με τις υπόλοιπες τεχνολογίες.

5.1 Εγκατεστημένο Τηλεφωνικό Δίκτυο

Όπως ίσως θα γνωρίζουμε, μια κανονική τηλεφωνική εγκατάσταση αποτελείται από ένα ζευγάρι από χάλκινα καλώδια που εγκαθιστά στο σπίτι μας μια τηλεφωνική εταιρεία. Τα χάλκινα καλώδια έχουν πολύ χώρο για να μπορούν να μεταφέρουν περισσότερα από τις τηλεφωνικές μας συνομιλίες, δηλαδή έχουν τη δυνατότητα να χειριστούν ένα πολύ μεγαλύτερο εύρος ζώνης (bandwidth) ή μια περιοχή συχνοτήτων, σε σχέση μ' αυτό που απαιτείται για τη μεταφορά της φωνής. Μια DSL σύνδεση, π.χ. αξιοποιεί αυτήν την

επιπλέον χωρητικότητα για να μπορέσει να μεταφέρει πληροφορίες μέσω του χάλκινου σύρματος χωρίς όμως να ενοχλεί τις επικοινωνίες που γίνονται μέσω της ίδιας γραμμής.

Οι ανθρώπινες φωνές στις κανονικές συνομιλίες μπορούν να μεταφερθούν στην περιοχή συχνοτήτων από 0 έως 3.400 Hertz. Αυτή η περιοχή συχνοτήτων είναι πολύ μικρή συγκρινόμενη με την περιοχή συχνοτήτων των περισσότερων στερεοφωνικών ηχείων, που κυμαίνεται από περίπου 20 Hertz έως 20.000 Hertz. Και τα ίδια τα σύρματα έχουν τη δυνατότητα να χειρισθούν συχνότητες έως και αρκετά εκατομμύρια Hertz.

Περιορίζοντας τις συχνότητες που μεταφέρονται μέσα από τα σύρματα, το τηλεφωνικό σύστημα μπορεί να πακετάρει πολλά καλώδια σ' έναν πολύ μικρό χώρο χωρίς να ανησυχεί για παρεμβολές (interference) ανάμεσα στις γραμμές. Τα σύγχρονα μηχανήματα, που στέλνουν ψηφιακά και όχι αναλογικά δεδομένα, μπορούν να χρησιμοποιήσουν με ασφάλεια πολύ περισσότερη από τη χωρητικότητα της τηλεφωνικής γραμμής.

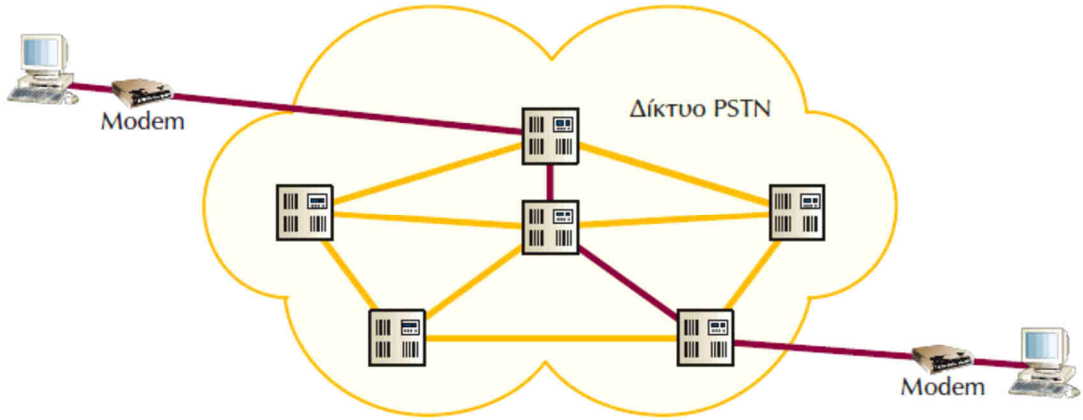
Εικόνα 5.1.α: Εγκατεστημένο τηλεφωνικό δίκτυο
(*Πηγή: http://commons.wikimedia.org/wiki/File:Trans-Canyon_Telephone_Line.jpg*)

5.1.1 Επιλεγόμενες Τηλεφωνικές Γραμμές

Το ίδιο δίκτυο, που χρησιμοποιείται για την επικοινωνία μέσω τηλεφωνικών συσκευών, είναι δυνατό να χρησιμοποιηθεί και για την επικοινωνία υπολογιστών. Το παγκόσμια εκτεταμένο αυτό δίκτυο είναι γνωστό σαν **δημόσιο τηλεφωνικό δίκτυο μεταγωγής (Public Switched Telephone Network, PSTN).** Για το χώρο των υπολογιστών, το PSTN, προσφέρει μέσω των επιλεγόμενων τηλεφωνικών γραμμών, τις γραμμές σύνδεσης, που απαιτούνται για το σχηματισμό WAN.

Επειδή ο αρχικός σχεδιασμός του PSTN έγινε για τη μετάδοση φωνής και όχι για τη μετάδοση ψηφιακών δεδομένων, απαιτούνται ειδικές συσκευές, τα modems, για τη διαμόρφωση των ψηφιακών σημάτων, που παράγουν οι υπολογιστές, σε αναλογικά και αντίστροφα.

Οι επιλεγόμενες τηλεφωνικές γραμμές προσφέρουν μικρούς ρυθμούς μετάδοσης. Η ποιότητά τους δεν είναι σταθερή και εξαρτάται από την ποιότητα των γραμμών, που συμμετέχουν στη δημιουργία της σύνδεσης. Η ταχύτητα ροής δεδομένων μπορεί να φθάσει σε αυτές τις γραμμές έως και τα 56 Kbps.



Σχήμα 5.1.1.α: Σύνδεση σταθμών μέσω δικτύου PSTN
(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Η επιλεγόμενη τηλεφωνική γραμμή ήταν πολύ διαδεδομένη υπηρεσία και χρησιμοποιείται πλέον για συνδέσεις περιορισμένης διάρκειας, όταν δεν δικαιολογείται το επιπλέον κόστος αφιερωμένης γραμμής. Μερικές τυπικές εφαρμογές της είναι η πρόσβαση στο Διαδίκτυο ή σε άλλες on-line υπηρεσίες χαμηλής ταχύτητας, η σύνδεση απομακρυσμένου κόμβου με το τοπικό δίκτυο, η τηλεργασία. Επίσης, χρησιμοποιείται σαν εφεδρική γραμμή σε περίπτωση βλάβης μιας μόνιμης γραμμής.

Πλεονεκτήματα	Μειονεκτήματα	Βασική χρήση
Υψηλή διαθεσιμότητα	Μικρή ταχύτητα	Απομακρυσμένη πρόσβαση
Μικρό κόστος	Μεταβλητή ποιότητα και αξιοπιστία	Εφαρμογές χωρίς απαιτήσεις υψηλής ταχύτητας

Πίνακας 5.1.1.α. Χαρακτηριστικά επιλεγόμενων γραμμών

5.1.2 Μισθωμένες γραμμές

Αντίθετα από τις επιλεγόμενες γραμμές, οι οποίες πρέπει να δημιουργούνται κάθε φορά, που απαιτείται σύνδεση μεταξύ δύο σημείων, οι μισθωμένες ή μόνιμες γραμμές παρέχουν μια επικοινωνιακή γραμμή έτοιμη να χρησιμοποιηθεί ανά πάσα στιγμή. Υπάρχουν αναλογικές και ψηφιακές μισθωμένες γραμμές, οι οποίες προσφέρονται από τους διάφορους τηλεπικοινωνιακούς φορείς.

Η **αναλογική μισθωμένη γραμμή** είναι περισσότερο γρήγορη και αξιόπιστη από την επιλεγόμενη γραμμή. Επίσης είναι σχετικά ακριβή, γιατί ο τηλεπικοινωνιακός φορέας δεσμεύει πολύτιμους πόρους του δικτύου του για τη μισθωμένη γραμμή, είτε αυτή χρησιμοποιείται είτε όχι. Οι αναλογικές μισθωμένες γραμμές, όπως και οι αναλογικές επιλεγόμενες γραμμές, απαιτούν τη χρήση modem, ενώ θέτουν όρια στην ποιότητα και στην ταχύτητα μετάδοσης. Οι μισθωμένες γραμμές είναι διαθέσιμες 24 ώρες το 24ωρο, 7 ημέρες τη βδομάδα, και γι' αυτό είναι κατάλληλες, π.χ. για τη μόνιμη σύνδεση μεταξύ των υποκαταστημάτων μιας εταιρείας, για τη σύνδεση εταιρειών με το Διαδίκτυο, προκειμένου να παρέχουν υπηρεσίες πληροφόρησης διαρκώς διαθέσιμες κ.α.

Όταν απαιτείται υψηλότερη ποιότητα επικοινωνίας και ευκολότερη διαχείριση, χρησιμοποιούνται οι **ψηφιακές μισθωμένες γραμμές.** Οι ταχύτητες των ψηφιακών

γραμμών κυμαίνονται από 19,2 Kbps μέχρι 45 Mbps. Πολύ συχνά χρησιμοποιούμενη επιλογή είναι οι γραμμές **E1** στα 2,048 Mbps (για την Ευρώπη) ή οι γραμμές **T1** στα 1,544 Mbps (για τη Β. Αμερική και την Ιαπωνία). Σε περιπτώσεις, που επαρκούν μικρότερες ταχύτητες, είναι δυνατό να χρησιμοποιηθεί ποσοστό των γραμμών E1 ή T1 σε πολλαπλάσια των 64 Kbps.

Η ψηφιακή γραμμή E1 επιτρέπει τη μετάδοση 32 καναλιών δεδομένων μέσα από μία δισύρματη τηλεφωνική γραμμή. Κάθε κανάλι δειγματοληπτείται 8.000 φορές το δευτερόλεπτο και κάθε δείγμα, που παράγεται, κωδικοποιείται σε σειρά των 8 bits. Έτσι καθένα από τα 32 κανάλια μπορεί να μεταδίδει δεδομένα με ρυθμό 64 Kbps. Η γραμμή E1 μπορεί να μεταδίδει συνολικά δεδομένα με ρυθμό 2,048 Mbps.

Επειδή η μετάδοση είναι από άκρη σε άκρη ψηφιακή, για τη σύνδεση του δικτύου με τη γραμμή δεν χρησιμοποιείται modem, αλλά άλλη συσκευή που ονομάζεται **μονάδα εξυπηρέτησης καναλιού-δεδομένων (Channel Service Unit/Data Service Unit, CSU/DSU).** Αυτή αφενός μετατρέπει το ψηφιακό σήμα, που παράγουν οι διάφοροι σταθμοί του δικτύου, σε ψηφιακό σήμα κατάλληλης μορφής (διπολικό), ώστε να μπορεί να μεταδοθεί στη γραμμή, αφετέρου περιέχει ειδικά ηλεκτρονικά κυκλώματα προστασίας των εγκαταστάσεων του παρόχου της υπηρεσίας.

Βασικό μειονέκτημα των ψηφιακών μισθωμένων γραμμών είναι ότι, αν παρουσιάσουν πρόβλημα, διακόπτεται η λειτουργία τους. Δεν υπάρχει, δηλαδή, η δυνατότητα να κρατηθεί η σύνδεση ανοιχτή σε χαμηλότερη ταχύτητα (κάτι που μπορεί να γίνει σε αναλογική γραμμή).

Η τιμολόγηση μισθωμένης γραμμής είναι συνάρτηση της ταχύτητας και της απόστασης μεταξύ των δύο ακραίων σημείων, κι όχι του όγκου των δεδομένων, που διακινούνται μέσα από αυτή. Αν πρόκειται να συνδέσουμε με αφιερωμένες γραμμές μικρό αριθμό σημείων και οι συνδέσεις να χρησιμοποιούνται πολλές ώρες την ημέρα, μπορεί η επιλογή τους να αποτελεί την πιο συμφέρουσα λύση από άποψη κόστους.

Πλεονεκτήματα	**Μειονεκτήματα**	**Βασική χρήση**
Υψηλή διαθεσιμότητα	Μεγάλο μηνιαίο πάγιο τέλος	Διασύνδεση τοπικών δικτύων, που βρίσκονται σε μεγάλη απόσταση
Ασφάλεια, ανήκει απο-κλειστικά στο χρήστη	Αν η γραμμή είναι ψηφιακή, δύσκολη η εφεδρεία σε περίπτωση προβλήματος στη γραμμή	Μόνιμη σύνδεση στο Διαδίκτυο
Μικρό κόστος, στην περίπτωση διαρκούς μετάδοσης μεγάλης ποσότητας δεδομένων		
Υψηλές ταχύτητες		

Πίνακας 5.1.2.α. Χαρακτηριστικά μισθωμένων γραμμών

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Στην Ευρώπη πλέον, υπάρχουν 5 τύποι μισθωμένων γραμμών, ανάλογα με το ρυθμό μετάδοσης, οι:

- E0 (64Kbps),
- E1 = 32 E0 lines (2Mbps),
- E2 = 128 E0 lines (8Mbps),
- E3 = 16 E1 lines (34Mbps), και
- E4 = 64 E1 lines (140Mbps).

Αντίστοιχα, στις Η.Π.Α. υπάρχουν οι:

- T1 (1.544 Mbps),
- T2 = 4 T1 lines (6 Mbps),
- T3 = 28 T1 lines (45 Mbps) και
- T4 = 168 T1 lines (275 Mbps).

5.1.3 Ψηφιακό Δίκτυο Ενοποιημένων Υπηρεσιών (ISDN)

Το **Ψηφιακό Δίκτυο Ολοκληρωμένων Υπηρεσιών (Integrated Services Digital Network – I.S.D.N.)** δημιουργήθηκε από την ανάγκη παροχής στους συνδρομητές προηγμένων υπηρεσιών και υψηλής ποιότητας επικοινωνίας. Το ISDN αποτελεί εξέλιξη του υφιστάμενου **Δημοσίου Επιλεγόμενου Τηλεφωνικού Δικτύου (Public Switched Telephone Network -P.S.T.N.)** με την εγκατάσταση σε ένα ψηφιακό κέντρο του ανάλογου λογισμικού και υλικού και υποστηρίζει ένα ευρύ φάσμα υπηρεσιών φωνής, δεδομένων, εικόνας και κειμένου. Ο ρυθμός μεταφοράς φθάνει τα 2 Mb/s.

Δύο είναι τα πρότυπα που χρησιμοποιούνται στα ψηφιακά δίκτυα ενοποιημένων υπηρεσιών: α) το **Euro – ISDN** το οποίο συμφωνεί με τις προδιαγραφές του E.T.S.I (European Telecommunications Standardisation Institute) και το οποίο ακολουθούν οι περισσότερες χώρες της Ευρώπης και β) Το **Αμερικανικό πρότυπο** για το ISDN.

Από την πλευρά του χρήστη το ISDN εμφανίζεται ως:

α) ένα σημείο πρόσβασης στο κοινό τηλεφωνικό δίκτυο, με τη διαφορά ότι μπορούμε να έχουμε δύο ταυτόχρονες συνδέσεις οι οποίες είναι ψηφιακές.
β) ένα δίκτυο μεταγωγής κυκλώματος.
γ) ένα δίκτυο ολοκληρωμένων υπηρεσιών (φωνής και δεδομένων) με παράλληλη υποστήριξή τους.
δ) ένας σύνδεσμος με ένα τοπικό δευτερεύον κέντρο ή με ένα τοπικό δίκτυο.

Οι ιδιότητες του δικτύου ISDN είναι οι παρακάτω:

- Πλήρης ψηφιακή μετάδοση της πληροφορίας από άκρο σε άκρο με υψηλούς ρυθμούς.
- Χρήση με τρόπο ενοποιημένο των υπηρεσιών φωνής, δεδομένων, εικόνας και κειμένου μέσω μίας μόνο σύνδεσης.
- Οικονομική, γρήγορη και ποιοτική ψηφιακή μετάδοση λιγότερο ευαίσθητη στα παράσιτα, τόσο στο τηλεφωνικό δίκτυο όσο και στη μετάδοση δεδομένων μεταξύ των τερματικών των πελατών που επικοινωνούν μέσω του ISDN.
- Ασφαλέστερη μετάδοση.
- Καλύτερη και πιο αποτελεσματική χρήση του τηλεφωνικού δικτύου.
- Υψηλές ταχύτητες μετάδοσης (κανάλια/γραμμές με ταχύτητα 64 kb/s) σε σχέση με το PSTN.
- Πλήρης συμβατότητα με όλα τα λειτουργούντα δίκτυα με χρήση κατάλληλων τερματικών διατάξεων.

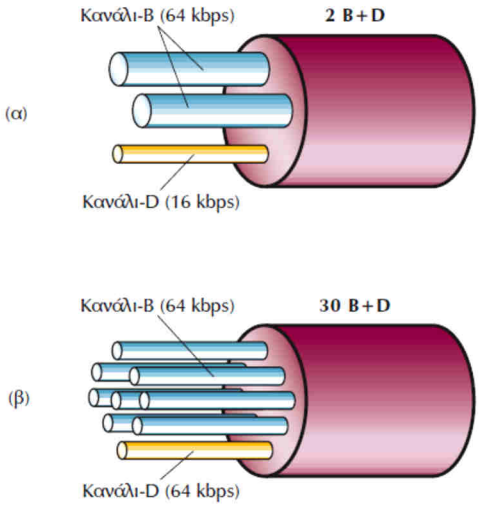
- Σύνδεση πολλαπλών τερματικών σε μια μόνο δισύρματη γραμμή μεταξύ της εγκατάστασης συνδρομητή και του τοπικού κέντρου ISDN (τηλεφωνική συσκευή, fax, H/Y, εικονοτηλέφωνο, ιδιωτικό τηλεφωνικό κέντρο κ.λπ.)

Τύποι πρόσβασης στο δίκτυο ISDN

Υπάρχουν δύο τύποι πρόσβασης στο δίκτυο ISDN:

- **Πρόσβαση βασικού ρυθμού (Basic Rate Access – *BRA*)** η οποία προσφέρει δύο κανάλια των *64 kb/s* (*B* channels) και ένα κανάλι των *16 kb/s* (*D* channel) που χρησιμοποιείται για σηματοδοσία (έναρξη κλήσης, κουδούνισμα κ.λπ.), δηλαδή ***2B + D* κανάλια**. Έτσι, ο χρήστης που διαθέτει βασική πρόσβαση, μπορεί να εκτελέσει ταυτόχρονα τρεις διαφορετικές επικοινωνίες: α) δύο ανεξάρτητες τηλεφωνικές γραμμές και μια επικοινωνία δεδομένων χαμηλής ταχύτητας β) μία οπτική τηλεφωνία και επικοινωνία δεδομένων χαμηλής ταχύτητας γ) οποιεσδήποτε δύο ανεξάρτητες επικοινωνίες (πλην οπτικής τηλεφωνίας) και επικοινωνία δεδομένων χαμηλής ταχύτητας.
- **Πρόσβαση πρωτεύοντος ρυθμού (Primary Rate Access – *PRA*)** η οποία προσφέρει 30 κανάλια B και ένα κανάλι D *των 16 kb/s,* δηλαδή ***30B + D* κανάλια** και απευθύνεται σε πελάτες με μεγαλύτερες ανάγκες. Μέσω των 30 *B* καναλιών πραγματοποιούνται 30 ισάριθμες ταυτόχρονες επικοινωνίες του συνδρομητικού κέντρου ενώ μέσω του καναλιού *D* παρέχεται η σηματοδοσία του ISDN.

(Πηγή: http://anamorfosi.teicm.gr/ekp_yliko/e-notes/Data/commnets/main.htm)

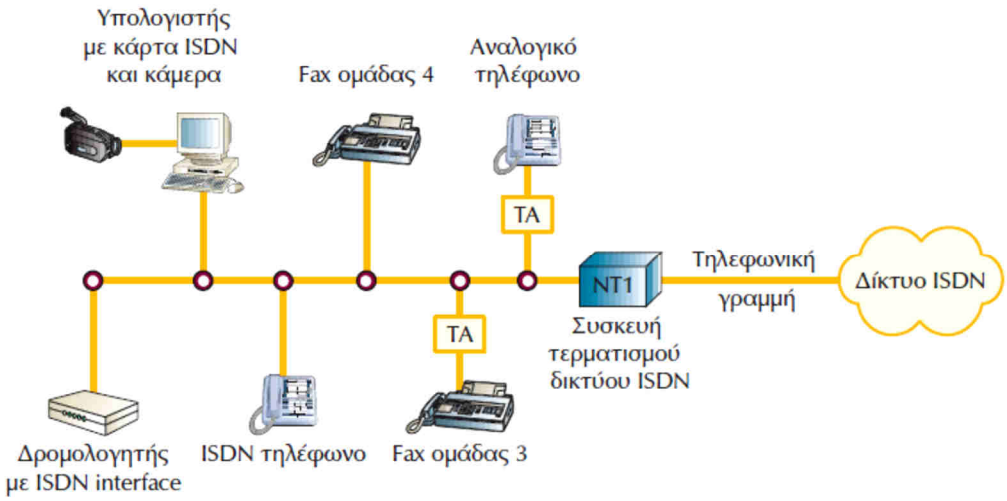


Σχήμα 5.1.3.α. Διεπαφή βασικού ρυθμού BRA (α) και Διεπαφή πρωτεύοντος ρυθμού PRA (β)

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Το ISDN χρησιμοποιεί την υπάρχουσα τηλεπικοινωνιακή υποδομή, όμως απαιτεί την εγκατάσταση ειδικής συσκευής στη μεριά του χρήστη, της **συσκευής τερματισμού δικτύου NT1.** Ο τηλεπικοινωνιακός φορέας τοποθετεί τη συσκευή αυτή στο χώρο του χρήστη - συνδρομητή και μετά τη συνδέει με τον κόμβο ISDN στο τηλεφωνικό κέντρο, αρκετά χιλιόμετρα μακριά, χρησιμοποιώντας το συνεστραμμένο ζεύγος καλωδίων, που παλιότερα χρησιμοποιούνταν στη σύνδεση με το τηλέφωνο του συνδρομητή. Μετά η κίνηση δρομολογείται από το δίκτυο του τηλεπικοινωνιακού φορέα (με τεχνικές μεταγωγής πακέτων, κυκλώματος κ.α.). Στη συσκευή τερματισμού NT1 είναι δυνατό να συνδεθούν μέχρι 8 συσκευές σε απόσταση 150 μέτρα. Μπορεί να είναι συσκευές ειδικά σχεδιασμένες

για το δίκτυο ISDN, όπως ψηφιακή τηλεφωνική συσκευή, Fax ομάδας 4, εικονοτηλέφωνο, δρομολογητής, ή απλές συσκευές, όπως η αναλογική τηλεφωνική συσκευή, κοινό τερματικό κ.α. Στην τελευταία περίπτωση, χρησιμοποιείται ειδική διάταξη, ο **τερματικός προσαρμογέας (Terminal Adaptor, TA).** Τα κανάλια B και D είναι λογικά κανάλια κι όχι φυσικά. Έτσι στη συσκευή NT1 καταλήγει πάντα μια απλή δισύρματη γραμμή κι όχι περισσότερα καλώδια.



Σχήμα 5.1.3.β. Ο εξοπλισμός του ISDN

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Η υπηρεσία ISDN είναι χρήσιμη, όταν η μετάδοση δεδομένων δεν είναι συνεχής και οι ανάγκες σε ταχύτητα κυμαίνονται. Ο χρήστης πληρώνει όσο διαρκεί η κλήση, γι' αυτό είναι αρκετά συνηθισμένο να χρησιμοποιείται σαν εφεδρική σύνδεση αφιερωμένων γραμμών.

Το ISDN, που περιγράψαμε, αναφέρεται και ως ISDN στενής ζώνης (Narrowband ISDN), ενώ αναπτύχθηκαν και πρότυπα για το **ISDN ευρείας ζώνης (Broadband ISDN, B-ISDN),** με ρυθμό μετάδοσης έως 2 Mb/s, το οποίο απαιτεί τη χρήση οπτικής ίνας.

Πλεονεκτήματα	Μειονεκτήματα	Βασική χρήση
Κόστος ανάλογο με την κίνηση	Ακριβή για συνεχή μεταφορά δεδομένων	Σποραδική κίνηση που περιλαμβάνει φωνή, εικόνα, δεδομένα
Μεταφορά φωνής, εικόνας και δεδομένων		Σαν εφεδρική γραμμή μαζί με τις ασύγχρονες επιλεγόμενες τηλεφωνικές γραμμές
Γρήγορη εγκαθίδρυση σύνδεσης		
Χρήση υπάρχουσας υποδομής		
Ιδανική για χρήση σαν εφεδρική γραμμή		

Πίνακας 5.1.3.α. Χαρακτηριστικά ISDN

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

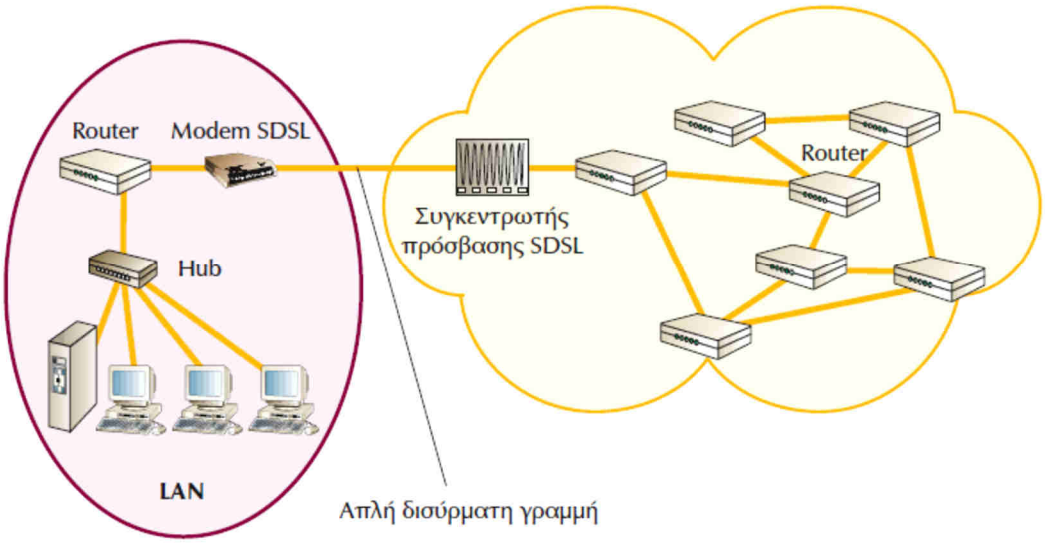
5.1.4 Τεχνολογίες Ψηφιακής Συνδρομητικής Γραμμής (xDSL)

Το **DSL** προέρχεται από τα αρχικά των λέξεων **D**igital **S**ubscriber **L**ine (Ψηφιακή Συνδρομητική Γραμμή) και στην ουσία αποτελεί μια τεχνολογία που μετατρέπει το απλό τηλεφωνικό καλώδιο σε ένα δίαυλο ψηφιακής επικοινωνίας μεγάλου εύρους ζώνης με τη χρήση ειδικών modems, τα οποία τοποθετούνται στις δυο άκρες της γραμμής. Ο δίαυλος αυτός μεταφέρει τόσο τις χαμηλές όσο και τις υψηλές συχνότητες ταυτόχρονα, τις χαμηλές για τη μεταφορά του σήματος της φωνής και τις υψηλές για τα δεδομένα. Οι συσκευές modems λειτουργούν όπως τα κλασικά modems, αφού λαμβάνουν ροή ψηφιακού σήματος, που στη συνέχεια το μεταδίδουν στην τηλεφωνική γραμμή με τη μορφή αναλογικού σήματος υψηλού ρυθμού (λέγονται και baseband modems).

Χρησιμοποιούνται διάφορες τεχνολογίες διαμόρφωσης, οι οποίες χωρίζουν το διαθέσιμο εύρος ζώνης της γραμμής σε τρία κανάλια: ένα για τη μετάδοση της φωνής, ένα για τη μετάδοση δεδομένων προς τα πάνω (upstream) κι ένα για τη μετάδοση των δεδομένων προς τα κάτω (downstream).

Ανάλογα με το είδος του modem που θα συνδέσουμε, πετυχαίνουμε και διαφορετικές επιδόσεις. Με το DSL επιτυγχάνονται υψηλότερες ταχύτητες μεταφοράς δεδομένων (μέχρι και 52,8 Mbps από το Διαδίκτυο ή άλλο απομακρυσμένο Τηλεπικοινωνιακό δίκτυο προς το χρήστη -downstream- και 2,3 Mbps από το χρήστη προς το Διαδίκτυο -upstream- ενώ ταυτόχρονα μεταφέρονται και τα αναλογικά σήματα της φωνής.

Οι διάφορες παραλλαγές xDSL υποστηρίζουν συμμετρική ή ασύμμετρη μετάδοση δεδομένων. Αυτό σημαίνει, ότι τα δεδομένα μπορεί να μεταδίδονται με την ίδια ή διαφορετική ταχύτητα προς τις δύο κατευθύνσεις (downstream και upstream). Έτσι, κάθε παραλλαγή μπορεί να είναι κατάλληλη για χρήση σε εφαρμογές, όπου απαιτείται υψηλότερη ταχύτητα στην κατεύθυνση μετάδοσης προς το χρήστη (π.χ. πρόσβαση σε ιστοσελίδες) ή ίδια ταχύτητα και προς τις δύο κατευθύνσεις (π.χ. υποκατάστατο για γραμμές E1, τηλεδιάσκεψη).



Σχήμα 5.1.4.α. Πρόσβαση τοπικού δικτύου σε δίκτυο ευρείας περιοχής με την τεχνολογία SDSL

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Οι τεχνολογίες DSL αναφέρονται γενικά ως **xDSL** και οι κυριότερες από αυτές είναι: **ADSL**, **HDSL**, **SDSL** και **VDSL**.

Τεχνολογία	Σημασία	Αριθμός Ζευγών	Ταχύτητα	Μέγιστη Απόσταση
ADSL	Asymmetric DSL	1	8 Mbps downstream 1,5 Mbps upstream	3 Km 6,6 - 7,5 Km
ADSL Lite		1	1 Mbps downstream 384 Kbps upstream	
HDSL	High-bit-rate DSL	2 3	2 Mbps full duplex (E1) 1,5 Mbps full duplex (T1)	3,5 - 4,5 Km
SDSL	Single-line DSL	1	2 Mbps full duplex (E1) 1,5 Mbps full duplex (T1)	3 Km
VDSL	Very-high-bit-rate DSL	1	13 - 52 Mbps downstream 1,5 - 2,3 Mbps upstream	0,3 - 1,4 km

Πίνακας 5.1.4.α. Οι τεχνολογίες xDSL

ADSL. Το **ADSL**, το οποίο προέρχεται από τα αρχικά των λέξεων **A**symmetric **D**igital **S**ubscriber **L**ine, είναι αυτό που δίνεται στους περισσότερους απλούς χρήστες στην Ελλάδα. Η τεχνολογία ADSL εξασφαλίζει πρόσβαση υψηλών ταχυτήτων στο Διαδίκτυο και σε άλλα τηλεπικοινωνιακά δίκτυα, δίνοντας τη δυνατότητα για ταυτόχρονη μετάδοση φωνής και δεδομένων (δεδομένα, κινούμενη εικόνα, γραφικά) μέσω της απλής τηλεφωνικής γραμμής. Κύριο χαρακτηριστικό της τεχνολογίας είναι ότι η μεταφορά δεδομένων γίνεται με **ασύμμετρο τρόπο**, δηλαδή προσφέρει διαφορετικό ρυθμό για τη λήψη (μέχρι 8 Mbps downstream) και διαφορετικό για την αποστολή δεδομένων (1 Mbps upstream). Το σημαντικότερο είναι ότι το εύρος ζώνης δεν το μοιραζόμαστε, αλλά είναι εξ ολοκλήρου στη διάθεσή μας. Ένα επιπλέον χαρακτηριστικό είναι ότι η σύνδεση ADSL είναι μόνιμη και διαθέσιμη ανά πάσα στιγμή (always-on), δηλαδή δεν απαιτείται σύνδεση και αποσύνδεση από το δίκτυο όπως συμβαίνει με τις τηλεφωνικές κλήσεις. Ωστόσο θα πρέπει να τονιστεί το γεγονός ότι η απόδοση του ADSL εξαρτάται σημαντικά από την απόσταση του χρήστη από τον τηλεπικοινωνιακό πάροχο και φθάνει τα:

- 1,5 Mbps για απόσταση 5,5 km
- 2,0 Mbps για απόσταση 4,9 km
- 6,3 Mbps για απόσταση 3,6 km
- 8,4 Mbps για απόσταση 2,7 km

Εξελιγμένες εκδόσεις του ADSL είναι το **ADSL2** και το **ADSL2+**, οι οποίες παρέχουν μεγαλύτερες ταχύτητες αξιοποιώντας διαφορετικά το εύρος ζώνης του καλωδίου. Η μέγιστη ταχύτητα που μπορεί να επιτύχει το ADSL2+ είναι τα 24/1 Mbps (ή τα 24/3,5 Mbps σε περίπτωση που υλοποιεί το πρότυπο ITU G.992.5 Annex M), αλλά στην πράξη πολύ λίγοι χρήστες μπορούν να συνδεθούν σε αυτές τις ταχύτητες, λόγω της απόστασής τους από το τηλεφωνικό κέντρο.

Όνομα προτύπου	Κοινή ονομασία	Μέγιστος ρυθμός λήψης	Μέγιστος ρυθμός αποστολής
ANSI T1.413-1998 Issue 2	ADSL	8 Mbit/s	1.0 Mbit/s
ITU G.992.1	ADSL (G.DMT)	8 Mbps	1.0 Mbps
ITU G.992.1 Annex A	ADSL over POTS	8 Mbps	1.0 Mbps
ITU G.992.1 Annex B	ADSL over ISDN	8 Mbps	1.0 Mbps
ITU G.992.2	ADSL Lite (G.Lite)	1.5 Mbps	0.5 Mbps
ITU G.992.3/4	ADSL2	12 Mbps	1.0 Mbps
ITU G.992.3/4 Annex J	ADSL2	12 Mbps	3.5 Mbps
ITU G.992.3/4 Annex L	RE-ADSL2	5 Mbit/s	0.8 Mbit/s
ITU G.992.5	ADSL2+	24 Mbit/s	1.0 Mbit/s
ITU G.992.5 Annex L	RE-ADSL2+	24 Mbit/s	1.0 Mbit/s
ITU G.992.5 Annex M	ADSL2+	24 Mbit/s	3.5 Mbit/s

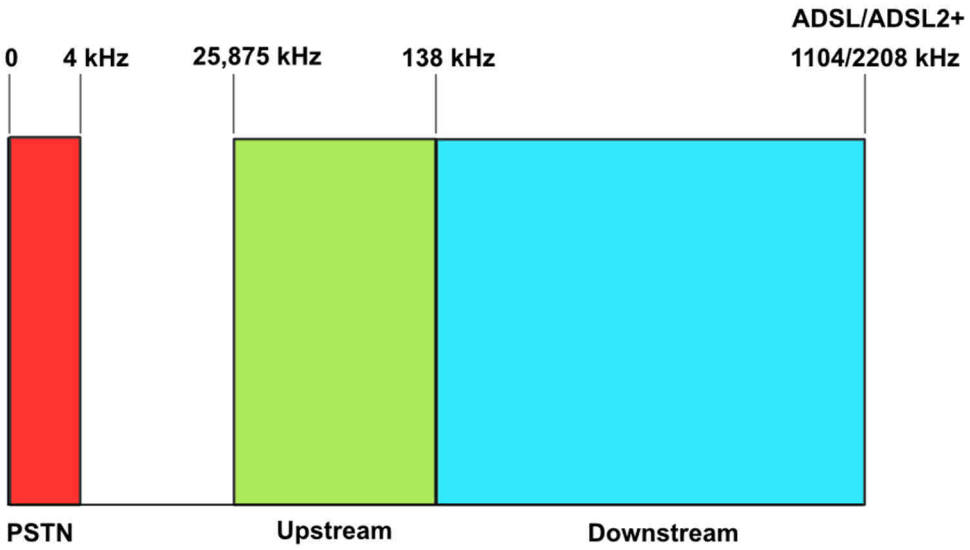
Πίνακας 5.1.4.β. Τα πρότυπα του ADSL

Τεχνολογία ADSL. Το **ADSL** εξασφαλίζει πρόσβαση υψηλών ταχυτήτων στο Διαδίκτυο και σε άλλα τηλεπικοινωνιακά δίκτυα, δίνοντας έτσι τη δυνατότητα για ταυτόχρονη μετάδοση φωνής και δεδομένων (δεδομένα, κινούμενη εικόνα, γραφικά) μέσω της απλής τηλεφωνικής γραμμής. Αυτό γίνεται εφικτό χάρη *στους εξελιγμένους αλγορίθμους και στη βελτιωμένη ψηφιακή επεξεργασία σήματος*, τα οποία συμπιέζουν σε μεγάλο βαθμό την πληροφορία που μεταδίδεται μέσα από τα υπάρχοντα τηλεφωνικά καλώδια, καθώς επίσης και στη βελτίωση των μετασχηματιστών, των αναλογικών φίλτρων και των μετατροπέων σήματος (από αναλογικό σε ψηφιακό).

Στις απλές τηλεφωνικές συνδέσεις με χάλκινο καλώδιο χρησιμοποιείται μόνο η περιοχή συχνοτήτων 0-4 kHz για τη μετάδοση της φωνής. Αυτό δίνει τη δυνατότητα να χρησιμοποιηθούν οι μεγαλύτερες συχνότητες για τη μετάδοση άλλων δεδομένων. Επειδή το εύρος είναι περιορισμένο και οι συνηθισμένοι οικιακοί χρήστες έχουν μεγαλύτερο όγκο στο κατέβασμα παρά στο ανέβασμα, χρησιμοποιείται μεγαλύτερο εύρος συχνοτήτων για την αποστολή από τον πάροχο προς τον τελικό χρήστη από το εύρος συχνοτήτων που χρησιμοποιείται για την αποστολή από τον τελικό χρήστη προς τον πάροχο.

Αυτές οι συχνότητες υποδιαιρούνται σε ακόμα μικρότερες περιοχές των 4.3125 kHz και συχνά ονομάζονται bins. Συνήθως τα modems κατά την έναρξη της επικοινωνίας ελέγχουν ξεχωριστά κάθε τέτοια περιοχή για να καθορίσουν ποιες από αυτές τις περιοχές μπορούν να χρησιμοποιηθούν.

Αυτή η σύνδεση χρησιμοποιείται για τη μεταφορά από τον τελικό χρήστη μέχρι το αντίστοιχο τηλεφωνικό κέντρο της περιοχής. Στο τηλεφωνικό κέντρο της περιοχής η μετάδοση των δεδομένων διακλαδώνεται μέσω των DSLAM και μεταβιβάζεται (συνήθως) με γραμμές πολύ μεγαλύτερης ταχύτητας στον αντίστοιχο πάροχο δεδομένων.



Σχήμα 5.1.4.β: Χρήση συχνοτήτων PSTN
(*Πηγή: https://el.wikipedia.org/wiki/Asymmetric_Digital_Subscriber_Line*)

Στο Σχήμα 5.1.4.β., με κόκκινο φαίνεται η περιοχή συχνοτήτων που χρησιμοποιεί η απλή τηλεφωνική σύνδεση (PSTN), με πράσινο η περιοχή του upload και με μπλε η περιοχή που χρησιμοποιείται για download από το ADSL.

Οι τηλεφωνικές γραμμές μεγάλου μήκους προκαλούν μεγάλη εξασθένιση στα σήματα υψηλών συχνοτήτων που μπορεί να φτάσει και τα 90 dB στο 1 MHz (το οποίο αποτελεί το άνω όριο της ζώνης που χρησιμοποιεί το ADSL), υποχρεώνοντας έτσι τα ADSL modems να "δουλεύουν πολύ σκληρά" για να πετύχουν μεγάλο δυναμικό εύρος, να διαχωρίσουν τα κανάλια και να κρατήσουν το θόρυβο σε χαμηλά επίπεδα. Για τον απλό χρήστη το ADSL φαίνεται κάτι απλό -διαφανείς "σωλήνες" σύγχρονων δεδομένων διαφορετικών ταχυτήτων πάνω από απλές τηλεφωνικές γραμμές. Μέσα στα ADSL modems, όπου όλα τα τρανζίστορς λειτουργούν, υπάρχει ένα θαύμα τεχνολογίας. Για να δημιουργηθούν πολλαπλά κανάλια επικοινωνίας, τα ADSL modems χωρίζουν το διαθέσιμο εύρος ζώνης μιας τηλεφωνικής γραμμής με ένα από τους δυο ακόλουθους τρόπους: α) Πολυπλεξία με διαίρεση συχνότητας (Frequency Division Multiplexing) ή β) *Καταστολή της ηχούς* (Echo Cancellation).

HDSL. Το ακρωνύμιο **HDSL** προέρχεται από τα αρχικά των λέξεων **H**igh-bit-rate **D**igital **S**ubscriber **L**ine και σε αντίθεση με το ADSL είναι **συμμετρικό** και προσφέρει τον ίδιο ρυθμό μεταφοράς δεδομένων (μέχρι 2 Mbps) τόσο για τη αποστολή όσο και για τη λήψη. Ωστόσο, η μέγιστη απόσταση μεταξύ των δύο άκρων δεν μπορεί να υπερβαίνει τα 3,5 km. Μια άλλη βασική διαφορά από το ADSL είναι ότι απαιτείται η εγκατάσταση 2 τηλεφωνικών γραμμών (2 συνεστραμμένα καλώδια). Νεότερες εκδόσεις της τεχνολογίας HDSL, είναι το HDSL2 (2 Mbps, 1 ζεύγος συνεστραμμένου καλωδίου) και το HDSL4 (2 Mbps, 2 ζεύγη συνεστραμμένων καλωδίων).

SDSL. Το **SDSL, S**ingle-line **D**igital **S**ubscriber **L**ine, είναι μια τεχνολογία παρόμοια με το HDSL όσον αφορά στο ρυθμό μεταφοράς δεδομένων (μέχρι 2 Mbps), που απαιτεί όμως μόνο ένα συνεστραμμένο ζεύγος χαλκού. Για το λόγο αυτό, η μέγιστη απόσταση μεταξύ των δύο άκρων δεν μπορεί να ξεπερνά τα 3 km.

VDSL. Το **VDSL, V**ery-high-data-rate **D**igital **S**ubscriber **L**ine, μπορεί να δώσει εντυπωσιακά μεγαλύτερες ταχύτητες που μπορεί να φτάνουν τα 52 Mbps, με περιορισμό όμως τη μέγιστη απόσταση μεταξύ των δύο άκρων του χάλκινου αγωγού. Ανάλογα με την υλοποίηση, το VDSL δε μπορεί να ξεπερνά το 1,5 km και οι ρυθμοί μετάδοσης κυμαίνονται

για τη λήψη έως 52 Mbps και για την αποστολή έως 12 Mbps. Διάδοχος τεχνολογία του VDSL είναι το **VDSL2**, που παρέχει ταχύτητες πάνω από 200 Mbps σε πολύ μικρή απόσταση, 100 Mbps στα 500 μέτρα και 50 Mbps στο 1 χιλιόμετρο.

5.1.4.1 Συσκευές τερματισμού δικτύου DSL Modem/DSLAM

Το DSL χρησιμοποιεί δύο κομμάτια εξοπλισμού, ένα στην πλευρά του πελάτη και ένα στον πάροχο υπηρεσιών Διαδικτύου, την τηλεφωνική εταιρεία ή έναν άλλον πάροχο υπηρεσιών DSL.

Στην πλευρά του πελάτη υπάρχει ένας **πομποδέκτης (transceiver) DSL**, ο οποίος μπορεί να παρέχει κι άλλες υπηρεσίες. Ο πάροχος υπηρεσιών DSL διαθέτει έναν **πολυπλέκτη/αποπολυπλέκτη των ψηφιακών συνδρομητικών γραμμών DSL (DSL Access Multiplexer, DSLAM)** για να λαμβάνει τις συνδέσεις των πελατών.

Πομποδέκτης (Transceiver). Οι περισσότεροι οικιακοί πελάτες αποκαλούν τον δικό τους DSL πομποδέκτη ένα "DSL modem". Οι τεχνικοί στην τηλεφωνική εταιρεία ή τον ISP τον αποκαλούν ένα ATU-R. Ανεξάρτητα από το πώς είναι γνωστός, είναι το σημείο όπου τα δεδομένα από τον υπολογιστή του χρήστη ή το δίκτυο συνδέονται με την DSL γραμμή. Ο πομποδέκτης μπορεί να συνδεθεί με τον εξοπλισμό ενός χρήστη με πολλούς τρόπους, αν και οι περισσότερες οικιακές εγκαταστάσεις χρησιμοποιούν συνδέσεις USB ή 10 base-T Ethernet (UTP).

Όλο και περισσότερες ADSL γραμμές χρησιμοποιούνται για τη σύνδεση δικτύων γραφείων με το Διαδίκτυο. Στην περίπτωση αυτή, χρησιμοποιούμε ένα ADSL modem/router (δρομολογητή) αντί για ένα απλό ADSL modem.

Συνήθως, υπάρχουν τα εξής είδη ADSL modems :

- Εξωτερικό ADSL modem για σύνδεση με μια κάρτα δικτύου στον υπολογιστή, συνήθως μέσω ενός καλωδίου 10baseT.
- Εξωτερικό ADSL modem για σύνδεση με βύσμα USB στον υπολογιστή.
- Εσωτερικό ADSL modem, που θυμίζει στην εμφάνιση μια κάρτα δικτύου.

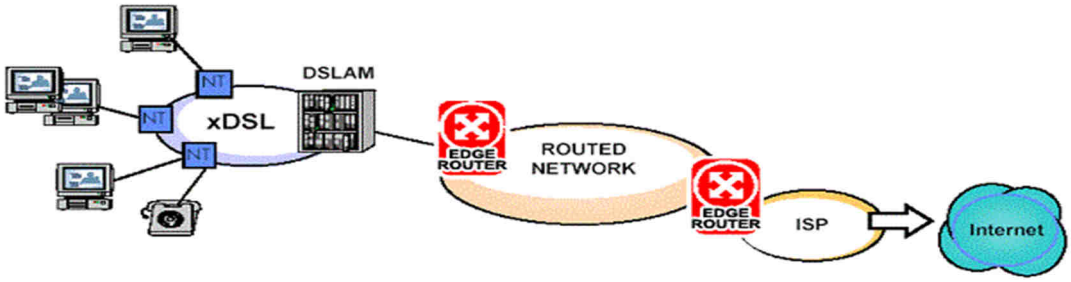
Εικόνα 5.1.4.1.α: Τυπικό εξωτερικό ADSL modem/router

DSLAM. Το **Digital Subscriber Line Access Multiplexer** (DSLAM) είναι ο πολυπλέκτης/αποπολυπλέκτης των ψηφιακών συνδρομητικών γραμμών DSL (Digital Subscriber Line). Είναι μια συσκευή που τοποθετείται είτε στο Κέντρο Τηλεπικοινωνιακών Παρόχων, είτε σε καμπίνες στο δρόμο, είτε αντικαθιστούν τους Κατανεμητές καλωδίων, είτε μέσα σε πολυκατοικίες.

Το DSLAM στην πλευρά του παρόχου είναι ο εξοπλισμός που επιτρέπει στο DSL να λειτουργεί. Ένα DSLAM λαμβάνει συνδέσεις από πολλούς πελάτες και τις συνενώνει σε μία σύνδεση υψηλής χωρητικότητας προς το Διαδίκτυο. Τα DSLAMs είναι γενικά ευέλικτα και

μπορούν να υποστηρίξουν πολλούς τύπους DSL στο ίδιο κεντρικό γραφείο και διαφορετικές ποικιλίες πρωτοκόλλων και διαμόρφωσης (modulation) στον ίδιο τύπο DSL. Επιπλέον, το DSLAM μπορεί να παρέχει επιπλέον λειτουργίες όπως δρομολόγηση (routing) ή εκχώρηση δυναμικών IP διευθύνσεων για τους πελάτες. Για περισσότερες πληροφορίες σχετικα με τη Διαμόρφωση Διακριτής Πολυτονίας (DMT) δείτε την ενότητα Π.3 στο Παράρτημα των σημειώσεων.

Το DSLAM περιέχει ένα μοναδικό modem (port) για κάθε συνδρομητή που συνδέεται σε αυτό. Κάθε κάρτα στο DSLAM τυπικά έχει 24 ports και, βεβαίως, μπορούν να εγκατασταθούν πολλαπλές κάρτες για να καλύψουν ολόκληρες περιοχές. Όταν συνδέσουμε και ανάψουμε το modem/router μας, το πρώτο πράγμα που κάνει είναι να συνδεθεί με το port του DSLAM που μας αντιστοιχεί. Αυτή η διαδικασία σύνδεσης μεταξύ των δύο modems ονομάζεται "συγχρονισμός", και συνήθως έχει ειδικό λαμπάκι με την ονομασία ADSL, line ή sync που δείχνει πως έγινε με επιτυχία. Η πραγματική ταχύτητα ADSL για τη σύνδεσή μας είναι η ταχύτητα που θα επιτευχθεί σε αυτόν τον συγχρονισμό.



Σχήμα 5.1.4.1.α. Κλασικό DSL δίκτυο με DSLAM

Το DSLAM παρέχει μια από τις κύριες διαφορές ανάμεσα στο ADSL και τα καλωδιακά (cable) modems. Επειδή οι χρήστες των cable modems μοιράζονται συνήθως έναν βρόγχο δικτύου (network loop) σε μια γειτονιά, η πρόσθεση χρηστών σημαίνει ελάττωση της απόδοσης σε πολλές περιπτώσεις. Το ίδιο ισχύει και για το DSL καθώς το DSLAM λειτουργεί σαν hub, δηλαδή πολλοί χρήστες μοιράζονται το ίδιο κανάλι (bus), με αποτέλεσμα τον κορεσμό του bandwidth.

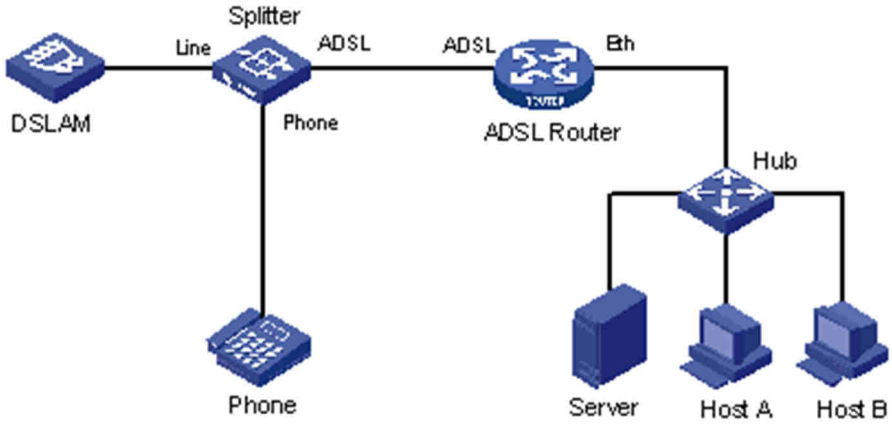
Εικόνα 5.1.4.1.β: Εξωτερικό DSLAM

Το καλωδιακό modem υπερτερεί σε θέματα ταχύτητας και κόστους, καθώς κλειδώνει σε FastEthernet με σχετικά φθηνότερο πάγιο ενώ παρέχονται και άλλες υπηρεσίες πάνω

απ' αυτό, όπως TV, Telephony κ.ά. Το ADSL παρέχει μια αφοσιωμένη (dedicated) σύνδεση από τον κάθε χρήστη έως το DSLAM, πράγμα που σημαίνει ότι οι χρήστες δεν θα διαπιστώσουν μια ελάττωση της απόδοσης με την προσθήκη νέων χρηστών, μέχρις ότου ο συνολικός αριθμός των χρηστών αρχίσει να παραγεμίζει (κορεσμός) τη σύνδεση υψηλής ταχύτητας προς το Διαδίκτυο. Τότε, μια αναβάθμιση (upgrade) από τον πάροχο υπηρεσιών μπορεί να προσθέσει επιπλέον απόδοση για όλους τους χρήστες που είναι συνδεδεμένοι στο DSLAM.

5.1.4.2 Τοπολογία - Εξοπλισμός

Όπως περιγράψαμε παραπάνω, μία τυπική τοπολογία δικτύου ADSL φαίνεται στο παρακάτω σχήμα 5.1.4.2.α:



Σχήμα 5.1.4.2.α. Τοπολογία ADSL
(*Πηγή:http://www.h3c.com/portal/Products___Solutions/Technology/WAN/Technology_Introduction/200701/195629_57_0.htm*)

Συνδεσμολογίες ADSL (splitterless και splitter-based)

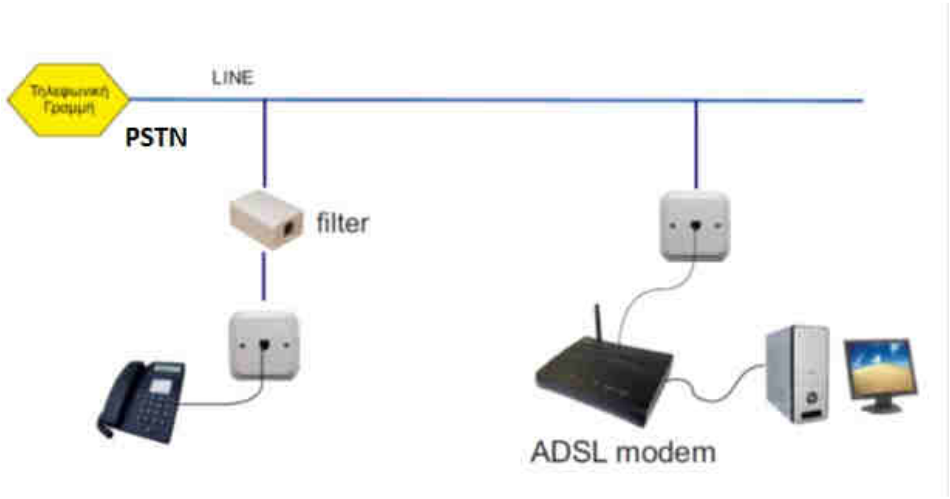
Όταν παίρνουμε ADSL στο σπίτι μας, ο τηλεπικοινωνιακός πάροχος τοποθετεί μία συσκευή στον πελάτη (Network Interface Device - NID), γνωστή και ως adsl modem/router, η οποία διαχωρίζει τις συχνότητες της φωνής, που κυμαίνονται μεταξύ 0 - 4kHz, από τις υψηλότερες συχνότητες των DSL σημάτων (25kHz - 1,1MHz). Ο διαχωριστής των σημάτων διαφορετικών συχνοτήτων, ένα χαμηλοπερατό φίλτρο, είναι μια παθητική συσκευή, δηλαδή δεν χρειάζεται επιπλέον παροχή ρεύματος και μπορεί να συνεχίζει να λειτουργεί, αν υπάρξει τοπική διακοπή παροχής ρεύματος. Υπάρχουν δύο βασικές κατηγορίες συνδεσμολογίας ADSL, η ***splitter-based*** και η ***splitterless***. Και στις δύο περιπτώσεις στο σπίτι μας φθάνει ένα δισύρματο καλώδιο. Ωστόσο, για την splitterbased τεχνολογία απαιτείται η εγκατάσταση ενός διαχωριστή σήματος από την τηλεφωνική εταιρεία στο χώρο του συνδρομητή (είτε μέσα στο σπίτι είτε έξω από αυτό), ώστε να διαχωριστεί το σήμα της φωνής από το σήμα που μεταφέρει τα δεδομένα. Για τη splitterless τεχνολογία, δεν έχουμε διαχωρισμό των δύο σημάτων. Η τεχνολογία splitterless είναι γνωστή και ως "***Universal DSL***" ή "***G.Lite***" ή "***DSL Lite***".

- Με το ***splitterless DSL***, το DSL modem συνδέεται απευθείας με την τηλεφωνική γραμμή, όπως και οι τηλεφωνικές συσκευές (Σχήμα 5.1.4.2.β). Το modem περιέχει ειδικά chips που διαχωρίζουν τα σήματα, αλλά λειτουργούν σε χαμηλότερη ισχύ, ώστε να μη δημιουργούν παρεμβολές στα σήματα της φωνής. ***Έτσι, η μέγιστη ταχύτητα μεταφοράς δεδομένων είναι μικρότερη σε σχέση με το splitter-based***

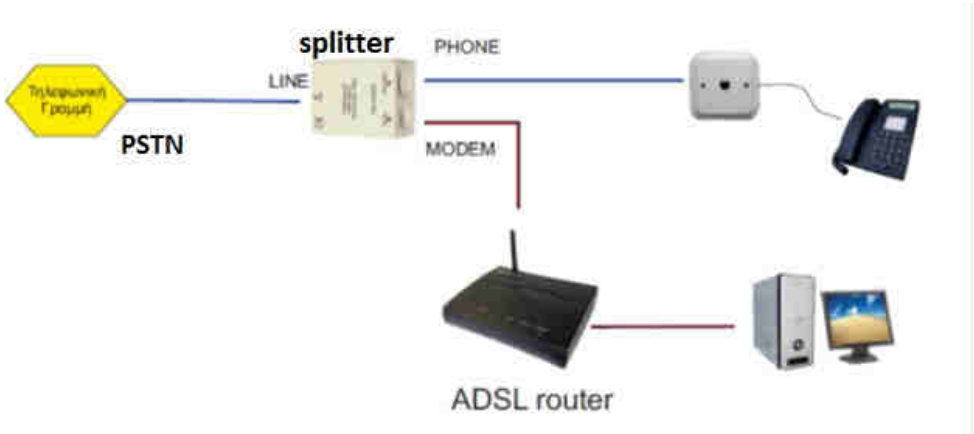
DSL. Επιπλέον, οι τηλεφωνικές συσκευές απαιτούν την ύπαρξη ενός φίλτρου (filter) που θα παρεμποδίζει τα σήματα DSL (δεδομένων), τα οποία μπορεί να ακουστούν ως θόρυβος στη γραμμή και να παρεμβληθούν στην κανονική λειτουργία του τηλεφώνου.

- Από την άλλη, με το ***splitter-based DSL***, το σήμα DSL (δεδομένων) διαχωρίζεται από τη γραμμή του τηλεφώνου και με διαφορετικό καλώδιο οδεύει προς το modem (Σχήμα 5.1.4.2.γ και δ). Αυτό απαιτεί, όπως καταλαβαίνουμε, επιπλέον καλωδίωση που στοιχίζει, όπως στοιχίζει επίσης και ο διαχωριστής σήματος. Το καλώδιο του modem συνδέεται μέσω διεπαφής (NIC-Network Interface Card) η οποία συνήθως είναι μία κάρτα Ethernet ή ένα hub το οποίο θα συνδέεται σε τοπικό δίκτυο.

Αν λοιπόν, η τηλεφωνική μας γραμμή είναι PSTN με ενεργοποιημένη σύνδεση ADSL, μπορούμε να διακρίνουμε τις παρακάτω περιπτώσεις εγκατάστασης δικτύου με χρήση φίλτρου (filter) ή διαχωριστή (splitter):

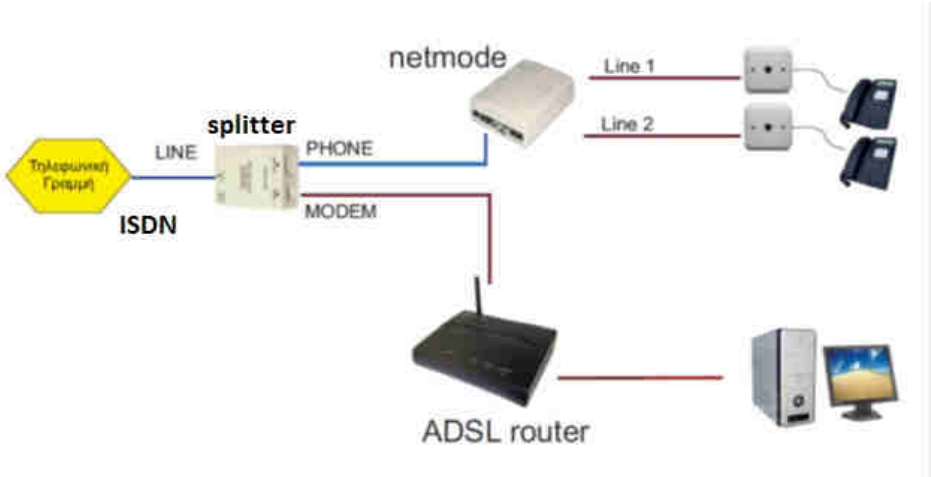


Σχήμα 5.1.4.2.β. Σύνδεση ADSL σε γραμμή PSTN με χρήση φίλτρου (splitterless)
(*Πηγή:http://users.sch.gr//iliaslamprou/images/stories/askiseis_electrikwn_egkatastasewn/phones_and_lan_installation_diagram.pdf*)



Σχήμα 5.1.4.2.γ. Σύνδεση ADSL σε γραμμή PSTN με χρήση διαχωριστή σήματος (splitter-based)
(*Πηγή:http://users.sch.gr//iliaslamprou/images/stories/askiseis_electrikwn_egkatastasewn/phones_and_lan_installation_diagram.pdf*)

Αντίστοιχα, αν η τηλεφωνική μας γραμμή είναι ISDN με ενεργοποιημένη σύνδεση ADSL, υπάρχει η **συσκευή τερματισμού δικτύου – netmode** και επομένως η εγκατάσταση του δικτύου θα γίνει ως εξής:



Σχήμα 5.1.4.2.δ. Σύνδεση ADSL σε γραμμή ISDN με χρήση διαχωριστή σήματος (splitter-based)

(*Πηγή:*[*http://users.sch.gr//iliaslamprou/images/stories/askiseis_electrikwn_egkatastasewn/phones_and_lan_installation_diagram.pdf*](http://users.sch.gr//iliaslamprou/images/stories/askiseis_electrikwn_egkatastasewn/phones_and_lan_installation_diagram.pdf))

Ένα τυπικό ADSL splitter (διαχωριστής σήματος) που χρησιμοποιείται στις εγκαταστάσεις δικτύου, φαίνεται στην παρακάτω εικόνα 5.1.4.2.α:

Εικόνα 5.1.4.2.α. Τυπικό ADSL splitter (διαχωριστής)

5.1.4.3 Το ντεσιμπέλ (dB), Λόγος Σήματος προς Θόρυβο (SNR), Εξασθένηση

Το ντεσιμπέλ (dB). Ο χειρισμός πολύ μεγάλων ή πολύ μικρών αριθμών και οι πράξεις μεταξύ τους οι οποίες έχουν ως αποτέλεσμα ακόμα μεγαλύτερους ή αντίστοιχα μικρότερους αριθμούς, δυσκόλευαν πάντα τους μηχανικούς και τεχνικούς επικοινωνιών ιδίως κατά τη διάρκεια εργασιών και μετρήσεων πεδίου.

Για παράδειγμα, εάν μια τηλεπικοινωνιακή συσκευή εκπέμπει σήμα ισχύος 0,001W ή 1mW (μιλιβάτ) το οποίο ταξιδεύει μέσα από ένα κανάλι επικοινωνίας με **εξασθένηση** 10.000 φορές, στον προορισμό φτάνει σήμα ισχύος 0,001 * 1/10.000 = 0,0000001W.

Νωρίς, ακόμη, το συγκεκριμένο πρόβλημα αντιμετωπίστηκε με την εισαγωγή μονάδων μετρήσεων και σύγκρισης οι οποίες βασίζονται στις μαθηματικές ιδιότητες των **λογαρίθμων**. Αν η τιμή του μεγέθους αντικατασταθεί από τον λογάριθμό της, τότε οι αριθμοί έχουν λιγότερα ψηφία και, αντί για πολλαπλασιασμούς και διαιρέσεις, κάνουμε προσθέσεις και αφαιρέσεις.

Στην περίπτωσή μας, log(0,001)=-3 και log(1/10.000)=-4. Η τελική στάθμη είναι -3 + (-4)=-7 ή σε κανονική μορφή 10^{-7} W.

Ο λογάριθμος του αριθμού που εκφράζει πόσες φορές είναι μεγαλύτερο ή μικρότερο ένα μέγεθος από ένα άλλο ονομάστηκε **Bel** (προς τιμήν του εφευρέτη της πρώτης πρακτικής

συσκευής τηλεφώνου, Alexander Graham Bell). Επειδή το Bel (B) είναι πρακτικά μεγάλη μονάδα, χρησιμοποιείται το δέκατο του Bel ή **deciBel (dB)**, 1 dB = 0,1 Bel ή 10 dB = 1 Bel.

Εξ ορισμού είναι: $dB = 10 \log\left(\frac{P_2}{P_1}\right)$, όταν συγκρίνουμε τιμές ισχύος σημάτων (ηλεκτρικών ή οπτικών).

Το **deciBel (dB)** είναι καθαρός αριθμός (σχετικός, συγκρίνει μεγέθη). Μόνο όταν οριστεί το μέγεθος αναφοράς (P_1, στον παρονομαστή), το **dB** συνοδεύεται από επιπλέον χαρακτήρα ο οποίος προσδιορίζει το μέγεθος αναφοράς και το **dB** είναι αριθμός στις ίδιες μονάδες με το μέγεθος αναφοράς.

Παράδειγμα: Μια ασύρματη κάρτα δικτύου εκπέμπει με ισχύ **100mW** ή **20 dBm** (m: το μέγεθος αναφοράς είναι το 1mW). Το σήμα οδηγείται μέσα από καλώδιο με εξασθένηση 3 **dB** (-) σε μια κεραία με κέρδος 6 **dBi** (+) (I συγκρίνεται με ισοτροπική κεραία - isotropic).

Η τελική ισχύς EIRP (Effective Isotropic Radiated Power), που εκπέμπεται, είναι 20 -3 +6 = 23 dBm (200mW), ενώ με μια ισοτροπική κεραία λείπει ο τελευταίος παράγοντας (+6dB) και εκπέμπει με 20 -3 = 17 dBm (50mW).

Γιατί χρησιμοποιούμε το dB;

Επειδή για διαδοχικές βαθμίδες ενισχυτών και εξασθενήσεων **ο υπολογισμός του συνολικού κέρδους** ανάγεται σε **πρόσθεση και αφαίρεση** των επιμέρους κερδών ή απωλειών σε dB, αντί για πολλαπλασιασμούς και διαιρέσεις.

Ο Πίνακας 5.1.4.3.α δείχνει την αντιστοιχία dB σε λόγους τιμών ισχύος και τάσεων/ρευμάτων. Με βάση τον πίνακα επαληθεύστε ότι οι τιμές ισχύος εκπομπής (σε mW) της ασύρματης κάρτας του παραδείγματος είναι αυτές που φαίνονται στις παρενθέσεις.

