

Δίκτυα Υπολογιστών II – Το Ανεπίσημο Βοήθημα

Μανώλης Κιαγιάς, MSc

07/12/2010

Κάθε γνήσιο αντίτυπο φέρει την υπογραφή του συγγραφέα:

2η Έκδοση – Χανιά, 07/12/2010

[Web Edition]

Copyright ©2009 – 2010 Μανώλης Κιαγιάς

Το Έργο αυτό διατίθεται υπό τους όρους της Άδειας:



Αναφορά – Μη Εμπορική Χρήση – Παρόμοια Διανομή 3.0 Ελλάδα

Μπορείτε να δείτε το πλήρες κείμενο της άδειας στην τοποθεσία:

<http://creativecommons.org/licenses/by-nc-sa/3.0/gr/>

Είναι Ελεύθερη:

Η Διανομή – Η αναπαραγωγή, διανομή, μετάδοση και παρουσίαση του Έργου σε κοινό

Υπό τις ακόλουθες προϋποθέσεις:

Αναφορά Προέλευσης — Θα πρέπει να αναγνωρίσετε την προέλευση στο έργο σας με τον τρόπο που έχει ορίσει ο δημιουργός



του ή το πρόσωπο που σας χορήγησε την άδεια (χωρίς όμως να αφήσετε να εννοηθεί ότι εγκρίνουν με οποιονδήποτε τρόπο εσάς ή τη χρήση του έργου από εσάς).



Μη Εμπορική Χρήση – Δεν μπορείτε να χρησιμοποιήσετε αυτό το έργο για εμπορικούς σκοπούς.



Παρόμοια Διανομή — Αν αλλοιώσετε, τροποποιήσετε ή δημιουργήσετε κάποιο παράγωγο έργο το οποίο βασίζεται στο παρόν έργο, μπορείτε να διανείμετε το αποτέλεσμα μόνο με την ίδια ή παρόμοια με αυτή άδεια.

Με την κατανόηση ότι:

Αποποίηση – Οποιεσδήποτε από τις παραπάνω συνθήκες μπορούν να παρακαμφθούν αν πάρετε την άδεια του δημιουργού ή κατόχου των πνευματικών δικαιωμάτων.

Άλλα Δικαιώματα – Σε καμιά περίπτωση τα ακόλουθα δικαιώματα σας, δεν επηρεάζονται από την Άδεια:

- Η δίκαιη χρήση και αντιμετώπιση του έργου
- Τα ηθικά δικαιώματα του συγγραφέα
- Τα ενδεχόμενα επί του έργου δικαιώματα τρίτων προσώπων, σχετικά με τη χρήση του έργου, όπως για παράδειγμα η δημοσιότητα ή ιδιωτικότητα.

Σημείωση – Για κάθε επαναχρησιμοποίηση ή διανομή, πρέπει να καταστήσετε σαφείς στους άλλους τους όρους της άδειας αυτού του Έργου. Ο καλύτερος τρόπος να το πράξετε αυτό, είναι να δημιουργήσετε ένα σύνδεσμο με το διαδικτυακό τόπο της παρούσας άδειας:

<http://creativecommons.org/licenses/by-nc-sa/3.0/gr/>

Το βιβλίο αυτό στοιχειοθετήθηκε σε X_ET_EX. Ο πηγαίος κώδικας του είναι διαθέσιμος στις δικτυακές τοποθεσίες που αναφέρονται παρακάτω και μέσω mercurial repository.

Επισκεφθείτε το δικτυακό τόπο του μαθήματος και κατεβάστε την τελευταία έκδοση του βιβλίου και διορθώσεις:

<http://diktia.chania-lug.gr>

Σε περίπτωση προβλήματος χρησιμοποιήστε το mirror site:

<http://www.freebsdworld.gr/diktia/theBookII.pdf>

Το βιβλίο αυτό αφιερώνεται σε όσους κάνουν αυτό που πιστεύουν και όχι αυτό που νομίζουν οι άλλοι σωστό...



“Ο μόνος αληθινός νόμος είναι εκείνος που οδηγεί στην ελευθερία”,
είπε ο Ιωνάθαν. “Δεν υπάρχει άλλος.”

“Ο Γλάρος Ιωνάθαν Λίβινγκστον”, Richard Bach

(Κενή Σελίδα)

Εισαγωγή στο Νέο Βοήθημα

Καλώς ήλθατε στην πρώτη έκδοση του νέου “ανεπίσημου” βοηθήματος για το μάθημα “Δίκτυα Υπολογιστών II” το οποίο διδάσκεται ως Πανελλαδικά εξεταζόμενο στην Γ’ Τάξη των Επαγγελματικών Λυκείων. Το βιβλίο αυτό καλύπτει την εξεταζόμενη ύλη όπως ανακοινώθηκε από το Υπουργείο Παιδείας για το σχολικό έτος 2010-2011. Το νέο ανεπίσημο βοήθημα, με απλοποιημένη αλλά άρτια τεχνικά γλώσσα, ευελπιστεί να καλύψει τις ατέλειες του σχολικού εγχειριδίου και να βοηθήσει τους αποφασισμένους μαθητές να πετύχουν στις εξετάσεις. Η επιτυχία του αρχικού βοηθήματος, με τέσσερις συνολικά εκδόσεις, μας οδηγεί να πιστεύουμε ότι ο στόχος αυτός είναι εφικτός.

Η έκδοση αυτή κυκλοφορεί ως “ελεύθερη” με βάση την άδεια Creative Commons που μπορείτε να διαβάσετε στις πρώτες σελίδες του βιβλίου.

Πρόλογος της Πρώτης Έκδοσης (2004)

Προλογίζει ο Αντώνης Αθανασάκης, καθηγητής στον Τομέα Οικονομίας, συνάδελφος του συγγραφέα στο ΤΕΕ Κισάμου.

Κάθε απόπειρα αγωγής καταλήγει σε σχέση μεταξύ προσώπων. Η διδασκαλία, δεν είναι ενέργεια κατά την οποία επικοινωνούν μόνο οι εγκέφαλοι, αλλά πορεία προσωπικής επικοινωνίας και αμοιβαίας προσπάθειας.

Το εγώ που δεν έχει απέναντί του κανένα συγκεκριμένο εσύ, αλλά είναι περιστοιχισμένο από μια πληθώρα “περιεχομένων”, δεν είναι διόλου παρόν και η στιγμή του είναι στερημένη από παρουσία. Μια παρουσία όμως δεν είναι κάτι που ζεφεύγει και γλιστράει αλλά είναι εκείνο που κατοικεί απέναντί μας και περιμένει την συνάντηση.

Αν η πραγματική συνάντηση είναι η πορεία, κατά την οποία ένας άνθρωπος αγγίζει έναν άλλον άνθρωπο στον πυρήνα του, τότε οι μαθητές του Μανώλη είχαν φέτος μια τρομερή ευκατρία.

Το μόνο που χρειάζονται είναι την ικανότητα για ανταπόκριση. Γιατί η ελευθερία μέσα στην αγωγή, είναι το να μπεις σε δεσμό. Το αντίθετο του εξαναγκασμού, σύμφωνα με τον Buter δεν είναι η ελευθερία, αλλά ο δεσμός. Δεν θα μπορούσαμε χωρίς ελευθερία, αλλά από μόνη της δεν είναι χρησιμοποιήσιμη.

Περιεχόμενα

I Βιβλίο Θεωρίας	1
6 Δίκτυα Ευρείας Περιοχής	3
6.1 Επεκτείνοντας το Δίκτυο	3
6.2 Επιλεγόμενες Τηλεφωνικές Γραμμές	4
6.5 ISDN	6
6.8 xDSL	11
7 Διαδικτύωση – Internet	17
7.1 Επίπεδο Δικτύου	17
7.1.1 Γενικές Αρχές	17
7.2 Τεχνολογία TCP/IP	22
7.2.1 Εισαγωγή στην Τεχνολογία TCP/IP	22
7.2.2 Σχέση OSI και TCP/IP	25
7.2.2.1 Επίπεδο Πρόσβασης Δικτύου	27
7.2.2.2 Επίπεδο Δικτύου	28
7.2.2.3 Επίπεδο Μεταφοράς	29
7.2.2.4 Επίπεδο Εφαρμογής	30
7.2.3 Βασικές Αρχές Επικοινωνίας στην Τεχνολογία TCP/IP και στο Διαδίκτυο	31
7.3 Πρωτόκολλο TCP	36
7.3.1 TCP Συνδέσεις	42
7.4 Πρωτόκολλο UDP	45
7.5 Πρωτόκολλο IP	48
7.6 Διευθυνσιοδότηση	55
7.6.1 Διεύθυνση Ελέγχου Πρόσβασης στο Μέσο (Media Access Control, Διεύθυνση MAC)	56
7.6.2 IP Διευθύνσεις	57
7.6.3 Υποδίκτυα και Μάσκα Υποδικτύου	62
7.6.3.1 Μάσκα Υποδικτύου	64
7.7 Πρωτόκολλο ARP	67

7.8 Σύστημα Ονομάτων Περιοχών, Domain Name System (DNS)	72
7.8.1 Χώρος Ονομάτων του DNS	78
7.9 Δρομολόγηση	81
7.9.1 Δρομολόγηση σε Δίκτυα TCP/IP	85
7.9.2 Άμεση Δρομολόγηση	89
7.9.3 Εμμεση Δρομολόγηση	90
7.9.4 Πίνακας Δρομολόγησης	92
7.11 Πρωτόκολλα Εφαρμογής	96
7.11.1 Γενικές Αρχές	96
7.11.2 Βασικές και Προηγμένες Υπηρεσίες Διαδικτύου	98
8 Διαχείριση και Ασφάλεια Δικτύου	117
8.1 Διαχείριση Δικτύου	118
8.1.1 Διαχείριση Παραμέτρων (Configuration Management)	118
8.1.2 Διαχείριση Επίδοσης του Δικτύου (Performance Management)	120
8.1.3 Διαχείριση Σφαλμάτων (Fault Management)	121
8.1.4 Διαχείριση Κόστους (Accounting Management)	123
8.1.5 Διαχείριση Ασφάλειας (Security Management)	123
8.3 Ασφάλεια Δικτύων	123
8.3.1 Ασφάλεια Πληροφοριών	124
8.3.2 Επεξήγηση Ορολογίας	127
8.3.3 Μέθοδοι Παραβίασης	129
8.3.4 Τεχνικές Ασφάλειας	133
8.3.4.1 Ψηφιακές Υπογραφές	138
8.3.5 Τεχνολογίες Ασφάλειας	140
8.3.6 Αποφυγή Καταστροφών	142
II Παραρτήματα	145
AΠ Θέματα Προηγούμενων Ετών	147

Κατάλογος σχημάτων

6.1	Σύνδεση υπολογιστών μέσω δικτύου <i>PSTN</i>	5
6.2	Διεπαφές βασικού και πρωτεύοντος ρυθμού στο <i>ISDN</i>	9
6.3	Ο εξοπλισμός του <i>ISDN</i>	10
6.4	Πρόσβαση τοπικού δικτύου σε δίκτυο ευρείας περιοχής μέσω τεχνολογίας <i>SDSL</i>	13
7.1	Αρχιτεκτονική Μοντέλου <i>OSI</i>	18
7.2	Γενική εικόνα δικτύου υπολογιστών	19
7.3	Λειτουργία Νοητών Κυκλωμάτων	21
7.4	Μοντέλα <i>OSI</i> και <i>TCP/IP</i>	26
7.5	Στοίβα Πρωτοκόλλων <i>TCP/IP</i>	26
7.6	Πρότυπο Πελάτη – Εξυπηρετητή	31
7.7	Επικοινωνία Επιπέδων <i>TCP/IP</i>	32
7.8	Επικοινωνία Εξυπηρετητών <i>SMTP</i>	33
7.9	Επικοινωνία στο Διαδίκτυο	35
7.10	Επικοινωνία στο Επίπεδο Δικτύου	37
7.11	Διάσπαση δεδομένων σε <i>TCP</i> τμήματα	38
7.12	Επικεφαλίδα (<i>Header</i>) <i>TCP</i>	38
7.13	Λειτουργία Θυρών <i>TCP</i>	41
7.14	<i>TCP</i> Σύνδεση	42
7.15	<i>TCP</i> Συνδέσεις	44
7.16	Πλήρης Δομή <i>UDP</i>	47
7.17	Δημιουργία <i>UDP</i> Τμήματος	47
7.18	<i>IP</i> Αυτοδύναμο Πακέτο	48
7.19	Διάσπαση σε <i>Fragments</i>	50
7.20	Διάσπαση σε <i>Fragments</i> και άφιξη στον προορισμό	54
7.21	Δομή Φυσικής Διεύθυνσης	57
7.22	Ιεραρχική διαίρεση δικτύου σε υποδίκτυα και χωρισμός διευθύνσεων σε υποδιευθύνσεις	59
7.23	Δομή Διεύθυνσης <i>IP</i>	59
7.24	Κλάσεις <i>IP</i> Διευθύνσεων	61

7.25	<i>Εσωτερική οργάνωση δικτύου σε υποδίκτυα</i>	63
7.26	<i>Χρήση Μάσκας Υποδικτύου</i>	65
7.27	<i>ARP Αίτηση και Απάντηση</i>	72
7.28	<i>TCP/IP Δίκτυο Τεσσάρων Υπολογιστών</i>	75
7.29	<i>Οργάνωση Δικτύου σε Ζώνες</i>	77
7.30	<i>Βασικές περιοχές χώρου ονομάτων DNS</i>	79
7.31	<i>Ιεραρχική οργάνωση χώρου ονομάτων DNS</i>	80
7.32	<i>TCP/IP Δίκτυο Τριών Υπολογιστών</i>	89
7.33	<i>TCP/IP διαδίκτυο αποτελούμενο από τρία TCP/IP δίκτυα</i>	91
7.34	<i>Διεπαφές των υπολογιστών Α,Β,Γ TCP/IP δικτύου</i>	93
7.35	<i>Διεπαφές των υπολογιστών Α,Δ,Ε,Ι TCP/IP δικτύου με δρομολογητή</i>	94
7.36	<i>Τρεις γνωστοί browsers: Google Chrome, Mozilla Firefox, Apple Safari</i>	107
7.37	<i>To γνωστό πρόγραμμα επικοινωνίας Skype</i>	111
8.1	<i>H διαχείριση δικτύων κατά το μοντέλο OSI</i>	118
8.2	<i>Παράδειγμα προγράμματος διαχείρισης δικτύου</i>	119
8.3	<i>Παρακολούθηση επιδόσεων δικτύου</i>	121
8.4	<i>Παρακολούθηση σφαλμάτων</i>	122
8.5	<i>Επικοινωνία με χρήση συμμετρικής κρυπτογράφησης</i>	134
8.6	<i>Εμπιστευτικότητα δεδομένων με χρήση δημόσιου κλειδιού</i>	136
8.7	<i>Αυθεντικοποίηση αποστολέα με χρήση ασυμμετρικής κρυπτογράφησης</i>	138
8.8	<i>Παράδειγμα δικτύου με χρήση firewall</i>	141

Μέρος Ι

Βιβλίο Θεωρίας

Κεφάλαιο 6

Δίκτυα Ευρείας Περιοχής

Εισαγωγή

Η επικράτηση της χρήσης των μικροϋπολογιστών (προσωπικών υπολογιστών) στις επιχειρήσεις, οδήγησε γρήγορα στη δημιουργία πολλών τοπικών δικτύων, μικρού ή μεγαλύτερου μεγέθους. Ωστόσο, καθώς κάθε επιχείρηση αναπτύσσεται, γρήγορα δημιουργείται η ανάγκη για επικοινωνία και μετάδοση δεδομένων μεταξύ των υποκαταστημάτων της. Η ανάγκη αυτή καλύπτεται σήμερα από τα Δίκτυα Ευρείας Περιοχής (ΔΕΠ). Στο μάθημα της Β' Τάξης, εξετάσαμε ήδη ένα μέρος του εξοπλισμού που χρησιμοποιείται σε αυτά τα δίκτυα. Στο κεφάλαιο αυτό θα αναφερθούμε πλέον στις τεχνολογίες μετάδοσης που χρησιμοποιούνται στα ΔΕΠ, εξετάζοντας τόσο τις κλασικές (επιλεγόμενο τηλεφωνικό δίκτυο) όσο και τις πιο σύγχρονες (xDSL).

6.1 Επεκτείνοντας το Δίκτυο

Τα τοπικά δίκτυα αποτελούν μια πολύ καλή λύση επικοινωνίας σε περύπτωση που το μέγεθος του δικτύου είναι σχετικά μικρό και καταλαμβάνει περιορισμένη γεωγραφικά έκταση. Για παράδειγμα μια εταιρία που διαθέτει μόνο ένα πολυόροφο κτίριο σε μια πόλη, εξυπηρετείται αποτελεσματικά από ένα τοπικό δίκτυο. Όταν όμως η δραστηριότητα της επεκταθεί σε γειτονικές πόλεις, η ανάγκη επικοινωνίας μεταξύ των υποκαταστημάτων της, απαιτεί τη χρήση ενός ΔΕΠ. Τα ΔΕΠ είναι γνωστά και με τον Αγγλικό όρο *Wide Area Networks* (WAN).

Χρησιμοποιώντας ένα ΔΕΠ, είναι δυνατόν να διασυνδέσουμε μεταξύ τους τα τοπικά δίκτυα κάθε υποκαταστήματος. Για το σκοπό αυτό χρησιμοποιείται κατάλληλος δικτυακός εξοπλισμός (γραμμές σύνδεσης, modem, δρομολογητές κ.α.). Στις γραμμές

ενός ΔΕΠ μπορεί να χρησιμοποιούνται δίκτυα μεταγωγής (κυκλώματος ή πιο συχνά πακέτου), δορυφορικές και μικροκυματικές συνδέσεις, οπτικές ίνες, ή ακόμα και συστήματα καλωδιακής τηλεόρασης.

Ο χρήστης που χρησιμοποιεί ένα ΔΕΠ δεν πρέπει να καταλαβαίνει καμιά διαφορά ως προς τον τρόπο χρήσης του σε σχέση με ένα τοπικό δίκτυο. Αυτό σημαίνει ότι το ΔΕΠ είναι διάφανο ως προς τη λειτουργία του.

Είναι αρκετά δύσκολο (ειδικά από άποψης κόστους) για μια εταιρεία να εγκαταστήσει και να διαχειρίζεται από μόνη της τις γραμμές ενός ΔΕΠ. Συνήθως είναι ευκολότερο να νοικιάσει τη χρήση τους από κάποιο φορέα που ειδικεύεται στις επικοινωνίες (π.χ. τον OTE) ο οποίος συνήθως έχει ήδη έτοιμη την καλωδιακή υποδομή και μπορεί να καλύψει κάθε σημείο της χώρας. Οι τεχνολογίες που χρησιμοποιούνται στις υπηρεσίες δικτύων ευρείας περιοχής (υπηρεσίες WAN) όπως παρέχονται από τους φορείς τηλεπικοινωνιών μπορεί να είναι:

- Οι κλασικές:
 - Επιλεγόμενες τηλεφωνικές γραμμές (το κλασικό τηλεφωνικό δίκτυο)
 - Μόνιμες ή μισθωμένες γραμμές
 - Γραμμές που χρησιμοποιούν το πρότυπο X.25
- αλλά και οι πιο σύγχρονες:
 - Frame Relay
 - ISDN
 - ATM
 - xDSL

Σημείωση: Από το 2001, υπάρχει στη χώρα μας πλήρη απελευθέρωση των τηλεπικοινωνιών. Έτσι πλέον κάθε εταιρία μπορεί να εγκαθιστά και να διαχειρίζεται εξοπλισμό και γραμμές κατάλληλες για ΔΕΠ. Λόγω του αυξημένου ανταγωνισμού, υπάρχει και αντίστοιχη βελτίωση στην ποιότητα (και το κόστος) των παρεχόμενων τηλεπικοινωνιακών υπηρεσιών.

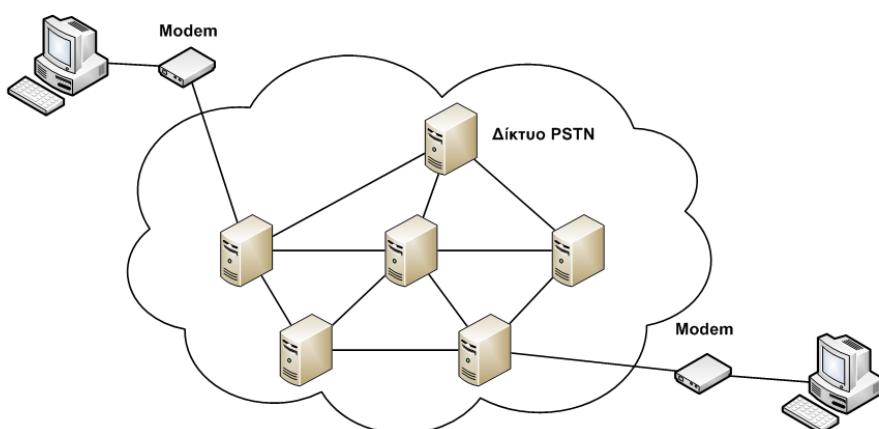
6.2 Επιλεγόμενες Τηλεφωνικές Γραμμές

Το γνωστό μας τηλεφωνικό δίκτυο, το οποίο χρησιμοποιούμε εδώ και πολλά χρόνια για μετάδοση φωνής, μπορεί επίσης να χρησιμοποιηθεί για μετάδοση δεδομένων.

Το τηλεφωνικό δίκτυο είναι γνωστό διεθνώς και με την ονομασία *PSTN*, *Public Switched Telephone Network*, το οποίο θα μπορούσαμε να μεταφράσουμε ως **Δημόσιο Τηλεφωνικό Επιλογικό (ή Μεταγωγής) Δίκτυο**. Η έννοια του “επιλογικού” σχετίζεται με την δυνατότητα που έχουμε να επιλέξουμε με ποιο συνδρομητή θα συνομιλήσουμε, σχηματίζοντας τον κατάλληλο αριθμό κλήσης. Θεωρώντας το ως δίκτυο μεταγωγής, θα λέγαμε ότι ανήκει στην κατηγορία της μεταγωγής κυκλώματος ενώ οι συνδέσεις που δημιουργούμε είναι προσωρινές.

Μέσω του τηλεφωνικού δίκτυου, μπορούμε να έχουμε μετάδοση δεδομένων μεταξύ υπολογιστών, χρησιμοποιώντας τις γραμμές του για να δημιουργήσουμε ένα ΔΕΠ. Υπάρχουν ωστόσο κάποιοι περιορισμοί: Το τηλεφωνικό δίκτυο σχεδιάστηκε για τη μετάδοση φωνής, αναλογικών δηλ. δεδομένων, και μάλιστα με μικρό εύρος συχνοτήτων (όσο χρειάζεται για να μεταδίδεται και να αναγνωρίζεται η ανθρώπινη φωνή) ενώ οι υπολογιστές μεταδίδουν γενικά ψηφιακά σήματα. Για να ξεπεράσουμε αυτό τον περιορισμό, χρησιμοποιούμε ειδικές συσκευές για την σύνδεση των υπολογιστών με το τηλεφωνικό δίκτυο, τα γνωστά μας *modem*.

Τα modems, για τα οποία έχουμε αναφερθεί και στο μάθημα της Β' τάξης, είναι συσκευές οι οποίες μετατρέπουν το ψηφιακό σήμα των υπολογιστών σε αναλογικό το οποίο μπορεί να μεταδοθεί μέσω της τηλεφωνικής γραμμής. Το modem που βρίσκεται στην άλλη μεριά της σύνδεσης αναλαμβάνει την ακριβώς αντίστροφη διαδικασία. Αν έχετε χρησιμοποιήσει modem για την σύνδεση σας στο Internet θα έχετε πιθανόν ακούσει τον χαρακτηριστικό ήχο που παράγεται από την μετατροπή (διαμόρφωση) του σήματος σε αναλογικό. Ουσιαστικά το modem μετατρέπει το ψηφιακό σήμα σε ήχο που μπορεί να μεταδοθεί μέσω της τηλεφωνικής γραμμής.



Σχήμα 6.1: Σύνδεση υπολογιστών μέσω δικτύου *PSTN*

Πλεονεκτήματα	Μειονεκτήματα	Βασική Χρήση
Υψηλή Διαθεσιμότητα	Μικρή Ταχύτητα	Απομακρυσμένη Πρόσβαση
Μικρό Κόστος	Μεταβλητή Ποιότητα και Αξιοπιστία	Εφαρμογές χωρίς απαιτήσεις υψηλής ταχύτητας

Πίνακας 6.1: Χαρακτηριστικά επιλεγόμενων γραμμών

Ο άλλος περιορισμός των επιλογικών τηλεφωνικών συνδέσεων είναι ο σχετικά μικρός ρυθμός μετάδοσης δεδομένων που μπορεί να επιτευχθεί. Η ταχύτητα δεν είναι σταθερή καθώς εξαρτάται από παράγοντες όπως η ποιότητα της γραμμής και του κυκλώματος που έχει σχηματιστεί μεταξύ των δύο υπολογιστών που επικοινωνούν. Η μέγιστη πρακτική ταχύτητα μετάδοσης που έχει επιτευχθεί σε δίκτυο PSTN είναι σήμερα τα 56Kbps. Πρέπει να σημειώσουμε ότι η τεχνολογία αυτή έχει σταματήσει να αναπτύσσεται, καθώς έχει αντικατασταθεί από πιο σύγχρονες και έτσι δεν αναμένεται να αυξηθεί η ταχύτητα της στο μέλλον.

Σήμερα, οι επιλογικές συνδέσεις χρησιμοποιούνται για μετάδοση δεδομένων περιορισμένης χρονικά διάρκειας, όταν δεν δικαιολογείται το επιπλέον κόστος χρήσης αφιερωμένης γραμμής ή κάποιας άλλης πιο σύγχρονης τεχνολογίας. Γνωστές εφαρμογές της είναι η πρόσβαση στο Internet ή σε άλλες on-line υπηρεσίες χαμηλής ταχύτητας, η σύνδεση κάποιου απομακρυσμένου υπολογιστή (π.χ. ενός φορητού) με το τοπικό δίκτυο μιας εταιρίας, καθώς και η τήλε-εργασία. Ακόμα, οι επιλογικές συνδέσεις χρησιμοποιούνται συχνά ως εφεδρικές σε περίπτωση βλάβης μιας μόνιμης γραμμής.

6.5 ISDN

Εκτός από τις κλασικές υπηρεσίες τηλεφωνίας (φωνής), τα τελευταία χρόνια παρουσιάστηκε μεγάλη ζήτηση για παροχή και άλλων υπηρεσιών (μετάδοση δεδομένων, εικόνας, video). Οι διάφοροι φορείς τηλεπικοινωνιών αναγκάστηκαν να δημιουργήσουν εξειδικευμένα δίκτυα (εκτός από το τηλεφωνικό που υπήρχε) για την μετάδοση των αντίστοιχων δεδομένων. Για παράδειγμα, ο ΟΤΕ ανέπτυξε τα δίκτυα Hellaspac και Hellascom για μετάδοση δεδομένων υπολογιστών. Ακόμα δημιουργήθηκαν δίκτυα για μετάδοση δεδομένων κειμένου telex (το οποίο όμως έχει πλέον καταργηθεί), δίκτυα καλωδιακής τηλεόρασης κ.α. Η ανάπτυξη ξεχωριστών δικτύων για κάθε διαφορετικό είδος υπηρεσίας, έχει μειονεκτήματα όπως:

- Μεγάλο κόστος διαχείρισης και συντήρησης των διαφορετικών τεχνολογιών από κάθε τηλεπικοινωνιακό φορέα.

- Αυξημένο κόστος για τον τελικό χρήστη, ο οποίος πρέπει να συντηρεί διαφορετικό εξοπλισμό για κάθε υπηρεσία, και να πληρώνει συνδρομή στον τηλεπικοινωνιακό φορέα. Με δεδομένο ότι ο φορέας έχει πολλά έξοδα για τα δίκτυα αυτά, οι τιμές των συνδρομών είναι αντίστοιχα αρκετά αυξημένες.
- Τα παραπάνω οδηγούν συνήθως σε αποθάρρυνση της εμπορικής ανάπτυξης.

Τα παραπάνω προβλήματα έρχεται να λύσει το *Ψηφιακό Δίκτυο Ενοποιημένων Υπηρεσιών* ή *Integrated Services Digital Network, ISDN*. Το ISDN επιτρέπει τη μετάδοση φωνής, εικόνας, video και δεδομένων σε ψηφιακή μορφή χρησιμοποιώντας την υπάρχουσα υποδομή δισύρματων τηλεφωνικών καλωδίων.

Επισήμανση: Τα δισύρματα τηλεφωνικά καλώδια (τα κοινά τηλεφωνικά καλώδια του ΟΤΕ που καταλήγουν στα σπίτια μας) αποτελούν μια τεράστια υποδομή που αναπτύχθηκε σε διάστημα πολλών ετών για να εξυπηρετήσει τις ανάγκες της κλασικής τηλεφωνίας (γνωστή και ως POTS, Plain Old Telephone System, το απλό δηλ. τηλεφωνικό δίκτυο). Οι γραμμές αυτές δεν έχουν σχεδιαστεί ειδική για μετάδοση δεδομένων, καθώς το τηλεφωνικό δίκτυο μεταδίδει φωνή με καθαρά αναλογικό τρόπο (και με αρκετά μικρό εύρος ζώνης, από 300HZ ως 3400HZ). Ωστόσο, η ανάπτυξη του ISDN επιτρέπει την χρήση των κλασικών γραμμών για μετάδοση καθαρά ψηφιακών σημάτων, τα οποία πλεονεκτούν σημαντικά σε σχέση με τα αναλογικά (Πως; Άσκηση για τον αναγνώστη).

Με την βοήθεια του ISDN, το τηλεπικοινωνιακό δίκτυο γίνεται ανεξάρτητο από το είδος της πληροφορίας που διακινείται, αφού μέσα από αυτό (και με καθαρά ψηφιακή μορφή), μπορεί πλέον να διακινηθούν δεδομένα υπολογιστών, φωνή, video. Αντίστοιχα, τυποποιείται και το είδος της διασύνδεσης διάφορων συσκευών (από διάφορους κατασκευαστές) στο δίκτυο, και δεν χρειάζεται ειδικός (και ενδεχομένως ακριβός) εξοπλισμός για την προσαρμογή τους.

Τα βασικά στοιχεία που χαρακτηρίζουν το ISDN είναι:

- **Ψηφιακή Μετάδοση:** Όλα τα δεδομένα στο δίκτυο ISDN κινούνται σε ψηφιακή μορφή. Ακόμα και η φωνή (τηλεφωνική συνδιάλεξη) ψηφιοποιείται πριν σταλεί στη γραμμή.
- **Η σηματοδοσία** γίνεται μέσω ιδιαίτερου καναλιού (common channel signaling). Η σηματοδοσία περιλαμβάνει τα βοηθητικά σήματα με τα οποία γίνεται η διαχείριση μιας επικοινωνίας (π.χ. το κουδούνισμα σε μια τηλεφωνική κλήση, η διαδικασία έναρξης και λήξης μιας σύνδεσης κ.λ.π.)
- **Ο ενιαίος τρόπος με τον οποίο συνδέονται συσκευές και χρήστες στο δίκτυο:** Οι υπηρεσίες του δικτύου είναι όλες διαθέσιμες μέσω ενός και μόνο τύπου σύνδεσης (από την ίδια απόληξη (prižα)).

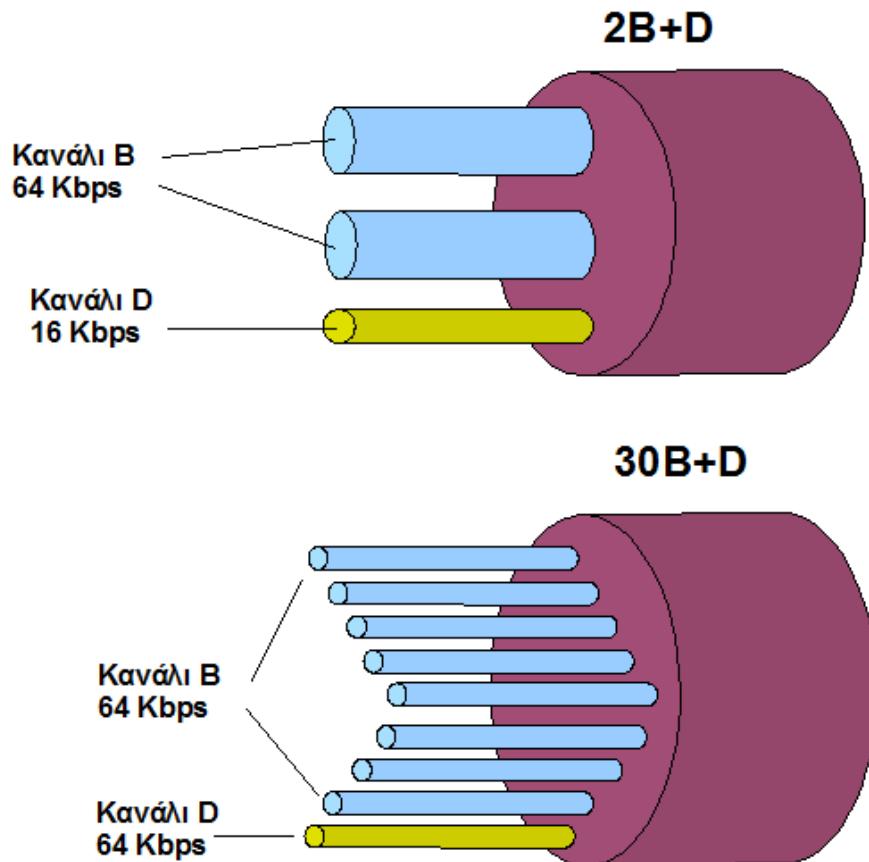
Το δίκτυο διαθέτει δύο τρόπους πρόσβασης, την διεπαφή βασικού ρυθμού και την διεπαφή πρωτεύοντος ρυθμού.

Η **διεπαφή βασικού ρυθμού** (Basic Rate Interface, BRI) παρέχει δύο κανάλια μετάδοσης δεδομένων (2 κανάλια-B) και ένα κανάλι σηματοδοσίας (1 κανάλι-D). Κάθε κανάλι B επιτυγχάνει ρυθμό μετάδοσης 64 KBps και μεταφέρει ψηφιακά δεδομένα. Η φωνή (τηλεφωνική κλήση) μεταφέρεται αφού πρώτα ψηφιοποιηθεί με ρυθμό δειγματοληψίας 8000 HZ και δείγματα 8bit. Το κανάλι D έχει ρυθμό μετάδοσης 16 KBps και χρησιμοποιείται για τις βοηθητικές λειτουργίες (έναρξη / λήξη σύνδεσης). Οι χρήστες έχουν τη δυνατότητα να χρησιμοποιούν το ένα ή και τα δύο κανάλια B ταυτόχρονα. Αυτό σημαίνει ότι μπορούν να χρησιμοποιούν το ένα κανάλι για μετάδοση δεδομένων και το άλλο για φωνή, ή και τα δύο για δεδομένα, ή τέλος και τα δύο για φωνή. Με το ISDN είναι δυνατόν να έχουμε ταυτόχρονα δύο τηλεφωνικές συνδιαλέξεις μέσω της ίδιας γραμμής. Αν συνδυάσουμε και τα δύο κανάλια για μετάδοση δεδομένων, επιτυγχάνουμε συνολικό ρυθμό μετάδοσης 128 KBps. Μαζί με το κανάλι D (το οποίο ωστόσο δεν μεταφέρει χρήσιμα δεδομένα χρήστη) ο ρυθμός μετάδοσης φτάνει τα 144 KBps.

Η **διεπαφή πρωτεύοντος ρυθμού** (Primary Rate Interface, PRI) παρέχει 30 κανάλια δεδομένων τύπου B (ταχύτητας 64 Kbps) και ένα κανάλι D σηματοδοσίας, το οποίο στη συγκεκριμένη περίπτωση είναι επίσης ρυθμού 64 Kbps (Θυμηθείτε ότι στο BRI είναι 16 Kbps). Εκτός από τα 30 κανάλια B και το 1 κανάλι D, χρησιμοποιείται ένα ακόμα κανάλι των 64 Kbps για πλαισίωση (framing) και συντήρηση του δικτύου. Το κανάλι αυτό δεν χαρακτηρίζεται ως B ή D.

Πλαισίωση ή framing (στημείωση κατανόησης): Στις τηλεπικοινωνίες, τα περισσότερα σήματα που μεταδίδονται ψηφιακά σε ένα μέσο (π.χ. καλώδιο) μεταφέρουν εκτός από τα χρήσιμα δεδομένα και επιπλέον πληροφορίες που χρησιμοποιούνται από τα κυκλώματα λήψης για να επιτύχουν το συγχρονισμό και τον έλεγχο ροής των δεδομένων από τον αποστολέα στον παραλήπτη. Στη διαδικασία της πλαισίωσης, ο παραλήπτης λαμβάνει και ξεχωρίζει αυτά τα σήματα από τα υπόλοιπα δεδομένα, τα οποία έπειτα μπορούν να αποκωδικοποιηθούν και να χρησιμοποιηθούν.

Ο συνολικός ρυθμός μετάδοσης είναι λοιπόν $30 \times 64 \text{ Kbps}$ (τα κανάλια B) + 1 X 64 Kbps (το κανάλι D) + 1 X 64 Kbps (το έξτρα κανάλι σηματοδοσίας) = $2048 \text{ Kbps} = 2,048 \text{ Mbps}$. Είναι η ίδια ταχύτητα που υποστηρίζει μια ψηφιακή γραμμή E1. Το πρότυπο αυτό χρησιμοποιείται στην Ευρώπη, στη Βόρεια Αμερική και στην Ιαπωνία χρησιμοποιείται το πρότυπο 23B+D. Και στην περίπτωση αυτή τόσο τα κανάλια B όσο και το κανάλι D είναι ρυθμού 64 Kbps ενώ χρησιμοποιείται ένα ακόμα κανάλι (που δεν χαρακτηρίζεται ως B ή D) με ταχύτητα 8 Kbps για πλαισίωση



Σχήμα 6.2: Διεπαφές βασικού και πρωτεύοντος ρυθμού στο ISDN

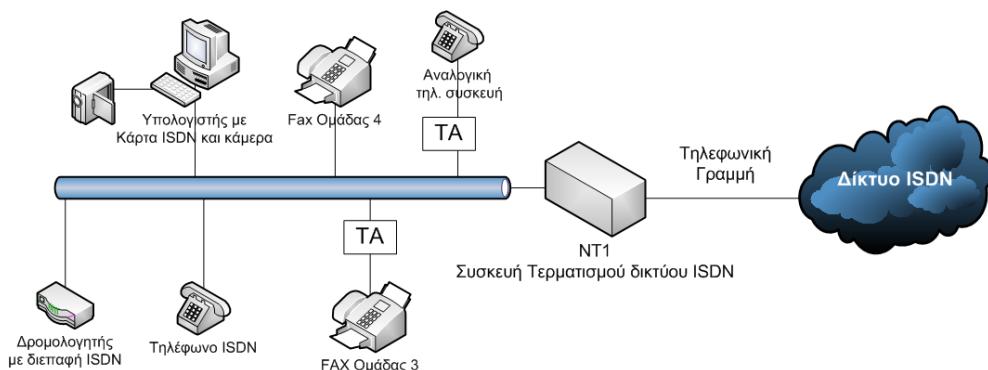
και συντήρηση του δικτύου. Στην περίπτωση αυτή ο συνολικός ρυθμός μετάδοσης είναι $23 \times 64 \text{ Kbps}$ (τα κανάλια B) + 1 X 64 Kbps (το κανάλι D) + 1 X 8 Kbps (το έξτρα κανάλι σηματοδοσίας) = 1544 Kbps = 1,544 Mbps.

Αν και το ISDN χρησιμοποιεί την ήδη υπάρχουσα τηλεπικοινωνιακή υποδομή (τα ίδια χάλκινα τηλεφωνικά καλώδια που χρησιμοποιούνται στην κλασικό τηλεφωνικό σύστημα), ωστόσο απαιτεί την εγκατάσταση μιας ειδικής συσκευής στη μεριά του χρήστη. Πρόκειται για την **συσκευή τερματισμού δικτύου NT1**. Ο παροχέας της υπηρεσίας ISDN (π.χ. OTE) εγκαθιστά τη συσκευή αυτή στο χώρο του συνδρομητή και την συνδέει στον κόμβο ISDN στο τηλεφωνικό κέντρο που μπορεί να βρίσκεται αρκετά χιλιόμετρα μακριά. Η σύνδεση γίνεται με το κανονικό καλώδιο (συνεστραμμένων ζευγών) του συνδρομητή που χρησιμοποιούνταν παλιότερα για το απλό τηλέφωνο. Η κίνηση έπειτα δρομολογείται στο δίκτυο του τηλεπικοινωνιακού φορέα με καθαρά ψηφιακό τρόπο (χρησιμοποιώντας τεχνικές μεταγωγής πακέτων, νοητού κυκλώματος κλπ). Η συσκευή τερματισμού NT1 μπορεί να συνδεθεί με μέχρι 8 συ-

σκευές σε απόσταση μέχρι 150 μέτρα. Οι συσκευές αυτές μπορεί να είναι είτε ειδικές για ISDN (μη ξεχνάμε ότι πρόκειται για ψηφιακά δεδομένα), είτε οι κλασικές αναλογικές τηλεφωνικές συσκευές μέσω του ειδικού **τερματικού προσαρμογέα TA**. Οι ειδικές συσκευές μπορεί να είναι ψηφιακά τηλέφωνα, FAX ομάδας 4, εικονοτηλέφωνα κλπ.