Το **ντεσιμπέλ** (**decibel dB**)

- Είναι **λογαριθμική** (log) μονάδα. Καθαρός **αριθμός**.
- Βασική μονάδα είναι το Bel. Επειδή είναι πρακτικά μεγάλη χρησιμοποιείται το deciBel (1 deci Bel = 0,1 Bel).
- Εκφράζει πόσες φορές είναι ένα μέγεθος **μεγαλύτερο (+)** ή **μικρότερο (-)** από ένα άλλο.
- **Μηδέν 0 dB** σημαίνει ότι τα δυο συγκρινόμενα μεγέθη **είναι ίσα** (και **ΟΧΙ μηδέν**).
- Όταν το dB συνοδεύεται και από **επιπλέον γράμμα**(-τα), παύει να είναι καθαρός αριθμός.
- Δείχνει πόσες φορές είναι μεγαλύτερο/μικρότερο από το **μέγεθος αναφορά**ς (στις ίδιες μονάδες).
    - **30 dBm** :
        - μέγεθος αναφοράς (P1) το 1 mW
        - 30 dB -> x 1000 φορές
        - P2 = 1000 mW ή 1 W
- +3dB σημαίνει διπλάσια ισχύ, -3dB μισή ισχύ
- +10dB σημαίνει δεκαπλάσια ισχύ, -10dB το ένα δέκατο της ισχύος

dB	λόγος τιμών ισχύος	λόγος τάσεων ή ρευμάτων	dB	λόγος τιμών ισχύος	λόγος τάσεων ή ρευμάτων
-10	**0,10**	**0,316**	7,0	5,01	2,24
-6,0	**0,25**	**0,501**	8,0	6,31	2,51
-3,0	**0,50**	**0,707**	9,0	7,94	2,82
0	**1,00**	**1,00**	10	10	3,2
0,5	1,12	1,06	15	31,6	5,6
1,0	1,26	1,12	**20**	**100**	**10**
1,5	1,41	1,19	25	316	18
2,0	1,58	1,26	30	1.000	32
3,0	**2,00**	**1,41**	**40**	**10.000**	**100**
4,0	2,51	1,58	50	100.000	316
5,0	3,16	1,78	**60**	**10^6**	**1.000**
6,0	**3,98**	**2,00**	90	10^9	31600

Πίνακας 5.1.4.3.α: Αντιστοιχία dB σε λόγους τιμών ισχύος και τάσεων/ρευμάτων

Παράδειγμα χρήσης dB

Στον Πίνακα 2.4.1.δ: Επιδόσεις καλωδίων (TP) σύμφωνα με το ANSI/TIA-568-C.2, του 2ου Κεφαλαίου, φαίνεται ότι ένα καλώδιο UTP Cat 5e σε απόσταση 100 μέτρων παρουσιάζει εξασθένηση 21,0 dB στους 100MHz.

Αν το σήμα που ξεκινά είναι V1=2V (βολτ), πόσα βολτ φτάνουν στην άλλη άκρη;

Δουλεύοντας με τυπικές μονάδες ισχύος το W και τα υπο/πολλαπλάσιά του:

α' τρόπος (κατ' ευθείαν μαθηματικός υπολογισμός)

Κάνοντας χρήση της σχέσης που ορίζει το dB για τιμές ισχύος, θέτουμε P_1=4mW και χρησιμοποιώντας μια αριθμομηχανή (scientific calculator) λύνουμε τη σχέση:

$$dB = 10\log(P_2/P_1) \Rightarrow -21 = 10\log(P_2/P_1) \Rightarrow P_2/P_1 = 10^{-21/10} \Rightarrow P_2/4 = 10^{-2,1} \Rightarrow$$
$$P_2 = 4 \square 0,007943 \Rightarrow P_2 = 0,03177\, mW$$

Το σήμα ξεκινάει 4mW και μετά από εξασθένηση 21dB φτάνει να είναι μόλις 0,03177mW

β' τρόπος (με πίνακες αντιστοιχίας dB σε λόγους τιμών ισχύος)

Αν ανατρέξουμε στον Πίνακα 1 για λόγους τιμών ισχύος, τα 21dB είναι 20+1 dB ή συντελεστής 100 *1,26 =126. Επειδή είναι εξασθένηση, ως dB το πρόσημο είναι αρνητικό ή ο συντελεστής “διά”. Η τελική ισχύς είναι 4mW/126 = 0,03175mW, τιμή ίδια σχεδόν με αυτήν που υπολογίσαμε.

Δουλεύοντας με τυπικές μονάδες ισχύος το dBm και χρησιμοποιώντας το dB:

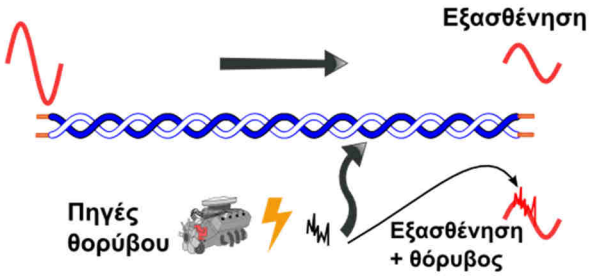
Το αρχικό σήμα είναι 6dBm και μετά από εξασθένηση -21dB φτάνει να είναι 6-21=-15dBm.

Δεν χρειάζεται να εμπλακούμε καθόλου με πολύπλοκους υπολογισμούς.

Εξασθένηση, Θόρυβος και Λόγος Σήματος προς Θόρυβο

Ένα σήμα, ηλεκτρικό, οπτικό ή ηλεκτρο-μαγνητικό, καθώς οδεύει μέσα από ένα επικοινωνιακό κανάλι, ένα φυσικό μέσο, σταδιακά χάνει μέρος της αρχικής ισχύος του και φτάνει στον προορισμό του με χαμηλότερη ισχύ. Η απώλεια οφείλεται στα φυσικά χαρακτηριστικά του μέσου, καλωδίου, οπτικής ίνας, τηλεφωνικής γραμμής κ.λπ.

Ως **εξασθένηση** ορίζεται ο λόγος της ισχύος του σήματος που φτάνει στην **είσοδο του δέκτη** λήψης προς την αρχική ισχύ στην **έξοδο του πομπού**. Η εξασθένηση μετράται σε **decibel (dB)** σε συγκεκριμένη συχνότητα, π.χ. 15dB @1kHz. Πολλές φορές, όταν χαρακτηρίζει φυσικά μέσα, δίνεται ως πίνακας τιμών για διαφορετικές συχνότητες ανά μονάδα μήκους.



Εικόνα 5.1.4.1.α: Εξασθένηση και θόρυβος

Το χρήσιμο σήμα της πληροφορίας παρότι ξεκινά από τον πομπό μόνο του, στη διαδρομή "εμπλουτίζεται" με διάφορα ανεπιθύμητα σήματα τα οποία το επηρεάζουν, το παραμορφώνουν και δυσχεραίνουν την ανάκτηση της πληροφορίας από τον δέκτη. Τα ανεπιθύμητα αυτά σήματα ονομάζονται **θόρυβος**. Ηλεκτρικός και ηλεκτρομαγνητικός θόρυβος επηρεάζουν αντίστοιχα ηλεκτρικά ή ηλεκτρομαγνητικά σήματα και προέρχεται από ηλεκτρομαγνητικές εκπομπές, ηλεκτρικές διατάξεις και μηχανές κακής σχεδίασης ή εσφαλμένη λειτουργία τους. Πηγή τέτοιου θορύβου μπορεί να είναι και ηλεκτρική δραστηριότητα της ατμόσφαιρας, όπως κεραυνοί και αστραπές. Ο ηλεκτρομαγνητικός θόρυβος δεν επηρεάζει τα οπτικά σήματα και τις οπτικές ίνες. Στα μεταλλικά-χάλκινα καλώδια ένας παράγοντας που μπορεί να μειώσει τον θόρυβο είναι η θωράκισή τους και γείωση της θωράκισης και των μεταλλικών μερών των συσκευών.

Εκτός από τους εξωτερικούς παράγοντες, θόρυβος παράγεται και εσωτερικά (ενδογενώς), από τα ηλεκτρονικά κυκλώματα ενίσχυσης και επεξεργασίας του σήματος. Αυτό όμως είναι κάτι για το οποίο δε μπορεί να γίνει τίποτε εκ των υστέρων, παρά μόνο κατά την σχεδίαση, επιλογή των εξαρτημάτων και την κατασκευή της συσκευής ή της ηλεκτρονικής διάταξης.

Η μέτρηση του θορύβου γίνεται στην είσοδο του δέκτη, γιατί εκεί ενδιαφέρει η επίδρασή του στο σήμα πληροφορίας. Η ισχύς του θορύβου μετράται στις ίδιες μονάδες με την ισχύ του ωφέλιμου σήματος πληροφορίας. Αυτό που ενδιαφέρει περισσότερο είναι η σχετική στάθμη του σήματος πληροφορίας σε σχέση με τη στάθμη του θορύβου. Η παράμετρος αυτή ονομάζεται **λόγος σήματος προς θόρυβο** (Signal to Noise Ratio, S/N ή SNR) και εκφράζεται σε deciBel (dB). Για παράδειγμα, αν σε μια γραμμή η στάθμη του σήματος είναι χίλιες (1000) φορές μεγαλύτερη από τη στάθμη του θορύβου, τότε ο λόγος σήματος προς θόρυβο (S/N) είναι 30dB.

Ο θόρυβος είναι σημαντικός παράγοντας, ιδιαίτερα σε μεγάλου μήκους επικοινωνιακές γραμμές, όπως οι τηλεφωνικές, επειδή το σήμα εκτίθεται για μεγάλες αποστάσεις σε πιθανούς παράγοντες δημιουργίας εξωτερικών θορύβων, ενώ παράλληλα το ωφέλιμο σήμα υπόκειται σε μεγαλύτερη εξασθένηση. Αυτό συνεπάγεται χειρότερο λόγο σήματος προς θόρυβο (S/N).

5.1.4.4 Άλλες παράμετροι γραμμών

Εκτός από την εξασθένηση και τον θόρυβο (λόγο S/N), υπάρχουν και άλλες μετρήσιμες παράμετροι οι οποίες χαρακτηρίζουν μια γραμμή επικοινωνίας και επηρεάζουν το μεταφερόμενο σήμα μέσω αυτής. Ήδη, από την αναφορά στην τεχνολογία Ethernet και τα μέσα που χρησιμοποιεί, έγινε λόγος για την **παραδιαφωνία** (cross-talk, NEXT/FEXT) η οποία είναι θόρυβος ο οποίος οφείλεται σε ωφέλιμα σήματα τα οποία οδεύουν σε γειτονικές γραμμές του ίδιου καλωδίου ή διαφορετικών καλωδίων.

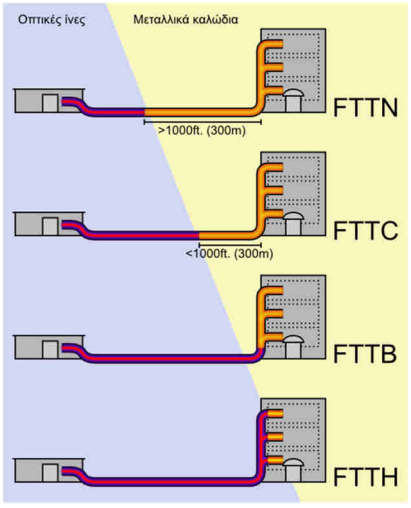
Σχεδόν όλες οι παράμετροι των γραμμών προσδιορίζουν παραμόρφωση του σήματος και χαρακτηρίζονται ως:

- Παραμόρφωση πλάτους. Επίδραση στο πλάτος του σήματος με ανομοιόμορφο τρόπο.
- Παραμόρφωση και αστάθεια φάσης. Οι διάφορες συχνότητες που απαρτίζουν το σήμα καθυστερούν σε διαφορετικό βαθμό να διανύσουν την απόσταση μέχρι το δέκτη.
- Αρμονική παραμόρφωση. Στον προορισμό εμφανίζονται συχνότητες οι οποίες δεν υπήρχαν στο αρχικό σήμα.
- Ολίσθηση συχνότητας. Η συχνότητα του σήματος στον προορισμό διαφέρει από την αρχική, κυρίως επειδή μεσολάβησε κάποια ενδιάμεση διαδικασία μετατροπής σε διατάξεις πολυπλεξίας.
- Ηχώ. Μέρος του σήματος ανακλάται προς τα πίσω, εξαιτίας κακής προσαρμογής των σύνθετων αντιστάσεων (εμπεδήσεων) στην διασύνδεση δυο γραμμών ή μιας γραμμής και μιας διάταξης. Η παράμετρος αυτή στις εκδόσεις υψηλών ταχυτήτων του Ethernet προσδιορίζεται από τις “απώλειες επιστροφής” (Return Loss).

Κάθε φαινόμενο παραμόρφωσης του σήματος με στιγμιαία μεγάλη επίδραση κυρίως στο πλάτος του σήματος και κατά τυχαία χρονικά διαστήματα χαρακτηρίζεται **κρουστικός θόρυβος**.

Συχνά στις επικοινωνίες γίνεται χρήση του όρου “**περιθώριο**” ή **margin**. Αυτό χαρακτηρίζει το περιθώριο που υπάρχει για τη σχετικά σίγουρη παροχή μιας υπηρεσίας ή λειτουργία με συγκεκριμένο τρόπο. Για παράδειγμα, εάν σε μια ασύρματη σύνδεση, για την επίτευξη σύνδεσης σε συγκεκριμένη ταχύτητα χωρίς συχνές αποσυνδέσεις, απαιτείται στάθμη σήματος τουλάχιστον -77dBm και η πραγματική στάθμη είναι -65dBm, τότε λέμε ότι το περιθώριο είναι 12dB.

5.2 Τεχνολογίες FTTH και Metro Ethernet

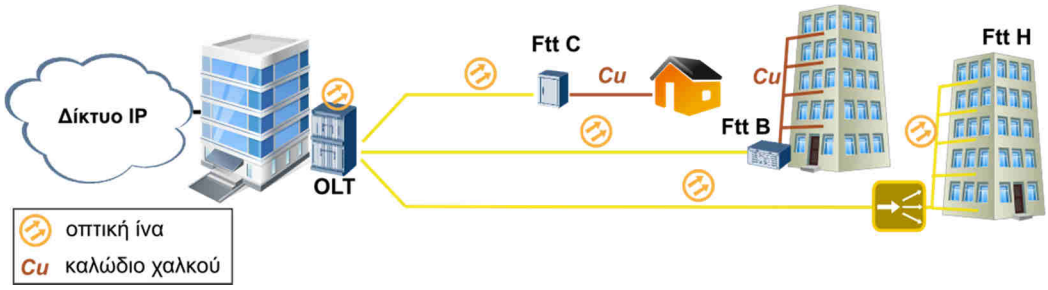


Εικόνα 5.2.α: Τεχνολογίες FttX (πηγή: wikipedia)

Οι ανάγκες των χρηστών δικτυακών υπηρεσιών και Διαδικτύου, σε ταχύτητα (εύρος ζώνης), διαρκώς αυξάνουν καθώς οι πάροχοι προσφέρουν νέες υπηρεσίες, όπως παρακολούθηση ταινιών (IPTV), και άλλες υπηρεσίες υψηλών απαιτήσεων σε ταχύτητες και μειωμένες καθυστερήσεις. Οι δισύρματες τηλεφωνικές γραμμές αδυνατούν να υποστηρίξουν σε όλο το μήκος τους τόσο υψηλές ταχύτητες. Ακόμα και στα τοπικά δίκτυα υψηλών ταχυτήτων, τα καλύτερα συνεστραμμένα ζεύγη (Cat 6A, 7) υποστηρίζουν τόσο μεγάλες ταχύτητες μόνο σε αποστάσεις της τάξης των 100m και μικρότερες. Το

]

φυσικό μέσο το οποίο διαθέτει εξαιρετικά μεγάλο εύρος ζώνης με μικρή εξασθένηση και υποστηρίζει αποστάσεις χιλιομέτρων είναι η **οπτική ίνα**. Οι τηλεπικοινωνιακοί οργανισμοί ήδη χρησιμοποιούν οπτικές ίνες στα δίκτυα κορμού και στα κέντρα δεδομένων τους (data centers). Αν μπορούσαν να φτάσουν μέχρι τον τελικό συνδρομητή με οπτική ίνα, τότε θα μπορούσε να του διατεθεί υψηλή ταχύτητα πρόσβασης στις παρεχόμενες υπηρεσίες και δυνατότητα παροχής νέων. Η τάση είναι να φτάσει η **οπτική ίνα** από το τηλεπικοινωνιακό κέντρο **στο σπίτι του συνδρομητή** ή όπως λέγεται **Fiber To The Home** (**FTTH**) με δυνατότητα παροχής ταχύτητας καλύτερης από 50Mbps και τυπικό στόχο τα 100-200Mbps προς τον συνδρομητή. Ο συνδρομητής μπορεί να έχει υπηρεσίες όπως ροή βίντεο (IPTV), πρόσβαση στο Διαδίκτυο και τηλεφωνία (VoIP).

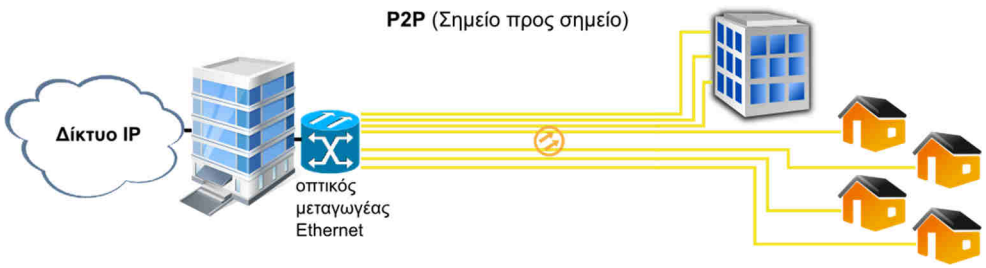


Εικόνα 5.2.β: Οπτική ίνα στην καμπίνα (Cabinet ή KV), στο κτίριο (Building) και στο σπίτι (Home)

Οι τηλεπικοινωνιακοί οργανισμοί και οι πάροχοι δικτυακών υπηρεσιών ήδη κινούνται προς αυτή την κατεύθυνση, υιοθετώντας εν τω μεταξύ και ενδιάμεσες λύσεις. Έτσι, η οπτική ίνα μπορεί να φτάνει μέχρι έναν απομακρυσμένο κατανεμητή κοντά στους συνδρομητές και να συνεχίζει με μικρά μήκη καλωδίων, να φτάνει ως την είσοδο της πολυκατοικίας ή και στο διαμέρισμα του συνδρομητή. Έτσι προκύπτουν όλες οι παραλλαγές του FTTH ή FTTX, όπως εναλλακτικά αναφέρεται, με το γράμμα X να αντικαθίσταται με άλλο, ώστε να δηλώνει το σημείο μέχρι το οποίο φτάνει η οπτική ίνα.

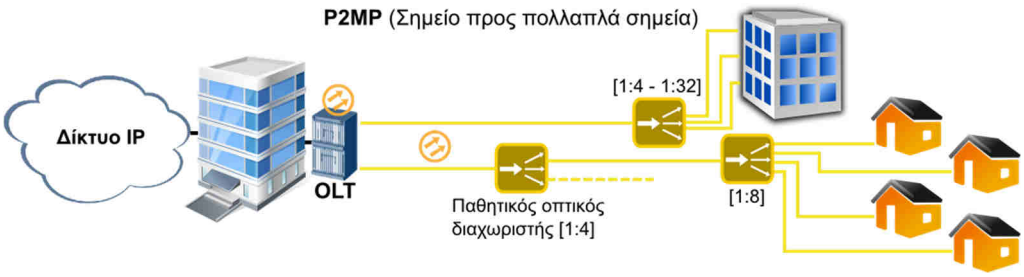
Οι αρχιτεκτονικές που διατίθενται για την υλοποίηση οπτικών δικτύων με τελικό στόχο την οπτική ίνα μέχρι το σπίτι του συνδρομητή καταλήγουν σε δυο προτάσεις.

- Δίκτυο με επικοινωνία “**σημείο προς σημείο**” (point to point - P2P). Η οπτική ίνα από το σπίτι του συνδρομητή καταλήγει σε **ενεργό εξοπλισμό** του παρόχου όπως έναν οπτικό μεταγωγέα (switch) Ethernet, χρησιμοποιώντας φυσική τοπολογία αστέρα ή και δακτυλίου, εφόσον χρησιμοποιηθεί άλλη τεχνολογία πρόσβασης στο μέσο.
- Δίκτυο με επικοινωνία “**σημείο προς σημεία**” (point to multipoint - P2MP). Οι οπτικές ίνες από τους συνδρομητές καταλήγουν σε παθητικούς οπτικούς διαχωριστές/μείκτες (splitters/combiners) και συνδυάζονται σε μία ίνα ή ζεύγος ινών για να καταλήξουν στον πάροχο.



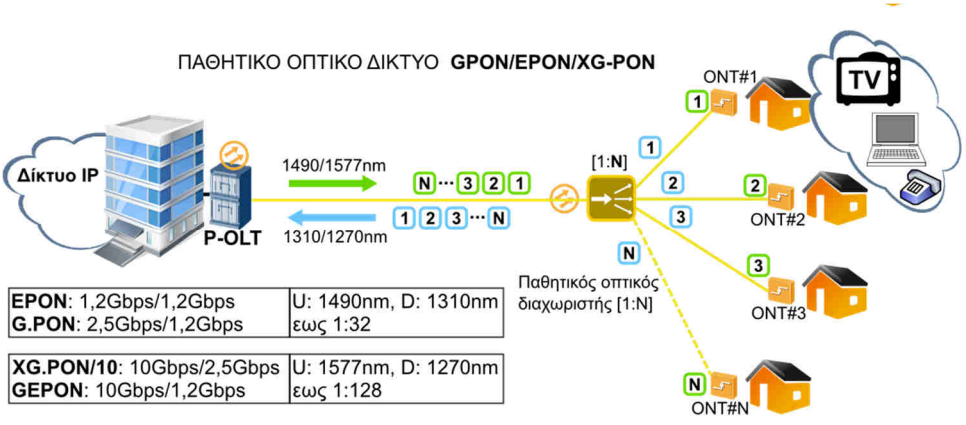
Εικόνα 5.2.γ: Αρχιτεκτονική "σημείο προς σημείο" (P2P)

Από τις ενέργειες των παρόχων φαίνεται να προκρίνεται η αρχιτεκτονική “σημείο προς σημεία” (p2mp) καθώς επιτρέπει στους παρόχους να την υλοποιήσουν σταδιακά, πλησιάζοντας στο σπίτι του συνδρομητή με ενδιάμεσες λύσεις, όπως την τοποθέτηση μίνι DSLAM (Digital Subscriber Line Access Multiplexer) στην καμπίνα διανομής (KV) ή μικρο-DSLAM στην πολυκατοικία και εξυπηρέτηση από εκεί και πέρα των συνδρομητών με τεχνολογίες καλωδίων χαλκού, ADSL και κυρίως VDSL.



Εικόνα 5.2.δ: Αρχιτεκτονική "σημείο προς σημεία"

Η τελική υλοποίηση ενός οπτικού δικτύου p2mp μέχρι το σπίτι του συνδρομητή αποκλειστικά με οπτικές ίνες (Fiber to the Home - FttH), επειδή σε όλη την ενδιάμεση διαδρομή από το τηλεπικοινωνιακό κέντρο του παρόχου μέχρι τον συνδρομητή χρησιμοποιεί **μόνο καλώδια οπτικών ινών και παθητικούς οπτικούς διαχωριστές/μείκτες** ονομάζεται “**παθητικό οπτικό δίκτυο**” (Passive Optical Network - **PON**). Ένα PON ανάλογα με τη χρησιμοποιούμενη τεχνολογία προσδιορίζεται ως E.PON (Ethernet PON), G.PON (Gigabit PON), GE.PON (Gigabit Ethernet PON), XG.PON (eXtra ή 10 Gigabit PON) και επιτυγχάνει διαφορετικές συνολικές (aggregate) ταχύτητες από (upstream) και προς (downstream) τον συνδρομητή. Οι υλοποιήσεις μεγαλύτερων ταχυτήτων έχουν τη δυνατότητα να διαμοιραστούν μέσω διαχωριστών σε περισσότερους συνδρομητές (από 1:32 μέχρι 1:128 για δίκτυο XGPON/10)



Εικόνα 5.2.ε: Παθητικό οπτικό δίκτυο (PON)

Για να μπορεί να περνά μέσα από μια οπτική ίνα πολλαπλό περιεχόμενο, ανερχόμενη και κατερχόμενη δικτυακή κίνηση, χρησιμοποιούνται διαφορετικά μήκη κύματος (wavelength) φωτός για κάθε κατεύθυνση. Η τεχνική είναι αντίστοιχη με την τεχνική πολυπλεξίας συχνότητας (FDM) των ηλεκτρικών σημάτων και λέγεται **πολυπλεξία μήκους κύματος** (Wavelength Division Multiplexing - **WDM**)

Τα δομικά στοιχεία του δικτύου είναι από τη μεριά του παρόχου:

1. η οπτική συσκευή τερματισμού της γραμμής (Optical Line Termination - OLT),
2. οι οπτικές ίνες,
3. οι ενδιάμεσοι παθητικοί οπτικοί διαχωριστές,
4. παθητικά εξαρτήματα συνδέσεων, πρίζες, συνδετήρες, και
5. στη μεριά του συνδρομητή, η συσκευή τερματισμού του οπτικού δικτύου (Optical Network Termination - ONT) ή μονάδα οπτικού δικτύου (Optical Network Unit - ONU) αντίστοιχη με το modem/router που δίνει ο πάροχος στην περίπτωση γραμμών ADSL/VDSL.

	Συνολική Ταχύτητα		**Μήκος κύματος**		
Τεχνολογία	**DownStream**	**UpStream**	**DownStream**	**UpStream**	**Διαχωριστής**
E.PON	1,2 Gbps	1,2 Gbps	1490nm	1310nm	έως 1:32 *(2,5:32 ≈ 80 Mbps)*
G.PON	2,5 Gbps	1,2 Gbps			
GE.PON	10 Gbps	1,2 Gbps	1578nm	1270nm	έως 1:128 *(10:32 ≈ 300 Mbps)*
XG.PON/10	10 Gbps	2,5 Gbps			

Πίνακας 5.2.α: Επιδόσεις παθητικών δικτύων οπτικών ινών

Παράλληλα με τις τεχνολογίες FttX, μερίδιο στις υλοποιήσεις δικτύων μητροπολιτικής αλλά και ευρύτερης έκτασης διεκδικεί και η τεχνολογία Ethernet, η οποία αποδεικνύεται εξαιρετικά ευέλικτη και προσαρμόσιμη στις νέες τεχνολογικές εξελίξεις. Ονομάζεται **μητροπολιτικό (metro) Ethernet** και χρησιμοποιεί τις δυνατότητες VLAN που έχει από το σχεδιασμό του το Ethernet, ώστε να παρέχει ιδιωτικές υπηρεσίες πάνω από δημόσια δίκτυα IP/MPLS. Η δυνατότητα VPLS – Virtual Private LAN Service (περιγράφεται στα IETF/RFC 4761 και 4762) καθιστά εφικτή τη χρήση του Ethernet σε κλίμακες μητροπολιτικής περιοχής (MAN) αλλά και ευρείας περιοχής (WAN). Αντίθετα με τις τεχνολογίες VPN πάνω από δίκτυα IP, οι οποίες επιτρέπουν συνδέσεις “σημείο προς σημείο”, το metro Ethernet επιτρέπει τη σύνδεση “πολλά σημεία προς σημεία” και υποστηρίζει τη δυνατότητα εκπομπής (broadcast). Χρησιμοποιεί οπτικές ίνες και υποστηρίζει ταχύτητες στο συνδρομητή 10/100/1000Mbps.

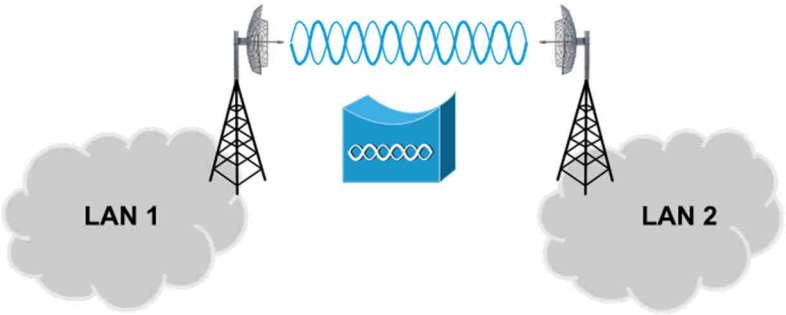
5.3 Ασύρματες ζεύξεις

Κατά την επέκταση του χώρου κάλυψης ενός τοπικού δικτύου, πολλές φορές προκύπτει η ανάγκη προσθήκης κόμβων ή και ολόκληρου υποδικτύου σε χώρο στον οποίο οι τρέχουσες τεχνολογίες τοπικής δικτύωσης δεν μπορούν να καλύψουν. Δύο είναι οι βασικές αιτίες αδυναμίας επέκτασης του δικτύου:

- Η απόσταση είναι αρκετά μεγάλη, πέρα από τις προδιαγραφές της καλωδίωσης ή της συμβατικής ασύρματης δικτύωσης (WiFi).
- Μεσολαβεί ιδιωτική ή δημόσια περιουσία (κτήματα, οικόπεδα ή κτίρια, δρόμοι) και δεν είναι εφικτή η διέλευση της καλωδίωσης μέσα από αυτήν, παρότι η απόσταση καλύπτεται από κάποια τεχνολογία ενσύρματης δικτύωσης.

Στις περιπτώσεις αυτές μοναδική λύση αποτελεί η χρήση ασύρματης ζεύξης μεταξύ των δυο τοποθεσιών. Υπάρχουν διάφορες τεχνολογίες ασύρματης μετάδοσης δεδομένων, όμως, η

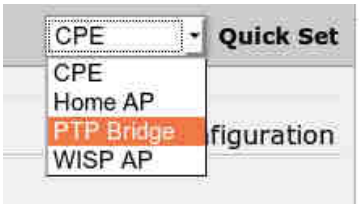
πιο συνηθισμένη είναι η **τεχνολογία WiFi** (IEEE802.11) και μάλιστα υποστηριζόμενη από **εξωτερικές κατευθυντικές κεραίες** σε συνθήκες **οπτικής επαφής** μεταξύ των δυο σημείων.



Εικόνα 5.3.α: Σύνδεση δυο δικτύων μέσω ασύρματης ζεύξης

Οι περιοχές συχνοτήτων 2,4GHz και 5GHz, στις οποίες λειτουργούν τα ασύρματα δίκτυα WiFi, διατίθενται για χρήση από διάφορες υπηρεσίες αλλά και βιομηχανικές, επιστημονικές, ιατρικές εφαρμογές (Industrial Scientific Medical Applications - ISM). Δεν διατίθενται για αποκλειστική χρήση ασύρματης δικτύωσης. Συσκευές ISM και ασύρματης δικτύωσης (RLAN) πωλούνται και χρησιμοποιούνται χωρίς άδεια (Unlicensed). Η χρήση τους πρέπει να είναι σύμφωνη με τα ευρωπαϊκά πρότυπα ETSI/EN 300328 (2,400-2,4835) και ETSI/EN 301893 (5,150-5,350 και 5,470-5,725) κατ' απαίτηση του Εθνικού Κανονισμού Κατανομής Ζωνών Συχνοτήτων (ΕΚΚΖΣ) που είναι νόμος του κράτους.

Απαιτούνται δυο συσκευές, μια για κάθε πλευρά ή κάθε δίκτυο, τα οποία πρόκειται να συνδεθούν μαζί. Λειτουργικά θα πρέπει ο εξοπλισμός να μπορεί να υποστηρίξει την διασύνδεση των δυο δικτύων, καθώς όλες οι ασύρματες συσκευές δικτύωσης δεν μπορούν να υποστηρίξουν όλους τους τρόπους λειτουργίας. Εξοπλισμός ο οποίος έχει την επιλογή για "**γεφύρωση**" (Bridging mode), υποστήριξη πλαισίων τεσσάρων διευθύνσεων MAC (4A) ή αναφέρει την **υποστήριξη WDS** (Wireless Distribution System) είναι κατάλληλος για τέτοια λειτουργία. Πολλοί κατασκευαστές προσφέρουν εξοπλισμό με υποστήριξη δικών τους πρωτοκόλλων γι' αυτή τη δουλειά. Η χρήση γεφύρωσης αποτελεί μια λύση διασύνδεσης των δυο δικτύων, δεν είναι όμως μοναδική. Μπορούν να χρησιμοποιηθούν και άλλες λύσεις, όπως η δρομολόγηση ή η λειτουργία επαναλήπτη. Επαφίεται στον υπεύθυνο υλοποίησης της λύσης διασύνδεσης των δυο δικτύων να διερευνήσει την τεχνική τεκμηρίωση του κατασκευαστή του υλικού, ώστε να βεβαιωθεί ότι είναι κατάλληλο για τη χρήση που το προορίζει.



Εικόνα 5.3.β: Τρόπος λειτουργίας

Από πλευράς υλικού, επειδή κατά κανόνα τοποθετείται σε εξωτερικό χώρο, στον ιστό της κεραίας και κοντά σε αυτή, θα πρέπει να είναι κατασκευασμένο να αντέχει στις εξωτερικές καιρικές συνθήκες και θερμοκρασίες.

Η τροφοδοσία με ρεύμα της συσκευής μπορεί να παρέχεται μέσω του καλωδίου Ethernet, χρησιμοποιώντας κάποια τεχνική Power Over Ethernet (POE).

Hardware specification		
PoE	Passive PoE (Up to 60 meters)	
Interface	**Wireless IEEE 802.11a/n** **LAN/WAN: 10/100Base-TX**, Auto-MDI/MDIX x 1 Grounding Terminal x 1	
Data Rate	802.11a: 54, 48, 36, 24, 18, 12, 9 and 6Mbps 802.11n (20MHz): up to 72Mbps 802.11n (40MHz): up to 150Mbp	
Media Access Control	CSMA/CA	
Modulation	Transmission/Emission Type: OFDM Data modulation type: OFDM with BPSK, QPSK, 16-QAM, 64-QAM	
Frequency Band *Ζώνη συχνοτήτων*	5.180-5.240GHz; 5.745-5.825GHz	
Operating Channel .	5.180GHz-CH36 5.765GHz-CH153 5.200GHz-CH40 5.785GHz-CH157 5.220GHz-CH44	5.805GHz-CH161 5.240GHz-CH48 5.825GHz-CH165 5.745GHz-CH149
RF Output Power ***Ισχύς εξόδου***	802.11a: 27 ± 1dBm 802.11n: 24 ± 1dBm	
Receiver Sensitivity ***Ευαισθησία δέκτη***	**802.11a:** 54M: -77dBm 48M: -79dBm 36M: -83dBm 24M: -86dBm 18M: -91dBm 12M: -92dBm 9M: -93dBm 6M: -94dBm	**802.11n:** 150M: -73dBm 121.5M: -76dBm 108M: -77dBm 81M: -81dBm 54M: -84dBm 40.5M: -88dBm 27M: -91dBm 13.5M: -93dBm
Software specification		
Wireless Mode ***Τρόπος ασύρματης λειτουργίας***	AP Client **WDS PTP**	**WDS PTMP** **WDS Repeater** (AP+WDS) Universal Repeater (AP+Client)

Πίνακας 5.3.α: Απόσπασμα από το φύλλο χαρακτηριστικών ενός AP (Access Point)

Αφού διασφαλιστούν όλες αυτές οι προϋποθέσεις και απαιτήσεις για τις συσκευές, θα πρέπει να υπολογιστεί αν είναι ικανές να καλύψουν την απόσταση μεταξύ των δυο σημείων. Αυτό χαρακτηρίζεται ως προϋπολογισμός ζεύξης (link budget), για τον οποίο γίνεται μια εκτενέστερη αναφορά στην ενότητα Π.2 του Παραρτήματος των σημειώσεων.

Σε μια ασύρματη ζεύξη, **αυτό** που ενδιαφέρει περισσότερο είναι τα χαρακτηριστικά του εξοπλισμού που έχουν να κάνουν με το **φυσικό επίπεδο**. Στο φυσικό επίπεδο ανήκει:

- ο πομπός (ενσωματωμένος),
- ο δέκτης (ενσωματωμένος),
- οι κεραίες (συνήθως εξωτερικές),
- τα εξαρτήματα διασύνδεσης εξοπλισμού - κεραιών καθώς και
- ο χώρος που μεσολαβεί μεταξύ των κεραιών των δυο κόμβων.

Ο σκοπός είναι το σήμα που θα φτάσει στην είσοδο του δέκτη να είναι αρκετό, ώστε να μπορέσει να διεγείρει τα κυκλώματα του δέκτη και να ανακτηθεί η πληροφορία που μεταφέρει. Από το φύλλο χαρακτηριστικών του εξοπλισμού, αυτά που μας ενδιαφέρουν είναι η **συχνότητα λειτουργίας** (Frequency Band, Operating Channel), η **ισχύς**

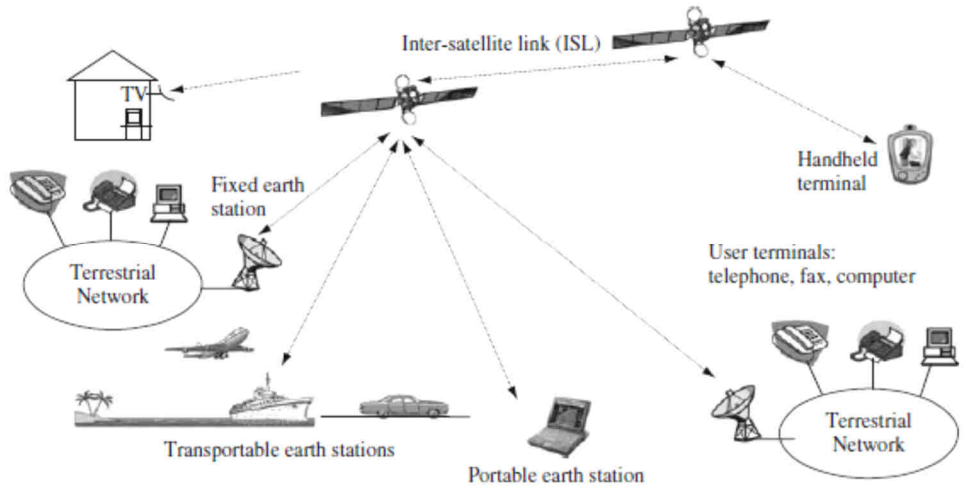
ραδιοσυχνότητας εξόδου του πομπού (RF Output Power) και η **ευαισθησία του δέκτη** (Receiver Sensitivity).

Η ζώνη των 5GHz προτιμάται, επειδή η ζώνη των 2,4GHz είναι πιο επιβαρυμένη (θόρυβος), από εξοπλισμό που ήδη λειτουργεί εκεί, όπως ασύρματα δίκτυα wifi, συσκευές Bluetooth, φούρνοι μικροκυμάτων κ.ά. Μελλοντικά προβλέπεται η χρήση και υψηλότερων συχνοτήτων για τις ασύρματες μεταδόσεις δεδομένων.

5.3.1 Δορυφορικές ζεύξεις

Εφαρμογές και υπηρεσίες δορυφορικών δικτύων. Η Δορυφορική Δικτύωση (Satellite Networking) είναι ένας αναπτυσσόμενος τομέας, ο οποίος έχει αναπτυχθεί σημαντικά από τη γέννηση του πρώτου τηλεπικοινωνιακού δορυφόρου, στις παραδοσιακές ραδιοτηλεοπτικές υπηρεσίες τηλεφωνίας και τηλεόρασης έως τα σύγχρονα ευρυζωνικά δίκτυα και το Διαδίκτυο, το βίντεο κατά παραγγελία και τις ψηφιακές δορυφορικές εκπομπές. Πολλές από τις τεχνολογικές εξελίξεις στους τομείς της δικτύωσης επικεντρώνονται σε δορυφορικές ζεύξεις. Με την αύξηση των απαιτήσεων για εύρος ζώνης και φορητότητα, ο δορυφόρος είναι μια λογική επιλογή, για να παρέχει μεγαλύτερο εύρος ζώνης με παγκόσμια κάλυψη, που υπερβαίνει τις δυνατότητες των επίγειων δικτύων και δίνει μεγάλη υπόσχεση για το μέλλον. Με την ανάπτυξη των τεχνολογιών δικτύωσης, τα δορυφορικά δίκτυα όλο και περισσότερο ενσωματώνονται στην υποδομή του παγκόσμιου δικτύου (Global Network Infrastructure – GNI). Η ενσωμάτωση των κινητών ad hoc δικτύων (MANET – Κεφ. 2) παρέχει νέα συστήματα για υπηρεσίες έκτακτης ανάγκης και διάσωσης με μεγάλη φορητότητα. Ως εκ τούτου, η διαδικτύωση με επίγεια δίκτυα και πρωτόκολλα είναι ένα σημαντικό μέρος της δορυφορικής δικτύωσης.

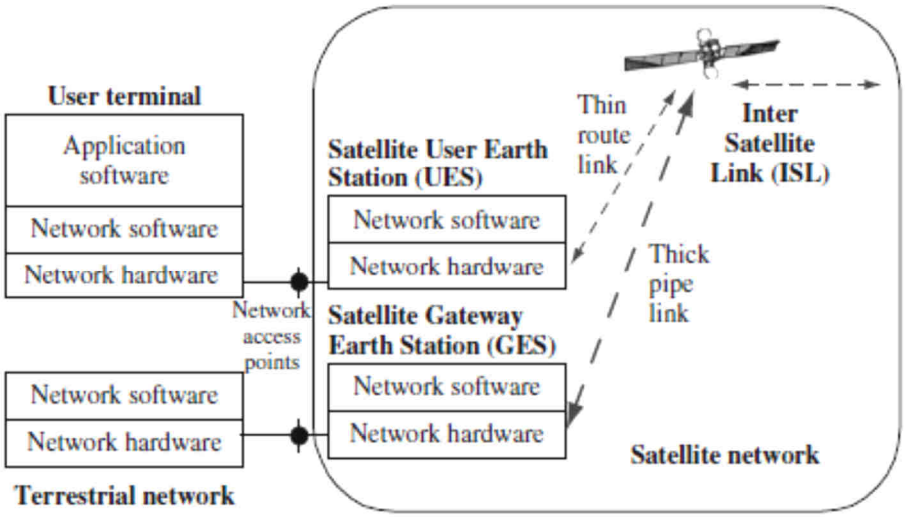
Ο απώτερος στόχος των δορυφορικών δικτύων είναι η παροχή υπηρεσιών και εφαρμογών. Τα τερματικά χρήστη παρέχουν υπηρεσίες και εφαρμογές απευθείας στους χρήστες. Το δίκτυο παρέχει υπηρεσίες μεταφοράς πληροφοριών μεταξύ των τερματικών των χρηστών δια μέσου των κόμβων του δικτύου, των switches και των δρομολογητών για μία ορισμένη απόσταση. Στο σχήμα 5.3.2.α παρουσιάζεται μια τυπική διαμόρφωση του δορυφορικού δικτύου που αποτελείται από επίγεια δίκτυα, δορυφόρους με μια σύνδεση μεταξύ δορυφόρων **(inter-satellite link - ISL)**, σταθερούς επίγειους σταθμούς, φορητούς επίγειους σταθμούς, φορητούς σταθμούς εργασίας, υπολογιστές χειρός και συσκευές χρηστών που συνδέονται σε δορυφορικές ζεύξεις, απευθείας ή μέσω επίγειων δικτύων (terrestrial networks).



Σχήμα 5.3.2.α: Τυπικές εφαρμογές και υπηρεσίες δορυφορικής δικτύωσης
(Πηγή: Zhili Sun, (2014), "Satellite networking principles and protocols")

Οι ρόλοι των Δορυφορικών Δικτύων. Στα επίγεια δίκτυα, πολλές συνδέσεις (links) και κόμβοι απαιτούνται, για να φτάσουμε σε μεγάλες αποστάσεις και να καλύψουμε ευρείες περιοχές. Αυτά τα δίκτυα έχουν οργανωθεί με στόχο την ανάπτυξη με το δυνατόν λιγότερο κόστος, τη συντήρηση και τη σωστή λειτουργία τους. Η φύση των δορυφόρων κάνει τα δορυφορικά δίκτυα να διαφέρουν ριζικά από τα επίγεια δίκτυα ως προς τις αποστάσεις, το διαμοιραζόμενο εύρος ζώνης, τις τεχνολογίες μεταφοράς, τον σχεδιασμό, την ανάπτυξη και λειτουργία, καθώς και τα έξοδα και τις εφαρμογές.

Λειτουργικά, τα δορυφορικά δίκτυα μπορούν να παρέχουν απευθείας συνδέσεις μεταξύ των τερματικών των χρηστών, συνδέσεις των τερματικών σταθμών σε επίγεια δίκτυα, καθώς και συνδέσεις μεταξύ των επίγειων δικτύων ως δίκτυα κορμού (backbones). Τα τερματικά χρήστη μπορούν να παρέχουν υπηρεσίες και εφαρμογές για τους ανθρώπους, τα οποία συχνά είναι ανεξάρτητα από τα δορυφορικά δίκτυα, δηλαδή, το ίδιο τερματικό μπορεί να χρησιμοποιηθεί για την πρόσβαση σε δορυφορικά δίκτυα, καθώς και σε επίγεια δίκτυα. Τα δορυφορικά τερματικά (satellite terminals), που ονομάζεται επίσης και επίγειοι σταθμοί (earth stations), είναι το επίγειο τμήμα των δορυφορικών δικτύων, παρέχοντας σημεία πρόσβασης προς τα δορυφορικά δίκτυα για τα τερματικά του χρήστη μέσω του επίγειου σταθμού χρήστη **(User Earth Station - UES)** και για τα επίγεια δίκτυα μέσω του επίγειου σταθμού πύλης **(Gateway Earth Station - GES)**. Ο δορυφόρος είναι ο πυρήνας των δορυφορικών δικτύων, αλλά και το κέντρο των δικτύων όσον αφορά τόσο τις λειτουργίες όσο και τις φυσικές συνδέσεις. Μερικές φορές υπάρχουν και συνδέσεις μεταξύ των δορυφόρων. Το σχήμα 5.3.2.β απεικονίζει τη σχέση μεταξύ του τερματικού χρήστη (user terminal), του επίγειου δικτύου (terrestrial network) και του δορυφορικού δικτύου (satellite network).



Σχήμα 5.3.2.β Σχέση επίγειου, δορυφορικού δικτύου και τερματικού χρήστη
(Πηγή: Zhili Sun, (2014), "Satellite networking principles and protocols")

Συνήθως, τα δορυφορικά δίκτυα αποτελούνται από δορυφόρους που επικοινωνούν με λίγους μεγάλους GES και πολλούς μικρούς UES. Οι μικροί GES χρησιμοποιούνται για άμεση πρόσβαση από τα τερματικά των χρηστών και οι μεγάλοι UES για τη διασύνδεση των επίγειων δικτύων. Οι δορυφορικοί UES και GES προσδιορίζουν τα όρια του δορυφορικού δικτύου. Όπως και σε άλλα είδη δικτύων, οι χρήστες έχουν πρόσβαση στα δορυφορικά δίκτυα μέσα στα όριά του. Για κινητά και μεταφερόμενα τερματικά, οι λειτουργίες του τερματικού χρήστη και του δορυφορικού UES μπορούν να ενσωματωθούν σε μια ενιαία μονάδα, αλλά για το μεταφερόμενο τερματικά, οι κεραίες τους είναι διακριτά ορατές. Υπάρχουν δύο μέρη: η εσωτερική μονάδα (**in-door unit - IDU**) και η εξωτερική μονάδα

(**outdoor-unit - ODU**). Η IDU περιέχει πομπό και δέκτη και η ODU περιέχει χαμηλού θορύβου μετατροπέα (Low Noise Block - LNB) και Block Up μετατροπέα (BUC).

Οι πιο σημαντικοί ρόλοι των δορυφορικών δικτύων είναι να παρέχουν πρόσβαση από τα τερματικά των χρηστών και να διασυνδέονται με επίγεια δίκτυα, έτσι ώστε οι εφαρμογές και οι υπηρεσίες που παρέχονται από επίγεια δίκτυα, όπως η τηλεφωνία, η τηλεόραση, η ευρυζωνική πρόσβαση και η σύνδεση στο Διαδίκτυο, να μπορεί να επεκταθεί σε μέρη όπου η καλωδιακή και επίγεια ραδιοφωνία δεν μπορεί να εγκατασταθεί οικονομικά και να συντηρηθεί. Επιπλέον, τα δορυφορικά δίκτυα μπορούν να φέρουν αυτές τις υπηρεσίες και τις εφαρμογές σε πλοία, αεροσκάφη, οχήματα, στο διάστημα και σε τόπους που υπερβαίνουν τις δυνατότητες των επίγειων δικτύων. Οι δορυφόροι παίζουν σημαντικό ρόλο και στο στρατιωτικό τομέα, στη μετεωρολογία, στα συστήματα παγκόσμιου εντοπισμού θέσης (GPS), στην παρατήρηση της γης και του περιβάλλοντος, στις ιδιωτικές υπηρεσίες δεδομένων και επικοινωνίας, και στη μελλοντική ανάπτυξη για νέες υπηρεσίες και εφαρμογές για άμεση κάλυψη παγκόσμιας εμβέλειας, όπως ευρυζωνικών δικτύων, και τις νέες γενιές κινητών δικτύων και ψηφιακών υπηρεσιών μετάδοσης σε όλο τον κόσμο. Επίσης, σε υπηρεσίες έκτακτης ανάγκης και σε υπηρεσίες διάσωσης από καταστροφές, όπως πλημμύρες, σεισμούς και ηφαίστεια.

Στην ενότητα Π.6 του Παραρτήματος μπορείτε να μελετήσετε πληροφορίες που σχετίζονται με το λογισμικό, το υλικό, τις υπηρεσίες και τις εφαρμογές των δορυφορικών δικτύων.

Διεπαφές δορυφορικών δικτύων

Τυπικά, τα δορυφορικά δίκτυα έχουν δύο τύπους εξωτερικών διεπαφών (interfaces): η μία είναι μεταξύ του δορυφορικού UES και του τερματικού χρήστη και η άλλη είναι μεταξύ των δορυφορικών GES και των επίγειων δικτύων.

Εσωτερικά, υπάρχουν τρεις τύποι διασύνδεσης: μεταξύ των UES και του συστήματος δορυφορικής επικοινωνίας (satellite communication payload system), μεταξύ των GES και του συστήματος δορυφορικής επικοινωνίας και η διασύνδεση (ISL) μεταξύ των δορυφόρων. Όλες κάνουν χρήση ραδιοζεύξεων, ενώ η ISL μπορεί να χρησιμοποιήσει και οπτικές συνδέσεις.

Όπως τα φυσικά καλώδια, το **εύρος ζώνης ραδιοσυχνοτήτων** είναι ένας από τους πιο σημαντικούς και σπάνιους πόρους για την παροχή πληροφοριών πάνω από τα δορυφορικά δίκτυα. Σε αντίθεση με τα καλώδια, το εύρος ζώνης δεν μπορεί να κατασκευαστεί με την προσθήκη περισσότερων καλωδίων, αλλά μπορεί να μοιραστεί και να βελτιστοποιηθεί η χρήση του μόνο.

Ο άλλος σημαντικός πόρος είναι η **ισχύς μετάδοσης**. Συγκεκριμένα, η ισχύς περιορίζεται για τερματικά των χρηστών που απαιτούν φορητότητα ή για εκείνα που εγκαθίστανται σε απομακρυσμένες περιοχές και βασίζονται στην παροχή ενέργειας από μπαταρία και για συστήματα επικοινωνίας σε δορυφόρους που βασίζονται σε μπαταρία και ηλιακή ενέργεια. Το εύρος ζώνης και η ισχύς μετάδοσης, μαζί με τις συνθήκες μετάδοσης και το περιβάλλον, καθορίζουν τη **χωρητικότητα** (capacity) των δορυφορικών δικτύων.

Η δορυφορική δικτύωση μοιράζεται πολλές βασικές έννοιες με τη γενική δικτύωση. Σε όρους τοπολογίας, μπορεί να ρυθμιστεί σε αστέρα (star) ή πλέγμα (mesh). Όσον αφορά την τεχνολογία μετάδοσης, μπορεί να συσταθεί για σημείο-προς-σημείο (point-to-point), σημείο-προς-σημεία (point-to-multipoint) και σημεία-προς-σημεία (multipoint-to-multipoint) συνδέσεις. Σε όρους διεπαφής, μπορούμε εύκολα να χαρτογραφήσουμε το δορυφορικό δίκτυο σε όρους γενικών δικτύων, όπως διεπαφή χρήστη του δικτύου (User Network Interface - UNI) και διεπαφή των κόμβων του δικτύου (Network Nodes Interface - NNI).

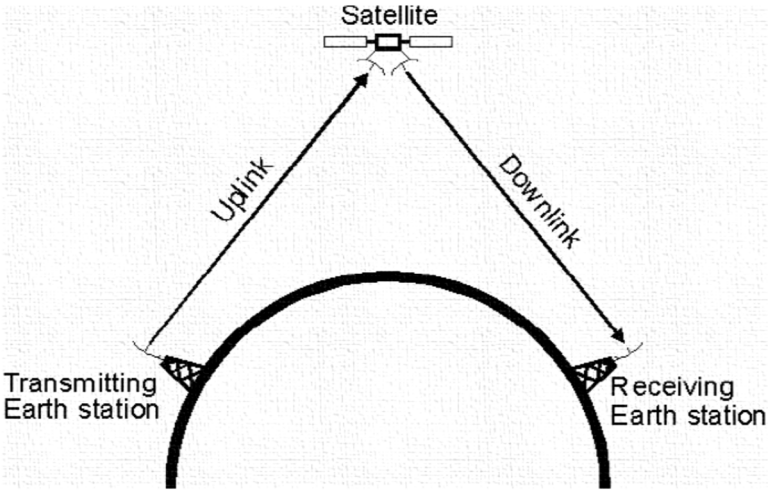
Όταν δύο δίκτυα πρέπει να συνδεθούν μεταξύ τους, μια διεπαφή δικτύου-σε-δίκτυο είναι απαραίτητη, που είναι η διεπαφή ενός κόμβου σε ένα δίκτυο με ένα κόμβο δικτύου σε ένα άλλο δίκτυο. Έχουν παρόμοιες λειτουργίες, όπως οι NNI. Ως εκ τούτου, οι NNI μπορούν επίσης να χρησιμοποιηθούν για να υποδηλώσουν μια διεπαφή δικτύου-σε-δίκτυο.

Οι υπηρεσίες αποτελούν τα βασικά στοιχεία που παρέχονται από τα δίκτυα. Οι εφαρμογές "χτίζονται" από αυτά τα βασικά στοιχεία. Συχνά, οι όροι υπηρεσίες και εφαρμογές χρησιμοποιούνται εναλλακτικά στη βιβλιογραφία. Μερικές φορές είναι χρήσιμο να τους διακρίνουμε.

Σχήμα 5.3.2.γ. Τηλεπικοινωνιακός δορυφόρος
(Πηγή: https://el.wikipedia.org/wiki/Τηλεπικοινωνιακός_δορυφόρος)

Τηλεπικοινωνιακός δορυφόρος. Τηλεπικοινωνιακός δορυφόρος ονομάζεται ο μη επανδρωμένος τεχνητός δορυφόρος (unmanned artificial satellite), μέσω του οποίου παρέχονται υπηρεσίες μεγάλων αποστάσεων, όπως τηλεοπτικής και ραδιοφωνικής μετάδοσης, τηλεφωνικών επικοινωνιών και συνδέσεων ηλεκτρονικών υπολογιστών. Οι δορυφόροι έχουν τη μοναδική δυνατότητα να παρέχουν κάλυψη μεγάλων γεωγραφικών περιοχών και να διασυνδέουν μακρινούς και δυσπρόσιτους τηλεπικοινωνιακούς κόμβους και γι' αυτό τα δορυφορικά δίκτυα αποτελούν σήμερα αναπόσπαστο τμήμα των περισσότερων τηλεπικοινωνιακών συστημάτων.

Ένας δορυφόρος λαμβάνει σήμα μικροκυμάτων από έναν επίγειο σταθμό (uplink), κατόπιν ενισχύει και αναμεταδίδει το σήμα σε έναν σταθμό λήψης στη Γη σε διαφορετική συχνότητα (η κατιούσα σύνδεση). Ένας δορυφόρος επικοινωνίας τοποθετείται σε γεωσύγχρονη τροχιά, πράγμα που σημαίνει ότι τίθεται σε τροχιά με την ίδια ταχύτητα με την οποία περιστρέφεται η Γη. Ο δορυφόρος μένει στην ίδια θέση σχετικά με την επιφάνεια της Γης, έτσι ώστε ο σταθμός αναμετάδοσης να μη χάσει ποτέ την επαφή με τον δέκτη.



Σχήμα 5.3.2.δ. Δορυφορική ζεύξη
(Πηγή: http://www.eceway.com/2015/06/do-you-know-how-satellites-work.html#)

Ο επικοινωνιακός δορυφόρος λειτουργεί απλά σαν καθρέφτης που επανεκπέμπει προς τη γη το λαμβανόμενο μικροκυματικό σήμα. Κάθε γεωστατικός δορυφόρος καλύπτει έναν ορίζοντα 120 μοιρών έτσι που με τρεις τέτοιους δορυφόρους καλύπτεται όλη η γη.

Συγκρίνοντας τα δορυφορικά συστήματα με τα άλλα μέσα παρατηρούμε τα εξής:

- Οι δορυφόροι καλύπτουν με άνεση απαιτήσεις εκπομπής σημάτων ευρείας ζώνης συχνοτήτων.
- Έχουν μεγάλη καθυστέρηση σήματος της τάξης των 250 msec που οφείλεται στην μεγάλη απόσταση. Η καθυστέρηση αυτή είναι ενοχλητική τόσο στην τηλεφωνία όσο και στην μετάδοση δεδομένων.
- Δεν παρέχεται καμία ασφάλεια στην μεταδιδόμενη πληροφορία καθώς όλος ο κόσμος μπορεί να λάβει την πληροφορία που εκπέμπει ο δορυφόρος. Αυτός είναι και ο λόγος που χρησιμοποιούνται εξειδικευμένα συστήματα κρυπτογράφησης.
- Δεν παίζει κανένα ρόλο η μεταξύ των επικοινωνούντων ανταποκριτών απόσταση
- Το κόστος χρήσης είναι ανεξάρτητο της απόστασης επικοινωνίας.

Οι επικοινωνιακοί δορυφόροι χρησιμοποιούνται κυρίως για τηλεφωνία, τηλεόραση και μετάδοση δεδομένων.

Ερωτήσεις - Ασκήσεις Κεφαλαίου

1. Ποιοι είναι οι ρυθμοί μετάδοσης δεδομένων των επιλεγόμενων τηλεφωνικών γραμμών (PSTN);
2. Το modem χρησιμοποιείται μόνο σε επιλεγόμενες τηλεφωνικές γραμμές.
   α. Σωστό.
   β. Λάθος.
3. Το Διαδίκτυο είναι το μεγαλύτερο WAN του κόσμου. Περιγράψτε με δυο λόγια το ρόλο, που πιστεύετε, ότι έπαιξαν/παίζουν οι επιλεγόμενες και οι μισθωμένες τηλεφωνικές γραμμές στην ανάπτυξή του αυτή.
4. Οι γραμμές E1 είναι ..... μισθωμένες γραμμές με ταχύτητα ..... , που χρησιμοποιούνται στην Ευρώπη.
5. Ποιες είναι οι βασικές χρήσεις των μισθωμένων γραμμών;
6. Ποιες είναι οι ιδιότητες ενός δικτύου ISDN;
7. Ποιοι είναι οι τύποι πρόσβασης στο δίκτυο ISDN;
8. Η τεχνολογία ISDN είναι ασύμφορη από την άποψη του κόστους, όταν απαιτείται συνεχής μεταφορά μεγάλου όγκου δεδομένων.
   α. Σωστό.
   β. Λάθος.
9. Τι είναι η τεχνολογία DSL;
10. Οι διάφορες παραλλαγές xDSL υποστηρίζουν ..... ή ..... μετάδοση δεδομένων.
11. Ποιο είναι το κύριο χαρακτηριστικό της τεχνολογίας ADSL;
12. Ποια η διαφορά των τεχνολογιών HDSL και SDSL;
13. Ποια είδη ADSL modems υπάρχουν;
14. Τι είναι το DSLAM;
15. Η διαδικασία σύνδεσης μεταξύ του modem/router και του port του DSLAM ονομάζεται ..... .
16. Περιγράψτε τις δύο βασικές κατηγορίες συνδεσμολογίας ADSL.
17. Σε ένα δίκτυο ADSL που χρησιμοποιεί γραμμή σύνδεσης ISDN, είναι απαραίτητη και η χρήση της συσκευής τερματισμού δικτύου (netmode).
   α. Σωστό.
   β. Λάθος.
18. Υπολογίστε πόσα μιλιβάτ (mW) είναι τα 24dBm. Χρησιμοποιήστε είτε τη σχέση είτε τις αντιστοιχίες ενός πίνακα μετατροπής dBm <--> mW. Περιγράψτε τον τρόπο που εργαστήκατε.
19. Για τις παρακάτω προτάσεις σημειώστε ποιες είναι σωστές και ποιες λάθος.
    - Μια τιμή μεγαλύτερη κατά 3dB σημαίνει 10 φορές μεγαλύτερο μέγεθος.
    - Σήμα στάθμης 0dBm σημαίνει μηδενικό (ανύπαρκτο) σήμα.
    - Ένα σήμα Α είναι -10 dBm. Ενα σήμα Β είναι +10 dBm. Αυτό σημαίνει ότι το σήμα Β είναι εκατό φορές μεγαλύτερο από το Α.
    - Ένα σήμα Α είναι 24 dBm. Ενα σήμα Β είναι 21 dBm. Αυτό σημαίνει ότι το σήμα Β είναι το μισό του Α.
    - Ένα σήμα Α είναι 0 dBm. Ενα σήμα Β είναι 6 dBm. Αυτό σημαίνει ότι το σήμα Β είναι το διπλάσιο του Α.
20. Ένα σήμα ισχύος 1 βατ (W) έχει θόρυβο 1 μιλιβάτ (mW). Ποιος είναι ο λόγος σήματος προς θόρυβο;
21. Τι είναι η παραδιαφωνία;
22. Αναφέρετε τρία είδη παραμορφώσεων που μπορεί να υποστεί ένα σήμα ταξιδεύοντας σε μια επικοινωνιακή γραμμή και περιγράψτε μια από αυτές.
23. Τι είναι ο κρουστικός θόρυβος;

24. Περιγράψτε ένα παθητικό οπτικό δίκτυο FTTH σημείου προς σημεία. Ποια είναι τα δομικά στοιχεία που χρησιμοποιεί;
25. Πώς μπορεί μέσα από μια οπτική ίνα να περάσει ταυτόχρονα ανερχόμενη (upstream) και κατερχόμενη (downstream) δικτυακή κίνηση;
26. Τι ταχύτητες μπορεί να υποστηρίξει ένα XG.PON/10 με παθητικό διαχωριστή 1:32 στους τελικούς χρήστες; Αιτιολογήστε την απάντησή σας.
27. Περιγράψτε δυο περιπτώσεις στις οποίες, για την επέκταση ενός δικτύου, καταφεύγουμε σε λύση ασύρματης ζεύξης.
28. Σε μια ασύρματη ζεύξη, ο πομπός εκπέμπει σήμα στάθμης 20dBm, το κατώφλι ευαισθησίας του δέκτη είναι -85dBm και οι συνολικές απώλειες καλωδίων, συνδετήρων και διαδρομής του σήματος -120dB. Πόσο πρέπει να είναι το κέρδος των κεραιών (συνολικά), ώστε να έχουμε περιθώριο λειτουργίας 20dB;
29. Υπολογίστε την ακτίνα της πρώτης ζώνης Fresnel σε μια ζεύξη ενός χιλιομέτρου, στους 2,4 GHz σε απόσταση 30m από το ένα άκρο. Επαναλάβετέ το για το μέσον της ζεύξης.
30. Τι είναι τα δορυφορικά δίκτυα και ποιος ο στόχος τους;
31. Ποιος ο ρόλος των δορυφορικών δικτύων;
32. Αντιστοιχίστε τη σωστή ορολογία:
    1. Επίγειος σταθμός χρήστη. A. GES.
    2. Επίγειος σταθμός πύλης. B. UES .
33. Ποιοι είναι οι δύο πιο σημαντικοί πόροι για την παροχή πληροφοριών πάνω από τα δορυφορικά δίκτυα;
34. Το εύρος ζώνης και η ισχύς μετάδοσης, μαζί με τις συνθήκες μετάδοσης και το περιβάλλον, καθορίζουν τη ..... των δορυφορικών δικτύων.
35. Ποιες είναι οι διαφορές των δορυφορικών συστημάτων με τα άλλα συστήματα;

Δραστηριότητες (συνδυαστικά στην αίθουσα, το εργαστήριο ή και το σπίτι)

1. Προσπαθήστε να σχεδιάσετε τη συνδεσμολογία οικιακού δικτύου ADSL σε γραμμή PSTN και κατόπιν σε γραμμή ISDN, με περισσότερες από μία πρίζες τηλεφώνου και δικτύου, χρησιμοποιώντας splitter και filters όπου χρειάζονται.
2. Αναζητήστε και συγκεντρώστε φυλλάδια χαρακτηριστικών (datasheets), σε ηλεκτρονική μορφή, για τα παρακάτω είδη εξοπλισμού.
    - Ασύρματο Σημείο Πρόσβασης (Access Point - AP) για εξωτερικό χώρο με δυνατότητα γεφύρωσης (point to point bridge ή WDS PTP) και λειτουργία στους 5GHz
    - Κατευθυντικές κεραίες τύπου πλέγματος, (grid) για τους 5GHz, με απολαβή/κέρδος καλύτερο από 18dBi
    - Συνδετήρες (connectors) τύπου N
    - Ομοαξονικό καλώδιο διαμέτρου τουλάχιστον 10mm χαμηλών απωλειών

    Εντοπίστε στο χάρτη δυο σημεία που απέχουν λιγότερο από 5 χιλιόμετρα μεταξύ τους και εκτιμάτε ότι έχουν οπτική επαφή. Χρησιμοποιήστε χάρτες Google, GoogleEarth ή οποιαδήποτε άλλη χαρτογραφική εφαρμογή γνωρίζετε και σημειώστε την ακριβή θέση και απόστασή τους.

    Στη συνέχεια, χρησιμοποιώντας ένα AP, δυο συνδετήρες N, 6m καλώδιο και μια κεραία για κάθε μια από τις δυο τοποθεσίες, κάντε τον προϋπολογισμό της ζεύξης.

    Επισκεφθείτε τη σελίδα “Radio Mobile” http://www.cplus.org/rmw/rmonline.html, δημιουργήστε έναν δωρεάν λογαριασμό και εξοικειωθείτε με τη χρήση του site. Εναλλακτικά επισκεφθείτε τη σελίδα http://www.qsl.net/n9zia/ και αναζητήστε στην ενότητα Interactive Wireless/RF Design Utilities εργαλεία για Wireless Network Link Analysis, Line of Sight Path Analysis ή Fresnel Zone Calculator.

Εισάγετε τα στοιχεία της ζεύξης σας και συγκρίνετε τα αποτελέσματα με τον δικό σας προϋπολογισμό. Αν χρειαστείτε οποιεσδήποτε μετατροπές μεγεθών αναζητήστε και χρησιμοποιήστε τους κατάλληλους πίνακες ή online calculators στο Διαδίκτυο. Συζητήστε για τους τρόπους που εργαστήκατε και τα αποτελέσματά σας.

3. Ελάτε σε επαφή με τοπικό ή κοντινό σύλλογο ραδιοερασιτεχνών και συζητήστε ή ζητήστε να σας κάνουν μια παρουσίαση για τη διάδοση των ραδιοκυμάτων. Ενδεχομένως μπορείτε να το εντάξετε στα πλαίσια κάποιου άλλου σχολικού προγράμματος ή μιας εκπαιδευτικής επίσκεψης.
4. Επιχείρηση που βρίσκεται στην Αθήνα θέλει να συνδεθεί με το υποκατάστημα της στη Θεσσαλονίκη με ταχύτητα 2 Mbps. Προσπαθήστε να καταλήξετε στη βέλτιστη λύση διασύνδεσης, λαμβάνοντας υπόψη το τηλεπικοινωνιακό κόστος που απαιτείται και τις τεχνικές απαιτήσεις.