Τερματικός Προσαρμογέας (TA) (σημείωση κατανόησης): Όπως είπαμε ήδη, για να συνδέσουμε ένα κλασικό αναλογικό τηλέφωνο σε μια γραμμή ISDN, χρειάζεται ειδικός προσαρμογέας. Γιατί συμβαίνει αυτό; Καθώς το ISDN χρησιμοποιεί ψηφιακή μετάδοση, το κλασικό τηλέφωνο δεν μπορεί να συνδεθεί απευθείας – τα δεδομένα φωνής είναι αναλογικά. Ο προσαρμογέας TA διαθέτει ένα μετατροπέα αναλογικού σε ψηφιακό (ADC, Analog to Digital Converter) ο οποίος μετατρέπει τη φωνή από τη συσκευή σε ψηφιακά δεδομένα, καθώς και μετατροπέα ψηφιακού σε αναλογικό (DAC, Digital to Analog Converter) ο οποίος κάνει την αντίστροφη διαδικασία. Στην πραγματικότητα ο προσαρμογέας αυτός βρίσκεται συνήθως ενσωματωμένος στη συσκευή NT1 που μας δίνει ο παροχέας. Για παράδειγμα ο OTE δίνει τη συσκευή Netmod η οποία περιέχει μέσα και το TA.

Μη ξεχνάμε ότι τα κανάλια στο ISDN είναι λογικά και όχι φυσικά. Όταν λέμε λοιπόν για 30 κανάλια Β δεν εννοούμε 30 καλώδια. Το ISDN λειτουργεί πάντα με την ίδια δισύρματη γραμμή που χρησιμοποιείται και στο κοινό τηλεφωνικό δίκτυο.



Σχήμα 6.3: Ο εξοπλισμός του ISDN

Μπορούμε να συνδυάσουμε το βασικό και τον πρωτεύοντα ρυθμό για να δημιουργήσουμε ένα δίκτυο με μια κεντρική θέση και πολλές περιφερειακές. Στην κεντρική θέση μπορούμε να χρησιμοποιήσουμε σύνδεση πρωτεύοντος ρυθμού και στις περιφερειακές βασικού ρυθμού. Έτσι μπορούμε για παράδειγμα να συνδέσουμε ταυτό-

χρονα ένα κεντρικό υπολογιστή σε 30 περιφερειακούς υπολογιστές (23 για Αμερική και Ιαπωνία). Η υπηρεσία ISDN είναι χρήσιμη όταν η μετάδοση δεδομένων δεν εί-

Πλεονεκτήματα	Μειονεκτήματα	Βασική Χρήση
Κόστος ανάλογο με την κίνηση	Αν και αναπτύσσεται διαρκώς δεν είναι ακόμα παγκόσμια διαθέσιμο	Σποραδική κίνηση που περιλαμβάνει φωνή, εικόνα, δεδομένα
Μεταφορά φωνής, εικόνας και δεδομένων	Υψηλό κόστος για συνεχή μεταφορά δεδομένων	Σαν εφεδρική γραμμή μαζί με τις ασύγχρονες επιλεγόμενες τηλεφωνικές γραμμές
Γρήγορη εγκαθίδρυση σύνδεσης		

Πίνακας 6.2: Χαρακτηριστικά ISDN

ναι συνεχής και οι ανάγκες σε ταχύτητα κυμαίνονται. Καθώς γίνεται κλήση για την αποκατάσταση της σύνδεσης, ο συνδρομητής πληρώνει για όση ώρα μεταφέρει δεδομένα (σε αντίθεση με την ADSL που η μετάδοση είναι συνεχής και η χρέωση είναι πάγια). Καθώς σήμερα χρησιμοποιούνται όλο και περισσότερο άλλες τεχνολογίες με μόνιμη σύνδεση (ADSL), το ISDN συνήθως περιορίζεται για χρήση ως εφεδρική σύνδεση σε απομακρυσμένα μηχανήματα / δίκτυα, σε περίπτωση βλάβης της κύριας γραμμής.

Το ISDN που περιγράψαμε σε αυτή την ενότητα, αναφέρεται και ως *ISDN στενής ζώνης* (Narrow Band ISDN). Ωστόσο αναπτύσσονται (έτσι νομίζει το βιβλίο σας δηλαδή) πρότυπα και για *ISDN ευρείας ζώνης* (Broadband ISDN) το οποίο χρησιμοποιεί οπτική ίνα.

6.8 xDSL

Η τεχνολογία xDSL (Digital Subscriber Line) αποτελεί μια εξέλιξη της τεχνολογίας ISDN και συνεχίζει να χρησιμοποιεί τα χάλκινα τηλεφωνικά καλώδια που χρησιμοποιούνται ήδη για τη μετάδοση φωνής. Το τμήμα του καλωδίου που ξεκινάει από τον συνδρομητή και καταλήγει στον τηλεπικοινωνιακό εξοπλισμό του παροχέα, ονομάζεται συνδρομητικός (τοπικός) βρόχος (local loop). Η γραμμή DSL υπάρχει σε διάφορες παραλλαγές, έτσι το x στην ονομασία μπορεί να συμβολίζει το ADSL, R-ADSL, HDSL, SDSL, VDSL. Η τεχνολογία γενικά αποτελεί εξέλιξη του ISDN βασικού ρυθμού που παρέχει δύο κανάλια δεδομένων (B) με ταχύτητα 64Kbps και ένα κανάλι σηματοδοσίας ταχύτητας 16Kbps.

Ο βασικός λόγος που ώθησε την ανάπτυξη της τεχνολογίας DSL είναι η χαμηλή ταχύτητα που επιτυγχάνονταν με τις προηγούμενες τεχνολογίες, ειδικά όσο αφορά τους οικιακούς χρήστες. Για παράδειγμα, η τυπική σύνδεση με τη βοήθεια modem σε PSTN γραμμή φτάνει μέχρι την ταχύτητα των 56Kbps (θεωρητικά) η οποία όμως δεν μπορεί να μεταφέρει το είδος των δεδομένων (πολυμέσα όπως ήχος και video, τηλεδιάσκεψη κλπ) που απαιτούνται στις σύγχρονες εφαρμογές Internet. Πράγματι τα 56Kbps (πρότυπο modem V90) σήμερα μόλις που επαρκούν για απλές χρήσεις όπως το email. Μεγάλες ταχύτητες μπορούν φυσικά να επιτευχθούν με τεχνολογία οπτικών ινών (Fiber to Home), το κόστος της όμως είναι γενικά απαγορευτικό για οικιακή χρήση.

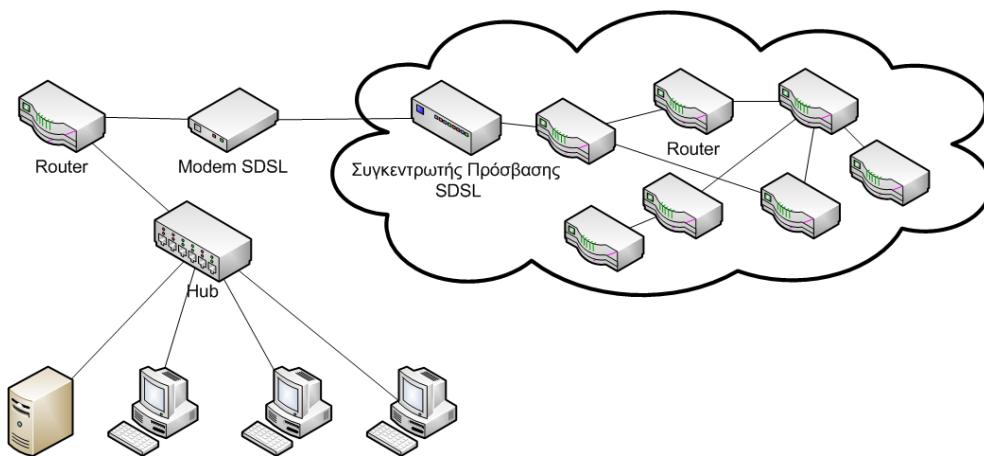
Αφόρτιστη γραμμή (σημείωση κατανόησης): Σε τηλεφωνικές γραμμές (ειδικά σε μεγάλου μήκους) χρησιμοποιούνται πολλές φορές κάποια εξαρτήματα γνωστά ως πηνία φόρτισης (loading coils). Τα πηνία φόρτισης αυξάνουν την επαγωγική αντίσταση της γραμμής, και σε συνδυασμό με τη χωρητική αντίσταση του καλωδίου δημιουργούν ένα φίλτρο που επιτρέπει μόνο στις συχνότητες της φωνής (300-3400Hz) να περάσουν από τη γραμμή. Αυτό βελτιώνει αισθητά την ποιότητα του ήχου στο τηλέφωνο, αποκόπτει όμως τις υψηλές συχνότητες που χρησιμοποιούνται στην DSL. Για το λόγο αυτό τα πηνία αυτά πρέπει να αφαιρεθούν για να χρησιμοποιηθεί η γραμμή ως DSL. Σε περιπτώσεις όμως που η απόσταση συνδρομητή - τηλεφωνικού κέντρου είναι μεγάλη (μεγαλύτερη από 6 χιλιόμετρα) δεν είναι δυνατή η αφαίρεση των πηνίων αυτών, καθιστώντας αδύνατη την εγκατάσταση DSL.

Η τεχνολογία xDSL μπορεί να προσφέρει ταχύτητες της τάξης των Mbps. Χρησιμοποιεί τον συνδρομητικό βρόχο ως μέρος του κυκλώματος μεταφοράς των δεδομένων (ως αφόρτιστη μισθωμένη γραμμή). Η χρήση αυτής της τεχνολογίας δεν απαιτεί επαναλήπτες ή ενισχυτές, και υποστηρίζει ταχύτητες προτύπων E1 (2,048 Mbps) και T1 (1,544 Mbps) για μετάδοση δεδομένων. Ταυτόχρονα είναι δυνατή και η μετάδοση φωνής για λειτουργία ως κανονικό τηλεφωνικό δίκτυο. Σε κάθε άκρο της σύνδεσης χρησιμοποιείται μια συσκευή τερματισμού (baseband modem). Η συσκευή αυτή λειτουργεί όπως το modem, λαμβάνοντας ροή ψηφιακών δεδομένων και μετατρέποντας τη σε αναλογικό σήμα το οποίο είναι κατάλληλο για τη μεταφορά μέσω του συνδρομητικού βρόχου. Το σήμα αυτό είναι σημαντικά υψηλότερου ρυθμού (μεγαλύτερης συχνότητας) από το κλασικό τηλεφωνικό σήμα (φωνή).

Σημείωση κατανόησης: Γνωρίζουμε ότι γενικά η τηλεφωνική γραμμή δεν είναι κατάλληλη για μετάδοση σημάτων υψηλών συχνοτήτων. Το μυστικό της DSL είναι ότι αυτή η αναλογική μετάδοση γίνεται μόνο σε μικρό τμήμα, στον τοπικό βρόχο. Πρακτικά αυτό σημαίνει από το σπίτι του συνδρομητή μέχρι το τηλεφωνικό κέντρο,

και όχι μέχρι τα τελικά μηχανήματα της εταιρείας παροχής Internet. Στις περισσότερες περιπτώσεις το τμήμα αυτό είναι μικρό - από μερικές εκατοντάδες μέτρα μέχρι 2-3 χιλιόμετρα. Σε περίπτωση που ο συνδρομητής είναι αρκετά μακριά από το τηλεφωνικό κέντρο, η ποιότητα και η ταχύτητα της γραμμής DSL μειώνονται δραματικά.

Για τη μετάδοση χρησιμοποιούνται διάφορες τεχνολογίες διαμόρφωσης (θυμάστε τι είναι η διαμόρφωση;) με τις οποίες το διαθέσιμο εύρος ζώνης της γραμμής χωρίζεται συνήθως σε τρία κανάλια: Ένα για τη μετάδοση δεδομένων προς τα πάνω (από το συνδρομητή προς τον παροχέα, γνωστό ως upstream), ένα προς τα κάτω (από τον παροχέα προς το συνδρομητή, γνωστό ως downstream) και ένα για την μετάδοση φωνής.



Σχήμα 6.4: Πρόσβαση τοπικού δικτύου σε δίκτυο ευρείας περιοχής μέσω τεχνολογίας SDSL

Ανάλογα με το αν η ταχύτητα μετάδοσης προς τις δύο κατευθύνσεις είναι ίδια ή διαφορετική έχουμε τις παραλλαγές της σύγχρονης DSL (SDSL, ίδια ταχύτητα upstream και downstream) και ασύγχρονης DSL (ADSL, διαφορετικές ταχύτητες upstream / downstream). Υπάρχουν διάφορες παραλλαγές xDSL που υποστηρίζουν αυτά τα είδη μεταδόσεων. Αν για παράδειγμα μας ενδιαφέρει η οικιακή χρήση, είναι σημαντικό να έχουμε μεγαλύτερη ταχύτητα στη λήψη δεδομένων, οπότε χρειαζόμαστε μεγαλύτερη ταχύτητα downstream (για να βλέπουμε ιστοσελίδες, να κατεβάζουμε αρχεία κλπ). Υπάρχουν περιπτώσεις που μας ενδιαφέρει να έχουμε μεγάλη ταχύτητα μετάδοσης (upstream) όπως για παράδειγμα αν παρέχουμε υπηρεσίες στο διαδίκτυο (web server κλπ) ή για τηλεδιάσκεψη. Μια τέτοια γραμμή DSL μπορεί να χρησιμοποιηθεί ως υποκατάστατο μιας μισθωμένης γραμμής E1 ή T1.

Σημείωση: Οι ταχύτητες που μπορούν να επιτευχθούν με την τεχνολογία DSL ανά-

Τεχνολογία	Σημασία	Αριθμός Ζευγών	Ταχύτητα	Μέγιστη Απόσταση
ADSL	Assymetric 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 6.3: Τεχνολογίες xDSL

μεσα στα baseband modems (το ένα διαθέτει ο συνδρομητής και το άλλο ο παροχέας) εξαρτώνται από την απόσταση που τα χωρίζει και από τη διατομή του τηλεφωνικού καλωδίου που χρησιμοποιείται. Πιο χοντρά καλώδια έχουν καλύτερη απόδοση, επιτυγχάνοντας μεγαλύτερη ταχύτητα σε μεγαλύτερες αποστάσεις, αλλά έχουν και μεγαλύτερο κόστος. Ο πίνακας 6.4 δείχνει τη σχέση απόστασης - ταχύτητας - διατομής για την τεχνολογία SDSL.

Ταχύτητα	0.4 mm	0.5 mm	0.6 mm	0.8 mm	1.0 mm	1.2 mm
128 Kbps	6.5	8.9	12.7	16.1	22.5	25.1
256 Kbps	5.5	7.5	10.8	13.6	19.0	21.2
384 Kbps	5.1	7.0	10.0	12.6	17.6	19.7
512 Kbps	4.7	6.4	9.2	11.6	16.3	18.1
768 Kbps	4.4	6.0	8.6	10.9	15.2	17.0
1152 Kbps	3.8	5.2	7.4	9.4	13.1	14.7
1536 Kbps	3.3	4.5	6.5	8.2	11.4	12.7
2048 Kbps	2.5	3.4	4.9	6.2	8.7	9.7
2304 Kbps	2.2	3.0	4.3	5.4	7.6	8.5

Πίνακας 6.4: Απόσταση (σε Km) που μπορεί να καλυφθεί ανάλογα με τη διατομή του καλωδίου και την επιθυμητή ταχύτητα σε σύνδεση με SDSL modem

Από τον πίνακα 6.3 βλέπουμε ότι για απλή πρόσβαση στο Διαδίκτυο, μπορούμε να χρησιμοποιήσουμε τεχνολογία ADSL ή ADSL Lite. Σε περίπτωση που απαιτούνται υψηλές ταχύτητες για π.χ. πολυμεσικές εφαρμογές (τηλεόραση υψηλής ευκρίνειας κλπ). Οι συμμετρικές παραλλαγές HDSL και SDSL που επιτυγχάνουν υψηλές ταχύτητες και προς τις δύο κατευθύνσεις, μπορούν να χρησιμοποιηθούν (αντί για τις

T1 και E1) για την διασύνδεση τοπικών δικτύων μεταξύ τους.

Οι διάφορες παραλλαγές της τεχνολογίας DSL είναι σε διαρκή εξέλιξη ενώ ταυτόχρονα και το κόστος εγκατάστασης και λειτουργίας τους όλο και μειώνεται. Για το λόγο αυτό αναμένεται ότι στα επόμενα χρόνια η τεχνολογία DSL θα έχει όλο και μεγαλύτερη εφαρμογή και θα αποτελεί την πλέον διαδεδομένη τεχνολογία για παροχή υπηρεσιών όπως η πρόσβαση τελικών χρηστών στο Διαδίκτυο και σε online υπηρεσίες, η τηλεδιάσκεψη, το video κατά απαίτηση (video on demand), η δικτυακή τηλεόραση, μετάδοση φωνής, IP telephony κ.α. Ο πίνακας 6.5 δείχνει τα σημαντικότερα πλεονεκτήματα και μειονεκτήματα αυτής της τεχνολογίας.

Πλεονεκτήματα	Μειονεκτήματα	Βασική Χρήση
Αξιοποίηση υπάρχουσας υποδομής	Μικρή Απόσταση	Πρόσβαση σε Internet, intranet, τηλεφωνία μέσω IP (VoIP, Voice Over IP)
Πολύ υψηλές ταχύτητες. Χαμηλό κόστος εγκατάστασης και λειτουργίας		Διασύνδεση τοπικών δικτύων, υποκατάστατο γραμμών E1 και T1.
Υποστήριξη μετάδοσης δεδομένων και φωνής μέσα από την ίδια τηλεφωνική γραμμή		Video κατά παραγγελία (Video on Demand), τηλεόραση υψηλής ευκρίνειας

Πίνακας 6.5: Χαρακτηριστικά xDSL

Κεφάλαιο 7

Διαδικτύωση – Internet

Εισαγωγή

Στο κεφάλαιο αυτό παρουσιάζεται ο τρόπος επικοινωνίας σε ένα δίκτυο υπολογιστών. Το κεφάλαιο εστιάζεται στο *Επίπεδο Δικτύου* του OSI (το οποίο είδατε στο μάθημα της Β' Τάξης). Γίνεται ωστόσο αναφορά και στα ανώτερα επίπεδα του OSI για να γίνουν καλύτερα κατανοητές οι διαδικασίες επικοινωνίας των εφαρμογών μέσω δικτύου. Οι βασικές αρχές επικοινωνίας εξηγούνται με τη βοήθεια του πρωτόκολλου *TCP/IP* (Transmission Control Protocol / Internet Protocol, Πρωτόκολλο Ελέγχου Μετάδοσης και Διαδικτύου) και με την εφαρμογή του στο *Παγκόσμιο Διαδίκτυο* (Internet).

Οι βασικές έννοιες του κεφαλαίου είναι:

- Η διεύθυνση ενός υπολογιστή
- Το όνομα ενός υπολογιστή
- Η διαδρομή που ακολουθούν τα πακέτα μέχρι να φτάσουν στον προορισμό τους

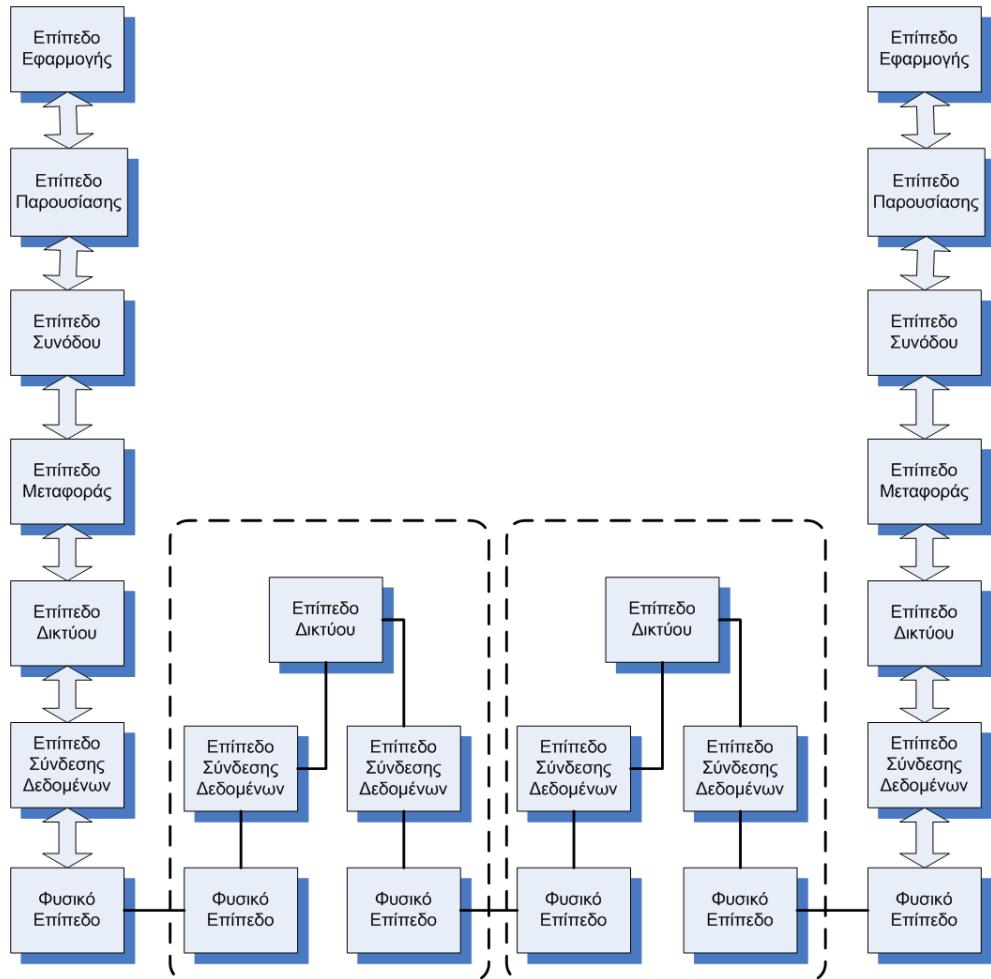
και φυσικά πως όλα τα παραπάνω συσχετίζονται μεταξύ τους.

7.1 Επίπεδο Δικτύου

7.1.1 Γενικές Αρχές

Το επίπεδο δικτύου ασχολείται με τη μεταφορά των πακέτων από την αφετηρία στον προορισμό τους και καθορίζει τη διαδρομή που θα ακολουθήσουν. Στα δίκτυα ευ-

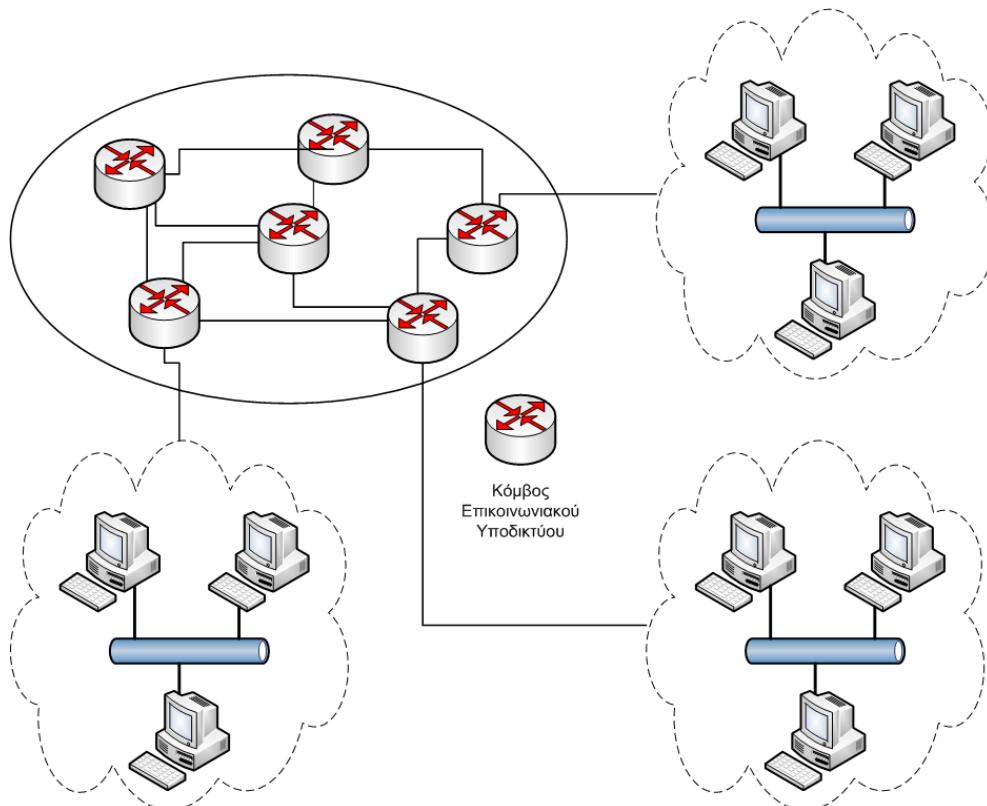
ρείας περιοχής που εξετάζουμε, τα πακέτα για να φτάσουν στον προορισμό τους χρειάζεται να περάσουν από ένα αριθμό ενδιάμεσων κόμβων. Οι κόμβοι αυτοί συμμετέχουν στη διαδικασία παράδοσης. Στο σχήμα 7.1 φαίνεται ότι το επίπεδο δικτύου είναι το χαμηλότερο από τα επίπεδα του OSI που ασχολείται με την επικοινωνία από άκρο σε άκρο. Το επίπεδο δικτύου παρέχει μια νοητή γραμμή επικοινωνίας μεταξύ δύο υπολογιστών ενός δικτύου. Το σημαντικό σημείο είναι ότι το επίπεδο δικτύου



Σχήμα 7.1: Αρχιτεκτονική Μοντέλου OSI

δεν χρησιμοποιείται μόνο στους κόμβους πηγής και προορισμού αλλά και σε όλους τους ενδιάμεσους κόμβους που συμμετέχουν στην επικοινωνία. Για να μπορέσει λοιπόν να παραδοθεί ένα πακέτο θα πρέπει να συνεργαστούν μεταξύ τους όλα τα επίπεδα δικτύου των ενδιάμεσων και των αρχικών κόμβων (πηγής και προορισμού). Αυτό σημαίνει ότι οι ενδιάμεσοι κόμβοι (Σχήμα 7.2) θα πρέπει να διαθέτουν και να μπορούν να χρησιμοποιήσουν όλα τα κατώτερα επίπεδα του OSI, τουλάχιστον μέχρι

το επίπεδο δικτύου (Δηλ. το φυσικό, το σύνδεσης δεδομένων και το δικτύου). Το σύνολο των ενδιάμεσων κόμβων που εξασφαλίζει την επικοινωνία μεταξύ των τελικών υπολογιστών ονομάζεται **επικοινωνιακό υποδίκτυο**. Σκοπός του υποδικτύου αυτού είναι η μεταφορά των πακέτων από την πηγή στον προορισμό. Με τον τρόπο αυτό γίνεται λογικός διαχωρισμός μεταξύ των θεμάτων επικοινωνίας (που αναλαμβάνει το επικοινωνιακό υποδίκτυο) και των θεμάτων των εφαρμογών (που είναι αρμοδιότητα των τελικών υπολογιστών και των οποίων ο χειρισμός γίνεται συνήθως σε ανώτερα επίπεδα του OSI). Το επίπεδο δικτύου σε κάθε κόμβο αποφασίζει για τη



Σχήμα 7.2: Γενική εικόνα δικτύου υπολογιστών

διαδρομή που θα ακολουθήσει κάθε πακέτο μέχρι να φτάσει στον επόμενο κόμβο. Η διαδρομή αυτή βασίζεται στα στοιχεία που έχει ο κόμβος στη διάθεση του και τα οποία αφορούν συνήθως την τοπολογία του δικτύου καθώς και την κατάσταση των γραμμών επικοινωνίας. Γίνεται πάντοτε προσπάθεια να επιλεχθεί η καλύτερη δυνατή διαδρομή: Για παράδειγμα καλύτερη μπορεί να είναι η συντομότερη (αυτή που περνάει από τον μικρότερο δυνατό αριθμό ενδιάμεσων κόμβων) ή αυτή που τη δεδομένη στιγμή χρησιμοποιεί τους κόμβους που έχουν τη μικρότερη κίνηση (εξασφαλίζοντας έτσι ότι η κατανομή του φορτίου στο δίκτυο είναι ομοιόμορφη, και δεν

υπάρχουν υπερφορτωμένες και άδειες γραμμές).

Το επίπεδο δικτύου προσφέρει γενικά δύο κατηγορίες υπηρεσιών:

- Υπηρεσίες χωρίς σύνδεση
- Υπηρεσίες προσανατολισμένες σε σύνδεση

Ανεξάρτητα από τον τύπο υπηρεσιών που υποστηρίζει το επίπεδο δικτύου, το επικοινωνιακό υποδίκτυο μπορεί να βασίζεται σε δύο διαφορετικές φιλοσοφίες:

- Νοητό Κυκλώματος (Virtual Circuit, VC)
- Αυτοδύναμων πακέτων (datagrams)

Σημείωση: Έχετε συναντήσει τις παραπάνω έννοιες στις τεχνικές μεταγωγής στο μάθημα της Β' τάξης.

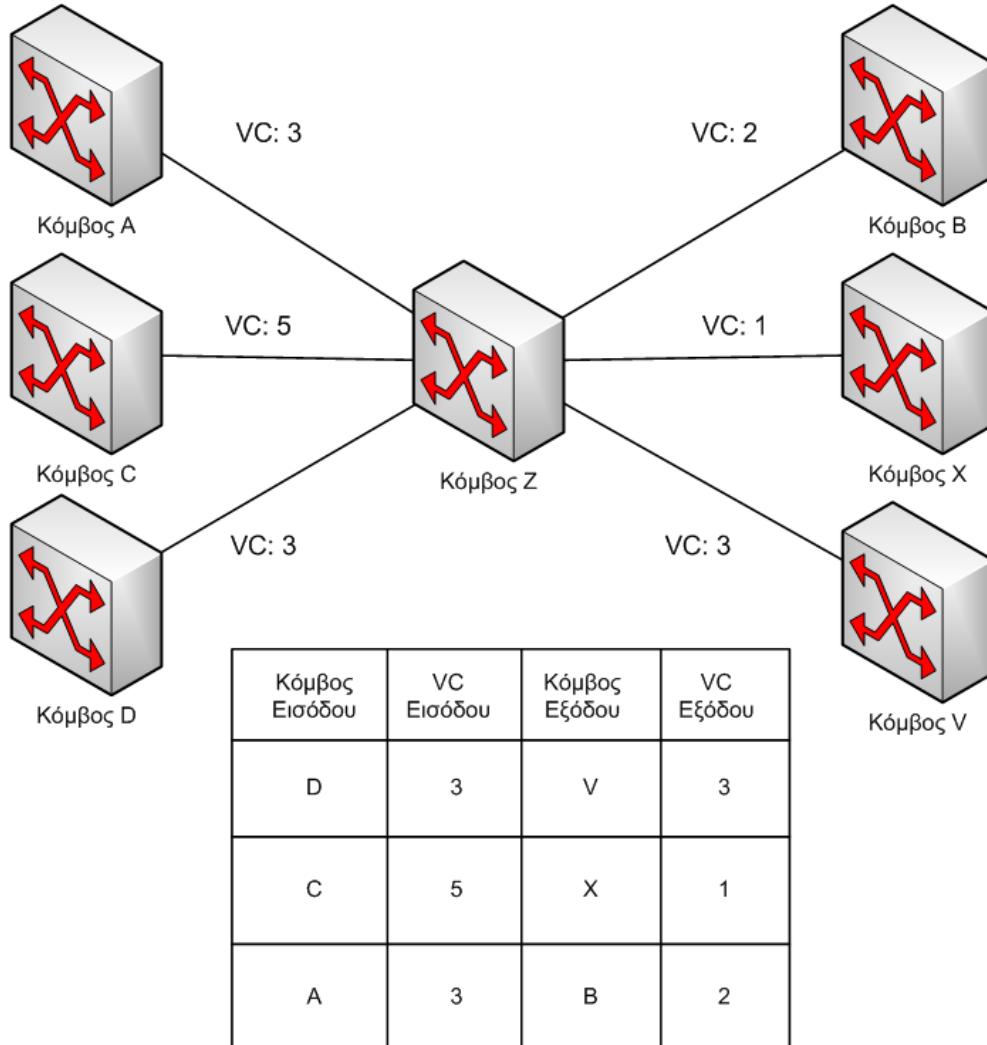
Τα νοητά κυκλώματα χρησιμοποιούνται κυρίως για υπηρεσίες με σύνδεση. Στην περίπτωση αυτή, όλες οι αποφάσεις που αφορούν τη διαδρομή που θα ακολουθήσουν τα πακέτα μέσα από το επικοινωνιακό δίκτυο λαμβάνονται από την αρχή, και πριν ξεκινήσει η κανονική μετάδοση των δεδομένων. Όλα τα πακέτα που ανήκουν στην ίδια επικοινωνία θα ακολουθήσουν την ίδια διαδρομή. Φαίνεται έτσι σαν να υπάρχει ένα συγκεκριμένο μονοπάτι μέσα από τους κόμβους, το οποίο όμως δεν έχει δημιουργηθεί από πραγματικές φυσικές γραμμές αλλά από συμφωνία των κόμβων μεταξύ τους.

Τι μεταγωγή θα είχαμε αν το μονοπάτι δημιουργούνταν με απευθείας φυσικές συνδέσεις;

Φυσικά, αυτό σημαίνει ότι για μια συγκεκριμένη σύνδεση κάθε κόμβος που μετέχει θα πρέπει να μπορεί να αναγνωρίσει ότι το εισερχόμενο πακέτο ανήκει σε αυτήν και να θυμάται σε ποιο επόμενο κόμβο πρέπει να το στείλει (καθώς όλα τα πακέτα μιας τέτοιας σύνδεσης πρέπει να ακολουθούν την ίδια διαδρομή). Για να γίνει αυτό, κάθε κόμβος του επικοινωνιακού υποδικτύου διαθέτει ένα πίνακα με μια καταχώριση για κάθε νοητό κύκλωμα στο οποίο μετέχει (ένας κόμβος μπορεί κάθε φορά να μετέχει σε ένα αριθμό από νοητά κυκλώματα και πρέπει να αναγνωρίζει ποιο πακέτο ανήκει σε ποιο κύκλωμα). Τα στοιχεία που περιλαμβάνει μια τέτοια καταχώριση είναι:

- Αριθμός εισερχόμενου νοητού κυκλώματος
- Γραμμή εισόδου
- Αριθμός εξερχόμενου νοητού κυκλώματος

- Γραμμή εξόδου



Σχήμα 7.3: Λειτουργία Νοητών Κυκλωμάτων

Σε κάθε περίπτωση, όταν γίνεται εγκατάσταση μιας σύνδεσης δικτύου ανατίθεται σε αυτήν ένας μοναδικός αναγνωριστικός αριθμός, ο **αριθμός νοητού κυκλώματος**. Ο αριθμός αυτός παράγεται τοπικά από τον κόμβο που ξεκινάει την αποστολή και δεν μπορεί να είναι ίδιος με κανένα άλλο που χρησιμοποιείται τη δεδομένη στιγμή από τον ίδιο κόμβο για κάποια άλλη σύνδεση. Ο αναγνωριστικός αριθμός γίνεται γνωστός και αποθηκεύεται στους πίνακες κατάστασης όλων των ενδιάμεσων κόμβων που μετέχουν στη συγκεκριμένη επικοινωνία. Βέβαια, μπορεί σε κάποιο ενδιάμεσο κόμβο ο αριθμός αυτός να χρησιμοποιείται ήδη από μια άλλη σύνδεση και να μην είναι ελεύθερος. Για αυτό το λόγο οι κόμβοι αυτοί έχουν την δυνατότητα να τροπο-

ποιούν τον αριθμό νοητού κυκλώματος των εισερχόμενων πακέτων και αποθηκεύουν την πληροφορία αυτή (ποιος αριθμός έχει τροποποιηθεί και με ποιο τρόπο) στον πίνακα κατάστασης τους.

Στο σχήμα 7.3 φαίνεται μια τέτοια περίπτωση: Τα πακέτα από τον κόμβο A με αναγνωριστικό αριθμό νοητού κυκλώματος 3, μεταδίδονται στο B με αναγνωριστικό αριθμό 2, καθώς το 3 χρησιμοποιείται ήδη για την επικοινωνία D και V.

Στα υποδίκτυα αυτοδύναμων πακέτων δεν επιλέγεται διαδρομή που πρέπει να ακολουθήσουν όλα τα πακέτα μιας επικοινωνίας, ακόμα και αν χρησιμοποιούμε υπηρεσίες με σύνδεση. Κάθε πακέτο μπορεί να ακολουθήσει διαφορετική διαδρομή για να φτάσει στον προορισμό του. Στην περίπτωση αυτή, οι πίνακες των κόμβων περιέχουν στοιχεία που προσδιορίζουν σε ποια γραμμή (κόμβο) πρέπει να σταλεί κάθε εισερχόμενο πακέτο ώστε να φτάσει στον προορισμό του.

Τόσο στην περίπτωση που ένα δίκτυο χρησιμοποιεί αυτοδύναμα πακέτα, όσο και στη περίπτωση που χρησιμοποιεί νοητά κυκλώματα, μπορούμε να έχουμε υπηρεσίες με σύνδεση και υπηρεσίες χωρίς σύνδεση.

7.2 Τεχνολογία TCP/IP

7.2.1 Εισαγωγή στην Τεχνολογία TCP/IP

Αν και στις μέρες μας ο όρος TCP/IP χρησιμοποιείται για να περιγράψει πολλές διαφορετικές έννοιες, η ερμηνεία που έχει επικρατήσει περισσότερο αναφέρεται σε ένα πρωτόκολλο επικοινωνίας για μεταφορά δεδομένων.

Σημείωση κατανόησης: Πρωτόκολλο γενικά στις επικοινωνίες ονομάζουμε ένα σύνολο κανόνων οι οποίοι ορίζουν μια γλώσσα επικοινωνίας. Σκοπός του πρωτοκόλλου είναι να δίνεται η δυνατότητα επικοινωνίας μεταξύ συσκευών διαφορετικού τύπου και κατασκευαστών μεταξύ τους. Για παράδειγμα, θα μπορούν να επικοινωνήσουν μεταξύ τους υπολογιστές με διαφορετικά λειτουργικά (π.χ. Windows και UNIX) ή ακόμα και διαφορετικές συσκευές (υπολογιστής με κινητό τηλέφωνο).

Το TCP/IP σημαίνει *Transmission Control Protocol / Internet Protocol* και θα μπορούσε να θεωρηθεί ότι πρόκειται για συνδυασμό αυτών των δύο πρωτοκόλλων. Στην πραγματικότητα ωστόσο, το TCP και το IP είναι δύο χωριστά πρωτόκολλα (χρησιμοποιούνται όμως πάρα πολύ συχνά σε συνδυασμό όπως θα δούμε, καθώς το ένα χρειάζεται για να μεταφέρει τα δεδομένα που δημιουργεί το άλλο).

Ακόμα το TCP/IP αποτελεί στην πραγματικότητα μια **τεχνολογία επικοινωνίας** η οποία περιλαμβάνει και πλήθος άλλων πρωτοκόλλων που δεν περιέχονται στο όνομα του.

Σημείωση κατανόησης: Μπορεί να έχετε ακούσει μερικά από αυτά: Πρόκειται για πρωτόκολλα όπως το FTP (File Transfer Protocol, πρωτόκολλο μεταφοράς αρχείων), SMTP (Simple Mail Transfer Protocol, απλό πρωτόκολλο μεταφοράς ταχυδρομείου) κλπ. Θα εξετάσουμε κάποια από αυτά σε επόμενες ενότητες.