Βιβλιογραφία

Αλεξόπουλος, Α., & Λαγογιάννης, Γ. (2012). *Τηλεπικοινωνίες και δίκτυα υπολογιστών,* (8η έκδ.). Αθήνα.

Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). *Τεχνολογία Δικτύων Επικοινωνιών* (1η έκδ.). Αθήνα: ΟΕΔΒ.

Τηλεπικοινωνιακό κέντρο Α.Π.Θ.: w*ww.tcom.auth.gr/.../**technologies/technologies**.html*

Bertoni, H. L. (2008). *Διάδοση ραδιοκυμάτων στα συστήματα ασύρματης επικοινωνίας*. Αθήνα: Κλειδάριθμος.

Butler, J., Pietrosemoli, E., & Zennaro, M. (2013). *Wireless Networking in the Developing World* (3rd ed.). http://wndw.net/.

Flickenger, R., Aichele, C. "Elektra," & Büttrich, S. (2007). *Wireless Networking in the Developing World, A practical guide to planning and building low-cost telecommunications infrastructure*

Fresnel zone. (2015, 25 Αυγούστου). In *Wikipedia, the free encyclopedia*. Ανακτημένο από https://en.wikipedia.org/w/index.php?title=Fresnel_zone&oldid=677715726

FTTH - Definition of Terms. (2015). FTTH Council Global Alliance - FCGA.

Gast, M. S. (2002). 802.11 Wireless Networks, The Definitive Guide. Sebastopol, CA USA: O'Reilly & Associates.

GEPON OLT, ONU, ODN in FTTH application. (χ.χ.), Ανακτημένο από http://www.fiberoptictel.com/gepon-olt-onu-odn-in-ftth-application/

PISCES., (2015, 26 Αυγούστου), Ανακτημένο από http://www.piscespacific.org/livesite/pages/guamsessions

Radio Mobile Online., (2015, 26 Αυγούστου), Ανακτημένο από http://www.cplus.org/rmw/rmonline.html

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks* (5th ed.). Prentice Hall Pearson.

Zhao, R., Ahl, K., & Bygrave, J. (2014). *FTTH Handbook*. FTTH Council Europe.

Zhili Sun, (2014), "*Satellite networking principles and protocols*", second edition, University of Surrey, UK

Κεφάλαιο 6ο

ΕΠΙΠΕΔΟ ΕΦΑΡΜΟΓΗΣ

Εισαγωγή

Το Επίπεδο Εφαρμογής (Application Layer) είναι το πιο πάνω επίπεδο των τεσσάρων επιπέδων του μοντέλου TCP/IP και βρίσκεται πάνω από το επίπεδο Μεταφοράς (Transport Layer). Το επίπεδο εφαρμογής ορίζει τα TCP/IP πρωτόκολλα εφαρμογής και το πώς τα προγράμματα του χρήστη επικοινωνούν με τις υπηρεσίες του επιπέδου μεταφοράς για να χρησιμοποιούν το δίκτυο. Το επίπεδο εφαρμογής περιλαμβάνει όλα τα πρωτόκολλα υψηλότερου επιπέδου, όπως το DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (Πρωτόκολλο Μεταφοράς Αρχείων), TFTP (Απλό πρωτόκολλο μεταφοράς αρχείων), SNMP (Απλό Πρωτόκολλο Διαχείρισης Δικτύου), SMTP (Απλό Πρωτόκολλο Μεταφοράς Ταχυδρομείου), DHCP (Dynamic Host Configuration Protocol), RDP (Remote Desktop Protocol) κ.λπ. Στη συνέχεια θα γνωρίσουμε μερικές από τις υπηρεσίες του Διαδικτύου που βασίζονται στα παραπάνω πρωτόκολλα.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 6ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- περιγράφουν το μοντέλο Πελάτη - Εξυπηρετητή (Client -Server) λειτουργίας των βασικών υπηρεσιών του επιπέδου εφαρμογής, όπως WEB, EMAIL, FTP, TELNET
- περιγράφουν τον τρόπο λειτουργίας και να κάνουν χρήση των βασικών υπηρεσιών και εφαρμογών Διαδικτύου

Διδακτικές Ενότητες

6.1 Σύστημα Ονοματολογίας DNS.
6.2 Υπηρεσίες Διαδικτύου.

6.1 Σύστημα Ονοματολογίας DNS

Όπως έχει ήδη αναφερθεί, κάθε υπολογιστής (host) που συμμετέχει σε ένα δίκτυο τεχνολογίας TCP/IP αποκτά μία και μοναδική διεύθυνση IP (π.χ. 128.174.5.50). Οι διευθύνσεις IP προσδιορίζουν διεπαφές υπολογιστών ή δρομολογητών και κάθε διεύθυνση IP περιέχει πληροφορία που χρησιμοποιείται για τη δρομολόγηση των πακέτων IP. Επειδή όμως οι χρήστες βρίσκουν αρκετά δύσκολο να θυμούνται διευθύνσεις αυτής της μορφής, χρησιμοποιούν συμβολικά ονόματα, με τα οποία αναφέρονται στις συσκευές και στα δίκτυα.

Για παράδειγμα, σε ένα TCP/IP δίκτυο αποτελούμενο από τέσσερις υπολογιστές, η αντιστοιχία IP διευθύνσεων και συμβολικών ονομάτων θα μπορούσε να είναι η εξής:

IP διεύθυνση	Όνομα υπολογιστή
128.174.5.1	atlas
128.174.5.2	kronos
128.174.5.3	aris

Προκειμένου να επικοινωνήσουμε με μία από τις συσκευές αυτές, είναι απαραίτητο να γνωρίζουμε την IP διεύθυνσή της. Αντί λοιπόν να πρέπει να θυμόμαστε τις διευθύνσεις αυτές, είναι σύνηθες να χρησιμοποιούμε τα συμβολικά τους ονόματα. Όπως είναι λογικό,

αυτή η προσέγγιση (διευθύνσεις-ονόματα) δουλεύει καλά σε μικρά δίκτυα με περιορισμένο αριθμό συσκευών.

Όταν όμως έχουμε συναλλαγές με το Διαδίκτυο (Internet), είναι προφανές ότι είναι δύσκολο να μπορούμε να απομνημονεύσουμε διευθύνσεις IP (έτσι ώστε να ξέρουμε π.χ τη διεύθυνση της κεντρικού εξυπηρετητή (server) του Πανεπιστημίου Πατρών). Γι' αυτό το λόγο έχει αναπτυχθεί ένα σύστημα ονοματοδοσίας των υπολογιστών του Διαδικτύου και μια υπηρεσία καταλόγου για αναζήτηση των ονομάτων. Η υπηρεσία αυτή ονομάζεται DNS (Domain Name Service – Υπηρεσία Ονομασίας Περιοχών).

Το σύστημα ονομασίας περιοχών (DNS) είναι μια κατανεμημένη βάση δεδομένων στο Διαδίκτυο που επιτρέπει τη μετάφραση ανάμεσα σε ονόματα και διευθύνσεις IP. Θα μπορούσαμε να πούμε ότι το DNS είναι ο «τηλεφωνικός κατάλογος του Διαδικτύου». Είναι ο μηχανισμός του Διαδικτύου για την αναφορά μέσω ονομάτων σε ό,τι πόρους χρησιμοποιούμε σε αυτό και που μας επιτρέπει τη μετάφραση ονομάτων σε διευθύνσεις IP και το αντίστροφο.

Πρόκειται για μία κατανεμημένη βάση δεδομένων που εφαρμόζεται σε μια ιεραρχία πολλών εξυπηρετητών ονομάτων (DNS servers).

Περιλαμβάνει:

- το χώρο ονομάτων
- τους εξυπηρετητές μέσω των οποίων γίνεται διαθέσιμος ο χώρος ονομάτων
- τους αναλυτές (resolvers) που ερωτούν τους εξυπηρετητές περί του χώρου ονομάτων

Τα δεδομένα της βάσης DNS διατηρούνται τοπικά, αλλά είναι διαθέσιμα παγκόσμια. Δεν υπάρχει υπολογιστής με όλη τη βάση DNS.

Το **πρωτόκολλο DNS** είναι **επιπέδου εφαρμογής** (Application Layer) που επιτρέπει σε υπολογιστές (hosts), δρομολογητές (routers) και εξυπηρετητές DNS (Name Servers) να επικοινωνούν για να αναλύσουν (resolve) ονόματα (μεταφράσουν ονόματα σε διεύθυνση IP). Είναι βασική λειτουργία του κορμού του Διαδικτύου, όπου οι αναζητήσεις DNS γίνονται από οποιοδήποτε μηχάνημα και οποιαδήποτε υπηρεσία. Τα αποτελέσματα από μακρινούς εξυπηρετητές ονομάτων αποθηκεύονται προσωρινά σε τοπική μνήμη ώστε να βελτιωθεί η επίδοση.

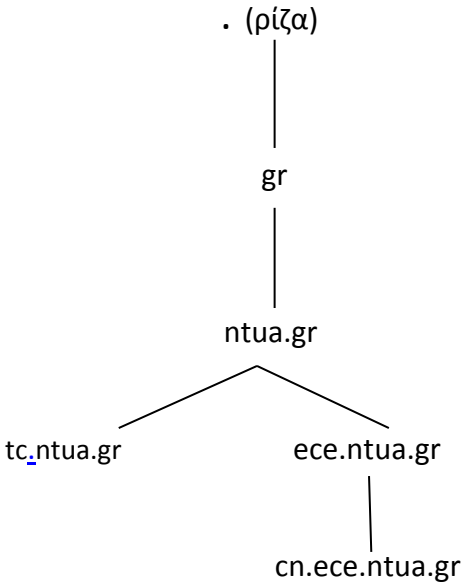
6.1.1 Χώρος ονομάτων του DNS

Το Διαδίκτυο είναι χωρισμένο νοητά σε εκατοντάδες διαφορετικές περιοχές (domains) υψηλού επιπέδου που αναλύονται σε υποπεριοχές (subdomains), κ.ο.κ., με πολλούς υπολογιστές (hosts) η καθεμία.

Οι περιοχές μπορεί να παρασταθούν με ένα δέντρο. Τα ονόματα των περιοχών απαρτίζουν μια ιεραρχία κατά τρόπο που τα ονόματα να είναι μοναδικά και να απομνημονεύονται εύκολα. Ένας οργανισμός είναι αρμόδιος για μέρος του χώρου ονομάτων και μπορεί να προσθέσει επιπλέον επίπεδα στην ιεραρχία.

Ιεραρχία του DNS. Κάθε κόμβος στο δένδρο DNS αναπαριστά ένα όνομα DNS (DNS name). Κάθε κλαδί κάτω από ένα κόμβο είναι μια περιοχή DNS (DNS domain). Η περιοχή DNS μπορεί να περιέχει hosts ή άλλες περιοχές (subdomains).

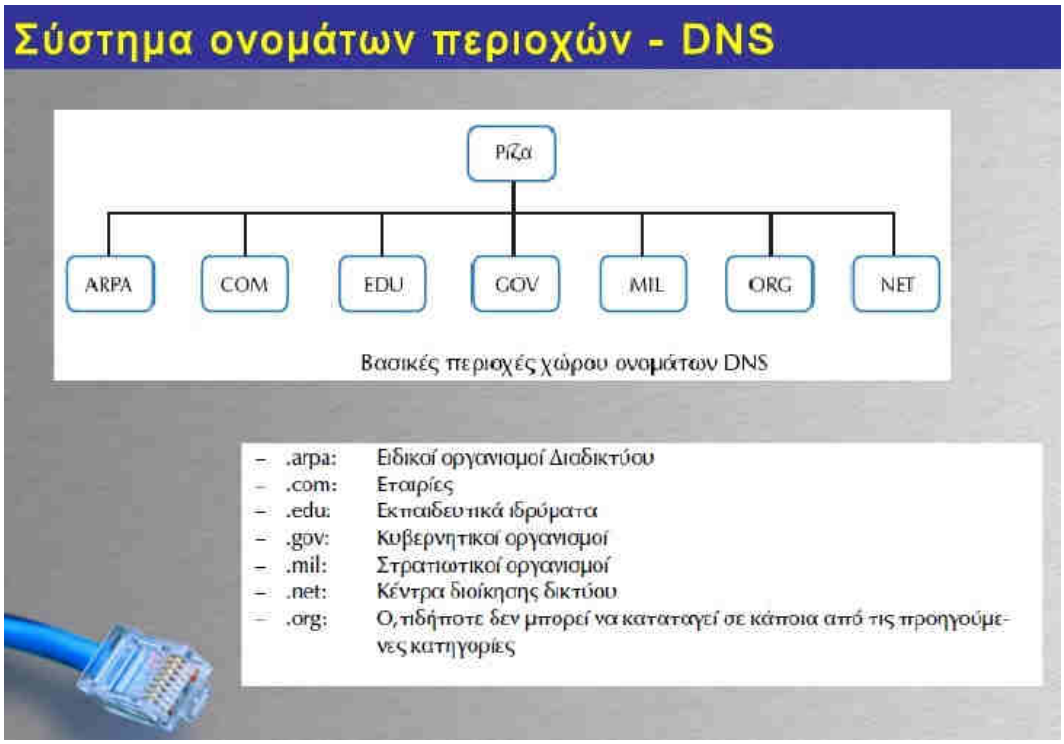
Παράδειγμα περιοχών DNS:.



Η κορυφή του δένδρου είναι η ρίζα (root) και συμβολίζεται με μία τελεία «.». Η IANA (Internet Assigned Numbers Authority) είναι η επίσημη αρχή που διαχειρίζεται τη ρίζα του DNS.

Κάτω από την κορυφή υπάρχουν οι **περιοχές ανωτάτου επιπέδου** (top level domains ή περιοχές 1ου επιπέδου ή βασικές περιοχές). Αρχικά (1988) υπήρχαν:

edu, gov, com, org, mil, net, int, arpa



Εικόνα 6.1.1.α: Περιοχές 1ου επιπέδου χώρου ονομάτων DNS

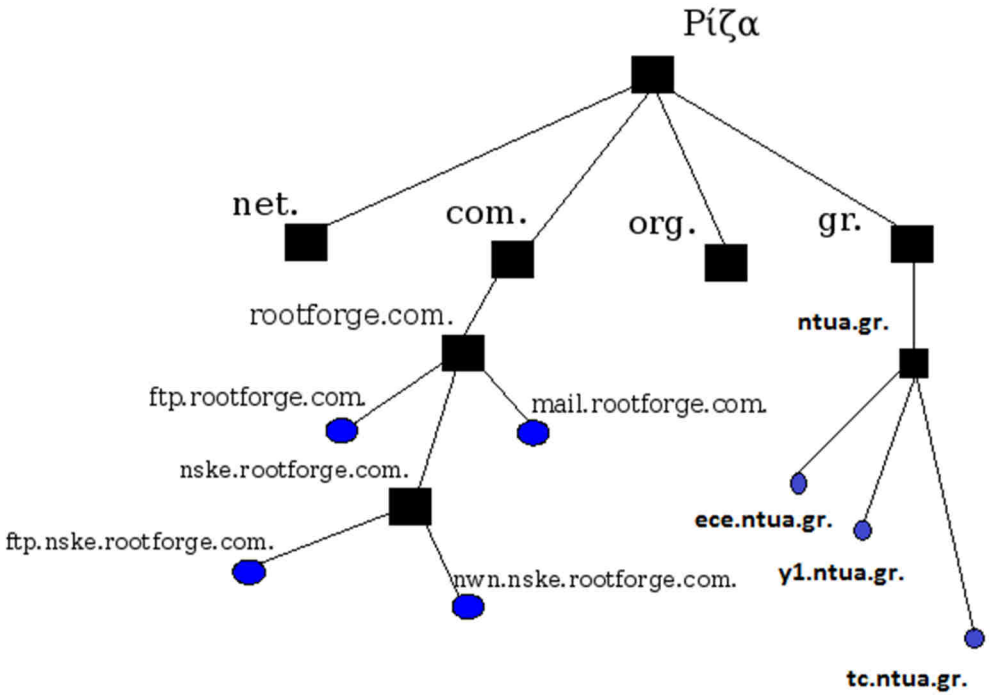
(Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών)

Αργότερα, προστέθηκαν περιοχές για κάθε χώρα (όνομα περιοχής με 2 γράμματα), όπως:

gr, nl, uk, us, jp, it, fr κ.ά.

Στη συνέχεια εγκρίθηκαν αρκετές νέες περιοχές (π.χ. biz, info, post, tel κ.ά.). Η διαχείριση τους (εκτός των .int και .arpa) έχει εκχωρηθεί από την IANA σε άλλους υπεύθυνους οργανισμούς.

Κάτω από κάθε περιοχή 1ου επιπέδου, υπάρχει δεύτερο επίπεδο περιοχών, που προσδιορίζει συνήθως τον οργανισμό ή την εταιρεία στην οποία ανήκει το δίκτυο. Οι περιοχές αυτές (**domains**) ονομάζονται **περιοχές 2ου επιπέδου** και κάθε μία είναι μοναδική. Η διαχείριση του χώρου ονομάτων κάτω από τις περιοχές ανωτάτου επιπέδου έχει εκχωρηθεί σε οργανισμούς, που μπορούν να εκχωρήσουν περαιτέρω τη διαχείριση υποπεριοχών τους (subdomains). Κάθε νέο subdomain αντιστοιχεί σε **περιοχή ονομάτων 3ου επιπέδου**.



Σχήμα 6.1.1.β: Ιεραρχική οργάνωση χώρου ονομάτων DNS

(Προσαρμογή από πηγή: http://computergiaolous.blogspot.gr/2012/12/dns-domain-name-system.html)

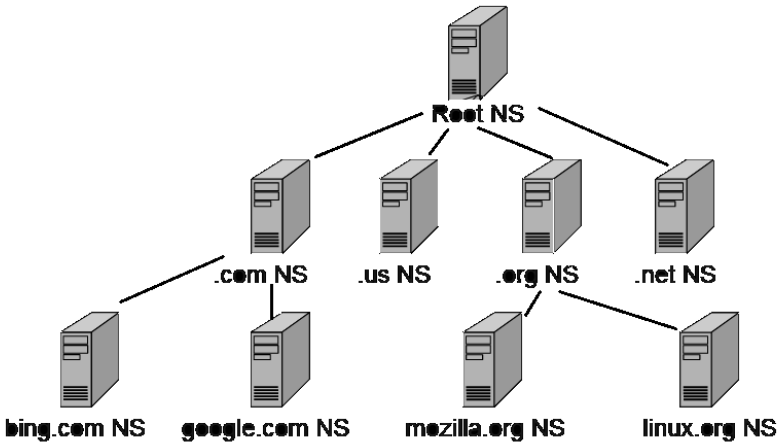
Παράδειγμα: Το όνομα ektor.tc.ntua.gr, προσδιορίζει τον ηλεκτρονικό υπολογιστή (host) με το συμβολικό όνομα “ektor”, που βρίσκεται στην υποπεριοχή (subdomain) “tc” (3ου επιπέδου) που δηλώνει τα μηχανήματα του εργαστηρίου τηλεπικοινωνιών, η οποία ανήκει στη περιοχή (domain) “ntua” (2ου επιπέδου) του Εθνικού Μετσόβιου Πολυτεχνείου και η οποία έχει καταχωρηθεί στη βασική περιοχή (1ου επιπέδου) “.gr”(1ου επιπέδου) που αφορά την Ελλάδα.

6.1.2 Οργάνωση DNS

Το DNS είναι οργανωμένο ως μία κατανεμημένη βάση δεδομένων που χρησιμοποιεί το μοντέλο πελάτη – εξυπηρετητή. Για να λειτουργήσει το DNS χρησιμοποιεί τους κόμβους της βάσης αυτής που είναι οι εξυπηρετητές ονομάτων (Name Servers), οι οποίοι βρίσκονται σε διαφορετικά σημεία του Διαδικτύου, συνεργάζονται μεταξύ τους και μας πληροφορούν σχετικά με το ποιο όνομα αντιστοιχεί σε ποια IP διεύθυνση και αντίστροφα.

Ιεραρχία των εξυπηρετητών ονομάτων

Η ιεραρχία του χώρου ονομάτων ανταποκρίνεται σε μία αντίστοιχη ιεραρχία εξυπηρετητών ονομάτων.



Σχήμα 6.1.2.α: Ιεραρχία των εξυπηρετητών ονομάτων (Name Servers)
(Πηγή: https://www.ssucet.org/~jhudson/14/etec3201/07-dns/)

Κάθε εξυπηρετητής είναι υπεύθυνος για ένα συμπαγές τμήμα του χώρου ονομάτων DNS που αποκαλείται **ζώνη (zone).** Ο εξυπηρετητής ονομάτων απαντά σε ερωτήσεις (queries) για τους υπολογιστές (hosts) της ζώνης του. Κάθε ζώνη είναι εμφωλευμένη σε ένα κόμβο του δένδρου. Οι ζώνες δεν είναι περιοχές (domains). Η ζώνη είναι τμήμα του χώρου ονομάτων DNS που εν γένει αποθηκεύεται σε ένα αρχείο. Ο εξυπηρετητής ονομάτων μπορεί να χωρίσει μέρος της ζώνης του και να το εκχωρήσει σε άλλους εξυπηρετητές.

Σχήμα 6.1.2.β: Οργάνωση δικτύου σε ζώνες

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Κανένας εξυπηρετητής DNS δεν έχει όλες τις αντιστοιχίες ονομάτων σε διευθύνσεις IP. Για να βρεθεί μία συγκεκριμένη αντιστοίχιση πιθανόν να πρέπει να γίνουν ερωτήσεις σε πολλούς εξυπηρετητές DNS.

Για κάθε ζώνη πρέπει να υπάρχει ένας κύριος εξυπηρετητής και ένας αριθμός από δευτερεύοντες εξυπηρετητές. Ο κύριος εξυπηρετητής (primary server) διατηρεί ένα αρχείο ζώνης με την πρωτότυπη πληροφορία για τη ζώνη. Ο δευτερεύων εξυπηρετητής (secondary server) διατηρεί αντίγραφα των δεδομένων που αποθηκεύονται στον κύριο εξυπηρετητή.

Η βάση μπορεί να ενημερωθεί δυναμικά με προσθήκη, διαγραφή, τροποποίηση οποιασδήποτε πληροφορίας. Όταν προστίθεται ένας host σε μια ζώνη, ο διαχειριστής προσθέτει την πληροφορία για τον host (διεύθυνση IP και όνομα) σε ένα αρχείο του κύριου εξυπηρετητή.

Σχεδόν κάθε οργανισμός, εταιρεία, πανεπιστήμιο, πάροχος έχει έναν τοπικό εξυπηρετητή ονομάτων, που είναι γνωστός και ως ο επιλεγμένος (default) εξυπηρετητής. Όταν γίνει μια ερώτηση, αυτή αποστέλλεται στον τοπικό εξυπηρετητή, που λειτουργεί ως ενδιάμεσος και προωθεί την ερώτηση, εάν απαιτείται. Αν ο τοπικός εξυπηρετητής ονομάτων δεν έχει καταλήξει στο πού θα βρει τη διεύθυνση που αντιστοιχεί στο όνομα κάποιου υπολογιστή, ρωτά τους εξυπηρετητές άλλων ζωνών, φτάνοντας μέχρι τους εξυπηρετητές ρίζας, αν χρειαστεί.

Πρωτόκολλο DNS. Το πρωτόκολλο DNS είναι του τύπου πελάτη – εξυπηρετητή και ανήκει στο επίπεδο εφαρμογής του μοντέλου TCP/IP. Ο πελάτης DNS ονομάζεται αναλυτής (resolver). Το πρωτόκολλο DNS υποστηρίζει τη μετατροπή ονομάτων σε διευθύνσεις (ανάλυση, resolution), καθώς και την ενημέρωση των δεδομένων μεταξύ των εξυπηρετητών ονομάτων.

Ανάλυση ονομάτων (name resolution) είναι η διαδικασία με την οποία αναλυτές και εξυπηρετητές ονομάτων συνεργάζονται ώστε να βρουν δεδομένα εντός του χώρου ονομάτων. Για την ανεύρεση δεδομένων, ο εξυπηρετητής ονομάτων χρειάζεται μόνο το όνομα και τη διεύθυνση IP των εξυπηρετητών ονομάτων κορυφής (ρίζας). Οι εξυπηρετητές κορυφής γνωρίζουν όλες τις περιοχές ανωτάτου επιπέδου και μπορούν να υποδείξουν τους εξυπηρετητές με τους οποίους μπορεί να γίνει επαφή.

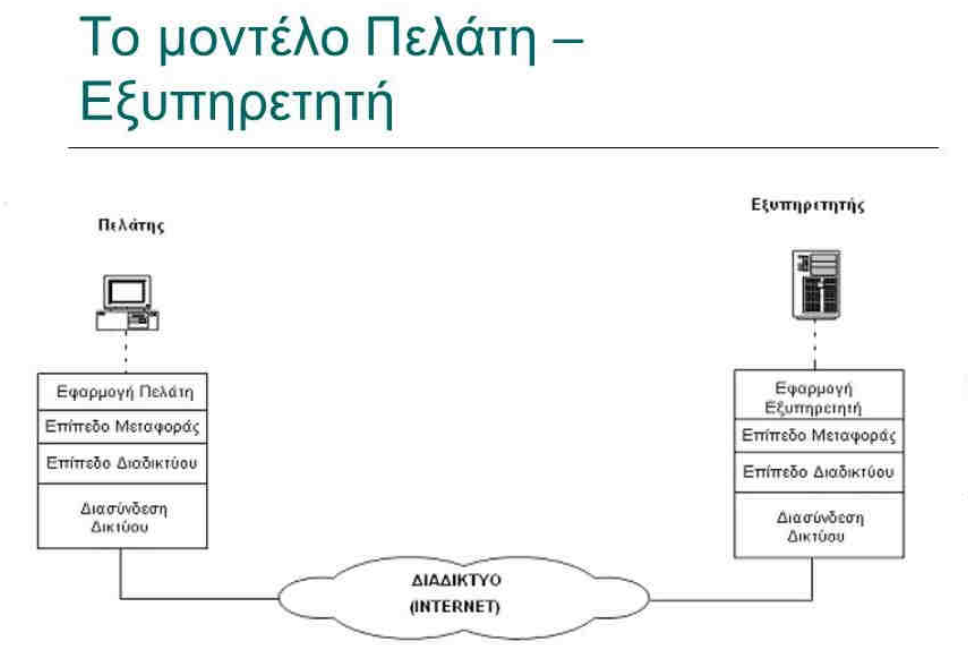
6.2 Υπηρεσίες Διαδικτύου

Όλες οι υπηρεσίες στο Διαδίκτυο, όπως και πολλές εφαρμογές λογισμικού, στηρίζονται στο μοντέλο **Πελάτη – Εξυπηρετητή**. Σύμφωνα με αυτό το μοντέλο ο Εξυπηρετητής οργανώνει, διαχειρίζεται το αρχείο δεδομένων, δέχεται ερωτήματα και απαντά στο πρόγραμμα Πελάτης. Από την άλλη πλευρά το πρόγραμμα Πελάτης θέτει ερωτήματα στον Εξυπηρετητή και μπορεί να αποκωδικοποιεί τις απαντήσεις του Εξυπηρετητή.

Το μοντέλο αυτό υλοποιείται με δύο ανεξάρτητα κομμάτια **λογισμικού**:

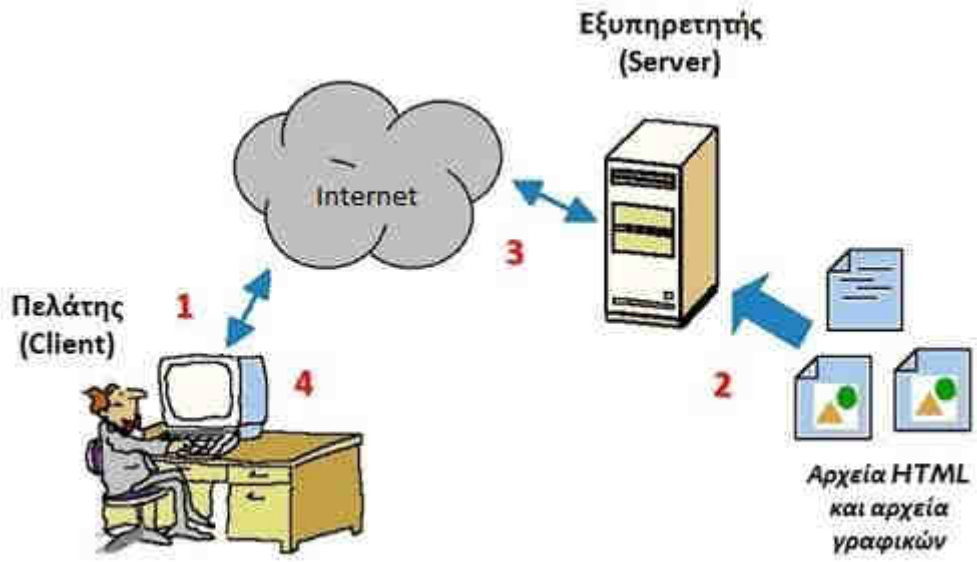
- Το πρόγραμμα του **Εξυπηρετητή (Server)** που εγκαθίσταται σε έναν (ή περισσότερους) υπολογιστή
- Το πρόγραμμα του **Πελάτη (Client)** που εγκαθίσταται σε πολλούς υπολογιστές

Ο Server διαχειρίζεται τα δεδομένα, λαμβάνει ερωτήσεις από τους Clients και απαντά στα ερωτήματά τους. Ο Client κάνει ερωτήσεις στον Server και εμφανίζει τις απαντήσεις των ερωτημάτων.



Σχήμα 6.2.α:. Το μοντέλο Πελάτη-Εξυπηρετητή σύμφωνα με το μοντέλο TCP/IP

(Πηγή: http://images.slideplayer.gr/7/1959162/slides/slide_34.jpg)



Σχήμα 6.2.β: Το μοντέλο Πελάτη-Εξυπηρετητή στην υπηρεσία WWW (Παγκόσμιου Ιστού)

(Πηγή:http://ebooks.edu.gr/modules/ebook/show.php/DSB101/535/3534,14522/extras/presentations/Kef1_4_client_server_model/swf/engage_content/image1.jpg)

6.2.1 Υπηρεσία ηλεκτρονικού ταχυδρομείου E-mail (POP3 - IMAP/SMTP)

Το ηλεκτρονικό ταχυδρομείο είναι ένα σύστημα για τη μετάδοση μηνυμάτων μεταξύ υπολογιστών. Τα μηνύματα μπορούν να περιέχουν πληροφορίες σε διάφορες μορφές. Μια ηλεκτρονική επιστολή έχει τη δυνατότητα να περιλαμβάνει, εκτός από κείμενο, εικόνες, ήχους, κινούμενες εικόνες, video, μια εφαρμογή, μέσα στο μήνυμα ή ως επισυναπτόμενα αρχεία. Ο χρήστης e-mail, μπορεί να στέλνει μηνύματα σ' άλλους χρήστες e-mail μέσω υπολογιστή, άνετα, γρήγορα και φθηνά. Παρέχει επίσης έναν αποτελεσματικό μηχανισμό για τη μετάδοση της πληροφορίας σε έναν ή πολλούς ανθρώπους (mailing lists) ταυτόχρονα. Παρόμοια με το συμβατικό ταχυδρομείο ο κάθε χρήστης έχει τη δική του διεύθυνση η οποία είναι της μορφής **xxxxx@yyyyy.zzz** όπου «xxxxx» συνήθως αποτελεί το όνομα ή κάποιο ψευδώνυμο του χρήστη, «yyyyy» είναι το όνομα της περιοχής (domain name) κάποιας εταιρείας που παρέχει τις υπηρεσίες του ηλεκτρονικού ταχυδρομείου και μπορεί να είναι ενός ή πολλών επιπέδων χωρισμένα με τελείες και «zzz» όπου αναφέρεται στο είδος της εταιρείας που εκτελεί χρέη ταχυδρομείου (π.χ .org, .com, .edu κ.λπ.) ή τη χώρα προέλευσης (π.χ .gr, .de, .au κ.λπ.). Δίνονται παραδείγματα διευθύνσεων ηλεκτρονικού ταχυδρομείου: **kostas@hotmail.com**, **g.papadopoulos@sch.gr, info@teiath.edu.gr**.

Στο Διαδίκτυο τα περισσότερα συστήματα ηλεκτρονικού ταχυδρομείου χρησιμοποιούν το μοντέλο πελάτη-εξυπηρετητή (client-server).

- **Πελάτης (client):**
  - Ξεκινάει την επαφή με τον εξυπηρετητή (διακομιστή) («μιλάει πρώτος»).
  - Ζητά εξυπηρέτηση από τον εξυπηρετητή.
  - Στο ηλεκτρονικό ταχυδρομείο ο πελάτης (client) είναι το πρόγραμμα που χρησιμοποιεί ο χρήστης. Το πρόγραμμα αυτό είναι υπεύθυνο για την ανάγνωση και δημιουργία του ηλεκτρονικού μηνύματος (π.χ. Outlook, Windows Live mail, Mozilla Thunderbird κ.ά.).
- **Εξυπηρετητής (server):**
  - Παρέχει στον πελάτη την εξυπηρέτηση που ζήτησε. Στο ηλεκτρονικό ταχυδρομείο ο εξυπηρετητής στέλνει το ηλεκτρονικό μήνυμα.
  - Κρατά στην ηλεκτρονική θυρίδα (mailbox) τα μηνύματα που πρόκειται να σταλούν στο χρήστη. Σε μια άλλη ουρά τα μηνύματα που πρόκειται να σταλούν από τον χρήστη.

Πλεονεκτήματα:

- Είναι πολύ γρήγορο.
- Ο χρήστης δεν χρειάζεται να παρακολουθεί τη μεταφορά του μηνύματος μέσω του ταχυδρομείου, όπως με την αποστολή fax.
- Είναι πιο οικονομικό από το συμβατικό ταχυδρομείο.
- Μπορεί να προσδιοριστεί μεγάλος αριθμός ταυτόχρονων αποδεκτών.

Μειονεκτήματα:

- Δεν υπάρχει απόλυτη εγγύηση ότι το μήνυμα έφτασε στον προορισμό του.

Υπάρχει διεθνές πρότυπο που καθορίζει τη μορφή των μηνυμάτων ηλεκτρονικού ταχυδρομείου με μορφή κειμένου. Ένα τέτοιο **μήνυμα** αποτελείται από:

- την **Επικεφαλίδα (header)**, που είναι ένα σύνολο γραμμών όπου κάθε γραμμή αποτελείται από μια λέξη-κλειδί, άνω και κάτω τελεία, κενό, και μία τιμή. Για παράδειγμα ένα αρχικό μέρος ενός μηνύματος ηλεκτρονικού ταχυδρομείου είναι:

- From: nick@aueb.gr
  To: john@cs.co.uk
  Reply-To: nick@aueb.gr
  Subject: Hello

- το **σώμα του μηνύματος** που περιέχει ASCII κείμενο. Ακολουθεί το αρχικό μέρος και διαχωρίζεται από αυτό με μια κενή γραμμή.

SMTP, POP3 και **IMAP** είναι πρωτόκολλα TCP/IP που χρησιμοποιούνται για την παράδοση και παραλαβή της αλληλογραφίας. Αν πρόκειται να δημιουργηθεί ένας διακομιστής ηλεκτρονικού ταχυδρομείου (Mail Server), ο διαχειριστής πρέπει να γνωρίζει για τι χρησιμοποιείται το καθένα. Κάθε πρωτόκολλο είναι απλώς ένα συγκεκριμένο σύνολο κανόνων επικοινωνίας μεταξύ των υπολογιστών.

SMTP. SMTP σημαίνει Πρωτόκολλο μεταφοράς απλών μηνυμάτων. Το SMTP χρησιμοποιείται όταν ένα ηλεκτρονικό μήνυμα παραδίδεται από έναν πελάτη ηλεκτρονικού ταχυδρομείου, όπως το Outlook, σε ένα διακομιστή ηλεκτρονικού ταχυδρομείου ή όταν ένα ηλεκτρονικό μήνυμα παρέχεται από ένα e-mail server σε ένα άλλο. Το SMTP χρησιμοποιεί τη TCP θύρα 25 ή τη θύρα 465 για κρυπτογραφημένη επικοινωνία (SSL) ή τη 587 (TLS).

POP3. POP3 σημαίνει πρωτόκολλο ταχυδρομικού γραφείου. Το POP3 επιτρέπει σε ένα e-mail client να "κατεβάσει" ένα ηλεκτρονικό μήνυμα από έναν εξυπηρετητή (διακομιστή) ηλεκτρονικού ταχυδρομείου στο σταθμό εργασίας του. Το πρωτόκολλο POP3 είναι απλό και δεν προσφέρει πολλές δυνατότητες εκτός από τη λήψη. Ο σχεδιασμός του υποθέτει ότι ο πελάτης ηλεκτρονικού ταχυδρομείου κατεβάζει όλα τα διαθέσιμα μηνύματα ηλεκτρονικού ταχυδρομείου από το διακομιστή, τα διαγράφει από το διακομιστή και στη συνέχεια αποσυνδέεται, ενώ υπάρχει και η δυνατότητα διατήρησης αντιγράφου των μηνυμάτων στο διακομιστή μέσω ρύθμισης του προγράμματος-πελάτης. Το POP3 κανονικά χρησιμοποιεί τη TCP θύρα 110 ή τη θύρα 995 για κρυπτογραφημένη επικοινωνία (SSL).

IMAP. IMAP σημαίνει πρωτόκολλο πρόσβασης μηνυμάτων Διαδικτύου. Το πρωτόκολλο IMAP έχει πολλά παρόμοια χαρακτηριστικά με το POP3. Είναι και αυτό ένα πρωτόκολλο που ένας πελάτης ηλεκτρονικού ταχυδρομείου μπορεί να χρησιμοποιήσει για να κατεβάσει αλληλογραφία από ένα διακομιστή ηλεκτρονικού ταχυδρομείου. Ωστόσο, το IMAP περιλαμβάνει πολλές περισσότερες δυνατότητες από το POP3. Το πρωτόκολλο IMAP έχει σχεδιαστεί για να επιτρέπει στους χρήστες να διατηρούν τα emails τους στο διακομιστή. Το IMAP απαιτεί περισσότερο χώρο στο δίσκο στον κεντρικό υπολογιστή (Mail server) και περισσότερους πόρους CPU από το POP3, καθώς όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου αποθηκεύονται στο διακομιστή. Το IMAP συνήθως χρησιμοποιεί τη TCP θύρα 143 ή τη θύρα 993 για κρυπτογραφημένη επικοινωνία (SSL).

Παράδειγμα

Ας υποθέσουμε ότι χρησιμοποιείτε ένα διακομιστή email (Mail server) για να στείλετε ένα μήνυμα στη διεύθυνση john@microsoft.com.

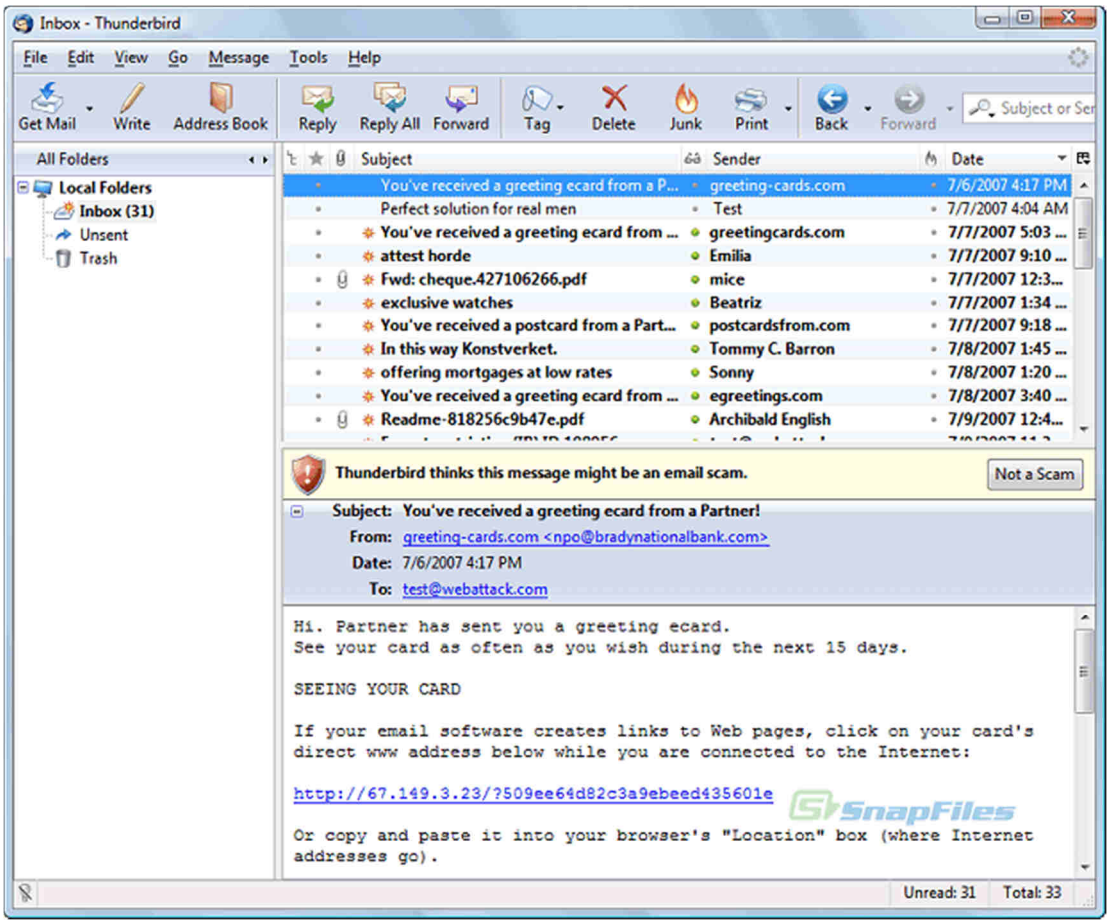
Γράφετε το μήνυμα στο πρόγραμμα Πελάτης (π.χ. Outlook) και κάνετε κλικ στο κουμπί «Αποστολή». Το Outlook παραδίδει το μήνυμα στο Mail server χρησιμοποιώντας το πρωτόκολλο SMTP. Ο Mail server παραδίδει το μήνυμα στο διακομιστή ηλεκτρονικού ταχυδρομείου της Microsoft (π.χ. mail.microsoft.com) χρησιμοποιώντας πάλι το SMTP.

Ο παραλήπτης του μηνύματος με το δικό του πρόγραμμα Πελάτη (π.χ. Mozilla Thunderbird) κατεβάζει το μήνυμα από το διακομιστή mail.microsoft.com στο φορητό υπολογιστή του χρησιμοποιώντας το πρωτόκολλο POP3 (ή IMAP).

Ένας διαφορετικός τύπος ηλεκτρονικού ταχυδρομείου είναι το **Web mail** που χρησιμοποιεί το πρωτόκολλο HTTP για να ολοκληρωθεί η επικοινωνία και διαβάζεται μέσα από

φυλλομετρητές (Browsers). Όπως φαίνεται και από το όνομά του, αυτό το είδος ηλεκτρονικού ταχυδρομείου είναι μία υπηρεσία του Παγκόσμιου Ιστού (World Wide Web).

Για να μπορέσει ένας χρήστης να διαβάσει τα μηνύματά του, θα πρέπει να πιστοποιηθεί από τον εξυπηρετητή εισερχόμενης αλληλογραφίας ότι είναι ο χρήστης που του αντιστοιχεί η ηλεκτρονική διεύθυνση που προσπαθεί να προσπελάσει. Η πιστοποίηση αυτή γίνεται με το συνδυασμό «Όνομα Χρήστη» (User ID ή Login User) και «Κωδικός Πρόσβασης» (Password).



Εικόνα 6.2.1.α: Το περιβάλλον λειτουργίας της e-mail εφαρμογής Thunderbird

(Πηγή: http://za.fileprogram.net/cdn/images/53-image-3-Thunderbird.gif)

Ένας διαφορετικός τύπος ηλεκτρονικού ταχυδρομείου είναι το Web mail, που χρησιμοποιεί το πρωτόκολλο HTTP για να ολοκληρωθεί η επικοινωνία και διαβάζεται μέσα από φυλλομετρητές (Browsers). Όπως φαίνεται και από το όνομά του, αυτό το είδος ηλεκτρονικού ταχυδρομείου είναι μία υπηρεσία του Παγκόσμιου Ιστού (World Wide Web).

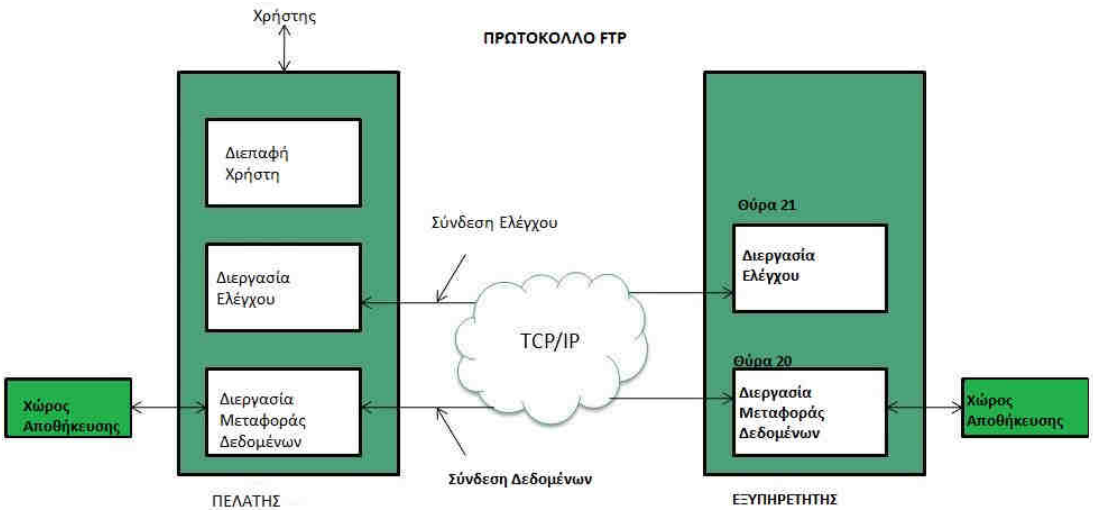
Για να μπορέσει ένας χρήστης να διαβάσει τα μηνύματά του, θα πρέπει να πιστοποιηθεί από τον εξυπηρετητή εισερχόμενης αλληλογραφίας ότι είναι ο χρήστης που του αντιστοιχεί η ηλεκτρονική διεύθυνση, την οποία προσπαθεί να προσπελάσει. Η πιστοποίηση αυτή γίνεται με το συνδυασμό «Όνομα Χρήστη» (User ID ή Login User) και «Κωδικός Πρόσβασης» (Password).

6.2.2 Υπηρεσία μεταφοράς αρχείων (FTP, TFTP)

Και τα δύο είναι πρωτόκολλα εφαρμογών που διατίθενται για τη μεταφορά αρχείων μεταξύ δύο συστημάτων που συνδέονται σε ένα τυπικό TCP/IP δίκτυο.

FTP (File Transfer Protocol) σημαίνει πρωτόκολλο μεταφοράς αρχείων. Χρησιμοποιείται για την αποστολή/λήψη αρχείων από τον απομακρυσμένο υπολογιστή (εξυπηρετητή). Το FTP δημιουργεί δύο συνδέσεις μεταξύ του συστήματος πελάτη και του server συστήματος, μία για πληροφορίες ελέγχου και η άλλη για τα δεδομένα που πρόκειται να μεταφερθούν. Η σύνδεση για πληροφορίες ελέγχου μεταφέρει εντολές και δέχεται απαντήσεις από το διακομιστή. Αρχικά πρέπει να γίνει ταυτοποίηση χρήστη (Authentication) μέσω της επικύρωσης με όνομα χρήστη (username) και τον κωδικό πρόσβασης (password). Μόλις γίνει αυτό, τα αρχεία μπορούν να μεταφερθούν μεταξύ των δύο συστημάτων. Το FTP χειρίζεται τόσο τα δυαδικά όσο και τα αρχεία μορφής κειμένου.

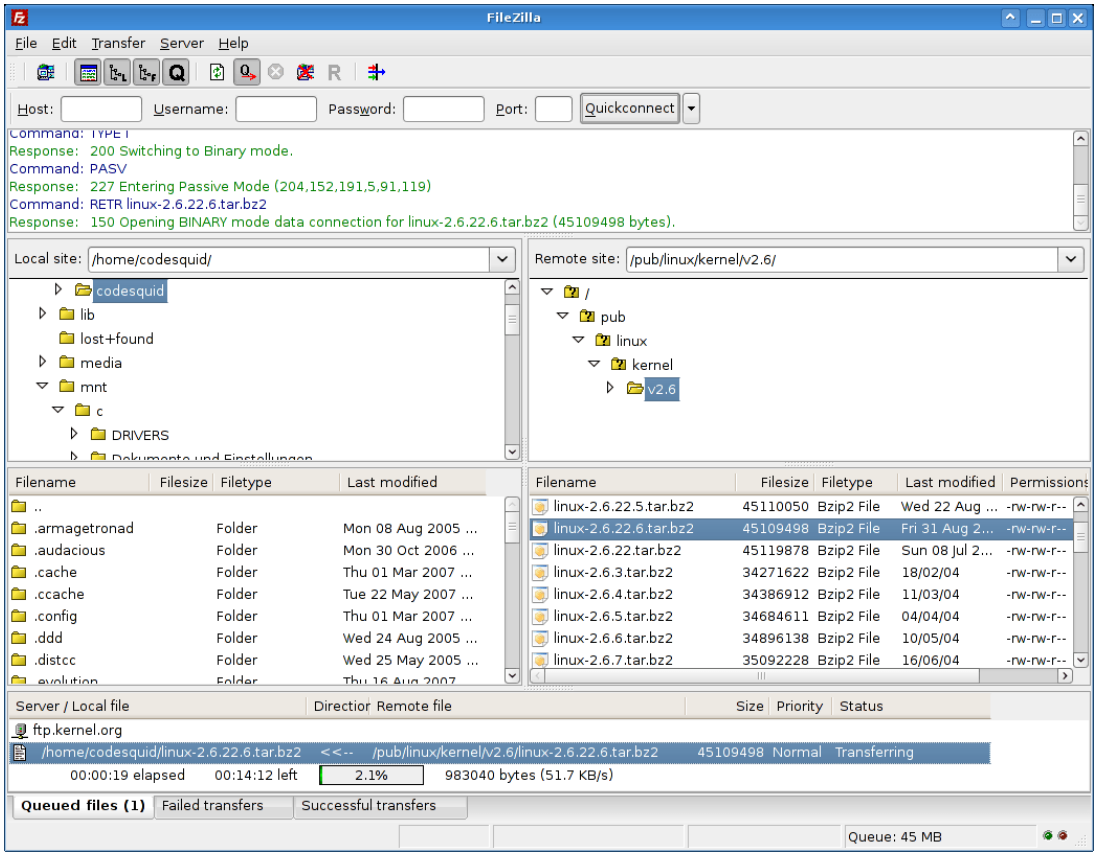
Όταν ένας πελάτης FTP ζητά να συνδεθεί με το διακομιστή FTP, μια σύνδεση TCP ιδρύεται στη θύρα 21 του διακομιστή FTP. Μετά τον έλεγχο ταυτότητας που γίνεται, μια άλλη σύνδεση TCP είναι υπό σύσταση για την πραγματική μεταβίβαση δεδομένων στη θύρα 20 του διακομιστή FTP.



Σχήμα 6.2.2.α: Το μοντέλο λειτουργίας του πρωτοκόλλου FTP

(Προσαρμογή από πηγή: http://www.tutorialspoint.com/internet_technologies/images/internet-ftp_model.jpg)

Η μεταφορά δεδομένων μέσω FTP μπορεί να γίνει με τη χρήση εντολών από το χρήστη. Οι εντολές get (πάρε), put (βάλε) είναι πολύ δημοφιλείς εντολές FTP για λήψη και αποστολή δεδομένων σε εξυπηρετητή. Προκειμένου να αποφευχθεί η χρήση των εντολών, υπάρχουν εφαρμογές FTP σε γραφικό περιβάλλον (GUI based) που έχουν αναπτυχθεί, όπως τα πολύ δημοφιλή FTP PRO και FileZilla.



Εικόνα 6.2.2.α: Το περιβάλλον λειτουργίας της ftp εφαρμογής FileZilla

(Πηγή: https://filezilla-project.org/images/screenshots/fz3_linux_main.png)

TFTP (Trivial File Transfer Protocol) σημαίνει απλό πρωτόκολλο μεταφοράς αρχείων. Είναι πιο απλό από το FTP, κάνει τη μεταφορά αρχείων μεταξύ του πελάτη και του διακομιστή, αλλά δεν παρέχει έλεγχο ταυτότητας χρήστη και άλλες χρήσιμες λειτουργίες που υποστηρίζονται από το FTP. Το TFTP χρησιμοποιεί πρωτόκολλο UDP, ενώ το FTP χρησιμοποιεί το πρωτόκολλο TCP. Στον Πίνακα 6.2.2.α παρουσιάζονται οι διαφορές των πρωτοκόλλων FTP και TFTP.

FTP (File Transfer Protocol)	TFTP (Trivial File Transfer Protocol)
Χρησιμοποιεί το TCP ως πρωτόκολλο επιπέδου μεταφοράς	Χρησιμοποιεί το UDP ως πρωτόκολλο επιπέδου μεταφοράς
Χρησιμοποιεί ισχυρές εντολές ελέγχου	Χρησιμοποιεί απλές εντολές ελέγχου
Στέλνει τα δεδομένα από μία ξεχωριστή σύνδεση TCP μέσω των εντολών ελέγχου	Δεν χρησιμοποιεί συνδέσεις γιατί το UDP είναι πρωτόκολλο χωρίς σύνδεση
Απαιτεί περισσότερη μνήμη και προγραμματιστική ισχύ	Απαιτεί λιγότερη μνήμη και προγραμματιστική ισχύ

Πίνακας 6.2.2.α: Διαφορές FTP και TFTP

6.2.3 Υπηρεσία παγκόσμιου ιστού WWW

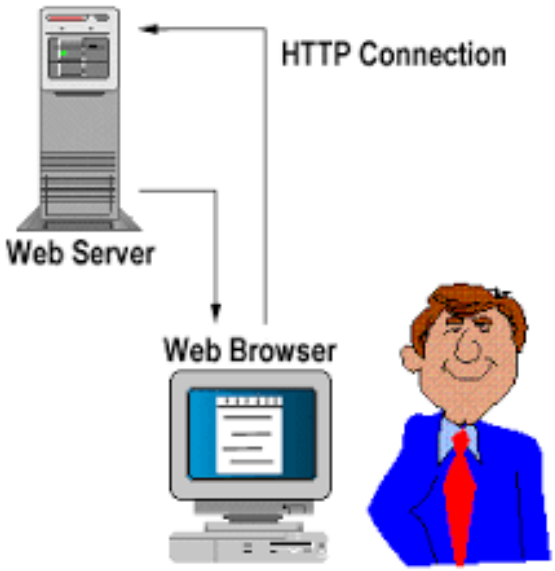
Η πιο γνωστή και πιο διαδεδομένη υπηρεσία του Διαδικτύου είναι ο Παγκόσμιος Ιστός (World, Wide Web, WWW). Κατ' αρχάς, επειδή πολλοί συγχέουν το Διαδίκτυο με τον Παγκόσμιο Ιστό, ας ξεκαθαρίσουμε ότι ο **ΠΑΓΚΟΣΜΙΟΣ ΙΣΤΟΣ (World Wide Web) δεν είναι συνώνυμο με το Διαδίκτυο (Internet).** Πολλές φορές στις συζητήσεις μας, όταν λέμε το ένα εννοούμε και το άλλο, αλλά στην πραγματικότητα αυτό είναι λάθος. Το Διαδίκτυο και ο Παγκόσμιος ιστός (εν συντομία Web) είναι δύο ξεχωριστά αλλά σχετιζόμενα πράγματα. Όταν λέμε Web, εννοούμε τον τρόπο που έχουμε πρόσβαση στην πληροφορία μέσω του Διαδικτύου. Είναι ένα μοντέλο διαμοιραζόμενης πληροφορίας που χτίζεται πάνω από το Διαδίκτυο.

Το χαρακτηριστικό γνώρισμα του Παγκόσμιου Ιστού είναι η μη γραμμική οργάνωση και αναζήτηση Πληροφοριών. Αναφέρουμε ως παράδειγμα μη γραμμικής αναζήτησης την περίπτωση που θέλουμε να αναζητήσουμε μία λέξη σε ένα λεξικό. Δεν ξεκινάμε από το Α για να φτάσουμε στη λέξη που θέλουμε, αλλά πάμε στο συγκεκριμένο γράμμα και ακολουθούμε τις λέξεις, έως ότου φτάσουμε στο επιθυμητό αποτέλεσμα.

Υπερκείμενο (Hypertext) ονομάζουμε ένα κείμενο στο οποίο η πληροφορία είναι οργανωμένη με μη γραμμική μορφή, δηλαδή η αναζήτηση της πληροφορίας δε γίνεται με κάποια συγκεκριμένη σειρά, αλλά τυχαία με βάση τους συνδέσμους (links) που υπάρχουν στο σώμα του κειμένου.

Υπερμέσα (Hypermedia) είναι μια συλλογή πολυμεσικών πληροφοριών (κείμενο, εικόνα, ήχο, video, animation) η οποία είναι οργανωμένη με μη γραμμικό τρόπο.

Ο Ιστός χρησιμοποιεί το **πρωτόκολλο HTTP** (HyperText Transfer Protocol – πρωτόκολλο μεταφοράς Υπερκειμένου), για να μεταφέρει δεδομένα.



Σχήμα 6.2.3.α: Σύνδεση HTTP

(Πηγή: http://homepages.uel.ac.uk/u0315352/Web%20server.htm)

Όπως αναφέρθηκε πιο πριν οι υπηρεσίες του Διαδικτύου είναι βασισμένες στο μοντέλο Πελάτη-Εξυπηρετητή. Έτσι και στην περίπτωση του Ιστού (της πιο διαδεδομένης υπηρεσίας του Διαδικτύου) ακολουθείται αυτό το μοντέλο. Το ρόλο του Εξυπηρετητή αναλαμβάνουν

προγράμματα γνωστά ως **Web Servers** (π.χ. Apache) που έχουν ως σκοπό την οργάνωση και διαχείριση των πληροφοριών μέσω Ιστοσελίδων (Web Pages). Οι ιστοσελίδες είναι μια εφαρμογή Υπερμέσου, δηλαδή μπορούν να περιέχουν κείμενο, εικόνες, video κ.λπ. Για να προσπελάσουμε μία ιστοσελίδα θα πρέπει να ξέρουμε τη «διεύθυνσή» της (URL – Uniform Resource Locator) που είναι της μορφής: **http://www.ntua.gr/info/studies.html.**

Αναλύοντας τη διεύθυνση μιας ιστοσελίδας διακρίνουμε:

1) **http:** Αναφέρεται στο πρωτόκολλο της υπηρεσίας που ανήκει η ιστοσελίδα.
2) **www:** Δηλώνει ότι πρόκειται για σελίδα του Ιστού. Πολλές φορές μπορεί και να παραλείπεται.
3) **ntua.gr:** Είναι η διεύθυνση του Web Server. Ουσιαστικά αυτό το κομμάτι της διεύθυνσης αναφέρεται σε έναν DNS Server και το όνομα (ntua.gr) μεταφράζεται σε IP διεύθυνση, όπως εξηγήσαμε παραπάνω.
4) **/info/:** Αναφέρεται σε φάκελο (directory) του Web Server.
5) **studies.html:** Είναι η ιστοσελίδα που θέλουμε να προσπελάσουμε.

Οι ιστοσελίδες έχουν σημεία σύνδεσης (hyperlinks) τα οποία μπορεί να είναι κείμενο, εικόνα κ.λπ. και μπορεί να παραπέμπει σε άλλο σημείο της ίδιας ιστοσελίδας, σε άλλη ιστοσελίδα στον ίδιο Web Server ή ακόμα και σε ιστοσελίδες που βρίσκονται οπουδήποτε στο Διαδίκτυο. Το μήκος μιας ιστοσελίδας δεν είναι απαραίτητο να έχει μήκος όσο μια σελίδα οθόνης ή μία εκτυπωμένη σελίδα, αλλά μπορεί να καταλαμβάνει πολύ περισσότερο μήκος ή και πλάτος. Ένα σύνολο πληροφοριών (π.χ παρουσίαση μια εταιρείας) οργανωμένη με ένα σύνολο ιστοσελίδων ονομάζεται τοποθεσία (site).

Οι **Φυλλομετρητές (Browsers)** είναι το πρόγραμμα Πελάτης που χρησιμοποιεί ο Ιστός για να απευθύνει «ερωτήματα» στον Εξυπηρετητή (Web Server). Υπάρχουν πολλά προγράμματα Φυλλομετρητών για το ίδιο ή διαφορετικά λειτουργικά συστήματα. Αναφέρουμε μερικά από αυτά: Internet Explorer, Firefox, Chrome, Opera κ.λπ.

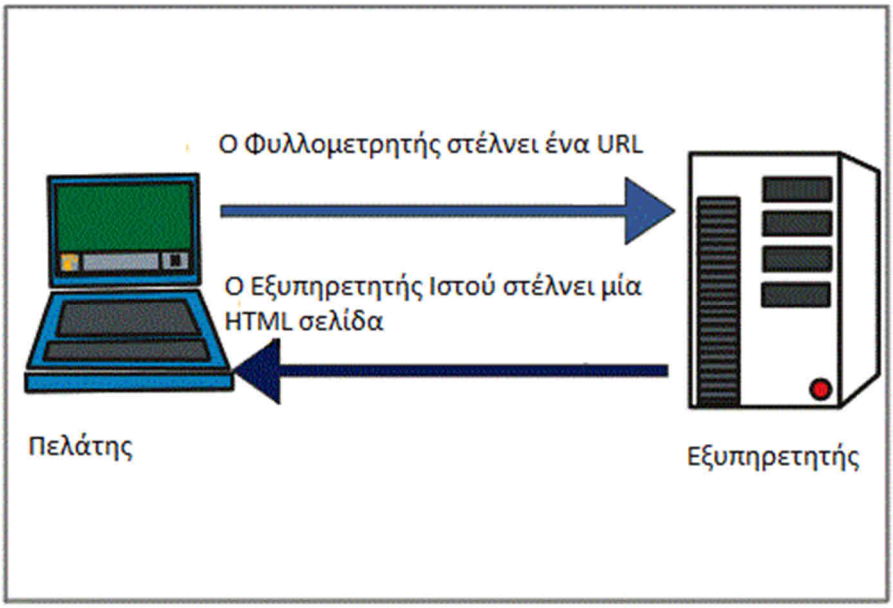
Οι βασικές λειτουργίες που τις συναντάμε σε όλα τα προγράμματα Φυλλομετρητών είναι να:

- αποστέλλει αιτήματα στους Εξυπηρετητές του Ιστού χρησιμοποιώντας το πρωτόκολλο HTTP
- σχεδιάζει την ιστοσελίδα σύμφωνα με τις πληροφορίες που του έστειλε ο Εξυπηρετητής
- τονίζει τα σημεία σύνδεσης, έτσι ώστε να είναι ευδιάκριτα και να είναι εύκολο να εντοπιστούν στην ιστοσελίδα
- δίνεται η δυνατότητα αποθήκευσης των διευθύνσεων των ιστοσελίδων σε καταλόγους
- κρατάει ιστορικό με τις διευθύνσεις των ιστοσελίδων που έχουμε επισκεφθεί

Με τους Φυλλομετρητές έχουμε τη δυνατότητα να διαβάζουμε τις ιστοσελίδες του Διαδικτύου, οι οποίες, όπως αναφέραμε και πιο πριν, είναι σελίδες Υπερμέσων, δηλαδή μπορεί να περιέχουν κείμενο, φωτογραφίες, animations κ.λπ. Για να διαβάσουμε μία ιστοσελίδα, θα πρέπει να ξέρουμε σε ποιον Web Server είναι αποθηκευμένη, δηλαδή να ξέρουμε τη «διεύθυνση» του Web Server και το όνομα της σελίδας που θέλουμε να διαβάσουμε. Τα πράγματα βέβαια είναι πιο απλά και δε χρειάζεται να θυμόμαστε τα ονόματα όλων των σελίδων που θέλουμε να διαβάσουμε αλλά μόνο τη «διεύθυνση» του Web Server. Αυτό γίνεται, γιατί υπάρχει ρύθμιση στους Web Servers για την αρχική σελίδα που θα εμφανίζεται (συνήθως ονομάζεται Home Page) αυτόματα, όταν κάποιος προσπελάζει τον συγκεκριμένο Server. Στη συνέχεια και μέσα από τους συνδέσμους (hyperlinks) που υπάρχουν σε αυτή τη σελίδα, μπορούμε να αναζητήσουμε τις πληροφορίες που θέλουμε, χωρίς να χρειάζεται να ξέρουμε το όνομα της συγκεκριμένης Ιστοσελίδας.

Έτσι, όταν πληκτρολογούμε **www.parliament.gr** τη διεύθυνση του Ελληνικού Κοινοβουλίου, στην ουσία διαβάσουμε μία ιστοσελίδα που έχει οριστεί ως Κύρια Ιστοσελίδα.

Είπαμε παραπάνω πως οι Φυλλομετρητές σχεδιάζουν την Ιστοσελίδα σύμφωνα με τα στοιχεία που τους στέλνει ο Web Server. Τα στοιχεία αυτά είναι σελίδες κειμένου της Γλώσσας Σήμανσης Υπερκειμένου (Hypertext Markup Language, **HTML**) και σύμφωνα με τα στοιχεία αυτής της σελίδας ο Φυλλομετρητής σχεδιάζει αυτό που βλέπουμε στην οθόνη του υπολογιστή μας.



Σχήμα 6.2.3.β. Απόκριση Εξυπηρετητή σε αίτημα Φυλλομετρητή

(Προσαρμογή από πηγή: http://homepages.uel.ac.uk/u0315352/Web%20server.htm)

6.2.4 Υπηρεσία απομακρυσμένης διαχείρισης (TELNET)

Τι είναι το Telnet. Είναι πρωτόκολλο για πρόσβαση σε απομακρυσμένους υπολογιστές. Το Telnet είναι μια υπηρεσία του Διαδικτύου που μας επιτρέπει να συνδεόμαστε με έναν απομακρυσμένο υπολογιστή μόνο μέσω γραμμής εντολών (και όχι μέσω διεπαφής χρήστη σε γραφικό περιβάλλον – GUI) και να δουλεύουμε αλληλεπιδραστικά στον υπολογιστή αυτό χρησιμοποιώντας τα προγράμματά του, σαν να είμαστε άμεσα συνδεδεμένοι μαζί του. Με άλλα λόγια, το δικό μας τερματικό - προσωπικός υπολογιστής, workstation, τερματικό ενός UNIX συστήματος, κ.λπ. - μετατρέπεται σε τερματικό του απομακρυσμένου υπολογιστή, ο οποίος ανταποκρίνεται στις εντολές μας.

Το Telnet βασίζεται στην αρχιτεκτονική client/server: για να χρησιμοποιήσουμε το Telnet, εκτελούμε στον υπολογιστή μας ένα πρόγραμμα πελάτη για Telnet (Telnet client), ενώ στον απομακρυσμένο υπολογιστή εκτελείται ένα πρόγραμμα που ονομάζεται εξυπηρετητής Telnet (Telnet server). Ο Telnet server είναι ένας ταυτόχρονος εξυπηρετητής που μπορεί να ανταποκριθεί σε πολλές αιτήσεις συγχρόνως, δημιουργώντας μια νέα διεργασία για κάθε νέα αίτηση.