Το όνομα TCP/IP έχει επικρατήσει επειδή πρόκειται για τα δύο πιο γνωστά πρωτόκολλα της ομάδας. Η ελληνική απόδοση των όρων είναι *Πρωτόκολλο Ελέγχου Μετάδοσης / Πρωτόκολλο Διαδικτύου*. Η ανάγκη για τη δημιουργία του TCP/IP προέκυψε από το γεγονός ότι πριν από αυτό, συσκευές διαφορετικών κατασκευαστών ή με διαφορετικά λειτουργικά δεν μπορούσαν (εύκολα) να επικοινωνήσουν μεταξύ τους. Η επικράτηση του TCP/IP οφείλεται στους παρακάτω λόγους:

- Είναι πρωτόκολλο ανοικτό και διαθέσιμο σε όλους
- Υπήρχε ανάγκη για ένα μόνο κοινό πρότυπο

Το πρωτόκολλο TCP/IP έχει σήμερα καθολική αναγνώριση και λειτουργεί με τον ίδιο τρόπο στις συσκευές όλων των κατασκευαστών, εξασφαλίζοντας έτσι εύκολη επικοινωνία μεταξύ διαφορετικών υπολογιστικών συστημάτων. Μάλιστα όταν χρησιμοποιείται TCP/IP, δεν χρειάζεται καμία διαδικασία μετατροπής δεδομένων για τη μεταφορά από ένα σύστημα σε ένα άλλο (ακόμα και αν αυτά είναι διαφορετικών κατασκευαστών, αποτελούνται από διαφορετικό υλικό (hardware) ή χρησιμοποιούν διαφορετικά λειτουργικά συστήματα).

Σημείωση: Όταν χρησιμοποιούμε τον όρο TCP/IP θα εννοούμε από εδώ και μπρος μόνο το πρωτόκολλο TCP και το πρωτόκολλο IP. Όταν θέλουμε να αναφερθούμε σε όλη την οικογένεια πρωτοκόλλων TCP/IP θα τα αναφέρουμε ως **πρωτόκολλα TCP/IP** ή **τεχνολογία TCP/IP** ή **τεχνολογία Διαδικτύου (Internet)**.

Τα δίκτυα που χρησιμοποιούν τα πρωτόκολλα TCP/IP, αναφέρονται και ως διαδίκτυα TCP/IP (TCP/IP internets). Δεν θα πρέπει ωστόσο να μπερδεύουμε την έννοια των TCP/IP διαδικτύων με το **Παγκόσμιο Διαδίκτυο (Internet)**.

Παρατηρήστε ότι όταν αναφερόμαστε στο Παγκόσμιο Διαδίκτυο γράφουμε τη λέξη Internet με κεφαλαίο “I” ενώ για ένα δικό μας διαδίκτυο TCP/IP, χρησιμοποιούμε τη λέξη internet με μικρό γράμμα.

Ένα διαδίκτυο TCP/IP μπορεί να είναι ένα οποιοδήποτε δίκτυο βασίζεται στην τεχνολογία TCP/IP. Το Διαδίκτυο (Internet) όμως είναι το μεγαλύτερο παγκόσμιο δίκτυο υπολογιστών το οποίο εκτείνεται σε όλες τις ηπείρους και συνδέει μεταξύ τους εκατομμύρια υπολογιστών. Η τεχνολογία του βασίζεται φυσικά στα πρωτόκολλα TCP/IP (στην πραγματικότητα δημιουργείται ενώνοντας μεταξύ τους πολλά μικρότερα δίκτυα υπολογιστών).

Είναι επίσης δυνατόν να σχεδιάσουμε το εσωτερικό (τοπικό) δίκτυο μιας εταιρίας ώστε να λειτουργεί με παρόμοιο τρόπο με το Internet. Θα μπορούσαμε π.χ. να δημιουργήσουμε τις εφαρμογές της εταιρίας μας με τέτοιο τρόπο ώστε ο χειρισμός τους να γίνεται μέσω ιστοσελίδων Παγκόσμιου Ιστού (World Wide Web, WWW). Ένα τέτοιο ιδιωτικό δίκτυο που μοιάζει στη λειτουργία του με το Internet, ονομάζεται εσωτερικό ιδιωτικό δίκτυο τεχνολογίας TCP ή *intranet*. Θα το ακούσετε ακόμα και με τον όρο *ενδοδίκτυο*.

Ιστορικό Σημείωμα: Οι βάσεις του Διαδικτύου τέθηκαν στις αρχές της δεκαετίας του 1960 από την Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων του Υπουργείου Αμύνης των ΗΠΑ (ARPA, Advanced Research Projects Agency). Η υπηρεσία αυτή μετονομάσθηκε αργότερα σε DARPA (Defense Advanced Research Projects Agency). Στα μέσα της δεκαετίας του 1960, υπήρχε ήδη μεγάλη εξάπλωση των υπολογιστών στις στρατιωτικές επικοινωνίες, αλλά και ένα μεγάλο πρόβλημα: Οι υπολογιστές αυτοί προέρχονταν από διαφορετικούς κατασκευαστές και δεν μπορούσαν να συνεργαστούν μεταξύ τους. Οι κατασκευαστές έντεχνα φρόντιζαν να φτιάχνουν πρωτόκολλα με τα οποία μπορούσαν να επικοινωνήσουν μόνο τα δικά τους προϊόντα μεταξύ τους. Έτσι ο στρατός είχε ετερογενή δίκτυα (υπολογιστές διάφορων κατασκευαστών) τα οποία όμως δεν μπορούσαν να επικοινωνήσουν μεταξύ τους.

Για την αντιμετώπιση αυτών των προβλημάτων, αλλά και με τη σκέψη ότι σε περίπτωση πολέμου θα έπρεπε να υπάρχει κάποιο σύστημα τηλεπικοινωνιών το οποίο να λειτουργεί ακόμα και αν έχει καταστραφεί μεγάλο μέρος των γραμμών επικοινωνίας, δημιουργήθηκε ένα δίκτυο βασισμένο στην τεχνική μεταγωγής πακέτων. Η βασική υπόθεση (παραδοχή) για τη σχεδίαση και δημιουργία του ήταν ότι οι συνδέσεις μεταξύ των πόλεων θα πρέπει να θεωρούνται εντελώς αναξιόπιστες. Το αρχικό αυτό δίκτυο ονομάστηκε ARPANET και αποτελούνταν από μισθωμένες γραμμές που συνδέονταν σε κόμβους μεταγωγής.

Το ARPANET άρχισε να λειτουργεί επίσημα το 1971, και οι πρώτες υπηρεσίες που παρείχε ήταν η μεταφορά αρχείων και η απομακρυσμένη σύνδεση (Σημείωση: Πρόκειται για τις υπηρεσίες FTP και telnet). Αργότερα προστέθηκε και η υπηρεσία ηλεκτρονικού ταχυδρομείου.

Καθώς οι ανάγκες επικοινωνίας του ARPANET αυξάνονταν, χρησιμοποιήθηκαν το 1974 τα πρωτόκολλα TCP/IP και η αρχιτεκτονική των δρομολογητών για την εξυ-

πηρέτηση τους. Το νέο πρωτόκολλο ήταν ανεξάρτητο από το υλικό και το λογισμικό χαμηλότερου επιπέδου: μπορούσε να λειτουργήσει με τον ίδιο τρόπο σε συσκευές οποιουδήποτε κατασκευαστή και καταργούσε τους περιορισμούς επικοινωνίας που επέβαλλαν οι διάφοροι κατασκευαστές. Λόγω και αυτής της καινοτομίας του, το νέο πρωτόκολλο προτάθηκε και για παγκόσμια διασύνδεση (μια ιδέα αρκετά πρωτοποριακή για την εποχή).

Το 1982 το TCP/IP καθιερώθηκε ως το βασικό πρωτόκολλο του δικτύου που αναπτύσσονταν και το οποίο συνέδεε πλέον συστήματα σε όλη την ήπειρο. Υπολογίζεται ότι την πρώτη δεκαετία λειτουργίας του TCP/IP συνδέονταν στο ARPANET ένας νέος υπολογιστής κάθε είκοσι μέρες.

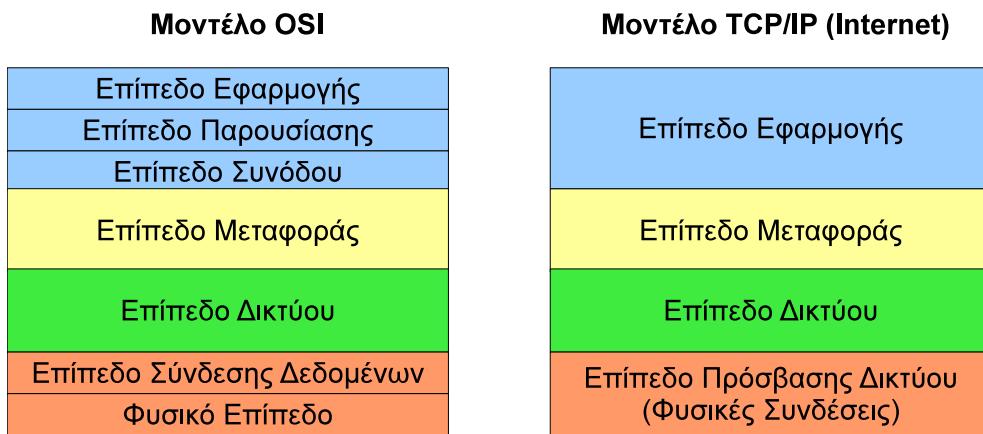
Με την εξέλιξη του ARPANET έγινε φανερό ότι το νέο δίκτυο θα μπορούσε να αξιοποιηθεί και από ερευνητές μη στρατιωτικών εφαρμογών. Δημιουργήθηκε έτσι το MILNET ως δίκτυο στρατιωτικών εφαρμογών ενώ το ARPANET παρέμεινε για ερευνητικές και άλλες δραστηριότητες που δεν σχετίζονταν με το στρατό. Με την πάροδο του χρόνου, το ARPANET ξεπέρασε τα όρια του στρατιωτικού δικτύου και άρχισαν να προστίθενται σε αυτό τα δίκτυα πανεπιστημίων, κοινωφελών οργανισμών καθώς και εταιριών. Το δίκτυο αυτό εξελίχθηκε στο γνωστό μας σήμερα Internet.

7.2.2 Σχέση OSI και TCP/IP

Το TCP/IP και το OSI ουσιαστικά αναπτύχθηκαν ταυτόχρονα. Δεν υπάρχει στην πραγματικότητα σύγκρουση μεταξύ των δύο προτύπων, ωστόσο υπάρχουν κάποιες ουσιαστικές διαφορές.

Στο μάθημα της Β τάξης μάθαμε ότι το πρότυπο OSI χωρίζει τη λειτουργία του δικτύου σε επίπεδα. Το TCP/IP χρησιμοποιεί επίσης το ίδιο μοντέλο. Μια από τις βασικές διαφορές των δύο είναι ότι το OSI χρησιμοποιεί επτά επίπεδα ενώ το TCP/IP μόνο τέσσερα. Αυτό σημαίνει ότι δεν υπάρχει αντιστοιχία των επιπέδων ένα – προς – ένα. Όπως μπορείτε να δείτε στο σχήμα 7.4, πλήρης αντιστοιχία υπάρχει στα επίπεδα μεταφοράς και δικτύου. Τα επίπεδα εφαρμογής, παρουσίασης και συνόδου του OSI συνδυάζονται στο επίπεδο εφαρμογής του TCP/IP, ενώ και τα επίπεδα σύνδεσης δεδομένων και φυσικό συνδυάζονται στο επίπεδο πρόσβασης δικτύου. Ο συνδυασμός των επιπέδων σύνδεσης δεδομένων και φυσικού στο TCP/IP είναι απαραίτητος, καθώς βασική αρχή της τεχνολογίας TCP/IP είναι η υλοποίηση πρωτοκόλλου χωρίς σύνδεση.

Στην πραγματικότητα ωστόσο, ακόμα και στο μοντέλο OSI το επίπεδο σύνδεσης δεδομένων και το φυσικό επίπεδο συνδυάζονται σε ένα έξυπνο ελεγκτή (κάρτα) δικτύου.



Σχήμα 7.4: Μοντέλα OSI και TCP/IP

Στο σχήμα 7.5 παρουσιάζονται τα επίπεδα του TCP/IP σε σχέση με τα επίπεδα του OSI ενώ παρουσιάζονται και τα πρωτόκολλα που χρησιμοποιούνται για την υλοποίηση κάθε επίπεδου. Πάνω από τα πρωτόκολλα TCP/IP, βρίσκονται τα πρωτόκολλα που χρησιμοποιούνται στο επίπεδο εφαρμογής. Τα πρωτόκολλα αυτά έχουν δημιουργηθεί με τέτοιο τρόπο ώστε να χρησιμοποιούν για την επικοινωνία είτε το *Πρωτόκολλο Ελέγχου Μετάδοσης TCP* είτε το *Πρωτόκολλο Αυτοδύναμων Πακέτων Χρήστη, User Datagram Protocol, UDP* στο επίπεδο μεταφοράς. Στο επίπεδο δικτύου χρησιμοποιείται το *Πρωτόκολλο Διαδικτύου, IP* καθώς και το *Πρωτόκολλο Μηνύματος Ελέγχου Διαδικτύου, Internet Control Message Protocol, ICMP*. Καθώς τα πρωτόκολλα αυτά υλοποιούνται με λογισμικό (προγράμματα) το σχήμα δείχνει και τη σχέση των προγραμμάτων μεταξύ τους.

	Εφαρμογές	Εφαρμογές
Επίπεδο Εφαρμογής	Telnet, FTP, SMTP	TFTP
Επίπεδο Μεταφοράς	TCP	UDP
Επίπεδο Δικτύου	IP/ICMP	

Σχήμα 7.5: Στοίβα Πρωτοκόλλων TCP/IP

Επεξήγηση των Πρωτοκόλλων του σχήματος 7.5: Τα πρωτόκολλα εφαρμογής που φαίνονται στην αριστερή στήλη χρησιμοποιούν το πρωτόκολλο TCP στο επίπεδο μεταφοράς. Τα πρωτόκολλα εφαρμογής της δεξιάς στήλης χρησιμοποιούν το πρωτόκολλο UDP στο επίπεδο μεταφοράς. Και στις δύο περιπτώσεις, στο επίπεδο δικτύου

χρησιμοποιούνται τα πρωτόκολλα IP και ICMP. Τα πρωτόκολλα που αναφέρονται στο σχήμα είναι:

- **Telnet:** Telecommunications Network (Σημ: Λάθος του βιβλίου – στην πραγματικότητα σημαίνει Teletype Network) το οποίο χρησιμεύει για την απομακρυσμένη σύνδεση και χειρισμό (σε περιβάλλον γραμμής εντολών) ενός υπολογιστή από ένα άλλο. Στις μέρες μας έχει αντικατασταθεί από το πολύ πιο ασφαλές SSH (Secure Shell).
- **FTP:** File Transfer Protocol ή Πρωτόκολλο Μεταφοράς Αρχείων το οποίο χρησιμοποιείται για τη μεταφορά αρχείων από ένα υπολογιστή σε ένα άλλο. Το χρησιμοποιούμε και σήμερα για να “κατεβάσουμε” αρχεία από τους λεγόμενους εξυπηρετητές FTP.
- **SMTP:** Simple Mail Transfer Protocol ή Απλό Πρωτόκολλο Μεταφοράς Ταχυδρομείου. Πρόκειται για το πρωτόκολλο που χρησιμοποιούν μεταξύ τους οι εξυπηρετητές ηλεκτρονικού ταχυδρομείου (το γνωστό μας email) στο Internet για να μεταφέρουν τα μηνύματα που στέλνουμε μέχρι τον παραλήπτη.
- **TFTP:** Πρόκειται για το Απλό Πρωτόκολλο Μεταφοράς Αρχείων (Trivial FTP) το οποίο χρησιμοποιείται για μεταφορά αρχείων όπως και το FTP αλλά έχει πολύ μικρότερες δυνατότητες και πολυπλοκότητα και χρησιμοποιείται σε ειδικές περιπτώσεις όπου δεν μπορεί (ή δεν χρειάζεται) να χρησιμοποιηθεί το κανονικό FTP.

Θα δούμε τώρα τις λειτουργίες που εκτελούν τα επίπεδα πρόσβασης δικτύου και μεταφοράς.

7.2.2.1 Επίπεδο Πρόσβασης Δικτύου

Το επίπεδο πρόσβασης δικτύου παρέχει την πρόσβαση στο φυσικό μέσο στο οποίο η πληροφορία μεταδίδεται με την μορφή πακέτων. Το επίπεδο πρόσβασης δικτύου αντιπροσωπεύει το χαμηλότερο επίπεδο λειτουργικότητας που απαιτείται από ένα δίκτυο και περιλαμβάνει όλα τα στοιχεία της φυσικής σύνδεσης: καλώδια, κάρτες δικτύου, πρωτόκολλα πρόσβασης τοπικών δικτύων. Όπως κάθε επίπεδο στο TCP/IP (αλλά και στο OSI), το επίπεδο αυτό παρέχει τις υπηρεσίες του στο αμέσως ανώτερο επίπεδο, το επίπεδο δικτύου. Στην τεχνολογία TCP/IP δεν υπάρχουν προδιαγραφές για τα χαμηλότερα επίπεδα του επιπέδου δικτύου και έτσι μπορούν να χρησιμοποιούνται εντελώς διαφορετικές τεχνολογίες. Αυτό πρακτικά σημαίνει ότι το TCP/IP μπορεί να χρησιμοποιηθεί σε διαφορετικά φυσικά μέσα και τεχνολογίες (Ethernet, Token ring κλπ).

7.2.2.2 Επίπεδο Δικτύου

Το επίπεδο αυτό είναι υπεύθυνο για τη μετάδοση στο φυσικό δίκτυο των πακέτων που δημιουργούνται από τα πρωτόκολλα TCP και UDP που βρίσκονται στο αμέσως ανώτερο επίπεδο (Μεταφοράς). Το βασικό πρωτόκολλο που χρησιμοποιείται σε αυτό το επίπεδο είναι το IP ή πρωτόκολλο Διαδικτύου και είναι αυτό που μας εξασφαλίζει την παγκόσμια διασυνδεσμότητα. Το πρωτόκολλο IP είναι υπεύθυνο για την παροχή λογικών διευθύνσεων (των γνωστών μας διευθύνσεων IP) στα σημεία διεπαφής του με το φυσικό δίκτυο (σε κάθε δηλ. συσκευή του δικτύου που διαθέτει δική της διεύθυνση). Είναι επίσης υπεύθυνο για την αντιστοίχηση των λογικών (IP) διευθύνσεων με τις φυσικές διευθύνσεις.

Σημείωση κατανόησης: Τι είναι η φυσική διεύθυνση; Κάθε συσκευή που έχει δυνατότητα να διαθέτει μια διεύθυνση IP (π.χ. μια κάρτα δικτύου σε ένα υπολογιστή) έχει επίσης και ένα μοναδικό χαρακτηριστικό αναγνωριστικό αριθμό, την φυσική διεύθυνση ή διεύθυνση MAC η οποία δίνεται από τον κατασκευαστή της και είναι σταθερή. Για τις φυσικές διευθύνσεις στο Ethernet, θα αναφερθούμε σε επόμενη ενότητα.

Οι φυσικές διευθύνσεις παρέχονται από το επίπεδο πρόσβασης δικτύου (φυσικό επίπεδο) ή από το υπο-επίπεδο ελέγχου προσπέλασης μέσου MAC (Media Access Control) του OSI. Το πρωτόκολλο IP παρέχει λογικές διευθύνσεις στα σημεία διεπαφής του με το φυσικό δίκτυο ενώ υπάρχει και αντιστοίχηση των λογικών διευθύνσεων με φυσικές. Για τις εργασίες αυτές χρησιμοποιούνται τα πρωτόκολλα ARP (Address Resolution Protocol) και RARP (Reverse Address Resolution Protocol).

ARP: Πρωτόκολλο Μετατροπής Διευθύνσεων

RARP: Πρωτόκολλο Ανάστροφης Μετατροπής Διευθύνσεων

Στο επίπεδο δικτύου λειτουργεί επίσης και το πρωτόκολλο ICMP, *Internet Control Message Protocol* ή Πρωτόκολλο Ελέγχου Μεταφοράς Μηνυμάτων. Αυτό χρησιμοποιείται για να αναφέρει προβλήματα και ασυνήθιστες καταστάσεις που σχετίζονται με το πρωτόκολλο IP. Συνήθως δημιουργεί και μεταφέρει μηνύματα που έχουν να κάνουν με την κατάσταση λειτουργίας των συσκευών του δικτύου. Δημιουργεί επίσης και μεταφέρει μηνύματα που σχετίζονται με την ίδια τη λειτουργία του TCP/IP και όχι από κάποια εφαρμογή που εκτελεί ο χρήστης. Για παράδειγμα όταν κάποιος προσπαθεί να συνδεθεί σε ένα υπολογιστή ο οποίος δεν είναι διαθέσιμος τη δεδομένη στιγμή (π.χ. γιατί δεν είναι ενεργός ή γιατί υπάρχει πρόβλημα στο συγκεκριμένο τμήμα του δικτύου) θα λάβει ένα μήνυμα ότι ο υπολογιστής είναι “απρόσι-

τος”.

Παράδειγμα από το Εργαστήριο μας

```
$ ping 10.14.28.11
Pinging 10.14.28.11 with 32 bytes of data:
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Ping statistics for 10.14.28.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Αντίθετα, μια επικοινωνία που λειτουργεί θα έχει το παρακάτω αποτέλεσμα:

```
$ ping www.freebsdgr.org
PING www.freebsdgr.org (94.71.112.109): 56 data bytes
64 bytes from 94.71.112.109: icmp_seq=0 ttl=62 time=21.849 ms
64 bytes from 94.71.112.109: icmp_seq=1 ttl=62 time=21.325 ms
64 bytes from 94.71.112.109: icmp_seq=2 ttl=62 time=20.689 ms
```

7.2.2.3 Επίπεδο Μεταφοράς

Το επίπεδο μεταφοράς είναι υπεύθυνο για την υλοποίηση των συνδέσεων μεταξύ των υπολογιστών ενός δικτύου. Το βασικό πρωτόκολλο εδώ είναι το TCP (πρωτόκολλο με σύνδεση) ενώ μπορεί να χρησιμοποιηθεί και το UDP (πρωτόκολλο χωρίς σύνδεση). Το TCP είναι υπεύθυνο για την αποκατάσταση αξιόπιστων ταυτόχρονων συνδέσεων διπλής κατεύθυνσης.

Η έννοια του αξιόπιστου είναι ότι το TCP αναλαμβάνει να διορθώσει τα λάθη που τυχόν παρουσιάζονται στη μετάδοση (π.χ. μεταδίδοντας ξανά ένα πακέτο που χάθηκε ή αλλοιώθηκε). Το TCP παρέχει τις υπηρεσίες του στο αμέσως ανώτερο επίπεδο (Εφαρμογής). Καθώς θεωρείται ότι οι συνδέσεις που παρέχει είναι αξιόπιστες, τα προγράμματα στο επίπεδο εφαρμογής δεν κάνουν κανένα έλεγχο για ορθότητα των δεδομένων που προέρχονται από το TCP.

Η έννοια του ταυτόχρονου είναι ότι ένας υπολογιστής μπορεί σε μια δεδομένη στιγμή να διατηρεί πλήθος διαφορετικών συνδέσεων TCP οι οποίες να λειτουργούν όλες μαζί αλλά καμιά να μην επηρεάζει την άλλη.

Επικοινωνία διπλής κατεύθυνσης σημαίνει ότι μέσω μιας σύνδεσης μπορούν ταυτόχρονα να μεταδίδονται και να λαμβάνονται δεδομένα.

Το πρωτόκολλο αυτοδύναμων πακέτων UDP είναι ένα πρωτόκολλο χωρίς σύνδεση. Δεν είναι ιδιαίτερα αξιόπιστο, αλλά επειδή είναι λιγότερο πολύπλοκο χρησιμοποιείται σε περιπτώσεις που η αξιοπιστία δεν είναι κρίσιμη και δεν είναι η επιθυμητή η χρήση του TCP.

Παραδείγματα κατανόησης UDP: Μια μετάδοση ραδιοφώνου μέσω Internet μπορεί να χρησιμοποιεί μετάδοση με πακέτα UDP. Αν κάποια πακέτα χαθούν ή αλλοιωθούν θα έχει σαν αποτέλεσμα την προσωρινή διακοπή ή παραμόρφωση του ήχου. Ωστόσο στη συγκεκριμένη εφαρμογή αυτό δεν είναι κρίσιμο. Από την άλλη δεν θα μπορούσαμε να κατεβάσουμε αρχεία μέσω UDP χωρίς έξτρα έλεγχο λαθών (ο οποίος θα πρέπει προφανώς να γίνει πλέον στο επίπεδο εφαρμογής). Διαφορετικά τα περιεχόμενα τους θα μπορούσαν να είναι κατεστραμμένα, χωρίς να μπορούμε να το αντιληφθούμε άμεσα.

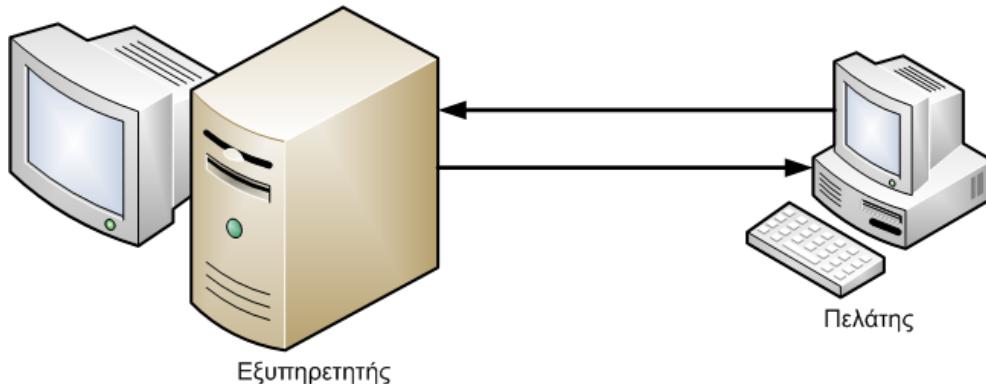
7.2.2.4 Επίπεδο Εφαρμογής

Το επίπεδο εφαρμογής παρέχει τις εφαρμογές (προγράμματα) που χρησιμοποιούν τα πρωτόκολλα του επιπέδου μεταφοράς. Παραδείγματα δώσαμε στην προηγούμενη ενότητα (μεταφορά αρχείων, ηλεκτρονικό ταχυδρομείο, απομακρυσμένη πρόσβαση). Το επίπεδο εφαρμογής είναι και το σημείο που ο τελικός χρήστης έρχεται σε επαφή με την στοίβα πρωτοκόλλων της τεχνολογίας TCP/IP.

Στο σχήμα 7.6 φαίνεται το βασικό μοντέλο επικοινωνίας που χρησιμοποιείται στις περισσότερες εφαρμογές TCP/IP και το οποίο δεν είναι άλλο από το μοντέλο πελάτη – εξυπηρετητή. Ο εξυπηρετητής είναι μια διεργασία (πρόγραμμα) η οποία εκτελείται σε ένα υπολογιστή (γνωστός ως server) και ελέγχει τις εισερχόμενες αιτήσεις πελατών για να δει αν κάποια απευθύνεται προς αυτήν. Αν υπάρχει κάποια τέτοια αίτηση, ο εξυπηρετητής αναλαμβάνει να βρει τα δεδομένα που ζητούνται και να τα στείλει στον πελάτη.

Ο πελάτης είναι πάλι αντίστοιχα το πρόγραμμα που χρησιμοποιείται (συνήθως από τον τελικό χρήστη) για να ζητήσει τα δεδομένα από τον εξυπηρετητή. Ο πελάτης στέλνει την αντίστοιχη αίτηση και περιμένει να λάβει τα δεδομένα που ζήτησε. Με το τέλος της εξυπηρέτησης ενός πελάτη, ο εξυπηρετητής επιστρέφει ξανά σε κατάσταση αναμονής, περιμένοντας νέα αίτηση (Σημείωση: Τυπικά ένας εξυπηρετητής είναι σε θέση να εξυπηρετήσει ταυτόχρονα περισσότερες από μια αιτήσεις).

Παράδειγμα Πελάτη – Εξυπηρετητή: Όταν χρησιμοποιείτε το Firefox για να συνδεθείτε σε μια ιστοσελίδα, το πρόγραμμα αυτό λειτουργεί ως πελάτης. Ζητάει τα



Σχήμα 7.6: Πρότυπο Πελάτη – Εξυπηρετητή

δεδομένα της ιστοσελίδας από τον αντίστοιχο εξυπηρετητή ιστοσελίδων (*Web Server*) ο οποίος εκτελείται στο μηχάνημα που προσπαθείτε να συνδεθείτε.

Εργαστηριακή άσκηση κατανόησης: Εκτελέστε σε ένα μηχάνημα:

- Linux: netstat -npl | more
- FreeBSD: sockstat -4l | more

για να δείτε ποιοι εξυπηρετητές εκτελούνται και αναμένουν αιτήσεις από πελάτες.

Ξεκινήστε να κατεβάζετε με FTP ένα αρχείο (π.χ. από την τοποθεσία <ftp://ftp.otenet.gr>) και χρησιμοποιήστε τις εντολές:

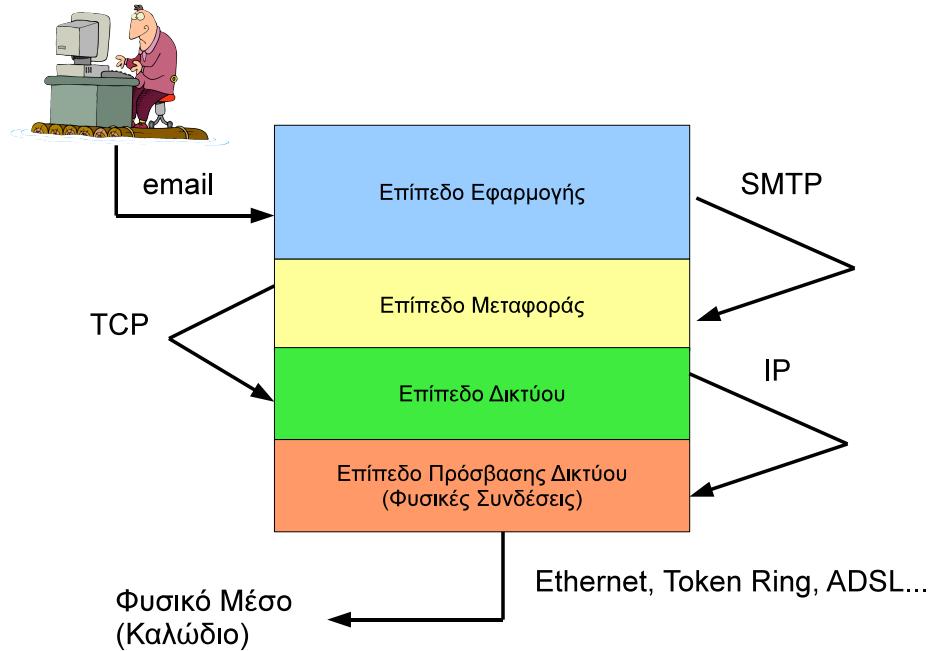
- Linux: lsof -Pnl +M -i4 | more
- FreeBSD: sockstat -4L | more

για να δείτε τη σύνδεση που έχει πραγματοποιηθεί μεταξύ του μηχανήματος σας και του απομακρυσμένου εξυπηρετητή. Αντίστοιχες εντολές υπάρχουν και για Windows, αλλά σας αφήνω να τις βρείτε μόνοι σας!

7.2.3 Βασικές Αρχές Επικοινωνίας στην Τεχνολογία TCP/IP και στο Διαδίκτυο

Για να αντιληφθούμε την επικοινωνία σύμφωνα με το μοντέλο TCP/IP, αρκεί να κατανοήσουμε το σχήμα 7.7.

Όπως βλέπουμε, στο υψηλότερο επίπεδο (εφαρμογών) του TCP/IP βρίσκονται οι εφαρμογές οι οποίες χρησιμοποιούν τα επίπεδα που βρίσκονται κάτω από αυτό,



Σχήμα 7.7: Επικοινωνία Επιπέδων TCP/IP

δηλ. τα μεταφοράς, δικτύου και πρόσβασης δικτύου. Το επίπεδο εφαρμογών του δικού μας υπολογιστή μπορεί να θεωρηθεί ότι επικοινωνεί με το αντίστοιχο επίπεδο εφαρμογών του απομακρυσμένου προκειμένου να ολοκληρωθεί μια εργασία (για παράδειγμα η αποστολή ενός μηνύματος Ηλεκτρονικού Ταχυδρομείου με βάση το πρωτόκολλο SMTP το οποίο ανήκει στο επίπεδο εφαρμογής). Τα ενδιάμεσα επίπεδα προσαρμόζουν και μεταφέρουν τα δεδομένα που παράγονται από το επίπεδο εφαρμογής. Στο παράδειγμα μας χρησιμοποιούμε το πρωτόκολλο SMTP:

- Τα αρχικά δεδομένα παράγονται από την εφαρμογή του χρήστη και παραδίδονται στο πρωτόκολλο που εκτελείται στο επίπεδο εφαρμογής. Το SMTP προσθέτει τις εντολές και τα μηνύματα που απαιτούνται για να γίνει η επικοινωνία με τον απομακρυσμένο εξυπηρετητή SMTP (στο σχήμα 7.8 μπορείτε να δείτε μια συνομιλία μεταξύ δύο εξυπηρετητών SMTP).
- Τα δεδομένα από το επίπεδο εφαρμογής παραδίδονται στο επίπεδο μεταφοράς στο οποίο μετατρέπονται σε πακέτα TCP ή UDP ανάλογα με την εφαρμογή. Για το SMTP χρειαζόμαστε επικοινωνία TCP.
- Τα πακέτα από το επίπεδο μεταφοράς εισέρχονται στο επίπεδο δικτύου όπου προστίθενται οι πληροφορίες διεύθυνσης IP που απαιτούνται για τη δρομο-

λόγηση.

- Τέλος, μεταφέρονται στο επίπεδο πρόσβασης δικτύου όπου προσαρμόζονται στο πρωτόκολλο του φυσικού μέσου (Ethernet, ADSL, token ring κλπ) και παραδίδονται μέσα από τη δικτυακή συσκευή (π.χ. την κάρτα δικτύου) στο φυσικό μέσο.