Λόγοι χρήσης του telnet. Μέσω του Telnet, μπορούμε να συνδεόμαστε με υπολογιστές του Διαδικτύου σε ολόκληρο τον κόσμο και να εκμεταλλευόμαστε τις υπηρεσίες που προσφέρουν. Π.χ. μπορούμε να χρησιμοποιούμε απομακρυσμένες βάσεις δεδομένων και

άλλες πηγές πληροφόρησης, να αναζητούμε πληροφορίες σε βιβλιογραφικούς καταλόγους διαφόρων βιβλιοθηκών, κ.λπ.

Ο αριθμός των υπολογιστών του Διαδικτύου που προσφέρουν την υπηρεσία Telnet είναι πολύ μεγάλος και οι πληροφορίες που διατίθενται καλύπτουν όλους τους τομείς. Αρκετοί από τους υπολογιστές αυτούς παρέχουν on-line συστήματα βοήθειας με μενού που κάνουν τη χρήση τους πιο εύκολη. Κατά τη σύνδεσή μας με έναν απομακρυσμένο υπολογιστή, μας ζητείται όνομα χρήστη (login name) και συνθηματικό (password). Επομένως, θα πρέπει να έχουμε (δηλαδή δικαίωμα πρόσβασης) στον υπολογιστή αυτό. Μερικές φορές, για υπηρεσίες που διατίθενται δημόσια, μας υποδεικνύεται από τον απομακρυσμένο υπολογιστή κάποιο ειδικό όνομα login (π.χ. guest), ώστε να μπορέσουμε να συνδεθούμε, ακόμη κι αν δεν διαθέτουμε λογαριασμό.

Αντίθετα, με το FTP (το οποίο πραγματοποιεί μια σύνδεση με μοναδικό σκοπό τη μεταφορά αρχείων), οι συνδέσεις μέσω Telnet είναι γενικές. Η αξιοποίηση μιας σύνδεσης Telnet εξαρτάται περισσότερο από το τι έχει να σας προσφέρει ο απομακρυσμένος υπολογιστής παρά από τα χαρακτηριστικά γνωρίσματα του Telnet. Μπορείτε να χρησιμοποιήσετε το Telnet για να έρθετε σε επαφή με αυτόνομες εφαρμογές ή ακόμα και με εφαρμογές πελάτη - εξυπηρετητή που βρίσκονται σε άλλους υπολογιστές.

6.2.5 Υπηρεσία τηλεφωνίας μέσω Διαδικτύου (VoIP/SIP)

Η ιδέα της μετατροπής της φωνής σε ηλεκτρικό σήμα είναι παλιά και αποτέλεσε τη βάση για τη λειτουργία της επικοινωνίας με φωνή σε μεγάλη απόσταση (τηλέφωνο, ασύρματος).

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

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

Η τεχνολογία της τηλεφωνικής επικοινωνίας μέσω δικτύων δεδομένων, που χρησιμοποιείται όλο και πιο πολύ, ονομάζεται VoIP (Voice over Internet Protocol). Σε αυτό το σημείο θα πρέπει να προσέξουμε να μην την μπερδέψουμε με το Διαδίκτυο. Το πρωτόκολλο IP χρησιμοποιείται στα περισσότερα δίκτυα υπολογιστών και όχι μόνο στο Διαδίκτυο. Η τεχνολογία VoIP μπορεί να εφαρμοστεί οπουδήποτε υπάρχει επικοινωνία μέσω ενός τέτοιου δικτύου.

Δύο είναι τα **βασικά πρότυπα**, για τα οποία γίνεται λόγος αυτόν τον καιρό:

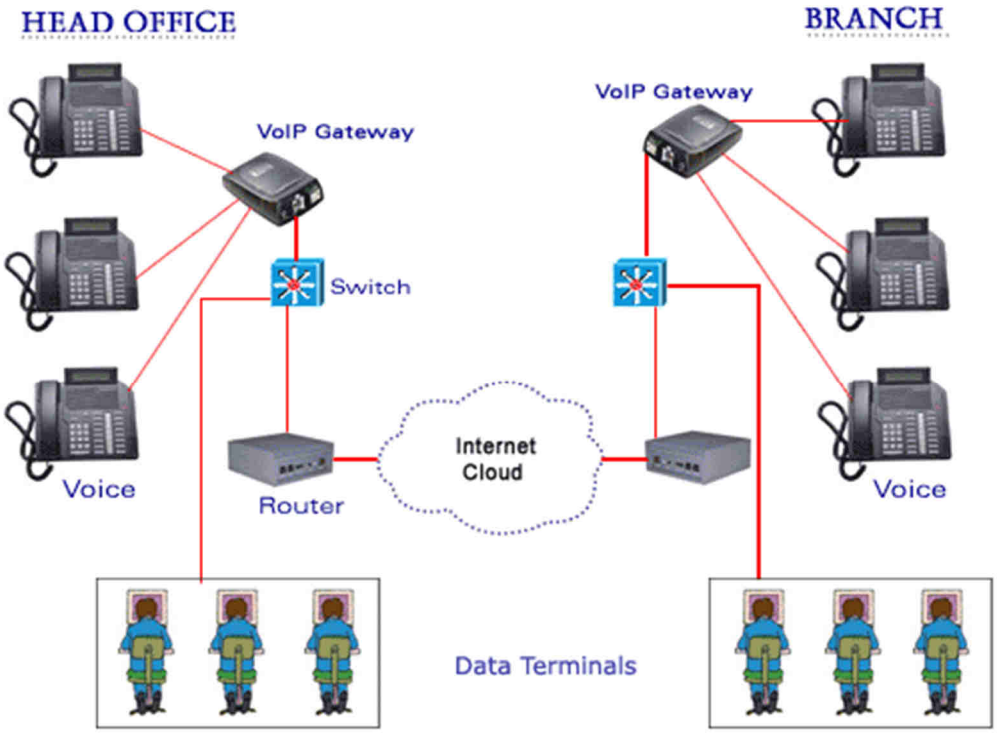
- το 1996 παρουσιάστηκε το πρότυπο H.323 της ITU και
- το 1999 το Session Initiation Protocol (SIP) της IETF (Internet Engineering Task Force).

Αυτά τα πρότυπα αφορούν κυρίως στον τρόπο διαχείρισης της κλήσης (τις διαδικασίες σύνδεσης/αποσύνδεσης κ.λπ.). Τον τελευταίο καιρό χρησιμοποιείται όλο και πιο πολύ το SIP.

Τι είναι το VoIP. Το VoIP (Voice over Internet Protocol) είναι ένας γενικός όρος για μια οικογένεια τεχνολογιών που επιτρέπει τη μετάδοση φωνής πάνω από το πρωτόκολλο του

Διαδικτύου (Internet Protocol). Έτσι με τη χρήση IP τηλεφωνικών συσκευών ή ειδικών μετατροπέων, δίνεται η δυνατότητα πραγματοποίησης τηλεφωνικών κλήσεων πάνω από την υπάρχουσα δικτυακή υποδομή και όχι το δημόσιο τηλεφωνικό δίκτυο. Τα βασικά στάδια για τη μετάδοση φωνής πάνω από το πρωτόκολλο του Διαδικτύου είναι η μετατροπή του αναλογικού σήματος φωνής σε ψηφιακή μορφή, η συμπίεση και μετατροπή του στο πρωτόκολλο του Διαδικτύου και τέλος η μετάδοση του σε μορφή πακέτων πάνω από το Διαδίκτυο. Η όλη διαδικασία στο απομακρυσμένο άκρο αντιστρέφεται. Οι διαδικασίες και στα δύο σημεία γίνονται σε πραγματικό χρόνο.

Για να λειτουργήσει το VoIP χρειαζόμαστε σύνδεση με το Διαδίκτυο. Ενώ λειτουργεί και με dial-up, ιδανικά προτιμούμε μόνιμες συνδέσεις (π.χ. ADSL) για να είναι πάντα ενεργό (always-on) το τηλέφωνο μας και να μπορούμε να δεχόμαστε κλήσεις ανά πάσα στιγμή. Το VoIP λειτουργεί με οποιαδήποτε σύνδεση στο Διαδίκτυο (ADSL, WiFi, GPRS, 3G, κ.λπ.) αρκεί να επιτρέπεται η διακίνηση των VoIP "πακέτων" στο εκάστοτε δίκτυο. Το VoIP σαν τεχνολογία υπάρχει από τις αρχές τις δεκαετίας του '90, αλλά άρχισε να γίνεται ιδιαίτερα διαδεδομένο στις αρχές του 2000. Σήμερα εκατομμύρια άνθρωποι σε όλο τον κόσμο χρησιμοποιούν τεχνολογίες VoIP για την επικοινωνία τους, είτε το ξέρουν (Skype) είτε δεν το ξέρουν (εναλλακτικοί πάροχοι). Το VoIP λειτουργεί, είτε μόνο για εξερχόμενες κλήσεις είτε και για εισερχόμενες με χρήση κανονικού τηλεφωνικού αριθμού.



Σχήμα 6.2.5.α: Δίκτυο VoIP

(Πηγή: http://www.mycomputerwiz.net/wp-content/uploads/2014/01/voip-diagram.gif)

Τα πλεονεκτήματα αλλά και τα προβλήματα του VoIP. Κατά την ψηφιοποίηση της φωνής μπορούν να εφαρμοστούν αλγόριθμοι συμπίεσης και κωδικοποίησης. Ένα σύστημα το οποίο συνδυάζει αυτές τις λειτουργίες ονομάζεται codec (Coder/Decoder). Χρησιμοποιώντας ένα codec με υψηλή συμπίεση μπορούμε να μεταφέρουμε από την ίδια γραμμή επικοινωνίας περισσότερες από μία κλήσεις.

Η τεχνολογία του VoIP επηρεάζεται από πολλές παραμέτρους. Τα πακέτα δεδομένων IP, που ταξιδεύουν από έναν υπολογιστή μέσω διαφόρων δικτύων στον προορισμό τους, μπορεί να φτάσουν καθυστερημένα, με διαφορετική σειρά ή ακόμα και να χάνονται. Με τις εξελίξεις στην τεχνολογία των δικτύων η ποιότητα τηλεφωνίας VoIP μπορεί σήμερα να φτάσει την αντίστοιχη των γραμμών ISDN.

Σημαντικό ρόλο στην ποιότητα παίζουν ο λόγος της συμπίεσης που εφαρμόζει το codec καθώς και η ταχύτητα και η διαθέσιμη χωρητικότητα στο δίκτυο μεταφοράς δεδομένων.

Για την καλή λειτουργία της IP τηλεφωνίας υπάρχουν κάποιες προϋποθέσεις. Όταν η υλοποίηση αφορά ένα δίκτυο υπολογιστών πλήρως ελεγχόμενο, π.χ. το εσωτερικό δίκτυο μίας επιχείρησης, τότε είναι εύκολο να εντοπισθούν και να βελτιωθούν τυχόν προβλήματα. Όταν όμως το IP τηλέφωνό μας είναι συνδεδεμένο μέσω Διαδικτύου σε έναν πάροχο IP τηλεφωνίας, τότε έρχονται να προστεθούν τυχόν «ανωμαλίες» των ενδιάμεσων φορέων. Η καλύτερη και οικονομικότερη σύνδεση προσφέρεται – θεωρητικά – μέσω γραμμών ADSL. Αν και αρκεί η ταχύτητα μεταφοράς δεδομένων μέσω γραμμών ISDN για τη λειτουργία του IP τηλεφώνου μας (με συμπίεση), η γραμμή ADSL παρέχει χαμηλότερη χρέωση, αφού δεν υπάρχει χρονοχρέωση και μπορούμε να είμαστε συνέχεια συνδεδεμένοι.

Γενικά, όταν μιλάμε για σύνδεση σε IP πάροχο μέσω Διαδικτύου, θα πρέπει να ξέρουμε ότι υπάρχουν πολλοί «αδύναμοι κρίκοι»:

- Το πακέτο ξεκινάει από το σπίτι μας μέσω του χάλκινου καλωδίου για να φτάσει στο πλησιέστερο κέντρο του παρόχου.
- Από το κέντρο του παρόχου θα πρέπει τα δεδομένα να φτάσουν σε ένα από τα κέντρα σύνδεσης των ISP (πάροχοι υπηρεσιών Διαδικτύου).
- Από τον ISP τα δεδομένα μεταφέρονται μέσω του δικού του δικτύου αλλά και άλλων δικτύων στον προορισμό τους, στον κόμβο του IP τηλεφωνικού παρόχου. Μέχρι να φτάσουν εκεί, ενδεχομένως έχουν μεγάλο ταξίδι, ακόμα και υπερατλαντικό.

Σε όλα αυτά τα στάδια υπάρχουν καθυστερήσεις και διάφορα άλλα προβλήματα που μπορούν να «χτυπήσουν» τα πακέτα της IP τηλεφωνίας μας. Δεν είναι μόνο ο χρόνος μεταφοράς πακέτων (τα μαγικά 200 ms, τα οποία συχνά αναφέρονται) αλλά και άλλα προβλήματα.

Πλεονεκτήματα. Το μεγαλύτερο πλεονέκτημα του VoIP είναι το μειωμένο κόστος. Οι υπηρεσίες VoIP είναι πολύ φθηνότερες από τις παραδοσιακές επίγειες υπηρεσίες και, σε ορισμένες περιπτώσεις, ακόμα και δωρεάν. Άλλο μεγάλο πλεονέκτημα του VoIP είναι η φορητότητά του – καθώς χρησιμοποιεί το παγκόσμιο δίκτυο του Διαδικτύου, οι χρήστες δεν δεσμεύονται με κάποια συγκεκριμένη τοποθεσία, για διάφορες υπηρεσίες. Αρκεί να έχετε υπολογιστή, ευρυζωνική σύνδεση και, σε ορισμένες περιπτώσεις, έναν προσαρμογέα τηλεφώνου, για να μπορείτε να κάνετε κλήσεις χρησιμοποιώντας το λογαριασμό σας VoIP.

Μειονεκτήματα. Οι γραμμές VoIP είναι ευαίσθητες στους ίδιους τύπους επιθέσεων στους οποίους εκτίθενται η σύνδεση Διαδικτύου και το e-mail σας και οι ειδικοί ασφάλειας προβλέπουν ότι οι επιτιθέμενοι είναι απασχολημένοι προετοιμάζοντας επιμελώς νέες επιθέσεις και απειλές στις υπηρεσίες VoIP. Πριν εγγραφείτε για υπηρεσία VoIP, πρέπει να γνωρίζετε αυτά τα πιθανά τρωτά σημεία:

- **Αλληλογραφία spam.** Η υπηρεσία VoIP υπόκειται στο δικό της τύπο ανεπιθύμητου μάρκετινγκ, γνωστού ως «Spam over Internet Telephony» (Spam μέσω τηλεφωνίας Internet) ή SPIT.
- **Διακοπές.** Επιθέσεις Διαδικτύου, όπως οι ιοί και ιοί τύπου worm (σκουληκιού) μπορεί να διαταράξουν την υπηρεσία ή ακόμη και να θέσουν την υπηρεσία VoIP εκτός λειτουργίας.

- **Ηλεκτρονικό «ψάρεμα» (phishing) μέσω φωνής.** Γνωστό και ως «vishing». Αυτό συμβαίνει όταν ένας επιτιθέμενος έλθει σε επαφή χρησιμοποιώντας τη γραμμή VoIP και επιχειρεί να σας ξεγελάσει, ώστε να αποκαλύψετε πολύτιμα προσωπικά δεδομένα, όπως στοιχεία πιστωτικής κάρτας ή τραπεζικού λογαριασμού.
- **Απώλεια ιδιωτικού απορρήτου.** Το μεγαλύτερο μέρος της κυκλοφορίας VoIP δεν είναι κρυπτογραφημένο, καθιστώντας εύκολο για τους εισβολείς να παρακολουθούν τις συνομιλίες μέσω VoIP.
- **Παράνομη πρόσβαση (Hacking).** Οι hackers μπορούν να αποκτήσουν πρόσβαση στη σύνδεση VoIP και να χρησιμοποιήσουν τη γραμμή σας για να πραγματοποιούν κλήσεις. Σε ορισμένες περιπτώσεις, μπορεί ακόμη και να πουλήσουν τα στοιχεία της σύνδεσής σας στη μαύρη αγορά. Μόλις βρεθούν εντός του οικιακού δικτύου σας, οι hackers μπορούν να ψάξουν για ευαίσθητα στοιχεία που ενδέχεται να έχουν αποθηκευτεί στον υπολογιστή σας.
- **Εξάρτηση από το Διαδίκτυο και το ηλεκτρικό δίκτυο.** Οποιαδήποτε στιγμή ο πάροχος της υπηρεσίας Διαδίκτυο ή το ηλεκτρικό δίκτυο τεθεί εκτός λειτουργίας, το ίδιο θα συμβεί και στην υπηρεσία VoIP. Η αδυναμία πραγματοποίησης εξερχόμενων κλήσεων από το οικιακό τηλέφωνό σας σε περίπτωση έκτακτης ανάγκης αποτελεί κίνδυνο, οπότε βεβαιωθείτε ότι έχετε πάντα φορτισμένο ένα κινητό τηλέφωνο ως εφεδρική συσκευή.

Μετριάζοντας τους κινδύνους. Η επικοινωνία μέσω τηλεφωνικών υπηρεσιών του Διαδικτύου (VoIP) είναι πολύ οικονομική και παρέχει πολλές συναρπαστικές λειτουργίες. Απλά βεβαιωθείτε ότι την εγκαθιστάτε με ασφάλεια λαμβάνοντας τις εξής προφυλάξεις:

- **Ασφάλεια του εξοπλισμού.** Επιλέξτε εξοπλισμό VoIP που χρησιμοποιεί τα τρέχοντα πρότυπα ασύρματης ασφάλειας, όπως τα Wi-Fi Protected Access (WPA), WPA2 και IEEE 802.11i. Μη βασίζεστε στο πρωτόκολλο ασφάλειας Wired Equivalent Privacy (WEP). Είναι μια παλαιότερη και λιγότερη ασφαλής τεχνολογία.
- **Πιστοποίηση γνησιότητας και κρυπτογράφηση.** Ενεργοποιήστε οποιεσδήποτε λειτουργίες πιστοποίησης γνησιότητας και κρυπτογράφησης που είναι διαθέσιμες στο σύστημα VoIP σας. Με τον τρόπο αυτό δεν θα επιτρέψετε σε μη εξουσιοδοτημένα άτομα να εισέλθουν στο δίκτυό σας και θα διασφαλίσετε το ιδιωτικό απόρρητο για τις κλήσεις σας. Οι συσκευές WPA, WPA2 και IEEE 802.11i διαθέτουν προηγμένη κρυπτογράφηση και τεχνολογία πιστοποίησης γνησιότητας.
- **Τείχος προστασίας (firewall) VoIP.** Χρησιμοποιήστε firewall ειδικά σχεδιασμένο για κυκλοφορία VoIP. Το firewall θα εντοπίσει ασυνήθιστα πρότυπα κλήσεων και θα παρακολουθεί για ενδείξεις επίθεσης.
- **Δύο συνδέσεις.** Αν είναι εφικτό, να έχετε ξεχωριστή σύνδεση Διαδικτύου για τη γραμμή VoIP σας, ώστε οι ιοί ή οι επιθέσεις που απειλούν το δίκτυο δεδομένων σας να μην επηρεάσουν το τηλέφωνό σας.
- **Ενημερωμένη προστασία από ιούς.** Χρησιμοποιήστε ενημερωμένη προστασία από ιούς και τεχνολογία προστασίας από αλληλογραφία spam στις συσκευές σας.
- **Επίγνωση.** Μπορείτε να ενεργήσετε ως μια συμπαγής γραμμή άμυνας, προσέχοντας για περίεργες δραστηριότητες στη γραμμή σας VoIP και αποκτώντας εξοικείωση με τις τεχνικές που χρησιμοποιούν οι επιτιθέμενοι.

Το πρωτόκολλο SIP

Το Πρωτόκολλο Έναρξης Συνόδου (Session Initiation Protocol, SIP) είναι ένα πρωτόκολλο σηματοδότησης, πολύ σημαντικό για τη βιομηχανία τηλεπικοινωνιών. Παρακάτω θα εξηγήσουμε γιατί είναι τόσο σημαντικό.

Ας κάνουμε μια εισαγωγή στο SIP, ώστε να το γνωρίσουμε καλύτερα. Το SIP είναι ένα ελαφρύ, επεκτάσιμο, αιτήματος - απάντησης πρωτόκολλο για την εκκίνηση επικοινωνιακών

συνδέσεων μεταξύ δύο τερματικών. Το SIP είναι εμπνευσμένο από το HTTP και το SMTP, ωστόσο είναι διαφορετικό. Μπορούμε να συγκρίνουμε τα μηνύματα του SIP με αυτά των CB. Το SIP δημιουργήθηκε από το IETF το 1999 και υλοποιήθηκε το 2002.

Ποια είναι τα πλεονεκτήματα του. Γενικά χρησιμοποιείται από δύο τερματικά σημεία για να την διαπραγμάτευση μίας κλήσης. Με τον όρο διαπραγμάτευση εννοούμε το μέσο (κείμενο, φωνή κ.λπ.), την μεταφορά (συνήθως μέσο του RTP, Real Time Protocol) και την κωδικοποίηση (codec). Όταν η διαπραγμάτευση πετύχει, τα δύο τερματικά σημεία χρησιμοποιούν την επιλεγμένη μέθοδο, για να μιλήσουν το ένα στο άλλο ανεξάρτητα του SIP. Όταν η κλήση τελειώσει, το SIP χρησιμοποιείται για να δηλώσει τον τερματισμό της. Το SIP και οι επεκτάσεις του παρέχουν και λειτουργίες άμεσων μηνυμάτων, εγγραφής και παρουσίας.

Ένα σημείο τερματισμού στην διάλεκτο του SIP λέγεται user agent. Αυτό μπορεί να είναι ένα softphone, ένας instant messenger, ένα IP τηλέφωνο ή και ένα απλό τηλέφωνο. Κεντροποιημένες υπηρεσίες, όπως από τους proxies ή τους servers εφαρμογών, παρέχονται από τον server user agent.

Η λειτουργία του SIP ακούγεται να είναι πολύ απλή, και είναι. Αλλά εξαιτίας της απλότητας είναι σημαντικό για το πρωτόκολλο να είναι σταθερό. Η απλότητα του SIP πάντως σε καμία περίπτωση δεν περιορίζει της δυνατότητες του, καθώς βρίσκει εφαρμογή σε μια πλειάδα λειτουργιών.

Σκεφτείτε το HTTP για παράδειγμα. Ο ορισμός του πρωτοκόλλου είναι μικροσκοπικός. Αλλά οι τρόποι χρήσεως του είναι απεριόριστοι. Έτσι και το SIP. Εκατοντάδες επεκτάσεις υπάρχουν ήδη και καλύπτουν ένα μεγάλο εύρος από εφαρμογές. Ας δούμε τώρα πιο αναλυτικά το SIP και ας ανακαλύψουμε γιατί είναι τόσο σημαντικό.

Είναι το SIP τόσο σημαντικό; Κάποιοι λένε ότι "ό,τι έκανε το HTTP για το Web, το SIP θα το κάνει για τις τηλεπικοινωνίες".

Το SIP έχει κορυφαίο αντίκτυπο στη βιομηχανία τηλεπικοινωνιών. Οι παραδοσιακές εταιρείες τεχνολογίας έχουν αποφασίσει να προτυποποιήσουν το SIP για όλες τις μελλοντικές τους εφαρμογές. Οι κατασκευαστές VoIP και instant messaging εφαρμογών (π.χ. MSN Messenger) έχουν προτυποποιήσει επίσης το SIP.

Ποια είναι όμως τα πλεονεκτήματα του SIP έναντι των άλλων πρωτοκόλλων σηματοδότησης και των τεχνολογιών σημείο-προς-σημείο; Μερικά από τα πλεονεκτήματα αναφέρονται παρακάτω:

- **Σταθερότητα**: Το πρωτόκολλο χρησιμοποιείται κάποια χρόνια τώρα και είναι “βράχος”.
- **Ταχύτητα**: Αυτό το μικροσκοπικό UTP πρωτόκολλο είναι εξαιρετικά αποδοτικό.
- **Ευελιξία**: Αυτό το πρωτόκολλο είναι βασισμένο σε κείμενο και είναι εύκολα επεκτάσιμο.
- **Ασφάλεια**: Δυνατότητες κρυπτογράφησης (SSL, S/MIME) και πιστοποίησης είναι διαθέσιμες.
  Διάφορες επεκτάσεις του SIP παρέχουν και άλλες δυνατότητες ασφάλειας.
- **Προτυποποίηση**: Σε ολόκληρη τη βιομηχανία τηλεπικοινωνιών το SIP γίνεται πλέον το πρότυπο. Άλλες τεχνολογίες, ακόμα και να έχουν κάποια πλεονεκτήματα έναντι του SIP, τους λείπει η ευρεία χρήση.

Στην ενότητα Π.5 του Παραρτήματος μπορείτε επίσης να μελετήσετε την ανατομία μιας SIP κλήσης.

6.2.6 Άλλες εφαρμογές και χρήσεις

Μετάδοση εικόνας και ήχου μέσω του Διαδικτύου (video chat). Η μετάδοση αρχείων video μέσω του Διαδικτύου αρχικά παρουσίαζε κάποιες δυσκολίες, λόγω των αυξημένων τους απαιτήσεων σε χώρο αποθήκευσης και σε συνδέσεις υψηλών ταχυτήτων (ώστε να είναι δυνατή η ικανοποιητική προβολή των αρχείων). Οι χρήστες δυσκολεύονταν να χειριστούν αρχεία γραφικών, ήχου και video μέσω του Διαδικτύου, λόγω του μεγάλου τους μεγέθους και, επομένως, του μεγάλου εύρους ζώνης, που απαιτούνταν κατά την μετάδοσή τους. Προκειμένου να γίνει δυνατή η μετάδοση video μέσω του Διαδικτύου, αναπτύχθηκαν ειδικές τεχνικές συμπίεσης και πρωτόκολλα, που μεταφέρουν συμπιεσμένο σήμα. Η συμπίεση είναι τεχνική, που προσφέρει τη δυνατότητα μεταφοράς σήματος με εύρος ζώνης μεγαλύτερο από αυτό, που επιτρέπει το κανάλι. Επιτυγχάνει, δηλαδή, την ελαχιστοποίηση της μεταδιδόμενης πληροφορίας, διατηρώντας, όμως, την ποιότητά της. Για τις τεχνικές συμπίεσης αναπτύχθηκαν αρχικά τα συστήματα MPE01 και MPE02, ενώ για τη μετάδοση εικόνας και ήχου στο Διαδίκτυο αναπτύχθηκε το πρωτόκολλο H.323.

Η συμπίεση των αρχείων σε συνδυασμό με την εμφάνιση νέων τεχνικών μετάδοσης, με τις οποίες επιτυγχάνονται υψηλές ταχύτητες και η δυνατότητα μεγάλων χώρων αποθήκευσης στους τελικούς χρήστες συντέλεσαν στο να ξεπεραστούν τα όποια προβλήματα μετάδοσης. Δίνεται, έτσι, στους χρήστες η δυνατότητα να επικοινωνούν σε πραγματικό χρόνο και να ανταλλάσσουν μεταξύ τους αρχεία πολυμέσων. Ο χρήστης μπορεί, σήμερα, να μεταφέρει σε πραγματικό χρόνο εικόνα από κάμερα, που είναι συνδεδεμένη στον υπολογιστή του και να συμμετέχει με αυτόν το τρόπο από το γραφείο του σε τηλεδιάσκεψη μέσω του Διαδικτύου.

Παράδειγμα εφαρμογής ομαδικής επικοινωνίας μέσω του Διαδικτύου αποτελεί η εφαρμογή ooVoo, που επιτρέπει την επικοινωνία μέχρι δώδεκα ατόμων ταυτόχρονα.

Για να πραγματοποιηθεί η τηλεδιάσκεψη μέσω του Διαδικτύου απαιτείται υπολογιστής, ο οποίος είναι εφοδιασμένος με κάρτα ήχου διπλής κατεύθυνσης (full duplex), κάρτα video και κάμερα. Επίσης, χρειαζόμαστε μικρόφωνο, ηχεία, ακουστικά και modem για τη σύνδεση στο Διαδίκτυο. Φυσικά, δεν πρέπει να παραλείψουμε το κατάλληλο λογισμικό, το οποίο πρέπει να είναι διαθέσιμο (το ίδιο ή συμβατό) σε όλους τους χρήστες.

Συνομιλία πραγματικού χρόνου στο Διαδίκτυο με την μορφή κειμένου (chat). Μέσω του Διαδικτύου μπορούμε να συζητάμε με τους φίλους μας, ανταλλάσσοντας μηνύματα σε μορφή κειμένου σε πραγματικό χρόνο. Τα μηνύματα και οι απαντήσεις, που πληκτρολογούμε στον υπολογιστή μας, εμφανίζονται την ίδια ακριβώς στιγμή στις οθόνες όλων όσων συμμετέχουν στη συζήτησή μας.

Δίνεται έτσι η δυνατότητα να δημιουργούνται ομάδες χρηστών, οι οποίοι συζητούν για συγκεκριμένα θέματα ειδικού ενδιαφέροντος. Με αυτό το τρόπο ορίζονται περιοχές (χώροι) συζητήσεων, όπου μπορεί ο καθένας να πάρει μέρος ανάλογα με τα ενδιαφέροντα του. Τα προγράμματα, που υποστηρίζουν τέτοιες εφαρμογές, χρησιμοποιούν τα πρωτόκολλα TCP/IP και δεν χρειάζεται να αναπτυχθεί κάποιο ειδικό πρωτόκολλο, όπως στην περίπτωση της μεταφοράς εικόνας και ήχου. Για να συμμετάσχουμε σε τέτοια συζήτηση, πρέπει να κάνουμε τα εξής βήματα:

- Αρχικά, να έχουμε εγκαταστήσει στον υπολογιστή μας το κατάλληλο λογισμικό.
- Αφού συνδεθούμε στο Διαδίκτυο, εκτελούμε το λογισμικό και δίνουμε την διεύθυνση του χρήστη ή του εξυπηρετητή, που φιλοξενεί το χώρο συζητήσεων, στον οποίο θέλουμε να συνδεθούμε.
- Περιμένουμε, μέχρι να μας απαντήσει, είτε ο συγκεκριμένος χρήστης με τον οποίο συνδεθήκαμε είτε ένας οποιοσδήποτε χρήστης από αυτούς που συμμετέχουν στο χώρο που θέλουμε να συνδεθούμε.

- Μόλις ο χρήστης ή κάποιος από την ομάδα που καλέσαμε απαντήσει, είμαστε έτοιμοι να ξεκινήσουμε την επικοινωνία μας. Στην οθόνη του υπολογιστή μας αρχίζουν και εμφανίζονται, σε ένα τμήμα, αυτά που πληκτρολογεί ο χρήστης με τον οποίο συνδεθήκαμε και, σε ένα άλλο τμήμα, αυτά που πληκτρολογούμε εμείς.

Προγράμματα που υποστηρίζουν γραπτή επικοινωνία σε πραγματικό χρόνο είναι πολλά, από τα οποία τα πιο χαρακτηριστικά είναι τα: Talk, WinTalk, Chat, IRC (Internet Relay Chat), IRCII For Windows. Η δυνατότητα αυτή πλέον υποστηρίζεται και από την υπηρεσία του παγκόσμιου ιστού (WWW).

Ηλεκτρονικό Εμπόριο. Με τον όρο ηλεκτρονικό εμπόριο εννοούμε κάθε είδος εμπορικής δραστηριότητας που πραγματοποιείται με τη χρήση ηλεκτρονικών μέσων. Η χρησιμοποίηση των τηλεπικοινωνιακών δικτύων προσφέρει τη δυνατότητα διεκπεραίωσης εμπορικών συναλλαγών από απόσταση, χωρίς να απαιτείται η φυσική παρουσία των ατόμων που λαμβάνουν μέρος στη συναλλαγή. Με το τρόπο αυτό, οι συναλλαγές πραγματοποιούνται αυτόματα, ηλεκτρονικά και από απόσταση, χωρίς να απαιτείται ούτε καν η χρήση χαρτιού ή fax. Οι συναλλαγές γίνονται μέσω ηλεκτρονικών υπολογιστών, που είναι συνδεδεμένοι στο Διαδίκτυο και για την επικοινωνία τους χρησιμοποιούν συνήθως τηλεφωνικές γραμμές.

Το ηλεκτρονικό εμπόριο δεν αναφέρεται σε κάποια συγκεκριμένη τεχνολογία. Αντίθετα, συμπεριλαμβάνει όλους τους μηχανισμούς και τεχνολογίες που συμμετέχουν στην ολοκλήρωση μιας εμπορικής συναλλαγής μέσω υπολογιστή. Παραδείγματα τέτοιων μηχανισμών είναι **η Ηλεκτρονική Ανταλλαγή Δεδομένων (Electronic Data Interchange - EDI)** που ορίζει μία τυποποιημένη μορφή ανταλλαγής πληροφοριών και το e-mail.

Η πρακτική, που συνήθως ακολουθείται από τις επιχειρήσεις που υποστηρίζουν το ηλεκτρονικό εμπόριο, είναι η ακόλουθη:

- Αρχικά δημιουργείται μία θέση (Web Site) στον Παγκόσμιο Ιστό, στο οποίο υπάρχουν κατάλογοι και διαφήμιση των προϊόντων τους.
- Μέσα από τις ιστοσελίδες τους, παρέχουν στους καταναλωτές τη δυνατότητα επικοινωνίας μαζί τους, είτε με την αποστολή γραπτών μηνυμάτων (e-mail) είτε με κλήση (συνήθως ατελώς) στο τηλεφωνικό τους κέντρο.
- Για την εξυπηρέτηση των πελατών υπάρχουν ειδικά εκπαιδευμένοι αντιπρόσωποι, οι οποίοι απαντούν στις κλήσεις, που δέχεται το τηλεφωνικό κέντρο και καλύπτουν τις ανάγκες των καταναλωτών.
- Δίνεται η δυνατότητα στους καταναλωτές να δώσουν παραγγελίες προϊόντων μέσω του Διαδικτύου, συνήθως με χρέωση της πιστωτικής τους κάρτας, αλλά ακόμη και με εξόφληση του τιμολογίου κατά την παραλαβή της παραγγελίας.
- Τα προϊόντα αποστέλλονται, είτε ηλεκτρονικά είτε φυσικά, και παραλαμβάνονται από τον πελάτη στη διεύθυνση που επιθυμεί.

Παρόλο που, αρχικά, υπήρχε η αντίληψη ότι το ηλεκτρονικό εμπόριο είναι κατάλληλο για συγκεκριμένα μόνο προϊόντα, όπως βιβλία, περιοδικά, ηλεκτρονικούς υπολογιστές, λογισμικό και CDs, σήμερα βλέπουμε ότι έχει επεκταθεί και σε άλλους τομείς, όπως έπιπλα, τρόφιμα, παιχνίδια, λουλούδια κ.ά. Αν και τα τελευταία χρόνια με τη ραγδαία εξάπλωση και χρήση του Διαδικτύου έχει αρχίσει να αναπτύσσεται σημαντικά, εντούτοις για να μπορέσει να φτάσει στο βαθμό ανάπτυξης, που όλοι θα επιθυμούσαν, χρειάζεται να λυθεί ένας αριθμός σημαντικών ζητημάτων, όπως η προστασία, η ασφάλεια και η νομική κάλυψη των εμπλεκομένων.

Ερωτήσεις - Ασκήσεις Κεφαλαίου

1. Τι είναι το Σύστημα Ονομασίας Περιοχών (DNS);
2. Αναφέρετε τους βασικούς κανόνες ονοματολογίας του χώρου ονομάτων DNS καθώς και ένα παράδειγμα εφαρμογής τους.
3. Σε ποια επίπεδα χωρίζεται η ιεραρχική αρχιτεκτονική της υπηρεσίας DNS;
4. Πώς ονομάζονται οι εξυπηρετητές του Συστήματος Ονομασίας Περιοχών (DNS) και ποια εργασία επιτελούν;
5. Τι ονομάζουμε ανάλυση ονομάτων (name resolution);
6. Το όνομα paris.uoa.gr αντιστοιχεί σε περιοχή ονομάτων 2^{ου} επιπέδου.
   α. Σωστό.
   β. Λάθος.
7. Περιγράψτε το μοντέλο πελάτη-εξυπηρετητή (client-server).
8. Τι είναι η υπηρεσία του ηλεκτρονικού ταχυδρομείου (e-mail);
9. Ποια τα πλεονεκτήματα και ποια τα μειονεκτήματα της υπηρεσίας e-mail;
10. Ποια είναι τα πρωτόκολλα TCP/IP που χρησιμοποιούνται για την παράδοση και παραλαβή της ηλεκτρονικής αλληλογραφίας;
11. Ποιες οι διαφορές των πρωτοκόλλων FTP και TFTP;
12. Τι είναι ο παγκόσμιος ιστός και ποιο πρωτόκολλο χρησιμοποιεί;
13. Τι είναι οι εξυπηρετητές ιστού (web servers) και ποιος ο ρόλος τους;
14. Τι είναι οι φυλλομετρητές; Αναφέρετε μερικούς.
15. Τι είναι το telnet;
16. Ποια η κυριότερη διαφορά του πρωτοκόλλου FTP από το πρωτόκολλο Telnet;
17. Τι είναι το VoIP;
18. Ποια προβλήματα παρουσιάζονται κατά τη μετάδοση φωνητικής τηλεφωνίας μέσω του Διαδικτύου;
19. Ποια είναι τα πλεονεκτήματα του πρωτοκόλλου SIP;
20. Περιγράψτε σε βήματα πως επιτυγχάνεται η συνομιλία σε πραγματικό χρόνο με τη μορφή κειμένου στο Διαδίκτυο (chat).
21. Ποια ήταν τα σημαντικότερα προβλήματα που έπρεπε να ξεπεραστούν για τη μετάδοση εικόνας και ήχου μέσω του Διαδικτύου;
22. Τι είναι το ηλεκτρονικό εμπόριο;

Άσκηση σε Εργαστηριακό Περιβάλλον

Προσπαθήστε να εξοικειωθείτε με τις υπηρεσίες του Διαδικτύου κάνοντας χρήση των κατάλληλων εργαλείων, π.χ. nslookup για DNS, ελεύθερου λογισμικού για e-mail (thunderbird), ftp (filezilla), www (firefox), chat και περιηγηθείτε σε ιστοσελίδες ηλεκτρονικού εμπορίου.

Βιβλιογραφία

Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). *Τεχνολογία Δικτύων Επικοινωνιών* (1η έκδ.). Αθήνα: ΟΕΔΒ.

Ι.Δ.ΕΚ.Ε., "*Ψυχαγωγία και Ενημέρωση με τη Χρήση Νέων Τεχνολογιών*", Γ.Γ. Εκπαίδευσης Ενηλίκων, Ι.Δ.ΕΚ.Ε., http://repository.edulll.gr/edulll/retrieve/3473/1037.pdf

rfwireless-world, *FTP vs TFTP | difference between FTP and TFTP,* ανακτημένο από: http://www.rfwireless-world.com/Terminology/FTP-vs-TFTP.html

Εργαστήριο Δικτύων Υπολογιστών του Ε.Μ.Π., *Το σύστημα ονομασίας περιοχών DNS,* ανακτημένο από: http://old-courses.cn.ntua.gr/file.php/56/mathima11-12_dns.pdf

Χρήστος Ι. Μπούρας (2004, Ιούνιος), *Τηλεματική και Νέες Υπηρεσίες,* Πανεπιστημιακές Σημειώσεις, Πάτρα

Χρήστος Ι. Μπούρας, (2008, Ιούνιος), *Δίκτυα Δημόσιας* Χρήσης *και Διασύνδεση Δικτύων,* Πανεπιστημιακές Σημειώσεις, Πάτρα

Κεφάλαιο 7ο

ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΟΥ

Εισαγωγή

Τα σύγχρονα δίκτυα δεδομένων αποτελούνται από πολλά και διαφορετικά στοιχεία, τα οποία πρέπει να επικοινωνούν μεταξύ τους και να μοιράζονται δεδομένα και πόρους του δικτύου. Όσο μεγαλύτερο είναι ένα δίκτυο τόσο πιο δύσκολο είναι να αντιμετωπιστεί μια δυσλειτουργία ή μια βλάβη σε αυτό. Για αυτό το σκοπό υπάρχουν συστήματα διαχείρισης δικτύων. Τα συστήματα αυτά βοηθούν τους διαχειριστές να διατηρούν τη λειτουργία των δικτύων που επιβλέπουν στα επίπεδα απόδοσης για τα οποία σχεδιάστηκαν και υλοποιήθηκαν.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 7ου κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- ορίζουν την έννοια και να διατυπώνουν τη σημασία της Διαχείρισης Δικτύου
- απαριθμούν τις επιμέρους περιοχές που εφαρμόζεται η Διαχείριση Δικτύου
- γνωρίζουν τα βασικά πρωτόκολλα διαχείρισης δικτύου και τον τρόπο λειτουργίας τους

Διδακτικές Ενότητες

7.1 Η αναγκαιότητα της Διαχείρισης Δικτύου.
7.2 Περιοχές/τομείς διαχείρισης δικτύου στο μοντέλο OSI.
7.3 Πρότυπα Διαχείρισης.

7.1 Η αναγκαιότητα της Διαχείρισης Δικτύου

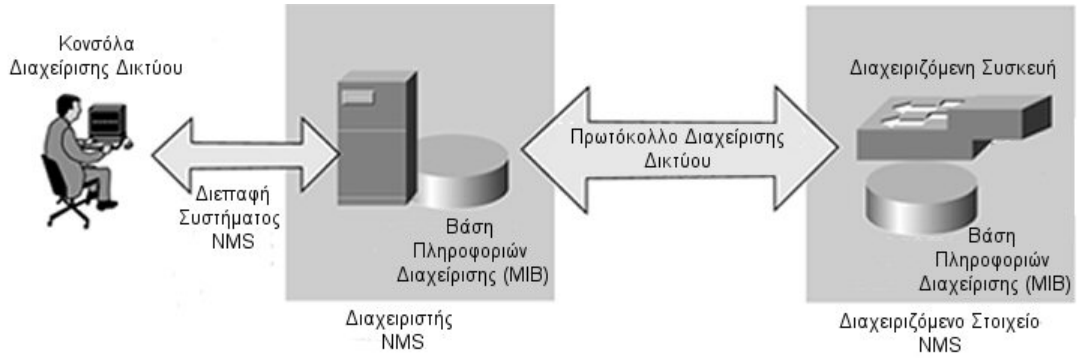
Ένα δίκτυο ηλεκτρονικών υπολογιστών (Η/Υ) είναι μια σύνθετη δομή που περιλαμβάνει τους Η/Υ και τις περιφερειακές συσκευές που συνδέονται σε αυτό, την καλωδίωση του κτιρίου και τις συσκευές που υποστηρίζουν τη λειτουργία των δικτυακών υπηρεσιών. Η **σύνθετη αυτή δομή καθιστά σχεδόν υποχρεωτική την ύπαρξη ενός συστήματος παρακολούθησης και διαχείρισης του δικτύου** για να μπορεί ένας διαχειριστής:

- να **εντοπίζει** στο συντομότερο δυνατό χρόνο την εστία του προβλήματος,
- να **επιδιορθώνει** το πρόβλημα και
- να **αποκαθιστά τη λειτουργία** και τις υπηρεσίες του δικτύου στα επίπεδα προδιαγραφών για τα οποία σχεδιάστηκε.

Για την αποτελεσματική διαχείριση ενός δικτύου δεδομένων είναι χρήσιμο, αν όχι απαραίτητο για τα μεγάλα σε μέγεθος δίκτυα, ο σχεδιασμός και η εγκατάσταση ενός **Συστήματος Διαχείρισης Δικτύου (Network Management System, NMS)**.

Ένα **Σύστημα Διαχείρισης Δικτύου (NMS)** είναι ένας συνδυασμός εργαλείων υλικού ή/και λογισμικού, τα οποία επιτρέπουν στο διαχειριστή να επιβλέπει τα επιμέρους στοιχεία από τα οποία αποτελείται ένα δίκτυο και να το ελέγχει για σημεία με προβληματική λειτουργία σε σχέση με τα αποδεκτά επίπεδα λειτουργίας.

Για το σκοπό αυτό έχουν σχεδιαστεί πρότυπα Διαχείρισης Δικτύου για αποτελεσματικότερη κάλυψη όλων των παραμέτρων που απαιτούνται για την ομαλή λειτουργία ενός δικτύου.



Εικόνα 7.1.α: Βασική δομή Συστήματος Διαχείρισης Δικτυού (NMS)

(Προσαρμοσμένη από Πηγή: http://etutorials.org/Networking/Lan+switching+first-step/Chapter+11.+Switch+Network+Management/Protocols/)

7.2 Περιοχές/τομείς διαχείρισης δικτύου στο μοντέλο OSI

Το **μοντέλο διαχείρισης δικτύου τηλεπικοινωνιών του οργανισμού OSI**, το οποίο ονομάζεται και FCAPS, αποτελεί το πλέον διαδεδομένο πλαίσιο για τη διαχείριση δικτύου. Το όνομα FCAPS προκύπτει από τις έννοιες **Fault** (**σφάλμα**), **Configuration** (**παραμετροποίηση**), **Accounting** (**κόστος**), **Performance** (**επίδοση**), **Security** (**ασφάλεια**). Αυτές είναι και οι κατηγορίες τις οποίες το μοντέλο OSI ορίζει σχετικά με τη διαχείριση δικτύου και τις επί μέρους διεργασίες που πρέπει να γίνονται για να την εξασφαλίσουν.

7.2.1 Παραμετροποίηση

Η **διαχείριση παραμετροποίησης (Configuration management, CM)** ασχολείται με την παρακολούθηση των πληροφοριών των παραμέτρων του δικτύου και τις όποιες αλλαγές συμβαίνουν σε αυτό.

Σκοπός της είναι η διατήρηση της συνοχής του δικτύου και όλων των λειτουργικών προδιαγραφών του. Η περιοχή διαχείρισης αυτή είναι ιδιαίτερα σημαντική, γιατί αρκετά προβλήματα στη λειτουργία των δικτύων προκύπτουν από τις αλλαγές σε παραμέτρους αρχείων, ενημερώσεις λογισμικού ή αλλαγές στο υλικό του συστήματος.

Μια σωστή διαχείριση παραμετροποίησης περιλαμβάνει την καταγραφή όλων των αλλαγών που συμβαίνουν στο υλικό και το λογισμικό του δίκτυο και κατά συνέπεια **καταγραφή όλων των στοιχείων εκείνων που πρέπει να παρακολουθούνται**. Αν και η παρακολούθηση των αλλαγών μπορεί να γίνει και χωρίς χρήση ειδικού λογισμικού καταγραφής, η πιο συνήθης πρακτική για τη συλλογή των απαραίτητων πληροφοριών είναι η **χρήση ενός λογισμικού διαχείρισης παραμετροποίησης**, όπως τα CiscoWorks 2000 ή Infosim.

Η διαχείριση παραμετροποίησης περιλαμβάνει τους στόχους:

- τη **συλλογή και αποθήκευση παραμέτρων των συσκευών** δικτύου, τοπικά ή από απόσταση
- την **απλοποίηση της παραμετροποίησης των συσκευών**
- την **παρακολούθηση αλλαγών** που συμβαίνουν στις παραμέτρους
- τη **διαμόρφωση κυκλωμάτων μέσα από δίκτυα χωρίς μεταγωγή** (non-switched networks)
- τον **σχεδιασμό μελλοντικών επεκτάσεων**

Η διαχείριση παραμετροποίησης, τόσο για τις παραμέτρους υλικού όσο και για αυτές του λογισμικού, αποτελείται από πέντε ξεχωριστές δράσεις:

:

- **Σχεδιασμός και Διαχείριση CM**. Περιλαμβάνει καταγραφή όλων των στοιχείων για το σχεδιασμό της παραμετροποίησης και ορισμό των διαδικασιών και των εργαλείων για την ολοκληρωμένη διαχείρισή τους.
- **Ταυτοποίηση Παραμετροποίησης**. Ορίζει τις βασικές προδιαγραφές του δικτύου, των υποδικτύων, των επί μέρους στοιχείων τους και όλων των αλλαγών/βελτιώσεων που γίνονται σε αυτά.
- **Έλεγχος Παραμετροποίησης.** Περιλαμβάνει τον έλεγχο και την αξιολόγηση όλων των αιτημάτων και προτάσεων για αλλαγές/βελτιώσεις και τις αντίστοιχες εγκρίσεις ή απορρίψεις τους.
- **Κοστολόγηση Κατάστασης Παραμετροποίησης.** Περιλαμβάνει τη διαδικασία καταγραφής του υλικού και λογισμικού των αντικειμένων του δικτύου και τις παρεκκλίσεις στην υλοποίησή του δικτύου σε σχέση με τον αρχικό σχεδιασμό.
- **Επαλήθευση και αξιολόγηση παραμετροποίησης.** Προβλέπει μια έκθεση του υλικού και του λογισμικού και αξιολογεί τη συμβατότητά τους με τις καθορισμένες προδιαγραφές απόδοσης.

7.2.2 Διαχείριση Σφαλμάτων

Για τη διατήρηση της σωστής λειτουργίας ενός δικτύου πρέπει να υπάρχει μέριμνα για την καλή λειτουργία τόσο ολόκληρου του δικτύου όσο και των επιμέρους στοιχείων του. Υπάρχει διαφορά ανάμεσα στις έννοιες σφάλμα/βλάβη και λάθος σε ένα δίκτυο.

Το **σφάλμα ή βλάβη** είναι μια μη φυσιολογική κατάσταση που απαιτεί την προσοχή του διαχειριστή και την άμεση διόρθωσή του. Ένα σφάλμα συνεπάγεται μη σωστή λειτουργία ή μεγάλο αριθμό λαθών (πχ. Όταν μια γραμμή επικοινωνίας είναι κομμένη και δεν διέρχεται σήμα ή υπάρχει υπερβολικά μεγάλος αριθμός από λανθασμένα bit).

Το **λάθος** είναι ένα μεμονωμένο γεγονός, που συνήθως δεν συνεπάγεται διακοπή της επικοινωνίας. Στην περίπτωση ύπαρξης λαθών (πχ. λάθος bit στη γραμμή επικοινωνίας) υπάρχει δυνατότητα αντιστάθμισης των συνεπειών τους με τη χρήση μηχανισμών ελέγχου λαθών στα διάφορα πρωτόκολλα που χρησιμοποιούνται.

Ο εντοπισμός ενός σφάλματος γίνεται είτε με τη **παρατήρηση ενδείξεων** από την κίνηση του δικτύου σε πραγματικό χρόνο (πχ. μη αποδεκτή καθυστέρηση στο άνοιγμα σελίδων Διαδικτύου ή άλλων δικτυακών υπηρεσιών), είτε σε **μορφή συναγερμού** (alarm) αν υπάρχει εγκατεστημένο και σωστά παραμετροποιημένο ένα Σύστημα Διαχείρισης Δικτύου.

Όταν συμβεί κάποιο σφάλμα υπάρχουν συγκεκριμένα βήματα για την επίλυση του, τα οποία ονομάζονται **Κύκλος Επεξεργασίας Διαχείρισης Σφαλμάτων** (Fault Management Process Cycle). Σύμφωνα με αυτόν και αφού συμβεί το σφάλμα, τα συνήθη βήματα που πρέπει να ακολουθούν είναι τα παρακάτω:

- Να **προσδιοριστεί** το σφάλμα, δηλαδή τι είδους σφάλμα είναι και από πού μπορεί να προέρχεται.
- Να **εντοπιστεί** το σφάλμα, ώστε να ανακαλυφθεί από ποιο σημείο του δικτύου βρίσκεται.
- Να **απομονωθεί** το υπόλοιπο του δικτύου, ώστε να μπορεί αυτό να λειτουργεί χωρίς παρεμπόδιση από το σφάλμα.
- Να **αναδιαμορφωθεί το δίκτυο**, ώστε να ελαχιστοποιηθεί η επίδραση της βλάβης σε κάποιο ή κάποια από στοιχεία του.
- Να γίνει **έλεγχος και ανάλυση** των ενδείξεων, ώστε να κατανοηθεί καλύτερα η αιτία και να δοθεί μια πληρέστερη εξήγηση της πηγής του σφάλματος.

- Να **επισκευαστεί ή να αντικατασταθεί** το στοιχείο της βλάβης, ώστε να επανέλθει το δίκτυο στην αρχική του κατάσταση.
- Να **παρακολουθηθεί το δίκτυο** από τον Διαχειριστή για ένα προκαθορισμένο χρονικό διάστημα, ώστε να βεβαιωθεί ότι το σφάλμα επιλύθηκε με επιτυχία.

Η επίδραση που έχει ένα σφάλμα στο δίκτυο μπορεί να μετριαστεί με τη χρήση επιπλέον στοιχείων/μονάδων δικτύου ή με την αλλαγή στη διαδρομή επιτυγχάνοντας έτσι ένα βαθμό ανοχής του δικτύου στα σφάλματα.

Για να μπορεί να επιτευχθεί γρήγορη επίλυση του προβλήματος χρειάζεται να γίνει γρήγορη και αξιόπιστη ανίχνευση και διάγνωση σφαλμάτων, ώστε να υπάρχει η μικρότερη δυνατή επιβάρυνση στη λειτουργία του δικτύου.

Δραστηριότητα 1η (Στο σχολικό εργαστήριο)

1. Χωριστείτε σε ομάδες.
2. Αναπτύξτε ύστερα από συζήτηση των μελών σας το εξής θέμα: *«Η υπηρεσία του Διαδικτύου στο σχολικό εργαστήριο σταματά να λειτουργεί. Καταγράψτε τα βήματα που θα πρέπει να πραγματοποιήσετε, σύμφωνα με το πρότυπο διαχείρισης σφάλματος του OSI, ώστε να εντοπίσετε και να επιλύσετε αυτό το σφάλμα στις υπηρεσίες του σχολικού εργαστηρίου».*
3. Να γίνει παρουσίαση των λύσεων που προτείνει κάθε ομάδα.
4. Να επιλεγεί από τους μαθητές ποια λύση προτείνεται ως η πιο αποτελεσματική με συνδυασμό των προτάσεων.
5. Πραγματοποιήστε μια αυτοψία στο δίκτυο του σχολικού εργαστηρίου, ώστε να εφαρμόσετε τα βήματα της λύσης που επιλέξατε και να διορθώσετε σφάλμα.

7.2.3 Διαχείριση Επιδόσεων

Η **Διαχείριση Επιδόσεων (Performance Management ή Capacity Management)** επικεντρώνεται στη διασφάλιση ότι η απόδοση του δικτύου παραμένει στα αποδεκτά επίπεδα, αυτά για τα οποία σχεδιάστηκε να λειτουργεί.

Μελετά το χρόνο απόκρισης του δικτύου, την απώλεια πακέτων, τη χρήση των γραμμών επικοινωνίας, τα ποσοστά χρήσης, το βαθμό λαθών που συμβαίνουν κ.α. Αυτές οι πληροφορίες συνήθως συλλέγονται με την εφαρμογή ενός συστήματος διαχείρισης δικτύου, όπως είναι το πρωτόκολλο SNMP, με τους εξής τρόπους:

- με **συνεχή παρακολούθηση** και εκτίμηση από το διαχειριστή της τρέχουσας κατάστασης
- με **ορισμό συναγερμών,** όταν τα επίπεδα απόδοσης ανέβουν ή κατέβουν από τα προκαθορισμένα και αποδεκτά επίπεδα

Η σωστά σχεδιασμένη **στρατηγική συλλογής και ανάλυσης των δεδομένων** απόδοσης του δικτύου επιτρέπει στους διαχειριστές των δικτύων:

- Να πιστοποιήσουν την αποτελεσματικότητα και την αξιοπιστία του δικτύου.
- Να προβλέψουν τα προβλήματα πριν αυτά συμβούν.
- Να επανασχεδιάσουν τη διάταξη του δικτύου για ακόμα καλύτερες επιδόσεις.
- Να προετοιμάσουν το δίκτυο για μελλοντικές βελτιώσεις.

Για το σκοπό αυτό πρέπει ο διαχειριστής του δικτύου να επικεντρώσει την προσοχή του στην παρακολούθηση κάποιων **επιλεγμένων πόρων του δικτύου,** για να μπορέσει να εκτιμήσει καλύτερα την κατάσταση.

7.2.4 Διαχείριση Κόστους

Η **διαχείριση κόστους (Accounting Management ή Billing Management)** ασχολείται με την παρακολούθηση των πληροφοριών που σχετίζονται με τη χρήση των πόρων ενός δικτύου και του κόστους που συνεπάγεται από αυτή τη χρήση.

Μάλιστα σε πολλές επιχειρήσεις και οργανισμούς υπάρχει χρέωση για τις προσφερόμενες υπηρεσίες του δικτύου. Ωστόσο, **στα δίκτυα που δεν έχουν στόχο το κέρδος, η έννοια του κόστους (Accounting)** μερικές φορές **αντικαθιστάται από την έννοια της διοίκησης (Administration)**.

Ο σκοπός της διαχείρισης κόστους, ανάλογα με την περίπτωση, είναι:

Για τις επιχειρήσεις με στόχο το κέρδος:

- Ο **υπολογισμός του σωστού ποσού χρέωσης** των υπηρεσιών στους αντίστοιχους χρήστες, ομάδες χρηστών, οργανισμούς ή επιχειρήσεις.

Για οργανισμούς χωρίς στόχο το κέρδος:

- Η **δημιουργία μιας κοστολόγησης της χρήσης των πόρων** του δικτύου ανά χρήστη ή ανά τμήμα, για τον καλύτερο προσδιορισμό λειτουργιών, όπως λήψη αντιγράφων ασφαλείας ή συγχρονισμός δεδομένων.

Η διαχείρισης κόστους επίσης στοχεύει να εντοπιστούν οι χρήστες ή ομάδα χρηστών που:

- **Παραβιάζουν τα δικαιώματα πρόσβασης** και επιβαρύνουν το δίκτυο.
- Μπορεί να κάνουν **μη αποτελεσματική χρήση του δικτύου.**

Θα πρέπει ο διαχειριστής του δικτύου να ορίσει τις παραμέτρους που θα καταγράφονται στους διάφορους κόμβους, τα χρονικά διαστήματα που θα καταγράφονται, καθώς επίσης και τον αλγόριθμο που θα χρησιμοποιηθεί για την κοστολόγηση. Σε περίπτωση που δεν απαιτείται χρέωση, τα δεδομένα που θα συλλεχθούν θα βοηθήσουν στη λήψη αποφάσεων για τη βελτίωση της απόδοσης.

Δραστηριότητα 2η (Στην αίθουσα διδασκαλίας)

1. Μελετώντας τις ακόλουθες πληροφορίες από τις παραμέτρους σε ένα δίκτυο, τι συμπεράσματα μπορούμε να βγάλουμε για τη λειτουργία του δικτύου;
   - Χαμηλό το επίπεδο χρήσης της χωρητικότητας.
   - Αυξημένη κυκλοφορία.
   - Ρυθμός απόδοσης είναι σε μη αποδεκτά επίπεδα.
   - Συνωστισμός δεδομένων σε κάποιο σημείο.
   - Αύξηση του χρόνου απόκρισης κάποιας δικτυακής υπηρεσίας.
2. Με βάση τις παραπάνω πληροφορίες, ποια πιθανή λύση ή ρύθμιση προτείνετε με σκοπό τη βελτίωση της απόδοσης του δικτύου;

7.2.5 Διαχείριση Ασφάλειας

Η **διαχείριση ασφάλειας (Security Management)** ενός δικτύου ασχολείται με τη διαχείριση πληροφοριών που σχετίζονται με:

- την **ομαλή λειτουργία** του δικτύου.
- την παρακολούθηση και τον **έλεγχο της πρόσβασης** σε τμήματα του ή και σε όλο το δίκτυο,
- την **ασφάλεια των δεδομένων** που διακινούνται και αποθηκεύονται στο αυτό.

Για να ολοκληρωθεί το έργο της διαχείρισης ασφάλειας ενός δικτύου, πρέπει σε τακτά χρονικά διαστήματα να συλλέγονται και να αναλύονται οι απαραίτητες πληροφορίες που σχετίζονται με τους παραπάνω τομείς ελέγχου. Για το σκοπό αυτό απαιτείται η **χρήση εργαλείων λογισμικού**, όπως:

- Πλατφόρμες συλλογής και ελέγχου δικτυακών δεδομένων (NMS Platforms)
- Εργαλεία κρυπτογράφησης (cryptography tools)
- Εργαλεία αυθεντικοποίησης (authentication) για έλεγχο πρόσβασης
- Συστήματα ελέγχου εισβολέων (intrusion detection systems)
- Διαμόρφωση και ενεργοποίηση δικτυακού τείχους προστασίας (network firewall)
- Εφαρμογή μεθόδων-πολιτικών ασφαλείας (security policies)
- Ημερολόγια καταγραφής (logs) κ.ά.

Κάθε ένα από τα παραπάνω εργαλεία στοχεύει να καλύψει επιμέρους τις ανάγκες ασφαλείας ενός δικτύου. Καθώς κάθε ένα από αυτά έχει διαφορετική φιλοσοφία χρήσης και αποτέλεσμα, καθιστά την διαχείριση ασφαλείας ενός δικτύου μια αρκετά περίπλοκη διαδικασία.

Για να είναι **αποτελεσματική** η διαχείριση ασφαλείας ενός δικτύου πρέπει να προβλεφθούν όλες οι πιθανές αιτίες ή τα σημεία κινδύνου, ώστε να επιλεγούν τα σημεία όπου χρειάζονται μεγαλύτερη προσοχή από τους διαχειριστές.

Στη συνέχεια να εγκατασταθεί το απαραίτητο λογισμικό στα σημεία του δικτύου που απαιτείται, ώστε να τους βοηθήσει να παρακολουθούν, να προστατεύουν και να εντοπίζουν τις πηγές κινδύνου στο συντομότερο χρονικό διάστημα.

Δραστηριότητα 3η (Στην αίθουσα διδασκαλίας)

Αντιστοιχίστε τα παρακάτω εργαλεία ασφάλειας (δεξιά στήλη) με τις ανάγκες των τομέων ασφαλείας (αριστερή στήλη) που καλύπτουν.

Την ομαλή λειτουργία του δικτύου.	Α.	1. Πλατφόρμες συλλογής και ελέγχου δικτυακών δεδομένων (NMS Platforms).
		2. Εργαλεία κρυπτογράφησης (cryptography tools).
Την παρακολούθηση και τον έλεγχο της πρόσβασης σε τμήματα του ή και σε όλο το δίκτυο.	Β.	3. Εργαλεία αυθεντικοποίησης (authentication) για έλεγχο πρόσβασης.
		4. Συστήματα ελέγχου εισβολέων (intrusion detection systems).
Την ασφάλεια των δεδομένων που διακινούνται και αποθηκεύονται στο δίκτυο.	Γ.	5. Διαμόρφωση και ενεργοποίηση δικτυακού τείχους ασφαλείας (network firewall).
		6. Εφαρμογή μεθόδων-πολιτικών ασφαλείας (security policies).
		7. Ημερολόγια καταγραφής (logs)

Δικαιολογήστε τις επιλογές σας.

7.3 Πρότυπα Διαχείρισης

Τα **βασικά συστατικά** ή οντότητες από τα οποία αποτελείται ένα τυπικό **Σύστημα Διαχείρισης Δικτύου** είναι:

- Ο Διαχειριστής Δικτύου (Manager Server)
- Ο Αντιπρόσωπος (Agent)
- Η Βάση Πληροφοριών Διαχείρισης (Management Information Base, MIB)

Τα πιο γνωστά **Πρότυπα Διαχείρισης Δικτύου (Network Management, NM)**, τα οποία υλοποιούν συστήματα διαχείρισης είναι τα:

- Το SNMP (Simple Network Management Protocol) του Διαδικτύου
- Το CMIP (Common Management Information Protocol) του OSI

7.3.1 Βασικά συστατικά συστήματος διαχείρισης (MS - MIB - AGENT)

Ο **Διαχειριστής Δικτύου (Manager Server)** είναι ένας ή περισσότεροι Η/Υ, ο οποίος διαχειρίζεται τα στοιχεία του δικτύου που έχουν επιλεγεί γι' αυτό το σκοπό.

Συνήθως έχει εγκατεστημένες διάφορες εφαρμογές και λογισμικό και, ανάλογα με το σχεδιασμένο σύστημα διαχείρισης δικτύου, πραγματοποιεί τις εξής βασικές λειτουργίες:

- Αποστέλλει αιτήματα στους αντιπροσώπους που είναι εγκατεστημένοι στο δίκτυο.
- Λαμβάνει απαντήσεις από τους αντιπροσώπους.
- Ορίζει μεταβλητές παρακολούθησης στους αντιπροσώπους.
- Παρακολουθεί τους συναγερμούς (alarms).
- Προσφέρει κατάλληλο περιβάλλον διεπαφής χρήστη για την καλύτερη παρακολούθηση των πληροφοριών του δικτύου.

Ένας **Αντιπρόσωπος Δικτύου (Agent)** είναι ένα λογισμικό που εκτελείται σε κάθε δικτυακή υπό διαχείριση συσκευή ή σύστημα.

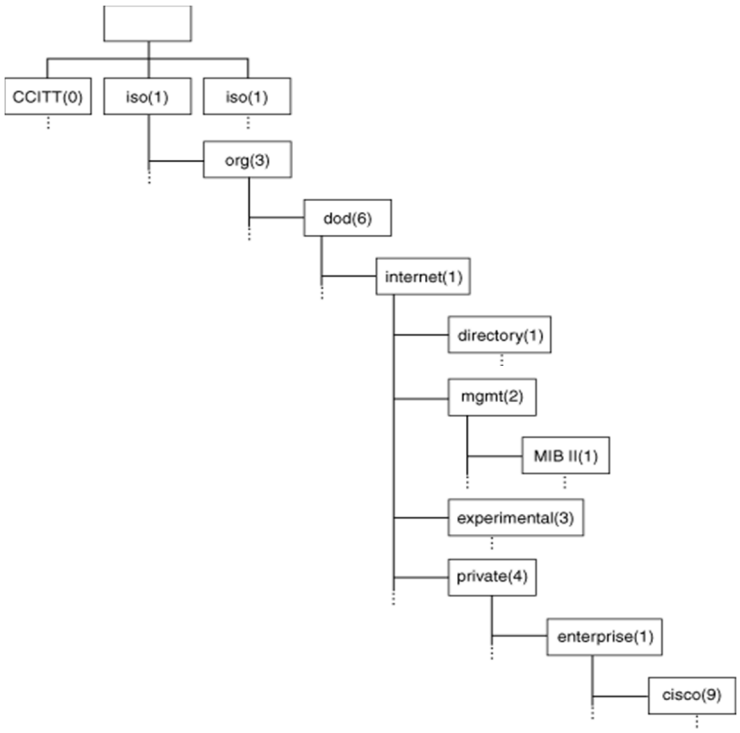
Βασικές λειτουργίες του είναι:

- η συλλογή πληροφοριών από τα διαχειριζόμενα αντικείμενα του δικτύου
- η διαμόρφωση των παραμέτρων των διαχειριζόμενων αντικειμένων
- η απάντηση στα αιτήματα των διαχειριστών δικτύου
- η δημιουργία συναγερμών και η αποστολή τους στους διαχειριστές

Μια **Βάση Πληροφοριών Διαχείρισης (Management Information Base, MIB)** είναι ένα σχήμα αποθήκευσης πληροφοριών σε μια βάση δεδομένων, που χρησιμοποιείται για τη διαχείριση των αντικειμένων/οντοτήτων σε ένα δίκτυο τηλεπικοινωνιών, όπως Η/Υ, εκτυπωτές, δρομολογητές, διανομείς κτλ.