```
Trying 10.14.28.10...
Connected to aquarius64.lab1.local.
Escape character is '^].
220 aquarius64.lab1.local ESMTP Sendmail 8.14.3/8.14.3; Wed, 21 Oct 2009 01:09:4
8 +0300 (EEST)
he1o atomic.chania-lug.gr
250 aquarius64.lab1.local Hello aquarius64.lab1.local [10.14.28.10], pleased to
meet you
MAIL FROM: manolis@chania-lug.gr
250 2.1.0 manolis@chania-lug.gr... Sender ok
RCPT TO: sonic@lab1.local
250 2.1.5 sonic@lab1.local... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Hello, this is a test message!
.
250 2.0.0 n9KM9mDF039141 Message accepted for delivery
quit
221 2.0.0 aquarius64.lab1.local closing connection
Connection closed by foreign host.
```

Σχήμα 7.8: Επικοινωνία Εξυπηρετητών SMTP

Προφανώς, στην μεριά του παραλήπτη ακολουθείται η αντίστροφη διαδικασία. Τα δεδομένα εισέρχονται από το φυσικό μέσο (επίπεδο πρόσβασης δικτύου) και ανεβαίνουν τα επίπεδα προς τα πάνω, όπου διαδοχικά ανασυνθέτονται μέχρι να φτάσουν στο επίπεδο εφαρμογής και να παραληφθούν από το πρωτόκολλο SMTP. Το πρωτόκολλο SMTP θεωρεί ότι η μετάδοση είναι αξιόπιστη (μη ξεχνάμε ότι γίνεται μέσω TCP, το οποίο είναι αξιόπιστο πρωτόκολλο). Ο έλεγχος λαθών (π.χ. πακέτα που χάθηκαν ή αλλοιώθηκαν) γίνεται στο επίπεδο μεταφοράς από το πρωτόκολλο TCP.

Επισήμανση: Οι εφαρμογές που χρησιμοποιούν τα πρωτόκολλα TCP/IP χρησιμοποιούν γενικά τέσσερα επίπεδα:

- *Πρωτόκολλο εφαρμογής:* Π.χ. SMTP, FTP, HTTP. Ανάλογα με το πρωτόκολλο εφαρμογής θα επιλεχθεί και το κατάλληλο πρωτόκολλο μεταφοράς (TCP ή UDP).
- *Πρωτόκολλο μεταφοράς:* TCP ή UDP. Έχουμε ήδη πει τις διαφορές τους. Παρέχουν τις υπηρεσίες τους στα πρωτόκολλα εφαρμογών.
- *Πρωτόκολλο δικτύου:* Το IP που παρέχει τις υπηρεσίες για τη μεταφορά των πακέτων στον προορισμό τους.

- **Πρωτόκολλα πρόσβασης δικτύου (φυσικού μέσου):** Απαιτούνται για τη διαχείριση του φυσικού μέσου (π.χ. Ethernet).
-

Η τεχνολογία TCP/IP βασίζεται σε μοντέλο που θεωρεί ότι οι υπολογιστές συνδέονται μεταξύ τους διαμέσου ενός μεγάλου αριθμού δικτύων. Με λίγα λόγια, τα δεδομένα από τον υπολογιστή πηγής θα περάσουν από ένα αριθμό ενδιάμεσων μηχανημάτων μέχρι να φτάσουν στον υπολογισμό προορισμού. Τα δίκτυα αυτά συνδέονται μεταξύ τους με τη βοήθεια ειδικών μηχανημάτων που ονομάζονται δρομολογητές.

Σημείωση κατανόησης: Ο δρομολογητής μπορεί να είναι εξειδικευμένη συσκευή (π.χ. ο δρομολογητής του εργαστηρίου που δρομολογεί τα δεδομένα των μηχανημάτων μας προς το Internet) ή και κανονικός υπολογιστής ο οποίος εκτελεί αυτή τη διαδικασία με το κατάλληλο λογισμικό.

Η αποστολή των πακέτων πρέπει να γίνεται με τέτοιο τρόπο ώστε ο χρήστης να μην αντιλαμβάνεται την διαδικασία (πρέπει να είναι διάφανη). Έτσι ο χρήστης δεν χρειάζεται να γνωρίζει από ποια ενδιάμεσα μηχανήματα και δρομολογητές θα περάσουν τα πακέτα για να φτάσουν στον προορισμό τους. Το μόνο που χρειάζεται να γνωρίζει πρακτικά, είναι η διεύθυνση IP του παραλήπτη.

Συνήθως μας είναι πιο εύκολο να θυμόμαστε ονόματα παρά αριθμούς, για το σκοπό αυτό υπάρχει κατάλληλο λογισμικό και μια βάση δεδομένων με την οποία αντιστοιχίζονται τα ονόματα στις IP διεύθυνσεις τους (πρόκειται για την υπηρεσία DNS για την οποία θα αναφερθούμε σε επόμενο μάθημα). Χρησιμοποιώντας απλώς το όνομα, γίνεται η κατάλληλη αναζήτηση και η σύνδεση στην αντίστοιχη IP διεύθυνση.

Τα πρωτόκολλα TCP/IP έχουν δημιουργηθεί με βάση την τεχνολογία χωρίς σύνδεση. Τα πακέτα μεταδίδονται στο δίκτυο αυτόνομα, καθένα από αυτά μπορεί να ακολουθεί διαφορετική διαδρομή μέχρι να φτάσει στον προορισμό του.

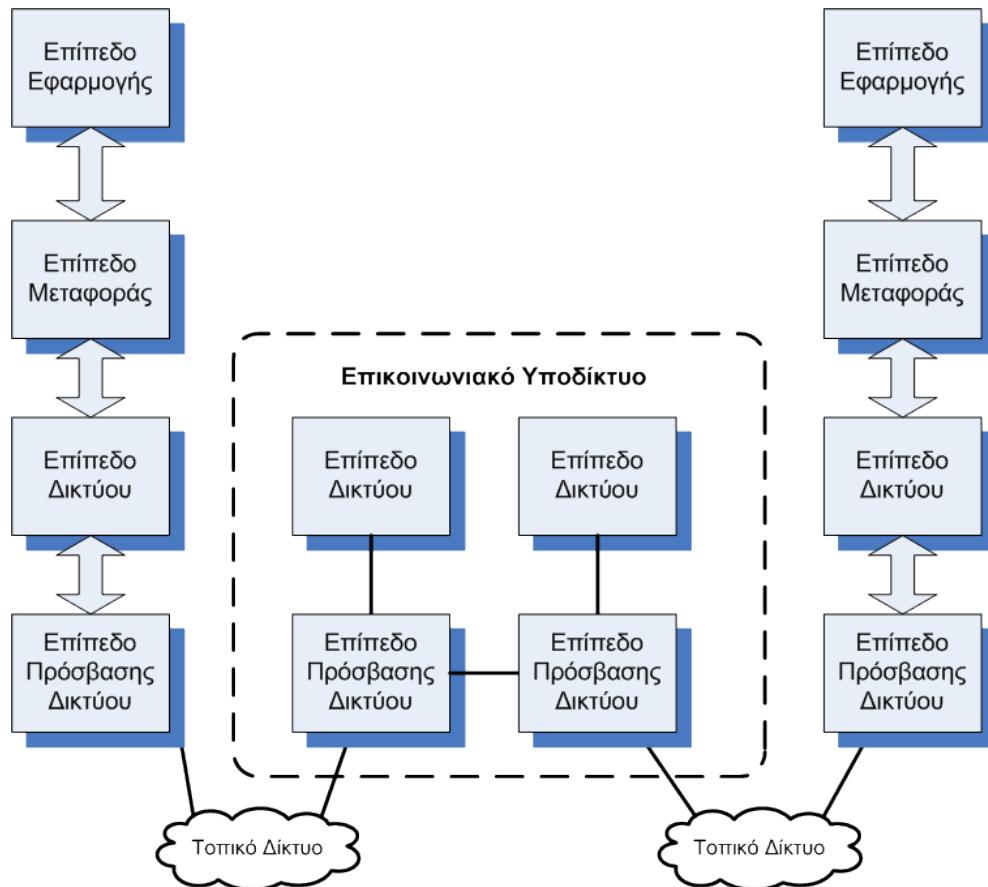
Παράδειγμα: Ας υποθέσουμε ότι θέλουμε να στείλουμε ένα αρχείο μεγέθους 15000 bytes (οκτάδων). Στις περισσότερες περιπτώσεις το μέσο του δικτύου δεν θα μας επιτρέψει να στείλουμε όλες αυτές τις πληροφορίες σε ένα πακέτο, γιατί είναι πολύ μεγάλο. Ας υποθέσουμε ότι αυτό το αρχείο θα σπάσει σε 30 πακέτα των 500 bytes. Καθένα από αυτά τα πακέτα θα σταλεί στον προορισμό του όπου και θα επανασυνδεθούν για να σχηματίσουν το αρχικό αρχείο των 15000 bytes.

Στη διάρκεια της μεταφοράς τους, το δίκτυο δεν γνωρίζει ότι τα πακέτα αυτά σχετίζονται μεταξύ τους (ότι είναι δηλ. μέρος της ίδιας μετάδοσης). Επίσης μπορεί κάποια

από αυτά να χαθούν, να αλλοιωθούν ή να φτάσουν με λάθος σειρά. Π.χ. το πακέτο 14 μπορεί να ακολουθήσει άλλη διαδρομή και να φτάσει πριν το πακέτο 13.

Σε κάθε περίπτωση όλα αυτά τα προβλήματα πρέπει να λυθούν πριν δημιουργηθεί ξανά το αρχείο στον προορισμό: Τα πακέτα που χάθηκαν πρέπει να σταλούν ξανά. Στον προορισμό πρέπει να μπουν ξανά στη σωστή σειρά. Όλες αυτές οι ενέργειες αποτελούν διεργασίες του πρωτοκόλλου TCP. Τίποτα από αυτά δεν γίνεται αντιληπτό από τον τελικό χρήστη.

Οι δρομολογητές που χρησιμοποιούνται στο Internet πρέπει να λειτουργούν μέχρι το επίπεδο δικτύου όπως φαίνεται στο σχήμα 7.9. Θα θυμάστε ότι και στο μοντέλο OSI λέγαμε ακριβώς το ίδιο, απλώς το OSI έχει ένα επιπλέον επίπεδο πριν το επίπεδο δικτύου (δείτε ξανά το σχήμα 7.1). Γιατί όμως συμβαίνει αυτό; Ο δρομολογητής όταν



Σχήμα 7.9: Επικοινωνία στο Διαδίκτυο

λαμβάνει κάποιο πακέτο μιας μετάδοσης πρέπει να αποφασίσει σε ποιον επόμενο

δρομολογητή θα το στείλει. Η διαδικασία αυτή επαναλαμβάνεται μέχρι το πακέτο να φτάσει στον προορισμό του. Για να το αποφασίσει όμως αυτό ο δρομολογητής θα πρέπει να κοιτάξει την διεύθυνση IP προορισμού. Γνωρίζουμε ότι οι διευθύνσεις IP προστίθενται στο επίπεδο δικτύου, άρα και για να τις διαβάσουμε από ένα πακέτο πρέπει να το “αποκωδικοποιήσουμε” μέχρι το επίπεδο δικτύου.

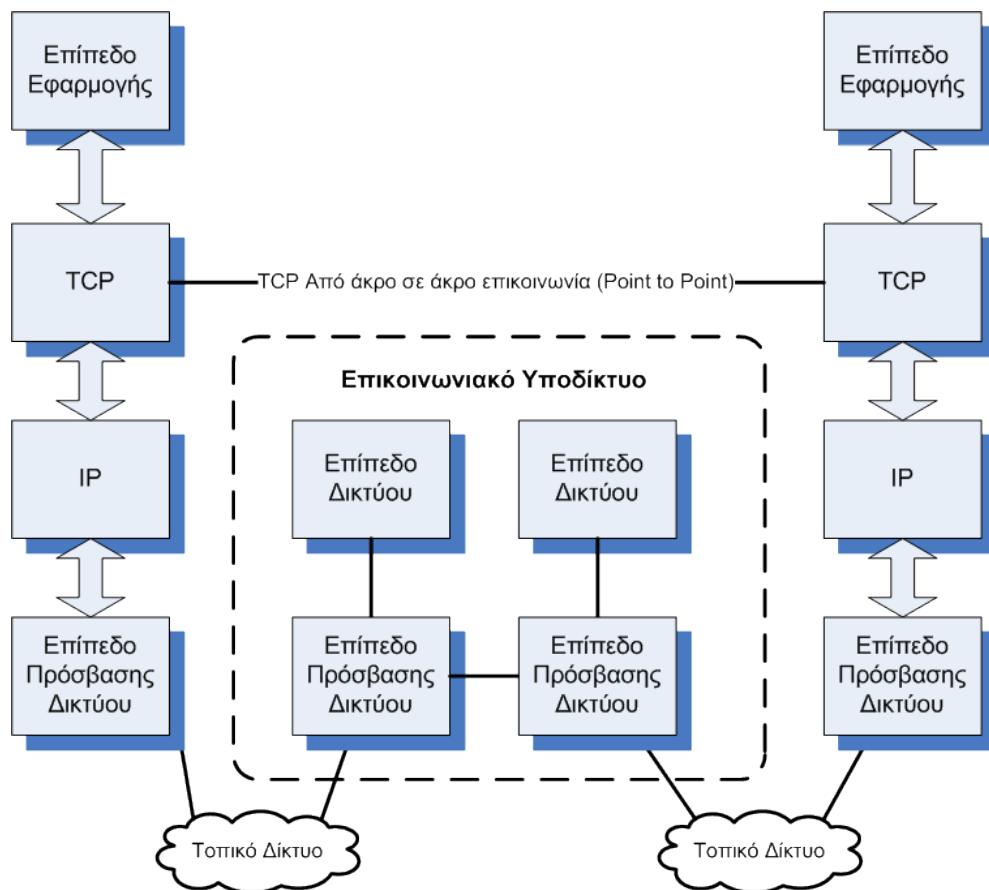
Συνοψίζοντας, ένα παράδειγμα αποστολής μεταξύ δύο υπολογιστών είναι το παρακάτω: Εστω ότι μια εφαρμογή στον υπολογιστή πηγής θέλει να επικοινωνήσει με την αντίστοιχη στον υπολογιστή προορισμού:

- Τα δεδομένα δημιουργούνται στο επίπεδο εφαρμογής του υπολογιστή αποστολής και κατεβαίνουν τα επίπεδα προς τα κάτω, σχηματίζοντας το πακέτο που πρόκειται τελικά να μεταδοθεί. Φτάνοντας στο επίπεδο πρόσβασης δικτύου, το πακέτο μεταβιβάζεται στο τοπικό δίκτυο του υπολογιστή αποστολής.
- Το πακέτο κατευθύνεται στο δρομολογητή του τοπικού δικτύου ο οποίος αναγνωρίζει ότι έχει προορισμό το Internet και το προωθεί (Ο τοπικός δρομολογητής είναι συνδεδεμένος με κάποιο δρομολογητή στο Διαδίκτυο. Για παράδειγμα, ο δικός μας δρομολογητής είναι συνδεδεμένος στο τοπικό μας δίκτυο και στην ADSL γραμμή που καταλήγει σε ένα δρομολογητή του Πανελλήνιου Σχολικού Δικτύου).
- Το πακέτο κινείται από δρομολογητή σε δρομολογητή μέσω του επικοινωνιακού υποδικτύου (των ενδιάμεσων δρομολογητών) μέχρι να φτάσει στο δίκτυο προορισμού. Ο κάθε δρομολογητής από τον οποίο περνάει το πακέτο, αναλύει την επικεφαλίδα του και βρίσκει αν προορίζεται για το δικό του δίκτυο. Αν αυτό δεν συμβαίνει το στέλνει σε άλλο δρομολογητή, ανάλογα με τη διεύθυνση IP που βρήκε στην επικεφαλίδα.
- Όταν το πακέτο βρεθεί στο δίκτυο προορισμού, παραλαμβάνεται από τον αντίστοιχο δρομολογητή και παραδίδεται στο τοπικό δίκτυο. Από εκεί οδηγείται στον υπολογιστή προορισμού όπου και ανεβαίνει ανάποδα τα επίπεδα μέχρι να φτάσει στο επίπεδο εφαρμογής. Τελικά, το επίπεδο εφαρμογής θα δώσει το πακέτο στην κατάλληλη εφαρμογή ολοκληρώνοντας έτσι τη διαδικασία μεταφοράς του πακέτου.

7.3 Πρωτόκολλο TCP

Το πρωτόκολλο *Ελέγχου Μετάδοσης*, *Transmission Control Protocol* ή *TCP* αποτελεί το βασικό πρωτόκολλο που βρίσκεται στο επίπεδο μεταφοράς της τεχνολογίας *TCP/IP* (το άλλο φυσικά είναι το *UDP* για το οποίο θα μιλήσουμε σε επόμενη ενότητα).

τητα). Το TCP παρέχει αξιόπιστες υπηρεσίες, προσανατολισμένες σε σύνδεση, με επικοινωνία από άκρο σε άκρο (σχήμα 7.10).

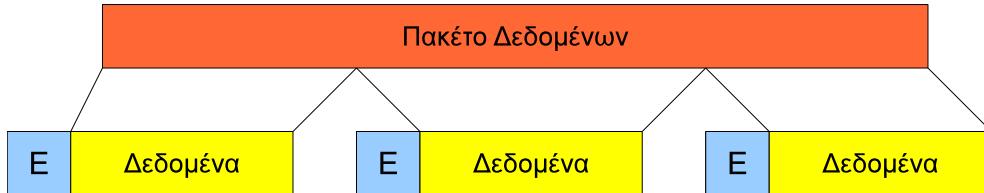


Σχήμα 7.10: Επικοινωνία στο Επίπεδο Δικτύου

Το πρωτόκολλο TCP λαμβάνει τα προς μετάδοση δεδομένα από τα πρωτόκολλα του ανώτερου επιπέδου (Εφαρμογής). Για παράδειγμα λαμβάνει από το SMTP τα δεδομένα ηλεκτρονικού ταχυδρομείου που πρέπει να αποσταλούν στον απομακρυσμένο αντίστοιχο εξυπηρετητή. Το TCP μεταδίδει μόνο όταν το πλήθος των δεδομένων που έχει λάβει είναι επαρκές για να συμπληρωθεί το μέγεθος του πακέτου που έχει συμφωνηθεί κατά την εγκατάσταση της σύνδεσης. Από την άλλη όταν λάβει δεδομένα τα οποία υπερβαίνουν αυτό το μέγεθος πακέτου, τα σπάει σε μικρότερα (σχήμα 7.11). Τα μικρότερα αυτά πακέτα στην ορολογία του TCP ονομάζονται *τμήματα* ή *segments*. Το *τμήμα* αποτελεί την μονάδα μεταφοράς στο πρωτόκολλο TCP.

Κάθε τμήμα αποτελείται από την *Επικεφαλίδα (Header)* και τα προς μετάδοση *Δεδομένα (Data)*. Η επικεφαλίδα γενικά αποτελείται από τα βοηθητικά δεδομένα που

προσθέτει το TCP και είναι απαραίτητα για τη μετάδοση. Τα δεδομένα είναι φυσικά κομμάτι των πραγματικών δεδομένων του χρήστη που θα μεταφερθούν από το συγκεκριμένο τμήμα.



Σχήμα 7.11: Διάσπαση δεδομένων σε TCP τμήματα

Η επικεφαλίδα περιέχει αρκετά πεδία, αλλά αυτά που θα μας απασχολήσουν σε αυτή την ενότητα είναι:

- Ο **Αριθμός Σειράς** ή Sequence Number
- Ο **Αριθμός Επιβεβαίωσης** ή Acknowledgment number
- Το **Παράθυρο** ή Window Size
- Οι **Θύρες (ports)** TCP αφετηρίας και προορισμού

Μπορείτε πάντως να δείτε την πλήρη μορφή της επικεφαλίδας TCP στο σχήμα 7.12 (πηγή: Wikipedia). Τα δεδομένα που έχουν χωρισθεί σε τμήματα πρέπει όταν φτά-

TCP Header																																		
Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
0	Source port																Destination port																	
32	Sequence number																Acknowledgment number																	
64																																		
96	Data offset	Reserved	C W R	E C E	U C R	A C K	P S H	R S T	S Y N	F I N	Window Size																							
128	Checksum																Urgent pointer																	
160	Options (if Data Offset > 5)																...																	
...																																		

Σχήμα 7.12: Επικεφαλίδα (Header) TCP

σουν στον προορισμό τους να ενωθούν ξανά για να δημιουργήσουν το αρχικό μεγαλύτερο πακέτο. Για να γίνει αυτό πρέπει να μπουν στη σωστή σειρά. Αυτή είναι και η λειτουργία του πεδίου που ονομάζεται **Αριθμός Σειράς**. Κάθε τμήμα έχει το δικό του αριθμό σειράς, ο οποίος δηλώνει σε ποια θέση πρέπει να μπει το συγκεκριμένο

τμήμα μαζί με τα υπόλοιπα για να δημιουργηθεί ξανά το αρχικό πακέτο. Για παράδειγμα, αν ο αριθμός σειράς έχει την τιμή 3, σημαίνει ότι πρόκειται για το τρίτο σε σειρά τμήμα από αυτά που διασπάσθηκε το αρχικό πακέτο.

Καθώς η επικοινωνία βρίσκεται σε εξέλιξη, ο παραλήπτης πρέπει να μπορεί να επιβεβαιώνει στον αποστολέα ότι λαμβάνει δεδομένα. Για το σκοπό αυτό ο παραλήπτης στέλνει τμήματα επιβεβαίωσης λήψης χρησιμοποιώντας στην επικεφαλίδα τους τον *Αριθμό Επιβεβαίωσης*. Ο αριθμός επιβεβαίωσης δηλώνει ότι έχουν ληφθεί όλες οι οκτάδες (bytes) μέχρι και αυτό τον αριθμό. Για παράδειγμα, ο αριθμός επιβεβαίωσης 1500 σημαίνει ότι έχουμε λάβει όλα τα δεδομένα μέχρι τον αριθμό οκτάδας 1500. Αν ο αποστολέας δεν λάβει επιβεβαίωση μέσα σε ένα λογικό χρονικό διάστημα, θα επαναλάβει τη μετάδοση των δεδομένων.

Το πρωτόκολλο TCP ελέγχει επίσης την ποσότητα των δεδομένων που μεταδίδονται κάθε φορά. Η λειτουργία αυτή είναι γνωστή ως έλεγχος ροής και πραγματοποιείται με τη βοήθεια του πεδίου επικεφαλίδας τμήματος που ονομάζεται *Παράθυρο (Window size)*. Για να έχουμε την καλύτερη δυνατή απόδοση η μετάδοση είναι συνεχής, δηλ. ο αποστολέας δεν περιμένει να λάβει επιβεβαίωση λήψης ενός τμήματος για να στείλει το επόμενο (διαφορετικά θα είχαμε πολύ μικρό ρυθμό μετάδοσης). Από την άλλη βέβαια δεν μπορεί να γίνεται συνέχεια αποστολή χωρίς κάποιο είδος επιβεβαίωσης λήψης. Αν στέλνουμε με ταχύτητα πολύ μεγαλύτερη από αυτή που μπορεί να δεχθεί ο απομακρυσμένος υπολογιστής, κάποια στιγμή θα γεμίσει η ενδιάμεση μνήμη που χρησιμοποιείται για την προσωρινή αποθήκευση των δεδομένων και ο παραλήπτης θα αρχίσει να απορρίπτει τα εισερχόμενα δεδομένα αφού δεν θα έχει που να τα αποθηκεύσει. Για το λόγο αυτό και τα δύο άκρα της σύνδεσης πρέπει να υποδεικνύουν πόσα δεδομένα μπορούν να δεχθούν κάθε φορά, βάζοντας τον αντίστοιχο αριθμό οκτάδων στο πεδίο “Παράθυρο” της επικεφαλίδας.

Παράδειγμα: Αν η τιμή του παραθύρου είναι 1000, σημαίνει ότι ο υπολογιστής είναι έτοιμος να δεχθεί 1000 οκτάδες δεδομένων. Αν η τιμή του πεδίου “Αριθμός Επιβεβαίωσης” είναι 12000, ο υπολογιστής είναι έτοιμος να δεχθεί δεδομένα που βρίσκονται στην περιοχή από 12000 μέχρι $12000+1000=13000$. Έχει δηλ. ήδη λάβει όλα τα δεδομένα μέχρι το 12000.

Σημείωση: Ο αριθμός επιβεβαίωσης είναι πάντα κατά 1 μεγαλύτερος από το τελευταίο byte δεδομένων που έχουμε λάβει. Δηλ. δείχνει πάντα το επόμενο byte που επιθυμούμε να λάβουμε. Στο παραπάνω παράδειγμα, ο αριθμός επιβεβαίωσης 12000 σημαίνει ότι έχουμε ήδη λάβει 11999 bytes και επιθυμούμε να λάβουμε από το 12000 και μετά.

Τέλος υπάρχει η έννοια των θυρών *TCP ports*. Το σχολικό βιβλίο γράφει ότι τα TCP ports είναι “αφηρημένα σημεία επικοινωνίας” αλλά αυτό δεν εξηγεί τη

χρήση τους. Αν θέλαμε να δώσουμε ένα ορισμό για τη θύρα TCP θα λέγαμε ότι είναι ένας αριθμός που χαρακτηρίζει πλέον μέσα στο μηχάνημα του αποστολέα (ή του παραλήπτη) την ίδια την εφαρμογή που πρόκειται να λάβει τα δεδομένα του συγκεκριμένου TCP τμήματος.

Για να γίνουμε πιο συγκεκριμένοι, σκεφτείτε ότι ένα TCP τμήμα που λαμβάνεται σαν τμήμα μιας μετάδοσης δεν ξέρει σε ποια εφαρμογή να κατευθυνθεί. Το πρόβλημα δεν θα υπήρχε προφανώς αν ένας υπολογιστής εκτελούσε κάθε φορά μόνο μια εφαρμογή επικοινωνίας (π.χ. αν μπορούσαμε να δούμε μόνο μια σελίδα στο Internet κάθε φορά, και να μην εκτελούμε ταυτόχρονα καμιά άλλη δικτυακή εφαρμογή), αλλά αυτό δεν συμβαίνει. Το πρόβλημα λύνεται αν κάθε τμήμα περιέχει μέσα του ένα αριθμό θύρας που θα το κατευθύνει στην εφαρμογή για την οποία προορίζεται.

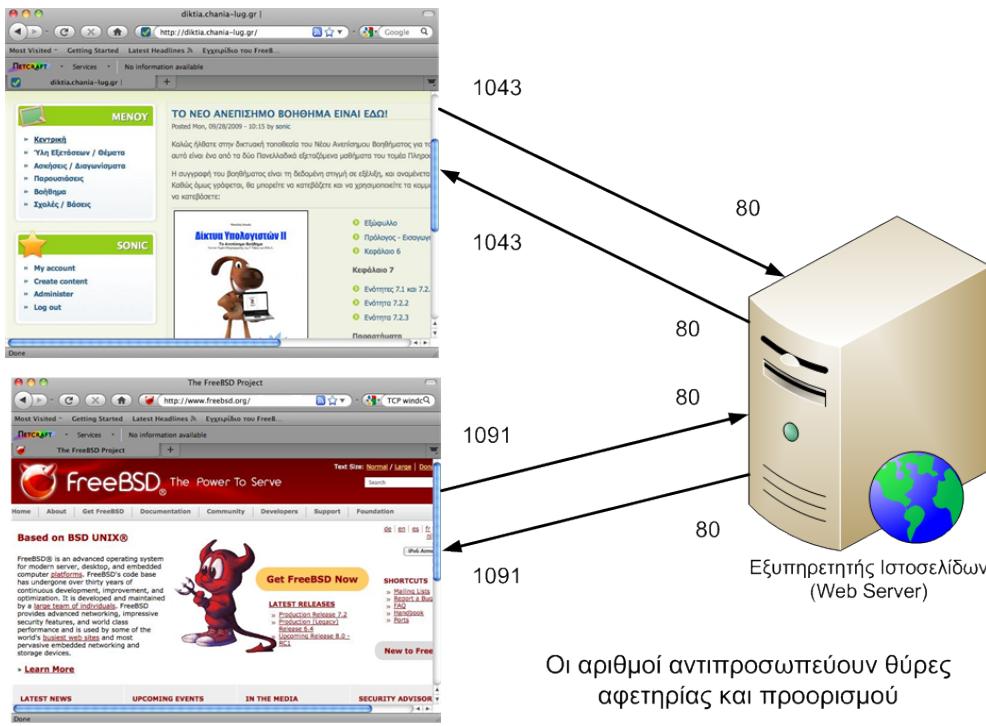
Εποι, όταν για παράδειγμα ανοίξουμε ένα φυλλομετρητή όπως το Firefox και αρχίσουμε να βλέπουμε μια σελίδα, τα τμήματα TCP που φεύγουν από τον υπολογιστή μας ως κομμάτι της συγκεκριμένης επικοινωνίας, χαρακτηρίζονται από ένα αριθμό ο οποίος είναι η θύρα αφετηρίας. Τα τμήματα αυτά περιέχουν επίσης και μια θύρα προορισμού η οποία εξασφαλίζει ότι όταν το τμήμα ληφθεί από το μηχάνημα προορισμού θα κατευθυνθεί στη σωστή εφαρμογή (στη συγκεκριμένη περίπτωση στον εξυπηρετητή ιστοσελίδων). Τα τμήματα που θα λάβουμε ως απάντηση, θα έχουν πλέον ως θύρα προορισμού την ίδια με την οποία ξεκινήσαμε την επικοινωνία, και άρα θα κατευθυνθούν στο ίδιο παράθυρο του Firefox.

Αν χρησιμοποιήσουμε το Firefox για να βλέπουμε πολλαπλές σελίδες (π.χ. ανοίξουμε πολλά παράθυρα ή tabs), τα τμήματα TCP για κάθε σελίδα θα χαρακτηρίζονται από διαφορετικούς αριθμούς θυρών αφετηρίας, και άρα τα δεδομένα που θα λαμβάνουμε ως απάντηση θα μπορούν πάντα να κατευθυνθούν στο σωστό παράθυρο. Δείτε και το σχήμα 7.13.

Καταλαβαίνετε γιατί υπάρχει πρόβλημα στο σχήμα 7-10 του βιβλίου;

Παράδειγμα από την καθημερινότητα: Αν όλοι κατοικούσαμε σε μονοκατοικίες, ο ταχυδρόμος δεν θα χρειαζόταν παρά μόνο τη διεύθυνση μας (οδός/αριθμός) για να μας παραδώσει ένα δέμα. Η διεύθυνση σε αυτή την περίπτωση αντιστοιχεί στην IP διεύθυνση του παραλήπτη. Επειδή όμως οι περισσότεροι μένουμε σε πολυκατοικίες, ο ταχυδρόμος πρέπει επίσης να ξέρει και τον όροφο/όνομα. Η διεύθυνση δύο παραληπτών (οδός/αριθμός, IP) μπορεί να είναι ίδια, διαφοροποιούνται όμως με βάση το όνομα/όροφο (αριθμός θύρας προορισμού).

Συνήθως, όταν γίνεται μια νέα σύνδεση TCP προσδιορίζονται αρχικά οι θύρες πηγής



Υπολογιστής Χρήστη

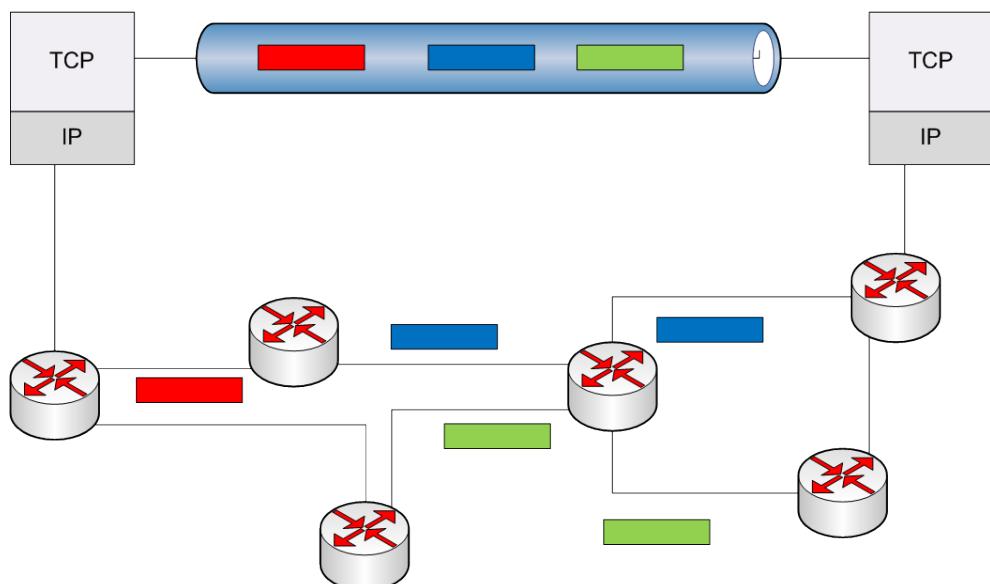
Σχήμα 7.13: Λειτουργία Θυρών TCP

και προορισμού και γνωστοποιούνται και στα δύο άκρα. Στην πράξη, τα προγράμματα που χρησιμοποιούνται στη μεριά του πελάτη (π.χ. ο φυλλομετρητής που εκτελούμε για να δούμε μια σελίδα) επιλέγουν μια τυχαία θύρα TCP, η οποία ανατίθεται δυναμικά και αλλάζει για κάθε νέα σύνδεση (Σημείωση: Οι θύρες αυτές ονομάζονται μη-προνομιούχες (non-privileged) και επιλέγονται με αριθμούς πάνω από το 1024). Από τη μεριά των εξυπηρετητών, χρησιμοποιούνται συγκεκριμένες, βάση σύμβασης, θύρες (λέγονται και προνομιούχες, privileged) οι οποίες έχουν από πριν συμφωνηθεί και έχουν συνήθως αριθμούς κάτω από το 1024.

Για παράδειγμα, η θύρα που χρησιμοποιείται από τον εξυπηρετητή ιστοσελίδων είναι η 80. Όταν ζητάμε μια σελίδα μέσω του Firefox, τα τμήματα TCP που δημιουργούνται έχουν μια τυχαία θύρα αφετηρίας αλλά κατευθύνονται πάντα στη θύρα 80 του εξυπηρετητή ιστοσελίδων που συνδεόμαστε. Αντίστοιχες τυποποιημένες θύρες υπηρεσιών υπάρχουν για κάθε σχεδόν πρόγραμμα εξυπηρετητή. Π.χ. για το πρωτόκολλο μεταφοράς αρχείων FTP η θύρα είναι η 21, για το πρωτόκολλο ταχυδρομείου SMTP η 25 κ.ο.κ. Οι εξυπηρετητές αυτοί πάντοτε λαμβάνουν και επεξεργάζονται όλα τα δεδομένα που κατευθύνονται στις θύρες τους (Σημείωση: Οι θύρες αυτές είναι γνωστές και ως θύρες ακρόασης, *listening ports*).

7.3.1 TCP Συνδέσεις

Όπως έχουμε ήδη αναφέρει, το TCP πρωτόκολλο είναι προσανατολισμένο στη σύνδεση. Σε αυτή την ενότητα θα εξηγήσουμε με ποιο τρόπο συσχετίζει το TCP πρωτόκολλο τα τμήματα τα οποία ανήκουν σε μια σύνδεση και πως τα ξεχωρίζει από άλλες συνδέσεις που μπορεί την ίδια στιγμή να υπάρχουν σε ένα μηχάνημα. Η σύν-



Σχήμα 7.14: TCP Σύνδεση

δεση στο TCP πρωτόκολλο έχει την έννοια της νοητής σύνδεσης που εγκαθίσταται από το TCP προκειμένου να συνδέσει τα δύο τελικά σημεία μεταξύ τους. Μπορούμε να φανταστούμε αυτή τη σύνδεση ως ένα νοητό σωλήνα (σχήμα 7.14) που ενώνει τα δύο τελικά σημεία και μεταφέρει τα δεδομένα από το ένα άκρο στο άλλο. Η σύνδεση είναι νοητή γιατί:

- Δεν υπάρχει απευθείας σύνδεση του ενός άκρου με το άλλο. Η σύνδεση γίνεται μέσω του επικοινωνιακού υποδικτύου.
- Δεν υπάρχει συγκεκριμένη διαδρομή που ακολουθούν όλα τα τμήματα προκειμένου να φτάσουν στον προορισμό τους. Αντίθετα, τα τμήματα διασπώνται σε κομμάτια από το πρωτόκολλο IP και το καθένα ακολουθεί δική του διαδρομή μέχρι τον προορισμό, όπου και φτάνουν μπερδεμένα με άλλα τμήματα (διαφορετικής επικοινωνίας) και πιθανόν με λάθος σειρά. Το πρωτόκολλο TCP πρέπει να βρει (με τη βοήθεια κάποιων αναγνωριστικών στοιχείων) ποια τμήματα ανήκουν σε ποια σύνδεση και να τα δώσει στην κατάλληλη εφαρμογή που θα τα χειριστεί.

Για να δούμε με ποιο τρόπο δουλεύουν οι TCP συνδέσεις, θα τις εξετάσουμε με βάση το παρακάτω παράδειγμα:

Παράδειγμα: Έστω ότι θέλουμε να μεταφέρουμε αρχεία μέσω της εφαρμογής FTP (File Transfer Protocol) από ένα υπολογιστή σε ένα άλλο. Έχουμε ήδη πει ότι το FTP (Πρωτόκολλο Μεταφοράς Αρχείων) ανήκει στο επίπεδο Εφαρμογής του TCP. Για να στείλουμε ένα αρχείο μέσω του FTP χρειαζόμαστε:

- Ένα πρόγραμμα FTP από τη μεριά του χρήστη που θα στείλει το αρχείο. Ο χρήστης αυτός θεωρείται ο “πελάτης” όσο αφορά τη σύνδεση. Τέτοια προγράμματα μπορεί είτε να χρησιμοποιούν γραφικό περιβάλλον είτε να μας επιτρέπουν να στείλουμε απευθείας τις εντολές του FTP από ένα τερματικό.
- Στο άκρο της επικοινωνίας που θα λάβει το αρχείο θα υπάρχει ένα αντίστοιχο πρόγραμμα εξυπηρετητή FTP το οποίο θα λάβει τα εισερχόμενα δεδομένα από τον πελάτη και θα τα αποθηκεύσει.

Από τα παραπάνω είναι (ελπίζουμε) εμφανές ότι η επικοινωνία ξεκινάει με πρωτοβουλία του πελάτη (χρήστη) ενώ ο εξυπηρετητής FTP είναι απλώς ένα πρόγραμμα που εκτελείται συνέχεια στο απομακρυσμένο μηχάνημα και περιμένει κάποιο πελάτη να συνδεθεί σε αυτό για να στείλει (ή να λάβει) κάποιο αρχείο.

Η διαδικασία θα μοιάζει με την παρακάτω:

- Ο πελάτης εκτελεί την εφαρμογή FTP με την οποία θα στείλει το αρχείο.
- Ο πελάτης επιλέγει (ή γράφει) τον εξυπηρετητή FTP με τον οποίο θα συνδεθεί.
- Ανοίγει μια σύνδεση TCP με τον εξυπηρετητή FTP στο άλλο άκρο της σύνδεσης.

Στο άκρο της σύνδεσης του πελάτη το πρόγραμμα FTP επιλέγει μια τυχαία θύρα (port), π.χ. το 1234. Όπως έχουμε ήδη πει, οι θύρες αυτές (μη-προνομιούχες) επιλέγονται τυχαία, γιατί κανείς δεν πρόκειται να τις αναζητήσει (δεν παρέχουν κάποια υπηρεσία).

Τα τμήματα TCP που φεύγουν από τον πελάτη με προορισμό τον εξυπηρετητή FTP έχουν ως θύρα προορισμού το 21. Το 21 είναι η τυποποιημένη (βάσει σύμβασης) θύρα που χρησιμοποιείται από τους εξυπηρετητές FTP. Αν οι θύρες για συγκεκριμένες υπηρεσίες δεν ήταν καθορισμένες, δεν θα μπορούσαμε με εύκολο τρόπο να ξεχωρίσουμε ποια τμήματα προορίζονται για ποια υπηρεσία (Ένας server μπορεί να παρέχει ταυτόχρονα πολλές διαφορετικές υπηρεσίες οι οποίες δέχονται εισερχόμενες συνδέσεις σε διαφορετικές θύρες).

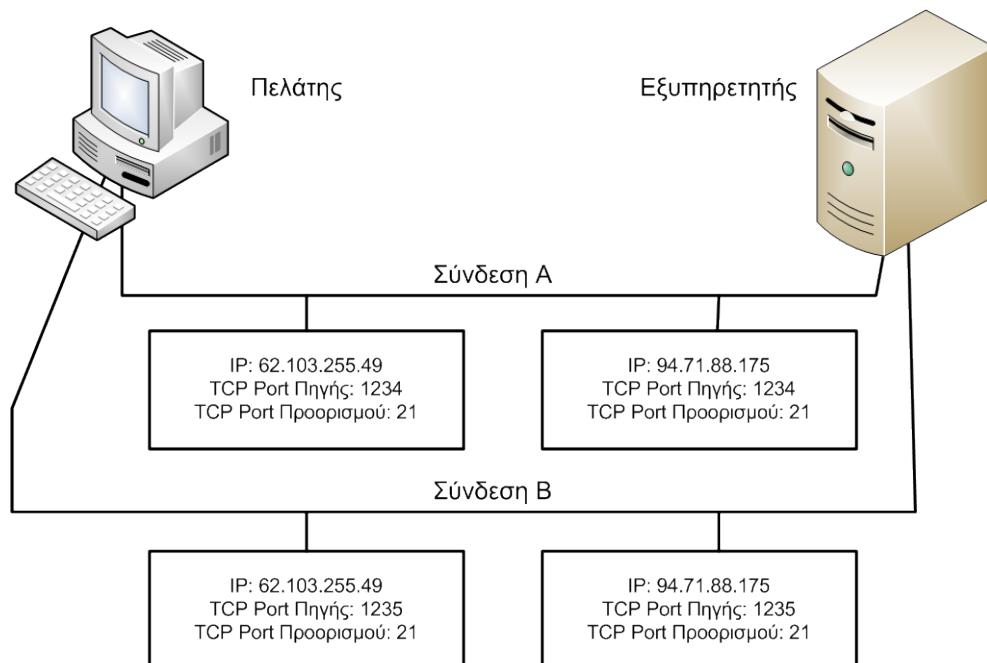
- Αρχίζει η μεταφορά του αρχείου, με τα τμήματα του πελάτη να ξεκινάνε από την θύρα 1234 και να καταλήγουν στη θύρα 21 του εξυπηρετητή

- Στο τέλος της επικοινωνίας, ειδοποιείται ο πελάτης ότι η αποστολή του αρχείου έχει ολοκληρωθεί και γίνεται τερματισμός της TCP σύνδεσης.

Είναι φανερό ότι όσο αφορά το TCP η σύνδεση χαρακτηρίζεται από τη θύρα πηγής (1234) και τη θύρα προορισμού (21). Μπορούμε εύκολα να καθορίσουμε το είδος της επικοινωνίας βλέποντας τη θύρα του προορισμού: Π.χ. το 21 είναι FTP, το 80 HTTP κλπ. Είναι επίσης προφανές ότι η επικοινωνία αυτή ακολουθεί το μοντέλο πελάτη – εξυπηρετητή στο οποίο έχουμε ήδη αναφερθεί.

Αν και το TCP ενδιαφέρεται για τις θύρες πηγής και προορισμού, δεν πρέπει να ξεχνάμε ότι η πλήρης επικοινωνία διέρχεται μέσα από το πρωτόκολλο IP και περιέχει μέσα ακόμα δύο αριθμούς: Την διεύθυνση IP του αποστολέα και την διεύθυνση IP του παραλήπτη. Συνολικά λοιπόν η επικοινωνία χαρακτηρίζεται με μοναδικό τρόπο από τέσσερις αριθμούς:

- Την διεύθυνση IP του αποστολέα π.χ. 62.103.240.22. Στο παράδειγμα μας θα ήταν ο πελάτης που επιθυμεί να στείλει το αρχείο.
- Την θύρα της πηγής. Στο παράδειγμα μας η 1234.
- Την διεύθυνση IP του παραλήπτη π.χ. 61.74.29.32.
- Την θύρα προορισμού, στο παράδειγμα μας το 21.



Σχήμα 7.15: TCP Συνδέσεις

Με βάση αυτούς τους τέσσερις αριθμούς, το TCP πρωτόκολλο μπορεί να ξεχωρίσει με μοναδικό τρόπο ποια τμήματα ανήκουν σε ποια σύνδεση (σημείωση: αυτή είναι η φράση του βιβλίου – ποιο είναι το λάθος εδώ). Δεν είναι δυνατόν δύο διαφορετικές συνδέσεις να μη διαφέρουν τουλάχιστον σε ένα από αυτά τα ψηφία.

Είναι στην πραγματικότητα δυνατόν να διαφέρουν μόνο σε ένα από αυτούς τους αριθμούς;

Και βέβαια. Φανταστείτε ένα από τα παρακάτω σενάρια (σχήμα 7.15):

- Έχετε ανοίξει δύο φορές το πρόγραμμα μεταφοράς αρχείων (FTP) και ταυτόχρονα στέλνετε δύο διαφορετικά αρχεία στον ίδιο εξυπηρετητή.