Η δομή της είναι ιεραρχική, μοιάζει με ανεστραμμένο δέντρο και κάθε φύλλο είναι ένα διαχειριζόμενο αντικείμενο, το οποίο αντιστοιχεί σε έναν πόρο του συστήματος. Κάθε εισαγωγή πληροφορίας γίνεται μέσω μιας ακολουθίας αριθμών που ονομάζεται **Ταυτοποίηση Αντικειμένου OID (Object Identifier)**.

Οι MIBs χρησιμοποιούν δομές **πινάκων**, δηλαδή αντικείμενα με πολλές μεταβλητές. Οι πίνακες έχουν μηδέν ή περισσότερες εγγραφές και τα συστήματα NMS τις διαχειρίζονται χρησιμοποιώντας **εντολές**, όπως **ανάκτηση**, **ανάκτηση επόμενης** ή **ενημέρωση**.



Εικόνα 7.3.1.α: Παράδειγμα δομής MIB του προτύπου SNMP

7.3.2 Πρωτόκολλο SNMP

Το **SNMP (Simple Network Management Protocol)** είναι ένα πρωτόκολλο που σχεδιάστηκε από τον οργανισμό IAB (Internet Architecture Board) για την ανταλλαγή πληροφοριών μεταξύ των δικτυακών συσκευών και αποτελεί μέρος του Επίπεδου Εφαρμογών του μοντέλου TCP/IP.

Το SNMP παρακολουθεί τα γεγονότα που συμβαίνουν σε ένα δίκτυο, ώστε ενημερώνει τον διαχειριστή. Ένα **δικτυακό γεγονός** μπορεί να είναι οτιδήποτε μπορεί να προκαλέσει αδυναμία συνδεσιμότητας, όπως η απώλεια γραμμής επικοινωνίας, και το SNMP μπορεί να το αντιληφθεί παρακολουθώντας για παράδειγμα το μέγεθος της κίνησης σε μια σύνδεση. Οποιαδήποτε συσκευή με τεχνολογία TCP/IP μπορεί να παρακολουθηθεί μέσω του πρωτοκόλλου SNMP.

Το πρωτόκολλο αποτελείται από:

- **Διαχειριστή/ές SNMP** (SNMP Manager)
- **Διαχειριζόμενες Συσκευές** (Managed devices)
- **Αντιπροσώπους SNMP** (SNMP agents)
- **Μια Βάση Πληροφοριών Διαχείρισης** (MIB)

Βασικός τρόπος λειτουργίας SNMP. Σε μια τυπική χρήση του πρωτοκόλλου SNMP, υπάρχει ένας αριθμός συστημάτων υπό διαχείριση καθώς και ένα ή περισσότερα συστήματα διαχείρισης. Το λογισμικό που εκτελείται σε κάθε δικτυακή υπό διαχείριση συσκευή ή σύστημα ονομάζεται **αντιπρόσωπος (agent)** και αναφέρει μέσω του πρωτοκόλλου SNMP στα συστήματα διαχείρισης. Η επικοινωνία του SNMP γίνεται μεταξύ των συσκευών και του σταθμού διαχείρισης του δικτύου, ο οποίος προβάλει τις πληροφορίες στο διαχειριστή.

Στη βασική του μορφή, το SNMP συλλέγει δεδομένα διαχείρισης τα οποία οργανώνονται σε ιεραρχικές δομές MIBs, όπως οι **SMI SNMPv1 και SNMPv2** (Structure of Management Information).

Με χρήση **μεταβλητών,** όπως free memory (διαθέσιμη μνήμη), system name (όνομα συστήματος), number of running processes (αριθμός εκτελούμενων διεργασιών), και **εντολών,** μπορεί και συλλέγει δεδομένα από τις συσκευές του δικτύου και ενημερώνει τον διαχειριστή για την κατάσταση τους. Επίσης, επιτρέπει ενέργειες, όπως η εφαρμογή **νέας παραμετροποίησης ή η αλλαγή της υπάρχουσας** της δικτυακής διάταξης.

Στον πίνακα 7.3.2.α παρουσιάζονται οι βασικές εντολές του SNMP και οι ενέργειες με τις οποίες αυτές σχετίζονται.

Εντολές επικοινωνίας SNMP	Ενέργεια
Get	ανάκτηση δεδομένου
GetNext	ανάκτηση επόμενου δεδομένου
GetBulk	μαζική ανάκτηση δεδομένων
Set	ορισμός τιμής μεταβλητής
Inform	πληροφόρηση
Response	απάντηση
Trap	ειδοποίηση σημαντικού γεγονότος

Πίνακας 7.3.2.α Βασικές εντολές του SNMP

Όπως παρατηρούμε στην εικόνα 7.3.2.α, η οποία παρουσιάζει σχηματικά τη διαχείριση μιας δικτυακής συσκευής με ενσωματωμένο Αντιπρόσωπο SNMP, λαμβάνουν χώρα τα εξής βήματα κατά την επικοινωνία:

Παράδειγμα εντολής **Set:**

- Ο **Διαχειριστής Δικτύου,** μέσω του **Σταθμού Διαχείρισης,** ξεκινά την επικοινωνία στέλνοντας την εντολή Set προς έναν **Αντιπρόσωπο SNMP**.
- Στη συνέχεια ενημερώνεται η τιμή ενός αντικείμενου-OID στον **Αντιπρόσωπο SNMP**, ο οποίος είναι εγκατεστημένος σε μια **Διαχειριζόμενη Συσκευή** του Δικτύου.

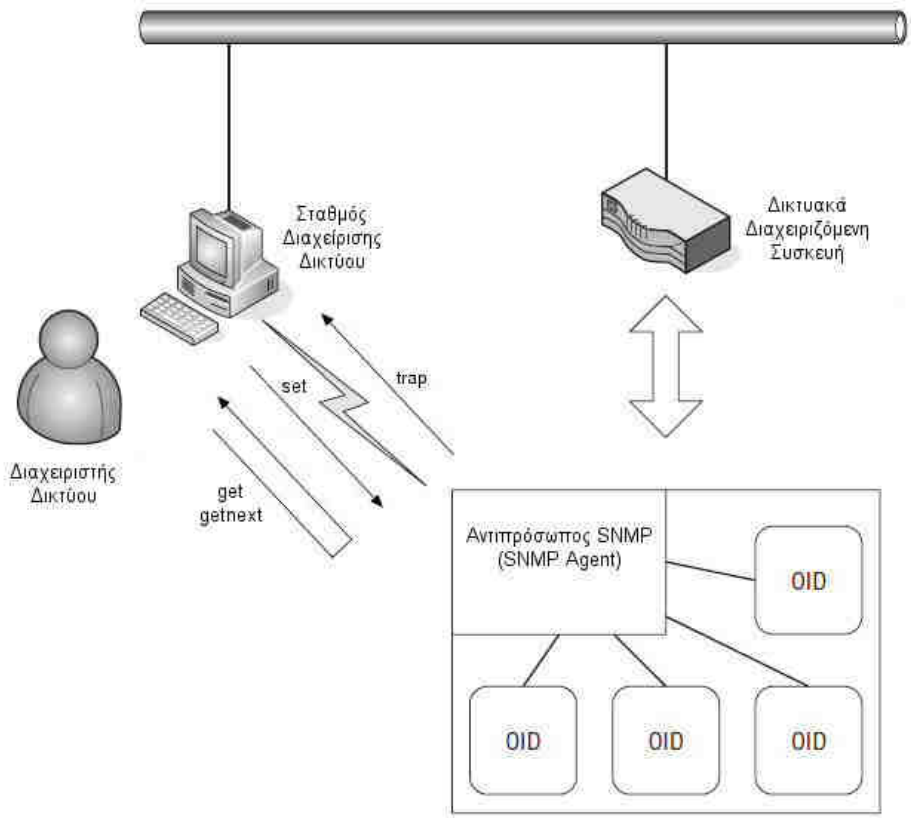
Παράδειγμα εντολής **Get:**

- Ο **Διαχειριστής Δικτύου,** μέσω του **Σταθμού Διαχείρισης,** ξεκινά την επικοινωνία στέλνοντας την εντολή Get προς έναν **Αντιπρόσωπο SNMP**.
- Στη συνέχεια ο **Σταθμός Διαχείρισης** λαμβάνει μια απάντηση με την τιμή ενός αντικείμενου-OID από τον **Αντιπρόσωπο SNMP**, ο οποίος είναι εγκατεστημένος σε μια **Διαχειριζόμενη Συσκευή** του Δικτύου.
- Ο **Διαχειριστής Δικτύου,** μέσω του **Σταθμού Διαχείρισης,** ενημερώνεται για την τιμή του αντικείμενου-OID από την απομακρυσμένη **Δικτυακή Συσκευή**.

Παράδειγμα εντολής **Trap:**

- Ο **Αντιπρόσωπος SNMP**, ο οποίος είναι εγκατεστημένος σε μια **Διαχειριζόμενη Συσκευή** του Δικτύου, δημιουργεί και αποστέλλει μια εντολή Trap προς τον **Σταθμό Διαχείρισης**.
- Ο **Διαχειριστής Δικτύου,** μέσω του **Σταθμού Διαχείρισης,** ενημερώνεται για το συμβάν που έλαβε χώρα στην απομακρυσμένη **Δικτυακή Συσκευή**.

Διευκρινίζουμε ότι τα αντικείμενα-OID βρίσκονται μέσα στις δομές MIB των Διαχειριζόμενων Συσκευών.



Εικόνα 7.3.2.α: Διαχείριση δικτυακής συσκευής με ενσωματωμένο Αντιπρόσωπο SNMP.

Το SNMP έχει εμφανιστεί στις εκδόσεις SNMP v1, SNMP v2c, SNMP v2u, SNMP v2 και στην πιο πρόσφατη SNMP v3, οι οποίες είναι εμπλουτισμένες με περισσότερες εντολές και καλύπτουν με διαφορετικό τρόπο τα επίπεδα ασφάλειας της αυθεντικοποίησης και της ακεραιότητας, όπως φαίνεται στον πίνακα 7.3.2.2.

Έκδοση SNMP	**Αυθεντικοποίηση**	**Κρυπτογράφηση**
SNMP v1	Χρήση Συμβολοσειράς (Community String)	Όχι
SNMP v2c	Χρήση Συμβολοσειράς (Community String)	Όχι
SNMP v2u	Χρήση Ονόματος Χρήστη (Username)	Όχι
SNMP v3	Χρήση αλγορίθμων MD5 ή SHA	Χρήση αλγορίθμων DES 56-bit ή AES-28

Πίνακας 7.3.2.β: Οι εκδόσεις του SNMP και οι δυνατότητες ασφάλειας τους.

 **Δραστηριότητα 4η (Στην αίθουσα διδασκαλίας)**

Κατά τη λειτουργία του πρωτοκόλλου SNMP σε ένα δίκτυο υπάρχουν τα ακόλουθα στοιχεία:

- Διαχειριστής Δικτύου (άνθρωπος)
- Σταθμός Διαχειριστής Δικτύου
- Διαχειριζόμενη συσκευή 1
- Αντιπρόσωπος συσκευής 1
- MIB συσκευής 1
- Διαχειριζόμενη συσκευή 2
- Αντιπρόσωπος συσκευής 2
- MIB συσκευής 2
- Εντολή GET
- Εντολή SET
- Εντολή TRAP
- Εντολή GETBULK

Πραγματοποιήστε ένα παιχνίδι ρόλων αναλαμβάνοντας να υποδυθείτε ένα από τα παραπάνω στοιχεία. Στη συνέχεια υλοποιήστε τα ακόλουθα σενάρια:

1. Εκτέλεση εντολής GET
2. Εκτέλεση εντολής SET
3. Εκτέλεση εντολής GETBULK
4. Αποστολή εντολής TRAP

Μετά την ολοκλήρωση της αναπαράστασης εκτέλεσης των εντολών, συζητήστε στην ολομέλεια της τάξης:

- Τι σας προβλημάτισε από τον τρόπο λειτουργίας του SNMP;
- Ποιοι είναι οι βασικοί συντελεστές που προκαλούν την εκτέλεση μιας εντολής;
- Σας φάνηκε περίπλοκη η λειτουργία του; Ναι ή όχι και γιατί;

7.3.3 Πρωτόκολλο CMIP

Το **CMIP (Common Management Information Protocol)** είναι ένα πρωτόκολλο διαχείρισης δικτύου του μοντέλου επικοινωνίας OSI, για την ανταλλαγή πληροφοριών μεταξύ εφαρμογών διαχείρισης δικτύου και των διαχειριζόμενων αντιπροσώπων.

Το CMIP αποτελεί έναν ανταγωνιστή του SNMP και επιτρέπει τη δικτυακή διαχείριση συσκευών διαφορετικών οργανισμών αλλά και κατασκευαστών. Υλοποιείται σε συνεργασία με τα πρωτόκολλα ACSE και ROSE, τα οποία είναι πρωτόκολλα του επιπέδου εφαρμογής του OSI:

- Το **ACSE** (Association Control Service Element) χρησιμοποιείται για να διαχειριστεί τις διασυνδέσεις ανάμεσα στις διαχειριζόμενες συσκευές, όπως την επικοινωνία μεταξύ του διαχειριστή και των CMIP αντιπροσώπων (CMIP agents).
- Το **ROSE** (Remote Operation Service Element) χρησιμοποιείται για όλες τις ανταλλαγές δεδομένων του CMIP.

Βασικός τρόπος λειτουργίας CMIP. Το πρωτόκολλο CMIP απαιτεί την εγκαθίδρυση ενός συσχετισμού μεταξύ των διαχειριζόμενων συσκευών πριν την έναρξη οποιασδήποτε άλλης επικοινωνίας και ανταλλαγής δεδομένων. Αυτό γίνεται με τη χρήση υπηρεσιών

συσχετισμού του CMIS. Το **CMIS (Common Management Information Services)** περιλαμβάνει ένα σύνολο υπηρεσιών, οι οποίες χρησιμοποιούνται για τη πρόσβαση και τον έλεγχο των δικτυακών στοιχείων και συσκευών. Στη συνέχεια με τη χρήση των υπηρεσιών ειδοποίησης και διαχείρισης του CMIS μπορεί να μεταφέρει δεδομένα διαχείρισης από και προς τις διαχειριζόμενες δικτυακές συσκευές.

Όπως προαναφέραμε το CMIS περιλαμβάνει υπηρεσίες συσχετισμού, ειδοποίησης και διαχείρισης, όπως αυτές φαίνονται στον πίνακα 7.3.3.α.

Υπηρεσίες CMIS	Ενέργειες
Υπηρεσίες συσχετισμού	
M-INITIALISE	δημιουργία συσχετισμού μεταξύ συσκευών
M-TERMINATE	διακοπή συσχετισμού μεταξύ συσκευών
M-ABORT	απότομη διακοπή συσχετισμού μεταξύ συσκευών
Υπηρεσίες ειδοποίησης	
M-EVENT-REPORT	αποστολή γεγονότων
Υπηρεσίες διαχείρισης	
M-GET	ανάκτηση ιδιότητας
M-SET	ορισμός ιδιότητας
M-ACTION	απαίτηση εκτέλεσης μιας ενέργειας
M-CREATE	δημιουργία ενός αντικειμένου διαχείρισης
M-DELETE	διαγραφή ενός αντικειμένου διαχείρισης

Πίνακας 7.3.3.α: Υπηρεσίες του CMIS

Ωστόσο, παρόλο που το CMIP προσφέρει πολύ περισσότερες λειτουργίες σε σχέση με το SNMP, οι δικτυακές συσκευές του Διαδικτύου υποστηρίζουν το πρωτόκολλο SNMP και όχι το CMIP. Αυτό συμβαίνει γιατί τα συστήματα διαχείρισης και οι αντιπρόσωποι του CMIP είναι πολύ πιο περίπλοκα και έχουν μεγαλύτερες απαιτήσεις σε πόρους συστήματος για τη λειτουργία τους.

7.3.4 Έλεγχος και παρατήρηση δικτύου με χρήση NMS

Όπως προαναφέραμε, ένα **Σύστημα Διαχείρισης Δικτύου (NMS)** είναι ένας συνδυασμός εργαλείων υλικού ή/και λογισμικού, τα οποία επιτρέπουν στο διαχειριστή να επιβλέπει τα επιμέρους στοιχεία από τα οποία αποτελείται ένα δίκτυο και να το ελέγχει για σημεία με προβληματική λειτουργία σε σχέση με τα αποδεκτά επίπεδα λειτουργίας.

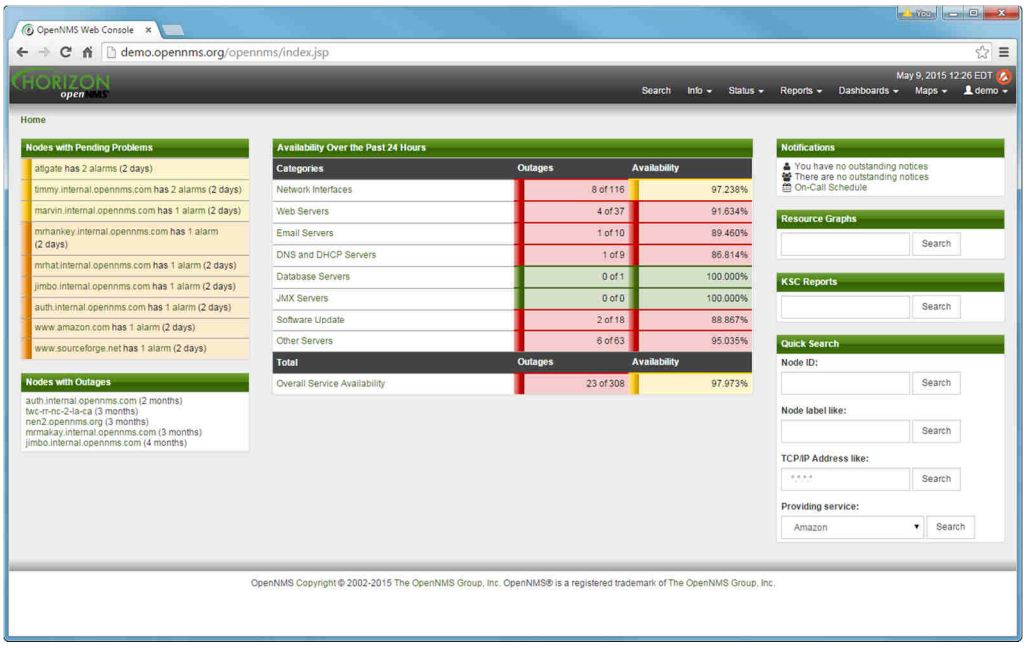
Το NMS **παρακολουθεί εσωτερικά διαρκώς το δίκτυο** για τμήματα με αργή λειτουργία ή αδυναμία απόκρισης, που πιθανό να οφείλονται σε υπερφόρτωση γραμμών, διακομιστές ή συσκευές εκτός λειτουργίας, υπηρεσίες χωρίς απόκριση, γραμμές χωρίς επικοινωνία κ.ά. και **ειδοποιεί τον διαχειριστή** μέσω e-mail, μηνύματος SMS ή κάποια άλλη μορφή συναγερμού.

Παραδείγματα για το πως μπορεί να **πραγματοποιήσει ελέγχους** είναι να στείλει αίτημα προβολής μιας ιστοσελίδας (HTML request) σε ένα Διακομιστή Ιστοσελίδων (Web Server) ή να στείλει ένα e-mail μέσω του SMTP σε ένα Διακομιστή Ηλεκτρονικής Αλληλογραφίας

(Email Server). Επίσης χρησιμοποιεί **προκαθορισμένες τιμές μετρήσεων**, όπως ο χρόνος απόκρισης, η διαθεσιμότητα, χρόνος λήξης κτλ.

Ουσιαστικά ένα NMS αποτελείται από στοιχεία που αναλαμβάνουν:

- **Εντοπισμό συσκευών δικτύου,** αυτόματο εντοπισμό ενός διαχειριζόμενου αντικειμένου, όπως ένας διανομέας, όταν αυτό συνδέεται στο δίκτυο.
- **Παρακολούθηση συσκευών δικτύου**, ώστε να έχουν υγιή λειτουργία και να ανταποκρίνονται στις προκαθορισμένες απαιτήσεις απόδοσής τους.
- **Ανάλυση απόδοσης δικτύου**, με παρακολούθηση χρήσης εύρους ζώνης, απώλειας πακέτων χρόνου λήξης και άλλες συσκευές με ενεργοποιημένο πρωτόκολλο SNMP.
- **Έξυπνες ειδοποιήσεις** με ορισμό συναγερμών για τα αντίστοιχα σενάρια προβλημάτων και αποστολή ειδοποιήσεων στους διαχειριστές.



Εικόνα 7.3.4.α: Παράθυρο διαχείρισης δικτύου με χρήση Demo OpenNMS

Σύστημα Διαχείρισης Δικτύου με χρήση πρωτοκόλλου SNMP. Όπως προαναφέραμε, υπάρχουν εφαρμογές NMS που υποστηρίζουν το πρωτόκολλο SNMP, καθώς πολλές συσκευές, ανεξαρτήτως κατασκευαστή, έχουν ενσωματωμένους SMNP agents και διευκολύνουν την παρακολούθησή τους μέσω του πρωτοκόλλου. Για να μπορέσει μια συσκευή να εντοπιστεί και να παρακολουθηθεί, αρκεί να αναγνωριστεί και να ενσωματωθεί στο λογισμικό του NMS το σχήμα MIB που απαιτείται για να γίνει η διαχείριση της συσκευής.

Γενικότερα τα NMS με χρήση πρωτοκόλλου SNMP επιτρέπουν:

- τη συλλογή δεδομένων από οποιαδήποτε προέλευση SNMP
- την επιλογή των αντικειμένων IOD που θα παρακολουθηθούν
- την υποστήριξη SNMP πινάκων και δημιουργία προσαρμοσμένων MIBs
- τη λήψη SNMP παγίδων (traps) από εφαρμογές και συσκευές του δικτύου
- τη διαμόρφωση συναγερμών και τιμών ορίων παρακολούθησης

Η εγκατάσταση ενός NMS δεν μπορεί από μόνη της να κάνει αποτελεσματική τη διαχείριση και έλεγχο του δικτύου. Για να συμβεί αυτό, οι διαχειριστές οφείλουν να ορίσουν στο σύστημα τους κατάλληλους συναγερμούς, στα κατάλληλα σημεία, ώστε να εντοπίζονται και να αντιμετωπιστούν τα προβληματικά σημεία σε διακομιστές, εφαρμογές και επικοινωνία, πριν αυτά εξελιχθούν σε πολύ σοβαρότερες βλάβες.

Η εφαρμογή με την πλατφόρμα διαχείρισης NMS εγκαθίστανται σε ένα σταθμό εργασίας, επικοινωνεί με τις δικτυακές συσκευές και συλλέγει δεδομένα από τις πληροφοριακές βάσεις (MIB) τους. Οι πληροφορίες προβάλλονται, είτε στο παράθυρο/κονσόλα διαχείρισης της εφαρμογής είτε ως απλές τιμές, είτε ως στατιστικά, είτε με μορφή γραφημάτων για καλύτερη κατανόηση τους από τους διαχειριστές.

Παραδείγματα NMS λογισμικού είναι τα Microsoft Nerwork Monitor, OpenNMS, Net-SNMP, Pandora FMS κ.ά.

Ερωτήσεις – Ασκήσεις Κεφαλαίου

1. Τι είναι ένα Σύστημα Διαχείρισης Δικτύου (NMS);
2. Τι δυνατότητες προσφέρει ένα σύστημα παρακολούθησης και διαχείρισης του δικτύου στον διαχειριστή;
3. Ποιους τομείς διαχείρισης περιλαμβάνει το μοντέλο διαχείρισης δικτύου τηλεπικοινωνιών του οργανισμού OSI;
4. Με τι ασχολείται η Διαχείριση Παραμετροποίησης (CM) του μοντέλου Διαχείρισης Δικτύων του OSI;
5. Ποιοι είναι ο στόχοι της Διαχείρισης Παραμετροποίησης του μοντέλου Διαχείρισης Δικτύων του OSI;
6. Αναφέρετε ονομαστικά τις πέντε δράσεις από τις οποίες αποτελείται η Διαχείριση Παραμετροποίησης του μοντέλου OSI, τόσο για το υλικό όσο και για το λογισμικό.
7. Τι εργασίες περιλαμβάνει ο *Σχεδιασμός και Διαχείριση CM* και ο *Έλεγχος Παραμετροποίησης* στην περιοχή Διαχείρισης Παραμετροποίησης του μοντέλου OSI;
8. Τι εργασίες περιλαμβάνει *η Ταυτοποίηση Παραμετροποίησης*, η *Κοστολόγηση Κατάστασης Παραμετροποίησης* και η *Επαλήθευση και Αξιολόγηση Παραμετροποίησης* στην περιοχή Διαχείρισης Παραμετροποίησης του μοντέλου OSI;
9. Τι είναι το σφάλμα και το λάθος και ποια η διαφορά τους, σύμφωνα με τη Διαχείριση Σφαλμάτων του μοντέλου OSI;
10. Με ποιο τρόπο μπορεί ο διαχειριστής δικτύου να εντοπίσει ένα σφάλμα στο δίκτυο;
11. Από ποια βήματα αποτελείται ο Κύκλος Επεξεργασίας Διαχείρισης Σφαλμάτων (Fault Management Process Cycle);
12. Τι είναι η Διαχείριση Επιδόσεων (Performance Management) του μοντέλου Διαχείρισης Δικτύων του OSI;
13. Τι οφείλει να κάνει ο διαχειριστής δικτύου κατά την Διαχείριση Επιδόσεων του μοντέλου OSI, ώστε να καταστρώσει μια αποτελεσματική στρατηγική συλλογής και ανάλυσης των δεδομένων απόδοσης του δικτύου;
14. Τι προσφέρει στον διαχειριστή δικτύου μια σωστά σχεδιασμένη στρατηγική συλλογής και ανάλυσης των δεδομένων απόδοσης του δικτύου;
15. Τι είναι η Διαχείριση Κόστους (Accounting Management) του μοντέλου Διαχείρισης Δικτύων του OSI;
16. Ποιος είναι ο σκοπός της Διαχείρισης Κόστους του μοντέλου Διαχείρισης Δικτύων του OSI, ανάλογα με το στόχο του εκάστοτε οργανισμού ή επιχείρησης;
17. Τι είναι η Διαχείριση Ασφαλείας (Security Management) του μοντέλου Διαχείρισης Δικτύων του OSI;
18. Τι πρέπει να πραγματοποιηθεί, ώστε να είναι αποτελεσματική η Διαχείριση Ασφαλείας του μοντέλου Διαχείρισης Δικτύων του OSI;
19. Τι είναι ο Διαχειριστής Δικτύου (Manager Server) και ποιες είναι οι βασικές λειτουργίες που επιτελεί;
20. Τι είναι ο Αντιπρόσωπος Δικτύου (Agent) και ποιες είναι οι βασικές λειτουργίες που επιτελεί;
21. Τι είναι η Βάση Πληροφοριών Διαχείρισης (Management Information Base, MIB) και ποια είναι η δομή της;
22. Τι είναι το πρωτόκολλο SNMP (Simple Network Management Protocol) και από ποια βασικά στοιχεία αποτελείται;
23. Τι είναι ένα δικτυακό γεγονός σύμφωνα με το πρωτόκολλο SNMP;
24. Πώς λειτουργεί το πρωτόκολλο SNMP;
25. Ποιες είναι οι βασικές εντολές του πρωτοκόλλου SNMP;

26. Ποια διαφορά έχει η πρώτη έκδοση SNMPv1 του πρωτοκόλλου SNMP με την πιο πρόσφατη έκδοση SNMPv3 αναφορικά με τα στοιχεία ασφάλειας της αυθεντικοποίησης και της ακεραιότητας;
27. Τι είναι το πρωτόκολλο CMIP (Common Management Information Protocol) και από ποια βασικά στοιχεία αποτελείται;
28. Ποια είναι τα δύο βασικά πρωτόκολλα που χρησιμοποιεί το CMIP, γιατί χρησιμοποιούνται και σε ποιο επίπεδο του μοντέλου OSI βρίσκονται;
29. Πως λειτουργεί το πρωτόκολλο CMIP;
30. Ποιες είναι οι βασικές υπηρεσίες του CMIS ανάλογα με την εργασίες που επιτελούν;

Ασκήσεις σε εργαστηριακό περιβάλλον

1. Μπείτε στην ιστοσελίδα του Demo OpenNMS (http://demo.opennms.org/opennms/index.jsp) και μελετήστε το περιβάλλον διαχείρισης δικτύου που προσφέρει.
   - Πλοηγηθείτε στους διακομιστές και δείτε τα στοιχεία που προβάλλονται στην οθόνη διαχείρισης.
   - Εντοπίστε ένα συναγερμό και δείτε την αιτία του.
   - Αναζητήστε μια διαχειριζόμενη συσκευή από την IP διεύθυνσή της.
   - Δείτε ένα γράφημα (μενού Reports->Charts) και συζητήστε τι συμπεράσματα βγάζετε από αυτά σχετικά με τη λειτουργία του δικτύου.
2. Εγκαταστήστε στο εργαστήριο μια εφαρμογή διαχείρισης δικτύου, ανάλογα με το περιβάλλον λειτουργικού συστήματος που είναι διαθέσιμο. Προτείνονται οι:

   OpenNMS (http://www.opennms.org/get-opennms/)

   Net-SNMP (http://www.net-snmp.org/download.html)

   ή όποια άλλη έχετε ήδη εγκατεστημένη στο εργαστήριό σας.

   - Μελετήστε το περιβάλλον διαχείρισης που προσφέρει η εγκατεστημένη εφαρμογή.
   - Εκτελέστε ένα παράδειγμα εντολής GET και δείτε τα αποτελέσματά της.

Βιβλιογραφία

Arne Mikalsen, P. B. (2002). *Local Area Network Management, Design and Security*. Wiley.

Asante. (2005). *Simple Network Managemet protocol*. Asante Inc.

Anttalainen T., (2003), *Introduction to Telecommunications Network Engineering*, Second Edition, Artech House

James Edwards, R. B. (2009). *Networking - OSI, TCP/IP, LANs, MANs, WANs, Implementation, Management and Maintenance*. Indianapolis: Wiley.

McCabe J, (2007), *Network Analysis, Architecture, and Design*, 3rd edition, Elsevier Inc., Morgan Kaufmann Publishers

The Internet Engineering Task Force (IETF), *IETF-related tools, standalone or hosted on tools.ietf.org*, https://tools.ietf.org/html/rfc1095.

Κεφάλαιο 8ο

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

Εισαγωγή

Σ' αυτό το κεφάλαιο θα μελετήσουμε την αναγκαιότητα της προστασίας των πληροφοριακών συστημάτων και των επικοινωνιών τους. Αρχικά θα γίνει μια προσπάθεια αναγνώρισης του προβλήματος, δηλαδή από ποιον και γιατί πρέπει να προστατευθούν τα πληροφοριακά συστήματα και οι επικοινωνίες τους. Κατόπιν θα μελετήσουμε τις βασικές έννοιες της ασφάλειας δικτύων και τέλος θα περιγράφουν οι τεχνικές και τα μέτρα αντιμετώπισης απειλών.

Διδακτικοί Στόχοι

Με την ολοκλήρωση του 8^{ου} κεφαλαίου οι μαθητές θα πρέπει να είναι σε θέση να:

- ορίζουν τις βασικές έννοιες της ασφάλειας πληροφοριών
- διατυπώνουν τους κινδύνους και τις αδυναμίες των δικτύων Η/Υ
- εφαρμόζουν μεθόδους και εργαλεία αναγνώρισης της παραβίασης της ασφάλειας και προστασίας της
- εφαρμόζουν τρόπους, μεθόδους και εργαλεία, ώστε να μπορούν να διασφαλίσουν τη διαθεσιμότητα των πόρων και των πληροφοριών ενός υπολογιστικού συστήματος - δικτύου
- χρησιμοποιούν και να ρυθμίζουν στοιχειωδώς το τείχος προστασίας (firewall) ενός Η/Υ - δικτύου
- εξηγούν τη σημασία της ασφάλειας πληροφοριών και δικτύων στο περιβάλλον μιας σύγχρονης επιχείρησης

Διδακτικές Ενότητες

8.1 Βασικές έννοιες Ασφάλειας δεδομένων.
8.2 Εμπιστευτικότητα - ακεραιότητα - διαθεσιμότητα - αυθεντικότητα – εγκυρότητα.
8.3 Αδυναμίες – κίνδυνοι.
8.4 Μέθοδοι και Τεχνικές προστασίας.

8.1 Βασικές έννοιες Ασφάλειας δεδομένων

Για να κατανοήσει κάποιος την έννοια της ασφάλειας, πρέπει να απαντήσει στα ερωτήματα τι σημαίνει η ασφάλεια για τον καθένα από εμάς, ποιοι είναι αυτοί που προσπαθούν να παραβιάσουν την ασφάλεια και ποιες είναι οι προθέσεις τους.

Για τους περισσότερους από εμάς, όταν σκεφτόμαστε την ασφάλεια σε σχέση με την τεχνολογία και τους υπολογιστές, εννοούμε ότι κάποιος θέλει να υποκλέψει τον αριθμό της πιστωτικής μας κάρτας ή τον τραπεζικό λογαριασμό μας για προφανείς λόγους. Από την άλλη μεριά, αν κάποιος είναι άνθρωπος που επιδρά και επηρεάζει κοινωνικοπολιτικά με τον τρόπο ζωής του και την δουλειά του, πιθανόν κάποιοι να ενδιαφέρονταν για τις πληροφορίες που αποθηκεύει στις ηλεκτρονικές συσκευές του και για τις πληροφορίες που μεταφέρει μέσω των δημοσίων δικτύων και να προσπαθήσουν να υποκλέψουν κάποιες πληροφορίες από το ηλεκτρονικό του ταχυδρομείο. Σε γενικές γραμμές, ο μέσος άνθρωπος είναι αδιάφορος πέραν των πληροφοριών που πιθανόν αποθηκεύει στους υπολογιστές και ανταλλάσσει μέσω ηλεκτρονικών συναλλαγών, των οποίων η υποκλοπή μπορεί να αποφέρει κάποιο οικονομικό όφελος.

Παρ' όλα αυτά, ας υποθέσουμε ότι γενικότερα ασφάλεια είναι η προσπάθεια προστασίας από εξωτερικές επιβουλές των πληροφοριών και των συστημάτων, κατά την διάρκεια της λειτουργίας τους ή κατά τη διάρκεια επικοινωνίας με άλλα ηλεκτρονικά πληροφοριακά συστήματα.

Σ' αυτό το σημείο πρέπει να διευκρινίσουμε τι είναι αυτό που πρέπει να προστατεύσουμε.

Πόρος πληροφοριακού Συστήματος ή Αγαθό (Asset). Κάθε αντικείμενο ή πόρος που ανήκει ή υποστηρίζει ένα πληροφοριακό σύστημα και το οποίο αξίζει να προστατευθεί.

Τα αγαθά είναι:

- Κτίρια, Υπολογιστές, Δικτυακή Υποδομή,
- Έπιπλα, κτλ
- Αρχεία (ηλεκτρονικά, έντυπα)
- Λογισμικό Εφαρμογών, Λειτουργικά Συστήματα, κτλ.

Όμως ποιος επιβουλεύεται την ασφάλεια των συστημάτων και των επικοινωνιών;

Αν γυρίσουμε πίσω στον δεύτερο παγκόσμιο πόλεμο να δούμε ένα παράδειγμα. Ας υποθέσουμε ότι είμαστε στην θέση των Γερμανών και θέλουμε να επικοινωνήσουμε μεταφέροντας μηνύματα για τις θέσεις που πρόκειται να πλήξει η αεροπορία σε όλη την Ευρώπη. Όλες οι ελεύθερες κυβερνήσεις τις κόσμου με κάθε τεχνολογικό μέσο θα προσπαθούσαν να υποκλέψουν αυτές τις πληροφορίες.

Επομένως ο πρώτος που έχει λόγους να παραβιάσει την ασφάλεια πληροφοριών και επικοινωνιών, καθώς και το αντίθετο να τις προστατεύσει με κάθε τρόπο και πιθανότητα διαθέτει και το καλύτερο εξοπλισμό, είναι οι κυβερνήσεις. Βασικό στοιχείο στην ασφάλεια είναι να καθορίσουμε ποιοι είμαστε και από ποιον θέλουμε να προστατευθούμε, δηλαδή ποιος είναι ο καλός και ποιος ο κακός.

Η συνήθης τακτική που ακολουθεί συνήθως μια εταιρεία ή ένας οργανισμός με πολλούς εργαζόμενους και πελάτες είναι να απευθυνθεί σε συμβούλους ασφάλειας. Η θεωρία που υποστηρίζεται από αυτούς είναι “όσο περισσότερη ασφάλεια επιτευχθεί τόσο καλύτερα”. Στη πραγματικότητα όμως ισχύει ότι **δεν υπάρχει απόλυτη ασφάλεια** και βασίζεται στην ιδέα ότι η απόλυτη ασφάλεια μπορεί να επιτευχθεί μόνο, όταν δεν διαχειριζόμαστε ευαίσθητα δεδομένα και όταν δεν υπάρχουν μυστικά που πρέπει να μεταδοθούν.

Βασιζόμενοι σ' αυτή τη θεωρία **η ασφάλεια που μπορεί να πετύχει κάποιος βασίζεται πάντα σε μια ανάλυση αντιστάθμισης τους κόστους και των ωφελημάτων που μπορούν να επιτευχθούν**, αντίθετα με τους ειδικούς ασφάλειας που υποστηρίζουν ότι πρέπει να επενδυθούν όσο το δυνατόν περισσότερα χρήματα, ώστε να επιτευχθεί η απόλυτη προστασία των πληροφοριών και επικοινωνιών. Για παράδειγμα σε μια τράπεζα ποιο είναι το μέγεθος της επένδυσης που κάνει στην ασφάλεια; Και αν ο αριθμός μιας πιστωτικής κάρτας που χάθηκε διαρρεύσει, ποιες είναι οι συνέπειες; Είναι πολλά τα παραδείγματα με περιπτώσεις που έγιναν αγορές με αντίγραφα πιστωτικών καρτών σε πόλεις ή και χώρες που δεν είχε επισκεφτεί ποτέ του ο κάτοχος της πιστωτικής κάρτας. Ποια είναι η επίδραση από τέτοια περιστατικά στην αξιοπιστία της τράπεζας και ποιο το κόστος σε αντιστάθμισμα με την επένδυση στην ασφάλεια που έχει κάνει;

Οι συνέπειες από την παραβίαση της ασφάλειας ενός αγαθού μπορεί να είναι άμεσες οικονομικές συνέπειες, όπου μπορεί εύκολα να μετρηθεί το κόστος τους, όπως για παράδειγμα η επαναγορά ενός υλικού μετά την καταστροφή, όμως μπορεί να υπάρχουν και έμμεσες συνέπειες που δεν είναι εύκολο να υπολογιστεί το κόστος. Για παράδειγμα, αν μια τράπεζα πέσει θύμα υποκλοπής των κωδίκων web banking, θα χαθεί η εμπιστοσύνη και μαζί θα χαθούν και οι πελάτες της. Ένα άλλο κόστος θα ήταν οι νόμιμες συνέπειες που πιθανόν να υπάρχουν ως αποτέλεσμα της παραβίασης ασφάλειας. Τέλος, αν το προϊόν που

παρέχει μια εταιρεία είναι υπηρεσίες που βασίζονται σε πληροφοριακά συστήματα και η παραβίαση της ασφάλειας προκάλεσε μόνιμη ή παροδική αδυναμία παροχής της υπηρεσίας (επίθεση DOS-Denial of service), το κόστος μη παροχής υπηρεσίας είναι ανυπολόγιστο πέρα από το κόστος που μπορεί να υπάρξει λόγω νομικών συνεπειών. Για παράδειγμα, αν μια τηλεπικοινωνιακή εταιρεία κινητής τηλεφωνίας δηλώσει αδυναμία να παρέχει κλήσεις, μηνύματα, Διαδίκτυο επί μια εβδομάδα, οι απώλειες πιθανόν να είναι ανυπολόγιστα μεγάλες.

8.2 Εμπιστευτικότητα - ακεραιότητα - διαθεσιμότητα - αυθεντικότητα – εγκυρότητα

Τέσσερα είναι τα βασικά προβλήματα που πρέπει να επιλύσει κάποιος κατά την ανάλυση και το σχεδιασμό του επίπεδου της ασφάλειας που θέλει να επιτύχει.

Το ένα αναφέρεται ως εμπιστευτικότητα των πληροφοριών και σχετίζεται με την πιθανότητα διαρροής πληροφοριών. Για παράδειγμα, όταν αποστέλλουμε τον αριθμό της πιστωτικής μας κάρτας, θέλουμε να το παραλάβει μόνο ο παραλήπτης και κανένας άλλος.

- **Εμπιστευτικότητα (Confidentiality)** είναι η αποτροπή της πρόσβασης σε ιδιωτικές πληροφορίες από άτομα που δεν έχουν εξουσιοδότηση.

Το δεύτερο βασικό πρόβλημα είναι να εξασφαλιστεί η αναγνωρισιμότητα της ταυτότητας αυτού που έχει πρόσβαση ή μεταδίδει τις πληροφορίες. Για παράδειγμα, όταν αποστέλλει κάποιος τον αριθμό της πιστωτικής του κάρτας, πρέπει να διασφαλιστεί με κάθε τρόπο ότι είναι και ο κάτοχος της κάρτας.

- **Αυθεντικοποίηση (authentication) ή πιστοποίηση ταυτότητας** είναι η εξασφάλιση ότι η πληροφορία προέρχεται από αυτόν που νομίζουμε ότι την μετέδωσε.

Το τρίτο πρόβλημα ορίζεται ως ακεραιότητα των πληροφοριών το οποίο σημαίνει ότι η μεταδιδόμενη πληροφορία δεν έχει υποστεί καμία αλλαγή κατά την αποστολή. Για παράδειγμα, αν κάποιος μπορούσε να αλλάξει το αριθμό λογαριασμού τραπέζης κατά πληρωμή μιας συναλλαγής για την αγορά ενός προϊόντος και έβαζε το δικό του λογαριασμό, θα ήταν παραβίαση της ακεραιότητας.

Σ' αυτό το σημείο είναι σημαντικό να διευκρινιστεί ποιος είναι ο **εξουσιοδοτούμενος**, δηλαδή ποιος έχει συγκεκριμένα δικαιώματα πρόσβασης και επεξεργασίας στις πληροφορίες και στα μέσα για τη διαχείρισή τους. Προφανώς εξουσιοδότηση έχει ο δημιουργός που αναφέρεται ως ιδιοκτήτης και κατ' επέκταση όλοι οι χρήστες στους οποίους έχει δώσει την άδεια με δικαιώματα μερικής ή πλήρους πρόσβασης.

- **Ακεραιότητα (integrity)** είναι η διασφάλιση ότι οι πληροφορίες έχουν υποστεί αλλαγές μόνο από εξουσιοδοτημένα άτομα.

Το τελευταίο βασικό ζήτημα είναι η πρόληψη στο σχεδιασμό της ασφάλειας ότι τα άτομα που συμμετέχουν σε ηλεκτρονικές επικοινωνίες και διαχειρίζονται εμπιστευτικές πληροφορίες να μην μπορούν να αρνηθούν την εμπλοκή τους.

- **Μη άρνηση ταυτότητας (Non repudiation)** ορίζεται ως η μη αποποίηση των ευθυνών εκ των υστέρων χρηστών που συμμετείχαν σε μια ηλεκτρονική επικοινωνία.

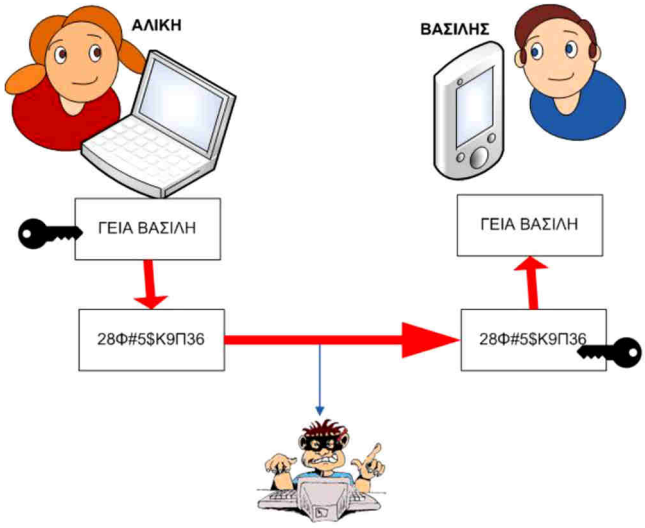
Συνήθως σε μια ηλεκτρονική επικοινωνία που μεταδίδονται ευαίσθητα δεδομένα είναι απαραίτητη η πιστοποίηση της ταυτότητας του χρήστη αλλά και η εξασφάλιση ότι τα δεδομένα δεν έχουν τροποποιηθεί από μη εξουσιοδοτημένο άτομο, δηλαδή ο συνδυασμός της αυθεντικότητας και της ακεραιότητας που είναι γνωστή ως εξασφάλιση της **Εγκυρότητας (Validity)** των πληροφοριών.

Τέλος σε μερικές περιπτώσεις όπου είναι απαραίτητο να διασφαλιστεί η αδιάλειπτη παροχή πρόσβασης σε πληροφορίες από εξουσιοδοτημένους χρήστες ορίζεται η έννοια της **διαθεσιμότητας** των πληροφοριών. Αν για παράδειγμα αρνούνταν ο δικτυακός τόπος ηλεκτρονικού ταχυδρομείου της Google σε μερικά εκατομμύρια λογαριασμούς την πρόσβαση στις πληροφορίες τους μετά από επίθεση hacker, θα ήταν παραβίαση της διαθεσιμότητας των πληροφοριών.

Λαμβάνοντας υπόψη όλα τα παραπάνω ζητήματα κατά το σχεδιασμό του επιπέδου ασφάλειας που θέλει να επιτύχει κάποιος ιδιώτης, εταιρεία, οργανισμός μπορεί να διατυπωθεί ένας γενικευμένος ορισμός για την ασφάλεια.

Ασφάλεια των πληροφοριών είναι η επίτευξη του σχεδιαζόμενου επιπέδου διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των πληροφοριών.

Για την επίλυση του πρώτου βασικού προβλήματος της εμπιστευτικότητας των πληροφοριών η πιο ευρέως χρησιμοποιούμενη μέθοδος είναι η τεχνική κρυπτογράφησης/ αποκρυπτογράφησης. Για παράδειγμα, ας θεωρήσουμε ότι δύο φίλοι θέλουν να επικοινωνήσουν ανταλλάσσοντας μηνύματα κειμένου με τις ηλεκτρονικές συσκευές τους μέσω του Διαδικτύου και δεν θέλουν όλος ο υπόλοιπος κόσμος να γνωρίζει για ποιο θέμα συζητάνε. Για το λόγο αυτό προσπαθούν με κάποιο μηχανισμό να τροποποιήσουν το αρχικό μήνυμά έτσι ώστε οποιοσδήποτε αποκτήσει πρόσβαση να είναι αδύνατο να το διαβάσει. Σε θέματα ασφάλειας θεωρούμε ότι πάντα κάποιος προσπαθεί να υποκλέψει πληροφορίες και πάντα έχει πιθανότητες να το επιτύχει. Τέλος, όταν το μήνυμα φτάσει στο προορισμό του, με αντίστροφο μηχανισμό το μήνυμα μετατρέπεται στην αρχική του μορφή ώστε να είναι αναγνωρίσιμο.



Εικόνα 8.2.α: Κρυπτογραφημένη Επικοινωνία

- **Κρυπτογράφηση ε**ίναι η εφαρμογή μια τεχνικής, συνήθως ενός μαθηματικού αλγορίθμου, μετατροπής πληροφορίας υπό μορφή απλού κειμένου σε μορφή μη αναγνωρίσιμη, έτσι ώστε κατά την αποθήκευση ή μεταφορά της να μην είναι προσβάσιμη από μη εξουσιοδοτημένα άτομα.
- **Αποκρυπτογράφηση** είναι η αντίστροφη τεχνική που εφαρμόζεται μόνο από εξουσιοδοτημένα άτομα σε κρυπτογραφημένη μη αναγνωρίσιμη πληροφορία, έτσι ώστε να μετασχηματιστεί στην αρχική μορφή απλού κειμένου.

Κρυπτογράφημα (Chiphertext) ορίζεται ο μετασχηματισμός του αρχικού απλού μηνύματος κειμένου (plain text) σε μορφή μη αναγνωρίσιμη από τον καθένα που δεν έχει το μηχανισμό αποκρυπτογράφησης.

Στη μεθοδολογία των τεχνικών κρυπτογράφησης και αποκρυπτογράφησης υπάρχει πάντα η έννοια κλειδί (key).

Κλειδί (key) μπορούμε να θεωρήσουμε ότι είναι ένας κωδικός από ψηφιακά δεδομένα που λειτουργεί σε συνδυασμό με κάποιον αλγόριθμο κρυπτογράφησης/αποκρυπτογράφησης.

Υπάρχουν δύο βασικοί τύποι κρυπτογραφικών συστημάτων: η κρυπτογράφηση με μυστικό κλειδί και η κρυπτογράφηση με δημόσιο κλειδί.

Στην κρυπτογράφηση με **μυστικό κλειδί (secret key)** ή **συμμετρικού κλειδιού (symmetric key**) χρησιμοποιείται το ίδιο κλειδί στη διαδικασία κρυπτογράφησης και στην διαδικασία αποκρυπτογράφησης, το οποίο όμως είναι γνωστό μόνο στους χρήστες που συμμετέχουν στην ηλεκτρονική επικοινωνία. Αντίθετα, στην κρυπτογράφηση με **δημόσιο κλειδί (public key)** χρησιμοποιείται ένα ζευγάρι **δημόσιου-ιδιωτικού** κλειδιού για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης, όπου το δημόσιο μεταδίδεται στους συμμετέχοντες δια μέσω ασφαλούς καναλιού των δημόσιων δικτύων, ενώ το ιδιωτικό παραμένει πάντα τοπικά αποθηκευμένο και προστατευμένο για χρήση.

8.2.1 Έλεγχος ακεραιότητας - συναρτήσεις κατακερματισμού - σύνοψη μηνύματος

Πριν μελετήσουμε λίγο βαθύτερα πώς εξασφαλίζουμε την εμπιστευτικότητα, δηλαδή πώς μπορούμε να κρύψουμε το περιεχόμενο του εμπιστευτικού μηνύματος από τα μάτια όσων θέλουν να δουν το περιεχόμενο του, θα ξεκινήσουμε εξετάζοντας το ζήτημα της εξασφάλισης της ακεραιότητας των πληροφοριών.

Ας υποθέσουμε ότι έχουμε ένα μήνυμά γραμμένο σε ένα κομμάτι χαρτί και με κάποιο τρόπο το έχουμε σφραγίσει, όπως στη ρωμαϊκή εποχή το δίπλωναν και το υπέγραφαν ρίχνοντας κερί και πριν στεγνώσει το κερί αποτύπωναν ένα σύμβολο με κάποια σφραγίδα που κατείχε μόνο ο αποστολέας. Με αυτό το τρόπο ταυτοποιούσαν τον αποστολέα και εξασφαλιζόταν την ακεραιότητα των περιεχομένων του έγγραφου. Τη σφραγίδα μπορούσε να τη σπάσει μόνο ο παραλήπτης και να διαβάσει τα περιεχόμενα του έγγραφου. Όμως πάντα υπάρχει η δυνατότητα να κλαπεί το αποτύπωμα και να γίνει αντίγραφο της σφραγίδας ή ακόμα και να κλαπεί η πραγματική σφραγίδα που συνήθως φύλασσαν επάνω τους οι κάτοχοι της. Επομένως κάποιοι θα μπορούσαν να καταφέρουν να παρέμβουν και να τροποποιήσουν τα περιεχόμενα των κρυπτογραφημένων μηνυμάτων και να εξαπατήσουν τον παραλήπτη.

Σήμερα στον κόσμο των υπολογιστών χρειαζόμαστε κάτι που να επιβεβαιώνει την ακεραιότητα των πληροφοριών. Για παράδειγμα, αν λάβουμε μέσω e-mail ένα κρίσιμο έγγραφο που χρειάζεται μια πιστοποίηση της ακεραιότητας των πληροφοριών που περιέχει, όπως μια βεβαίωση από τη εφορία ή την ιατρική γνωμάτευση ή ιατροφαρμακευτική συνταγή για την ασθένεια μας, πρέπει με κάποιο τρόπο ψηφιακά να υπογραφεί. Συνήθως περιέχει μια σειρά από χαρακτήρες, αριθμούς και γράμματα, σταθερού μήκους στο τέλος του μηνύματος, ώστε με τον έλεγχο στον υπολογιστή μας να επιβεβαιωθεί η ακεραιότητα των πληροφοριών. Πώς δουλεύει όμως αυτή η μέθοδος;

Η **ψηφιακή υπογραφή** παράγεται από ένα λογισμικό, που με κάποιον μαθηματικό αλγόριθμο δέχεται ένα μεγάλο τμήμα κειμένου, που μπορεί να περιέχει οποιουσδήποτε χαρακτήρες και παράγει ένα μικρό συγκεκριμένο αριθμό από χαρακτήρες, αριθμούς και γράμματα και συνήθως προστίθεται επισυναπτόμενο στο τέλος του μηνύματος.

Ο μαθηματικός αλγόριθμος, που παράγει τις ψηφιακές υπογραφές, στην ουσία είναι η εφαρμογή μιας μαθηματικής συνάρτησης που ονομάζεται Συνάρτηση Κερματισμού.

Η Κρυπτογραφική **Συνάρτηση Κερματισμού (Hash Function)** είναι μια μαθηματική συνάρτηση που παίρνει ένα οποιοδήποτε τμήμα από δεδομένα και επιστρέφει μια τιμή κερματισμού (hash value) η οποία αποτελείται από μία συγκεκριμένου μεγέθους συμβολοσειρά. Η τιμή κερματισμού συνήθως ονομάζεται **Σύνοψη Μηνύματος (Message Digest)** και αν για κάποιο λόγο αλλάξει έστω και ένα ψηφίο (bit) από τα δεδομένα που κωδικοποιούμε με τη συνάρτηση κατακερματισμού, αυτόματα η επιστρεφόμενη τιμή κερματισμού είναι διαφορετική.

Τελικά μία σύνοψη μηνύματος μπορεί να χρησιμοποιηθεί για εξασφάλιση της ακεραιότητας της μεταφοράς και αυθεντικότητας των δεδομένων, όπως οι κωδικοί πρόσβασης (Passwords), οι ψηφιακές υπογραφές κ.ά.

Αν κάποιος γνωρίζει τη σύνοψη μηνύματος, δεν υπάρχει αντίστροφη συνάρτηση για να παράγει το αρχικό τμήμα δεδομένων που χρησιμοποιήθηκε.

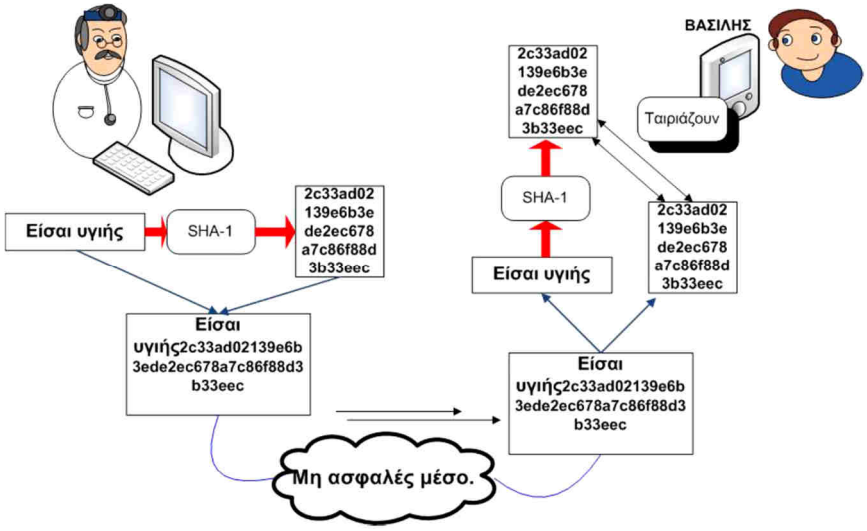
ΑΠΛΟ ΚΕΙΜΕΝΟ	ΣΥΝΟΨΗ ΜΗΝΥΜΑΤΟΣ
Αυτό	F113daf9 9596041d 5248ee95 2ad5bac4
Αυτό είναι	4042e887 266169d7 f6ac0db7 3af48a4c
Αυτό είναι 1	B58189c0 ebfa6030 20cfbc6a b6e64bf7
Αυτό είναι 1 Message	Ad31811d da59b23c 34371638 7bec2d6a
Αυτό είναι 1 Message Digest !	Bb157172 e8f76083 96929946 eac349af

Εικόνα 8.2.1.α: Σύνοψη Μηνύματος

Υπάρχουν αρκετοί διαφορετικοί αλγόριθμοι και συναρτήσεις κερματισμού, όπως οι Secure Hash Algorithm (SHA), Message Digest 4 (MD4), Message Digest (MD5), και ένα ολόκληρο πεδίο των μαθηματικών και της επιστήμης των υπολογιστών ασχολείται με τις κρυπτογραφικές συναρτήσεις κερματισμού.

Πώς όμως γίνεται ο έλεγχος της ακεραιότητας ενός μηνύματος, όταν φτάσει στον παραλήπτη; Ας δούμε το παράδειγμα που μετά από μια ιατρική εξέταση ο “Βασίλης” περιμένει τα αποτελέσματα με ηλεκτρονικό ταχυδρομείο. Έστω ότι ο γιατρός συντάσσει το κείμενο “Είσαι υγιής” και χρησιμοποιεί τον αλγόριθμο SHA-1 για να δημιουργήσει τη σύνοψη μηνύματος.

Κατόπιν προσθέτει στο τέλος του μηνύματος τη σύνοψη βάζοντας την ψηφιακή υπογραφή του και το στέλνει δια μέσω μη ασφαλούς καναλιού στο “Βασίλη”. Μετά την παραλαβή του μηνύματος γίνεται διαχωρισμός του μηνύματος από τη σύνοψη. Αφού περάσει το μήνυμα από τον αλγόριθμο SHA-1, παράγεται μια νέα σύνοψη μηνύματος και συγκρίνεται με αυτή που έχει αποσταλεί με το μήνυμα. Αν ταιριάζουν, τότε το μήνυμα προέρχεται από το γιατρό και το περιεχόμενο του δεν έχει τροποποιηθεί από κάποιο τρίτο μετά την αποστολή.



Εικόνα 8.2.1.β: Ψηφιακή Υπογραφή

Ας δεχτούμε ότι κάποιος κακοπροαίρετος έχει τροποποιήσει το μήνυμα, εισάγει τη λέξη “Δεν” στην αρχή του μηνύματος και έχει μετασχηματιστεί το μήνυμα στη φράση μαζί με τη σύνοψη σε:

“**Δεν Είσαι υγιής2c33ad02139e6b3ede2ec678a7c86f88d3b33eec**”

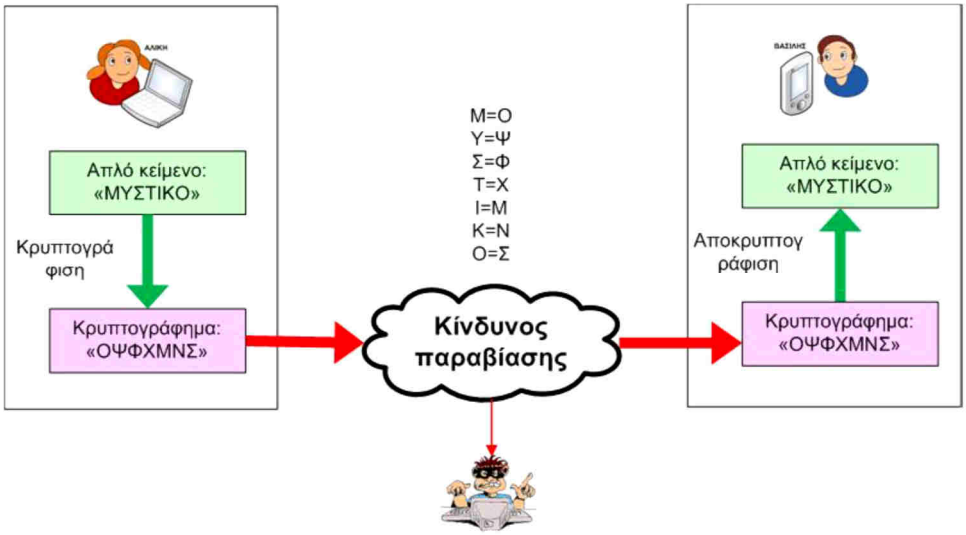
Όταν παραληφθεί το μήνυμα, γίνεται ο διαχωρισμός του κειμένου από τη σύνοψη και παράγεται η νέα σύνοψη η οποία δεν ταιριάζει με αυτήν που παραλήφθηκε με το μήνυμα.

“**Δεν Είσαι υγιής” : SHA-1(e2447161706b9a4898cfd132dd633c812bc8c739)**

Το συμπέρασμα που εξάγεται είναι ότι είτε το έγγραφο δεν προήλθε από το γιατρό είτε ότι κάποιος το τροποποίησε κατά τη μεταφορά. Επομένως γίνεται έλεγχος της ακεραιότητας και της αυθεντικότητας των πληροφοριών.

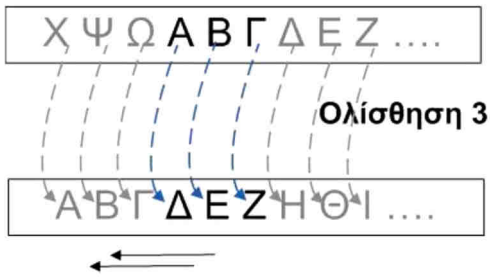
8.2.2 Συμμετρική κρυπτογράφηση

Η πρώτη τεχνική κρυπτογράφησης, που θα μελετήσουμε, βασίζεται στο διαμοιρασμό ενός κοινού μυστικού κλειδιού στους συμμετέχοντες στην επικοινωνία και γι' αυτό ονομάζεται και κρυπτογράφηση με συμμετρικό κλειδί. Οι δύο συμμετέχοντες γνωρίζουν το κοινό μυστικό και το αλγόριθμο κρυπτογράφησης /αποκρυπτογράφησης. Στον υπολογιστή του αποστολέα εφαρμόζεται η μέθοδος κρυπτογράφησης στο απλό κείμενο του μηνύματος και, πριν φύγει από τον υπολογιστή του αποστολέα, έχει μετατραπεί σε μη αναγνωρίσιμο κρυπτογράφημα. Μεταδίδεται μέσω καναλιών που πιθανά να εγκυμονούν τον κίνδυνο κάποιος να παρακολουθεί την κυκλοφορία των πληροφοριών και, αφού φτάσει στον παραλήπτη με τον αντίστροφό μηχανισμό, μετατρέπεται στο αρχικό απλό κείμενο.



Εικόνα 8.2.2.α: Κρυπτογράφηση με Μυστικό κλειδί

Μια τέτοια μέθοδος είναι η κρυπτογράφηση του Καίσαρα (Caesar Cipher) που είναι ίσως η απλούστερη και ευρέως διαδεδομένη τεχνική κρυπτογράφησης. Σ' αυτή την τεχνική κρυπτογράφησης χρησιμοποιείται η μέθοδος της ολίσθησης ή περιστροφής του αλφάβητου με βάση ένα συγκεκριμένο αριθμό από γράμματα. Αυτός ο αριθμός που ορίζει πόσα γράμματα ολισθαίνει η αλφάβητος στην ουσία αποτελεί το μυστικό κλειδί που διαμοιράζονται οι συμμετέχοντες στην επικοινωνία. Στην πραγματικότητα πρόκειται για την παραγωγή ενός κρυπτογραφήματος με αντικατάσταση των γραμμάτων του μηνύματος απλού κειμένου με γράμματα από το αλφάβητο που έχουν μετακινηθεί συγκεκριμένο αριθμό θέσεων προς τα αριστερά κατά την διαδικασία της κρυπτογράφησης και αντίστροφα προς τα δεξιά στην διαδικασία της αποκρυπτογράφησης.



Δραστηριότητα

Σ' αυτό το σημείο οι μαθητές ανά ομάδες σ' ένα παιχνίδι ρόλων, υποδύονται τους συνομιλητές που ανταλλάσσουν κρυπτογραφημένα μηνύματα και το ρόλο αυτού που θέλει να υποκλέψει τα μηνύματα τους εφαρμόζοντας πάνω σ' αυτά διάφορες τεχνικές που θα αποκαλύψουν το περιεχόμενά τους. Έστω ότι η Αλίκη κρυπτογραφεί το μήνυμα "Καλημέρα" με ολίσθηση κατά ένα συγκεκριμένο αριθμό γραμμάτων, όπως έχει συμφωνήσει με τον Βασίλη κατά την εκκίνηση της επικοινωνίας, και παράγει το κρυπτογράφημα "ΝΔΞΚΟΘΥΔ".

Ο Γιάννης (κακός) τώρα παρακολουθεί το κανάλι και με το κατάλληλο λογισμικό υποκλέπτει το κρυπτογράφημα και προσπαθεί να το “σπάσει”, δηλαδή εφαρμόζει τεχνικές χρησιμοποιώντας κατάλληλο λογισμικό και το αντίστοιχο ισχυρό υπολογιστικό σύστημα, ώστε να καταφέρει να αποκαλύψει το περιεχόμενο του μηνύματός. Η συνηθέστερη τεχνική, για να ανακαλύψει το περιεχόμενο του κρυπτογραφήματος, είναι να δοκιμάσει όλους τους δυνατούς συνδυασμούς κλειδιών, δηλαδή να ολισθαίνει κατά ένα γράμμα το αλφάβητο κάθε φορά και να εφαρμόζει την αντίστροφη διαδικασία αποκρυπτογράφησης. Έτσι παράγει τις εικοσιτέσσερις διαφορετικές αντιστοιχίσεις των γραμμάτων της αλφάβητου και καταλήγει να αποκαλύψει το μήνυμα χρησιμοποιώντας το κλειδί με ολίσθηση τρία γράμματα. Μέσα στην τάξη οι μαθητές μπορούν να χρησιμοποιήσουν τον Πίνακας 1 και να προσπαθήσουν να αποκρυπτογραφήσουν τα μηνύματα των συμμαθητών τους.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
ΑΠΛΟ ΚΕΙΜΕΝΟ	**Α**	**Β**	**Γ**	**Δ**	**Ε**	**Ζ**	**Η**	**Θ**	**Ι**	**Κ**	**Λ**	**Μ**	**Ν**	**Ξ**	**Ο**	**Π**	**Ρ**	**Σ**	**Τ**	**Υ**	**Φ**	**Χ**	**Ψ**	**Ω**
ΟΛΙΣΘΗΣΗ 1	**Β**	**Γ**	**Δ**	**Ε**	**Ζ**	**Η**	**Θ**	**Ι**	**Κ**	**Λ**	**Μ**	**Ν**	**Ξ**	**Ο**	**Π**	**Ρ**	**Σ**	**Τ**	**Υ**	**Φ**	**Χ**	**Ψ**	**Ω**	**Α**
ΟΛΙΣΘΗΣΗ 2	**Γ**	**Δ**	**Ε**	**Ζ**	**Η**	**Θ**	**Ι**	**Κ**	**Λ**	**Μ**	**Ν**	**Ξ**	**Ο**	**Π**	**Ρ**	**Σ**	**Τ**	**Υ**	**Φ**	**Χ**	**Ψ**	**Ω**	**Α**	**Β**
ΟΛΙΣΘΗΣΗ 3	**Δ**	**Ε**	**Ζ**	**Η**	**Θ**	**Ι**	**Κ**	**Λ**	**Μ**	**Ν**	**Ξ**	**Ο**	**Π**	**Ρ**	**Σ**	**Τ**	**Υ**	**Φ**	**Χ**	**Ψ**	**Ω**	**Α**	**Β**	**Γ**
ΟΛΙΣΘΗΣΗ 4	**Ε**	**Ζ**	**Η**	**Θ**	**Ι**	**Κ**	**Λ**	**Μ**	**Ν**	**Ξ**	**Ο**	**Π**	**Ρ**	**Σ**	**Τ**	**Υ**	**Φ**	**Χ**	**Ψ**	**Ω**	**Α**	**Β**	**Γ**	**Δ**
ΟΛΙΣΘΗΣΗ 5	**Ζ**	**Η**	**Θ**	**Ι**	**Κ**	**Λ**	**Μ**	**Ν**	**Ξ**	**Ο**	**Π**	**Ρ**	**Σ**	**Τ**	**Υ**	**Φ**	**Χ**	**Ψ**	**Ω**	**Α**	**Β**	**Γ**	**Δ**	**Ε**
...												**...**												

Πίνακας 8.2.2.1: Κρυπτογράφηση με Μυστικό κλειδί

Κ = Ν
Α = Δ
Λ = Ξ
Η = Κ
Μ = Ο
Ε = Θ
Ρ = Υ
Α = Δ

Αυτές οι μέθοδοι παραβίασης που χρησιμοποιούν όλους τους συνδυασμούς γραμμάτων, χαρακτήρων, συμβόλων, ψηφίων και τις εφαρμόζουν σ' ένα κρυπτογραφημένο κείμενο, ώστε να αποκαλύψουν το περιεχόμενο του, ονομάζονται “**Brute Force**” επιθέσεις.

Όμως στις περισσότερες περιπτώσεις τα πράγματα δεν είναι τόσο απλά, π.χ. δεν ξέρουμε αν στην κωδικοποίηση των γραμμάτων που χρησιμοποιήθηκαν στην κρυπτογράφηση συμπεριλαμβάνονται και πεζά γράμματα, αριθμοί, γράμματα του λατινικού αλφάβητου κ.λπ.

Εάν το αλφάβητο εισόδου έχει μέγεθος 24+26=50 (π.χ. τα πεζά γράμματα του ελληνικού και λατινικού αλφάβητου) και αν υπολογίσουμε και τα κεφαλαία, τους 10 αριθμητικούς χαρακτήρες, τότε έχουμε 50+50+10=110, χωρίς να λάβουμε υπόψη σημεία στίξης και σύμβολα.

Στις μεθόδους κρυπτογράφησης αυτού του τύπου, δηλαδή αντικατάστασης των χαρακτήρων του αλφάβητου με κάποιους άλλους από το ίδιο αλφάβητο, ώστε να μην είναι αναγνωρίσιμες οι συνθέσεις των λέξεων, παραμένουν κάποιες ιδιότητες της γλώσσας που

είναι εύκολα αναγνωρίσιμες. Για παράδειγμα έστω ότι έχουμε να "σπάσουμε" το παρακάτω κρυπτογράφημα.

"Π ΛΑΕΚΛΠΤ ΖΚΞΒΚ Π ΖΞΒ"

Παρατηρώντας το βλέπουμε μονοσύλλαβες λέξεις που παριστάνονται με το γράμμα "Π". Ποιες λέξεις του ελληνικού αλφάβητου αποτελούνται από ένα γράμμα και τις συναντάμε πολύ συχνά στις προτάσεις; Τα άρθρα "Ο", "Η" τα συναντάμε συχνά στις προτάσεις. Αν στον προηγούμενο πίνακα με όλες τις ολισθήσεις του αλφάβητου αναζητήσουμε τις δύο περιπτώσεις "ΟΛΙΣΘΙΣΗ 1 και ΟΛΙΣΘΙΣΗ 8", που το κρυπτογραφημένο γράμμα "Π" αντιστοιχεί στα άρθρα "Ο", "Η" και δοκιμάζουμε μόνο αυτές τις δυο περιπτώσεις, για να αποκρυπτογραφήσουμε το μήνυμα, θα καταλήξουμε αμέσως στη πρώτη περίπτωση:

Ολίσθηση 1

Το μήνυμα είναι: **"Ο ΚΩΔΙΚΟΣ ΕΙΝΑΙ Ο ΕΝΑ"**

Βλέπουμε ότι μπορούμε να σπάσουμε το μήνυμα πολύ πιο γρήγορα χωρίς να δοκιμάσουμε όλους τους δυνατούς συνδυασμούς.

Οι μέθοδοι παραβίασης που χρησιμοποιούν ένα συγκεκριμένο σύνολο από συνδυασμούς γραμμάτων, χαρακτήρων, συμβόλων, ψηφίων, συντάσσοντας έτσι ένα λεξικό με τις πιο πιθανές λέξεις που μπορεί να ταιριάζουν και τις εφαρμόζουν σ' ένα κρυπτογραφημένο κείμενο, ώστε να αποκαλύψουν το περιεχόμενο του, ονομάζονται **επιθέσεις με Λεξικό (Dictionary Attack).**

Από την παραπάνω μεθοδολογία συμπεραίνουμε πόσο εύκολο είναι να παραβιαστεί η μέθοδος κρυπτογράφησης του Καίσαρα και είναι αξιοπερίεργο για πόσο μεγάλο χρονικό διάστημα επικράτησε ως μέθοδος αποστολής κρυπτογραφημένων μηνυμάτων. Σήμερα χρησιμοποιούνται πιο σύγχρονοι αλγόριθμοι κρυπτογράφησης που βρίσκουν εφαρμογή, όπως ο αλγόριθμος συμμετρικής κρυπτογράφησης **Advanced Encryption Algorithm (AES)**, με μήκος κλειδιού τα 256 bit, οι οποίοι ενσωματώνουν χαρακτηριστικά της κρυπτογράφησης αντικατάστασης. Το σημαντικότερο όμως πρόβλημα, που αντιμετωπίζεται στην κρυπτογράφηση με διαμοιραζόμενο μυστικό κλειδί, είναι ότι δεν είναι δυνατό να μεταδοθεί το κλειδί δια μέσω του ανασφαλούς δημόσιου δικτύου. Από την άλλη πλευρά δεν είναι και δυνατό οι χρήστες που θέλουν να κάνουν ηλεκτρονικές συναλλαγές με κάποιο ηλεκτρονικό κατάστημα να μεταβαίνουν στα κεντρικά του καταστήματος που πιθανόν να βρίσκονται σε άλλη χώρα για να παραλάβουν το μυστικό κλειδί.

8.2.3 Κρυπτογράφηση Δημόσιου/Ιδιωτικού κλειδιού

Το βασικό πρόβλημα με όλο αυτό το θέμα κρυπτογράφησης και μεταφοράς ασφαλών πληροφοριών είναι ότι βασίζεται στο διαμοιρασμό και ανταλλαγή μυστικών (μυστικά κλειδιά). Για παράδειγμα, αν κάποιος θέλει να κάνει συναλλαγές με το ηλεκτρονικό κατάστημα της Amazon, θα έπρεπε να μεταβεί στα κεντρικά της εταιρείας, να ταυτοποιηθεί και να παραλάβει ένα μυστικό κλειδί. Για όσο διάστημα ο χρήστης διατηρεί αυτό το μυστικό κλειδί, μπορεί να κάνει συναλλαγές με την Amazon. Αν το κλειδί για κάποιο λόγο χαθεί, το μυστικό κλειδί είναι δύσκολο να ανακτηθεί. Σε γενικές γραμμές η εξασφάλιση της εμπιστευτικότητας στη μεταφορά πληροφοριών μέσω δημοσίων δικτύων δεν μπορεί να γίνει με την απόδοση των μυστικών κλειδιών με μεθόδους δημόσιας απόδοσης και μεταφοράς.

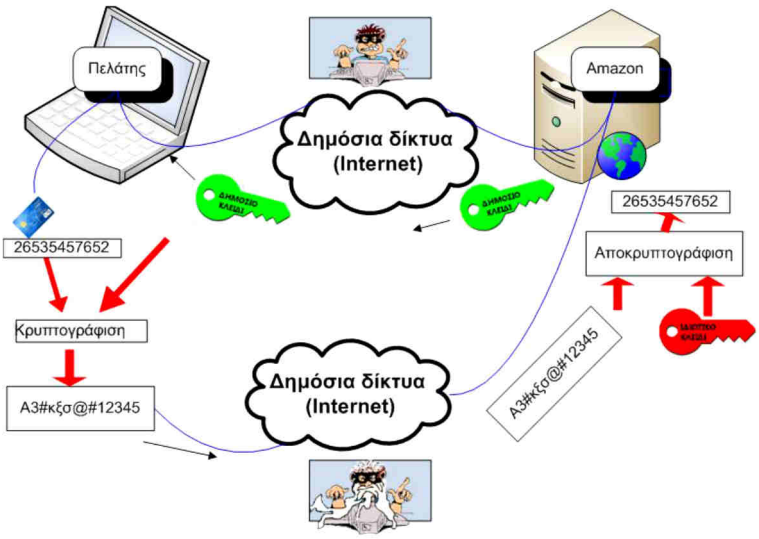
Μια πολύ καλή μέθοδος επίλυσης αυτών των προβλημάτων είναι η χρήση ζευγαριών δημόσιου και ιδιωτικού μυστικού κλειδιού που το ένα χρησιμεύει στην κρυπτογράφηση και το άλλο στην αποκρυπτογράφηση. Η ιδέα βασίζεται στην τεχνική με την οποία παράγονται από το υπολογιστή δυο κλειδιά ενός δημόσιου και ενός ιδιωτικού κλειδιού, όπου το

δημόσιο κλειδί μπορεί να μεταδοθεί μέσω των δημοσίων δικτύων και χρησιμοποιείται για την κρυπτογράφηση των πληροφοριών, ενώ το ιδιωτικό κλειδί αποθηκεύεται εσωτερικά στον υπολογιστή και χρησιμοποιείται για την αποκρυπτογράφηση. Αυτή η τεχνική κρυπτογράφησης από πλευράς μαθηματικών είναι ευρέως διαδεδομένη και κατανοητή, αλλά είναι πολύ δύσκολο να υπολογιστεί λόγω του μεγάλου μεγέθους αριθμητικών δεδομένων. Επομένως, η βασική υπόθεση της λειτουργικότητας αυτής της τεχνικής βασίζεται στο γεγονός ότι είναι πολύ δύσκολο να υπολογιστεί το ιδιωτικό κλειδί με βάση το δημόσιο κλειδί και το κρυπτογραφημένο κείμενο. Το ενδιαφέρον σημείο εδώ είναι ότι αυτή η τεχνική κρυπτογράφησης βασίζεται στην διατύπωση για την ύπαρξη της απόλυτης ασφάλειας των πληροφοριών που είναι «*να μην μεταδοθεί ποτέ η κρίσιμη πληροφορία*» η οποία στην προκειμένη περίπτωση είναι το ιδιωτικό κλειδί. Στις τεχνικές κρυπτογράφησης δημόσιου ιδιωτικού – κλειδιού καθώς και στη συμμετρική κρυπτογράφηση είναι ευρέως γνωστές οι μέθοδοι παραβίασης τους, όμως το ερώτημα στο οποίο στηρίζονται αυτές οι τεχνικές είναι: *«Οι ηλεκτρονικοί υπολογιστές είναι αρκετά γρήγοροι για να τα καταφέρουν;»*. Όσο οι υπολογιστές γίνονται ταχύτεροι τότε τα κλειδιά γίνονται μεγαλύτερα.

Ο πυρήνας της μεθόδου βασίζεται στον αλγόριθμο που παράγει δύο πολύ μεγάλους τυχαίους «πρώτους» αριθμούς με εκατοντάδες, αν όχι χιλιάδες, ψηφία και κατόπιν τους πολλαπλασιάζει και έτσι παράγεται ακόμα ένας πιο μεγάλος αριθμός. Κατόπιν εφαρμόζοντας κάποιον αλγόριθμο επεξεργασίας του αριθμού, παράγεται το ζεύγος δημόσιου ιδιωτικού κλειδιού. Η τεχνική αυτή στηρίζεται στην ιδιότητα των μαθηματικών για τους πρώτους αριθμούς και είναι τόσο δύσκολο να αναλύσει κάποιος το γινόμενο πρώτων αριθμών στους αριθμούς που το παράγουν, όσο και η προσπάθεια να ψάξει κανείς «ψύλλους στα άχυρα».

Ας δούμε ένα τέτοιο παράδειγμα ασυμμετρικής κρυπτογράφησης.

- Έστω ένας χρήστης εισάγει το αριθμό της πιστωτικής κάρτας visa για μια online αγορά από το δικτυακό τόπο της Amazon. Ο δικτυακός τόπος της Amazon θα παράγει ένα ζευγάρι δημόσιου και ιδιωτικού κλειδιού και θα αποστείλει το δημόσιο κλειδί μέσω του Διαδικτύου στον υπολογιστή του πελάτη μετά την εγκατάσταση μιας ασφαλούς σύνδεσης.
- Στο ενδιάμεσο της μεταφοράς, ας υποθέσουμε ότι κάποιοι «κακοί τύποι» καραδοκούν, για να υποκλέψουν πληροφορίες και ας αποδεχθούμε ότι μπορούν.
- Όταν το δημόσιο κλειδί φτάσει, ο χρήστης χρησιμοποιεί το κλειδί, κρυπτογραφεί τις πληροφορίες, παράγει ένα κρυπτογραφημένο μήνυμα κειμένου και το αποστέλλει πίσω μέσω του δημόσιου δικτύου στο οποίο καραδοκούν κίνδυνοι υποκλοπής.
- Έστω ότι εκτός από το δημόσιο κλειδί οι «κακοί τύποι» μπορούν να υποκλέψουν και το κρυπτογραφημένο μήνυμα. Επίσης ας αποδεχτούμε ότι έχουν και την υπολογιστική ισχύ και το χρόνο και μετά από μήνες και μήνες καταφέρνουν να αποκρυπτογραφήσουν το μήνυμα.
- Από την άλλη πλευρά η Amazon έχει παραλάβει το κρυπτογραφημένο μήνυμα και, επειδή διαθέτει το ιδιωτικό κλειδί, έχει αποκρυπτογραφήσει το μήνυμα σε ελάχιστο χρόνο.

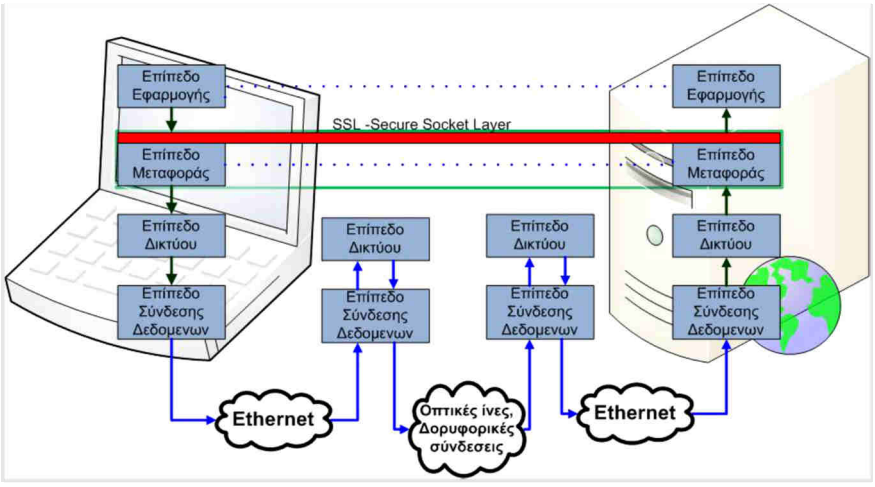


Εικόνα 8.2.3.α: Κρυπτογράφηση με Δημόσιο κλειδί

Συνοψίζοντας τα παραπάνω, δυο χρήστες, ο **Α** και ο **Β**, μπορούν να ανταλλάξουν εμπιστευτικές πληροφορίες κρυπτογραφώντας ο **Α** με το δημόσιο κλειδί του **Β** και, όταν ο **Β** παραλάβει το κρυπτογραφημένο μήνυμα, χρησιμοποιεί το ιδιωτικό του κλειδί για την αποκρυπτογράφηση. Άρα, για αμφίδρομη επικοινωνία χρειάζεται να παράγουν από ένα ζευγάρι κλειδιών δημόσιου-ιδιωτικού ο καθένας.

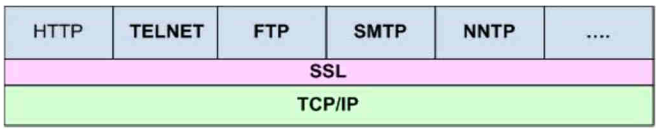
Στις περισσότερες των περιπτώσεων δεν έχει νόημα να κρυπτογραφήσει κάποιος με το ιδιωτικό του κλειδί και να αποκρυπτογραφήσει κάποιος άλλος με το δημόσιο, αφού ως γνωστό το δημόσιο κλειδί μπορεί να διαρρεύσει και να το αποκτήσει ο καθένας. Εκτός αν η διανομή του δημόσιου κλειδιού είναι περιορισμένη και δεν γίνεται μέσω δημοσίων καναλιών, για παράδειγμα με το χέρι και με ένα έγγραφο. Είναι διαδεδομένοι αρκετοί αλγόριθμοι κρυπτογράφησης δημοσίου – ιδιωτικού κλειδιού με πιο γνωστούς τους αλγόριθμους RSA και DSA/Elgamal.

Η υιοθέτηση αυτής της μεθόδου ασφαλούς μετάδοσης των πληροφοριών επέφερε μια αλλαγή στο μοντέλο διαστρωμάτωσης του TCP. Όπως έχει ήδη αναφερθεί, το επίπεδο μεταφοράς είναι υπεύθυνο για τις μεταδόσεις και αναμεταδόσεις των μηνυμάτων δεδομένων εξασφαλίζοντας την αξιοπιστία της σύνδεσης μεταξύ των εφαρμογών που βρίσκονται στα δυο άκρα της σύνδεσης.



Εικόνα 8.2.3.β: Διαστρωμάτωση TCP/IP με TLS

Ανάμεσα στο επίπεδο εφαρμογής και στο επίπεδο μεταφοράς δημιουργήθηκε ένα υποεπίπεδο (mini layer) το οποίο ονομάζεται **SSL - Secure Socket Layer**. Κατά βάση αυτό το επίπεδο δέχεται στο ένα άκρο απλό κείμενο το οποίο μετατρέπει σε κρυπτογραφημένο κείμενο και αντίστοιχα στο άλλο άκρο παραλαμβάνει το κρυπτογραφημένο μήνυμα και το μετατρέπει στο αρχικό απλό κείμενο. Οι εφαρμογές δεν κρυπτογραφούν τα δεδομένα, άλλα χρησιμοποιούν το πρωτόκολλο ασφάλειας **https** στο επίπεδο εφαρμογής το οποίο συμπεριλαμβάνει ένα σύνολο βιβλιοθηκών λογισμικού που χρησιμοποιούνται για την κρυπτογράφηση.



Από την άλλη πλευρά, το υπόλοιπο δίκτυο συνεχίζει να λειτουργεί ανεπηρέαστο, χωρίς να γνωρίζει αν έχει εφαρμοστεί ή όχι κάποια μέθοδος κρυπτογράφησης, όπως έχει ήδη περιγραφεί.

Όλη αυτή η μεθοδολογία αναφέρεται ως ασφάλεια του επίπεδου μεταφοράς (**TLS-Transport Layer Security**) και βασίζεται στις παρακάτω τέσσερις αρχές:

- Τοποθετείται ως υποεπίπεδο μεταξύ του επίπεδου εφαρμογής και μεταφοράς και χρησιμοποιείται για τις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης.
- Η κρυπτογράφηση και αποκρυπτογράφηση απαιτεί σημαντικό μέρος από τους πόρους του συστήματος, γι' αυτό και πρέπει να παρέχεται η δυνατότητα να χρησιμοποιείται μόνο όταν είναι απαραίτητο.
- Βασίζεται στην υπόθεση ότι μπορεί να παραβιαστεί, αλλά ο απλός άνθρωπος δεν έχει την υπολογιστική ισχύ, ώστε πρακτικά να μπορέσει να το παραβιάσει.
- Η υπόλοιπη λειτουργία του δικτύου παραμένει ανεπηρέαστη.

Με την ασφαλή διασύνδεση από το ένα άκρο στο άλλο λύνεται το πρόβλημα της εμπιστευτικότητας, δηλαδή να διαβάσει το μήνυμα μόνο ο παραλήπτης και κανένας άλλος.

Τι γίνεται, όμως, όταν η παραβίαση συμβεί, πριν μεταδοθούν τα δεδομένα; Για παράδειγμα ένας ιός που παρακολουθεί το κείμενο που πληκτρολογεί κάποιος ή κάποιος επαναδρομολογεί την διεύθυνση της ιστοσελίδας σε κάποια άλλη διεύθυνση που παρουσιάζεται σαν την διεύθυνση που θέλουμε, αλλά έχει σκοπό να υποκλέψει κρίσιμα απόρρητα δεδομένα. Άρα το επόμενο πρόβλημα είναι να εξασφαλίσουμε ότι αυτός που μιλάμε είναι αυτός που νομίζουμε ότι είναι.

8.2.4 Ψηφιακές υπογραφές – πιστοποιητικά

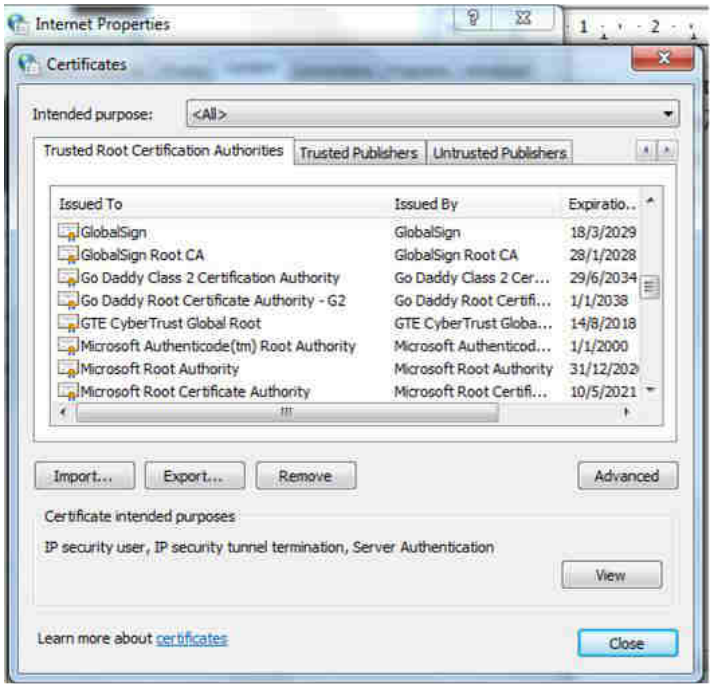
Σ' αυτό το σημείο είναι σημαντικό να εξετάσουμε αν ο δικτυακός τόπος που επισκεπτόμαστε είναι αξιόπιστος και ιδιαίτερα, όταν στέλνουμε εμπιστευτικά προσωπικά δεδομένα ή κάνουμε ηλεκτρονικές συναλλαγές. Όταν ανοίξουμε μια σελίδα σε ασφαλή σύνδεση, όπως η σελίδα μιας τράπεζας ή η σελίδα ενός ηλεκτρονικού καταστήματος, στην αρχή της URL διεύθυνσης σύνδεσης, εκτός από το ασφαλές πρωτόκολλο https, εμφανίζεται συνήθως κάποιο εικονίδιο με πληροφορίες για τη σελίδα. Επιλέγοντας αυτήν την ένδειξη εμφανίζονται συνήθως πληροφορίες για τη σύνδεση. Όπως αναφέρθηκε στην προηγούμενη ενότητα, όταν χρειάζεται να γίνει ασφαλής μεταφορά δεδομένων, μεταφέρεται στον υπολογιστή του πελάτη το δημόσιο κλειδί. Στην πραγματικότητα υπάρχουν δυο είδη δημόσιων κλειδιών.

Στην πρώτη περίπτωση, όπως μελετήθηκε παραπάνω, δημιουργείται ένα δημόσιο κλειδί και αποστέλλεται στον υπολογιστή του πελάτη. Στην δεύτερη περίπτωση, το δημόσιο κλειδί επικυρώνεται και υπογράφεται από μια επίσημη ανεξάρτητη αρχή η οποία πιστοποιεί την ταυτότητα αυτού που αποστέλλει το δημόσιο κλειδί. Στην κρυπτογραφία αυτή η διαδικασία

ορίζεται ως πιστοποιητικό δημοσίου κλειδιού ή **Ψηφιακά Πιστοποιητικά** (Digital Certificates).

Τα ψηφιακά πιστοποιητικά είναι ηλεκτρονικά έγγραφα τα οποία συνδέουν ένα δημόσιο κλειδί με μια ταυτότητα, δηλαδή πληροφορίες για το άτομο ή τον οργανισμό που ανήκει το κλειδί. Έτσι από πλευράς αξιοπιστίας, επειδή πρέπει να γνωρίζουμε με ποιον ανταλλάσσουμε πληροφορίες, έχουμε την ψηφιακή υπογραφή που επικυρώνει την ταυτότητα του ιδιοκτήτη του δημόσιου κλειδιού..

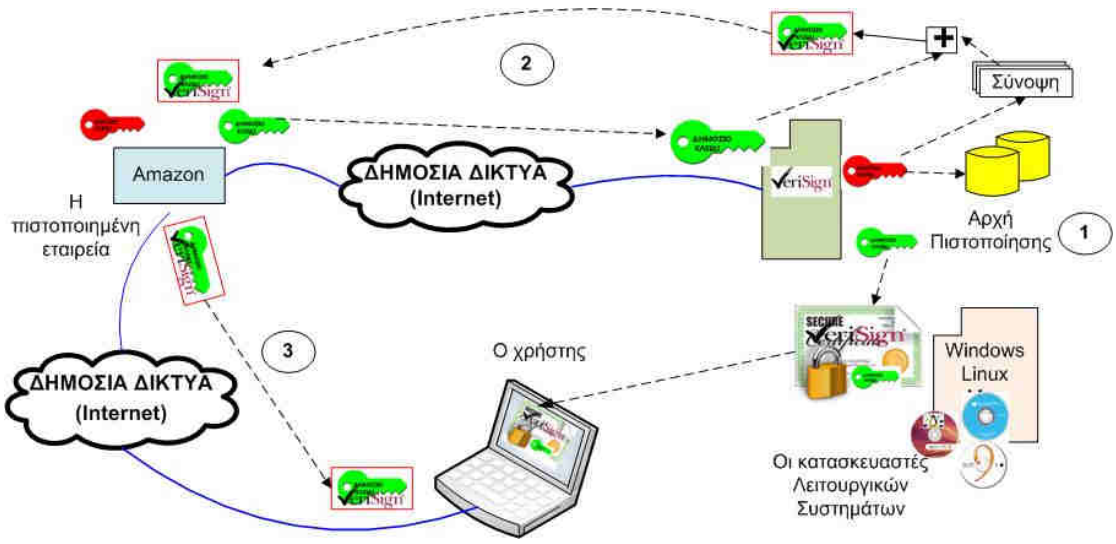
Υπάρχουν αρκετές αρχές πιστοποίησης (CA-Certificates Authorities), όπως οι GoDaddy, GlobalSign, Verisign.



Εικόνα 8.2.4.α: Ενσωματωμένα ψηφιακά πιστοποιητικά

Μια από τις παλαιότερες και πιο δημοφιλείς αρχές πιστοποίησης είναι η Verisign, με πολλούς πελάτες σε ατομικό επίπεδο και σε επίπεδο οργανισμών ή εταιρειών, όπως η Intel, Microsoft, Apple και άλλους. Το κόστος ενός ψηφιακού πιστοποιητικού ανέρχεται από μερικές εκατοντάδες ευρώ μέχρι μερικές χιλιάδες, άλλα από την άλλη πλευρά, οι αρχές πιστοποίησης είναι υπεύθυνες για να ελέγξουν και να επικυρώσουν την ταυτότητα σε οντότητες, άτομα, εταιρείες, οργανισμούς που διαχειρίζονται κρίσιμα εμπιστευτικά δεδομένα.

Πώς όμως λειτουργεί αυτός ο κύκλος εμπιστοσύνης μεταξύ αρχής πιστοποίησης και εταιρειών/οργανισμών και πελατών; Συνήθως όλες οι κατασκευάστριες λειτουργικών συστημάτων, όπως των Linux, Microsoft Windows, Apple Os, έχουν προεγκατεστημένο ως μέρος του λειτουργικού συστήματος ηλεκτρονικά έγγραφα - ψηφιακά πιστοποιητικά που στην ουσία αποτελούν δημόσια κλειδιά από τις αρχές πιστοποίησης. Αυτό σημαίνει ότι ένα δημόσιο κλειδί που αποστέλλεται σε μια ηλεκτρονική εμπορική συναλλαγή από μια εταιρεία, οργανισμό, ιδιώτη που είναι ψηφιακά υπογεγραμμένο, για παράδειγμα από τη Verisign, είναι εύκολα αναγνωρίσιμο.



Εικόνα 8.2.4.β: Επικοινωνία με Ψηφιακά πιστοποιητικά

Στα παρακάτω βήματα, σε συνέχεια με το παράδειγμα της προηγούμενης ενότητας, δίνεται μια απλοποιημένη περιγραφή της περίπτωσης σύνδεσης με ψηφιακό πιστοποιητικό από την αρχή πιστοποίησης, που θα θεωρήσουμε ότι είναι η Verisign.

- Η αρχή πιστοποίησης εκδίδει ένα δημόσιο και ένα ιδιωτικό κλειδί. Το ιδιωτικό κλειδί αποθηκεύεται σε μια τράπεζα δεδομένων και το δημόσιο κλειδί σε μορφή ψηφιακού πιστοποιητικού δημοσιεύεται και εγκαθίσταται μέσω του λειτουργικού συστήματος στους υπολογιστές.
- Στη συνέχεια, η εταιρεία ή ο ιδιώτης, εδώ η Amazon, που θέλει να πιστοποιηθεί από την επίσημη αρχή για την ανταλλαγή των πληροφοριών, επικοινωνεί με την Verisign και αιτείται την έκδοση ψηφιακού πιστοποιητικού. Όπως έχει ήδη περιγραφεί για τη μεταφορά εμπιστευτικών πληροφοριών, δημιουργείται ένα ζευγάρι δημόσιου - ιδιωτικού κλειδιού, όπου το ιδιωτικό κλειδί αποθηκεύεται εσωτερικά στην Amazon, ενώ το δημόσιο κλειδί αποστέλλεται στην Verisign μαζί με άλλες απαραίτητες πληροφορίες της εταιρείας.
- Η Verisign, αφού ελέγξει και επικυρώσει τις πληροφορίες της εταιρείας, παράγει μια σύνοψη. Η σύνοψη αυτή είναι μια ψηφιακή υπογραφή, η οποία παράγεται με κρυπτογράφηση από το δικό της ιδιωτικό κλειδί. Τέλος το προσθέτει μέσα στο δημόσιο κλειδί που παρέλαβε από την Amazon δημιουργώντας ένα ψηφιακά υπογεγραμμένο δημόσιο κλειδί. Κατόπιν το υπογεγραμμένο δημόσιο κλειδί επιστρέφεται πίσω στην Amazon και πλέον δεν είναι απλά ένα δημόσιο κλειδί, αλλά ταυτοποιεί επίσημα τον αποστολέα.
- Κάποια στιγμή ένας χρήστης στον κόσμο από το φορητό του υπολογιστή αποφασίζει να αγοράσει από την Amazon ρούχα, παπούτσια, βιβλία ή ότι άλλο θελήσει. Ο χρήστης συνδέεται στο δικτυακό τόπο της Amazon με πρωτόκολλο σε ασφαλή σύνδεση https, δηλαδή κρυπτογράφηση δημόσιου κλειδιού. Από την Amazon αποστέλλεται το υπογεγραμμένο δημόσιο κλειδί στο φορητό υπολογιστή του χρήστη. Όταν παραληφθεί, ελέγχεται με το εγκατεστημένο πιστοποιητικό από την Verisign, επαληθεύοντας τη σύνοψη που έχει παραχθεί με το ιδιωτικό κλειδί της Verisign και έχει επισυναφθεί στο δημόσιο κλειδί της Amazon. Με αυτό τον τρόπο επικυρώνεται η ταυτότητα του αποστολέα με την πιστοποίηση της Amazon. Αν για οποιοδήποτε λόγο το πιστοποιημένο δημόσιο κλειδί δεν θεωρηθεί έγκυρο, μπορεί να αποσταλεί για έλεγχο στην Verisign.

- Κατόπιν συνεχίζεται η μεταφορά των κρίσιμων δεδομένων με την μέθοδο κρυπτογράφησης δημοσίου κλειδιού, όπως έχει περιγραφεί στην προηγούμενη ενότητα. Καθ όλη την διάρκεια της επικοινωνίας η ανταλλαγή δεδομένων γίνεται με κρυπτογράφηση δημόσιου κλειδιού διαμέσω των δημόσιων δικτύων και πάντα υπάρχει η πιθανότητα παρακολούθησης και υποκλοπής των δεδομένων. Όμως και εδώ από καμιά πλευρά της επικοινωνίας δεν μεταφέρεται μέσω των δημοσίων δικτύων το ιδιωτικό κλειδί που είναι απαραίτητο για την αποκρυπτογράφηση.

Συνοψίζοντας, μπορούμε να διατυπώσουμε τα εξής:

- Το σύνολο των δεδομένων που επισυνάπτονται μαζί με τα δεδομένα της πληροφορίας που θέλουμε να μεταδώσουμε και σχετίζονται μεταξύ τους με οποιοδήποτε τρόπο, έτσι ώστε να πιστοποιηθεί η γνησιότητα τους, ονομάζεται **ηλεκτρονική (ψηφιακή) υπογραφή**.
- Η βασική μέθοδος δημιουργίας ψηφιακής υπογραφής είναι η χρήση αλγορίθμων που βασίζονται σε μονόδρομες συναρτήσεις κερματισμού (hash functions) οι οποίες παράγουν ένα σύνολο από δεδομένα που ονομάζονται σύνοψη μηνύματος.
- Αν θέλουμε η αυθεντικότητα των πληροφοριών που μεταδίδουμε να έχει το ίδιο βάρος και τις συνέπειες της χειρόγραφης υπογραφής, πρέπει να επικυρωθεί από τρίτο ουδέτερο οργανισμό που δεν συμμετέχει στην επικοινωνία, εκδίδοντας ένα ψηφιακό πιστοποιητικό.

8.3 Αδυναμίες – κίνδυνοι

Για τον σχεδιασμό-διαχείριση της ασφάλειας ενός συστήματος, πριν εφαρμοστούν τα κατάλληλα μέτρα προστασίας, είναι απαραίτητη η καταγραφή των απειλών και των αδυναμιών του συστήματος.

Όπως έχει αναφερθεί στην αρχή του κεφαλαίου, αντικειμενικός σκοπός της ασφάλειας είναι να προστατεύσει τους πληροφοριακούς πόρους (αγαθά) του συστήματος.

Όμως τι είδους απειλές δέχονται τα αγαθά, από ποιους και τι πρέπει να προστατευθεί;

Απειλή (Threat) είναι οποιοδήποτε γεγονός μπορεί να προκληθεί εσκεμμένα ή όχι και να επηρεάσει αρνητικά κάποιο αγαθό.

Οι απειλές μπορεί να προκληθούν από **φυσικά φαινόμενα**, όπως φωτιά, σεισμός, πλημμύρα, καταιγίδα, προβλήματα κλιματισμού, προβλήματα ηλεκτρισμού κτλ. ή από **εσκεμμένες** ανθρώπινες ενέργειες, όπως απάτη πλαστοπροσωπίας, εύρεση κωδικού, εκμετάλλευση αδυναμιών δικτύου, λογισμικού, λειτουργικού συστήματος, κακή χρήση των πόρων, μη εξουσιοδοτημένη πρόσβαση, κλοπή, βανδαλισμός, εμπρησμός κτλ. Υπάρχει πάντα βέβαια και η περίπτωση **μη σκόπιμης** ανθρώπινης απειλής, όπως λανθασμένη χρήση συστήματος, προγραμματιστικά λάθη, άγνοια κίνδυνου αποκάλυψης δεδομένων, μη εσκεμμένη καταστροφή υλικού κτλ.

Οι απειλές της παραβίασης ασφάλειας των πόρων του πληροφοριακού συστήματος διακρίνονται σε Εξωτερικές και Εσωτερικές απειλές.

- **Εξωτερικές απειλές**. Γεγονότα που προέρχονται από το εξωτερικό περιβάλλον και απειλούν την ασφάλεια του συστήματος.

Συνήθως οι εξωτερικές απειλές εμφανίζονται και πραγματοποιούνται επιθέσεις από εξωτερικούς εισβολείς που είναι γνωστοί ως Hackers, Crackers, Vandals, Hacktivists.

- **Εσωτερικές Απειλές**. είναι γεγονότα που προέρχονται από τους χρήστες του συστήματος οι οποίοι προσπαθούν να υπερβούν την εξουσιοδότηση που έχουν και να αποκτήσουν πρόσβαση σε πόρους του συστήματος.

Συνήθως παρακάμπτουν τις διαδικασίες ελέγχου του συστήματος για να αποκτήσουν πρόσβαση σε αναβαθμισμένες πληροφορίες είτε υποκλέπτουν τα στοιχεία από λογαριασμούς χρηστών με περισσότερα δικαιώματα σε σχέση με τα δικαιώματα που ήδη έχουν.

Αδυναμία (Vulnerability) είναι οποιοδήποτε έλλειμμα ή αμέλεια της ασφάλειας σε κάποιο πληροφοριακό πόρο του συστήματος, ώστε να τον αφήνει ευάλωτο σε απειλές.

Για παράδειγμα, εάν η πρόσβαση στη βάση δεδομένων που αποθηκεύονται οι κωδικοί των λογαριασμών δεν προστατεύεται επαρκώς, έστω και αν οι κωδικοί είναι κρυπτογραφημένοι, τότε υπάρχει μεγάλη πιθανότητα υποκλοπής.

8.3.1 Παραβίαση ασφάλειας

Όπως έχει ήδη αναφερθεί, οι απειλές διακρίνονται σε αυτές που έχουν αιτίες φυσικά φαινόμενα είτε αιτίες από εσκεμμένες ή όχι ανθρώπινες ενέργειες.

Επιθέσεις (attacks) συνήθως εξαπολύονται από εξωτερική προέλευση και λιγότερο συχνά από το εσωτερικό περιβάλλον και εκμεταλλεύονται μια ή και περισσότερες αδυναμίες του συστήματος με συνέπεια την παραβίαση της διαθεσιμότητας εμπιστευτικότητας, της αυθεντικότητας ή της ακεραιότητας της ασφάλειας.

Οι πιο συνήθεις μέθοδοι παραβίασης της ασφάλειας είναι:

- Κοινωνική Μηχανική (Social Engineering): Είναι ένα σύνολο από μεθόδους στις οποίες βασίζονται συνήθως άνθρωποι που αποσκοπούν στην παραβίαση συστημάτων και εκμεταλλεύονται τον ανθρώπινο παράγοντα για να αποσπάσουν κρίσιμες πληροφορίες, ώστε να παρακάμψουν τους μηχανισμούς ασφάλειας και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο σύστημα.
- Η σάρωση και η εύρεση προγραμμάτων εφαρμογών και πρωτοκόλλων που χρησιμοποιούνται στο σύστημα που στοχεύεται να παραβιαστεί, με σκοπό την ανεύρεση αδυναμιών.
- Hacking είναι η προσπάθεια παράκαμψης των μηχανισμών ασφάλειας, εκμεταλλευόμενοι συνήθως ελλείμματα του λογισμικού συστημάτων με σκοπό τη πρόσβαση σε κάποιο αγαθό του συστήματος.
- Χρήση κακόβουλου λογισμικού, όπως οι Ιοί (Viruses), τα Σκουλήκια (Worms), οι Δούρειοι Ίπποι (Trojan Horses), οι εφαρμογές spyware/adware που σκοπό έχουν είτε να εκμεταλλευτούν, είτε να δημιουργήσουν την αδυναμία για την μη εξουσιοδοτημένη πρόσβαση, είτε για την άμεση παραβίαση της ασφάλειας.
- Εύρεση και συλλογή στοιχείων από τα ηλεκτρονικά ίχνη που αφήνουν οι χρήστες του πληροφοριακού συστήματος, συνήθως από τις επικοινωνίες και συναλλαγές που κάνουν δια μέσω των δημοσίων δικτύων, όπως IP διευθύνσεις, e-mail, ονόματα υπολογιστών, υπηρεσίες εφαρμογές που χρησιμοποιούν κ.λπ.

Οι εσκεμμένες ή μη επιθέσεις από ανθρώπινες ενέργειες κατηγοριοποιούνται ανάλογα με τις συνέπειες και τους πόρους που επηρεάζουν σε:

- Επιθέσεις παραβίασης της εμπιστευτικότητας που ονομάζονται **Επιθέσεις Υποκλοπής** και στόχο έχουν την πρόσβαση σε πόρους χωρίς εξουσιοδότηση και αφαίρεση πληροφοριών. Τέτοιες επιθέσεις είναι η υποκλοπή αρχείων με εμπιστευτικά δεδομένα, όπως κωδικοί, αριθμοί λογαριασμών, κωδικοί από πιστωτικές κάρτες και γενικότερα κρίσιμα δεδομένα για τον ιδιοκτήτη τους που είναι αποθηκευμένα σε συστήματα ή μεταφέρονται μέσω δικτύου, όπως με την μέθοδο ανάλυσης κίνησης από τις γραμμές επικοινωνίας (packet sniffing-Man in the Middle), υποκλοπή λογισμικού, αντιγραφή προγραμμάτων κ.λπ.

- Επιθέσεις παραβίασης της διαθεσιμότητας που ονομάζονται **Επιθέσεις Διακοπής** και έχουν στόχο την καταστροφή ή να καταστήσουν τους πληροφοριακούς πόρους των συστημάτων σε ανενεργή κατάσταση. Τέτοια παραδείγματα είναι η διαγραφή αρχείων, δεδομένων, οι επιθέσεις στο λογισμικό, όπως ο τερματισμός εκτέλεσης μιας εφαρμογής, στο υλικό, όπως οι συνεχείς επανεκκινήσεις συστημάτων, οι επιθέσεις στα συστήματα υποδικτύου, όπως οι δρομολογητές ή οι επιθέσεις σε εξυπηρετητές, ώστε να επέλθουν σε κατάσταση άρνησης παροχής υπηρεσιών (DOS attacks) κ.λπ.
- Επιθέσεις παραβίασης της ακεραιότητας που ονομάζονται **Επιθέσεις Αλλοίωσης** και σκοπό έχουν την μη εξουσιοδοτημένη πρόσβαση και αλλοίωση του περιεχόμενου ενός πληροφοριακού πόρου του συστήματος. Τέτοια παραδείγματα είναι η επέμβαση στο υλικό, λογισμικό ή στα δεδομένα, έτσι ώστε να επηρεάσουν την πληρότητα και ακρίβεια των δεδομένων με σκοπό την δολιοφθορά ή την εξαπάτηση. Για παράδειγμα η παρέμβαση και αλλοίωση στρατιωτικών πληροφοριών που μεταδίδονται από τις γραμμές επικοινωνιών ή η μεταβολή του ποσού για μεταφορά ή πληρωμή από ένα τραπεζικό λογαριασμό σε μια ηλεκτρονική συναλλαγή.
- Επιθέσεις παραβίασης της αυθεντικότητας και κατ' επέκταση και της ακεραιότητας είναι οι **Επιθέσεις Εισαγωγής** που σκοπό έχουν μια πλαστή οντότητα να εισέλθει ως εξουσιοδοτημένο μέλος στο σύστημα. Τέτοιες επιθέσεις είναι οι περιπτώσεις **παραπλανητικής αλληλογραφίας (phishing)** που προσποιούνται για παράδειγμα κάποιον αρμόδιο της τράπεζας και ζητούν τα στοιχεία του λογαριασμού μας, οι επιθέσεις **πλαστοπροσωπίας (spoofing)** όπου ο επιτιθέμενος αλλάζει τα περιεχόμενα σε πακέτα δεδομένων που ήδη μεταφέρονται, έτσι προσποιούμενος κάποιον άλλο περνάει τα δεδομένα προς το δημόσιο κανάλι. Αφού έχει τροποποιήσει την δρομολόγηση των πακέτων δεδομένων, παραλαμβάνει όσα πακέτα εισέλθουν στο δίκτυο και απευθύνονται στον πραγματικό παραλήπτη.

8.4 Μέθοδοι και Τεχνικές προστασίας

Τα μέτρα αντιμετώπισης για την προστασία της ασφάλειας των πληροφοριακών πόρων του συστήματος πρέπει να βασίζονται στο σχεδιασμό μιας ολοκληρωμένης πολιτικής ασφάλειας που διακρίνεται σε τρία επίπεδα.

1. Το πρώτο επίπεδο αναφέρεται στην **πρόληψη** η οποία στηρίζεται στην ανίχνευση των ευπαθειών, αδυναμιών όσον αφορά την επίδραση του φυσικού περιβάλλοντος, τις αδυναμίες υλικού, λογισμικού, αποθήκευσης και μεταφοράς δεδομένων. Οι συνήθεις τεχνικές που χρησιμοποιούνται είναι :
   - ο έλεγχος της πρόσβασης στους πόρους
   - η εγκατάσταση προγραμμάτων προστασίας από κακόβουλο λογισμικό, όπως anti-virus, antispyware
   - η εγκατάσταση τείχους προστασίας (Firewall) για τον έλεγχο της εισερχόμενης και εξερχόμενης κίνησης δεδομένων
   - οι συνεχείς ενημερώσεις και αναβαθμίσεις λογισμικού που διορθώνουν αδυναμίες και ελλείψεις ασφάλειας
2. Το δεύτερο επίπεδο περιγράφει την **Αντιμετώπιση** καταστροφών και επαναφορά του συστήματος στην προηγούμενη λειτουργική του κατάσταση. Οι συνήθεις πρακτικές που χρησιμοποιούνται είναι:
   - ο ολοκληρωμένος και τεκμηριωμένος σχεδιασμός της διαδικασίας ανάνηψης μετά από παραβιάσεις της ασφάλειας καθώς και η μέθοδος ανατροφοδότησης για το πρόβλημα που προέκυψε και πώς αντιμετωπίστηκε
   - η δημιουργία μερικών ή ολοκληρωμένων αντιγράφων ασφάλειας

- ο καθορισμός διαδικασιών ενεργοποίησης των μεθόδων ανάνηψης από παραβιάσεις, καταστροφές (Fault Tolerance)

2. Στο τρίτο επίπεδο κατατάσσονται τα συστήματα Ανίχνευσης εισβολών. Εφόσον αποτύχουν οι σχεδιασμοί πρόληψης, η ασφάλεια του συστήματος πρέπει να βασιστεί σε μηχανισμούς ανίχνευσης εισβολών. Οι συνήθεις μηχανισμοί που χρησιμοποιούνται για την ανίχνευση παραβιάσεων της ασφάλειας σε συνεργασία με τα τυπικά εργαλεία - προγράμματα ανίχνευσης ευπαθειών, όπως για παράδειγμα οι σαρωτές για ιούς, είναι η εγκατάσταση ειδικού λογισμικού ανίχνευσης εισβολών Intrusion Detection System (IDS).

8.4.1 Αντίγραφα ασφαλείας

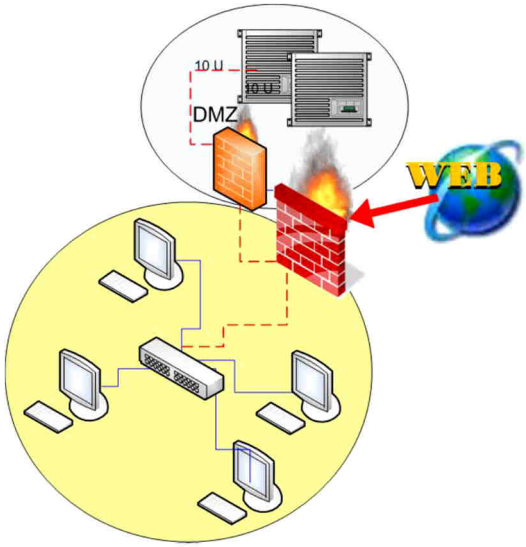
Η διαδικασία ανάνηψης του πληροφοριακού συστήματος μετά από καταστροφή βασίζεται κατά ένα μεγάλο μέρος στην διαδικασία των αντιγράφων ασφαλείας (Backup Data). Κατά την διαδικασία αυτή με τη χρήση κατάλληλων εργαλείων λογισμικού ή δυνατοτήτων που προσφέρει το λειτουργικό σύστημα αποθηκεύονται σε ασφαλή μέσα αντίγραφα των δεδομένων, προγραμμάτων, βάσεων δεδομένων και γενικότερα πληροφοριακών πόρων και δημιουργούνται αντίγραφα που ονομάζονται αντίγραφα εφεδρείας ή αντίγραφα ασφαλείας. Μετά από καταστροφή των πόρων ή ακόμα και του υλικού παρέχεται η δυνατότητα επαναφοράς ολόκληρου του πληροφοριακού συστήματος ή μόνο ενός μέρους των πληροφοριακών πόρων σε πρότερη κανονική κατάσταση λειτουργίας.

Τα μέσα και οι συσκευές που χρησιμοποιούνται για την αποθήκευση των αντιγράφων διαφέρει ανάλογα με το είδος και το μέγεθος των δεδομένων καθώς και τις προδιαγραφές για την ανάκτηση τους. Συνήθως χρησιμοποιούνται μαγνητικά μέσα (σκληροί δίσκοι), οπτικά μέσα (CD, DVD κ.λπ), μνήμες μόνιμης αποθήκευσης (flash, Solid State disk) και τέλος, με την εξέλιξη των γραμμών τηλεπικοινωνιών και δικτύων, είναι δυνατή η αποθήκευση και ανάκτηση σε απομακρυσμένους υπολογιστές ή ανάλογα με την κρισιμότητα των δεδομένων σε εξωτερικούς online εξυπηρετητές.

8.4.2 Τείχος προστασίας (Firewall)

Τα συστήματα τείχους προστασίας (firewall) προστατεύουν τους πληροφοριακούς πόρους ενός συστήματος ή ενός δικτύου απομονώνοντας το σύστημα από το εξωτερικό δίκτυο ελέγχοντας την διακίνηση των εισερχομένων και εξερχομένων πακέτων δεδομένων. Έτσι ένα firewall προστατεύει το σύστημα από επιθέσεις μη εξουσιοδοτημένης πρόσβασης. Το firewall μπορεί είναι είτε εφαρμογές λογισμικού είτε εξειδικευμένο ολοκληρωμένο σύστημα που λειτουργεί σε όλα τα επίπεδα του μοντέλου TCP/IP. Οι βασικές λειτουργίες του είναι:

- το φιλτράρισμα εισερχομένων και εξερχόμενων πακέτων (packet filters).Ελέγχει κάθε πακέτο που εισέρχεται-εξέρχεται και αποφασίζει με βάση τις πληροφορίες της επικεφαλίδας του πακέτου, δηλαδή την Διεύθυνση προέλευσης και προορισμού, τον αριθμό πρωτοκόλλου (protocol number) και τον αριθμό θύρας (port number).
- και ως πύλες (gateways) στο επίπεδο εφαρμογής. Το firewall ανιχνεύει και αντιλαμβάνεται το είδος της κίνησης των δεδομένων στο επίπεδο εφαρμογής και εφαρμόζει έλεγχους σε επίπεδο εξουσιοδότησης χρήστη καθώς και στις υπηρεσίες και στα πρωτόκολλα που επιτρέπονται ή όχι, όπως τα http, ftp, telnet, κ.λπ.



Εικόνα 8.4.2.α: Firewall

- Απομονώνει διαφορετικές περιοχές του δικτύου εφαρμόζοντας διαφορετικές πολιτικές ασφάλειας, π.χ. ο διαχωρισμός ενός web server ή ενός web mail server, που δέχεται επισκέψεις από εξωτερικό δημόσιο δίκτυο (internet), από την πολιτική ασφάλειας που υπάρχει για το υπόλοιπο εσωτερικό δίκτυο.

Σ' αυτό το σημείο θα πρέπει να υλοποιήσετε μια άσκηση εμπέδωσης, όπως είναι η Άσκηση 4 που περιγράφεται στην ενότητα «Ασκήσεις» στην αίθουσα εργαστηρίου.

8.4.3 Σύστημα εντοπισμού εισβολέων IDS

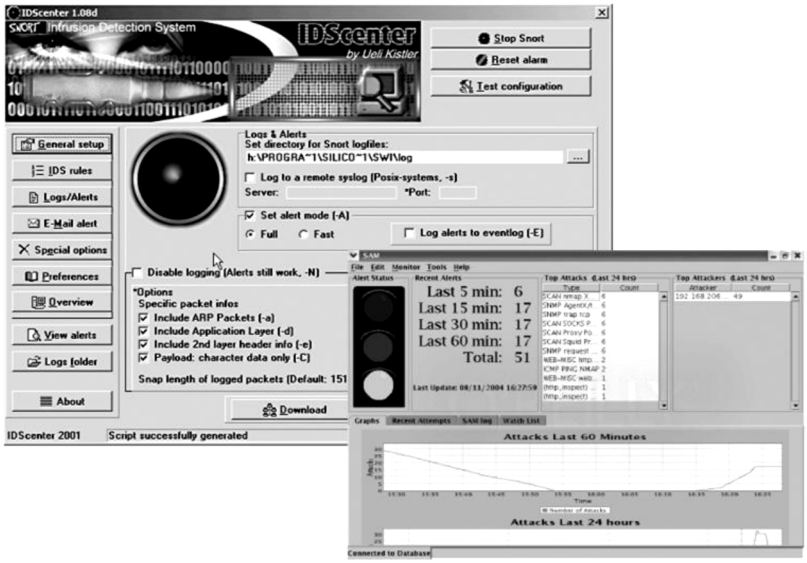
Όπως έχει αναφερθεί από την αρχή του κεφαλαίου, δεν υπάρχει η έννοια της απόλυτης ασφάλειας. Από την άλλη πλευρά καθημερινά δημιουργούνται καινούργιες ευπάθειες στο υλικό και περισσότερο στο λογισμικό των πληροφοριακών συστημάτων με αποτέλεσμα να γεννούνται νέες δυνατότητες παραβίασης της ασφάλειας των συστημάτων. Κατά το σχεδιασμό της πολιτικής ασφάλειας, όπως έχει ήδη αναφερθεί, αφού αποτύχει η προσπάθεια πρόληψης κατά των εισβολών, πρέπει να έχει υιοθετηθεί ένα σύστημα ανίχνευσης και εντοπισμού τους.

Ένα σύστημα εντοπισμού εισβολέων (Intrusion Detection Systems, IDS) αποτελείται από μια πλατφόρμα εργαλείων λογισμικού που ελέγχουν τα αρχεία καταγραφής του συστήματος, ώστε να ανιχνεύσει ίχνη από γνωστές παραβιάσεις ασφάλειας, όπως:

- επαναλαμβανόμενες προσπάθειες εισαγωγής κωδικών
- δραστηριότητες σάρωσης των θυρών επικοινωνίας (port scan)
- ενέργειες παράνομων εγγραφών στο μητρώο του συστήματος
- απόπειρες αυξημένης ροής πακέτων προς ένα σύστημα -επίθεση DOS
- εντοπισμός αυξημένης διαρροής πόρων κατά την εκτέλεση εφαρμογών

Επίσης ελέγχουν και αναλύουν την διερχόμενη κίνηση των κόμβων και των συσκευών δικτύου.

Ένα IDS μπορεί να έχει καθαρά μόνο ενημερωτικό ρόλο, δηλαδή, μετά την παρακολούθηση του συστήματος, ανιχνεύει κάποια ύποπτη ενέργεια και επιστρέφει κάποιο μήνυμα για πιθανή εισβολή ή μπορεί να διαθέτει μηχανισμούς αυτόματης αντιμετώπισης ή συνεργασίας με άλλα εργαλεία αντιμετώπισης παραβιάσεων, όπως το firewall. Τα συστήματα που διαθέτουν μηχανισμούς που μπλοκάρουν πιθανές εισβολές ονομάζονται Intrusion Detection and Prevention Systems (IDPS).



Εικόνα 8.4.3.α: Ελεύθερο Λογισμικό IDS - SNORT

8.4.4 Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών

Κάθε οντότητα (ιδιώτης, εταιρεία, οργανισμός), που διαχειρίζεται ευαίσθητα εμπιστευτικά δεδομένα πληροφορίες, πρέπει να υιοθετήσει ένα σύνολο από αυστηρές συστηματικές διαδικασίες που εξασφαλίζουν την προστασία των πληροφοριών. Αυτές οι διαδικασίες προκύπτουν κατόπιν λεπτομερειακής ανάλυσης, μελέτης και σχεδιασμού του επιπέδου ασφάλειας, που πρέπει να διασφαλιστεί, σε σχέση πάντα με το κόστος επένδυσης και διαμορφώνουν το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.

Οι συνιστώσες που πρέπει να μελετηθούν για να δημιουργηθούν οι κατάλληλες διαδικασίες αφορούν:

- τον λεπτομερειακό καθορισμό κανόνων ασφαλείας που πρέπει να τηρούνται και την εκπαίδευση των χρηστών για την ορθή χρήση του πληροφοριακού συστήματος
- τον προσδιορισμό των εξουσιοδοτήσεων πρόσβασης των χρηστών και την περιγραφή των δικαιωμάτων τους στο πληροφοριακό σύστημα
- την περιγραφή αδυναμιών του συστήματος και τις ενδεχόμενες περιπτώσεις παραβίασης καθώς και τα μέτρα αντιμετώπισης τους
- τις ακριβείς ενέργειες για την υλοποίηση μιας ολοκληρωμένης πολιτικής ασφάλειας
- την δημιουργία ενός ολοκληρωμένου σχεδίου συνέχειας που περιλαμβάνει ένα σχέδιο ανάνηψης σε περίπτωση κάποιας καταστροφής καθώς και ένα πλάνο διαχείρισης και αντιμετώπισης των κινδύνων

Ο διεθνής οργανισμός τυποποίησης δημιούργησε ένα πρότυπο το ISO27001 που παρέχει ένα σύνολο προδιαγραφών. Οι προδιαγραφές αυτές καθορίζουν τις απαιτήσεις για την υιοθέτηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών και αφορούν την διοίκηση του προσωπικού, τις διαδικασίες και τα πληροφοριακά συστήματα για κάθε είδους επιχειρησιακό κλάδο και οποιουδήποτε μεγέθους οργανισμό.

Για περισσότερες πληροφορίες μελετήστε την ενότητα Π.4 του Παραρτήματος των σημειώσεων.

Ερωτήσεις – Ασκήσεις Κεφαλαίου

1. Περιγράψτε πώς μπορεί να επιτευχθεί η απόλυτη ασφάλεια.
2. Κατά τον σχεδιασμό της ασφάλειας ενός πληροφοριακού συστήματος, τι είναι αυτό που πρέπει να προστατεύσουμε και από ποιον πρέπει να το προστατεύσουμε;
3. Περιγράψτε τις έννοιες: εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, διαθεσιμότητα.
4. Δώστε τον ορισμό για τις έννοιες: κρυπτογράφηση, κρυπτογράφημα, μυστικό κλειδί.
5. Ποιος είναι ο ρόλος της κρυπτογραφικής συνάρτησης κερματισμού;
6. Ποιος είναι ο λόγος της υπογραφής ενός μηνύματος χρησιμοποιώντας τη σύνοψη μηνύματος;
7. Ένας χρήστης, η Αλίκη, θέλει να επικοινωνήσει με τον Βασίλη. Συντάσσει το μήνυμα "**Αύριο θα συναντηθούμε στις 2**" και, αφού το περάσει από τη συνάρτηση κερματισμού SHA1, παράγει και επισυνάπτει τη σύνοψη μηνύματος **bc6a187be1034b1ee0aff99719c574cdff0a49d5** και το αποστέλλει. Ο Βασίλης παραλαμβάνει το μήνυμα:

   " **Αύριο θα συναντηθούμε στις 1bc6a187be1034b1ee0aff99719c574cdff0a49d5".**

   Ποια διαδικασία ακολουθεί ο Βασίλης, όταν παραλάβει το μήνυμα, και ποιο συμπέρασμα βγάζει;
   Ελέγξτε την απάντηση σας, εφαρμόζοντας την μετάδοση των μηνυμάτων στην αίθουσα εργαστηρίου, με βάση την Άσκηση 3 της ενότητας "Ασκήσεις Στην Αίθουσα Εργαστηρίου".
8. Ας υποθέσουμε ότι ένας hacker άφησε ένα cd υποδηλώνοντας ότι το ξέχασε πάνω στο γραφείο ενός υπαλλήλου μιας τράπεζας που είχε τίτλο "Βιντεο Αποκάλυψη για τεράστιο σκάνδαλο". Μέσα δε στο cd υπάρχει αποθηκευμένο πρόγραμμα σε μορφή αυτόματης εκτέλεσης που περιέχει ένα δούρειο ίππο που ανιχνεύει τα πλήκτρα που πατά κάποιος, συλλέγει πληροφορίες και τις αποστέλλει στο Διαδίκτυο. Τι είδους απειλή εγκυμονεί για το πληροφοριακό σύστημα; Αν επιτύχει η παραβίαση της ασφάλειας, τι είδους επίθεση έχουμε;
9. Ένας hacker αποκτά πρόσβαση στη βάση δεδομένων που έχει αποθηκευμένους στον πίνακα users τους κωδικούς χρηστών από τους λογαριασμούς των διαχειριστών ενός μεγάλου δικτυακού τόπου. Στον πίνακα υπάρχει η εγγραφή:

   admin:781e5e245d69b566979b86e28d23f2c7

   Ο hacker χρησιμοποιώντας το online λογισμικό, όπως το "md5pass.info", ξεκινά να παράγει όλους τους δυνατούς συνδυασμούς από χαρακτήρες μέχρι γράμματα και ψηφία του αγγλικού αλφάβητου και μέσα σε λίγα εκατοστά του δευτερολέπτου λαμβάνει την επιστροφή "0123456789".
   Ποια μέθοδο χρησιμοποίησε ο hacker για να παραβιάσει τον κωδικό; Περιγράψτε την διαδικασία που εκτελεί το λογισμικό για να βρει τον κωδικό. Τι συμπέρασμα βγάζετε για τον κωδικό;
   Εφαρμόστε την διαδικασία ως άσκηση στο εργαστήριο. Χρησιμοποιήστε κωδικούς, που κατασκευάζονται, χρησιμοποιώντας τον αλγόριθμο SHA1 για την παραγωγή σύνοψης με το εργαλείο GnuPG.
10. Περιγράψτε τη βασική λειτουργία της κρυπτογράφησης με κοινό μυστικό. Ποιο είναι το αδύναμο σημείο αυτής της μεθόδου;
11. Ποιες είναι οι βασικές μέθοδοι παραβίασης κωδικών; Να τις εξηγήσετε.
12. Η παρακάτω ερώτηση είναι κρυπτογραφημένη με την τεχνική Caesar Cipher. **ΗΓ ΩΘΖΗΦΧΓ ΧΨΡΦΠΦ ΩΔΓΕΡΦ ΑΝ ΩΡΗΝΠΓΥΡΦ ΝΔΓ ΠΤΩΓΖΦΓ ΧΝΑΝΨΦ;** Χρησιμοποιείστε το παρακάτω πίνακα 1 για την αποκρυπτογράφηση του κειμένου

της ερώτησης. Μια από τις ολισθήσεις – κλειδιά 4, 7, 12, 22 του αλφάβητου είναι η σωστή.

13. Επιλέξτε τη σωστή απάντηση για την παραπάνω ερώτηση από τα παρακάτω κρυπτογραφήματα με κλειδί **11**
    - **ΕΛΕΖΒ**
    - **ΧΜΤΒΕ**

Πίνακας 1: Κλειδιά-Ολισθήσεις Ελληνικού Αλφάβητου

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
ΑΠΛΟ ΚΕΙΜΕΝΟ	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
ΟΛΙΣΘΗΣΗ 1	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α
ΟΛΙΣΘΗΣΗ 2	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β
ΟΛΙΣΘΗΣΗ 3	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ
ΟΛΙΣΘΗΣΗ 4	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ
ΟΛΙΣΘΗΣΗ 5	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε
ΟΛΙΣΘΗΣΗ 6	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ
ΟΛΙΣΘΗΣΗ 7	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η
ΟΛΙΣΘΗΣΗ 8	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ
ΟΛΙΣΘΗΣΗ 9	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι
ΟΛΙΣΘΗΣΗ 10	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ
ΟΛΙΣΘΗΣΗ 11	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ
ΟΛΙΣΘΗΣΗ 12	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ
ΟΛΙΣΘΗΣΗ 13	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν
ΟΛΙΣΘΗΣΗ 14	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ
ΟΛΙΣΘΗΣΗ 15	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο
ΟΛΙΣΘΗΣΗ 16	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π
ΟΛΙΣΘΗΣΗ 17	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ
ΟΛΙΣΘΗΣΗ 18	Τ	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ
ΟΛΙΣΘΗΣΗ 19	Υ	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ
ΟΛΙΣΘΗΣΗ 20	Φ	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ
ΟΛΙΣΘΗΣΗ 21	Χ	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ
ΟΛΙΣΘΗΣΗ 22	Ψ	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ
ΟΛΙΣΘΗΣΗ 23	Ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ

Ελέγξτε τις απαντήσεις στο δικτυακό τόπο:
http://users.sch.gr/xefterakis/caesar.html

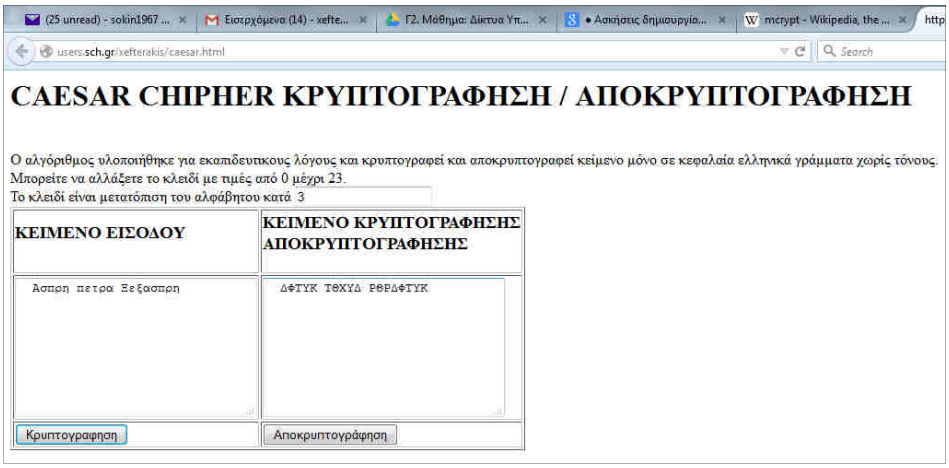
14. Ποιο είναι το μεγαλύτερο πρόβλημα που πρέπει να αντιμετωπιστεί με τη χρήση της κρυπτογράφησης με διαμοιραζόμενο μυστικό κλειδί;
15. Περιγράψτε την τεχνική κρυπτογράφησης με δημόσιο κλειδί.
16. Γιατί η κρυπτογράφηση των δεδομένων με το ιδιωτικό κλειδί, ώστε να εξασφαλιστεί η αυθεντικότητα του αποστολέα, και η αποκρυπτογράφηση με το δημόσιο κλειδί στο άλλο άκρο ουσιαστικά δεν έχει κανένα νόημα; Με ποιο τρόπο πιστοποιείται η αυθεντικότητα του ιδιοκτήτη των δεδομένων;
17. Πώς αντιμετωπίστηκε η διαχείριση της ασφαλούς επικοινωνίας στο επίπεδο διαστρωμάτωσης του TCP/IP;
18. Ποιες είναι οι βασικές αρχές στις οποίες βασίζεται η μεθοδολογία διαχείρισης ασφάλειας της μεταφοράς δεδομένων (TLS - Transport Layer Security);
19. Περιγράψτε τη λειτουργία χρήσης ενός ψηφιακού πιστοποιητικού.
20. Ποιες είναι οι συνήθεις μέθοδοι παραβίασης των πληροφοριακών συστημάτων;
21. Περιγράψτε τις βασικές κατηγορίες επιθέσεων και ποια χαρακτηριστικά της ασφάλειας παραβιάζονται.