- Έχετε ανοίξει δύο φορές ένα πρόγραμμα φυλλομετρητή (π.χ. Firefox) και βλέπετε το ίδιο site (ίσως διαφορετική σελίδα) και από τα δύο παράθυρα.
- Έχετε ένα υπολογιστή που χρησιμοποιείται ταυτόχρονα από δύο χρήστες οι οποίοι έχουν συνδεθεί στην ίδια ιστοσελίδα. (Σημείωση: Μη βιαστείτε να πείτε ότι αυτό δεν γίνεται, στο UNIX εργαστήριο μας τα μηχανήματα είναι γραφικά τερματικά ενός και μόνου υπολογιστή. Ουσιαστικά όλα αυτά τα μηχανήματα είναι ένας υπολογιστής).

Σε κάθε μια από τις παραπάνω περιπτώσεις αλλάζει μόνο ένας αριθμός: *H θύρα της πηγής*. Ας το δούμε αναλυτικότερα:

- Ο υπολογιστής πηγής είναι ένας, το IP πηγής είναι το ίδιο.
- Ο υπολογιστής προορισμού είναι ο ίδιος, το IP προορισμού είναι το ίδιο.
- Η υπηρεσία στην οποία προσπαθούμε να συνδεθούμε είναι σε κάθε περίπτωση η ίδια, άρα και η θύρα προορισμού είναι ίδια.
- Το μόνο που αλλάζει είναι η θύρα της πηγής, καθώς αυτή επιλέγεται κάθε φορά τυχαία και είναι διαφορετική ακόμα και αν εκτελέσουμε πολλές φορές το ίδιο πρόγραμμα στον ίδιο υπολογιστή.

7.4 Πρωτόκολλο UDP

Το πρωτόκολλο TCP μεταξύ άλλων είναι υπεύθυνο για το τεμαχισμό των μηνυμάτων σε τμήματα και την επανασύνδεση τους στον προορισμό. Είδαμε επίσης ότι το TCP είναι πρωτόκολλο με σύνδεση και προσφέρει αξιόπιστη επικοινωνία. Εξασφαλίζει δηλ. ότι τα δεδομένα θα ληφθούν σωστά και στην αντίθετη περίπτωση φροντίζει για την επαναμετάδοση τους. Η διαδικασία αυτή είναι διάφανη όσο αφορά τα πρωτόκολλα εφαρμογής που εξυπηρετούνται από το TCP: Αν κάνουμε μια μεταφορά αρχείου μέσω FTP και κάποια TCP τμήματα δεν φτάσουν, το TCP θα τα μεταδώσει ξανά και η εφαρμογή FTP δεν θα ενημερωθεί για αυτό.

Τα σημαντικά αυτά πλεονεκτήματα του πρωτοκόλλου TCP έρχονται με κάποιο κόστος: Εκτελώντας τόσες λειτουργίες (τεμαχισμός, έλεγχος λαθών, έλεγχος σειράς κλπ) το TCP είναι σχετικά πολύπλοκο πρωτόκολλο στη λειτουργία του. Ένα αποτέλεσμα αυτής της πολυπλοκότητας είναι ότι εισάγει κάποιες καθυστερήσεις στην επικοινωνία. Καθώς μάλιστα είναι πρωτόκολλο με σύνδεση, πρέπει να έχει και αρχική επικοινωνία με τον υπολογιστή στην άλλη μεριά πριν καν ξεκινήσει η μετάδοση.

Όταν χρειαζόμαστε όλες αυτές τις λειτουργίες που παρέχει, το TCP είναι το κατάλληλο πρωτόκολλο. Υπάρχουν όμως εφαρμογές που ένα πιο απλό πρωτόκολλο θα μας εξυπηρετούσε καλύτερα. Τέτοια είδη εφαρμογών είναι:

- Εφαρμογές που τα μηνύματα τους χωράνε κάθε φορά σε ένα μόνο τμήμα. Προφανώς σε αυτή την περίπτωση δεν χρειαζόμαστε τη λειτουργία τεμαχισμού που μας παρέχει το TCP.
- Εφαρμογές που δεν έχει σημασία αν χαθούν κάποια δεδομένα στη μετάδοση, ή δεν έχει νόημα η επαναμετάδοση τους: Για παράδειγμα σε εφαρμογές φωνής δεν έχει νόημα να μεταδώσουμε ξανά δεδομένα που χάθηκαν, μας ενδιαφέρει ωστόσο η μετάδοση να προχωράει όσο το δυνατόν πιο γρήγορα και χωρίς καθυστερήσεις. Διαφορετικά θα έχουμε φωνή πολύ κακής ποιότητας.
- Γενικά εφαρμογές που έχει περισσότερη σημασία να μπορούμε να μεταδώσουμε με τις μικρότερες δυνατές καθυστερήσεις και μεγαλύτερη ταχύτητα παρά με ακρίβεια και αξιοπιστία.

Για τις περιπτώσεις αυτές, έχει σχεδιαστεί ένα ακόμα πρωτόκολλο στο επίπεδο μεταφοράς, το *UDP*, *User Datagram Protocol* ή διαφορετικά *Πρωτόκολλο Αυτοδύναμων Πακέτων Χρήστη*.

Γενικά για το UDP μπορούμε να πούμε:

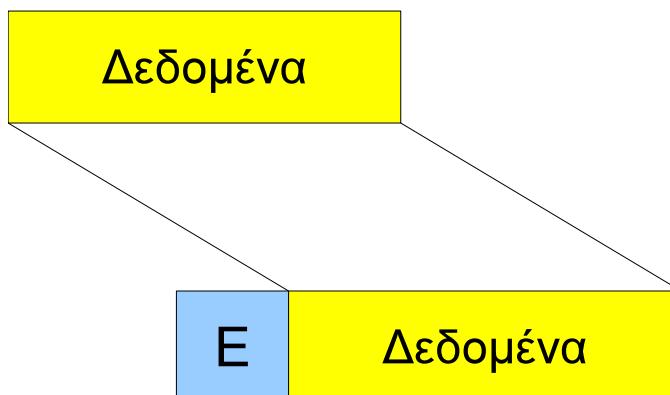
- Είναι πολύ απλούστερο από το TCP: Δεν διαθέτει τεμαχισμό, για το λόγο αυτό κάθε μήνυμα που μεταδίδεται από μια εφαρμογή μέσω UDP πρέπει να χωράει εξ'ολοκλήρου σε ένα τμήμα UDP.
- Είναι πρωτόκολλο αυτοδύναμου πακέτου χωρίς σύνδεση: Η αποστολή ξεκινάει αμέσως χωρίς να γίνει επικοινωνία με την άλλη μεριά. Δεν έχει έτσι επιπλέον καθυστερήσεις.
- Δεν διαθέτει έλεγχο λαθών. Δεν κάνει επαναμετάδοση δεδομένων και δεν κρατάει αντίγραφο των δεδομένων που στάλθηκαν για επιβεβαίωση. Δεν εξασφαλίζει επίσης ότι τα τμήματα θα φτάσουν στον προορισμό τους με τη σωστή σειρά. Αν μια εφαρμογή που χρησιμοποιεί UDP χρειάζεται να εξασφαλίσει ότι τα δεδομένα της δεν έχουν επηρεαστεί από τα παραπάνω προβλήματα, θα πρέπει να τα ελέγξει η ίδια. Μεταφέρεται δηλ. ο έλεγχος λαθών από το επίπεδο

μεταφοράς στο επίπεδο εφαρμογής.

Όπως και με το πρωτόκολλο TCP, το UDP χρησιμοποιεί θύρες (ports), τα UDP ports. Η χρήση τους είναι ακριβώς ίδια με του πρωτοκόλλου TCP (είναι δηλ. κατά το βιβλίο σας αφηρημένα σημεία επικοινωνίας) και προσδιορίζονται από ένα ακέραιο αριθμό 16 bits (παίρνουν δηλ. τιμές από 0 – 65535). Ο αριθμός αυτός γράφεται στην επικεφαλίδα του UDP τμήματος.

bits	0 - 15	16 - 31
0	Source Port	Destination Port
32	Length	Checksum
64	Data	

Σχήμα 7.16: Πλήρης Δομή UDP



Σχήμα 7.17: Δημιουργία UDP Τμήματος

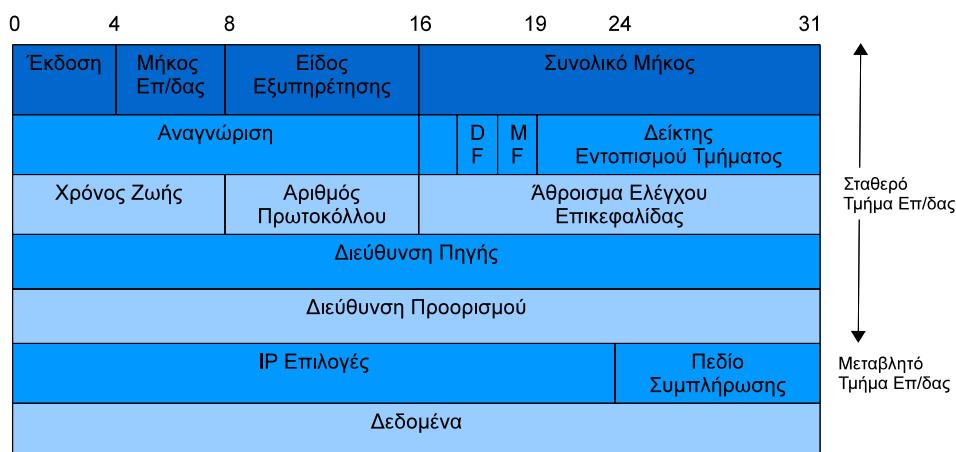
Η επικοινωνία στο πρωτόκολλο UDP είναι πολύ απλή: Σε συγκεκριμένα UDP ports έχουν ανατεθεί συγκεκριμένες εφαρμογές που εκτελούνται από τους εξυπηρετητές. Για παράδειγμα, ο εξυπηρετητής DNS (μετατρέπει τα φιλικά προς το χρήστη ονόματα όπως www.sch.gr σε διευθύνσεις IP π.χ. 194.63.238.40) χρησιμοποιεί τη θύρα UDP 53 για να λαμβάνει αιτήματα. Στο πρωτόκολλο SNMP (Απλό Πρωτόκολλο Διαχείρισης Δικτύου) χρησιμοποιείται η θύρα 161. Από τη μεριά του πελάτη, επιλέγεται (όπως και στο TCP) μια τυχαία θύρα. Το κάθε UDP τμήμα αποτελείται από δύο βασικά κομμάτια, την επικεφαλίδα και τα δεδομένα (Απλουστευμένη μορφή στο σχήμα 7.17, πλήρης απεικόνιση στο σχήμα 7.16 - πηγή: Wikipedia).

Το πρωτόκολλο IP στο επίπεδο Δικτύου μπορεί από την επικεφαλίδα κάθε εισερχόμενου τμήματος να ξεχωρίσει αν είναι TCP ή UDP και το παραδίδει στο αντίστοιχο πρωτόκολλο. Η βασική λειτουργικότητα που προσθέτει το UDP σε αυτές του πρωτοκόλλου IP είναι η πολυπλεξία της πληροφορίας διαφορετικών εφαρμογών με τη χρήση των θυρών UDP.

7.5 Πρωτόκολλο IP

Στο επίπεδο δικτύου της τεχνολογίας TCP/IP, συναντάμε το πρωτόκολλο *IP, Internet Protocol*. Η λειτουργία του IP βασίζεται αποκλειστικά στην ιδέα του αυτοδύναμου πακέτου ή *datagram*, το οποίο σημαίνει ότι τα πακέτα μεταφέρονται από την πηγή στον προορισμό χωρίς να ακολουθούν συγκεκριμένη διαδρομή (το κάθε ένα μπορεί να ακολουθήσει διαφορετική). Οι έλεγχοι για αξιόπιστη μετάδοση γίνονται από το επίπεδο μεταφοράς, εφόσον χρησιμοποιείται το πρωτόκολλο TCP.

Κάθε φορά που το TCP ή το UDP πρωτόκολλο από το επίπεδο μεταφοράς θέλει να μεταδώσει κάποιο τμήμα (θυμηθείτε ότι το TCP και το UDP παράγουν *segments*), το παραδίδει στο πρωτόκολλο IP. Η μόνη άλλη πληροφορία που χρειάζεται το IP (και η οποία του παρέχεται από το επίπεδο μεταφοράς) είναι η διεύθυνση του υπολογιστή προορισμού. Αυτό είναι και το μόνο στοιχείο που ενδιαφέρει το πρωτόκολλο IP. Το IP δεν ενδιαφέρεται καθόλου για το περιεχόμενο του τμήματος ή για το πως (και αν) σχετίζεται με το προηγούμενο ή επόμενο τμήμα που λαμβάνει. Απλώς τα προωθεί στον προορισμό τους.



Σχήμα 7.18: IP Αυτοδύναμο Πακέτο

Για να γίνει αυτό βέβαια, θα πρέπει το IP αφού παραλάβει το τμήμα από το επίπεδο μεταφοράς να προσθέσει τη δική του επικεφαλίδα (Σχήμα 7.18) με τα απα-

ραίτητα στοιχεία, σχηματίζοντας έτσι ένα αυτοδύναμο IP πακέτο. Το μέγιστο μήκος του πακέτου αυτού έχει ορισθεί στα 64 Kbytes. Μετά το σχηματισμό του πακέτου, αποστολή του IP είναι να βρει την κατάλληλη διαδρομή που θα το οδηγήσει στον προορισμό του.

Μετά τον προσδιορισμό της διαδρομής του πακέτου, γίνεται η μετάδοση του μέσω των φυσικών δικτύων (που αντιστοιχούν στο επίπεδο πρόσβασης δικτύου της τεχνολογίας TCP/IP – ή στα επίπεδα σύνδεσης δεδομένων και φυσικό του OSI – και περιγράφονται από τα αντίστοιχα πρωτόκολλα π.χ. Ethernet και τα φυσικά μέσα και συσκευές – καλώδια, κάρτες δικτύου – τα οποία χρησιμοποιούνται).

Ένα φυσικό δίκτυο μπορεί ωστόσο να χρησιμοποιεί διαφορετικό μέγιστο μήκος μονάδας μεταφοράς σε σχέση με τα 64 Kbyte που χρησιμοποιεί το IP.

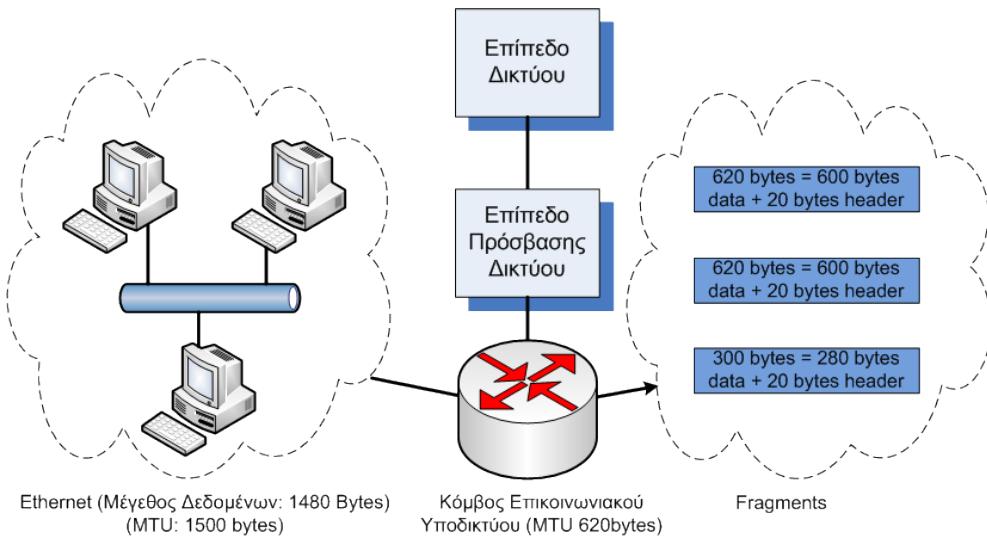
Σημείωση: Το μέγιστο μήκος μονάδας μεταφοράς ονομάζεται και *MTU, Maximum Transfer Unit*. Εξαρτάται συνήθως από το πρωτόκολλο που χρησιμοποιείται στο επίπεδο πρόσβασης δικτύου (το οποίο προφανώς έχει φτιαχτεί για συγκεκριμένα φυσικά μέσα, δικτυακές συσκευές κλπ). Για παράδειγμα στο Ethernet το MTU είναι 1500 bytes.

Αυτό προφανώς είναι πρόβλημα αν το MTU είναι μικρότερο από το IP πακέτο, καθώς αυτό σημαίνει ότι κυριολεκτικά το IP πακέτο “δεν χωράει να περάσει” μέσα από το συγκεκριμένο φυσικό δίκτυο. Για να ξεπεραστεί αυτό το πρόβλημα, το πρωτόκολλο IP έχει τη δυνατότητα να διασπάσει τα αυτοδύναμα πακέτα σε μικρότερα τμήματα που ονομάζονται *κομμάτια ή fragments*. Το IP αναλαμβάνει να επανασυνθέσει αυτά τα κομμάτια στον προορισμό τους και να σχηματίσει ξανά το αρχικό αυτοδύναμο IP πακέτο.

Η διάσπαση των πακέτων σε fragments γίνεται όταν το πακέτο φτάσει στον πρώτο δρομολογητή του δικτύου (Σχήμα 7.19). Ο δρομολογητής αντιλαμβάνεται ότι το φυσικό δίκτυο που συνδέεται σε αυτόν δεν μπορεί να μεταδώσει ολόκληρο το πακέτο που έλαβε και το διασπά σε κομμάτια. Μη ξεχνάμε ότι ο δρομολογητής είναι μια συσκευή που λειτουργεί στο επίπεδο δικτύου και άρα αντιλαμβάνεται τις πληροφορίες της επικεφαλίδας IP. Τα κομμάτια που δημιουργούνται είναι και αυτά εντελώς αυτοδύναμα και ανεξάρτητα μεταξύ τους και μπορεί πάλι το καθένα να ακολουθήσει διαφορετική διαδρομή μέχρι τον προορισμό.

Το πεδίο *Αναγνώριση* στην επικεφαλίδα του πακέτου IP χρησιμοποιείται ώστε το IP να αναγνωρίζει σε ποιο αυτοδύναμο IP πακέτο ανήκει το fragment που λαμβάνει τη δεδομένη στιγμή. Όλα τα κομμάτια που έχουν την ίδια τιμή σε αυτό το πεδίο, ανήκουν στο ίδιο αυτοδύναμο πακέτο.

Το πεδίο *Δείκτης Εντοπισμού Τμήματος* στην επικεφαλίδα του πακέτου IP χρησιμο-



Σχήμα 7.19: Διάσπαση σε Fragments

ποιείται ώστε το IP να αναγνωρίζει σε ποια θέση πρέπει να τοποθετηθεί το συγκεκριμένο fragment που λαμβάνεται για να δημιουργηθεί ξανά το αυτοδύναμο IP πακέτο. Η τιμή του δίνεται σε blocks των 8 bytes (οκτάδες οκτάδων γράφει το βιβλίο σας, γιατί δεν κατάφερε να μεταφράσει σωστά τη wikipedia).

Προφανώς το IP χρειάζεται και ένα τρόπο να γνωρίζει αν το πακέτο που λαμβάνει τη δεδομένη στιγμή είναι ένα κανονικό ξεχωριστό αυτοδύναμο πακέτο ή αν αποτελεί τμήμα (fragment) κάποιου πακέτου. Για το σκοπό αυτό χρησιμοποιείται το πεδίο *More Fragments (MF)* ή *Ένδειξη Υπαρξής Περισσότερων Κομματιών*. Αν αυτό το πεδίο έχει την τιμή 1, σημαίνει ότι τη δεδομένη στιγμή λαμβάνουμε ένα fragment ενός μεγαλύτερου πακέτου. Αν έχει την τιμή 0 σημαίνει είτε ότι λαμβάνουμε το τελευταίο fragment ή ότι το πακέτο είναι αυτοδύναμο. Σε κάθε πακέτο που έχει κομματιαστεί, όλα τα κομμάτια έχουν MF=1 εκτός από το τελευταίο. (Σημείωση: στην πραγματικότητα τα πεδία που χρησιμοποιούνται με αυτό τον τρόπο – με τιμές 0 ή 1 – ονομάζονται flags ή σημαίες)

Είναι πιθανόν ο υπολογιστής προορισμού να μην μπορεί για οποιοδήποτε λόγο να δεχθεί δεδομένα τα οποία έχουν κομματιαστεί. Αν συμβαίνει αυτό, θέτει την τιμή του πεδίου *Don't Fragment, (DF)*, *Ένδειξης Απαγόρευσης Διάσπασης Αυτοδύναμου Πακέτου* στην τιμή 1. Στην περίπτωση αυτή θα πρέπει να βρεθεί διαδρομή μέσα από το φυσικό δίκτυο η οποία να είναι ικανή να περάσει τα αυτοδύναμα IP πακέτα χωρίς να τα κομματιάσει. Αν δεν υπάρχει αυτή η δυνατότητα, το αυτοδύναμο πακέτο απορρίπτεται.

Τα υπόλοιπα πεδία που υπάρχουν στην επικεφαλίδα είναι τα εξής:

- **Έκδοση:** Προσδιορίζει την έκδοση του πρωτοκόλλου που χρησιμοποιείται. Για να υπάρχει επικοινωνία μεταξύ πηγής και προορισμού πρέπει οπωσδήποτε να χρησιμοποιείται η ίδια έκδοση πρωτοκόλλου (Σημείωση: Οι διαθέσιμες εκδόσεις είναι το IPv4 και το IPv6. Μελλοντικά αναμένεται να χρησιμοποιείται όλο και περισσότερο το IPv6).
- **Μήκος Επικεφαλίδας:** Δηλώνει το μήκος της επικεφαλίδας του πακέτου σε λέξεις των 32 bits. Η μικρότερη τιμή που μπορεί να έχει το πεδίο αυτό είναι 5. Η μικρότερη δυνατή επικεφαλίδα έχει μήκος $5*32=160$ bits, και αν διαιρέσουμε με το 8, $160/8=20$ bytes.
- **Είδος Εξυπηρέτησης:** Με το πεδίο αυτό δηλώνει ο υπολογιστής το είδος της υπηρεσίας που ζητάει από το επικοινωνιακό υποδίκτυο. Τα χαρακτηριστικά που προσδιορίζουν την υπηρεσία που προσφέρει το υποδίκτυο και που χρησιμοποιούνται από το IP για να περιγράψουν τις απαιτήσεις του είναι: Η ρυθμοαπόδοση, η αξιοπιστία και η καθυστέρηση.

Τι θέλει να πει εδώ ο ποιητής; Το πεδίο αυτό ονομάζεται TOS, Type of Service και μπορούμε σε αυτό να ορίσουμε τι προτιμάμε κατά την επικοινωνία: Μεγαλύτερο ρυθμό μετάδοσης, όσο το δυνατόν καλύτερη αξιοπιστία ή τη μικρότερη δυνατή καθυστέρηση

- **Συνολικό Μήκος:** Δίνει το συνολικό μήκος του συγκεκριμένου IP πακέτου, στο οποίο περιλαμβάνεται τόσο η επικεφαλίδα όσο και τα δεδομένα. Έχουμε ήδη πει ότι το μέγιστο μέγεθος είναι 64 Kbytes = $64*1024 = 65536$ bytes. Ξέρουμε επίσης ότι η μικρότερη δυνατή επικεφαλίδα είναι 20 bytes. Άρα το μέγιστο μέγεθος για τα δεδομένα μας είναι $65536-20=65516$ bytes.
- **Χρόνος Ζωής:** Πρόκειται για ένα μετρητή που μειώνεται κατά 1 κάθε φορά που το πακέτο διέρχεται από ένα δρομολογητή. Όταν φτάσει την τιμή μηδέν, το πακέτο απορρίπτεται (το καταστρέφει ο δρομολογητής στον οποίο βρίσκεται εκείνη τη στιγμή). Με αυτό τον τρόπο αποφεύγεται να περιφέρονται στο δίκτυο “χαμένα” πακέτα που έχουν χάσει τον προορισμό τους και κάνουν κύκλους ή απλά έχουν καθυστερήσει πάρα πολύ να φτάσουν στον προορισμό τους λόγω λανθασμένης διαδρομής ή διεύθυνσης.
- **Αριθμός Πρωτοκόλλου:** Πρόκειται για ένα αριθμό που χαρακτηρίζει το πρωτόκολλο του επιπέδου μεταφοράς στο οποίο θα πρέπει το IP να παραδώσει το εισερχόμενο αυτοδύναμο πακέτο. Για παράδειγμα, αν αυτό το πεδίο έχει την τιμή 6, το πακέτο θα παραδοθεί στο πρωτόκολλο TCP. Η τιμή αυτή προφανώς έχει τεθεί κατά την αποστολή (από το επίπεδο μεταφοράς του αποστολέα, όταν παρέδωσε το τμήμα στο IP)

- **Άθροισμα Ελέγχου:** Επιτρέπει στο πρωτόκολλο IP στην απέναντι πλευρά (προορισμός) να ελέγξει την ορθότητα των δεδομένων της επικεφαλίδας. Αυτό είναι σημαντικό, καθώς η επικεφαλίδα τροποποιείται κάθε φορά που περνάει από κάποιο δρομολογητή αυξάνοντας έτσι την πιθανότητα να συμβεί κάποιο σφάλμα.
- **Διεύθυνση Πηγής:** Πρόκειται για τη διεύθυνση IP του υπολογιστή πηγής. Θα μιλήσουμε αναλυτικά για τις διευθύνσεις σε επόμενη ενότητα.
- **Διεύθυνση Προορισμού:** Πρόκειται για τη διεύθυνση IP του υπολογιστή προορισμού. Η διεύθυνση αυτή διαβάζεται από τους ενδιάμεσους δρομολογητές (ή τον αντίστοιχο δικτυακό εξοπλισμό) προκειμένου να προωθήσουν το πακέτο στον προορισμό του.
- **IP Επιλογές:** Χρησιμοποιείται για ειδικές λειτουργίες του πρωτοκόλλου.
- **Συμπλήρωση:** Χρησιμοποιείται ώστε το μέγεθος της επικεφαλίδας να είναι πάντα πολλαπλάσιο των 32 bits. (Στην πραγματικότητα ανήκει στις “IP Επιλογές”)

Παράδειγμα: Ας υποθέσουμε ότι έχουμε ένα αυτοδύναμο πακέτο με 1400 bytes δεδομένων και επικεφαλίδα μεγέθους 20 bytes, το οποίο πρέπει να μεταδοθεί μέσα από ένα δίκτυο που υποστηρίζει πακέτα συνολικού μεγέθους 620 bytes. Στο πακέτο αυτό η τιμή του πεδίου “Don’t Fragment” (DF) έχει την τιμή 0, άρα επιτρέπεται η διάσπαση του σε κομμάτια. Πόσα θα είναι αυτά τα κομμάτια, τι μέγεθος θα έχει το καθένα και ποιες θα είναι οι τιμές των πεδίων “MF” και “Δείκτης Εντοπισμού Τμήματος”;

Για να επιλύσουμε ένα τέτοιο πρόβλημα πρέπει να προσέξουμε κάποια από τα δεδομένα:

- Αν μας δίνουν το συνολικό μήκος των πακέτων ή το μήκος μόνο των δεδομένων. Εδώ μας δίνουν το μήκος των δεδομένων και της επικεφαλίδας χωριστά. Το Συνολικό Μέγεθος του πακέτου είναι 1420 bytes.
- Άν το πακέτο δεν έχει DF=0, δεν μπορεί να διασπαστεί!
- Αν το πακέτο χωράει μέσα στο δίκτυο στο οποίο θα μεταδοθεί δεν πρόκειται να διασπαστεί!
- Αν γίνει διάσπαση του πακέτου, το MF σε όλα τα fragments θα έχει τιμή 1 εκτός από το τελευταίο που θα έχει τιμή 0.
- Για το “Δείκτη Εντοπισμού Τμήματος” πρέπει να διαιρέσουμε με το 8 το συνολικό μέγεθος δεδομένων που έχει μεταδοθεί μέχρι στιγμής (χωρίς το fragment στο οποίο βρισκόμαστε αυτή τη στιγμή).

Στη συγκεκριμένη περίπτωση θα έχουμε:

- Το πρώτο fragment θα έχει μέγεθος 620 bytes. *Προσοχή:* Αυτό είναι το συνολικό μέγεθος του fragment. Κάθε κομμάτι έχει δική του επικεφαλίδα, άρα εδώ τα 600 bytes είναι δεδομένα και τα 20 bytes είναι επικεφαλίδα.
- Η τιμή του MF θα είναι 1. Ακολουθούν και άλλα κομμάτια.
- Ο Δείκτης Εντοπισμού Τμήματος θα έχει τιμή 0. Δεν έχουμε μεταδώσει τίποτα πριν από αυτό το κομμάτι.

Για το δεύτερο κομμάτι θα έχουμε:

- Το μέγεθος θα είναι ξανά 620 bytes. Από αυτά τα 600 bytes είναι δεδομένα και τα 20 bytes επικεφαλίδα.
- Η τιμή του MF θα είναι 1. Υπάρχει και άλλο κομμάτι μετά από αυτό.
- Συνολικά έχουμε μεταδώσει μέχρι στιγμής (χωρίς το συγκεκριμένο κομμάτι) 600 bytes δεδομένων. Ο Δείκτης Εντοπισμού Τμήματος θα έχει τιμή $600/8=75$.

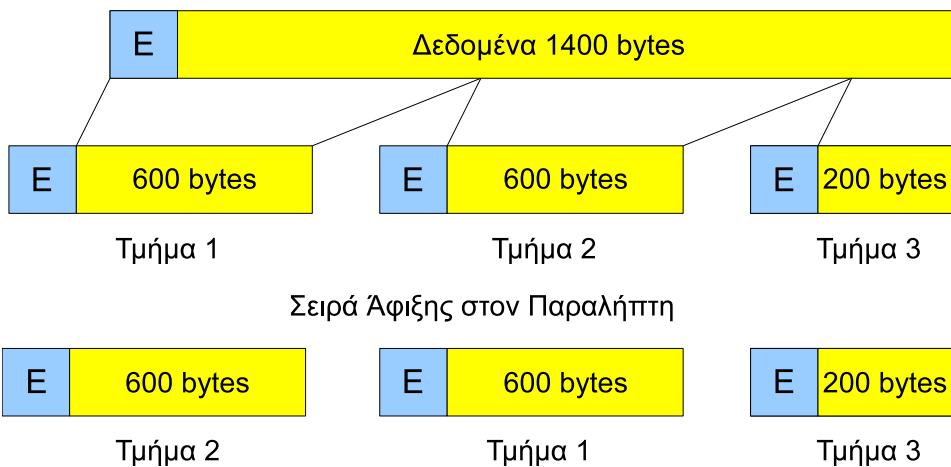
Για το τρίτο και τελευταίο κομμάτι έχουμε:

- Έχουν απομείνει ακόμα 200 bytes δεδομένων να μεταδώσουμε. Άρα το μέγεθος του τελευταίου κομματιού θα είναι 200 bytes δεδομένα + 20 bytes επικεφαλίδα = 220 bytes.
- Η τιμή του MF θα είναι 0. Πρόκειται για το τελευταίο κομμάτι του αρχικού πακέτου.
- Έχουμε μέχρι στιγμής μεταδώσει $600+600=1200$ bytes δεδομένων. Άρα η τιμή του πεδίου Δείκτης Εντοπισμού Τμήματος θα είναι $1200/8=150$

Τι άλλες πληροφορίες έχουμε για το πακέτο:

- Επικεφαλίδα 20 bytes σημαίνει $20*8=160$ bit. Αυτό σημαίνει ότι η τιμή του πεδίου “Μήκος Επικεφαλίδας” είναι 5 ($5 \times 32 = 160$).
- Τυπικά κάθε κομμάτι που προκύπτει θα έχει ίδιο μέγεθος επικεφαλίδας με το αρχικό πακέτο.
- Το πεδίο “Αναγνώριση” θα είναι το ίδιο για κάθε κομμάτι που έχει προκύψει από το ίδιο αρχικό IP πακέτο.
- Όταν τα κομμάτια φτάσουν τελικά στον προορισμό τους, είναι πιθανόν να έχουν διαφορετική τιμή στο πεδίο “Χρόνος Ζωής”. Η τιμή του συγκεκριμένου πεδίου μειώνεται κατά 1 κάθε φορά που περνάει το κομμάτι από κάποιο δρομολογητή. Καθώς τα πακέτα IP είναι αυτοδύναμα, είναι πιθανόν καθένα να ακολουθήσει διαφορετική διαδρομή.
- Οι διευθύνσεις πηγής και προορισμού παραμένουν στα κομμάτια ίδιες με αυτές στο αρχικό πακέτο.

- Εφόσον η επικεφαλίδα έχει μέγεθος 20 bytes, συμπεραίνουμε ότι δεν υπάρχουν IP επλογές και πεδίο συμπλήρωσης. Η επικεφαλίδα αποτελείται μόνο από το σταθερό τμήμα της.
- Το πεδίο “Αθροισμα Ελέγχου” θα είναι διαφορετικό σε κάθε κομμάτι. Αυτό συμβαίνει γιατί η επικεφαλίδα αλλάζει κάθε φορά που το κομμάτι διέρχεται από ένα δρομολογητή (αλλάζει ο Χρόνος Ζωής) και επίσης κάθε κομμάτι έχει διαφορετική τιμή στο Δείκτη Εντοπισμού Τμήματος (και το τελευταίο κομμάτι έχει MF=0).



Σχήμα 7.20: Διάσπαση σε Fragments και άφιξη στον προορισμό

Συναρμολόγηση του αρχικού πακέτου: Όταν τα κομμάτια φτάσουν στον υπολογιστή προορισμού, πρέπει να συναρμολογηθούν ξανά και να μας δώσουν το αρχικό πακέτο. Το πρόβλημα είναι ότι καθώς τα κομμάτια φτάνουν ενδεχομένως από διαφορετικές διαδρομές, είναι πιθανόν να φτάσουν με εντελώς λάθος σειρά. Για το παράδειγμα μας ας υποθέσουμε ότι τα πακέτα φτάνουν με την εξής σειρά: Πρώτα το δεύτερο, μετά το πρώτο και τελευταίο το τρίτο. Υποθέτουμε ακόμα ότι η τιμή του πεδίου αναγνώρισης είναι 100 (Σχήμα 7.20).

- Λαμβάνεται το δεύτερο κομμάτι. Το IP στον υπολογιστή προορισμού εξετάζει τις τιμές των πεδίων MF και Δείκτης Εντοπισμού Τμήματος. Επειδή το MF είναι 1, συμπεραίνει ότι το πακέτο δεν είναι αυτοδύναμο, αλλά κομμάτι κάποιου μεγαλύτερου πακέτου. Καθώς η τιμή στο Δείκτη Εντοπισμού Τμήματος δεν είναι 0 αλλά 75, δεν πρόκειται καν για το πρώτο κομμάτι αλλά για κάποιο ενδιάμεσο. Το κομμάτι αποθηκεύεται σε μια ενδιάμεση μνήμη μέχρι να φτάσουν τα υπόλοιπα.
- Λαμβάνεται το πρώτο κομμάτι. Το IP αντιλαμβάνεται ότι είναι το πρώτο κομμάτι, καθώς MF=1 και ο Δείκτης Εντοπισμού Τμήματος είναι μηδέν. Σε κάθε

περίπτωση το IP ελέγχει ότι κάθε ένα από τα κομμάτια έχει τον ίδιο αριθμό στο πεδίο αναγνώρισης (100) και έτσι ανήκουν όλα στο ίδιο αρχικό IP πακέτο. Το κομμάτι αποθηκεύεται επίσης στην ενδιάμεση μνήμη.

- Λαμβάνεται το τρίτο κομμάτι. Το IP αντιλαμβάνεται ότι πρόκειται για το τελευταίο κομμάτι καθώς ο Δείκτης Εντοπισμού Τμήματος δεν είναι μηδέν, αλλά το MF είναι 0.
 - Από τις τιμές των πεδίων Εντοπισμού Τμήματος το IP αντιλαμβάνεται ότι έχουν πλέον φτάσει όλα τα κομμάτια. Συναρμολογεί το αρχικό IP πακέτο και διαβάζει το πεδίο “Αριθμός Πρωτοκόλλου”. Η τιμή του πεδίου αυτού δείχνει ποιο πρωτόκολλο του επιπέδου μεταφοράς (π.χ. TCP, UDP) έχει δημιουργήσει το πακέτο. Το IP παραδίδει το έτοιμο πακέτο στο αντίστοιχο πρωτόκολλο του επιπέδου μεταφοράς.
-

7.6 Διεύθυνσιοδότηση

Η IP διεύθυνση προορισμού είναι αυτή που υποδεικνύει σε ένα σύστημα, που πρέπει να παραδώσει ένα IP αυτοδύναμο πακέτο. Εκτός από τη διεύθυνση, χρησιμοποιούμε συχνά και τους όρους “όνομα” και “διαδρομή” οι οποίοι σχετίζονται επίσης με τη διαδικασία παράδοσης.

- **Η διεύθυνση** προσδιορίζει που βρίσκεται μια συσκευή, συνήθως τη λογική ή φυσική θέση της σε ένα δίκτυο.
- **Το όνομα** μπορεί επίσης να προσδιορίζει μια συσκευή ή ένα δίκτυο και χρησιμοποιείται κυρίως για λόγους ευκολίας (είναι πιο εύκολο να θυμόμαστε ένα όνομα από μια σειρά αριθμών). Όταν χρησιμοποιούμε όνομα, γίνεται τελικά αντιστοίχιση του σε μια διεύθυνση με τη βοήθεια κατάλληλης υπηρεσίας που θα δούμε αργότερα (DNS).
- **Η διαδρομή** είναι το μονοπάτι που πρέπει να ακολουθήσει ένα αυτοδύναμο IP πακέτο για να φτάσει στον προορισμό του.

Μια συνηθισμένη διαδικασία είναι να προσδιορίσουμε τον παραλήπτη χρησιμοποιώντας ένα συμβολικό όνομα, το οποίο μετατρέπεται από το σύστημα στην αντίστοιχη IP διεύθυνση. Κατόπιν καθορίζεται η διαδρομή που πρέπει να ακολουθήσει ένα αυτοδύναμο πακέτο για να φτάσει στον προορισμό του.

7.6.1 Διεύθυνση Ελέγχου Πρόσβασης στο Μέσο (Media Access Control, Διεύθυνση MAC)

Κάθε συσκευή που επικοινωνεί σε ένα δίκτυο διαθέτει δύο διευθύνσεις: Η μία είναι η διεύθυνση IP η οποία αποδίδεται από το πρωτόκολλο δικτύου και η άλλη είναι η φυσική διεύθυνση γνωστή και ως διεύθυνση υλικού (*hardware address*).

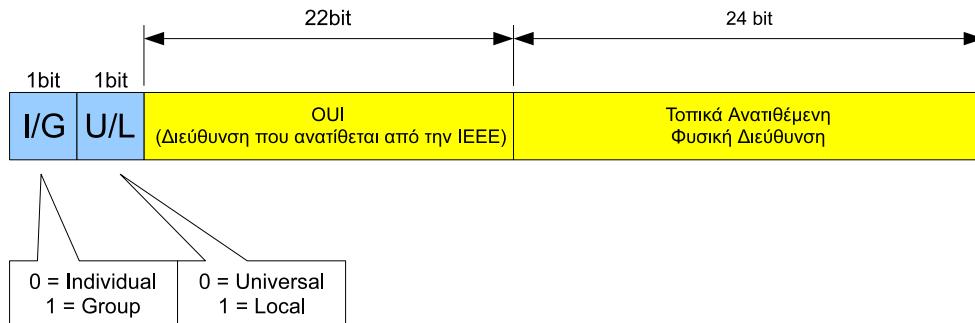
Οι φυσικές διευθύνσεις είναι μοναδικές, γιατί διαφορετικά δεν θα μπορούσαμε να προσδιορίσουμε τις συσκευές στο δίκτυο. Για παράδειγμα μια κάρτα δικτύου (που είναι από τις πλέον κοινές συσκευές σε ένα δίκτυο) διαθέτει μια φυσική διεύθυνση που της έχει αποδοθεί από τον κατασκευαστή της στο στάδιο της κατασκευής της. Σύμφωνα με το μοντέλο OSI, η φυσική διεύθυνση βρίσκεται στο υπο-επίπεδο πρόσβασης στο μέσο γνωστό και ως *Media Access Control*, για το λόγο αυτό ονομάζεται και διεύθυνση MAC.