22. Αν μαζικά εκατοντάδες χρήστες σ' όλο το κόσμο έστελναν συνεχόμενα πακέτα ελέγχου με το πρωτόκολλο ICMP, δηλαδή εκτελούσαν την εντολή ping προς ένα συγκεκριμένο εξυπηρετητή κάποιας υπηρεσίας για παράδειγμα webserver, τι είδους επίθεση θα είχαμε; Δικαιολογήστε την απάντηση σας.
23. Δώστε ένα παράδειγμα από κάθε κατηγορία επίθεσης από εσκεμμένες ανθρώπινες ενέργειες.
24. Αναφέρετε τα μέτρα αντιμετώπισης των απειλών ασφάλειας.
25. Ποιες είναι οι βασικές λειτουργίες που εκτελούν συνήθως τα firewalls;
26. Ένα firewall επιτρέπει την εισερχόμενη και εξερχόμενη επικοινωνία σε ένα τοπικό δίκτυο στις θύρες TCP 80 και 25 και απαγορεύει την κυκλοφορία στις θύρες 21 και 23. Ποιες υπηρεσίες Διαδικτύου επιτρέπεται στο εσωτερικό του δικτύου να επικοινωνήσουν με το Διαδίκτυο;
27. Τι είναι ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών και πώς διαμορφώνεται ένα τέτοιο σύστημα;
28. Ένα σύστημα ανίχνευσης εισβολών IDS ποια συνήθη ίχνη παραβιάσεων μπορεί να ανιχνεύσει;
29. Ποια η διαφορά ενός συστήματος IDS και ενός IDPS;
30. Περιγράψτε τις φάσεις για την ανάπτυξη ενός Συστήματος Διαχείρισης της Ασφάλειας Πληροφοριών (ΣΔΑΠ) και αναφέρετε τα πλεονεκτήματα της υιοθέτησης ενός τέτοιου συστήματος στην πολιτική ασφάλειας ενός οργανισμού.

Ασκήσεις στην Αίθουσα Εργαστηρίου

Άσκηση 1: Κρυπτογράφηση /Αποκρυπτογράφηση με την μέθοδο Caesar Chipher

Στο εργαστήριο οι μαθητές μπορούν να διερευνήσουν τη μέθοδο κρυπτογράφησης και αποκρυπτογράφησης δεδομένων κειμένου με τη χρήση εκπαιδευτικού εργαλείου-βοηθήματος για το ελληνικό αλφάβητο που βρίσκεται σε δικτυακούς τόπους, όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 10: Caesar Chipher
(Πηγή: http://users.sch.gr/xefterakis/caesar.html)

Δραστηριότητα 1η

Οι μαθητές ανά ομάδες μπορούν να διερευνήσουν τα χαρακτηριστικά του αλγόριθμου Caesar Chipher ανταλλάσοντας μηνύματα χρησιμοποιώντας διαφορετικά κλειδιά.

Άσκηση 2: Κρυπτογράφηση/Αποκρυπτογράφηση με συμμετρικό κλειδί

Σ' αυτή την άσκηση θα χρησιμοποιήσουμε την εντολή mcrypt για την κρυπτογράφηση αρχείων. Στην πραγματικότητα η εντολή mcrypt αποτελεί αντικατάσταση της δημοφιλούς εντολής crypt του Unix. Η εντολή Crypt ήταν ένα εργαλείο κρυπτογράφησης που χρησιμοποιούσε τον αλγόριθμο κρυπτογράφησης της γερμανικής μηχανής "Αίνιγμα". Η μηχανή αυτή χρησιμοποιήθηκε για την μετάδοση πολεμικών μηνυμάτων κατά το δεύτερο παγκόσμιο πόλεμο. Σήμερα το πρόγραμμα Mcrypt υποστηρίζει ένα σύνολο από διαφορετικούς αλγόριθμους κρυπτογράφησης δεδομένων, όπως ο AES.

Στην ουσία θα χρησιμοποιήσουμε την εντολή στο linux για να κρυπτογραφήσουμε αρχεία δεδομένων. Υπάρχουν αντίστοιχες διανομές για linux και Windows που πρέπει να εγκατασταθούν καθώς και διαδεδομένα script σε php για την ενσωμάτωση του σε σελίδες στο Διαδίκτυο.

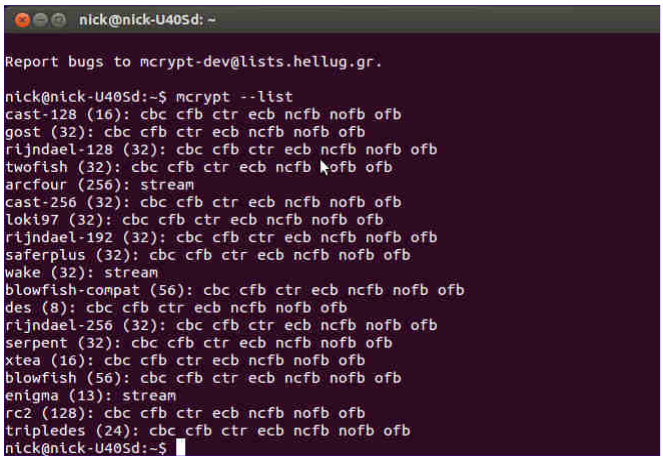
Βήμα 1: Η σύνταξη της εντολής

Μπορούμε να εκτελέσουμε σε ένα τερματικό του linux την εντολή:

```
mcrypt --help
```

για να δούμε τη σύνταξη και όλες τις παραμέτρους που παρέχονται, π.χ. για να δούμε όλους τους διαθέσιμους αλγόριθμους κρυπτογράφησης που υποστηρίζονται εκτελούμε την εντολή:

```
mycript --list .
```



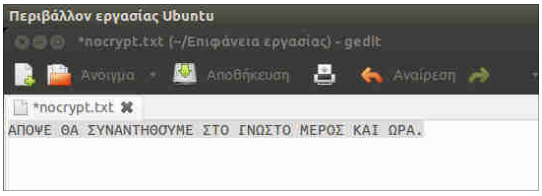
Εικόνα 2: Διαθέσιμοι Αλγόριθμοι Κρυπτογράφησης/Αποκρυπτογράφησης

Βήμα 2: Κρυπτογράφηση

Για να κρυπτογραφήσουμε ένα αρχείο με όνομα nocrypt.txt χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης blowfish εκτελούμε την εντολή:

```
mcrypt -a blowfish nocrypt.txt
```

όπου θα μας ζητηθεί η λέξη κλειδί δύο φορές. Το μέγεθος του κλειδιού δεν πρέπει να ξεπερνά τους 512 χαρακτήρες.

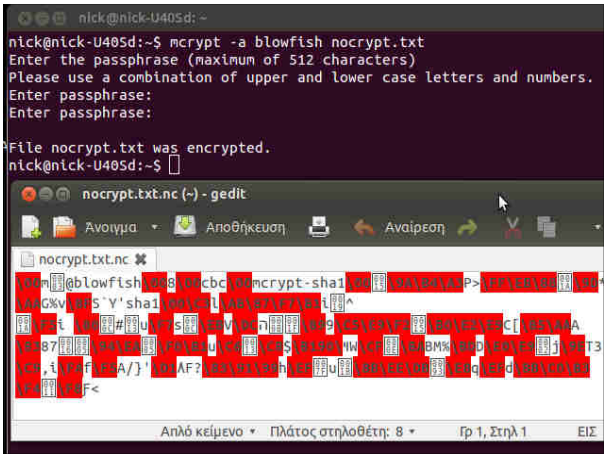


Εικόνα 3: Το έγγραφο που θα κρυπτογραφηθεί

Επίσης μπορούμε να χρησιμοποιήσουμε την παράμετρο -u για να διαγράψουμε το αρχικό αρχείο κατά την διαδικασία της κρυπτογράφησης.

Μετά την εκτέλεση της εντολής παράγεται το κρυπτογραφημένο αρχείο nocrypt.txt.nc

και είναι αδύνατο να το ανοίξουμε με ένα κειμενογράφο, όπως φαίνεται παρακάτω.



Εικόνα 4: Αποτέλεσμα μετά την κρυπτογράφηση

Βήμα 3. Αποκρυπτογράφηση

Για να αποκρυπτογραφήσουμε το αρχείο εκτελούμε την εντολή:

```
mcrypt -d nocrypt.txt.nc
```

και δημιουργείται το αποκρυπτογραφημένο αρχείο με όνομα nocrypt.txt.

Δραστηριότητα 2η

1. Διερευνήστε τα χαρακτηριστικά του αλγόριθμου Blowfish και των άλλων αλγορίθμων που υποστηρίζονται από το εργαλείο κρυπτογράφησης mcrypt. Εντοπίστε τον αλγόριθμο που αντιστοιχεί στον AES-128.
2. Οι μαθητές, είτε κατά άτομα είτε κατά ομάδες, θα μπορούσαν να συμφωνήσουν μεταξύ τους κάποια μυστικά κλειδιά και να ανταλλάξουν κρυπτογραφημένα μηνύματα ακολουθώντας τα παραπάνω βήματα.

Άσκηση 3: Κρυπτογράφησης/Αποκρυπτογράφησης με τη χρήση Δημόσιου κλειδιού

Σ' αυτή την άσκηση θα χρησιμοποιήσουμε το εργαλείο gnupg που μας επιτρέπει λειτουργίες κρυπτογράφησης-αποκρυπτογράφησης δημόσιου κλειδιού και ψηφιακών υπογραφών. Το εργαλείο αυτό έρχεται προεγκατεστημένο σε αρκετές διανομές του linux. Αν δεν είναι εγκατεστημένο, υπάρχουν διανομές για Linux, Windows και MacOs που μπορούν να εγκατασταθούν στους υπολογιστές του εργαστηρίου. Μπορείτε να αναζητήσετε περισσότερες πληροφορίες στο δικτυακό τόπο https://gnupg.org. Ολη η λειτουργία του εργαλείου gnupg, που θα δούμε, υλοποιείται σε μορφή εντολών τερματικού, παρόλα αυτά υπάρχουν αρκετά εργαλεία με γραφικό περιβάλλον που χειρίζονται τις εντολές του GnuPG, όπως το gpa ή το seahorse κ.ά.

Βήμα 1. Δημιουργία ζεύγους κλειδιών

Αρχικά κατά την κρυπτογράφηση με το δημόσιο κλειδί πρέπει να δημιουργηθεί ένα ζευγάρι δημόσιου-ιδιωτικού κλειδιού. Η εντολή για την δημιουργία των κλειδιών είναι:

```
gpg --gen-key
```

```
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Αρχικά μας ζητάτε να επιλέξουμε τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιήσουμε μεταξύ των RSA και DSA/Elgamal. Προτείνεται ο αλγόριθμος DSA/Elgamal, καθώς δεν υπάρχουν περιορισμοί στη χρήση του.

```
Παρακαλώ επιλέξτε τον τύπο του κλειδιού που θέλετε:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (για υπογραφή μόνο)
   (4) RSA (για υπογραφή μόνο)
Η επιλογή σας; 2
```

Οι επόμενες επιλογές αφορούν το μήκος κλειδιού και την διάρκειά του.

```
DSA keys may be between 1024 and 3072 bits long.
What keysize do you want? (2048) 1024
Το μέγεθος κλειδιού που ζητήθηκε είναι 1024 bits
Παρακαλώ ορίστε για πόσο καιρό το κλειδί θα είναι έγκυρο.
         0 = το κλειδί δεν λήγει ποτέ
      <n>  = το κλειδί λήγει σε n μέρες
      <n>w = το κλειδί λήγει σε n εβδομάδες
      <n>m = το κλειδί λήγει σε n μήνες
      <n>y = το κλειδί λήγει σε n έτη
Το κλειδί είναι έγκυρο για; (0) 0
Key does not expire at all
Is this correct? (y/N) y
```

Τέλος μας ζητούνται στοιχεία, όπως το όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου που θα συσχετιστούν και θα ταυτοποιούν το κλειδί, καθώς και μία Μυστική Φράση που θα μας επιτρέπει τη χρησιμοποίηση του ιδιωτικού κλειδιού.

```
You need a user ID to identify your key; the software constructs the
user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"
Αληθινό Όνομα: Nikos X.
Διεύθυνση Email: gtest4sek@gmail.com
Σχόλιο: Αυτο ειναι ενα  δοκιμαστικό κλειδί!
Χρησιμοποιείτε το `utf-8' σετ χαρακτήρων.
Επιλέξατε το USER-ID:
    "Nikos X. (Αυτο ειναι ενα  δοκιμαστικό κλειδί!)
<gtest4sek@gmail.com>"
```

```
Αλλαγή (N)όνομα, (C)σχόλιο, (E)mail ή (O)εντάξει/(Q)τερματισμός; O
Χρειάζεστε μια Φράση κλειδί για να προστατεύσετε το μυστικό κλειδί.
```

Κατόπιν παράγεται το ζευγάρι κλειδιών. Επειδή ο αλγόριθμος, που παράγονται οι τυχαίοι πρώτοι αριθμοί, βασίζεται σε τυχαία bytes που χρησιμοποιούνται από την μνήμη του υπολογιστή, ο αλγόριθμος μας προτείνει να εκτελέσουμε διάφορες άλλες λειτουργίες στον υπολογιστή.

```
Πρέπει να δημιουργηθούν πολλά τυχαία bytes. Είναι καλή ιδέα να κάνετε
κάποια εργασία (πληκτρολογήστε, μετακινήστε το ποντίκι,
χρησιμοποιήστε
τους δίσκους) κατα τη διάρκεια υπολογισμού πρώτων αριθμών. Αυτό δίνει
στη γεννήτρια τυχαίων αριθμών μια ευκαιρία να μαζέψει αρκετή
εντροπία.
++++++++++++++++++++.+++++.++++++++++.+++++..++++++++++.++++++++++++
++++++++++++++++..++++++++++++++++++++++++.++++++++++++++.++++++++
+++++++.........................>..+++++.............................
....+++++
Δεν υπάρχουν αρκετά διαθέσιμα τυχαία bytes.  Προτείνεται να
αναμείνετε ή
να απασχολείτε το λειτουργικό σύστημα μέχρι αυτό να συγκεντρώσει
περισσότερη εντροπία! (Χρειάζονται 156 περισσότερα bytes)
Πρέπει να δημιουργηθούν πολλά τυχαία bytes. Είναι καλή ιδέα να κάνετε
κάποια εργασία (πληκτρολογήστε, μετακινήστε το ποντίκι,
χρησιμοποιήστε
τους δίσκους) κατά τη διάρκεια υπολογισμού πρώτων αριθμών. Αυτό δίνει
στη γεννήτρια τυχαίων αριθμών μια ευκαιρία να μαζέψει αρκετή
εντροπία.
++++++++++++++++++++.++++++++++++++++++++++++++++++.++++++++++++++++
++++++++..+++++.+++++.++++++++++.++++++++++++++++++++++++.+++++.++++
+>.+++++.........+++++^^^^
gpg: key 218051DA marked as ultimately trusted
το δημόσιο και το μυστικό κλειδί δημιουργήθηκαν και υπογράφηκαν.
gpg: έλεγχος της trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
pub   1024D/218051DA 2015-08-24
      Key fingerprint = B220 22D2 BB69 F8BA 6716  351C 33F2 AE7D 2180
51DA
uid                  Nikos X. (Αυτό είναι ένα δοκιμαστικό κλειδί!)
<gtest4sek@gmail.com>
sub   1024g/874D9A17 2015-08-24
```

Αφού δημιουργηθούν τα κλειδιά, το ιδιωτικό κλειδί φυλάσσεται εσωτερικά μέσα στον υπολογιστή και το δημόσιο κλειδί πρέπει να το εξάγουμε προς δημοσίευση.

Τα χαρακτηριστικά του δημόσιου κλειδιού που εμφανίζονται και πρέπει να γνωρίζουμε, ώστε να μπορούμε να το διαχειριζόμαστε, είναι τα: uID, keyID και fingerprint.

Στο συγκεκριμένο παράδειγμα είναι:

- **uid:** Nikos X. (Αυτό είναι ένα δοκιμαστικό κλειδί!) <gtest4sek@gmail.com>
- **keyid:** 218051DA
- **fingerprint:** B220 22D2 BB69 F8BA 6716 351C 33F2 AE7D 2180 51DA

Στις περισσότερες περιπτώσεις, που απαιτείται η εισαγωγή του uID με την παράμετρο –u, μπορούμε να χρησιμοποιήσουμε το keyID με την παράμετρο -k.

Δραστηριότητα 3η (Α' Μέρος)

1. Αρχικά θα μπορούσε να ξεκινήσει σε ατομικό ή σε ομαδικό επίπεδο μέσα στο εργαστήριο μια ιστοεξερεύνηση για την διερεύνηση του προγράμματος PGP και κατ' επέκταση του GnuPG. Επίσης θα μπορούσαν να διερευνηθούν τα χαρακτηριστικά των αλγόριθμων RSA και DSA/Elgamal.
2. Κατόπιν θα μπορούσε να διερευνηθεί η εντολή gpg –help η οποία εμφανίζει όλες τις παραμέτρους και τη σύνταξη των εντολών του εργαλείου.
3. Τέλος, σε ατομικό επίπεδο ή ομαδικό επίπεδο, οι μαθητές θα πρέπει να δημιουργήσουν τα δικά τους ζευγάρια κλειδιών ακολουθώντας τη διαδικασία, όπως έχει περιγραφεί.

Βήμα 2: Εξαγωγή Δημόσιου κλειδιού

Στο επόμενο βήμα πρέπει να εξάγουμε το δημόσιο κλειδί και να το μεταδώσουμε σ' αυτούς με τους οποίους θέλουμε να ανταλλάσσουμε δεδομένα που έχουμε προστατεύσει. Η εντολή για την εξαγωγή του δημόσιου κλειδιού είναι: gpg -a --export -o [όνομα αρχείου].

Η παράμετρος –export ενεργοποιεί την εξαγωγή του δημόσιου κλειδιού και η παράμετρος -a χρησιμεύει, ώστε η εξαγωγή του κλειδιού να γίνει σε μορφή 7 bit ASCII κειμένου αντί σε μορφή binary που είναι η προεπιλογή. Ο λόγος γι' αυτό είναι, ότι σ' αυτή τη μορφή μπορεί εύκολα το δημόσιο κλειδί να το διαχειριστεί κάποιος σαν κείμενο. Κατόπιν πρέπει με κάποιο τρόπο να το δημοσιεύουμε, είτε ανακοινώνοντάς το μέσω ηλεκτρονικού ταχυδρομείου, είτε μέσω δικτύου, είτε με το χέρι ή εκτύπωση, αν το κλειδί είναι αρκετά μικρό, είτε τέλος δημοσιεύοντάς το σε κάποιο δημόσιο εξυπηρετητή κλειδιών (public key server). Για περισσότερες πληροφορίες για την δημοσίευση σε keyservers συμβουλευτείτε τη σελίδα https://www.gnupg.org/gph/en/manual/x457.html.

```
gpg   -a  --export   -o pkfile.txt
cat pkfile.txt
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQGiBFXaxUcRBADfY8sW8htJYRENMRHr2DIz8UCQLiH/YrtM6AstkTlWynuljWdY
UUBK7YuFoRDR8h/FfHFM+Pn9k5GOjmmre7Sz8QWeXitf2uuBjUQJV6hBAfM07DPi
J/qd/oue6g74+BXmWBK7lwojWLWG+QoVMjJvW7xjmHvLG5zX78kALJurawCglYSU
Xjn5XpMKJGonjGyi11ATFaUD/jYFQ9nHIst5VYPer+zACa3icFjnA7p0OHy/C7xZ
hYu1j/jIZcbINP+eXfwmPwMcN4TGV5j1tNE25QlPyne5Dwq3M3ahbUJckFcADJoS
ZyISjVqUNe4IrjpyfDFGx98mwUfU7/v2LhjXj1f9VM9vcuPRcpNiwmkCSjmmsts8
+RvGBADQbTS12fiB1MZxRkpKjI1PhE/H+Gu8Vlc3je9wjk/xZNB8XmzlYFFSiEAm
m5q3vTjjalaM8DhTW3oMVoq4B7w5jfLBL/7IgXb9YeNiv/SO3WgsP+fFAvv/BGid
Onzdg0ylhFeY1ZkIHJ8G+TiN4W7xntgp72hIXeIn7vwuKJ7cqrRhTmlrb3MgWC4g
KM6Rz4XPhM6/IM61zrnOvc6xzrkgzrXOvc6xICDOtM6/zrrOuc68zrHPg8+EzrnO
```

```
us+MIM66zrvOtc65zrTOryEpIDxndGVzdDRzZWtAZ21haWwuY29tPohiBBMRAgAi
BQJV2sVHAhsDBgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRBe76Lwq5U+YTud
AJ9Ip6D+KhaboueGP3By4Q/j3of32ACfba+JQmKx7Fm3hB9uPfUc1RpxL265AQ0E
VdrFRxAEAJhNLLFnh0KH+CdztzV4DaFpBLXj5x29UiCXkJno92yRcXhUe102VZDB
7uHza0KDAETwojRNUy1TTZa02qt9VWYWsjuN+J91ggGDuWIARvWyVBrJ2BhtY4r7
h70BU+gmUgSdFunmT5oFQuvHAP8o9PqSweqyS7i3mYV1qBhX87iXAAQNBACLIoDx
gA1yq2jcjf3ffQJaCiSpgeyKFZMB2E464EmsaxpdA3o1lJ47aYo/5aHbPqfgTZOJ
QjOQ1ysq76fERhaLwdesqcakz/VkugPH2uzf+u9XG88thUwtiOfnn8P8SC5fyAWx
OIS/gj3bMC+TMEo10dkON4teWp8KHyCvxk3Jd4hJBBgRAgAJBQJV2sVHAhsMAAoJ
EF7vovCrlT5hZJ4AnRMN+d5218J2YCZBMvY8shxYcwncAJ9hVwRfxNtB9Emjzcfn
EsBY3VTbzg==
=SpdW
-----END PGP PUBLIC KEY BLOCK-----
```

Από την άλλη πλευρά υπάρχει η δυνατότητα εξαγωγής του ιδιωτικού κλειδιού με την εντολή:

gpg --export-secret-keys key-id [uID] -o [Αρχείο Εξαγωγής]

```
gpg -a --export-secret-keys -u gtest4sek@gmail.com -o pksecret.txt
cat pksecret.txt
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

lQHhBFXaxUcRBADfY8sW8htJYRENMRHr2DIz8UCQLiH/YrtM6AstkTlWynuljWdY
UBK7YuFoRDR8h/FfHFM+Pn9k5GOjmmre7Sz8QWeXitf2uuBjUQJV6hBAfM07DPi
J/qd/oue6g74+BXmWBK7lwojWLWG+QoVMjJvW7xjmHvLG5zX78kALJurawCglYSU
Xjn5XpMKJGonjGyi11ATFaUD/jYFQ9nHIst5VYPer+zACa3icFjnA7p0OHy/C7xZ
hYu1j/jIZcbINP+eXfwmPwMcN4TGV5j1tNE25QlPyne5Dwq3M3ahbUJckFcADJoS
ZyISjVqUNe4IrjpyfDFGx98mwUfU7/v2LhjXj1f9VM9vcuPRcpNiwmkCSjmmsts8
+RvGBADQbTS12fiB1MZxRkpKjI1PhE/H+Gu8Vlc3je9wjk/xZNB8XmzlYFFSiEAm
m5q3vTjjalaM8DhTW3oMVoq4B7w5jfLBL/7IgXb9YeNiv/SO3WgsP+fFAvv/BGid
Onzdg0ylhFeY1ZkIHJ8G+TiN4W7xntgp72hIXeIn7vwuKJ7cqv4DAwJw5/ih8ayJ
EWC3GQTtrdxEODK0sQ4QXc8lC/7D7Be6C5tHkRr0LZh5BXb13teOvZZAjifAy4bL
QuG39LRhTmlrb3MgWC4gKM6Rz4XPhM6/IM61zrnOvc6xzrkgzrXOvc6xICDOtM6/
zrrOuc68zrHPg8+EzrnOus+MIM66zrvOtc65zrTOryEpIDxndGVzdDRzZWtAZ21h
aWwuY29tPohiBBMRAgAiBQJV2sVHAhsDBgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIX
gAAKCRBe76Lwq5U+YTudAJ9Ip6D+KhaboueGP3By4Q/j3of32ACfba+JQmKx7Fm3
hB9uPfUc1RpxL26dAVgEVdrFRxAEAJhNLLFnh0KH+CdztzV4DaFpBLXj5x29UiCX
kJno92yRcXhUe102VZDB7uHza0KDAETwojRNUy1TTZa02qt9VWYWsjuN+J91ggGD
uWIARvWyVBrJ2BhtY4r7h70BU+gmUgSdFunmT5oFQuvHAP8o9PqSweqyS7i3mYV1
qBhX87iXAAQNBACLIoDxgA1yq2jcjf3ffQJaCiSpgeyKFZMB2E464EmsaxpdA3o1
lJ47aYo/5aHbPqfgTZOJQjOQ1ysq76fERhaLwdesqcakz/VkugPH2uzf+u9XG88t
```

```
hUwtiOfnn8P8SC5fyAWxOIS/gj3bMC+TMEo10dkON4teWp8KHyCvxk3Jd/4DAwJw
5/ih8ayJEWDarMTRkCLkTV+itgI/q1dQTgbV49uLNirzatRlbBFjZA+5QDAOxEt4
PGzNqTt9/XSqp1QDWZTqSkd0Wx+MQIhJBBgRAgAJBQJV2sVHAhsMAAoJEF7vovCr
lT5hZJ4AoJAoAslUtf3EQaTEPtnDYV6GLxkrAJ0Twg8NI2JIpSOvQBV6Kwo5g2Kx
xQ==
=ypEv
-----END PGP PRIVATE KEY BLOCK-----
```

Την εξαγωγή του ιδιωτικού κλειδιού την κάνουμε μόνο για λόγους πρόληψης, περιπτώσεων καταστροφής ή απώλειας, έτσι ώστε να μπορέσουμε να το εισάγουμε ξανά στη βάση κλειδιών. Σε καμία περίπτωση δεν το ανακοινώνουμε και δεν το αποστέλλουμε μέσω δημόσιων καναλιών επικοινωνίας.

Δραστηριότητα 3η (Β' Μέρος)

4. Σ' αυτή τη φάση οι μαθητές πρέπει να εξάγουν το δημόσιο κλειδί και να το μεταδώσουν με κάθε δυνατό τρόπο στους άλλους μαθητές.
5. Κατόπιν θα μπορούσε να γίνει μια ιστοεξερεύνηση για δημόσιους εξυπηρετητές κλειδιών και να γίνει μια δοκιμαστική καταχώρηση κλειδιών.

Βήμα 2. Πιστοποιητικό ανάκλησης

Αν για κάποιο λόγο το κλειδί αχρηστευτεί, για παράδειγμα ξεχάσουμε τη μυστική φράση, χαθεί ή διαγραφεί ή διαρρεύσει το ιδιωτικό κλειδί, πρέπει με κάποιο τρόπο να γνωστοποιήσουμε την ανάκληση του δημόσιου κλειδιού, ιδιαίτερα αν το έχουμε γνωστοποιήσει σε ευρεία κλίμακα. Αυτό το ρόλο έχει ένα πιστοποιητικό ανάκλησης κλειδιού. Για να δημιουργήσουμε το πιστοποιητικό χρησιμοποιούμε την εντολή:

gpg --gen-revoke [uID]

Η παράμετρος --gen-revoke ενεργοποιεί τη λειτουργία δημιουργίας του πιστοποιητικού και το [uID] αναφέρεται σε μέρος ή όλο το userID που ταυτοποιεί το κλειδί.

```
gpg -o  pist_anaklisis.txt --gen-revoke gtest4sek@gmail.com
```

```
sec  1024D/AB953E61 2015-08-24 Nikos X. (Αυτό είναι ένα δοκιμαστικό κλειδί!) <gtest4sek@gmail.com>
```

Θα μας ζητηθεί ο λόγος που θέλουμε να δημιουργήσουμε το πιστοποιητικό.

```
Create a revocation certificate for this key? (y/N) y
Παρακαλώ επιλέξτε την αιτία για την ανάκληση:
  0 = Δεν έχει οριστεί αιτία
  1 = Το κλειδί έχει εκτεθεί
  2 = Το κλειδί έχει παρακαμφθεί
  3 = Το κλειδί δε χρησιμοποιείται πλέον
  Q = Ακύρωση
(Πιθανώ να θέλετε να επιλέξετε το 1 εδώ)
Η απόφαση σας; 0
```

```
Πληκτρολογήστε μια προαιρετική περιγραφή· τέλος με μια άδεια γραμμή:
>
Αιτία για ανάκληση: Δεν έχει οριστεί αιτία
(Δεν δόθηκε περιγραφή)
Is this okay? (y/N) y
```

Τέλος θα μας ζητηθεί η Μυστική Φράση που είναι συνδεδεμένη με το μυστικό κλειδί.

```
You need a passphrase to unlock the secret key for
user: "Nikos X. (Αυτό είναι ένα δοκιμαστικό κλειδί!)
<gtest4sek@gmail.com>"
1024-bit DSA key, ID AB953E61, created 2015-08-24


Εξαναγκασμός εξόδου σε θωρακισμένο ASCII.
Το πιστοποιητικό ανάκλησης δημιουργήθηκε.


Παρακαλώ μετακινείστε το σε ένα μέσο που μπορεί να κρυφτεί εύκολα· εάν η
Mallory αποκτήσει πρόσβαση σε αυτό το πιστοποιητικό μπορεί να αχρηστεύσει
το κλειδί σας. Είναι έξυπνο να τυπώσετε αυτό το πιστοποιητικό και να το
φυλάξετε μακριά, για την περίπτωση που το μέσο δεν διαβάζεται πια. Αλλά
προσοχή το σύστημα εκτύπωσης στο μηχάνημά σας μπορεί να αποθηκεύσει την
εκτύπωση και να την κάνει διαθέσιμη σε άλλους!
```

Σημαντικό είναι να αποθηκεύσουμε σε ασφαλές μέρος το πιστοποιητικό εκεί, όπου δεν υπάρχει πρόσβαση από άλλους, αφού μια πιθανή διαρροή μπορεί να αχρηστεύσει το κλειδί. Σε περίπτωση ανάκλησης μπορούμε ακόμα να αποκρυπτογραφούμε παλαιότερα δεδομένα με το ιδιωτικό κλειδί και να επαληθεύουμε υπογραφές, όπως θα δούμε παρακάτω, αλλά πλέον δεν θα είναι δυνατή η κρυπτογράφηση νέων δεδομένων.

Δραστηριότητα 3η (Γ' Μέρος)

6. Σ' αυτή τη δραστηριότητα οι μαθητές θα πρέπει να δημιουργήσουν πιστοποιητικά ανάκλησης και να τα προστατεύσουν αποθηκεύοντάς τα σε κάποιο προσωπικό φάκελο.
7. Σε τελική φάση μετά την εκτέλεση των επόμενων δραστηριοτήτων θα μπορούσε να γίνει ανάκληση του δημόσιου κλειδιού.

Βήμα 4: Εισαγωγή Δημόσιου κλειδιού.

Τώρα, στην πλευρά του παραλήπτη, πρέπει το δημόσιο κλειδί του αποστολέα να αποθηκευτεί σε κάποια λίστα – βάση δεδομένων κλειδιών, ώστε να μπορεί να χρησιμοποιηθεί με το εργαλείο gnupg στη διαδικασία κρυπτογράφησης. Η εντολή για την εισαγωγή του δημόσιου κλειδιού είναι gpg --import [δεδομένα]

```
gpg --import pkfile.txt
```

```
gpg: key 218051DA: "Nikos X. (Αυτό είναι ένα δοκιμαστικό κλειδί!)
<gtest4sek@gmail.com>" not changed

gpg: Συνολικός αριθμός που επεξεργάστηκαν: 1

gpg:              αμετάβλητα: 1
```

Επίσης έχουμε ένα σύνολο από εντολές και μπορούμε να διαχειριστούμε τη βάση με τα κλειδιά, είτε τα έχουμε δημιουργήσει εμείς είτε τα έχουμε εισάγει ως δημόσια κλειδιά.

Για να εμφανίσουμε λίστες με τα γνωστά κλειδιά και τα χαρακτηριστικά τους οι εντολές είναι:

- gpg --list-keys. Εμφανίζει τα δημόσια κλειδιά.
- gpg --list-secret-keys. Εμφανίζει τα ιδιωτικά κλειδιά.
- gpg --list-sigs. Εμφανίζει τις υπογραφές.
- gpg --fingerprint. Εμφανίζει το χαρακτηριστικό αποτύπωμα του κλειδιού.

Επίσης έχουμε την δυνατότητα να διαγράψουμε κάποιο κλειδί

- gpg --delete-secret-key uID. Διαγράφει το μυστικό κλειδί.
- gpg --delete-key uID. Διαγράφει το δημόσιο κλειδί.

Τέλος έχουμε την δυνατότητα να επεξεργαστούμε τα χαρακτηριστικά που σχετίζονται με το κλειδί, όπως την διάρκεια, το όνομα κ.λπ.

- gpg --edit-key uID

Με την εντολή αυτή έχουμε την δυνατότητα να υπογράψουμε το δημόσιο κλειδί ω εισάγοντας μέσα στα περιεχόμενα του το επίπεδο ασφάλειας που επιθυμούμε.

Δίνοντας την εντολή:

```
gpg --edit-key gtest4sek@gmail.com
```

```
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
gpg>
```

Μεταφερόμαστε στο περιβάλλον διαχείρισης του κλειδιού όπου έχουμε την δυνατότητα να δούμε το αποτύπωμα του με την εντολή:

```
gpg> frp
```

```
pub   1024D/AB953E61 2015-08-24 Nikos X. (Αυτό είναι ένα δοκιμαστικό
κλειδί!) <gtest4sek@gmail.com>
 Αποτύπωμα πρωτεύοντος κλειδιού: 6041 A15D BD2A 9821 6084  49D0 5EEF
A2F0 AB95 3E61
```

Τώρα μπορούμε, αν θέλουμε, να επαληθεύσουμε το κλειδί με τον ιδιοκτήτη του, για παράδειγμα τηλεφωνικά, και αφού το επιβεβαιώσουμε, μπορούμε να χρησιμοποιήσουμε την εντολή:

```
gpg> sign
```

και κατόπιν να επιβεβαιώσουμε το κλειδί αν έχει επικυρωθεί.

```
gpg> check
```

```
uid  Nikos X. (Αυτό είναι ένα δοκιμαστικό κλειδί!)
<gtest4sek@gmail.com>
sig!3        AB953E61 2015-08-24  [ιδιο-υπογραφή]
```

Δραστηριότητα 3η (Δ' Μέρος)

8. Σ' αυτή τη δραστηριότητα οι μαθητές θα πρέπει να εισάγουν στη βάση κλειδιών τα δημόσια κλειδιά που τους έχουν αποσταλεί.
9. Με τις εντολές διαχείρισης μπορούν να ελέγξουν τα δημόσια και ιδιωτικά κλειδιά που διαθέτουν, μπορούν να τα επεξεργαστούν, καθώς και να διαγράψουν κάποιο απ' αυτά και να το ξαναεισάγουν.

Βήμα 5. Κρυπτογράφηση δεδομένων

Τώρα αν θέλει ο παραλήπτης με τον ιδιοκτήτη του κλειδιού με κρυπτογραφημένα δεδομένα χρησιμοποιεί την εντολή:

gpg -e -r [uID] [δεδομένα]

Η παράμετρος -r αναφέρεται στον παραλήπτη που πρέπει να εισάγει μέρος ή όλο το uID του ιδιοκτητη που δημιούργησε το δημόσιο κλειδί.

```
gpg -e  -r gtest4sek@gmail.com nocrypt.txt
```

Και έτσι δημιουργείται το κρυπτογραφημένο αρχείο nocrypt.txt.gpg.

```
cat nocrypt.txt.gpg
□□□/□○□*ش□□C4<T□x$G□
1#C□2□#(□□□\]`□□h□#□□□*#□□□□□#□]□;□f#>A&□#fx:p#□-
#□□q□□/□ў□□□□o□i5□□)□Z#□rlY}ª a□□#q□: #!lאaL#-ן--#W-#.--\-7"d---9#5---
[#-#-¯=#g-S-OP-wA- ˚R6U#-m------^zV4Z---:T-E--t-
      -[}-Z-4--t@-I-----t-Nr#"-
X---Z-#--Bty#-@-- -Ò-w)ъ+#Y---r-'---##--W---0+---[ 喇Y •p ••ㄷ ᕮ? ₾].
 ••XMu# •


 J ••0 @ЂW5 # ••' H/ • # h f pa ˇ¨6 ••3-∩◆◆<ᵡ0◆#◆◆◆
```

Τώρα μπορεί με κάποιο τρόπο να σταλεί το κρυπτογραφημένο αρχείο πίσω στον ιδιοκτήτη των κλειδιών που κατέχει και το ιδιωτικό κλειδί και μπορεί να το αποκρυπτογραφήσει.

Δραστηριότητα 3η (Ε' Μέρος)

10. Εδώ οι μαθητές έχουν την δυνατότητα να κρυπτογραφήσουν αρχεία κειμένου με τα δημόσια κλειδιά των συμμαθητών τους και να τους τα αποστείλουν, ώστε να ακολουθήσει η διαδικασία αποκρυπτογράφησης.

Βήμα 6. Αποκρυπτογράφηση

Με την εντολή gpg -d nocrypt.txt.gpg μπορεί ο κάτοχος του ιδιωτικού κλειδιού να αποκρυπτογραφήσει τα δεδομένα. Η παράμετρος -o [Αρχείο Εξόδου] μπορεί να χρησιμοποιηθεί για να αποθηκευτούν τα αποκρυπτογραφημένα δεδομένα.

```
gpg -o output.txt -d nocrypt.txt.gpg
```

Και, αφού ζητηθεί η Μυστική Φράση, γίνεται η αποκρυπτογραφηση.

```
You need a passphrase to unlock the secret key for
user: "Nikos X. (Αυτό είναι ένα δοκιμαστικό κλειδί!)
<gtest4sek@gmail.com>"
1024-bit ELG-E key, ID E75AC1FD, created 2015-08-24 (main key ID
AB953E61)
gpg: encrypted with 1024-bit ELG-E key, ID E75AC1FD, created 2015-08-
24
      "Nikos X. (Αυτό είναι ένα δοκιμαστικό κλειδί!)
<gtest4sek@gmail.com>"
ΑΠΟΨΕ ΘΑ ΣΥΝΑΝΤΗΘΟΎΜΕ ΣΤΟ ΓΝΩΣΤΟ ΜΕΡΟΣ ΚΑΙ ΩΡΑ.
```

Δραστηριότητα 3η (ΣΤ' Μέρος)

11. Εδώ αντίστοιχα οι μαθητές που παραλαμβάνουν τα αρχεία κειμένου πρέπει να τα αποκρυπτογραφήσουν χρησιμοποιώντας το ιδιωτικό τους κλειδί, όπως περιγράφηκε στο παραπάνω βήμα.

Βήμα 7. Ψηφιακή υπογραφή

Χρησιμοποιείται για να πιστοποιήσουμε την αυθεντικότητα των δεδομένων, δηλαδή ότι εμείς στέλνουμε τα δεδομένα και όχι κάποιος άλλος. Για να το πετύχουμε αυτό χρησιμοποιούμε τις ψηφιακές υπογραφές.

Η εντολή για να ενεργοποιήσουμε την δημιουργία μιας ψηφιακής υπογραφής με βάση το ιδιωτικό κλειδί και τα δεδομένα είναι:

gpg --sign [δεδομένα]

Με τη χρήση όμως αυτής της εντολής το αποτέλεσμα δεν είναι σε αναγνώσιμη μορφή και γι' αυτό χρησιμοποιούμε την εντολή:

gpg --clearsign [δεδομένα]

```
gpg --clearsign nocrypt.txt
```

και, αφού μας ζητηθεί η Μυστική Φράση, για να χρησιμοποιηθεί το μυστικό κλειδί, παράγεται η σύνοψη μηνύματος με βάση τον αλγόριθμο SHA-1 και παράγεται το υπογεγραμμένο αρχείο με κατάληξη .asc.

```
You need a passphrase to unlock the secret key for
user: "Nikos X. (Αυτό είναι ένα δοκιμαστικό κλειδί!)
<gtest4sek@gmail.com>"
1024-bit DSA key, ID AB953E61, created 2015-08-24
```

```
cat nocrypt.txt.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
```

```
ΑΠΟΨΕ ΘΑ ΣΥΝΑΝΤΗΘΟΎΜΕ ΣΤΟ ΓΝΩΣΤΟ ΜΕΡΟΣ ΚΑΙ ΩΡΑ.
```

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

iEYEARECAAYFAlXayMQACgkQXu+i8KuVPmE5pQCdHAa4/TCuUUaL9Swyb7nwFc+j
MBwAn2wQ0nZUPYHCGPviH+DHAedXtIuJ
=yxCv
-----END PGP SIGNATURE-----
```

Πολλές φορές χρειάζεται να παραχθεί η ψηφιακή υπογραφή σε ξεχωριστό αρχείο, ώστε να τη αποστείλουμε για λόγους μεγαλύτερης ασφάλειας ξεχωριστά, ιδιαίτερα αν τα δεδομένα είναι σε μορφή binary. Η εντολή που χρησιμοποιούμε σ' αυτή την περίπτωση είναι:

gpg -b [δεδομένα]

Δραστηριότητα 3η (Ζ' Μέρος)

12. Σ' αυτή τη δραστηριότητα οι μαθητές με τη χρήση του εργαλείου έχουν την δυνατότητα να παράγουν τη σύνοψη μηνύματος με τη συνάρτηση κατακερματισμού του αλγόριθμου SHA-1 με βάση το ιδιωτικό τους κλειδί και τα δεδομένα και είτε να την επισυνάψουν ως ψηφιακή υπογραφή στο ίδιο αρχείο με το κείμενο, είτε να αποστείλουν την ψηφιακή υπογραφή ως ξεχωριστό αρχείο.
13. Σαν δεύτερη δραστηριότητα οι μαθητές μπορούν να κρυπτογραφήσουν το υπογεγραμμένο αρχείο και μετά να το αποστείλουν στους συμμαθητές τους.

Βήμα 8. Ψηφιακή υπογραφή

Τέλος, αν ο παραλήπτης του μηνύματος θέλει να επαληθεύσει την υπογραφή, πρέπει να χρησιμοποιήσει την εντολή:

gpg --verify [όνομα υπογεγραμμένου αρχείου]

```
gpg --verify nocrypt.txt.asc
```

⇩

```
gpg: Signature made Δευ 24 Αύγ 2015 10:33:24 πμ EEST using DSA key ID
AB953E61
gpg: Good signature from "Nikos X. (Αυτό είναι ένα δοκιμαστικό
κλειδί!) <gtest4sek@gmail.com>"
```

Δραστηριότητα 3η (Η' Μέρος)

1. Εδώ αντίστοιχα οι μαθητές που παραλαμβάνουν τα υπογεγραμμένα αρχεία κειμένου μπορούν να επαληθεύσουν την ταυτότητα του αποστολέα. Αν τα δεδομένα είναι κρυπτογραφημένα, θα πρέπει σε πρώτο στάδιο να τα αποκρυπτογραφήσουν χρησιμοποιώντας το ιδιωτικό τους κλειδί και κατόπιν να τα επαληθεύσουν.
2. Ως ολοκληρωμένη εργασία θα μπορούσε να επαναληφθεί η διαδικασία με άλλο τύπο δεδομένων ή χρησιμοποιώντας για δεδομένα μηνύματα ηλεκτρονικού ταχυδρομείου.

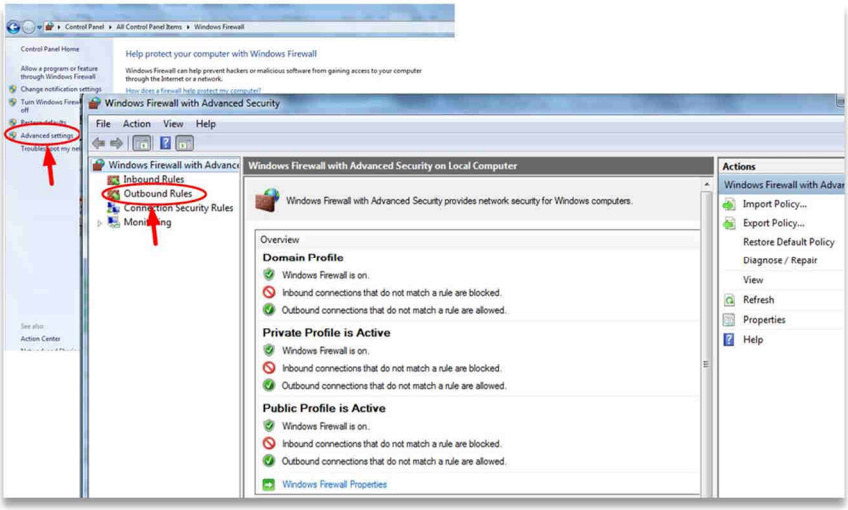
Άσκηση 4: Διερεύνηση του firewall.

Επειδή το firewall που είναι εγκατεστημένο στους υπολογιστές μπορεί να ποικίλλει από εργαστήριο σε εργαστήριο,, το παρακάτω παράδειγμα αποτελεί μια ενδεικτική μέθοδο για την περιγραφή της λειτουργίας φιλτραρίσματος και μπορεί να διαμορφωθεί κατάλληλα κατά περίπτωση. Σκοπός της άσκησης είναι οι μαθητές να κατανοούν την λειτουργία του firewall και να αποκτήσουν την ικανότητα να εφαρμόζουν στοιχειωδώς ρυθμίσεις της λειτουργίας του.

Υπάρχουν πολλές ελεύθερες διανομές λογισμικού firewall καθώς και εμπορικές που μπορούν να χρησιμοποιηθούν ανάλογα για την προστασία από ένα σταθμό εργασίας μέχρι και στην διαχείριση του τείχους προστασίας ενός τοπικού δικτύου. Μερικά λογισμικά που μπορεί εύκολα να γίνει η αναζήτηση τους, η λήψη και εγκατάσταση τους είναι τα ZoneAlarm, TinyWall, Comodo FireWall κ.α. Στην συγκεκριμένη περίπτωση σαν παράδειγμα θα χρησιμοποιηθεί το προεγκατεστημένο τείχος ασφάλειας των Windows 7, όπου θα εφαρμοστεί φιλτράρισμα σε ορισμένες θύρες επικοινωνίας και κατόπιν για να γίνει κατανοητό από τους μαθητές θα γίνει έλεγχος στην επικοινωνία με αυτά τα χαρακτηριστικά. Σημειώνεται ότι παρόμοια μέθοδος μπορεί να εφαρμοστεί σε οποιοδήποτε firewall.

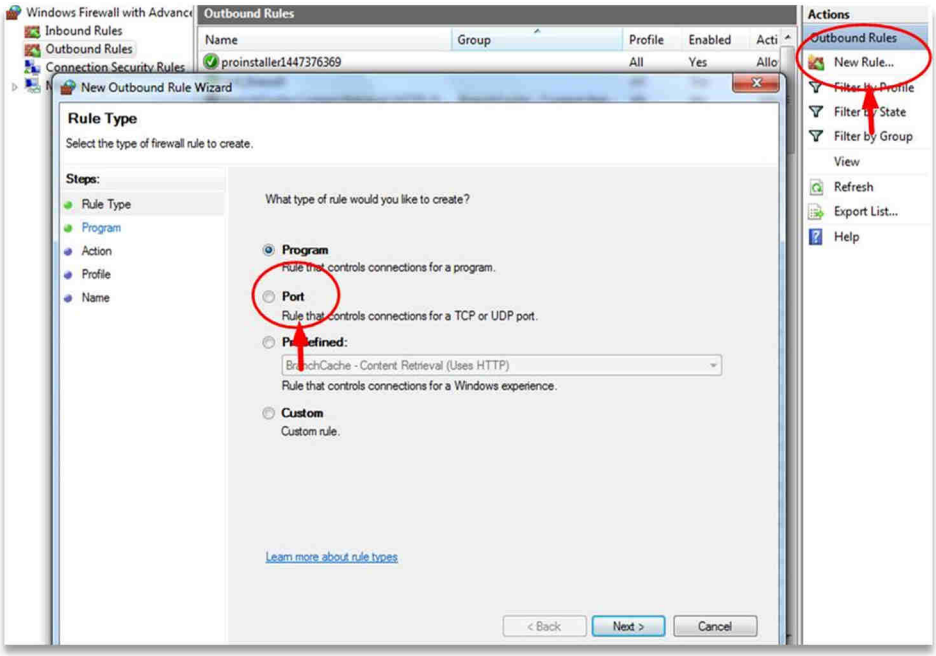
Βήμα 1. Στον πίνακα ελέγχου των Windows οι μαθητές ξεκινούν τη διαχείριση του Windows Firewall

και επιλέγουν ρυθμίσεις για προχωρημένους «Advanced settings». Εδώ παρουσιάζονται όλα τα φίλτρα που έχουν δημιουργηθεί είτε αυτόματα από το σύστημα είτε από τους χρήστες του υπολογιστή για όλες τις εισερχόμενες και εξερχόμενες μεταφορές δεδομένων.



Εικόνα 5: Windows Firewall

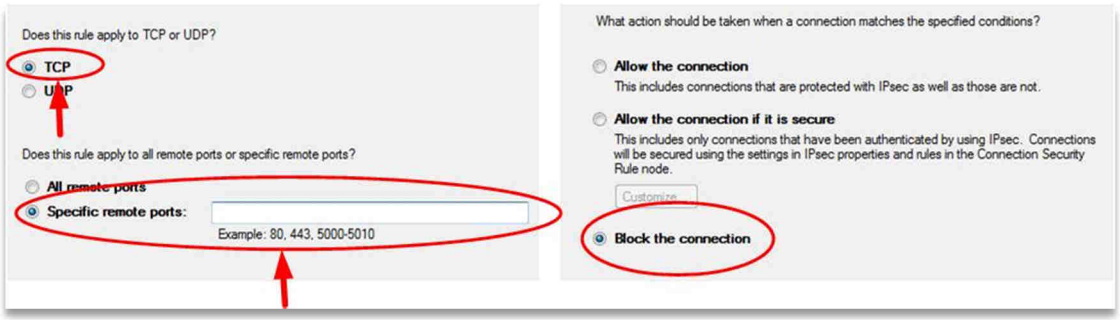
Βήμα 2. Σ' αυτό το σημείο θα δημιουργηθεί ένας κανόνας (φίλτρο) για την εξερχόμενη κίνηση δεδομένων επιλέγοντας «Κανόνες Εξερχόμενης επικοινωνίας – Outbound Rules». Στο παράθυρο που εμφανίζεται επιλέγεται «Προσθήκη νέου κανόνα- New Rule» και στο επόμενο παράθυρο διαλόγου «Τύπος Κανόνα- Rule Type» που εμφανίζεται επιλέγεται «Θύρα – Port».



Εικόνα 6: Δημιουργία νέου κανόνα

Στο πλαίσια διαλόγου που εμφανίζεται καθορίζεται το πρωτόκολλο μεταφοράς το «TCP» και στις πόρτες στο άλλο άκρο του εξυπηρετητή που πρέπει να ελέγχονται οι πόρτες «23-80». Κατόπιν, στην επόμενη επιλογή που επιτρέπει ή αποτρέπει την επικοινωνία με αυτά τα χαρακτηριστικά επιλέγεται «Block this Connection» δηλαδή αποτροπή της επικοινωνίας.

Τέλος πρέπει να καθοριστεί ένα όνομα γι' αυτό το φίλτρο όπως «test_firewall» με το οποίο θα αποθηκευτεί. Από αυτή την στιγμή και μετά αποτρέπεται όσο είναι ενεργό αυτό το φίλτρο η εξερχόμενη επικοινωνία σε υπηρεσίες που κάνουν χρήση του πρωτόκολλου TCP και θύρες 23-80 στην πλευρά του εξυπηρετητή. Τέτοιες υπηρεσίες είναι οι τυπικές υπηρεσίες διαδικτύου όπως 23-Telnet ή 80 –Http κ.λπ.



Εικόνα 7: Ορισμός φίλτρου

Τέλος πρέπει να ενεργοποιηθεί το φίλτρο με την επιλογή «Enable Rule». Επίσης όταν κατασκευάζεται ένα νέο φίλτρο πρέπει να γίνει έλεγχος ότι δεν συγκρούεται με κανόνες που έχουν καθορίσει άλλα φίλτρα.

Βήμα 3. Σ' αυτό το βήμα πολύ εύκολα να ελεγχθεί η λειτουργία αυτού του φίλτρου, για παράδειγμα θα πρέπει μέσω ενός φυλλομετρητή να γίνει προσπάθεια οι μαθητές να πλοηγηθούν στην ιστοσελίδα http που τυπικά χρησιμοποιεί το TCP και την πόρτα 80, όπως η ιστοσελίδα http://www.sch.gr. Αμέσως διαπιστώνεται ότι δεν είναι δυνατή η πλοήγηση σ' αυτή την ιστοσελίδα. Αν τώρα γίνει αλλαγή στις ρυθμίσεις του φίλτρου και επιτρέπουν

οι συνδέσεις με αυτά τα χαρακτηριστικά δηλαδή να ενεργοποιηθεί η επιλογή «Allow the connection» θα διαπιστωθεί ότι επιτρέπεται πάλι η δυνατότητα πλοήγησης στην ιστοσελίδα.

Δραστηριότητα

1. Οι μαθητές μπορούν να επικυρώσουν τη λειτουργία του φίλτρου που περιγράφηκε στην άσκηση χρησιμοποιώντας κάποια άλλη υπηρεσία στο εύρος των θυρών που έχει καθοριστεί 23-80, π.χ. η υπηρεσία telnet στη θύρα 23. Θα μπορούσαν σε γραμμή εντολής να εκτελεστεί η **telnet telehack.com** με ενεργό ή όχι το φίλτρο του τείχους ασφάλειας.
2. Σε επόμενο στάδιο οι μαθητές διερευνώντας τις δυνατότητες του Firewall των Windows, θα μπορούσαν να δημιουργήσουν φίλτρα για τη εισερχόμενη κίνηση ή να ελέγχουν άλλα χαρακτηριστικά όπως:
    - το πρόγραμμα- διεργασία που δημιούργησε την κίνηση
    - τον υπολογιστή ή τον χρήστη που δημιούργησε την κίνηση
    - την διεύθυνση ή το εύρος των διευθύνσεων.

Βιβλιογραφία

Αλεξόπουλος, Α., & Λαγογιάννης, Γ. (2012). *Τηλεπικοινωνίες και δίκτυα υπολογιστών,* (8η έκδ.). Αθήνα.

Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). *Τεχνολογία Δικτύων Επικοινωνιών* (1η έκδ.). Αθήνα: ΟΕΔΒ.

Kizza, J. M. (2015). *Guide to Computer Network Security 3rd Edition,* Springer.

Schneier, Bruce (2001). *Secrets and Lies: Digital Security in a Networked World.* Wiley Computer Publishing.

Tanenbaum, A. S. (2000). *Δίκτυα Υπολογιστών* (3η έκδ.). Αθήνα: Εκδόσεις Παπασωτηρίου.

ΠΑΡΑΡΤΗΜΑ

Π.1 Πρωτόκολλα Token Bus/Ring

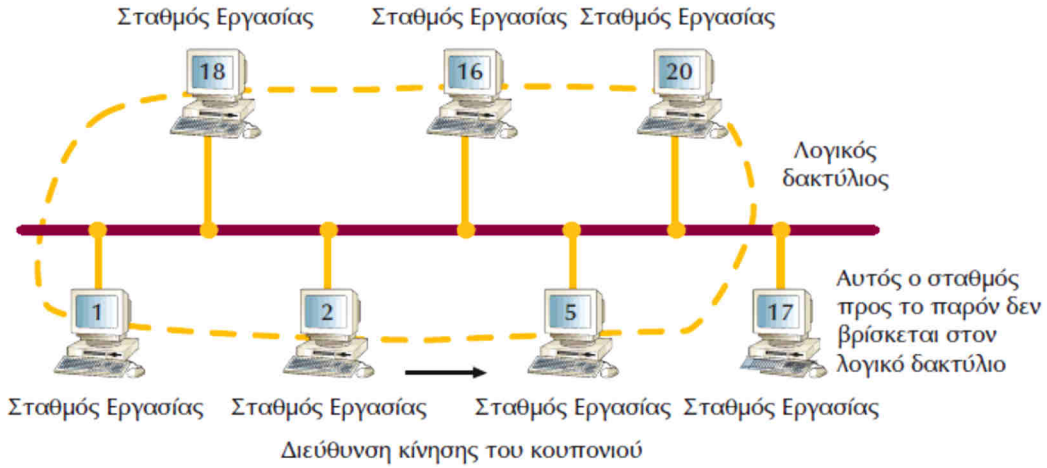
Πρότυπο πρόσβασης στο μέσο IEEE 802.4 - Αρτηρία με Κουπόνι (Token Bus)

Όταν η IEEE έβγαζε το πρότυπο 802.3, η χρήση του οποίου είναι πλέον πολύ διαδεδομένη, οι άνθρωποι της βιομηχανίας και κυρίως αυτοί που ασχολούνται με αυτοματισμούς, όπως η General Motors, είχαν κάποιους ενδοιασμούς. Οι επιφυλάξεις ξεκινούσαν από τον πιθανοτικό τρόπο λειτουργίας του 802.3. Για παράδειγμα ένας σταθμός ίσως να χρειαστεί να περιμένει αυθαίρετα μεγάλο χρόνο για να στείλει κάποια πλαίσια. Στην περίπτωση όμως της βιομηχανίας μπορεί ένας σταθμός να χρειαστεί να στείλει σήμα συναγερμού (αλάρμ). Είναι λογικό να θέλουμε να σχεδιάζουμε συστήματα πραγματικού χρόνου με τη δυνατότητα πρόβλεψης της καθυστέρησης κρίσιμης πληροφορίας.

Ετσι δημιουργήθηκε το πρότυπο **IEEE 802.4,** που ονομάζεται και **αρτηρία με κουπόνι (token bus).** Παράδειγμα πρωτοκόλλου, που στηρίζεται στο token bus, είναι το MAP (Manufacturing Automation Protocol, Πρωτόκολλο Αυτοματισμού Κατασκευής), που αναπτύχθηκε από την εταιρεία General Motors. Πάντως πρέπει να επισημάνουμε, ότι το IEEE 802.4 δεν είναι ιδιαίτερα διαδεδομένο, επειδή έχει αρκετά πολύπλοκο μηχανισμό λειτουργίας και παρουσιάζονται δυσχέρειες στην εμφάνιση ελκυστικών εναλλακτικών λύσεων στη χρήση ποικίλων φυσικών μέσων.

Σε φυσικό επίπεδο γίνεται χρήση ομοαξονικού καλωδίου 75 Ohm ευρείας ζώνης διαφόρων χαρακτηριστικών (RG6, RG11, RG59, και JT4750J από 0.5 έως 1 ίντσα). Δυνατές ταχύτητες μετάδοσης είναι από 1.5 και 10 Mbps. Για τη μετάδοση των σημάτων μπορούν να χρησιμοποιηθούν τρεις διαφορετικές αναλογικές τεχνικές διαμόρφωσης: διαμόρφωση συχνότητας συνεχούς φάσης (phase continuous FSK), διαμόρφωση συχνότητας σύμφωνης φάσης (phase coherent FSK) και πολυεπίπεδη διπλοδυαδική διαμόρφωση κατά πλάτος και συχνότητα (multi level duobinary AM/FSK). Επίσης καθορίζονται πλήρως τα ηλεκτρικά και μηχανικά χαρακτηριστικά για το μέσο μετάδοσης καθώς και οι υπηρεσίες, που παρέχει το φυσικό επίπεδο στο υποεπίπεδο ελέγχου πρόσβασης στο μέσο (MAC).

Το πρότυπο IEEE 802.4 καθορίζει επίσης και υπηρεσίες, που προσφέρει το υποεπίπεδο ελέγχου πρόσβασης στο μέσο προς το υποεπίπεδο ελέγχου λογικής σύνδεσης (LLC).



Σχήμα Π.1.α: Αρτηρία με κουπόνι

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Στη συνέχεια, θα περιγράψουμε τα κυριότερα χαρακτηριστικά της μεθόδου ελέγχου πρόσβασης στο μέσο αρτηρίας με κουπόνι. Η αρτηρία με κουπόνι είναι μια τοπολογία γραμμικής ή δενδρικής μορφής. Οι σταθμοί εργασίας σχηματίζουν λογικό δακτύλιο. Η φυσική θέση των σταθμών στο δίκτυο είναι άσχετη και ανεξάρτητη από τη θέση τους στο λογικό δακτύλιο (βλέπε Σχήμα Π.1.α).

Ο κάθε σταθμός στον λογικό δακτύλιο γνωρίζει τη διεύθυνση των σταθμών, που λογικά βρίσκονται πριν και μετά από αυτόν. Στο δίκτυο κυκλοφορεί ειδικό πλαίσιο, που ονομάζεται κουπόνι (token). Κάθε κουπόνι περιέχει διεύθυνση προορισμού. Ο σταθμός, που λαμβάνει το κουπόνι, έχει το δικαίωμα πρόσβασης στο μέσο για κάποιο μέγιστο χρόνο. Στο χρόνο, που έχει ο σταθμός εργασίας, μπορεί να μεταδώσει τα πλαίσια του. Ο σταθμός περνάει το κουπόνι στο λογικά επόμενο του σταθμό όταν:

- δεν έχει να μεταδώσει πλαίσια δεδομένων,
- ή έχει στείλει όλα τα πλαίσια δεδομένων, που είχε για μετάδοση, πριν λήξει ο χρόνος του,
- ή όταν τελειώσει ο μέγιστος χρόνος, που είχε στη διάθεση του.

Όπως είναι φανερό από τον τρόπο λειτουργίας του token bus, από τη στιγμή που μόνο ένας σταθμός εργασίας κατέχει το κουπόνι κάθε φορά, δεν γίνονται συγκρούσεις. Τα πλαίσια, που στέλνονται από ένα σταθμό εργασίας στο μέσο, περιέχουν τη διεύθυνση προορισμού και, έτσι, είναι δυνατό ο σταθμός που θα δει πλαίσια με διεύθυνση προορισμού ίδια με τη δική του, να λάβει τα πλαίσια που τον αφορούν. Τα πλαίσια με διαφορετική διεύθυνση προορισμού απορρίπτονται.

Στο πρότυπο αρτηρίας με κουπόνι ορίζονται τέσσερα είδη προτεραιότητας, 0,2,4 και 6 για τα πλαίσια, όπου 0 είναι η χαμηλότερη μορφή προτεραιότητας και 6 η υψηλότερη. Είναι σαν να έχει ο κάθε σταθμός τέσσερις διαφορετικές ουρές για τα πλαίσια που θέλει να μεταδώσει, με την κάθε ουρά να έχει διαφορετική προτεραιότητα. Όταν τα δεδομένα έρχονται στο υποεπίπεδο MAC, ελέγχεται η προτεραιότητά τους και προωθούνται σε μία από τις τέσσερις ουρές. Όταν ένας σταθμός έχει το κουπόνι, ξεκινά την αποστολή των δεδομένων από την ουρά με τη μεγαλύτερη προτεραιότητα, δηλαδή την ουρά 6 και στη συνέχεια, την ουρά 4,2 και 0 με τη σειρά. Υπάρχει, βέβαια, η δυνατότητα, να γίνουν ρυθμίσεις σε μετρητές, που κρατά ο κάθε σταθμός εργασίας χωριστά και να καθορισθούν τα ποσοστά χρόνου, που έχει η κάθε ουρά στη διάθεση της από το συνολικό χρόνο, που έχει ο σταθμός εργασίας το κουπόνι. Αν μία ουρά δεν έχει δεδομένα να στείλει, ο χρόνος, που αντιστοιχεί στη συγκεκριμένη ουρά, δεν χάνεται αλλά υπάρχει η δυνατότητα χρησιμοποίησής του από τις ουρές χαμηλότερης προτεραιότητας. Είναι φανερό, ότι οι ουρές με χαμηλές προτεραιότητες μπορεί να μην προλάβουν να στείλουν τα δεδομένα τους όταν ο σταθμός εργασίας έχει το κουπόνι. Από την άλλη πλευρά όμως, μπορούμε με σωστή ρύθμιση των μετρητών ενός σταθμού, να είμαστε σίγουροι, ότι σημαντικά δεδομένα (όπως αλάρμ μηχανής) θα μεταδοθούν. Επιπλέον, μπορούμε να κάνουμε εκτίμηση της μέγιστης δυνατής καθυστέρησης. Ο μηχανισμός προτεραιοτήτων του IEEE 802.4 είναι ένας από τους σημαντικούς λόγους, που τον έχει κάνει δημοφιλή σε δίκτυα βιομηχανικών αυτοματισμών.

Άλλες λειτουργίες, οι οποίες περιγράφονται στο πρότυπο, σχετίζονται με τη συντήρηση του λογικού δακτυλίου. Τέτοιες λειτουργίες είναι: η αρχικοποίηση του λογικού δικτύου, η πρόσθεση ή αφαίρεση σταθμών εργασίας στο λογικό δακτύλιο καθώς και η επανόρθωση από λάθος. Για τις λειτουργίες συντήρησης του δακτυλίου οι σταθμοί εργασίας σε περιοδικά διαστήματα στέλνουν κουπόνια ειδικής μορφής. Για τον έλεγχο των κουπονιών ειδικής μορφής υπάρχουν διάφορες μεταβλητές, όπως για παράδειγμα ο μέγιστος αριθμός αναζήτησης σταθμών, ή ο μέγιστος χρόνος περιστροφής του κουπονιού. Κάθε σταθμός, που συμμετέχει στο δακτύλιο δέχεται ένα κουπόνι ειδικής μορφής για τη συντήρηση του δακτυλίου, ελέγχει τις διάφορες παραμέτρους και, όταν χρειάζεται τροποποιεί, κάποιες από τις μεταβλητές του κουπονιού ή το ακυρώνει, προκειμένου να εξασφαλίσει την

απρόσκοπτη λειτουργία του δακτυλίου. Γενικά θα λέγαμε, ότι ο μηχανισμός συντήρησης δακτυλίου είναι σχετικά περίπλοκος και για την υλοποίησή του χρειάζεται η συμβολή αρκετών μετρητών, που ελέγχει ο κάθε σταθμός εντός του δακτυλίου.

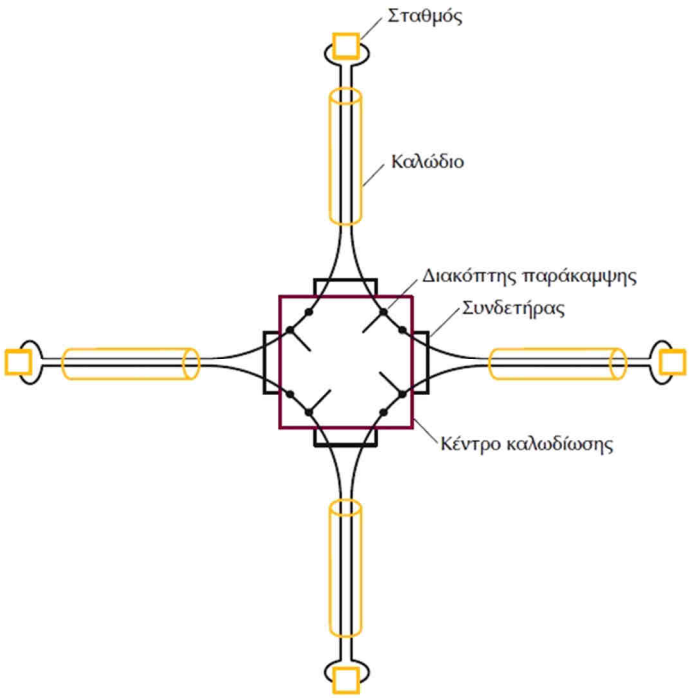
Πρότυπο πρόσβασης στο μέσο IEEE 802.5 - Δακτύλιος με Κουπόνι (Token Ring)

Το δίκτυο token ring αναπτύχθηκε αρχικά από την IBM και παραμένει η κύρια τοπολογία τοπικού δικτύου, που χρησιμοποιεί η IBM. Το πρότυπο **IEEE 802.5** είναι σχεδόν ταυτόσημο και πλήρως συμβατό με το token ring. Το IEEE 802.5 αναπτύχθηκε μετά από το token ring. Γενικά, η χρήση του όρου token ring χρησιμοποιείται τόσο για το token ring της IBM, όσο και για το IEEE 802.5.

Το πρότυπο καθορίζει τις υπηρεσίες, που προσφέρει το υποεπίπεδο ελέγχου πρόσβασης στο μέσο (MAC) προς το υποεπίπεδο ελέγχου λογικής (LLC). Επίσης, καθορίζει τις προδιαγραφές σύνδεσης του σταθμού εργασίας στο φυσικό μέσο και τα λειτουργικά, ηλεκτρικά και μηχανικά χαρακτηριστικά της σύνδεσης με το μέσο μετάδοσης. Υποτίθεται, ότι ο κάθε σταθμός εργασίας συνδέεται στο δακτύλιο μέσω μονάδας σύζευξης με το καλώδιο. Το πρότυπο αναφέρει λεπτομέρειες, που αφορούν τη σηματοδοσία, την κωδικοποίηση και τους υποστηριζόμενους ρυθμούς δεδομένων. Προδιαγράφονται, επίσης, οι υπηρεσίες, τις οποίες παρέχει το φυσικό επίπεδο προς το υποεπίπεδο MAC. Το πρότυπο, όμως, δεν καθορίζει προδιαγραφές για το ίδιο το μέσο, δηλαδή το καλώδιο.

Στην πραγματικότητα, η υλοποίηση του δακτυλίου γίνεται με συνδέσεις από σημείο σε σημείο. Μία από τις επικρίσεις για τα δίκτυα δακτυλίου είναι, ότι, εάν κάπου έχουμε διακοπή του καλωδίου, ο δακτύλιος πεθαίνει. Το πρόβλημα αυτό λύνεται με τη χρήση κέντρου καλωδίωσης, όπως φαίνεται και στο Σχήμα Π.1.β.

Μέσα στο κέντρο καλωδίωσης υπάρχουν διακόπτες παράκαμψης, οι οποίοι τροφοδοτούνται με ηλεκτρικό ρεύμα από τους σταθμούς. Εάν κοπεί ο δακτύλιος ή εάν σταθμός τεθεί εκτός λειτουργίας, η διακοπή του ρεύματος θα απελευθερώσει το ρελέ και θα παρακάμψει το σημείο, που υπάρχει πρόβλημα. Η ενεργοποίηση των ρελέ μπορεί να γίνεται και με κάποιο λογισμικό.



Σχήμα Π.1.β: Υλοποίηση δακτυλίου με κουπόνι με τη χρήση κέντρου καλωδίωσης

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

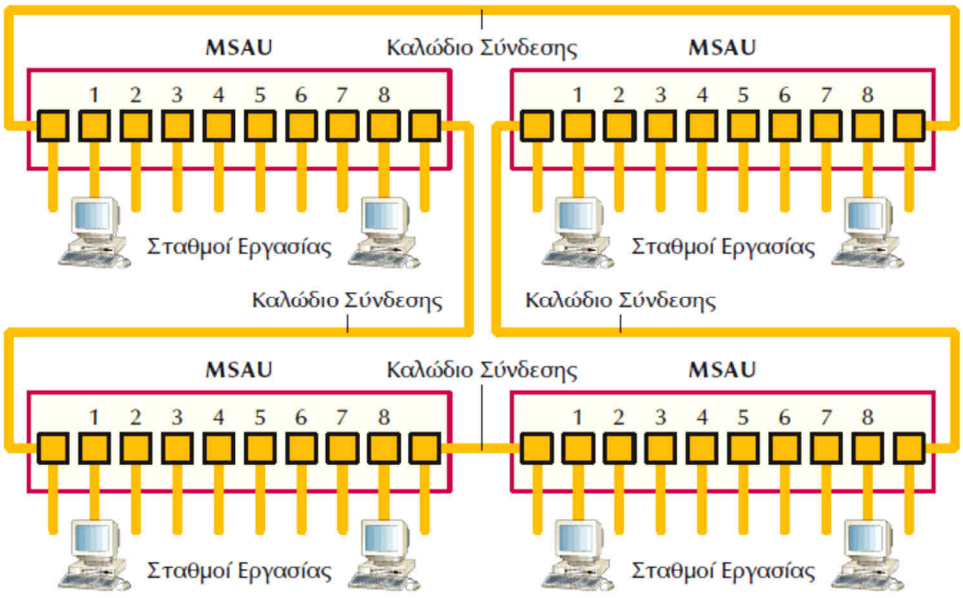
Όπως έχουμε ήδη αναφέρει το token ring και το IEEE 802.5 είναι σχεδόν ταυτόσημα. Παρόλα αυτά υπάρχουν κάποιες διαφορές, που θα αναφέρουμε στη συνέχεια. Το token ring καθορίζει φυσική τοπολογία αστέρα, όπου όλοι οι σταθμοί εργασίας συνδέονται σε συσκευές, οι οποίες ονομάζονται **"Μονάδες Πρόσβασης Πολλαπλών Σταθμών " (Multistation Access Unit, MSAU),** ενώ το IEEE 802.5 δεν καθορίζει την τοπολογία συνδεσμολογίας, αν και στην πράξη οι περισσότερες υλοποιήσεις του IEEE 802.5 βασίζονται σε κέντρα καλωδιώσεων, δηλαδή δακτυλίους με μορφή αστέρα. Στο token ring χρησιμοποιείται συνεστραμμένο ζεύγος, ενώ στο IEEE 802.5 το καλώδιο δεν περιγράφεται. Στον παρακάτω πίνακα Π.1.α, αναφέρονται συνοπτικά τα κυριότερα χαρακτηριστικά του token ring και του IEEE 802.5.

	IBM Token Ring Δίκτυο	IEEE 802.5
Ρυθμοί δεδομένων	4.16Mbps*	4.16Mbps
Σταθμοί / Τμήμα	260 (για καλώδιο S.T.P)	250
	72 (για καλώδιο U.T.P)	
Φυσική Τοπολογία	Αστέρας	Δεν καθορίζεται
Μέσο	Συνεστραμένο ζεύγος	-//-
Σηματοδοσία	Βασικής ζώνης	Βασικής ζώνης
Μέθοδος πρόσβασης	Πέρασμα κουπονιού	Πέρασμα κουπονιού
Κωδικοποίηση σήματος	Διαφορική Manchester	Διαφορική Manchester

Πίνακας Π.1.α: Χαρακτηριστικά token ring και IEEE802.5

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

*Πρέπει να αναφέρουμε ότι υπάρχει δακτύλιος με κουπόνι που υποστηρίζει 16Mbps. Πρόκειται για το λεγόμενο "Early release token" της εταιρείας IBM.



Σχήμα Π.1.γ: Σύνδεση των MSAU για τη δημιουργία ενός μεγάλου δακτυλίου με κουπόνι

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Στο Σχήμα Π.1.γ μπορούμε να δούμε, πώς υλοποιείται η φυσική συνδεσμολογία των σταθμών εργασίας με τη βοήθεια των συσκευών MSAU. Στο Σχήμα αυτό, οι σταθμοί συνδέονται απευθείας στα MSAU. Μπορούμε να συνδέσουμε διάφορα MSAU μεταξύ τους, προκειμένου να σχηματίσουμε μεγάλο δακτύλιο. Οι συσκευές MSAU έχουν ρελέ παράκαμψης για την απομόνωση σταθμών με κάποια βλάβη από τον δακτύλιο.

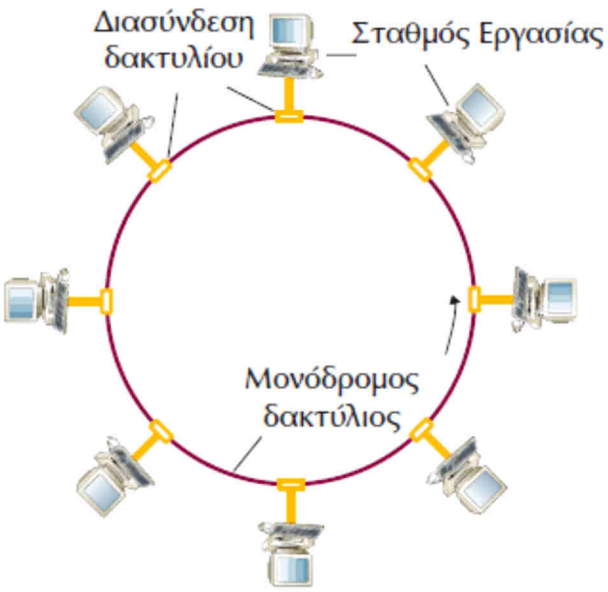
Τα δίκτυα token ring και IEEE 802.5 είναι από τα πρώτα παραδείγματα δικτύων, που λειτουργούν με πέρασμα κουπονιού (token passing). Στο δίκτυο κυκλοφορεί μικρό πλαίσιο, το λεγόμενο κουπόνι. Ο σταθμός, ο οποίος λαμβάνει το κουπόνι, έχει το δικαίωμα να μεταδώσει τα δικά του πλαίσια. Εάν ο σταθμός, που δέχεται το κουπόνι δεν έχει δεδομένα να μεταδώσει, απλώς περνά το κουπόνι στο επόμενο σταθμό του δακτυλίου. Ο σταθμός που δέχεται κουπόνι, διαθέτει καθορισμένο χρόνο που μπορεί να το κρατήσει, δηλαδή μέσα σε αυτό το χρόνο μπορεί να μεταδώσει όσα δεδομένα προλάβει.

Εάν ο σταθμός, ο οποίος λάβει το κουπόνι, έχει δεδομένα να μεταδώσει, μετατρέπει ένα bit του πλαισίου του κουπονιού, δηλαδή μετατρέπει το κουπόνι σε αρχή ακολουθίας πλαισίων (start - frame - sequence). Στη συνέχεια, ο σταθμός προσκολλά τα δεδομένα, προς μετάδοση και τα στέλνει στο δακτύλιο προς τον επόμενό του σταθμό. Κατά τη διάρκεια μετάδοσης των δεδομένων από ένα σταθμό δεν κυκλοφορεί κανένα κουπόνι μέσα στο δακτύλιο. Συνεπώς, οι σταθμοί, που θέλουν να μεταδώσουν τα δικά τους πλαίσια, πρέπει να περιμένουν. Με τον τρόπο αυτό αποφεύγονται οι συγκρούσεις μέσα στο δακτύλιο.

Όταν το πλαίσιο με τα δεδομένα φθάσει, τελικά, στο σταθμό προορισμού, αυτός αντιγράφει τα δεδομένα για περαιτέρω επεξεργασία και ταυτόχρονα μεταβάλει κάποιο bit του πλαισίου, για να μπορέσει να καταλάβει ο σταθμός, που το έστειλε, ότι το πλαίσιο παραλήφθηκε. Το πλαίσιο, όμως, συνεχίζει να κυκλοφορεί μέσα στο δακτύλιο και, τελικά, φθάνει στο σταθμό, που το έστειλε. Ο σταθμός, που έστειλε το πλαίσιο, έχει την ευθύνη να σταματήσει και την κυκλοφορία του πλαισίου από το δακτύλιο. Ο σταθμός, που έστειλε το πλαίσιο βλέποντας τυχόν αλλαγές σε κάποια bit του πλαισίου, που έλαβε, σε σχέση με αυτό που αρχικά έστειλε μπορεί να καταλάβει: εάν ο σταθμός, για τον οποίον προόριζε το πλαίσιο, δεν υπάρχει η είναι ανενεργός, εάν ο σταθμός υπάρχει στο δίκτυο, αλλά για κάποιο λόγο δεν παρέλαβε το πλαίσιο, ή εάν το πλαίσιο έχει παραληφθεί κανονικά.

Ο σταθμός, ο οποίος στέλνει τα δεδομένα, δεν έχει περιορισμό στο μέγεθος του πλαισίου, που μπορεί να στείλει. Κατά συνέπεια, υπάρχει συνήθως πλαίσιο, που ταξιδεύει στο δακτύλιο. Υπάρχει, όμως, και η δυνατότητα να τεμαχίσει τα δεδομένα του σε μικρότερα πλαίσια, πάντα όμως μέσα στο χρόνο, που μπορεί να κρατήσει το κουπόνι.

Με βάση όσα έχουμε αναφέρει, μπορούμε να ξεχωρίσουμε τη λειτουργία των σταθμών στο δακτύλιο σε δύο φάσεις: τη φάση ακρόασης και τη φάση μετάδοσης. Στη φάση ακρόασης βρίσκονται οι σταθμοί που δεν έχουν το κουπόνι. Στη φάση ακρόασης, τοποθετούν κάθε bit του πλαισίου, που δέχονται σε ενδιάμεσο καταχωρητή ενός bit και, κατόπιν, το αντιγράφουν έξω ξανά στο δακτύλιο. Όταν το bit βρίσκεται στον ενδιάμεσο καταχωρητή, η τιμή του μπορεί να επιθεωρηθεί ή και να μεταβληθεί από τον σταθμό. Στη φάση της ακρόασης έχουμε τη λεγόμενη καθυστέρηση 1 - bit. Ο σταθμός, που θα λάβει το κουπόνι και στέλνει το πλαίσιο με τα δεδομένα του βρίσκεται πλέον σε φάση μετάδοσης. Είναι σαν να έχει σπάσει τον δακτύλιο και από το ένα σημείο να στέλνει τα bits του πλαισίου και από το άλλο να λαμβάνει το πλαίσιο, που έχει στείλει, για να ελέγξει ποία ήταν η τύχη του και ταυτόχρονα να σταματά την επανακυκλοφορία της πληροφορίας μέσα στον δακτύλιο.



Σχήμα Π.1.δ. Δίκτυο δακτυλίου με κουπόνι

(*Πηγή: Αρβανίτης, Κ., Κολυβάς, Γ., & Ούτσιος, Σ. (2001). Τεχνολογία Δικτύων Επικοινωνιών*)

Στο τέλος, αφού ο σταθμός μεταδώσει όλα τα δεδομένα του ή του τελειώσει ο χρόνος μετάδοσης που είχε στη διάθεση του, πρέπει να εκδώσει καινούργιο κουπόνι και να το περάσει στον επόμενο σταθμό.

Στο token ring και IEEE 802.5, υποστηρίζονται οκτώ (8) επίπεδα προτεραιότητας. Ο μηχανισμός προτεραιοτήτων είναι αρκετά πολύπλοκος. Μέσα στο κουπόνι υπάρχει πεδίο όπου δηλώνεται ο βαθμός προτεραιότητας. Ένας σταθμός, που θέλει να μεταδώσει δεδομένα με προτεραιότητα Χ, θα πρέπει να περιμένει να περάσει κουπόνι με προτεραιότητα μικρότερη η ίση του Χ. Υπάρχει τρόπος ο σταθμός, που θέλει να μεταδώσει, να δεσμεύσει το επόμενο κουπόνι αλλάζοντας πεδίο του τρέχοντος κουπονιού (κάνοντας δηλαδή ένα είδος κράτησης προτεραιότητας). Επειδή, γενικά, ο μηχανισμός της κράτησης οδηγεί τελικά στην αύξηση της προτεραιότητας, έχουν δημιουργηθεί κανόνες, σύμφωνα με τους οποίους οι σταθμοί, που αυξάνουν την προτεραιότητα, στο τέλος της μετάδοσης του πλαισίου τους, να μεταδώσουν κουπόνι με μικρότερη προτεραιότητα.

Επίσης, στα δίκτυα token ring και IEEE 802.5, υπάρχει και ο μηχανισμός συντήρησης του δακτυλίου. Για τον λόγο αυτόν, ορίζεται σταθμός ως "ενεργός ελεγκτής" (active monitor), ο οποίος ανιχνεύει και διορθώνει, όσο μπορεί, πιθανές καταστάσεις δυσλειτουργίας. Διαθέτει, επίσης, τη δυνατότητα "καθαρισμού" του δακτυλίου, εκδίδοντας το λεγόμενο πλαίσιο καθαρισμού (purge frame). Οι υπόλοιποι σταθμοί του δικτύου συνεργάζονται μεταξύ τους για την παρακολούθηση της συνέχειας του δακτυλίου. Σε περίπτωση βλάβης του ενεργού ελεγκτή, αυτόματα αναλαμβάνει το ρόλο του κάποιος άλλος σταθμός εργασίας μέσα στο δακτύλιο.

Από τον τρόπο λειτουργίας των δικτύων token ring και IEEE 802.5 είναι φανερό, ότι υπάρχει, γενικά, η δυνατότητα εκτίμησης της καθυστέρησης μετάδοσης πλαισίου στο δίκτυο, σε αντίθεση με το πρότυπο IEEE 802.3 (Ethernet). Έτσι, μπορεί να χρησιμοποιηθεί για εφαρμογές, που χρειάζονται μετάδοση σε πραγματικό χρόνο, αρκεί, βέβαια, να καλύπτονται από το εύρος ζώνης, που μπορεί να προσφέρει το δίκτυο.

Π.2 Προϋπολογισμός ζεύξης (Link Budget)

Για να είναι εφικτή μια ασύρματη ζεύξη, θα πρέπει η στάθμη ισχύος του σήματος που εκπέμπεται από τον πομπό και φτάνει στον δέκτη να είναι πάνω από το κατώφλι ευαισθησίας του δέκτη. Αναφερόμενοι στη συσκευή της οποίας τα χαρακτηριστικά δίνονται στον Πίνακα 5.3.α, για να είναι εφικτή η σύνδεση σε ταχύτητα 150MBps (IEEE802.11n), το σήμα που φτάνει στην είσοδο του δέκτη θα πρέπει να είναι μεγαλύτερο από -73dBm.

Τα στοιχεία για τη στάθμη εκπομπής, την ευαισθησία λήψης του δέκτη, τις εξασθενήσεις των καλωδίων και των συνδετήρων, όπως και τα κέρδη (gain) των κεραιών δίνονται από τους κατασκευαστές στα τεχνικά φυλλάδιά τους. Αυτό που πρέπει να υπολογιστεί είναι **η εξασθένηση του σήματος,** καθώς διατρέχει τον χώρο από τον πομπό στον δέκτη και εξαρτάται από **την μεταξύ τους απόσταση** και τη συχνότητα εκπομπής.

Η εξασθένηση του χώρου L_{FS} (σε dB) σε μια ικανοποιητική προσέγγιση δίνεται από τη σχέση:

$$L_{FS}= 32{,}44+20\log(D_{km})+20\log(f_{MHz})$$

Το αλγεβρικό άθροισμα όλων των εξασθενήσεων (-) και των κερδών (+) με τη στάθμη εκπομπής μας δίνει τον **προϋπολογισμό της ζεύξης**

$$P_{rx}= P_{tx}+G_{tant}- L_t- L_{fs}- L_r+G_{rant}$$

P_{rx}: ισχύς στην είσοδο του δέκτη, P_{tx}: ισχύς εκπομπής πομπού, G_{tant}: κέρδος κεραίας πομπού, L_t: απώλειες καλωδίων και συνδετήρων στον πομπό, L_{fs}: εξασθένηση διάδοσης στο χώρο, L_r: απώλειες καλωδίων και συνδετήρων στον δέκτη, G_{rant}: κέρδος κεραίας δέκτη, Ισχύς εκπομπής σε dBm όλα τα άλλα μεγέθη είναι σε dB.

Αν το αποτέλεσμα είναι μεγαλύτερο από το κατώφλι ευαισθησίας του δέκτη, τότε η ζεύξη είναι εφικτή. Πάντα όμως φροντίζουμε να υπάρχει ένα περιθώριο ασφαλείας για τη λειτουργία, ώστε να μη διακοπεί η ζεύξη, εάν αυξηθεί η εξασθένηση διάδοσης λόγω διαφόρων αστάθμητων παραγόντων, όπως έντονη βροχή, πυκνή ομίχλη κ.ά.

Παράδειγμα

Πρόκειται να χρησιμοποιηθεί ένα ζεύγος συσκευών AP με τα χαρακτηριστικά του πίνακα 5.3.α για να αποκατασταθεί μια ζεύξη IEEE802.11n με ταχύτητα 150Mbps σε απόσταση 2300m. Στη μια τοποθεσία χρησιμοποιούνται κατευθυντική κεραία κέρδους 20dBi, δυο συνδετήρες τύπου N με απώλειες 0,15dB ο καθένας και 5m καλώδιο τύπου LMR400 με εξασθένηση 34dB/100m @5,7GHz. Στην άλλη τοποθεσία χρησιμοποιείται ίδιος εξοπλισμός εκτός από την κεραία η οποία έχει κέρδος 18dBi.

Να γίνει ο προϋπολογισμός της ζεύξης και να εκτιμηθεί εάν είναι εφικτή η σύνδεση με περιθώριο 15dB.

Η ισχύς εξόδου σε λειτουργία IEEE802.11n είναι 24dBm

- Οι απώλειες στους συνδετήρες είναι 2 * 0,15 = - 0,3dB
- Οι απώλειες του καλωδίου είναι 5m * 0,34dB/m = -1,7dB
- Το κέρδος της κεραίας είναι +20dB

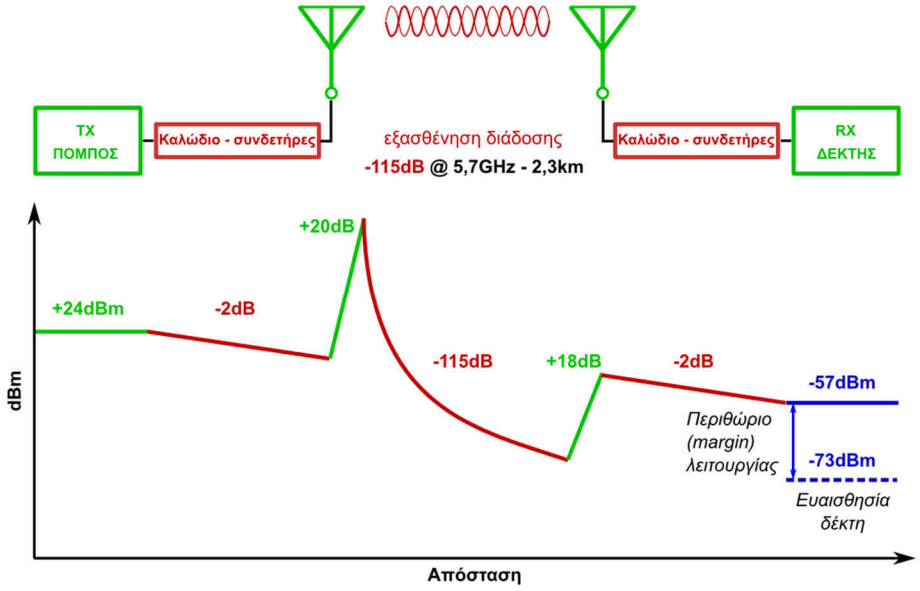
Η εξασθένηση διάδοσης στο χώρο είναι

$$L_{FS}= 32{,}44+20\log(2{,}3)+20\log(5700)= 32{,}44+7{,}235+75{,}117= 114{,}792\approx 115dB$$

δηλ. -115dB

Στην άλλη τοποθεσία,

- Το κέρδος της κεραίας είναι +18dB
- Οι απώλειες στους συνδετήρες είναι 2 * 0,15 = - 0,3dB
- Οι απώλειες του καλωδίου είναι 5m * 0,34dB/m = -1,7dB



Εικόνα Π.2.α: Προϋπολογισμός ζεύξης (Link budget)

Συνολικά είναι 24dBm+20dB-2dB-115dB-2dB+18dB=62-119=-57dBm

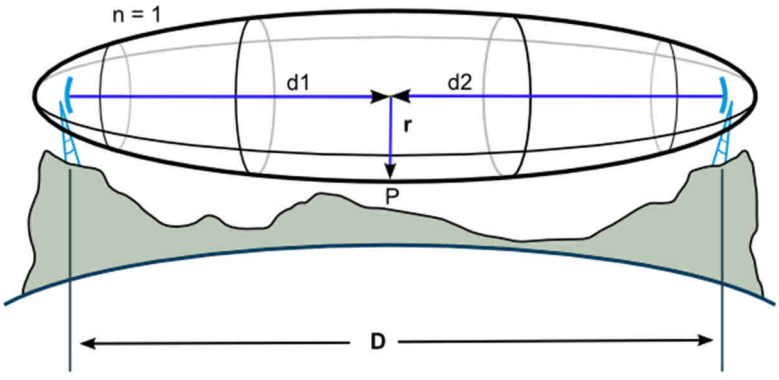
Το περιθώριο είναι -57-(-73)=16dB

Αφού η στάθμη σήματος που φτάνει στην είσοδο του δέκτη είναι -57dBm και είναι μεγαλύτερη από το κατώφλι ευαισθησίας (-73dBm) έχοντας περιθώριο 16dB, η ζεύξη είναι εφικτή με τον επιλεγέντα εξοπλισμό.

Παρατήρηση: Οι εξασθενήσεις και οι απώλειες πάντοτε λαμβάνονται στον προϋπολογισμό με αρνητικό πρόσημο. Τα κέρδη και οι ενισχύσεις με θετικό.

Ζώνη Fresnel

Για να ισχύουν χονδρικά οι παραπάνω σχέσεις και υπολογισμοί, θα πρέπει μεταξύ των κεραιών να υπάρχει οπτική επαφή και σε μια ορισμένη ακτίνα γύρω από τη νοητή ευθεία που ενώνει τις δυο κεραίες να μην παρεμβάλλεται κανένα εμπόδιο. Η περιοχή αυτή έχει σχήμα στερεού ελλειψοειδούς και ονομάζεται **ζώνη Fresnel**.



Εικόνα Π.2.β: Πρώτη ζώνη Fresnel [by Jcmcclurg, wikimedia.org]

Η **ζώνη Fresnel n**, δίνεται από τη σχέση

$$F_n = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}},\ n = 1, 2, 3, \ldots$$

όπου n=1 είναι η πρώτη ζώνη Fresnel κ.ο.κ. Οι αποστάσεις d_1, d_2 και το μήκος κύματος του σήματος (λ) δίνονται σε μέτρα. Το αποτέλεσμα, η ακτίνα r της n ζώνης Fresnel, εξάγεται επίσης σε μέτρα.

Την πιο σημαντική επίδραση στη διάδοση έχει η πρώτη ζώνη, στην οποία δεν πρέπει να παρεμβάλλεται κάποιο αντικείμενο, όπως δέντρα, ψηλά κτίρια κ.λπ. γιατί εισάγουν επιπλέον εξασθένηση.

Αν θεωρήσουμε ότι μας ενδιαφέρει μόνο η **πρώτη ζώνη Fresnel** (n=1) στο μέσον της απόστασης (d1=d2=D/2) και αντί για το μήκος κύματος (λ) θέλουμε να χρησιμοποιήσουμε τη συχνότητα (f=c/λ), τότε η σχέση απλοποιείται σε

$$r_{F1} = 8{,}657\sqrt{\frac{D}{f}}$$

όπου D η απόσταση της ζεύξης σε χιλιόμετρα (km), f η συχνότητα σε Ghz και rF1 σε μέτρα.

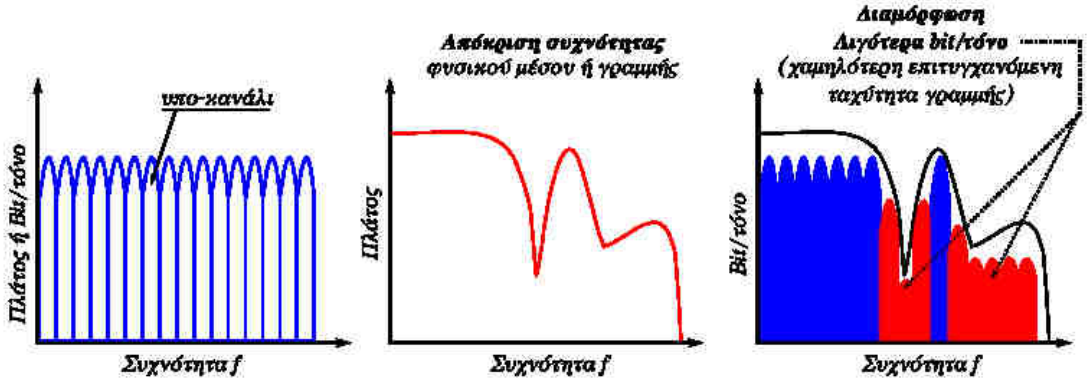
Προσοχή το r δεν είναι απόσταση από το έδαφος, αλλά ακτίνα γύρω από τη νοητή ευθεία που ενώνει τις δυο κεραίες. Αν οι κεραίες βρίσκονται σε ύψος h μέτρων, τότε από το ύψος h-r από το έδαφος και πάνω δεν πρέπει να εξέχει ούτε δέντρο, ούτε κτίριο ή να παρεμβάλλεται κάτι άλλο.

Στο παράδειγμά μας η πρώτη ζώνη Fresnel είναι $r_{F1} = 8{,}657\sqrt{\frac{2{,}3}{5{,}7}} = 5{,}50\,m$

Αν το ύψος των κεραιών είναι 20m από το έδαφος, τότε σε ύψος πάνω από 20-5,5=14,5m δεν πρέπει να εξέχει τίποτε.

Π.3 Διαμόρφωση Διακριτής Πολυτονίας (DMT)

Το διαθέσιμο εύρος ζώνης μιας τηλεφωνικής γραμμής, χωρίς οποιονδήποτε περιορισμό, όπως φίλτρα και περιορισμό εύρους ζώνης για αποκλειστική χρήση απλής τηλεφωνίας φωνής, φτάνει σχεδόν τα 2MHz. Για την εκμετάλλευση όλου αυτού του διαθέσιμου εύρους στην τεχνολογία xDSL, επικράτησε η χρήση της διαμόρφωσης Διακριτής Πολυτονίας (Discrete MultiTone, DMT). Σύμφωνα με αυτή, όλο το διαθέσιμο εύρος ζώνης της γραμμής χωρίζεται σε τμήματα των 4,3125 kHz τα οποία ονομάζονται τόνοι (Tones) ή bins και σε κάθε ένα από αυτά στέλνονται ταυτόχρονα από 2 έως 15 bit. Υπάρχει περίπτωση, ανάλογα με τις πραγματικές συνθήκες της γραμμής, ορισμένοι τόνοι να μην χρησιμοποιηθούν καθόλου ενώ άλλοι να μεταφέρουν περισσότερα ή λιγότερα bit. Από το γεγονός αυτό προκύπτει και η διευκρίνηση των παρόχων Internet ότι μπορούν να προσφέρουν ταχύτητα "μέχρι" μια μέγιστη τιμή (24MBps), γιατί η πραγματική εξαρτάται από τις παραμέτρους της γραμμής, την χρήση των τόνων και το πόσα bit συμφώνησαν το DSL modem με το DSLAM να μεταφέρει κάθε τόνος. Η διαδικασία αυτή είναι δυναμική και προσαρμόζεται πάντα στις τρέχουσες συνθήκες της γραμμής.



Εικόνα Π.3.α: Διαμόρφωση Διακριτής Πολυτονίας (DMT)

Η ίδια τεχνική διαμόρφωσης βρίσκει χρήση και σε άλλες εφαρμογές μετάδοσης δεδομένων όπως στο 100GBps Ethernet.

Π.4 Πρότυπο Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) ISO27001

Το ISO 27001 αποτελεί ένα πρότυπο ΣΔΑΠ με συγκεκριμένες προδιαγραφές που πρέπει να εφαρμόζονται όσον αφορά την διαχείριση της ασφάλειας των πληροφοριών. Αυτό το πρότυπο έχει ευρεία εφαρμογή σε όλους τους τομείς δραστηριοτήτων, από έναν ιδιώτη μέχρι τη βιομηχανία, το εμπόριο, τις υπηρεσίες κ.λπ.

Η ανάπτυξη ενός Συστήματος Διαχείρισης της Ασφάλειας Πληροφοριών (ΣΔΑΠ), σύμφωνο με τις προδιαγραφές του προτύπου ISO 27001, απαιτεί την υλοποίηση τριών φάσεων:

1. Αρχικά πρέπει να δημιουργηθεί ένα πλαίσιο διαχείρισης των πληροφοριών που περιγράφει τις επιδιώξεις και στόχους της ασφάλειας πληροφοριών και καθορίζει τους κανόνες και την πολιτική που είναι δεσμευτικοί και πρέπει αυστηρά να ακολουθούνται.
2. Εντοπισμός και αξιολόγηση των πιθανών κινδύνων λόγω των αδυναμιών ασφαλείας που εντοπίζονται. Με βάση αυτή την αξιολόγηση πρέπει να προσδιοριστούν τα απαιτούμενα μέτρα για την διαχείριση των κίνδυνων της ασφάλειας των πληροφοριών.
3. Στην τρίτη φάση πρέπει να επιλεγούν και να εφαρμοστούν διαδικασίες ελέγχου που εξασφαλίζουν την διαχείριση των κινδύνων ασφαλείας σε αποδεκτά επίπεδα, σύμφωνα με τις επιδιώξεις και τους στόχους για την εφαρμογή της ασφάλειας που έχει αρχικά καθοριστεί. Οι διαδικασίες ελέγχου μπορεί να έχουν την μορφή πολιτικής, πρακτικών, διαδικασιών, οργανικών δομών και λειτουργιών λογισμικού οι οποίες θα διαφοροποιούνται σε κάθε περίπτωση εφαρμογής. Το κόστος επένδυσης για τους απαιτούμενους ελέγχους πρέπει να επιλέγεται και να εφαρμόζεται σε σχέση με τις αρνητικές συνέπειες που τυχόν προκύψουν από αποτυχία της ασφάλειας.

Η εφαρμογή του ISO 27001 δεν εξασφαλίζει την τυχόν παραβίαση της ασφάλειας πληροφοριών, όμως η πιστή εφαρμογή μπορεί να μειώσει κατά πολύ την πιθανότητα παραβίασης ή να μειώσει τις συνέπειες που θα επιφέρει η παραβίαση της ασφάλειας.

Όταν ολοκληρωθεί ή σχεδίαση, εφαρμογή και τεκμηρίωση του συστήματος διαχείρισης ασφάλειας πληροφοριών (ΣΔΑΠ) σύμφωνα με το πρότυπο ISO 27001, μπορεί να γίνει αξιολόγηση και πιστοποίηση από ανεξάρτητο και διαπιστευμένο φορέα πιστοποίησης. Ένας οργανισμός, μια εταιρεία που έχει λάβει πιστοποιητικό ISO 27001 αποδεικνύει ότι έχει λάβει σοβαρά υπόψη και εφαρμόζει συστηματικά μεθόδους προστασίας των πληροφοριών.

Η πιστοποίηση προσφέρει τα ακόλουθα πλεονεκτήματα:

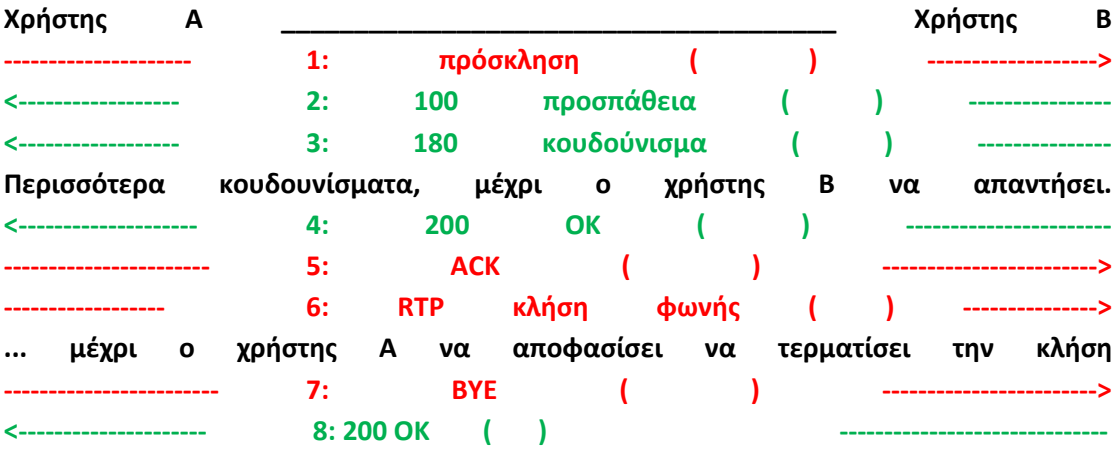
- Εξασφαλίζει την ύπαρξη δέσμευσης για την ασφάλεια πληροφοριών σε όλα τα επίπεδα του οργανισμού.
- Αυξάνει το επίπεδο αξιοπιστίας και εμπιστοσύνης των πελατών, υπαλλήλων, συνεργαζόμενων και γενικά όλων όσων ενδιαφέρονται για την εξασφάλιση της πληροφοριών τους.
- Διασφαλίζει την τήρηση των σχετικών νόμων και κανονισμών που πρέπει να τηρούνται σχετικά με την ασφάλεια των πληροφοριών.
- Συνήθως αποφέρει μείωση κόστους λόγω αποφυγής των συνεπειών από τους κινδύνους παραβιάσεων και καταστροφών πληροφοριών.

Π.5 Η ανατομία μιας SIP κλήσης

Ας δούμε τώρα την τεχνολογία του SIP. Το SIP συνήθως μεταφέρεται με UDP πακέτα και η TCP υποστήριξη παρέχεται από κάποια εργαλεία. Ένα SIP μήνυμα περιλαμβάνει δύο κομμάτια:

- Ένα φάκελο που περιγράφει το αίτημα ή το αποτέλεσμα του αιτήματος (απάντηση) σε μία φόρμα από πεδία header (επικεφαλίδας).
- Ένα προαιρετικό περιεχόμενο που περιέχει δεδομένα σχετικά με το αίτημα.

Ως παράδειγμα ας αναλύσουμε μία τυπική SIP κλήση. Σε αυτό το σενάριο, ο χρήστης Α θέλει να καλέσει τον χρήστη Β. Το παρακάτω σχήμα Π.5.α δείχνει την κλήση:



Σχήμα Π.5.α: Βήματα SIP κλήσης

Τι άλλο μπορεί να κάνει το SIP; Υπάρχουν πολλές άλλες εφαρμογές που μπορούν να υλοποιηθούν με το SIP και τις επεκτάσεις του:

- VoIP
- Βιντεοκλήσεις
- Instant messaging για κείμενο και δεδομένα
- Εγγραφή
- Παρουσία (είναι ο φίλος μου διαθέσιμος;)
- Click-και-μίλα (πατήστε εδώ για να μιλήσετε με έναν από τους τεχνικούς μας)
- Αλληλεπιδραστικό τηλεφωνικό σύστημα (IVR)
- Δικτυακά παιχνίδια (π.χ. Quake)
- Εφαρμογές για κινητά τηλέφωνα

Βασικά, οτιδήποτε χρειάζεται δυο τερματικά σημεία να επικοινωνήσουν, το SIP μπορεί να το κάνει.

Π.6 Λογισμικό, υλικό, υπηρεσίες και εφαρμογές Δορυφορικού Δικτύου

Λογισμικό και υλικό δικτύου. Όσον αφορά την υλοποίηση, το τερματικό χρήστη αποτελείται από το υλικό και το λογισμικό του δικτύου και το λογισμικό εφαρμογών. Το λογισμικό και το υλικό του δικτύου παρέχουν λειτουργίες και μηχανισμούς, για να στείλουν πληροφορίες στη σωστή μορφή, χρησιμοποιώντας σωστά πρωτόκολλα σε ένα κατάλληλο σημείο πρόσβασης του δικτύου (access point). Μπορούν επίσης να λαμβάνουν πληροφορίες από το σημείο πρόσβασης με τον ίδιο τρόπο.

Το υλικό του δικτύου παρέχει μετάδοση του σήματος κάνοντας αποτελεσματική και αποδοτική χρήση των πόρων του εύρους ζώνης και των τεχνολογιών μετάδοσης. Φυσικά, μια ραδιοζεύξη χρησιμοποιείται για να διευκολύνει την κινητικότητα των τερματικών των χρηστών που σχετίζονται με τις συνδέσεις πρόσβασης (access links), ενώ υψηλής χωρητικότητας οπτικές ίνες χρησιμοποιούνται για τις συνδέσεις κορμού (backbone). Λόγω του περιβάλλοντος διάδοσης χρησιμοποιούνται ραδιοζεύξεις στο δορυφορικό σύστημα μεταξύ της Γης και δορυφορικών τμημάτων. Γίνεται επίσης έρευνα για τη σύνδεση μεταξύ δορυφόρων με τη χρήση οπτικών επικοινωνιών.

Με την πρόοδο της ψηφιακής επεξεργασίας σήματος (DSP), οι παραδοσιακές υλοποιήσεις του υλικού αντικαθίστανται όλο και περισσότερο από το λογισμικό, για να αυξηθεί η ευελιξία της αναδιαμόρφωσης (reconfiguration) και ως εκ τούτου, να επέλθει μείωση του κόστους. Κατά συνέπεια, η αναλογία της υλοποίησης σε λογισμικό γίνεται όλο και περισσότερη και όλο και λιγότερο στο υλικό. Πολλές υλοποιήσεις υλικού πρώτα υλοποιούνται και προσομοιώνονται σε λογισμικό, αν και το υλικό είναι το θεμέλιο της κάθε υλοποίησης συστήματος. Για παράδειγμα, τα παραδοσιακά τηλεφωνικά δίκτυα είναι κυρίως σε υλικό (hardware), ενώ τα σύγχρονα τηλεφωνικά δίκτυα, τα δίκτυα υπολογιστών, των έξυπνων τηλεφώνων και τα δίκτυα δεδομένων και το Διαδίκτυο είναι κυρίως στον τομέα του λογισμικού (software).

Υπηρεσίες Δικτύου (services). Οι UES και GES παρέχουν υπηρεσίες δικτύου. Σε παραδοσιακά δίκτυα, οι υπηρεσίες αυτές κατατάσσονται σε δύο κατηγορίες: τηλε-υπηρεσιών (teleservices) και υπηρεσιών κομιστή (bearer services). Οι τηλε-υπηρεσίες είναι υψηλού επιπέδου υπηρεσίες που μπορούν να χρησιμοποιηθούν άμεσα από τους χρήστες, όπως τηλέφωνο, φαξ, βίντεο, δεδομένων, e-mail και υπηρεσίες web. Οι υπηρεσίες κομιστή είναι χαμηλότερου επιπέδου υπηρεσίες που παρέχονται από τα δίκτυα για να υποστηρίξουν τις τηλε-υπηρεσίες.

Εφαρμογές (applications). Οι εφαρμογές είναι συνδυασμοί από μία ή περισσότερες υπηρεσίες δικτύου. Για παράδειγμα, η τηλε-εκπαίδευση και οι εφαρμογές τηλεϊατρικής βασίζονται σε συνδυασμούς υπηρεσιών φωνής, βίντεο και δεδομένων. Οι συνδυασμοί των στοιχειών φωνής, βίντεο και δεδομένων ονομάζονται επίσης και υπηρεσίες πολυμέσων (multimedia services). Ορισμένες εφαρμογές μπορεί να χρησιμοποιηθούν με τις υπηρεσίες δικτύου για τη δημιουργία νέων εφαρμογών.

Ορολογία και Ακρωνύμια

Access method	Μέθοδος προσπέλασης
Access Point, AP	Ασύρματο Σημείο Πρόσβασης
Accounting	Κόστος/κοστολόγηση
Accounting Management ή Billing Management	Διαχείριση κόστους
Acknowledged connectionless service	Υπηρεσία με επιβεβαίωση λήψης χωρίς σύνδεση
Acknowledgment	(Αριθμός) Επιβεβαίωση(ς)
Address Resolution Protocol, ARP	Πρωτόκολλο Ανάλυσης διευθύνσεων
Ad-Hoc Wireless Networks	Ασύρματο δίκτυο αυτοοργανωμένο ή κατ' απαίτηση
Advanced Encryption Algorithm, AES	Αλγόριθμος συμμετρικής κρυπτογράφησης
Agent	Αντιπρόσωπος
Alarm	Συναγερμός
Anycast	Μη αποκλειστική διανομή
Application layer	Επίπεδο Εφαρμογής
ARP Reply	Απάντηση ARP
ARP request	Ερώτημα ARP
Asset	Πόρος/Αγαθό
Association Process	Διαδικασία συσχετισμού
Asynchronous Transfer Mode, ATM	Ασύγχρονος Τρόπος Μεταφοράς (δεδομένων)
Attack	Επίθεση
Attenuation/insertion loss	Εξασθένηση
Audio/Video On Demand	Εικόνα/Ηχος κατά παραγγελία
Authentication	Αυθεντικοποίηση/πιστοποίηση ταυτότητας
Automatic configuration	Αυτόματη ρύθμιση
Auto-Negotiation	Αυτόματη διαπραγμάτευση
Autonomous Systems, AS	Αυτόνομα συστήματα
Backbone	Δίκτυο κορμού
Bandwidth	Εύρος ζώνης
Base station	Σταθμός βάσης
Baseband	Βασική Ζώνη
Basic Rate Access, BRA	Πρόσβαση βασικού ρυθμού
Bits per second, Bps	Ψηφία ανά δευτερόλεπτο
Bitwise	Ψηφίο προς ψηφίο
Bridging	Γεφύρωση
Broadband/Wide band	Ευρεία ζώνη
Broadcast	Εκπομπή
Broadcast domain	Πεδίο εκπομπής
Buffers	Ενταμιευτές
Bus	Κανάλι, αρτηρία, διάδρομος
Carrier Sense Multiple Access with Collision Detection, CSMA/CD	Πολλαπλή Προσπέλαση με Ακρόαση Φέροντος και Ανίχνευση Συγκρούσεων
Cell	Κυψέλη ή κυψελίδα
Certificates Authorities, CA	Αρχές πιστοποίησης

Channel Service Unit/Data Service Unit, CSU/DSU	Μονάδα εξυπηρέτησης καναλιού/δεδομένων
Chat	Συνομιλία πραγματικού χρόνου στο Διαδίκτυο με την μορφή κειμένου
Checksum	Άθροισμα Ελέγχου
Chiphertext	Κρυπτογράφημα
Client	Πελάτης
Client-server	(Μοντέλο) πελάτη-εξυπηρετητή
Collision	Σύγκρουση
Collision avoidance	Αποφυγή σύγκρουσης
Collision detection	Ανίχνευση σύγκρουσης
Collision domain	(Ενιαίο) πεδίο συγκρούσεων
Combiners	Μεικτές
Common Management Information Protocol, CMIP	Πρωτόκολλο Κοινής Διαχείρισης Δικτύου
Common Management Information Services, CMIS	Υπηρεσίες Κοινής Διαχείρισης Δικτύου
Confidentiality	Εμπιστευτικότητα
Configuration	Παραμετροποίηση
Configuration management, CM	Διαχείριση παραμετροποίησης
Connection oriented	Προσανατολισμένο σε σύνδεση
Connection oriented service	Υπηρεσία με σύνδεση
Connectionless	Υπηρεσία χωρίς σύνδεση, ασυνδεσμικός
Connector	Συνδετήρας
Constant Bit Rate, CBR	Σταθερός ρυθμός δυαδικών ψηφίων
Cracker	Κράκερ, άτομο το οποίο προσπαθεί, χωρίς εξουσιοδότηση, να αποκτήσει πρόσβαση σε (υπολογιστικά) συστήματα ή δίκτυα.
Cross talk	Παραδιαφωνία
Crossover cable	Ακροδέκτες εκπομπής της μιας μεριάς οδηγούνται στους ακροδέκτες λήψης της άλλης
Cryptography	Κρυπτογραφία
Data frame	Πλαίσιο δεδομένων
Data Link layer	Επίπεδο Ζεύξης ή Σύνδεσης Δεδομένων
Datagram	Πακέτο πρωτοκόλου IP
Datasheet	Φύλλο δεδομένων (ή χαρακτηριστικών)
Delay	Καθυστέρηση
Desktop Conferencing	Διάσκεψη από γραφείο σε γραφείο
Destination	Προορισμός
Dictionary Attack	Επιθέσεις με Λεξικό
Differentiated Services Code Point, DSCP	Σύνολο διαφοροποιημένων υπηρεσιών
Digital Subscriber Line Access Multiplexer, DSLAM	Πολυπλέκτης/αποπολυπλέκτης των ψηφιακών συνδρομητικών γραμμών DSL
Digital Subscriber Line, DSL	Ψηφιακή Συνδρομητική Γραμμή
Distance Vector Algorithm	Αλγόριθμος Διανύσματος Απόστασης
Domain	Περιοχή
Domain Name System - DNS	Υπηρεσία Ονομάτων Περιοχών
Don't Fragment, DF	Σημαία απαγόρευσης διάσπασης
Downstream	Μετάδοση των δεδομένων προς τα κάτω

Drivers	Οδηγοί συσκευών
Dynamic configuration	Δυναμική ρύθμιση/παραμετροποίηση
Discrete MultiTone, DMT	Διαμόρφωση Διακριτής Πολυτονίας
Dynamic Host Configuration Protocol, DHCP	Πρωτόκολλο Δυναμικής απόδοσης ρυθμίσεων Υπολογιστών/δεκτών
Earth stations	Επίγειοι σταθμοί
Echo Cancellation	Καταστολή ηχούς
ElectroMagnetic Compatibility – EMC	Ηλεκτρομαγνητική συμβατότητα
Electronic Data Interchange. EDI	Ηλεκτρονική Ανταλλαγή Δεδομένων
Encapsulation	Ενθυλάκωση
European Computer Manufacturing Association, ECMA	Ευρωπαϊκή Ένωση Κατασκευαστών Υπολογιστών
Extented Unique Identifier	Εκτεταμένο μοναδικό αναγνωριστικό
Exterior Gateway Protocol, EGP	Εξωτερικό Πρωτόκολλο Πύλης
Fault	Σφάλμα
Fiber/Fiber optic	Οπτική ίνα
File Transfer Protocol, FTP	Πρωτόκολλο μεταφοράς αρχείων
Firewall	Τείχος προστασίας
Flag	Σημαία Ελέγχου
Four-part dotted decimal notation	Δεκαδική σημειογραφία με τελείες
Fragment Offset	Σχετική Θέση Τμήματος
Fragmentation	Κατάτμηση, διάσπαση
Frame	Πλαίσιο
Frame Check Sequence, FCS	Ακολουθία ελέγχου πλαισίου
Frequency Band	Ζώνη Συχνοτήτων
Frequency Division Multiplexing, FDM	Πολυπλεξία διαίρεσης συχνότητας
FTP	Πρωτόκολλο μεταφοράς αρχείων
Full duplex	Πλήρως αμφίδρομη (επικοινωνία)
Gateway Earth Station, GES	Επίγειος σταθμός πύλης
Hacker	Χάκερ, εξωτερικός εισβολέας, άτομο με βαθύτερη γνώση της εσωτερικής λειτουργίας συστημάτων, υπολογιστών και δικτύων.
Hacking	Παράνομη πρόσβαση, ύφος προγραμματισμού
Hacktivist	Άτομο που χρησιμοποιεί ανατρεπτικά υπολογιστές και δικτύα για την προώθηση κυρίως ιδεολογιών.
Half duplex	Ημιαμφίδρομη
Hash Function	Συνάρτηση Κερματισμού
Header	Επικεφαλίδα
Header Checksum	Άθροισμα Ελέγχου της Επικεφαλίδας
Home Page	Αρχική σελίδα
Hop	Άλμα (μεταξύ δρομολογητών)
Host	Υπολογιστής/δέκτης
Host ID - suffix	Αναγνωριστικό υπολογιστή στο δίκτυο
Hub	Διανομέας
Hypermedia	Υπερμέσα
Hypertext	Υπερκείμενο
Hypertext Markup Language, HTML	Γλώσσα Σήμανσης Υπερκειμένου
HyperText Transfer Protocol, HTTP	Πρωτόκολλο μεταφοράς Υπερκειμένου

Identification	Αναγνώριση
In-door unit, IDU	Εσωτερική μονάδα
Infrastructure	Υποδομή
Infrastructure Wireless Networks	Ασύρματα δίκτυα υποδομής
Institute of Electrical and Electronic Engineers, IEEE	Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών
Integrated Services Digital Network, ISDN	Ψηφιακό Δίκτυο Ολοκληρωμένων Υπηρεσιών
Integrity	Ακεραιότητα
Interface	Διεπαφή, διασύνδεση
Interference	Παρεμβολή
Interior Gateway Protocols, IGP	Εσωτερικά Πρωτόκολλα Πύλης
International Organization for Standardization, ISO	Διεθνής Οργανισμός Τυποποίησης
Internet	Διαδίκτυο
Internet Control Message Protocol, ICMP	Πρωτόκολλο μηνυμάτων ελέγχου διαδικτύου
Internet Engineering Task Force, IETF	Τακτική Δύναμη Μηχανικών Διαδικτύου
Internet Group Management Protocol, IGMP	Πρωτόκολλο διαχείρισης ομάδων διαδικτύου
Internet Header Length, IHL	Μήκος επικεφαλίδας πακέτου IP
Internet Protocol, IP	Πρωτόκολλο Διαδικτύου
Internet Service Provider, ISP	Φορέας παροχής υπηρεσιών Διαδικτύου
Inter-Process Communication - IPC	Επικοινωνία διεργασιών
Intrusion Detection and Prevention System, IDPS	Σύστημα εντοπισμού και πρόληψης εισβολής
Intrusion Detection System, IDS	Σύστημα εντοπισμού εισβολέων
Layers	Στρώματα ή Επίπεδα
Lease	Μίσθωση
Link	Σύνδεση ή ζεύξη
Link budget	Προϋπολογισμός ζεύξης
Link State Algorithm	Αλγόριθμος Κατάστασης Σύνδεσης
Load	Φορτίο (γραμμής)
Local Area Network, LAN	Τοπικό δίκτυο
Local Internet Registry, LIR	Τοπικοί καταχωρητές Διαδικτύου
Log	Ημερολόγιο καταγραφής
Logical Link Control	Επίπεδο ή υποεπίπεδο Λογικού Ελέγχου της Ζεύξης
Logical Link Control, LLC	Υποεπίπεδο Ελέγχου Λογικής Σύνδεσης
Log-in	Διαδικασία εισόδου
Login name	Όνομα χρήστη
Loopback	Επανατροφοδότηση, Ανατροφοδότηση
MAC Address	Διεύθυνση υλικού ή φυσική διεύθυνση
Mail Server	Διακομιστής ηλεκτρονικού ταχυδρομείου
Management Information Base, MIB	Βάση Πληροφοριών Διαχείρισης
Manager Server	Διαχειριστής Δικτύου
Manual configuration	Μη αυτόματη (χειροκίνητη) ρύθμιση
Margin	Περιθώριο

Maximum Transmission Unit, MTU	Μέγιστο μήκος δεδομένων του πλαισίου (μονάδας εκπομπής)
Media Access Control, MAC	Επίπεδο ή υποεπίπεδο Ελέγχου Πρόσβασης στο Μέσο
Medium Dependent Interface, MDI	Διεπαφή εξαρτώμενη από το μέσο
Mesh	Πλέγμα
Message Digest	Σύνοψη Μηνύματος
Metric	Μετρικό/ τιμή μέτρησης
Metropolitan Area Network, MAN	Μητροπολιτικό δίκτυο
Mini layer	Υποεπίπεδο
More Fragments, MF	Σημαία ύπαρξης περισσότερων τμημάτων
Multi level duobinary AM/FSK	Πολυεπίπεδη διπλοδυαδική διαμόρφωση κατά πλάτος και συχνότητα
Multicast domain	Πεδίο πολυδιανομής
Multiplexing	Πολυπλεξία
Multipoint-to-multipoint, MP2MP	Σημεία προς σημεία
Multistation Access Unit, MSAU	Μονάδες Πρόσβασης Πολλαπλών Σταθμών
Name resolution	Ανάλυση ονόματος
Name resolve	Ανάλυση ονόματος
Narrowband	Στενής ζώνης
National Internet Registry, NIR	Εθνικοί καταχωρητές Διαδικτύου
Net ID – prefix	Αναγνωριστικό δικτύου
Network Access layer/Link layer	Επίπεδο Πρόσβασης (Διεπαφής) Δικτύου
Network Address Translation, NAT	Μετάφραση διευθύνσεων δικτύου
Network Attached Storage, NAS	Δικτυακό μέσο αποθήκευσης
Network Control Protocol, NCP	Πρωτόκολλο Ελέγχου Δικτύου
Network File Systems, NFS	Δικτυακά συστήματα αρχείων
Network Interface Controller, NIC	Προσαρμογέας/ελεγκτής/κάρτα δικτύου
Network layer	Επίπεδο Δικτύου
Network loop	Βρόγχος δικτύου
Network Management System, NMS	Σύστημα Διαχείρισης Δικτύου
Network Nodes Interface, NNI	Διεπαφή κόμβων του δικτύου
Network, Computer	Δίκτυο υπολογιστών
NMS Platforms	Πλατφόρμες συλλογής και ελέγχου δικτυακών δεδομένων
Node	Κόμβος
Non repudiation	Μη άρνηση ταυτότητας
Non-switched networks	Δίκτυα χωρίς μεταγωγή
Object Identifier, OID	Ταυτοποίηση Αντικειμένου
Octets/ bytes	Οκτάδες
Open Shortest Path First, OSPF	Πρωτόκολλο Βραχύτερου Μονοπατιού
Open Systems Interconnection, OSI	Διασύνδεση Ανοικτών Συστημάτων
Optical Network Termination, ONT	Συσκευή τερματισμού του οπτικού δικτύου
Optical Network Unit, ONU	Μονάδα οπτικού δικτύου
OUI – Organizational Unique Identifier	Μοναδική Ταυτότητα Οργανισμού
outdoor-unit, ODU	Εξωτερική μονάδα
Padding	Συμπλήρωμα
Password	Συνθηματικό

Payload	Ωφέλιμα δεδομένα χρήστη, ωφέλιμο φορτίο
Performance	Επίδοση
Performance Management ή Capacity Management	Διαχείριση Επιδόσεων ή Διαχείριση Χωρητικότητας
Permanent Virtual Circuit, PVC	Μόνιμο νοητό κανάλι
Phase coherent FSK	Διαμόρφωση συχνότητας σύμφωνης φάσης
Phase continuous FSK	Διαμόρφωση συχνότητας συνεχούς φάσης
Phishing	Παραπλανητική αλληλογραφία
Physical layer	Φυσικό Επίπεδο
Point to multipoint, P2MP	Σημείο προς σημεία
Point to Point Protocol, PPP	Πρωτόκολλο Σύνδεσης Σημείου προς Σημείο
Point to point, P2P	Σημείο προς σημείο
Port	Θύρα
Port scan	Σάρωση θυρών επικοινωνίας
Post Office Protocol 3, POP3	Πρωτόκολλο ταχυδρομικού γραφείου
Preamble	Προοίμιο
Presentation layer	Επίπεδο Παρουσίασης
Primary Rate Access – PRA	Πρόσβαση πρωτεύοντος ρυθμού
Protocol Data Unit	Μονάδα πληροφορίας πρωτοκόλλου
Protocol, Network	Πρωτόκολλο επικοινωνίας ή Πρωτόκολλο δικτύου
Public key	Δημόσιο κλειδί
Public Switched Telephone Network, PSTN	Δημόσιο Τηλεφωνικό Δίκτυο Μεταγωγής, Δημόσιο Επιλεγόμενο Τηλεφωνικό Δίκτυο
Purge frame	Πλαίσιο καθαρισμού
Quality of service, QoS	Ποιότητα υπηρεσίας
Query	Ερώτημα
Receiver Sensitivity	Ευαισθησία δέκτη
Reconfiguration	Αναδιαμόρφωση
Reference Model	Μοντέλο αναφοράς
Regional Internet Registry, RIR	Περιφερειακοί καταχωρητές Διαδικτύου
Relaying	Αναμετάδοση
Repeater	Επαναλήπτης
Request For Comments, RFC	Έγγραφα του IETF (Internet Engineering Task Force) που περιγράφουν/προτείνουν μεθόδους και συμπεριφορές
Resolver	Αναλυτής
Return Loss	Απώλειες επιστροφής
Reverse Address Resolution Protocol, RARP	Πρωτόκολλο αντίστροφης ανάλυσης διευθύνσεων
RF Output Power	Ισχύς ραδιοσυχνότητας εξόδου (του πομπού)
Root	Ρίζα
Round Trip Time	Χρόνος πλήρους περιφοράς
Router	Δρομολογητής
Routing	Δρομολόγηση
Routing Information Protocol, RIP	Πρωτόκολλο Πληροφορίας Δρομολόγησης
SAPs – Service Access Points	Σημεία Πρόσβασης για Εξυπηρέτηση
Satellite communication payload system	Σύστημα δορυφορικής επικοινωνίας
Satellite terminal	Δορυφορικό τερματικό
Secret key	Μυστικό κλειδί

Security	Ασφάλεια
Security Management	Διαχείριση ασφάλειας
Security policy	Πολιτική ασφαλείας
Segment	Τμήμα
Sequence Number	Αριθμός Σειράς
Server	Εξυπηρετητής ή Διακομιστής
Server clustering	Συστοιχίες Εξυπηρετητών/διακομιστών
Session Initiation Protocol, SIP	Πρωτόκολλο έναρξης συνόδου
Session layer	Επίπεδο Συνόδου
Shared medium	Διαμοιραζόμενο μέσο
Shut down	Τερματισμός λειτουργίας
Signal to Noise Ratio, S/N ή SNR	Λόγος Σήματος προς Θόρυβο
Simple Mail Transfer Protocol, SMTP	Πρωτόκολλο μεταφοράς απλών μηνυμάτων
Simple Network Management Protocol, SNMP	Πρωτόκολλο Απλής Διαχείρισης Δικτύου
Site	Τοποθεσία
Social Engineering	Κοινωνική Μηχανική
Sockets	Υποδοχές ή πρίζες
Source	Πηγή ή Προέλευση
Spam	Αποστολή ασχέτων ή μη αποδεκτών μηνυμάτων στο Διαδίκτυο σε μεγάλο αριθμό χρηστών
Splitter	Διαχωριστής
Spoofing	Πλαστοπροσωπία ή μεταμφίεση
Star	Αστέρας
Start – frame – sequence	Ακολουθία (ψηφίων) έναρξης πλαισίου
Storage Area Network, SAN	Δικτυακή περιοχή αποθήκευσης
Straight through cable	Αντιστοιχία ακροδεκτών είναι “ένα προς ένα” μεταξύ των δυο άκρων
Streams	Ροές
Subdomain	Υποπεριοχή
Subnet	Υποδίκτυο
Switch	Μεταγωγέας
Switched Virtual Circuit, SVC	Επιλεγόμενο νοητό κανάλι
Switching	Μεταγωγή
Symmetric key	Συμμετρικό κλειδί
Synchronous Transfer Mode, STM	Σύγχρονος Τρόπος Μεταφοράς
TELNET	Απομακρυσμένη σύνδεση τερματικού (πρωτόκολλο)
Terminal Adaptor, TA	Τερματικός προσαρμογέας
Terrestrial network	Επίγειο δίκτυο
Threat	Απειλή
Throughput	Διακίνηση
Time To Live, TTL	(Πεδίο) Χρόνος Ζωής
Token	Κουπόνι
Token Bus	Αρτηρία με Κουπόνι
Token passing	Πέρασμα κουπονιού
Token Ring	Δακτύλιος με Κουπόνι
Topology, Network	Τοπολογία δικτύου
Trailer	Ουρά

Transceiver	Πομποδέκτης
Transmission Control Protocol, TCP	Πρωτόκολλο ελέγχου μετάδοσης
Transport Layer	Επίπεδο Μεταφοράς
Transport Layer Security, TLS	Ασφάλεια του επίπεδου μεταφοράς
Trap	Παγίδα
Trivial File Transfer Protocol, TFTP	Απλό πρωτόκολλο μεταφοράς αρχείων
Unacknowledged connectionless service	Υπηρεσία χωρίς επιβεβαίωση και χωρίς σύνδεση
Unicast	Αποκλειστική διανομή
Unmanned artificial satellite	Μη επανδρωμένος τεχνητός δορυφόρος
Upgrade	Αναβάθμιση
Uplink	Επίγειος σταθμός
Upstream	Μετάδοση δεδομένων προς τα πάνω
User Datagram Protocol, UDP	Πρωτόκολλο αυτοδύναμων πακέτων χρήστη
User Earth Station, UES	Επίγειος σταθμός χρήστη
User Network Interface, UNI	Διεπαφή χρήστη δικτύου
User terminal	Τερματικό χρήστη
Validity	Εγκυρότητα
Vandal	Βάνδαλος
Variable Bit Rate, VBR	Μεταβλητός ρυθμός δυαδικών ψηφίων
Variable Length Subnet Masking, VLSM	Μεταβλητό μήκος μασκών υποδικτύωσης
Version	Έκδοση
Video Conferencing	Τηλεδιάσκεψη
Videophone	Εικονοτηλέφωνο
Virtual LAN, VLAN	Εικονικό ή νοητό τοπικό δίκτυο
Voice over Internet Protocol, VoIP	Τηλεφωνική επικοινωνία μέσω δικτύων δεδομένων
Vulnerability	Αδυναμία
Wavelength Division Multiplexing, WDM	Πολυπλεξία μήκους κύματος
Web browser	Φυλλομετρητής/πλοηγός
Web server	Διακομιστής/εξυπηρετητής του παγκόσμιου ιστού
Web Site	Ιστότοπος
Wide Area Networks, WAN	Δίκτυα ευρείας περιοχής
Wireless Local Area Network, WLAN	Ασύρματο τοπικό δίκτυο
Workstation	Τερματικό ή προσωπικός υπολογιστής ή σταθμός εργασίας
World Wide Web, WEB	Παγκόσμιος Ιστός
Worm	Σκουλήκι