Στο υπο-επίπεδο ελέγχου πρόσβασης στο μέσο, εκτελείται ανάλυση των εισερχόμενων πακέτων και ελέγχεται η MAC διεύθυνση τους. Αν η MAC διεύθυνση προορισμού αντιστοιχεί στην φυσική διεύθυνση της συσκευής που εκτελεί τον έλεγχο, τότε το πακέτο παραλαμβάνεται και προωθείται προς τα ανώτερα επίπεδα. Διαφορετικά, το πακέτο αγνοείται. Η ανάλυση αυτή στο χαμηλότερο επίπεδο του OSI μας απαλλάσσει από όσκοπες καθυστερήσεις που θα είχαμε αν έπρεπε να οδηγήσουμε κάθε πακέτο σε ανώτερο επίπεδο για να δούμε αν προορίζεται για τη συγκεκριμένη συσκευή (ελέγχοντας την IP διεύθυνση προορισμού).

Το μήκος της MAC διεύθυνσης προορισμού διαφέρει ανάλογα με το σύστημα (το πρωτόκολλο που χρησιμοποιείται στο φυσικό μέσο). Για παράδειγμα στα περισσότερα συστήματα (όπως το Ethernet) χρησιμοποιούνται διευθύνσεις μεγέθους 48 bits. Σε κάθε πακέτο αναγράφονται προφανώς τόσο η διεύθυνση του αποστολέα όσο και του παραλήπτη.

Προκειμένου να εξασφαλιστεί η μοναδικότητα των διευθύνσεων, η ανάθεση τους γίνεται από το *Instituto Hellenic of Electrical and Electronic Engineers*. Τα 24 πρώτα bits της διεύθυνσης MAC περιέχουν ένα μοναδικό για κάθε κατασκευαστή αναγνωριστικό αριθμό ο οποίος αποδίδεται σε αυτόν από το IEEE. Τα άλλα 24 bits μπορεί ο κάθε κατασκευαστής να τα χρησιμοποιήσει όπως θέλει (Σχήμα 7.21).

Τα πρώτα 24 bits είναι γνωστά με την ονομασία *tautóτητα οργανισμού*, OUI, *Organization Unique Identifier*. Το λιγότερο σημαντικό bit της διεύθυνσης (το πρώτο στο σχήμα) προσδιορίζει αν η διεύθυνση είναι ατομική ή ομαδική. Αν είναι 0 πρόκειται για ατομική (Individual) ενώ αν είναι για ομαδική (Group). Μια ομαδική διεύθυνση δεν προσδιορίζει ένα συγκεκριμένο μηχάνημα ή κάρτα δικτύου, αλλά ένα σύνολο διεύθυνσεων για το οποίο απαιτείται επιπλέον ανάλυση.



Σχήμα 7.21: Δομή Φυσικής Διεύθυνσης

Αν όλα τα ψηφία της OUI έχουν την τιμή 1, η διεύθυνση έχει ιδιαίτερη σημασία: Το πακέτο αυτό πρέπει να ληφθεί από όλους τους υπολογιστές του συγκεκριμένου συστήματος.

Το δεύτερο bit προσδιορίζει ποια αρχή έχει κάνει την ανάθεση της διεύθυνσης. Αν είναι 0, η διεύθυνση έχει αποδοθεί σε παγκόσμιο επίπεδο από την IEEE, αν είναι 1 έχει ανατεθεί τοπικά. Αυτό γίνεται για να προσδιορίζεται εύκολα αν μια διεύθυνση είναι πραγματικά μοναδική σε παγκόσμιο δίκτυο. Μια διεύθυνση που έχει ανατεθεί τοπικά μπορεί να είναι όμοια με μια που έχει ανατεθεί σε παγκόσμιο επίπεδο από την IEEE. Το bit αυτό κάνει το διαχωρισμό (χωρίς αυτό δεν θα μπορούσαμε να εξασφαλίσουμε τη μοναδικότητα των διευθύνσεων).

Τα επόμενα 22 bit συνθέτουν τη φυσική διεύθυνση υποδικτύου που ανατέθηκε από το IEEE στο συγκεκριμένο οργανισμό. Η δεύτερη ομάδα των 24 bit προσδιορίζουν διευθύνσεις τις οποίες διαχειρίζεται τοπικά ο οργανισμός. Οργανισμοί στους οποίους ανατίθενται από την IEEE διευθύνσεις υποδικτύου (OUI), είναι συνήθως οι κατασκευαστές καρτών δικτύου (π.χ. Ethernets) και δικτυακού υλικού. Κάθε τέτοια εταιρία προγραμματίζει σε κάθε κάρτα δικτύου που κυκλοφορεί στο εμπόριο ένα διαφορετικό αριθμό φυσικής διεύθυνσης στα δεύτερα 24 bit (στα πρώτα 24 χρησιμοποιείται το OUI που της έχει ανατεθεί). Αν εξαντλήσει όλη την δεύτερη περιοχή διευθύνσεων, μπορεί να ζητήσει από το IEEE και δεύτερο OUI.

7.6.2 IP Διευθύνσεις

Η τεχνολογία TCP/IP χρησιμοποιεί διευθύνσεις IP μεγέθους 32 bit. Μια διεύθυνση IP προσδιορίζει δύο πράγματα:

- Ένα τμήμα του δικτύου
- Ένα υπολογιστή που συνδέεται σε αυτό το τμήμα

Πρέπει να διευκρινίσουμε ότι η IP διεύθυνση προσδιορίζει στην πραγματικότητα τη σύνδεση (θέση) μιας συσκευής στο δίκτυο και όχι τη συσκευή σαν μηχάνημα. Αυτό σημαίνει για παράδειγμα ότι αν μετακινήσουμε ένα υπολογιστή από ένα τμήμα του δικτύου σε ένα άλλο, θα χρειαστεί να αλλάξουμε τη διεύθυνση του ώστε να ταιριάζει με το τμήμα προορισμού. Μπορούμε όμως να κρατήσουμε το ίδιο όνομα υπολογιστή (ενημερώνοντας κατάλληλα το DNS που θα δούμε παρακάτω).

Μια συσκευή μπορεί να έχει περισσότερες από μια διευθύνσεις IP αν ανήκει ταυτόχρονα σε πολλά διαφορετικά δίκτυα. Αυτό μπορεί να γίνει αν μια συσκευή διαθέτει για παράδειγμα περισσότερες από μια διεπαφές (κάρτες) δικτύου (αν και μπορεί να γίνει και με μία). Μια συνηθισμένη περίπτωση είναι οι δρομολογητές που διαθέτουν μια διεύθυνση δικτύου για καθένα από τα δίκτυα στα οποία είναι συνδεδεμένοι και δρομολογούν πακέτα.

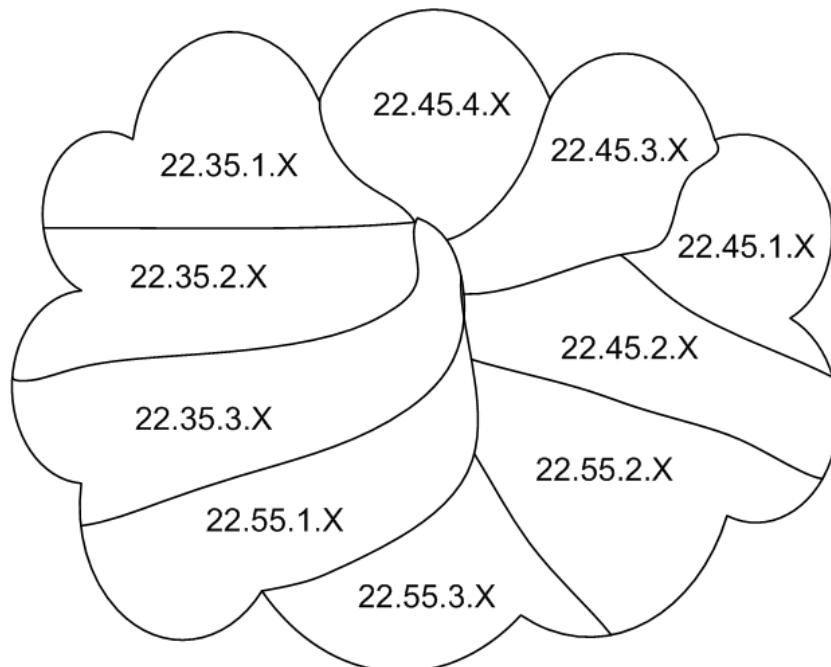
Παράδειγμα: Στο εργαστήριο μας, ο δρομολογητής που μας συνδέει με το Internet έχει δύο διευθύνσεις: Τη διεύθυνση 10.14.28.10 η οποία φαίνεται στο εσωτερικό μας δίκτυου Ethernet και τη διεύθυνση 81.186.52.182 με την οποία συνδέεται στο Internet μέσω του Πανελλήνιου Σχολικού Δικτύου.

Μια διεύθυνση IP χωρίζεται τυπικά σε δύο πεδία, το πεδίο δικτύου και το πεδίο υπολογιστή. Ουσιαστικά αυτό σημαίνει ότι έχουμε – όπως θα δούμε παρακάτω – συμφωνήσει ότι ένα μέρος των ψηφίων της διεύθυνσης χρησιμοποιείται για να αναγνωρίσει το τμήμα του δικτύου ή υποδίκτυο και το υπόλοιπο το συγκεκριμένο μηχάνημα (σχήμα 7.23). Με τον τρόπο αυτό, οι διευθύνσεις IP ακολουθούν ιεραρχική αρχιτεκτονική και αντανακλούν την εσωτερική ιεραρχική διαίρεση του δικτύου σε υποδίκτυα. Βλέποντας το σχήμα 7.22 παρατηρούμε μια ιεραρχία τριών επιπέδων:

- Ολόκληρο το δίκτυο αναγνωρίζεται από τον αριθμό 22.
- Έχει χωριστεί σε τρία υποδίκτυα, τα 35, 45 και 55.
- Καθένα από αυτά διαιρείται σε ακόμα μικρότερα υποδίκτυα που χαρακτηρίζονται από τον τρίτο αριθμό (1,2,3,4)
- Ο τελευταίος αριθμός που εδώ φαίνεται ως “X” χαρακτηρίζει τον υπολογιστή.

Όπως καταλαβαίνετε, στο συγκεκριμένο δίκτυο έχουμε αποφασίσει οι τρεις πρώτοι αριθμοί (octets) να χαρακτηρίζουν το δίκτυο και ο τελευταίος τον υπολογιστή.

Σημείωση: Οι αριθμοί αυτοί ονομάζονται οκτάδες ή octets και είναι η αναπαράσταση στο δεκαδικό σύστημα 8 δυαδικών ψηφίων δηλ. ενός byte. Αυτό σημαίνει ότι καθένας από τους αριθμούς αυτούς μπορεί να πάρει τιμές από το 0 ως το 255. Αν χρησιμοποιούμε (όπως στο παράδειγμα μας) τους τρεις πρώτους για την διεύθυνση



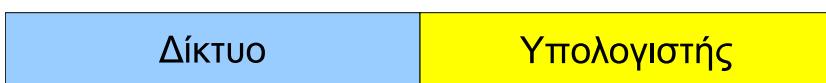
Σχήμα 7.22: Ιεραρχική διαίρεση δικτύου σε υποδίκτυα και χωρισμός διευθύνσεων σε υποδιευθύνσεις

του δικτύου και τον τέταρτο για τη διεύθυνση του υπολογιστή έχουμε την παρακάτω κατανομή ψηφίων για τη διεύθυνση IP:

- Τρία bytes για τη διεύθυνση δικτύου $= 3 * 8 = 24$ bits.
- Ένα byte για τη διεύθυνση του υπολογιστή $= 8$ bits

Να σημειώσουμε ότι το συνολικό μήκος της διεύθυνσης είναι 32 bits.

Όπως καταλαβαίνετε, είναι δυνατόν να χωρίσουμε τη διεύθυνση σε διαφορετικό σημείο ανάλογα με το αν θέλουμε να δημιουργήσουμε πολλά δίκτυα με λίγους υπολογιστές το καθένα (όπως στο παράδειγμα μας, όπου μπορούμε να έχουμε μέχρι 254 υπολογιστές) ή αν θέλουμε να δημιουργήσουμε ένα δίκτυο με πολλούς υπολογιστές.



Σχήμα 7.23: Δομή Διεύθυνσης IP

Όταν το δίκτυο μας είναι αυτόνομο και δεν συνδέεται (ή δεν είναι ορατό) στο δημόσιο Internet, έχουμε τη δυνατότητα να επιλέξουμε τις διευθύνσεις που θέλουμε και να χωρίσουμε τα υποδίκτυα μας όπως επιθυμούμε. Ωστόσο αν τα μηχανήματα μας είναι απευθείας προσβάσιμα στο Internet πρέπει με κάποιο τρόπο να εξασφαλιστεί ότι οι διευθύνσεις τους είναι μοναδικές και δεν χρησιμοποιούνται από κανένα άλλο υπολογιστή. Σε αντίθετη περίπτωση η σύνδεση μας θα δημιουργήσει σοβαρά προβλήματα στη λειτουργία του Διαδικτύου.

Για το σκοπό αυτό, η ανάθεση τέτοιων διευθύνσεων δεν γίνεται τυχαία αλλά έχει ανατεθεί στο *Κέντρο Πληροφορίας Δικτύου, Network Information Center, NIC* ή *InterNIC*. Όταν πρόκειται να συνδέουμε ένα δικό μας δίκτυο ή υπολογιστή απευθείας στο δίκτυο, το NIC θα μας δώσει τη διεύθυνση ή περιοχή διευθύνσεων που πρέπει να χρησιμοποιήσουμε εξασφαλίζοντας ταυτόχρονα ότι είναι μοναδική και δεν χρησιμοποιείται αλλού.

Σημείωση: Τι γίνεται με τους υπολογιστές στο σπίτι μας; Αν για παράδειγμα έχουμε μια σύνδεση ADSL, υπεύθυνος για τη διεύθυνση IP που έχουμε είναι ο παροχέας Internet (η εταιρία που μας συνδέει). Στην εταιρία αυτή έχει δοθεί από το NIC μια ή περισσότερες περιοχές διευθύνσεων και κάθε φορά που συνδεόμαστε, μας ανατίθεται μια διεύθυνση από αυτές. Κάθε φορά μπορεί να έχουμε διαφορετική διεύθυνση, αλλά σίγουρα τη στιγμή που τη χρησιμοποιούμε εμείς δεν την έχει κανείς άλλος.

Στην αρχική σχεδίαση του Διαδικτύου υπήρχε η αίσθηση ότι θα υπάρξουν πάρα πολλά δίκτυα. Η αρχική σκέψη ήταν να δεσμευτούν για το τμήμα δικτύου της διεύθυνσης 24 bits, ώστε να υπάρχουν διαθέσιμες διευθύνσεις για κάθε δίκτυο που θα δημιουργηθεί. Τα δίκτυα αυτά προβλέπονταν να είναι μικρά, υπήρχε όμως η εντύπωση ότι θα δημιουργηθούν και κάποια πολύ μεγάλα δίκτυα τα οποία ενδεχομένως να χρειάζονταν 24 bits για το τμήμα Υπολογιστή της διεύθυνσης για να μπορούν να περιλάβουν όλους τους υπολογιστές τους.

Με βάση τα παραπάνω φαίνεται ότι θα χρειαζόμασταν το συνολικό μήκος της διεύθυνσης IP να είναι $24 + 24 = 48$ bits. Οι σχεδιαστές όμως επιθυμούσαν να χρησιμοποιήσουν διευθύνσεις συνολικού μήκους 32 bits. Υποθέτοντας ότι τα περισσότερα δίκτυα θα είναι τελικά μικρά, δημιούργησαν τέσσερις διαφορετικές δομές διευθύνσεων (και μια πέμπτη που είναι δεσμευμένη για μελλοντική χρήση) οι οποίες χρησιμοποιούνται ανάλογα με το μέγεθος του δικτύου. Οι δομές αυτές κατατάσσουν τα δίκτυα σε τέσσερις κλάσεις, A, B, C και D (σχήμα 7.24). Τα πρώτα ψηφία κάθε κλάσης μας βοηθούν να καταλάβουμε απευθείας σε ποια κλάση ανήκει το συγκεκριμένο δίκτυο, με τον τρόπο που περιγράφεται παρακάτω.

- **Κλάση A:** Στην κλάση A το πρώτο ψηφίο είναι 0. Αυτό σημαίνει ότι το πρώτο octet έχει τιμές από 00000000 ως 01111111 δηλ. σε δεκαδικό από 0 ως 127.

A	0	Δίκτυο (7 bit)	Υπολογιστής (24 bit)
B	10	Δίκτυο (14 bit)	Υπολογιστής (16 bit)
C	110	Δίκτυο (21 bit)	Υπολογιστής (8 bit)
D	1110	Ομάδική Διεύθυνση (28 bit)	

Σχήμα 7.24: Κλάσεις IP Διευθύνσεων

Στην κλάση αυτή δεσμεύονται 7 bits για τη διεύθυνση δικτύου και τα υπόλοιπα 24 για τη διεύθυνση υπολογιστή. Η κλάση A προορίζεται για πολύ μεγάλα δίκτυα: Μπορούμε να δημιουργήσουμε 128 δίκτυα με περισσότερους από 16 εκατομμύρια υπολογιστές το καθένα.

- **Κλάση B:** Στην κλάση B τα δύο πρώτα ψηφία έχουν τιμή 10. Για το τμήμα Υπολογιστή χρησιμοποιούνται 16 bits (τα δυο τελευταία octets) ενώ για το τμήμα Δικτύου 14 bits. Με βάση το παραπάνω, το πρώτο octet θα έχει τιμές από 10000000 ως 10111111 δηλ. από 128 ως 191. Τα υπόλοιπα octets θα έχουν φυσικά τιμές από 0 ως 255. Η κλάση αυτή προορίζεται για τη δημιουργία δικτύων μεσαίου μεγέθους. Μπορούμε να δημιουργήσουμε 16384 δίκτυα με 65536 υπολογιστές το καθένα.
- **Κλάση C:** Στην κλάση C τα τρία πρώτα ψηφία είναι 110. Για το τμήμα του δικτύου χρησιμοποιούνται 21 bits, ενώ για το τμήμα υπολογιστή μόνο 8 bits. Αυτό σημαίνει ότι μπορούμε να έχουμε περίπου 2 εκατομμύρια δίκτυα με μέχρι 256 υπολογιστές το καθένα. Το πρώτο octet παίρνει τιμές από 11000000 ως 11011111 δηλ. από 192 ως 223. Τα υπόλοιπα octets θα έχουν φυσικά τιμές από 0 ως 255.
- **Κλάση D:** Η κλάση D έχει ειδικό σκοπό: Υποστηρίζει ομαδικές διευθύνσεις υπολογιστών (multicast). Οι διευθύνσεις αυτές δεν απευθύνονται σε ένα συγκεκριμένο μηχάνημα αλλά σε μια ομάδα μηχανημάτων και χρησιμοποιούνται για μεταδόσεις εκπομπής. Στην κλάση D τα τέσσερα πρώτα ψηφία του πρώτου octet έχουν την τιμή 1110.

Όπως έχουμε ήδη δει, τις IP διευθύνσεις τις γράφουμε σαν ομάδες των τεσσάρων αριθμών των 8 bits (octets ή οκτάδες) οι οποίες διαχωρίζονται μεταξύ τους με τελεία. Π.χ. μια διεύθυνση του εσωτερικού μας δικτύου στο σχολείο είναι:

10.14.28.32

Η γραφή αυτή μας εξυπηρετεί καθώς χρησιμοποιούμε δεκαδικό αντί για δυαδικό. Ανάλογα με την κλάση του δικτύου, κάθε οκτάδα μπορεί να αντιπροσωπεύει ένα τμήμα της διεύθυνσης δικτύου ή του Υπολογιστή. Για παράδειγμα στην κλάση A, μια διεύθυνση αντιπροσωπεύει:

Δίκτυο.Υπολογιστής.Υπολογιστής.Υπολογιστής

ενώ σε μια κλάση C, θα είναι:

Δίκτυο.Δίκτυο.Δίκτυο.Υπολογιστής

Για παράδειγμα, σε ένα δίκτυο κλάσης C ίσως υπάρχει η διεύθυνση 192.168.2.34. Το 192.168.2 αντιπροσωπεύει το δίκτυο, ενώ το 34 το συγκεκριμένο υπολογιστή. Από τη διεύθυνση είναι σχετικά εύκολο να εξάγουμε πληροφορίες σχετικά με το δίκτυο κάτι το οποίο μας διευκολύνει και στην αποτελεσματική δρομολόγηση των αυτοδύναμων πακέτων.

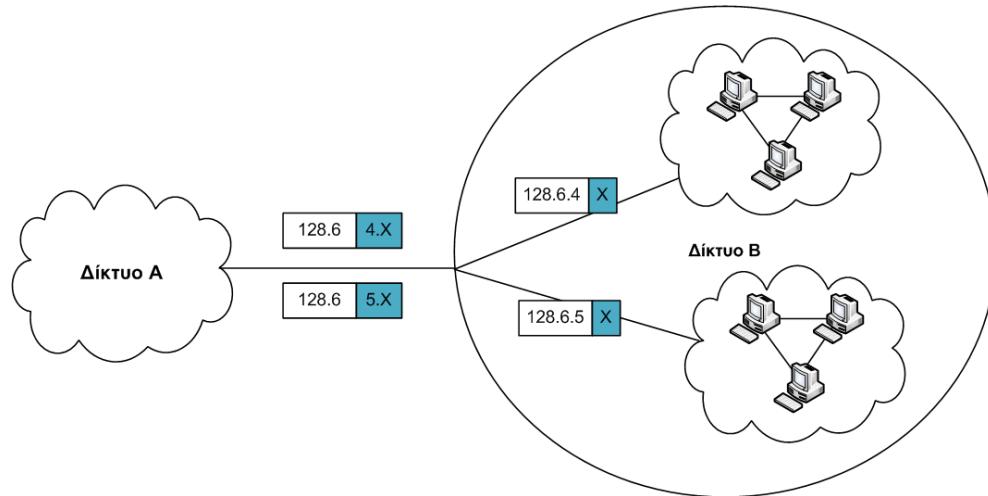
7.6.3 Υποδίκτυα και Μάσκα Υποδικτύου

Εταιρίες και οργανισμοί οι οποίοι διαθέτουν μεγάλα δίκτυα, προτιμούν να χωρίζουν τα δίκτυα τους σε επιμέρους υποδίκτυα (subnets) στα οποία για τους τελικούς υπολογιστές διατίθεται ένας μικρός αριθμός από bits.

Όπως είπαμε και στην προηγούμενη ενότητα, είναι δυνατόν να ορίσουμε πόσα ψηφία χρησιμοποιούνται για το πεδίο Δικτύου και πόσα για το πεδίο Υπολογιστή στη διεύθυνση IP. Η ρύθμιση γίνεται ανάλογα με τις ανάγκες, μας ώστε να μπορούμε να δημιουργήσουμε λίγα δίκτυα με πολλούς υπολογιστές ή πολλά δίκτυα με λίγους υπολογιστές. Για λόγους διαχείρισης είναι τις περισσότερες φορές πιο βολικό να έχουμε πολλά μικρότερα δίκτυα από ένα μεγάλο. Αυτό θα γίνει περισσότερο κατανοητό με το παρακάτω παράδειγμα:

Παράδειγμα: Ας υποθέσουμε ότι σε ένα μεγάλο οργανισμό ή εταιρία έχει ανατεθεί μια περιοχή διευθύνσεων δικτύου κλάσης B, η 128.6.X.X. Εσωτερικά, αυτός ο οργανισμός μπορεί να χωρίσει αυτή την περιοχή διευθύνσεων ώστε η τρίτη οκτάδα να δηλώνει ένα διαφορετικό υποδίκτυο. Για παράδειγμα, μπορεί το εσωτερικό δίκτυο να αποτελείται από δύο δίκτυα Ethernet. Στο ένα θα χρησιμοποιηθεί η περιοχή 128.6.5.X και στο άλλο η 128.6.4.X. Σε κάθε περίπτωση το πεδίο Υπολογιστή της διεύθυνσης θα αντιστοιχεί μόνο στην τελευταία οκτάδα (X). Ο διαχωρισμός αυτός έχει σημασία μόνο στο εσωτερικό δίκτυο του οργανισμού.

Οι υπολογιστές που βρίσκονται έξω από αυτό το δίκτυο (π.χ. στο Δίκτυο A του σχήματος 7.25) δεν χρειάζονται να γνωρίζουν κάτι για αυτό, αφού μπορούν να συνεχίσουν να δρομολογούν αυτοδύναμα πακέτα στο 128.6.X.X (χωρίς να κοιτάζουν την



Σχήμα 7.25: Εσωτερική οργάνωση δικτύου σε υποδίκτυα

τρίτη οκτάδα) και μάλιστα μέσα από τον ίδιο δρομολογητή. Στο εσωτερικό δίκτυο του οργανισμού, η διαχείριση των πακέτων αλλάζει: οι δρομολογητές του οργανισμού έχουν διαφορετικές εγγραφές για το δίκτυο 128.6.4 και το 128.6.5, με σκοπό να μπορούν πλέον να διαχωρίσουν και να δρομολογήσουν τα πακέτα προς το κατάλληλο υποδίκτυο. Οι δρομολογητές που βρίσκονται έξω από το δίκτυο δεν χρειάζεται να κάνουν αυτό το διαχωρισμό και έτσι έχουν μόνο μια εγγραφή που είναι κοινή για όλες τις διευθύνσεις 128.6.X.X.

Αν σκεφτούμε αυτό το παράδειγμα, είναι σαν να έχουμε πάρει ένα δίκτυο κλάσης B και να το έχουμε χωρίσει εσωτερικά σε μικρότερα υποδίκτυα κλάσης C. Κανονικά σε ένα δίκτυο κλάσης B, οι δύο τελευταίες οκτάδες χαρακτηρίζουν τον Υπολογιστή. Σε ένα δίκτυο κλάσης C όμως, μόνο η τελευταία οκτάδα χαρακτηρίζει τον Υπολογιστή. Εδώ ζητήσαμε από το NIC να μας αναθέσει μια περιοχή διευθύνσεων σε Class B, αλλά εσωτερικά αποφασίσαμε να χρησιμοποιήσουμε και την τρίτη οκτάδα για να δηλώσουμε το δίκτυο, διαιρώντας ουσιαστικά το δίκτυο Class B σε μικρότερα υποδίκτυα Class C.

Θα μπορούσαμε με την ίδια λογική αντί να ζητήσουμε ένα Class B δίκτυο από το NIC, να ζητήσουμε απευθείας περισσότερα από ένα Class C; Ναι. Αλλά αυτό θα έκανε πιο πολύπλοκη την επικοινωνία με εξωτερικά δίκτυα. Στην περίπτωση που έχουμε το διαχωρισμό εσωτερικά στον οργανισμό, οι εξωτερικοί δρομολογητές έχουν μια μοναδική εγγραφή για το δίκτυο μας, ενώ οι δικοί μας δρομολογητές έχουν περισσότερες και εκτελούν το διαχωρισμό μέσα στον οργανισμό. Αν ζητήσουμε περισσότερα από ένα Class C υποδίκτυα, θα έχουμε αναθέσει το διαχωρισμό σε δρομολογητές που βρίσκονται έξω από τον οργανισμό. Αυτό σημαίνει ότι οι δρο-

μολογητές έξω από το δίκτυο μας δεν θα μπορούν απλώς να δρομολογούν στο 128.6 αλλά θα πρέπει να γνωρίζουν το ακριβές μας υποδίκτυο, 128.6.4 ή 128.6.5. Κάτι τέτοιο σημαίνει φυσικά ότι θα έχουν και περισσότερες από μια καταχωρίσεις ειδικά για το συγκεκριμένο οργανισμό.

Μεταφέροντας αυτή την διαίρεση σε υποδίκτυα στο εσωτερικό του οργανισμού, κρύβουμε την πολυπλοκότητα (εσωτερική δομή) του δικού μας δικτύου από τον έξω κόσμο και απλοποιούμε κατά πολύ τις ρυθμίσεις των δρομολογητών που βρίσκονται έξω από το δίκτυο μας.

7.6.3.1 Μάσκα Υποδικτύου

Η μάσκα υποδικτύου (*subnet mask*) είναι ένας αριθμός με τον οποίο μπορούμε να καθορίσουμε με ακρίβεια πλέον ενός bit, ποια ψηφία μιας διεύθυνσης IP ανήκουν στο πεδίο Δικτύου και ποια στο πεδίο Υπολογιστή. Η μάσκα υποδικτύου έχει μέγεθος 32 bit και χωρίζεται σε οκτάδες όπως και η διεύθυνση IP.

Η σύμβαση που χρησιμοποιείται είναι η παρακάτω. Έστω ότι έχουμε τη διεύθυνση IP:

10.14.28.10

Τη γράφουμε παρακάτω με τη δυαδική της μορφή, ανά οκτάδα:

00001010.00001110.00011100.00001010

Ας υποθέσουμε ότι μας έχουν δώσει τον παρακάτω αριθμό ως μάσκα υποδικτύου:

255.255.255.0

Τον γράφουμε και αυτόν στη δυαδική του μορφή:

11111111.11111111.11111111.00000000

Βάζουμε τον ένα αριθμό κάτω από τον άλλο, και εκτελούμε τη λογική πράξη AND ανά ψηφίο. AND σημαίνει ότι το αποτέλεσμα θα είναι 1 μόνο αν KAI τα δύο ψηφία είναι 1:

00001010.00001110.00011100.00001010

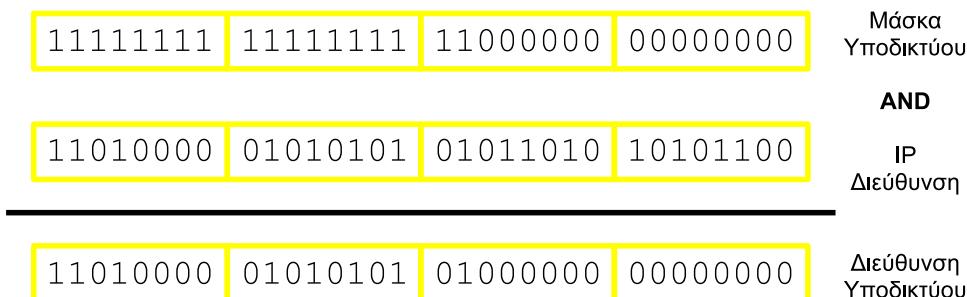
11111111.11111111.11111111.00000000

AND

00001010.00001110.00011100.00000000

Ο αριθμός που προκύπτει, αν τον μετατρέψουμε σε δεκαδικό ξανά είναι ο 10.14.28.0 και ονομάζεται Διεύθυνση Υποδικτύου.

Γενικά ένας εύκολος κανόνας είναι: Όπου τα ψηφία της μάσκας υποδικτύου είναι 1, τα αντίστοιχα ψηφία στη διεύθυνση IP ανήκουν στο πεδίο Δίκτυο. Όπου τα ψη-



Σχήμα 7.26: Χρήση Μάσκας Υποδικτύου

φία της μάσκας είναι 0, τα αντίστοιχα ψηφία της διεύθυνσης IP ανήκουν στο πεδίο Υπολογιστή. Δείτε και το παράδειγμα στο σχήμα 7.26.

Όπως και στην περίπτωση των φυσικών (MAC) διευθύνσεων, και στις IP διευθύνσεις αν θέσουμε όλα τα bits σε 1 (κάτι το οποίο αντιστοιχεί σε μια διεύθυνση 255.255.255.255 στο δεκαδικό) δηλώνουμε ότι θέλουμε να στείλουμε το μήνυμα μας σε όλους τους υπολογιστές του συγκεκριμένου δικτύου και μάλιστα άσχετα από το υποδίκτυο στο οποίο ανήκουν. Αν πάλι θέλουμε να στείλουμε το μήνυμα μας σε όλους τους υπολογιστές ενός συγκεκριμένου υποδικτύου χρησιμοποιούμε ως διεύθυνση τη διεύθυνση υποδικτύου θέτοντας σε 1 όλα τα ψηφία του πεδίου Υπολογιστή.

Χρησιμοποιώντας το προηγούμενο μας παράδειγμα: Έστω ότι θέλουμε να στείλουμε το μήνυμα σε όλους τους υπολογιστές του υποδικτύου 10.14.28.X. Έχουμε βρει ότι η διεύθυνση υποδικτύου είναι:

10 . 14 . 28 . 0

Στον παραπάνω αριθμό, το “0” αντιπροσωπεύει το τμήμα Υπολογιστή. Θα πρέπει να θέσουμε όλα τα ψηφία αυτού του αριθμού στο 1, άρα ο αριθμός που θα προκύψει θα είναι ο $11111111=255$. Για να στείλουμε το μήνυμα θα χρησιμοποιήσουμε τη διεύθυνση:

10 . 14 . 28 . 255

Αν είχαμε διεύθυνση IP 176.44.25.19 με μάσκα 255.255.0.0 τι διεύθυνση θα χρησιμοποιούσαμε για να στείλουμε το μήνυμα σε όλο το υποδίκτυο;

Τα τελευταία χρόνια έχει σημειωθεί μια εντυπωσιακή ανάπτυξη του Διαδικτύου (Internet). Αυτό είχε ως αποτέλεσμα να εμφανιστούν τα πρώτα προβλήματα, καθώς το πλήθος των διευθύνσεων που μπορούμε να γράψουμε με 32 bit είναι πε-

περασμένο (και στην πραγματικότητα έχουμε ήδη χρησιμοποιήσει το μεγαλύτερο μέρος). Καθώς τα δίκτυα που συνδέονται μεταξύ τους μέσω Διαδικτύου αυξάνονται, ο διαθέσιμος χώρος διευθύνσεων μειώνεται ενώ ταυτόχρονα μεγαλώνουν και γίνονται περισσότεροι πολύπλοκοι οι πίνακες δρομολόγησης.

Το πρόβλημα γίνεται ακόμα πιο έντονο καθώς μεγάλο μέρος των διευθύνσεων παραμένει αχρησιμοποίητο από τους οργανισμούς στους οποίους έχει ανατεθεί. Για παράδειγμα αν ένας οργανισμός χρειάζεται ένα δίκτυο με 70000 υπολογιστές, η κλάση B δεν τον καλύπτει, αλλά με την κλάση A περισσεύουν εκατομμύρια διευθύνσεις οι οποίες όμως δεσμεύονται και δεν μπορούν να χρησιμοποιηθούν κάπου αλλού. Το ίδιο συμβαίνει και αν θέλουμε να συνδέσουμε σε ένα δίκτυο 300 υπολογιστές. Η κλάση C δεν μας καλύπτει, ωστόσο στην κλάση B θα μείνουν αχρησιμοποίητες περισσότερες από 65000 διευθύνσεις!

Για να αντιμετωπιστούν τα παραπάνω προβλήματα, προτάθηκε η *Ανεξαρτήτου Κλάσεων Δρομολόγηση Υπερ-Περιοχών* (*Classless InterDomain Routing*) ή CIDR. Το σύστημα αυτό καταργεί εντελώς τις κλάσεις διευθύνσεων και μας επιτρέπει να καθορίσουμε με απόλυτη ακρίβεια πόσα ψηφία διατίθενται στο πεδίο Δίκτυο και πόσα στο πεδίο Υπολογιστή, ανάλογα με τις ανάγκες του οργανισμού. Για το σκοπό αυτό χρησιμοποιείται το σύστημα με την μάσκα υποδικτύου που είδαμε προηγουμένως.

Ένας σύντομος τρόπος για να δηλώσουμε το μέγεθος κάθε πεδίου (Δίκτυο/Υπολογιστής) της διεύθυνσης IP είναι χρησιμοποιώντας το *πρόθεμα*. Το πρόθεμα είναι ένας αριθμός που γράφουμε μετά τη διεύθυνση IP και δηλώνει από πόσα ψηφία αποτελείται η μάσκα δικτύου (ή υποδικτύου) κάθε διεύθυνσης. Για παράδειγμα, γράφοντας:

10.14.28.10/24

δηλώνουμε ότι η μάσκα δικτύου αποτελείται από 24 ψηφία. Με άλλα λόγια χρησιμοποιούνται 24 bit για το πεδίο δικτύου (δηλ. 3 bytes, άρα οι τρεις πρώτες οκτάδες) και μένουν 8 bit για το πεδίο Υπολογιστή. Αυτό αντιστοιχεί σε μια μάσκα δικτύου 255.255.255.0.

Δεν είναι απαραίτητο ωστόσο το πρόθεμα να διαιρείται ακριβώς με το 8. Θα μπορούσαμε να έχουμε το παρακάτω:

10.14.28.10/27

Αυτό σημαίνει ότι χρησιμοποιούμε 27 ψηφία για το πεδίο Δικτύου, άρα μας απομένουν 5 ψηφία για το πεδίο Υπολογιστή. Σε ένα τέτοιο δίκτυο θα μπορούσαμε να συνδέσουμε ένα μέγιστο 32 μηχανημάτων.

Το σύστημα CIDR επιτρέπει την ανάθεση μεγάλων συνεχόμενων περιοχών διευθύνσεων σε εταιρίες που παρέχουν υπηρεσίες Διαδικτύου (τους γνωστούς μας *ISP, Internet Service Providers*). Οι εταιρίες αυτές είναι έπειτα υπεύθυνες να αναθέσουν

μικρότερες περιοχές διευθύνσεων στους πελάτες τους ανάλογα με τις ανάγκες του καθενός. Με αυτό τον τρόπο επιτυγχάνεται η ομαδοποίηση των διευθύνσεων που εξυπηρετούνται από τον ίδιο ISP. Η ομαδοποίηση επιτρέπει τη δρομολόγηση της κίνησης προς το σωστό προορισμό, διατηρώντας μόνο μια εγγραφή για όλους τους προορισμούς (διευθύνσεις) που εξυπηρετούνται από τον ίδιο ISP.

Σημείωση: Μπορείτε να δείτε τη διεύθυνση IP και τη Μάσκα σε ένα μηχάνημα Windows μέσα από το εικονίδιο δικτύου του Πίνακα Ελέγχου. Επιλέξτε το πρωτόκολλο TCP/IP και πιέστε “Ιδιότητες”. Μπορείτε επίσης να δείτε τις ίδιες πληροφορίες στη γραμμή εντολών, γράφοντας:

```
ipconfig /all |more
```

Σε UNIX μηχανήματα μπορείτε να πάρετε αυτές τις πληροφορίες γράφοντας στη γραμμή εντολών:

```
ifconfig
```

7.7 Πρωτόκολλο ARP

Έχουμε πλέον μιλήσει και για τα δύο είδη διευθύνσεων:

- Τη φυσική (MAC) διεύθυνση που δίνει ο κατασκευαστής του δικτυακού υλικού στις συσκευές του (π.χ. στις κάρτες δικτύου). Η περιοχή διευθύνσεων που μπορεί να χρησιμοποιηθεί, αποδίδεται στον κατασκευαστή από το IEEE.
- Τη διεύθυνση IP που ανήκει στην τεχνολογία TCP/IP και αποδίδεται στις συσκευές του δικτύου από τον διαχειριστή του δικτύου. Αν το δίκτυο αυτό είναι απευθείας συνδεδεμένο με το δημόσιο Internet, οι διευθύνσεις αυτές υπαγορεύονται από το NIC, διαφορετικά ο διαχειριστής μπορεί να επιλέξει τις διευθύνσεις που τον εξυπηρετούν.

Το πρόβλημα που τίθεται πλέον είναι πως γίνεται η μετατροπή από το ένα είδος διεύθυνσης στην άλλη. Σε ένα περιβάλλον τοπικού δικτύου (συνήθως Ethernet) αυτό επιτυγχάνεται με το πρωτόκολλο ARP, *Address Resolution Protocol*, Πρωτόκολλο Μετατροπής Διεύθυνσης. Να σημειώσουμε εδώ ότι το ARP ανήκει στα πρωτόκολλα του χαμηλότερου επιπέδου (Σύνδεσης Δικτύου) στην ιεραρχία του TCP/IP.

Γιατί είναι σημαντικό το ARP; Σε ένα δίκτυο Ethernet, όλα τα μηχανήματα λαμβάνουν όλα τα μηνύματα, άσχετα με το που απευθύνονται (στο κλασικό Ethernet όλα

τα μηχανήματα μοιράζονται το ίδιο φυσικό μέσο). Κάθε μηχάνημα προφανώς πρέπει να επεξεργαστεί μόνο τα δεδομένα που απευθύνονται σε αυτό. Αν δεν υπήρχε το πρωτόκολλο ARP, το μηχάνημα θα έπρεπε να παραλάβει κάθε πακέτο από το φυσικό μέσο και να το επεξεργαστεί μέχρι το επίπεδο δικτύου για να διαπιστώσει αν η διεύθυνση IP προορισμού ταυτίζεται με τη δική του. Με τη βοήθεια του ARP, μπορεί να το διαπιστώσει άμεσα στο επίπεδο σύνδεσης δικτύου αποφεύγοντας έτσι περιττή επεξεργασία.

Το πρωτόκολλο ARP αναλαμβάνει να μετατρέψει μια IP διεύθυνση στην αντίστοιχη φυσική. Αυτό θα μπορούσαμε να το επιτύχουμε αποθηκεύοντας την αντιστοίχιση αυτή σε ένα πίνακα δύο στηλών (IP Διεύθυνση, Φυσική Διεύθυνση). Ωστόσο αν κάνουμε αυτή τη διαδικασία χειροκίνητα, σύντομα θα έχουμε μεγάλο πρόβλημα, ειδικά όταν προστίθενται νέες συσκευές (οπότε και θα απαιτείται ενημέρωση). Εννοείται ότι το πρόβλημα γίνεται ακόμα πιο έντονο σε μεγάλα δίκτυα.

Το πρωτόκολλο ARP κάνει ακριβώς αυτή την αντιστοίχιση από IP διεύθυνση στην φυσική και διατηρεί τον πίνακα τον οποίο συζητήσαμε παραπάνω αλλά δυναμικά. Αυτό σημαίνει ότι αναλαμβάνει να ανακαλύψει αρχικά ποια διεύθυνση IP αντιστοιχεί σε ποια διεύθυνση MAC αλλά και να ενημερώνει αυτές τις καταχωρίσεις όταν προστίθενται νέα μηχανήματα (ή όταν γίνεται αλλαγή διευθύνσεων σε υπάρχοντα). Κεντρικό στοιχείο στη λειτουργία του πρωτοκόλλου ARP είναι ο πίνακας δύο στηλών (IP Διεύθυνση, Φυσική Διεύθυνση). Κάθε γραμμή του πίνακα αντιστοιχεί σε μια εγγραφή δηλ. σε μια συσκευή. Ένα παράδειγμα ARP πίνακα φαίνεται παρακάτω:

IP Διεύθυνση	Ethernet Διεύθυνση
223.1.2.1	08-00-39-00-2F-C3
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

Όταν το πρωτόκολλο ARP λάβει μια διεύθυνση IP, αρχικά θα διερευνήσει τον πίνακα ARP για να δει αν υπάρχει η αντίστοιχη εγγραφή:

- Αν βρεθεί η εγγραφή στον πίνακα ARP, το πρωτόκολλο θα επιστρέψει την αντίστοιχη φυσική διεύθυνση που αναφέρει ο πίνακας.
- Αν δεν βρεθεί εγγραφή, το πρωτόκολλο θα δημιουργήσει μια αίτηση ARP. Η αίτηση αυτή είναι ένα μήνυμα το οποίο απευθύνεται σε όλα τα μηχανήματα του τοπικού δικτύου. Περιέχει την διεύθυνση IP του υπολογιστή προορισμού. Αν μια συσκευή στο δίκτυο αναγνωρίσει αυτή την IP ως δική της, θα στείλει τη φυσική της διεύθυνση ως απάντηση στη συσκευή που δημιούργησε την αίτηση.

Αμέσως μετά τη λήψη της απάντησης, η συσκευή που δημιούργησε την αίτηση θα ενημερώσει τον πίνακα ARP, δημιουργώντας μια νέα εγγραφή με τη διεύθυνση IP και τη φυσική διεύθυνση της συσκευής που μόλις έλαβε. Όταν χρειαστεί ξανά να βρει τη φυσική διεύθυνση αυτής της συσκευής, θα διαβάσει απλώς τον πίνακα και δεν θα χρειαστεί να δημιουργηθεί νέο αίτημα ARP.

Όπως είναι φυσικό, καθώς συνδέουμε και αφαιρούμε συσκευές από το δίκτυο, ο πίνακας ARP ενημερώνεται αυτόματα, καθώς στέλνονται νέες αιτήσεις και λαμβάνονται οι απαντήσεις τους. Η προσαρμογή έτσι επιτυγχάνεται αυτόματα και δυναμικά, χωρίς να απαιτείται επέμβαση από το διαχειριστή του δικτύου. Αν ο πίνακας ARP δεν υπήρχε, θα έπρεπε συνέχεια να στέλνονται αιτήσεις (ακόμα και για διευθύνσεις που έχουν διευκρινιστεί στο παρελθόν). Κάτι τέτοιο θα αύξανε την κίνηση στο δίκτυο και θα είχε επιπτώσεις στην απόδοση του. Μπορεί ωστόσο να χρησιμοποιηθεί σε κάποια απλά δίκτυα, και ειδικά αν ο αριθμός των συνδεδεμένων υπολογιστών είναι μικρός οπότε η αύξηση της κίνησης δεν είναι σημαντική.

Όταν συνδέουμε μια νέα συσκευή στο δίκτυο, αυτή ενδεχομένως δεν διαθέτει ακόμα IP διεύθυνση. Ένα μειονέκτημα του πρωτοκόλλου ARP είναι ότι δεν προβλέπει κάποιο είδος μηνύματος με το οποίο μια τέτοια συσκευή να δημιουργεί αίτηση για να της χορηγηθεί IP. Στην περίπτωση αυτή η συσκευή γνωρίζει μόνο τη φυσική της διεύθυνση. Μια λύση σε αυτό το πρόβλημα δίνεται από το πρωτόκολλο *RARP*, *Reverse Address Resolution Protocol*, Πρωτόκολλο Αντίστροφης Μετατροπής Διεύθυνσης το οποίο κάνει την αντίστροφη δουλειά από το ARP. Δημιουργεί δηλ. ένα αίτημα στο οποίο δίνεται η φυσική διεύθυνση και περιμένει ως απάντηση την αντίστοιχη IP διεύθυνση. Το αίτημα αυτό απευθύνεται (όπως και το ARP) σε όλες τις συσκευές του δικτύου, αλλά μπορεί να απαντηθεί μόνο από συγκεκριμένες συσκευές που ονομάζονται εξυπηρετητές *RARP*.

Τι θέλει να πει εδώ ο πουλτής; Τι εννοεί λέγοντας ότι μια νέα συσκευή δεν γνωρίζει την IP διεύθυνση της; Μα προηγουμένως λέγαμε ότι ο διαχειριστής ή / και το NIC είναι υπεύθυνα για να δίνουν IP διευθύνσεις στα μηχανήματα!

Η πραγματικότητα είναι η εξής: Σε πολλά τοπικά δίκτυα, η σύνδεση στο Internet γίνεται μέσω μόνος σημείου (π.χ. στο εργαστήριο του σχολείου γίνεται μέσω του ADSL δρομολογητή). Το σημείο αυτό είναι και το μόνο που φαίνεται άμεσα στο Internet. Όλες οι διευθύνσεις του εσωτερικού δικτύου μπορούν να αποδοθούν από τον τοπικό διαχειριστή όπως αυτός θέλει. Υπάρχουν δύο τρόποι για να γίνει αυτό:

- Να διθούν στατικές διευθύνσεις. Δηλ. ο διαχειριστής να πάει σε ένα-ένα τα μηχανήματα του δικτύου και να ρυθμίσει χειροκίνητα την κατάλληλη διεύθυνση, προσέχοντας να μη δώσει την ίδια διεύθυνση παραπάνω από μια φορά.

- Να χρησιμοποιήσει κάποιο σύστημα το οποίο κάθε φορά που συνδέεται ένα νέο μηχάνημα, να του αποδίδεται αυτόματα μια διεύθυνση IP. Προφανώς το σύστημα αυτό θα φροντίζει να δίνει διαφορετικές διευθύνσεις σε διαφορετικά μηχανήματα αλλά και να ανανεώνει τον αντίστοιχο ARP πίνακα. Ο διαχειριστής θα πρέπει να καθορίσει από πριν μια περιοχή έγκυρων διευθύνσεων, από τις οποίες θα δίνεται κάθε φορά ένα νέο IP.

Ένα τέτοιο σύστημα είναι το RARP. Το νέο σύστημα το οποίο δεν έχει IP διεύθυνση, δημιουργεί ένα ερώτημα RARP το οποίο αποστέλλεται σε ολόκληρο το δίκτυο (υποχρεωτικά: δεν μπορεί να σταλεί σε συγκεκριμένο μηχάνημα χωρίς να έχουμε IP διεύθυνση!). Το μήνυμα αυτό λαμβάνεται από τον κατάλληλο εξυπηρετητή ARP ο οποίος στέλνει ως απάντηση την IP διεύθυνση που θα πρέπει να χρησιμοποιήσει το μηχάνημα.

Στην πραγματικότητα, σήμερα το RARP δεν χρησιμοποιείται πλέον. Αντικαταστάθηκε από τα πρωτόκολλα BOOTP και το πιο καινούριο DHCP το οποίο εκτελεί αντίστοιχες λειτουργίες, αλλά μπορεί να στείλει (εκτός από τη διεύθυνση IP) και άλλες παραμέτρους λειτουργίας στο νέο μηχάνημα.

Παράδειγμα: Ας υποθέσουμε ότι ένα σύστημα με διεύθυνση IP 128.6.4.194 θέλει να συνδεθεί με το 128.6.4.7:

- Το σύστημα θα ελέγξει αρχικά αν το 128.6.4.194 βρίσκεται στο ίδιο δίκτυο με το 128.6.4.7 για να προσδιοριστεί αν μπορούν να επικοινωνήσουν απευθείας μέσω του τοπικού δικτύου (Ethernet). Προφανώς αυτό συμβαίνει στη συγκεκριμένη περίπτωση (παρατηρήστε ότι αλλάζει μόνο η τελευταία οκτάδα).
- Το σύστημα θα ψάξει στον πίνακα ARP για να δει αν υπάρχει καταχωρημένη η διεύθυνση 128.6.4.7. Αν υπάρχει θα ανακτήσει από εκεί απευθείας την φυσική διεύθυνση.
- Αν δεν υπάρχει καταχώριση για το 128.6.4.7 στον πίνακα ARP, θα πρέπει να προσδιοριστεί η φυσική διεύθυνση του συστήματος πριν γίνει αποστολή του πακέτου. Δημιουργείται μια αίτηση ARP με το ερώτημα “Χρειάζομαι την Ethernet διεύθυνση του 128.6.4.7”. Το αίτημα λαμβάνεται από όλους τους υπολογιστές του τοπικού δικτύου και θα απαντηθεί από την συσκευή που αναγνωρίζει αυτή τη διεύθυνση ως δική της με μια απάντηση του τύπου “Η φυσική διεύθυνση του 128.6.4.7 είναι 08:00:20:01:56:34” (Οι φυσικές διεύθυνσεις στο Ethernet είναι 48 bit, δηλ. 6 οκτάδες).
- Έχοντας πλέον και τη φυσική διεύθυνση, ο υπολογιστής 128.6.4.194 μπορεί να στείλει το πακέτο στον 128.6.4.7.

Όταν μια ARP εγγραφή δεν έχει χρησιμοποιηθεί για μεγάλο χρονικό διάστημα, στα περισσότερα συστήματα διαγράφεται αυτόματα.

Ο πίνακας ARP είναι αναγκαίος, καθώς δεν υπάρχει κάποια σύνδεση μεταξύ της IP διεύθυνσης και της φυσικής (δεν υπάρχει δηλ. αλγόριθμος ή τρόπος υπολογισμού που να δίνουμε την μία και να μας υπολογίζει την άλλη – το IP το δίνει ο διαχειριστής του δικτύου με βάση την περιοχή που του έχει αποδοθεί από το NIC, η φυσική διεύθυνση δίνεται από τον κατασκευαστή του δικτυακού υλικού με βάση την περιοχή διευθύνσεων που του έχει ανατεθεί από το IEEE).

Ας υποθέσουμε ότι μια εφαρμογή δικτύου (π.χ. απομακρυσμένη πρόσβαση, Telnet) θέλει να συνδεθεί με ένα απομακρυσμένο υπολογιστή. Για να γίνει αυτό θα πρέπει να δημιουργηθεί μια TCP σύνδεση μεταξύ των δύο υπολογιστών (το telnet βασίζεται σε σύνδεση TCP). Τα δεδομένα του TCP θα μεταφερθούν στο επίπεδο δικτύου και θα παραληφθούν από το πρωτόκολλο IP για να μετατραπούν σε αυτοδύναμα IP πακέτα. Στο σημείο αυτό, θα πρέπει να προσδιοριστεί και η φυσική (Ethernet) διεύθυνση προορισμού.

Αν η πληροφορία δεν είναι άμεσα διαθέσιμη μέσω του πίνακα ARP, το πακέτο IP θα τοποθετηθεί σε μια ουρά αναμονής και θα δημιουργηθεί το αίτημα ARP (παράδειγμα στο σχήμα 7.27). Στο αίτημα αυτό είναι συμπληρωμένα τα πεδία του αποστολέα και του προορισμού εκτός από την “Ethernet διεύθυνση προορισμού”. Το αίτημα θα ληφθεί από όλα τα μηχανήματα του τοπικού δικτύου. Ο υπολογιστής που θα αναγνωρίσει την διεύθυνση του, θα δημιουργήσει την ARP απάντηση στην οποία τα πεδία αποστολέα και προορισμού είναι αντεστραμμένα σε σχέση με την αίτηση και περιέχει την φυσική διεύθυνση που ζητήθηκε. Η απάντηση θα ληφθεί από τον υπολογιστή που έστειλε την αίτηση. Η ARP μονάδα του εξετάζει την απάντηση και καταχωρεί την διεύθυνση IP και τη φυσική διεύθυνση στον πίνακα ARP, δημιουργώντας έτσι δυναμικά μια νέα εγγραφή. Το πακέτο IP βγαίνει από την ουρά αναμονής, η διεύθυνση IP του μετατρέπεται στη γνωστή πλέον φυσική (Ethernet) διεύθυνση από τον ενημερωμένο ARP πίνακα, σχηματίζεται το πλαίσιο Ethernet και διαβιβάζεται στο δίκτυο.

Συνοψίζοντας, θα γίνουν οι παρακάτω ενέργειες:

- Δημιουργείται η ARP ερώτηση.
- Το IP αυτοδύναμο πακέτο μπαίνει σε ουρά αναμονής.
- Λαμβάνεται η ARP απάντηση και καταχωρείται μια νέα εγγραφή στον πίνακα ARP.
- Με βάση τον ενημερωμένο πίνακα, μετατρέπεται η διεύθυνση IP στην αντίστοιχη Ethernet.

ARP Αίτηση

IP Διεύθυνση Αποστολέα	223.1.2.1
Ethernet Διεύθυνση Αποστολέα	08:00:39:00:2F:C3
IP Διεύθυνση Προορισμού	223.1.2.2
Ethernet Διεύθυνση Προορισμού	<Κενό>

ARP Απάντηση

IP Διεύθυνση Αποστολέα	223.1.2.2
Ethernet Διεύθυνση Αποστολέα	08:00:28:00:38:A9
IP Διεύθυνση Προορισμού	223.1.2.1
Ethernet Διεύθυνση Προορισμού	08:00:39:00:2F:C3

Σχήμα 7.27: ARP Αίτηση και Απάντηση

- Το αυτοδύναμο IP πακέτο βγαίνει από την ουρά αναμονής, σχηματίζεται ένα πλαίσιο Ethernet και αποστέλλεται στο δίκτυο.

Αν κανείς υπολογιστής του δικτύου δεν απαντήσει στην αίτηση ARP, δεν θα υπάρξει εγγραφή στον πίνακα ARP και το πρωτόκολλο IP θα απορρίψει το αυτοδύναμο IP πακέτο που βρίσκεται στην ουρά αναμονής.

7.8 Σύστημα Ονομάτων Περιοχών, Domain Name System (DNS)

Όπως έχουμε ήδη αναφέρει, ο κύριος τρόπος αναγνώρισης ενός υπολογιστή στο δίκτυο είναι η IP διεύθυνση του. Θυμάστε ότι η διεύθυνση IP έχει μέγεθος 32 bit και τυπικά την γράφουμε με τη μορφή τεσσάρων δεκαδικών αριθμών (των οκτάδων ή octets) τα οποία χωρίζονται μεταξύ τους με τελείες. Για παράδειγμα μια έγκυρη διεύθυνση IP είναι:

94 . 69 . 78 . 90

Οι χρήστες όμως βρίσκουν αρκετά δύσκολο να απομνημονεύσουν αυτούς τους αριθμούς προκειμένου να τους χρησιμοποιήσουν για να μπορέσουν π.χ. να συνδεθούν σε ένα υπολογιστή. Για το σκοπό αυτό, κρίθηκε σκόπιμο να χρησιμοποιούνται στους υπολογιστές συμβολικά ονόματα.

Παράδειγμα: Το κεντρικό μηχάνημα του εργαστηρίου μας έχει την διεύθυνση:

10.14.28.10

Μπορείτε όμως να αναφερθείτε σε αυτό και με το συμβολικό του ονόμα, το οποίο είναι:

aquarius64.lab1.local

Με τον ίδιο τρόπο και τα υπόλοιπα μηχανήματα του δικτύου διαθέτουν ονόματα όπως PC1, PC2, PC3...

Είναι ελπίζουμε προφανές, ότι όταν χρησιμοποιούμε το ονόμα για να αναφερθούμε σε ένα υπολογιστή αυτό με κάποιο τρόπο μετατρέπεται στην διεύθυνση IP του υπολογιστή. Για το σκοπό αυτό χρησιμοποιείται το σύστημα DNS για το οποίο θα μιλήσουμε.

Όπως έχουμε πει, μια διεύθυνση IP χαρακτηρίζει κατά βάση τη θέση ενός υπολογιστή στο δίκτυο. Έτσι αν μετακινήσουμε τον υπολογιστή σε άλλο δίκτυο θα πρέπει να αλλάξουμε και τη διεύθυνση του. Το ονόμα ωστόσο χαρακτηρίζει τον ίδιο τον υπολογιστή, προσφέροντας ένα αναγνωριστικό στοιχείο που τον ξεχωρίζει από άλλους υπολογιστές του δικτύου. Το ονόμα δεν χρειάζεται να αλλάξει όταν αλλάξουμε τη θέση του υπολογιστή ή το IP του. Προφανώς βέβαια θα αλλάξει η διεύθυνση IP που αντιστοιχεί στο ονόμα του.

Καθώς ένας υπολογιστής μπορεί να έχει περισσότερες από μια IP διευθύνσεις (αν είναι συνδεδεμένος σε πολλαπλά δίκτυα για παράδειγμα), με τον ίδιο τρόπο μπορεί να έχει και περισσότερα από ένα ονόματα, το καθένα να αντιστοιχεί και σε μια IP.

Οι χρήστες μπορούν επίσης να αναφέρονται με ονόματα όχι μόνο σε συγκεκριμένες συσκευές (υπολογιστές) αλλά σε ολόκληρα δίκτυα. Τα ονόματα των υπολογιστών είναι συνήθως περιγραφικά ώστε να μπορεί ο υπολογιστής να αναγνωρίζεται εύκολα μέσα στο δίκτυο, αλλά τα ονόματα των δικτύων αντικατοπτρίζουν συνήθως το ονόμα του οργανισμού ή της εταιρίας στην οποία ανήκουν. Σε μεγάλα δίκτυα, τα ονόματα των ατομικών υπολογιστών είναι συνήθως συμβολικά και προκύπτουν κωδικοποιώντας δεδομένα όπως τον τύπο της συσκευής, τη θέση της, το σκοπό που εξυπηρετεί (τη χρήση της).

Παράδειγμα: Σε μια μεγάλη εταιρία, ο πρώτος υπολογιστής του λογιστηρίου θα μπορούσε να ονομαστεί π.χ:

accounting - pc01

Το όνομα δηλώνει:

- Τη θέση του και το σκοπό του (accounting, λογιστήριο)
- Το είδος της συσκευής (pc, προσωπικός υπολογιστής)
- Έναν αριθμό (01) που τον ξεχωρίζει από άλλους υπολογιστές που βρίσκονται στο λογιστήριο.

Ισως το χαρακτηριστικό “pc” να φαίνεται περιττό, αλλά φανταστείτε ότι στο ίδιο τμήμα του δικτύου (λογιστήριο) μπορεί να υπάρχουν δικτυακές συσκευές ορατές στο δίκτυο, οι οποίες ωστόσο δεν είναι υπολογιστές. Για παράδειγμα ένας δικτυακός εκτυπωτής στον ίδιο χώρο θα μπορούσε να ονομάζεται:

accounting - lpr01

(Το lpr προκύπτει από τα αρχικά line printer, εκτυπωτής γραμμής)

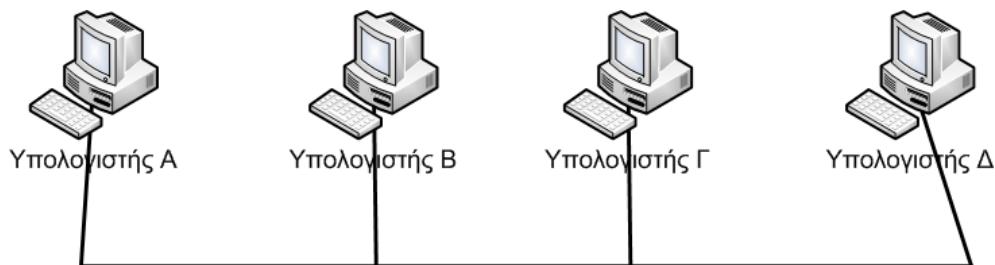
Τα ονόματα που χρησιμοποιούνται σε αυτές τις περιπτώσεις μπορεί να είναι εύκολα κατανοητά από τους ανθρώπους που χρησιμοποιούν το δίκτυο καθημερινά στην εργασία τους, αλλά πιθανόν να μην σημαίνουν κάτι το ιδιαίτερο για κάποιον τρίτο.

Σε κάθε περίπτωση, για να επικοινωνήσουμε με κάποια απομακρυσμένη συσκευή είναι απαραίτητο να χρησιμοποιήσουμε την διεύθυνση IP της. Όταν χρησιμοποιούμε το όνομα της (το οποίο είναι πιο εύκολο να το θυμόμαστε), πρέπει με κάποιο τρόπο να γίνει η μετατροπή του στην αντίστοιχη IP διεύθυνση.

Ένας απλός τρόπος να γίνει αυτό είναι κάθε υπολογιστής να διαθέτει ένα αρχείο το οποίο να περιέχει την αντιστοιχία συμβολικών ονομάτων και IP διευθύνσεων. Για να δουλέψει αυτό το σύστημα, θα πρέπει αυτό το αρχείο να περιέχει τα ονόματα και τις διευθύνσεις όλων των υπολογιστών του δικτύου, να υπάρχει σε όλους τους υπολογιστές και να διατηρείται ενημερωμένο όταν γίνονται αλλαγές.

Ο υπολογιστής που ξεκινάει μια αποστολή δεδομένων, θα ψάξει μέσα σε αυτό το αρχείο να βρει το όνομα του υπολογιστή προορισμού και από την ίδια γραμμή θα διαβάσει την διεύθυνση IP που πρέπει να χρησιμοποιήσει.

Θεωρείστε για παράδειγμα ότι έχουμε το απλό δίκτυο του σχήματος 7.28. Εστω ότι οι υπολογιστές έχουν τα συμβολικά ονόματα A, B, Γ, Δ (Φυσικά σε ένα κανονικό δίκτυο χρησιμοποιούμε πιο περιγραφικά ονόματα). Ένα παράδειγμα αρχείου που αντιστοιχεί τα ονόματα σε διευθύνσεις μπορεί να είναι το παρακάτω:



Σχήμα 7.28: *TCP/IP Δίκτυο Τεσσάρων Υπολογιστών*

Διεύθυνση	Όνομα
192.168.0.1	A
192.168.0.2	B
192.168.0.3	Γ
192.168.0.4	Δ

Στον παραπάνω πίνακα, η πρώτη στήλη δίνει τη διεύθυνση και η δεύτερη το όνομα που αντιστοιχεί.

Όταν ο υπολογιστής A θέλει να επικοινωνήσει με τον υπολογιστή Γ, θα ψάξει χρησιμοποιώντας ως κλειδί το “A” σε αυτό το αρχείο και θα βρει ότι αντιστοιχεί στο 192.168.0.3. Από κει και πέρα το όνομα πλέον δεν χρειάζεται: Θα χρησιμοποιηθεί η διεύθυνση IP που βρέθηκε.

Σημείωση: Στα περισσότερα λειτουργικά συστήματα το αρχείο αυτό ονομάζεται `hosts`. Για παράδειγμα, στο μηχάνημα του εργαστηρίου μας το αρχείο `hosts` μοιάζει με το παρακάτω:

127.0.0.1	localhost	localhost.lab1.local
10.14.28.10	aquarius64	lab1.local aquarius64
10.14.28.11	PC1	lab1.local PC1
10.14.28.12	PC2	lab1.local PC2
10.14.28.13	PC3	lab1.local PC3
10.14.28.14	PC4	lab1.local PC4

Σε κάθε διεύθυνση IP μπορούν να αντιστοιχίζονται περισσότερα από ένα ονόματα τα οποία απλώς τοποθετούνται το ένα δίπλα από το άλλο.

Η τοποθεσία του αρχείου `hosts` είναι διαφορετική από λειτουργικό σε λειτουργικό. Για παράδειγμα, σε μηχανήματα Windows θα το βρείτε στη θέση:

`C:\Windows\System32\Drivers\etc\hosts`

Σε μηχανήματα με λειτουργικά τύπου UNIX θα το βρείτε στη θέση:

`\etc\hosts`

Η μορφή του είναι πάντως η ίδια.

Η μέθοδος αυτή με το αρχείο αντιστοίχισης διευθύνσεων – ονομάτων δουλεύει καλά όταν το δίκτυο είναι μικρό. Τα βασικά προβλήματα για να το χρησιμοποιήσουμε σε ένα μεγάλο δίκτυο είναι:

- Κάθε υπολογιστής του δικτύου πρέπει να έχει ένα αντίγραφο αυτού του αρχείου.
- Το αρχείο πρέπει να διατηρείται ενημερωμένο κάθε φορά που γίνεται κάποια αλλαγή στο δίκτυο. Για παράδειγμα όταν προσθέτουμε ή αφαιρούμε ένα υπολογιστή, ή όταν αλλάζουμε ένα όνομα ή διεύθυνση. Επίσης πρέπει να κρατάμε ενημερωμένα όλα τα αντίγραφα του αρχείου.
- Αν το πλήθος των υπολογιστών είναι μεγάλο, η αναζήτηση σε ένα απλό αρχείο κειμένου (ASCII) θα είναι πολύ αργή. Επίσης ενδέχεται να ξεπεράσουμε το μέγιστο μέγεθος αρχείου. Σε κάθε περίπτωση θα σπαταλήσουμε πολύ χρόνο και κόπο για να ενημερώσουμε όλα τα αντίγραφα.

Γνωρίζετε όμως ότι μπορούμε να κάνουμε εύκολες και γρήγορες αναζητήσεις σε δεδομένα, αν τα αποθηκεύσουμε με κατάλληλο τρόπο σε μια βάση δεδομένων. Η λύση του παραπάνω προβλήματος δόθηκε με την ανάπτυξη του *Συστήματος Ονομάτων Περιοχών* ή *DNS, Domain Name System*. Το DNS είναι ένας μηχανισμός απεικόνισης διευθύνσεων σε ονόματα και το αντίστροφο. Το DNS περιέχει ένα χώρο ονομάτων **οργανωμένο ιεραρχικά** και η λειτουργία του βασίζεται σε μια **κατανεμημένη** βάση δεδομένων.

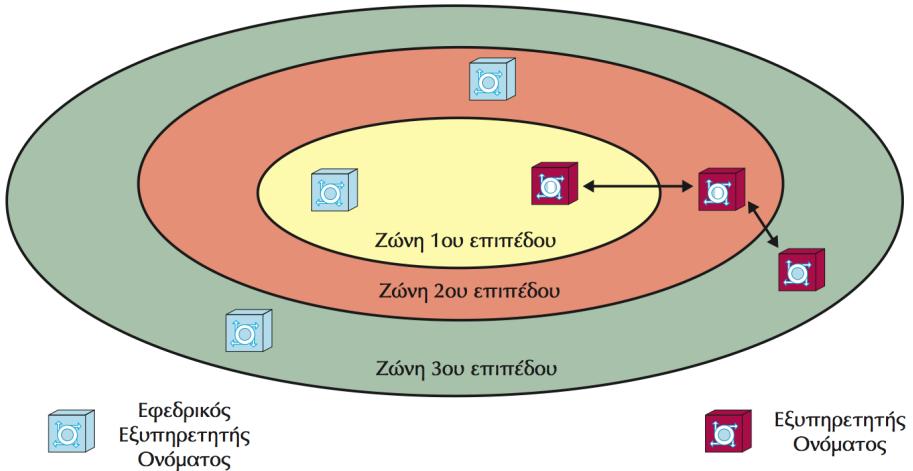
Κατανεμημένη είναι μια βάση δεδομένων όταν τα δεδομένα της είναι διασκορπισμένα σε περισσότερα από ένα μηχανήματα, αντί για ένα και μοναδικό κεντρικό αρχείο. Για να λειτουργήσει το σύστημα DNS που καλύπτει όλα τα μηχανήματα του Internet, δεν θα ήταν δυνατόν να χρησιμοποιηθεί ένα μόνο μηχάνημα: θα είχε τεράστια κίνηση δεδομένων λόγω του μεγάλου αριθμού ερωτήσεων και θα αργούσε σημαντικά. Επίσης τυχόν πρόβλημα στη λειτουργία του θα σήμαινε ουσιαστικά διακοπή των υπηρεσιών του Internet.

Όταν λέμε ότι το σύστημα DNS είναι **ιεραρχικά οργανωμένο** εννοούμε ότι χρησιμοποιούμε περιοχές ονομάτων. Για παράδειγμα, ένας υπολογιστής δεν χαρακτηρίζεται μόνο από το όνομα του, αλλά και από το όνομα του δικτύου στο οποίο βρίσκεται:

joshua.freebsdgr.org

Πρόκειται για τον υπολογιστή “joshua” στο δίκτυο “freebsdgr.org”. Κάποιος υπολογιστής στο σύστημα DNS είναι επιφορτισμένος με την τήρηση των ονομάτων και

διευθύνσεων όλων των υπολογιστών του δίκτυου “freebsdgr.org”. Το όνομα του υπολογιστή “joshua” μπορεί να χρησιμοποιηθεί ξανά σε ένα άλλο δίκτυο με διαφορετικό όνομα.



Σχήμα 7.29: Οργάνωση Δικτύου σε Ζώνες

Για τη λειτουργία του συστήματος DNS, χρησιμοποιούνται οι εξυπηρετητές ονομάτων οι οποίοι βρίσκονται σε διάφορα σημεία στο δίκτυο. Συνήθως κάθε εξυπηρετητής ονομάτων είναι υπεύθυνος για συγκεκριμένες περιοχές ονομάτων. Οι εξυπηρετητές συνεργάζονται μεταξύ τους προκειμένου να απαντήσουν σε ερωτήματα για υπολογιστές που δεν γνωρίζουν (που δεν βρίσκονται στη περιοχή ευθύνης τους). Αν το δίκτυο είναι μικρό, ο εξυπηρετητής DNS μπορεί να καλύπτει όλη την περιοχή του, σε αντίθετη περίπτωση καλύπτει κάποιο τμήμα της το οποίο ονομάζεται ζώνη (σχήμα 7.29). Έτσι η βάση δεδομένων του DNS χωρίζεται σε τμήματα τα οποία δεν επικαλύπτονται μεταξύ τους. Σε μεγάλα δίκτυα είναι δυνατόν να έχουμε βασικούς και εφεδρικούς εξυπηρετητές για να εξασφαλίσουμε τη συνέχεια της λειτουργίας σε περίπτωση βλάβης. Τυπικά οι εξυπηρετητές αυτοί δεν βρίσκονται καν στην ίδια φυσική τοποθεσία προκειμένου να μην επηρεάζονται από τα ίδια φαινόμενα (π.χ. διακοπή ρεύματος ή μια φυσική καταστροφή).

Η ιεραρχική οργάνωση των ονομάτων του DNS ακολουθείται από τους εξυπηρετητές DNS που είναι έτσι και αλλιώς οργανωμένοι κατά ζώνες. Το σύστημα DNS λειτουργεί με τη μορφή ζωνών που η μια περιέχει την άλλη (φωλιασμένες ζώνες). Κάθε εξυπηρετητής ονόματος επικοινωνεί με τους εξυπηρετητές της αμέσως υψηλότερης και χαμηλότερης (αν υπάρχει) ιεραρχικά ζώνης.

Για να το καταλάβετε φανταστείτε ξανά ότι ψάχνετε την διεύθυνση του υπολογιστή:

joshua.freebsdgr.org

Η αναζήτηση σας μπορεί να γίνει ως εξής:

- Το μηχάνημα σας θα επικοινωνήσει με τον εξυπηρετητή DNS που είναι υπεύθυνος για την περιοχή “.org”.
- Ο εξυπηρετητής DNS δεν γνωρίζει τον υπολογιστή “joshua” αλλά γνωρίζει ποιος υπολογιστής DNS είναι υπεύθυνος για τη ζώνη “freebsdgr.org” η οποία είναι ένα μικρό κομμάτι του “org”. Θα ρωτήσει τον εξυπηρετητή αυτό για τη διεύθυνση του υπολογιστή “joshua”.
- Θα λάβει την απάντηση “joshua.freebsdgr.org = 94.71.69.206” την οποία και θα στείλει στο δικό σας υπολογιστή.

Αυτός είναι ένας μόνο τρόπος λειτουργίας. Ένας διαφορετικός τρόπος είναι: ο εξυπηρετητής DNS της κεντρικής ζώνης “.org” να παραπέμψει το δικό σας υπολογιστή λέγοντας “Δεν ξέρω ποιος είναι ο joshua.freebsdgr.org αλλά για το freebsdgr.org είναι υπεύθυνος ο DNS εξυπηρετητής 204.13.248.75. Ρωτήστε εκεί”.

Είναι ελπίζουμε φανερό από τα παραπάνω ότι η ιεραρχική οργάνωση των εξυπηρετητών ακολουθεί αυτή των ονομάτων.

Για να ρωτήσετε ένα εξυπηρετητή DNS, μπορείτε να χρησιμοποιήσετε τις εντόλες:

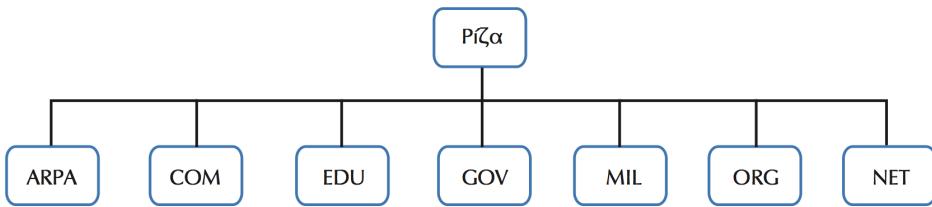
**nslookup
dig**

Θα γίνει μια σύντομη επίδειξη των εντολών αυτών στο εργαστήριο.

7.8.1 Χώρος Ονομάτων του DNS

Έχουμε ήδη αναφέρει ότι ο χώρος ονομάτων του DNS χρησιμοποιεί ιεραρχική αρχιτεκτονική. Έτσι ο χώρος διαιρείται σε ένα σύνολο περιοχών που μπορούν να διαιρεθούν ξανά σε περισσότερες περιοχές. Μια τέτοια δομή μοιάζει με δέντρο και φαίνεται στο σχήμα 7.30.

Το πρώτο επίπεδο περιοχών ονομάζονται βασικές περιοχές και βρίσκονται στα δεξιά του ονόματος. Στις ΗΠΑ υπάρχουν επτά τέτοιες περιοχές οι οποίες έχουν καθιερωθεί ουσιαστικά παγκόσμια, και στις οποίες κατατάσσονται τα δίκτυα ανάλογα με τις



Σχήμα 7.30: Βασικές περιοχές χώρου ονομάτων DNS

δραστηριότητες του οργανισμού ή της επιχείρησης στην οποία ανήκουν. Οι περιοχές αυτές είναι οι παρακάτω:

- **.arpa:** Ειδικοί οργανισμοί διαδικτύου
- **.com:** Εταιρίες
- **.edu:** Εκπαιδευτικά ιδρύματα
- **.gov:** Κυβερνητικοί οργανισμοί
- **.mil:** Στρατιωτικοί οργανισμοί
- **.net:** Κέντρα διοίκησης δικτύου
- **.org:** Οτιδήποτε δεν μπορεί να καταταγεί σε κάποια από τις προηγούμενες κατηγορίες (τυπικά μη-κερδοσκοπικοί οργανισμοί)

Εκτός από τις παραπάνω κατηγορίες οι οποίες ισχύουν στις ΗΠΑ (αν και αυτό δεν σημαίνει ότι μια δικτυακή τοποθεσία που τελειώνει π.χ. σε **.com** θα βρίσκεται στις ΗΠΑ – μπορεί να βρίσκεται οπουδήποτε και γενικά αυτός ο διαχωρισμός χρησιμοποιείται διεθνώς) υπάρχει επίσης μια βασική περιοχή ανά χώρα. Ο προσδιορισμός τους γίνεται με βάση ένα μικρό τμήμα (δύο – τρία γράμματα) του ονόματος της χώρας. Για παράδειγμα, η περιοχή που αντιστοιχεί στην Ελλάδα ονομάζεται **.gr**, της Γερμανίας είναι **.de** και της Μεγάλης Βρετανίας είναι **.uk**.

Κάτω από κάθε βασική περιοχή βρίσκεται ένα δεύτερο επίπεδο περιοχών το οποίο ονομάζεται *domain*. Το δεύτερο αυτό επίπεδο, τυπικά προσδιορίζει τον οργανισμό ή την επιχείρηση ο οποίος χρησιμοποιεί το όνομα (και στον οποίο ανήκει το αντίστοιχο δίκτυο). Κάθε μια από αυτές τις περιοχές είναι μοναδική. Τα ονόματα (*domain names*) που εκχωρούνται είναι συνήθως αντιπροσωπευτικά της εταιρίας ή οργανισμού στον οποίο ανήκουν. Τα *domain names* τοποθετούνται αριστερά του ονόματος της βασικής περιοχής και διαχωρίζονται με μια τελεία.

Για παράδειγμα, το **ntua.gr** αναφέρεται στο δίκτυο του Εθνικού Μετσόβειου Πολυτεχνείου. Το όνομα *domain* **ntua** έχει αποδοθεί στο ίδρυμα για αυτό το σκοπό και

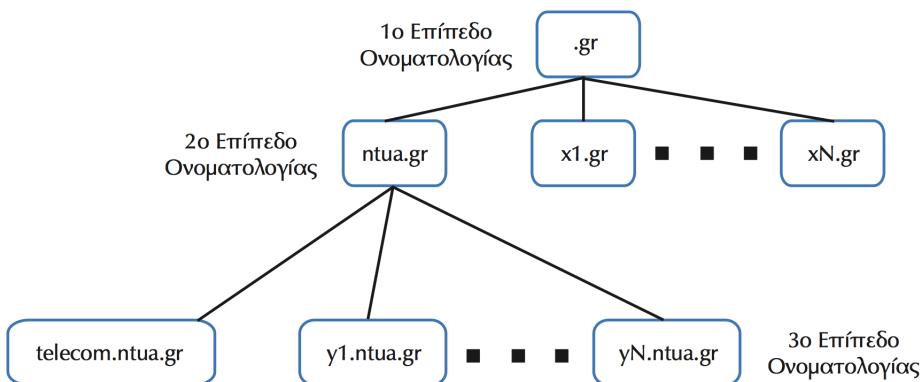
το .gr δείχνει ότι ανήκει στη βασική περιοχή που έχει εκχωρηθεί για την Ελλάδα (NTUA=National Technical University of Athens).

Παρόμοια, το freebsdgr.org δείχνει το domain με όνομα freebsdgr το οποίο είναι καταχωρημένο στην περιοχή .org. Από την βασική περιοχή καταλαβαίνουμε ότι πιθανώς πρόκειται για ένα μη κερδοσκοπικό οργανισμό.

Η εταιρία ή οργανισμός στην οποία έχει εκχωρηθεί ένα domain name είναι ο αποκλειστικά υπεύθυνος για την διαχείριση του. Για παράδειγμα, αν ο διαχειριστής δικτύου της εταιρίας αποφασίσει ότι το δίκτυο θα χωριστεί σε μικρότερα τμήματα (υποδίκτυα) το ίδιο μπορεί να γίνει και με την περιοχή ονομάτων του οργανισμού. Κάθε νέο υποδίκτυο αντιστοιχεί σε περιοχή ονομάτων τρίτου επιπέδου και ονομάζεται subdomain. Στο όνομα, εμφανίζεται αριστερά του domain name και χωρίζεται πάλι με μια τελεία. Για παράδειγμα:

telecom.ntua.gr

To telecom είναι ένα subdomain του domain ntua που βρίσκεται στην περιοχή .gr (Ελλάδας). Το συγκεκριμένο όνομα έχει αποδοθεί στην περιοχή που ανήκει το εργαστήριο τηλεπικοινωνιών του Πολυτεχνείου (ένα από τα πολλά εργαστήρια που διαθέτει) για την απεικόνιση του δικού του δικτύου (σχήμα 7.31).



Σχήμα 7.31: Ιεραρχική οργάνωση χώρου ονομάτων DNS

Ένα όνομα μπορεί να αναφέρεται σε ένα συγκεκριμένο υπολογιστή αντί για μια ολόκληρη περιοχή διευθύνσεων. Για παράδειγμα, αν έχουμε το subdomain:

telecom.ntua.gr

και θέλουμε να αναφερθούμε στον υπολογιστή “pc01” που ανήκει σε αυτόν, το πλήρες όνομα θα ήταν:

pc01.telecom.ntua.gr

Καθώς καταλαβαίνετε, με αυτό τον τρόπο έχουμε φτιάξει ονόματα **τετάρτου επιπέδου**. Ωστόσο δεν είναι απαραίτητο να φτάσουμε στο τέταρτο επίπεδο για να ονομάσουμε συγκεκριμένα μηχανήματα. Το όνομα του subdomain μπορεί ήδη να δείχνει σε ένα συγκεκριμένο μηχάνημα του δικτύου αντί για μια ολόκληρη περιοχή διευθύνσεων. Για παράδειγμα:

www.freebsdgr.org

δείχνει ένα υπολογιστή με όνομα “www” που ανήκει στο domain freebsdgr.org. Προφανώς ο υπολογιστής αυτός είναι επιφορτισμένος με την εξυπηρέτηση ιστοσελίδων.

Αυτό που μπορούμε να αντιληφθούμε από τα παραπάνω παραδείγματα είναι ότι η ιεραρχία των ονομάτων πηγαίνει από το δεξιότερο μέρος (ρίζα) προς τα αριστερά. Η ρίζα δείχνει πάντα τη μεγαλύτερη περιοχή και όσο μετακινούμαστε αριστερά, βρισκόμαστε σε όλο και πιο συγκεκριμένο κομμάτι του δικτύου:

Παράδειγμα: pc01.telecom.ntua.gr

- **gr:** Ρίζα (το πιο γενικό, όλη η περιοχή που έχει αποδοθεί στη χώρα μας)
- **ntua:** Η περιοχή που έχει αποδοθεί στο ΕΜΠ. Είναι ένα μικρό μέρος από τις διευθύνσεις που έχουν δοθεί στο “.gr”
- **telecom:** Η περιοχή που έχει αποδοθεί στο εργαστήριο τηλεπικοινωνιών του ΕΜΠ. Είναι ένα μικρό μέρος των διευθύνσεων που έχουν δοθεί στο “ntua”.
- **pc01:** Ένα συγκεκριμένο μηχάνημα που βρίσκεται στο εργαστήριο τηλεπικοινωνιών του ΕΜΠ.

Ενδιαφέρον πείραμα: Μπορείτε να βρείτε ποιος έχει κατοχυρώσει (ουσιαστικά σε ποιον ανήκει) ένα domain, χρησιμοποιώντας την εντολή **whois** σε ένα μηχάνημα UNIX. Για παράδειγμα:

whois freebsdgr.org

Θα σας πει σε ποιον είναι κατοχυρωμένο το όνομα freebsdgr.org (ποιος να είναι άραγε...). Σημειώστε ότι αυτό δεν λειτουργεί στην περιοχή “.gr”.

7.9 Δρομολόγηση

Ο αλγόριθμος δρομολόγησης ανήκει στο επίπεδο δικτύου και σκοπός του είναι να κατευθύνει ένα πακέτο από την πηγή στον προορισμό του. Ο όρος “δρομολόγηση”

αναφέρεται στη διαδικασία εύρεσης της διαδρομής που πρέπει να ακολουθήσει ένα πακέτο για να φτάσει στον προορισμό του. Η διαδικασία αυτή δεν είναι πάντα εύκολη, τη στιγμή που γνωρίζουμε ότι ένα σύνθετο δίκτυο (όπως το Internet) μπορεί να διαθέτει πολλές εναλλακτικές διαδρομές που να οδηγούν το πακέτο στον ίδιο προορισμό.

Γενικά μπορείτε να φανταστείτε ότι ένα αντίστοιχο πρόβλημα είναι να βρει ένα παιδί τη διαδρομή ανάμεσα σε τραπέζια ενός εστιατορίου για να κατευθυνθεί στο τραπέζι των γονιών του. Αν και ενδεχομένως ένας ενήλικας μπορεί να λύσει αυτό το πρόβλημα εύκολα (κρίνοντας πολύ γρήγορα ποια διαδρομή είναι η βέλτιστη), το παιδί δεν έχει ακόμα την πλήρη εποπτεία του χώρου και την απαιτούμενη εμπειρία. Φανταστείτε ότι ο αλγόριθμος δρομολόγησης θα πρέπει να κρίνει με βάση αρκετά κριτήρια ποια διαδρομή θα πρέπει να επιλεχθεί για ένα πακέτο που κατευθύνεται προς ένα συγκεκριμένο προορισμό.

Η χρονική στιγμή κατά την οποία λαμβάνονται οι αποφάσεις δρομολόγησης εξαρτάται από το δίκτυο και ειδικότερα από το αν χρησιμοποιούνται νοητά κυκλώματα ή αυτοδύναμα πακέτα.

- Αν χρησιμοποιούνται νοητά κυκλώματα, η εγκαθίδρυση της σύνδεσης γίνεται στην αρχή της επικοινωνίας και υποχρεωτικά όλα τα πακέτα ακολουθούν την ίδια διαδρομή (νοητό κύκλωμα). Στην περίπτωση αυτή, η επιλογή της διαδρομής γίνεται στην αρχή, κατά την εγκατάσταση της σύνδεσης.
- Αν χρησιμοποιούνται αυτοδύναμα πακέτα, δεν είναι απαραίτητο τα πακέτα που ανήκουν στην ίδια σύνδεση να ακολουθούν την ίδια διαδρομή. Στην περίπτωση αυτή, η απόφαση για τη διαδρομή που θα ακολουθήσει κάθε πακέτο, λαμβάνεται για καθένα από αυτά, ξεχωριστά.

Ανεξάρτητα από τα παραπάνω, ένας αλγόριθμος δρομολόγησης είναι γενικά επιθυμητό να διαθέτει τις παρακάτω ιδιότητες:

- **Απλότητα:** Ο αλγόριθμος πρέπει να είναι απλός - να περιέχει σαφείς και κατανοητούς κανόνες που να διέπουν τη λειτουργία του.
- **Ορθότητα:** Ο αλγόριθμος πρέπει να επιλύει σωστά το πρόβλημα της δρομολόγησης.
- **Ανθεκτικότητα:** Ο αλγόριθμός πρέπει να είναι σε θέση να αντιμετωπίζει αλλαγές στην τοπολογία του δικτύου - π.χ. στην περίπτωση που κάποιος ενδιάμεσος κόμβος ή γραμμή σύνδεσης σταματήσουν να λειτουργούν.
- **Δικαιοσύνη:** Τα πακέτα που προέρχονται από διαφορετικές συνδέσεις θα πρέπει να αντιμετωπίζονται με δίκαιο τρόπο. Για παράδειγμα δεν θα πρέπει τα πακέτα μιας σύνδεσης να καθυστερούν συνέχεια για να μεταδοθούν με μεγαλύτερη ταχύτητα τα πακέτα κάποιας άλλης. Ωστόσο αυτό μπορεί να έρχεται

σε αντίθεση με την ιδιότητα της βελτιστοποίησης.

- **Βελτιστοποίηση:** Στοχεύει στην καλύτερη δυνατή αξιοποίηση των πόρων του δικτύου. Για παράδειγμα στην μεγιστοποίηση της συνολικής κίνησης που εξυπηρετείται από το δίκτυο.

Το έργο της δρομολόγησης είναι ιδιαίτερα πολύπλοκο καθώς χρειάζεται συντονισμός και συνεργασία όλων των ενδιάμεσων κόμβων του δικτύου – και όχι μόνο των γειτονικών όπως απαιτείται από τα πρωτόκολλα των χαμηλότερων επιπέδων του OSI και του TCP/IP (π.χ. από το επίπεδο σύνδεσης δεδομένων). Τυπικά, για τη δρομολόγηση σε ένα δίκτυο συνεργάζονται μεταξύ τους πολλοί αλγόριθμοι οι οποίοι ως ένα σημείο λειτουργούν μεταξύ τους ανεξάρτητα.

Οι δύο βασικές λειτουργίες ενός αλγόριθμου δρομολόγησης είναι:

- Η επιλογή της διαδρομής για τη μεταφορά των δεδομένων από την πηγή στον προορισμό τους.
- Η παράδοση των πακέτων στον προορισμό τους όταν πλέον έχει καθοριστεί η διαδρομή.

Η παράδοση των πακέτων στον προορισμό τους γίνεται με τη χρήση των πινάκων δρομολόγησης. Η επιλογή της διαδρομής και η ενημέρωση των πινάκων δρομολόγησης αποτελεί ένα δύσκολο πρόβλημα το οποίο επηρεάζει την απόδοση του δικτύου. Τα βασικά μέτρα απόδοσης που επηρεάζονται από τον αλγόριθμο δρομολόγησης είναι:

- Η ρυθμοαπόδοση (δηλ. ο ρυθμός μετάδοσης που επιτυγχάνεται)
- Η μέση καθυστέρηση (ο χρόνος δηλ. που χρειάζεται για να γίνει η δρομολόγηση των πακέτων στον προορισμό τους – κατά μέσο όρο)

Είναι προφανές ότι η μέση καθυστέρηση που υφίστανται τα πακέτα, εξαρτάται από την διαδρομή που θα ακολουθήσουν μέχρι τον προορισμό τους. Η διαδρομή αυτή ωστόσο αποφασίζεται από τον αλγόριθμο δρομολόγησης. Οι αποφάσεις του αλγορίθμου έχουν κατά συνέπεια άμεση επίδραση στη μέση καθυστέρηση. Όταν η καθυστέρηση αυξάνεται ιδιαίτερα, σημαίνει ότι η εισερχόμενη κίνηση δεν μπορεί να εξυπηρετηθεί. Μπορείτε να φανταστείτε τις γραμμές ενός δικτύου σαν μια οδική αρτηρία. Όταν η κίνηση είναι αυξημένη, τα αυτοκίνητα κινούνται με μικρότερη ταχύτητα. Αν η κίνηση αυξηθεί ακόμα περισσότερο θα δημιουργηθεί κυκλοφοριακή συμφόρηση (μποτιλιάρισμα) και η κίνηση σχεδόν θα σταματήσει. Αντίστοιχα φαινόμενα παρατηρούνται και στα δίκτυα δεδομένων.

Όταν η μέση καθυστέρηση αυξάνεται πάνω από ένα όριο, ενεργοποιείται ένας μηχανισμός προστασίας που ονομάζεται έλεγχος ροής. Ο έλεγχος ροής εμποδίζει την είσοδο νέου φορτίου στο δίκτυο. Σκοπός του είναι να εξισορροπήσει την ρυθμοαπόδοση με την καθυστέρηση. Όσο πιο αποτελεσματικός είναι ο αλγόριθμος στην

διατήρηση χαμηλής καθυστέρησης, τόσο περισσότερη κίνηση μπορεί να δεχθεί το δίκτυο και άρα επιτυγχάνει και μεγαλύτερη ρυθμοαπόδοση.

Οι αλγόριθμοι δρομολόγησης διακρίνονται σε:

- Πρώτον σε **Κατανεμημένους και Συγκεντρωτικούς**
- Δεύτερον σε **Στατικούς και Προσαρμοζόμενης Δρομολόγησης**

Στους συγκεντρωτικούς αλγόριθμους οι αποφάσεις δρομολόγησης λαμβάνονται εξ' ολοκλήρου από ένα κεντρικό κόμβο. Ο κόμβος αυτός πρέπει να γνωρίζει πλήρως την κατάσταση του δικτύου και άρα οι πίνακες δρομολόγησης που θα διατηρεί θα έχουν αρκετά μεγάλο μέγεθος. Έτσι ο κόμβος πρέπει να έχει μεγάλες δυνατότητες τοπικής αποθήκευσης δεδομένων αλλά και πολύ ισχυρή κεντρική μονάδα επεξεργασίας (CPU, Central Processing Unit) ώστε η αναζήτηση στους πίνακες να γίνεται με μεγάλη ταχύτητα.

Αντίθετα στους κατανεμημένους αλγόριθμους οι αποφάσεις δρομολόγησης λαμβάνονται κατανεμημένα μεταξύ των κόμβων του δικτύου. Όταν χρειάζεται, οι κόμβοι αυτοί επικοινωνούν μεταξύ τους και ανταλλάσσουν πληροφορίες για να λάβουν σωστότερες αποφάσεις (π.χ. μαθαίνουν το φορτίο που αντιμετωπίζει τη δεδομένη στιγμή κάποιο συγκεκριμένο τμήμα του δικτύου, ώστε αν χρειάζεται και είναι εφικτό να αποφεύγουν να χρησιμοποιήσουν τη συγκεκριμένη διαδρομή).

Οι στατικοί αλγόριθμοι δρομολόγησης χρησιμοποιούν σταθερές διαδρομές για τη μεταφορά δεδομένων. Οι διαδρομές είναι ανεξάρτητες από τις συνθήκες κίνησης που επικρατούν στο δίκτυο και αλλάζουν μόνο αν ένας κόμβος ή μια γραμμή σύνδεσης τεθούν εκτός λειτουργίας. Οι στατικοί αλγόριθμοι χρησιμοποιούνται συνήθως σε σχετικά απλά δίκτυα καθώς δεν μπορούν να επιτύχουν μεγάλες ρυθμοαποδόσεις και είναι ακατάλληλοι για δίκτυα που το φορτίο έχει μεγάλες διακυμάνσεις.

Οι αλγόριθμοι προσαρμοζόμενης δρομολόγησης έχουν τη δυνατότητα να τροποποιούν τις διαδρομές ανάλογα με το φορτίο των γραμμών του δικτύου. Για παράδειγμα, όταν αντιληφθούν ότι ένα τμήμα του δικτύου έχει υποστεί συμφόρηση λόγω μεγάλης εισερχόμενης κίνησης, έχουν τη δυνατότητα να τροποποιήσουν τις διαδρομές τους ώστε τα πακέτα να ακολουθούν διαδρομή που δεν περνάει από αυτό το τμήμα. Για να αποφασίσουν για τις διαδρομές, οι αλγόριθμοι αυτοί μετρούν ή εκτιμούν έμμεσα την κίνηση του δικτύου με βάση την τοπολογία του (μπορούν επίσης να ενημερώνονται με μηνύματα σχετικά με την κίνηση του δικτύου από αντίστοιχους αλγόριθμους απομακρυσμένων κόμβων).

Σημαντική παρατήρηση: Τα κριτήρια με τα οποία λαμβάνουν τις αποφάσεις τους οι αλγόριθμοι δρομολόγησης είναι:

- Η Συντομότερη Διαδρομή η οποία καθορίζεται με βάση:

- είτε τον αριθμό των χωριστών τμημάτων που την αποτελούν
 - είτε τη μέση καθυστέρηση (ουράς και μετάδοσης) που εισάγει
 - είτε τη χρησιμοποίηση τους εύρους ζώνης τη γραμμής του δικτύου
 - Τον *Αριθμό Πακέτων* που περιμένουν προς μετάδοση στην ουρά εξόδου
 - Το *Κόστος Γραμμής*. Είναι μια συνάρτηση στην οποία συμμετέχουν με διαφορετικούς συντελεστές βαρύτητας οι παράγοντες: μέση καθυστέρηση, μέσο μήκος ουράς, χρήση εύρους ζώνης.
-

7.9.1 Δρομολόγηση σε Δίκτυα TCP/IP

Μέχρι τώρα έχουμε έξετάσει το πρωτόκολλο TCP/IP και έχουμε αντιληφθεί ότι το πρωτόκολλο IP είναι υπεύθυνο για την μεταφορά των αυτοδύναμων πακέτων στο προορισμό τους (όπως δηλώνεται από τη διεύθυνση προορισμού), αλλά δεν έχουμε πει ακόμα με ποιο τρόπο πραγματοποιείται η δρομολόγηση.

Θα πρέπει καταρχήν να διευκρινίσουμε ότι σε ένα δίκτυο TCP/IP δεν είναι όλοι οι κόμβοι υπεύθυνοι να εκτελούν υπηρεσίες δρομολόγησης. Γενικά μπορούμε να διακρίνουμε δύο είδη κόμβων:

- **Τους τελικούς υπολογιστές - hosts:** Οι υπολογιστές αυτοί παίρνουν αποφάσεις δρομολόγησης μόνο για τα δικά τους αυτοδύναμα πακέτα. Όταν λαμβάνουν πακέτα που δεν προορίζονται για αυτούς, δεν εκτελούν καμιά διαδικασία για να τα προωθήσουν στον πραγματικό προορισμό τους.
- **Τους δρομολογητές - routers:** Τα μηχανήματα αυτά παίρνουν αποφάσεις δρομολόγησης για όλα τα πακέτα που λαμβάνουν και τα προωθούν στον προορισμό τους.

Να σημειώσουμε εδώ ότι η παραπάνω διάκριση έχει να κάνει με το σκοπό και λειτουργία του μηχανήματος και όχι τη φυσική του υπόσταση: Ένας κανονικός υπολογιστής μπορεί να λειτουργήσει ως δρομολογητής αν τον εξοπλίσουμε με το κατάλληλο λογισμικό. Σε πολλές περιπτώσεις χρησιμοποιούμε ως δρομολογητές εξειδικευμένα μηχανήματα (*routers*). Όταν χρησιμοποιούμε κανονικό υπολογιστή για δρομολόγηση, είναι δυνατόν το ίδιο μηχάνημα να έχει και το ρόλο του τελικού μηχανήματος (αυτό συνήθως συμβαίνει σε μικρά δίκτυα). Αντίστοιχα, σε πολύ μεγάλα δίκτυα ένας εξειδικευμένος δρομολογητής μπορεί να είναι απλώς ένας πολύ ισχυρός γενικός υπολογιστής με κατάλληλο πρόγραμμα.

Βασικό ρόλο στη διαδικασία δρομολόγησης έχει ο πίνακας δρομολόγησης. Το πρωτόκολλο IP χρησιμοποιεί αυτό τον πίνακα για να πάρει όλες τις αποφάσεις που έχουν

να κάνουν με την δρομολόγηση πακέτων στον προορισμό τους.

Σε μεγάλα επικοινωνιακά κέντρα, υπάρχουν συνήθως δρομολογητές που διασυνδέουν πολλά δίκτυα μεταξύ τους. Στο IP, η δρομολόγηση συνήθως βασίζεται στην διεύθυνση του δικτύου προορισμού. Κάθε υπολογιστής διαθέτει ένα πίνακα με διεύθυνσεις δικτύων, για καθένα από τα οποία αντιστοιχεί ένας δρομολογητής. Όταν δημιουργείται ένα αυτοδύναμο πακέτο προς κάποιο δίκτυο, ο υπολογιστής συμβουλεύεται αυτό τον πίνακα για να τα στείλει στον αντίστοιχο δρομολογητή ο οποίος και θα τα προωθήσει τελικά στο δίκτυο προορισμού. Σημειώστε εδώ ότι ο δρομολογητής αυτός δεν είναι απαραίτητο να είναι συνδεδεμένος απευθείας με το δίκτυο προορισμού: αρκεί να αποτελεί την καλύτερη επιλογή για διασύνδεση με το συγκεκριμένο δίκτυο σε σχέση με τους υπόλοιπους δρομολογητές του πίνακα. Ο δρομολογητής θα αναλάβει να στείλει το πακέτο σε άλλο δρομολογητή κ.ο.κ. μέχρις ότου να φτάσει σε ένα δρομολογητή ο οποίος να είναι συνδεδεμένος απευθείας με το δίκτυο προορισμού.

Ο αλγόριθμος δρομολόγησης που χρησιμοποιείται από το πρωτόκολλο IP για τη δρομολόγηση αυτοδύναμων πακέτων διακρίνει δύο περιπτώσεις:

- **Άμεση Δρομολόγηση (direct routing):** Στην περίπτωση αυτή ο υπολογιστής προορισμού βρίσκεται στο ίδιο δίκτυο με τον υπολογιστή αποστολής. Το πακέτο μπορεί να σταλεί απευθείας χωρίς άλλα βήματα, και άρα δεν γίνεται καμιά προώθηση του πακέτου. Πρόκειται για την απλούστερη μορφή δρομολόγησης.
- **Έμμεση Δρομολόγηση (indirect routing):** Στην περίπτωση αυτή ο υπολογιστής προορισμού βρίσκεται σε διαφορετικό δίκτυο από τον υπολογιστή αποστολής. Θα πρέπει το πακέτο να δρομολογηθεί μέσω των κατάλληλων δρομολογητών για να φτάσει στον προορισμό του. Προφανώς για το σκοπό αυτό θα χρησιμοποιηθούν οι πίνακες δρομολόγησης που αναφέραμε προηγουμένως.

Όταν ένας υπολογιστής δημιουργήσει και πρόκειται να στείλει ένα αυτοδύναμο IP πακέτο, ελέγχει πρώτα αν η διεύθυνση προορισμού του βρίσκεται στο ίδιο τοπικό δίκτυο με την δική του. Για παράδειγμα, αν ο υπολογιστής αποστολής έχει διεύθυνση 192.168.0.42 και ο προορισμός 192.168.0.31, βρίσκονται και οι δύο στο ίδιο δίκτυο, το 192.168.0. Στην περίπτωση αυτή το πακέτο μπορεί να σταλεί απευθείας και δεν απαιτούνται επιπλέον βήματα. Σε αντίθετη περίπτωση, το σύστημα θα βρει μια εγγραφή στον πίνακα δρομολόγησης που να αναφέρει σε ποιο δρομολογητή πρέπει να σταλεί το πακέτο για να προωθηθεί στο δίκτυο προορισμού. Καθώς το Διαδίκτυο (Internet) αναπτύσσεται με ραγδαίους ρυθμούς και διασυνδέει πολλά εκατομμύρια υπολογιστών, είναι φανερό ότι το μέγεθος ενός τέτοιου πίνακα δρομολόγησης αυξάνει επικίνδυνα και η διαχείριση του γίνεται προβληματική. Για το σκοπό αυτό έχουν αναπτυχθεί τεχνικές για τη μείωση του μεγέθους των πινάκων δρομολόγησης. Μια τέτοια τεχνική είναι η χρήση ενός και μόνο ορισμένου από πριν προεπιλεγμένου

δρομολογητή. Σε πολλά δίκτυα υπάρχει ένας και μόνο δρομολογητής που συνδέει το δίκτυο με τον έξω κόσμο (Για παράδειγμα, στο σχολείο μας η σύνδεση γίνεται με ένα δρομολογητή στο rack του εργαστηρίου που μας συνδέει με το Πανελλήνιο Σχολικό Δίκτυο). Ένας τέτοιος δρομολογητής τυπικά συνδέει ένα τοπικό δίκτυο σε κάποιο δίκτυο κορμού.

Στην παραπάνω περίπτωση, ο πίνακας δρομολόγησης κάθε υπολογιστή του τοπικού δικτύου είναι ιδιαίτερα απλός, αφού δεν χρειάζεται μια εγγραφή για κάθε δίκτυο προορισμού. Απλώς δηλώνεται ο προεπιλεγμένος δρομολογητής ο οποίος και θα αναλάβει κάθε κίνηση που προορίζεται για τον εξωτερικό κόσμο, ανεξάρτητα από το δίκτυο προορισμού.

Σημείωση κατανόησης: Πρόκειται για το μηχάνημα που ονομάζουμε **προεπιλεγμένη πύλη ή default gateway**. Σε ένα συνηθισμένο μικρό δίκτυο μπορεί να υπάρχει μόνο αυτός. Μπορείτε να βρείτε ποιος είναι σε ένα δίκτυο γράφοντας την εντολή (είναι ίδια για Windows / Linux / FreeBSD):

`netstat -rn`

και θα δείτε ως απάντηση κάτι σαν το παρακάτω:

`Routing tables`

`Internet:`

Destination	Gateway	Flags	Refs	Use	Netif	Expire
default	192.168.0.250	UGS	0	325353	r10	
127.0.0.1	127.0.0.1	UH	0	13404	lo0	

Εδώ είναι προφανές ότι ο προεπιλεγμένος δρομολογητής είναι ο 192.168.0.250. Η μορφή της απάντησης αλλάζει ελαφρά ανάλογα με το λειτουργικό, αλλά αν δεν μπορείτε να καταλάβετε ποιος είναι ο προεπιλεγμένος δρομολογητής, ψάξτε στη στήλη “Flags” για την καταχώριση που περιέχει το γράμμα “G”.

Προεπιλεγμένος δρομολογητής μπορεί να υπάρχει και σε δίκτυο το οποίο περιέχει περισσότερους από ένα δρομολογητής. Σε αυτό το δρομολογητή αυτό προωθούνται τα αυτοδύναμα πακέτα τα οποία στην επικεφαλίδα τους δεν καθορίζουν κάποιον από τους άλλους διαθέσιμους δρομολογητές. Εάν ο προεπιλεγμένος δρομολογητής δεν μπορέσει να προωθήσει κάποιο αυτοδύναμο πακέτο στον προορισμό του, υπάρχει πρόβλεψη ώστε οι δρομολογητές να στέλνουν ένα μήνυμα του τύπου: “Δεν είμαι η κατάλληλη επιλογή δρομολογητή – χρησιμοποιήστε τον δρομολογητή X”. Το μήνυμα αυτό στέλνεται μέσω του πρωτοκόλλου ICMP. Τα μηνύματα αυτά λαμβάνονται από το επίπεδο δικτύου και χρησιμοποιούνται συνήθως για την προσθήκη και ενημέρωση εγγραφών στους πίνακες δρομολόγησης.

Παράδειγμα: Έστω το δίκτυο με διεύθυνση 128.6.4 του Πανεπιστημίου Αθηνών, με δύο δρομολογητές τον 128.6.4.59 και 128.6.4.1. Ο 128.6.4.59 συνδέει το δίκτυο με άλλα δίκτυα που βρίσκονται επίσης μέσα στο πανεπιστήμιο, ενώ ο 128.6.4.1 συνδέει το δίκτυο απευθείας με το Πανεπιστήμιο Πειραιώς. Ας υποθέσουμε ότι έχουμε ορίσει τον 128.6.4.59 ως προεπιλεγμένο και δεν έχουμε άλλες εγγραφές στον πίνακα δρομολόγησης. Τι θα συμβεί αν δημιουργήσουμε και προσπαθήσουμε να στείλουμε ένα αυτοδύναμο πακέτο προς το Πανεπιστήμιο Πειραιά;

1. Καθώς δεν υπάρχει άλλη γραμμή στον πίνακα δρομολόγησης, το πακέτο θα κατευθυνθεί προς τον προεπιλεγμένο δρομολογητή, τον 128.6.4.59. Αυτός όμως συνδέει το δίκτυο με άλλα δίκτυα εντός του Πανεπιστημίου Αθηνών.
2. Καθώς ο δρομολογητής αυτός δεν είναι ο σωστός για τον προορισμό, θα στείλει το πακέτο στο δρομολογητή 128.6.4.1 για να το προωθήσει. Ταυτόχρονα θα στείλει και ένα μήνυμα λάθους στο σύστημα που δημιούργησε το αυτοδύναμο πακέτο. Το μήνυμα αυτό θα σταλεί μέσω του ICMP και θα είναι κάτι σαν αυτό: “Για δρομολόγηση στο Πανεπιστήμιο Πειραιά, χρησιμοποιήστε το δρομολογητή 128.6.4.1”.
3. Ο υπολογιστής που θα λάβει το μήνυμα ICMP, θα το χρησιμοποιήσει για να προσθέσει μια εγγραφή στον πίνακα δρομολόγησης του. Κατά συνέπεια, κάθε αυτοδύναμο πακέτο που θα παράγει από αυτό το σημείο και μετά με προορισμό το Πανεπιστήμιο Πειραιά, θα στέλνεται απευθείας στον δρομολογητή 128.6.4.1.

Ο αλγόριθμος δρομολόγησης μπορεί να προσδιορίζει το επόμενο βήμα του στη διαδρομή όχι με βάση τη διεύθυνση του δικτύου προορισμού αλλά με βάση τον υπολογιστή προορισμού (Σημείωση: Δεν είμαι σίγουρος για το τι ακριβώς εννοεί εδώ ο ποιητής).

Παρακάτω θα βρείτε ένα συνοπτικό διάγραμμα του αλγόριθμου δρομολόγησης που χρησιμοποιείται από το πρωτόκολλο IP:

$\Delta\pi$ = Διεύθυνση Προορισμού π.χ 128.6.3.2, $\Delta\Delta\pi$ = Διεύθυνση Δικτύου Προορισμού π.χ. 128.6.3

Ξεχώρισε τη $\Delta\pi$ από το αυτοδύναμο πακέτο

Υπολόγισε τη $\Delta\Delta\pi$ από τη $\Delta\pi$

Αν η $\Delta\Delta\pi$ ανήκει σε δίκτυο με το οποίο ο δρομολογητής είναι άμεσα συνδεδεμένος

Προώθησε το πακέτο προς τον προορισμό του μέσω του δικτύου με τη $\Delta\Delta\pi$

Διαφορετικά Αν η ΔΠ υπάρχει στον πίνακα δρομολόγησης με βάση τον υπολογιστή προορισμού

Δρομολόγησε το πακέτο όπως αναγράφει ο πίνακας

Διαφορετικά Αν η ΔΔΠ υπάρχει στον πίνακα δρομολόγησης

Δρομολόγησε το πακέτο όπως αναγράφει ο πίνακας

Διαφορετικά Αν έχει προσδιοριστεί πρότυπη διαδρομή

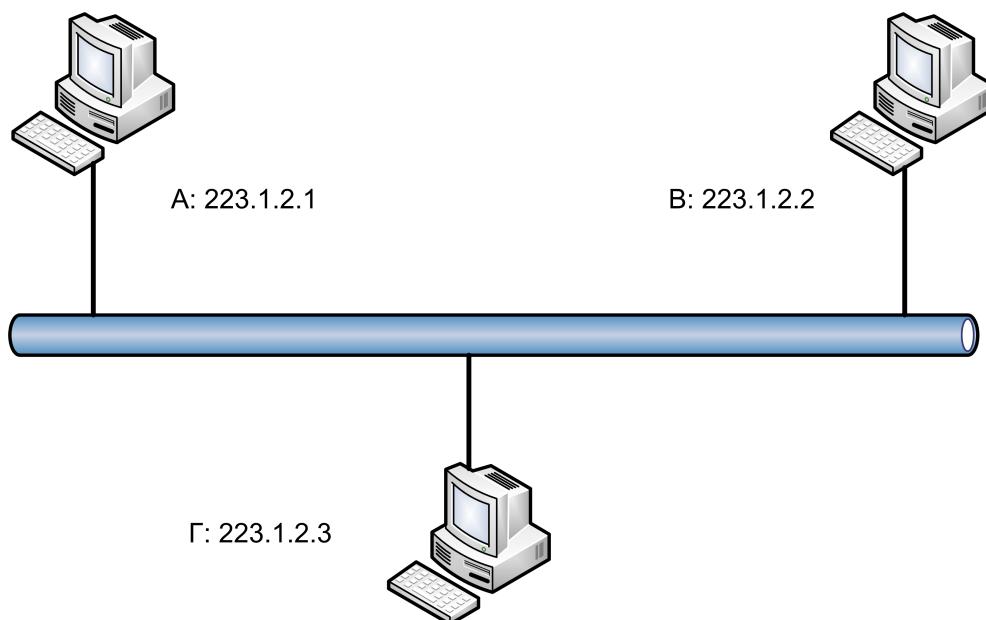
Δρομολόγησε το αυτοδύναμο πακέτο προς τον

αντίστοιχο δρομολογητή

Διαφορετικά σημείωσε λάθος στη δρομολόγηση

7.9.2 Άμεση Δρομολόγηση

Για να αντιληφθούμε πως λειτουργεί η άμεση δρομολόγηση, ας πάρουμε το δίκτυο του σχήματος 7.32. Πρόκειται για ένα απλό δίκτυο τριών υπολογιστών τύπου Ethernet. Είναι εμφανές ότι και οι τρεις υπολογιστές έχουν την ίδια διεύθυνση δικτύου, άρα τα πακέτα μπορούν να δρομολογηθούν απευθείας από τον ένα στον άλλο, χωρίς τη μεσολάβηση κάποιου δρομολογητή. Να θυμηθούμε ακόμα ότι στο Ethernet έχουμε και τις φυσικές διευθύνσεις (το γνωστό μας MAC Address). Και φυσικά κάθε μηχάνημα διαθέτει μια διεύθυνση IP που φαίνεται στο σχήμα.



Σχήμα 7.32: TCP/IP Δίκτυο Τριών Υπολογιστών

Όταν ο υπολογιστής A στέλνει ένα IP αυτοδύναμο πακέτο στον υπολογιστή B, στην επικεφαλίδα του πακέτου η διεύθυνση πηγής είναι η IP του A και προορισμού η IP του B. Κατά την αποστολή, όταν το πακέτο φτάσει στο φυσικό επίπεδο του Ethernet δημιουργούνται τα αντίστοιχα πλαίσια Ethernet τα οποία περιέχουν αντίστοιχα σαν διεύθυνση αποστολής την φυσική διεύθυνση του A και προορισμού την αντίστοιχη διεύθυνση του B, όπως φαίνεται στον παρακάτω πίνακα:

	Διεύθυνση Πηγής	Διεύθυνση Προορισμού
IP Επικεφαλίδα	Διεύθυνση A	Διεύθυνση B
Ethernet Επικεφαλίδα	Διεύθυνση A	Διεύθυνση B

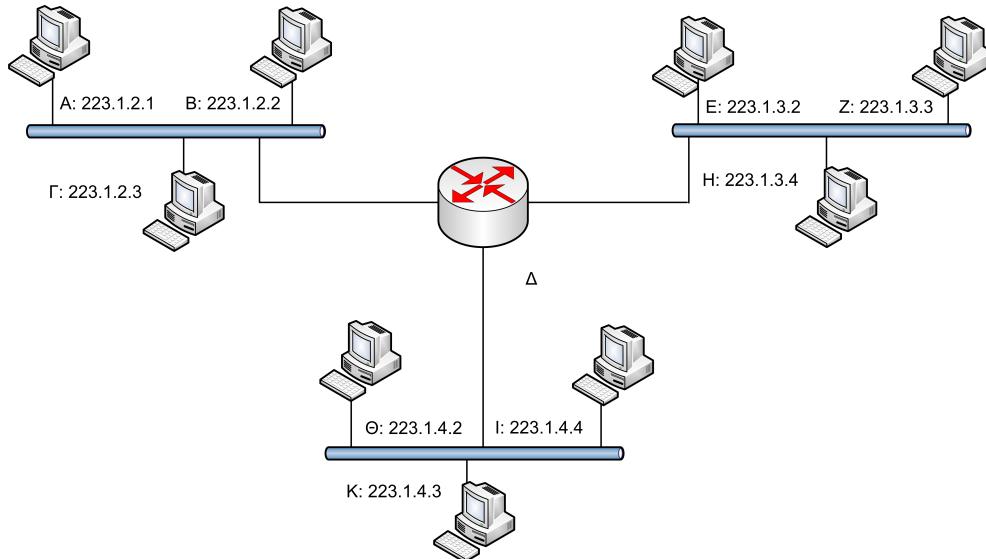
Στην παραπάνω περίπτωση απλής μεταφοράς πακέτων από το A στο B, το πρωτόκολλο IP δεν προσφέρει κάποια επιπλέον υπηρεσία σε σχέση με αυτές που παρέχονται ήδη από το φυσικό επίπεδο Ethernet. Για την ακρίβεια, μάλλον μας επιβαρύνει τη στιγμή που θα πρέπει να δημιουργηθεί, μεταδοθεί και αναλυθεί σε κάθε περίπτωση η αντίστοιχη επικεφαλίδα IP. Θυμηθείτε ότι αν και στο Ethernet κάθε μηχάνημα μπορεί να δει όλες τις μεταδόσεις των υπολογίων (αφού βρίσκονται πρακτικά πάνω στο ίδιο φυσικό μέσο), ο κάθε κόμβος μπορεί να ξεχωρίζει ποια δεδομένα προορίζονται για αυτόν κοιτάζοντας ήδη στο φυσικό επίπεδο την επικεφαλίδα Ethernet προορισμού. Όπως έχουμε πει αυτή είναι μια γρήγορη διαδικασία η οποία γίνεται από την κάρτα δικτύου – δεν χρειάζεται να φτάσουμε μέχρι το επίπεδο δικτύου και την επικεφαλίδα IP για να δούμε αν το πακέτο προορίζεται για το συγκεκριμένο μηχάνημα.

Όταν το πρωτόκολλο IP του B λάβει το IP αυτοδύναμο πακέτο από το A, θα εξετάσει την IP διεύθυνση προορισμού για να δει αν είναι ίδια με τη δική του (και θα είναι φυσικά, γιατί θα έχει ήδη επιλεγεί με βάση την Ethernet διεύθυνση). Αν είναι, το πακέτο θα περάσει στα ανώτερα επίπεδα. Η επικοινωνία του A με το B γίνεται με άμεση δρομολόγηση.

7.9.3 Έμμεση Δρομολόγηση

Στο σχήμα 7.33 φαίνεται ένα δίκτυο το οποίο αποτελείται από τρία TCP/IP δίκτυα που ενώνονται μεταξύ τους με τη βοήθεια ενός δρομολογητή (Δ). Το δίκτυο αυτό είναι πιο αντιπροσωπευτικό από το απλό δίκτυο που παρουσιάσαμε στην προηγούμενη ενότητα. Το κάθε δίκτυο χρησιμοποιεί Ethernet και αποτελείται από τρεις υπολογιστές.

Καθώς ο δρομολογητής (Δ) είναι ένας IP δρομολογητής, είναι συνδεδεμένος και στα τρία δίκτυα. Λογικό είναι λοιπόν ότι διαθέτει τρεις διευθύνσεις IP (μια για κάθε δίκτυο, και προφανώς με την αντίστοιχη για κάθε δίκτυο διεύθυνση) καθώς και τρεις διευθύνσεις Ethernet.



Σχήμα 7.33: TCP/IP διαδίκτυο αποτελούμενο από τρία TCP/IP δίκτυα

Όταν η επικοινωνία γίνεται μεταξύ ενός υπολογιστής ενός δικτύου σε ένα άλλο **του ίδιου** δικτύου, ο δρομολογητής δεν κάνει τίποτα. Για παράδειγμα, αν ο υπολογιστής Α στείλει ένα πακέτο στον Β, καθώς και οι δύο βρίσκονται στο ίδιο υποδίκτυο η δρομολόγηση είναι άμεση και ακολουθεί τους απλούς κανόνες που παρουσιάσαμε στην προηγούμενη ενότητα.

Η επικοινωνία έχει μεγαλύτερο ενδιαφέρον όταν γίνεται μεταξύ υπολογιστών που ανήκουν σε διαφορετικά υποδίκτυα. Για παράδειγμα υποθέστε ότι ο υπολογιστής Α θέλει να επικοινωνήσει με τον υπολογιστή Ε. Είναι εμφανές ότι δεν υπάρχει άμεση σύνδεση μεταξύ Α και Ε, άρα τα πακέτα θα πρέπει να περάσουν διαμέσου του δρομολογητή (Δ). Παρατηρήστε ότι καθώς ο δρομολογητής (Δ) έχει μια σύνδεση σε καθένα από τα δίκτυα, η δρομολόγηση πακέτων προς αυτόν είναι άμεση. Από τον Α όμως προς τον Ε η επικοινωνία δεν είναι άμεση, καθώς παρεμβάλλεται ο (Δ). Μια τέτοια επικοινωνία ονομάζεται **έμμεση**.

Για να στείλει το πακέτο ο υπολογιστής Α στον υπολογιστή Ε, θέτει ως IP διεύθυνση πηγής τη δική του και ως IP διεύθυνση προορισμού την διεύθυνση του Ε. Αντίστοιχα θέτει ως διεύθυνση Ethernet πηγής τη δική του, αλλά ως διεύθυνση προορισμού την διεύθυνση του δρομολογητή Δ . Αυτό συμβαίνει επειδή ο Α δεν μπορεί να στείλει απευθείας (άμεσα) το πακέτο στον Ε καθώς δεν είναι στο ίδιο δίκτυο (Για την ακρίβεια, δεν γνωρίζει καν την Ethernet διεύθυνση του Ε). Βάζοντας ως διεύθυνση Ethernet προορισμού την αντίστοιχη του δρομολογητή (Δ), το πακέτο (για να είμαστε πιο ακριβείς τα πλαίσια που το αποτελούν) θα κατευθυνθεί στο δρομολογητή. Ο δρομολογητής θα αναλάβει να προωθήσει το πακέτο στο δίκτυο που βρίσκεται ο

Ε για να παραληφθεί από αυτόν.

Παρατηρούμε λοιπόν ότι σε σχέση με την άμεση δρομολόγηση που εξετάσαμε, η πραγματική διαφορά όσο αφορά τις επικεφαλίδες βρίσκεται στην επικεφαλίδα Ethernet προορισμού. Όταν γίνεται έμμεση δρομολόγηση, η επικεφαλίδα αυτή δείχνει πάντα την διεύθυνση Ethernet του δρομολογητή που ενώνει τα δίκτυα μεταξύ τους.

	Διεύθυνση Πηγής	Διεύθυνση Προορισμού
IP Επικεφαλίδα	Διεύθυνση A	Διεύθυνση E
Ethernet Επικεφαλίδα	Διεύθυνση A	Διεύθυνση (Δ)

Το πρωτόκολλο IP του δρομολογητή (Δ) λαμβάνει το IP αυτοδύναμο πακέτο από τον Α και εξετάζοντας την IP διεύθυνση προορισμού αντιλαμβάνεται ότι δεν απευθύνεται στην πραγματικότητα σε αυτόν, αλλά στον υπολογιστή E του άλλου δικτύου. Για να το στείλει πλέον στον υπολογιστή E, αλλάζει την διεύθυνση Ethernet προορισμού με αυτήν του E. Τελικά, το πακέτο που φεύγει από τον δρομολογητή για τον E, έχει τα παρακάτω:

	Διεύθυνση Πηγής	Διεύθυνση Προορισμού
IP Επικεφαλίδα	Διεύθυνση A	Διεύθυνση E
Ethernet Επικεφαλίδα	Διεύθυνση Δ	Διεύθυνση E

7.9.4 Πίνακας Δρομολόγησης

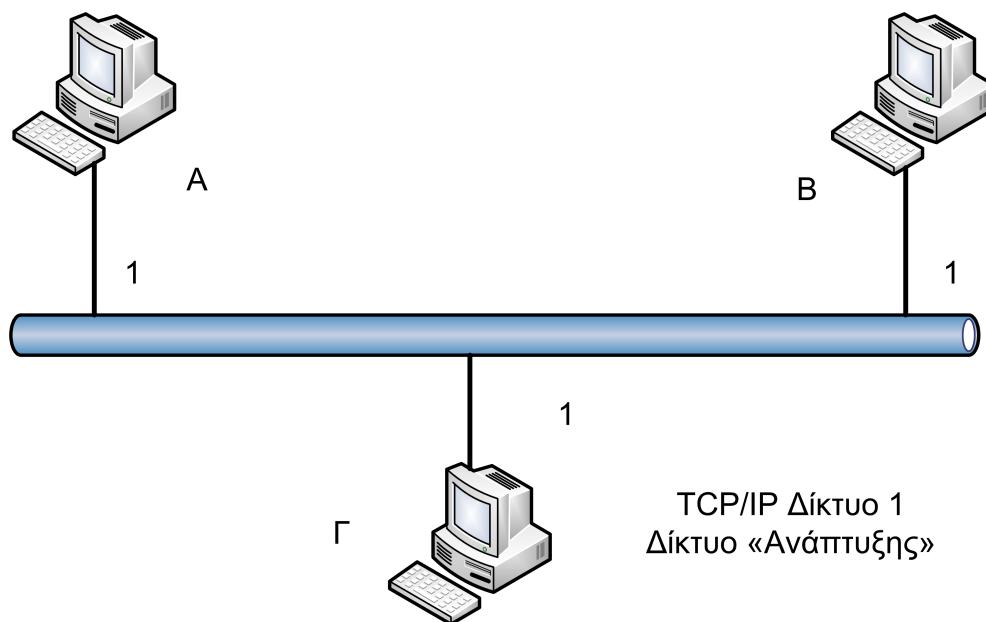
Θα μελετήσουμε τώρα πως γίνεται η δρομολόγηση στο Διαδίκτυο, με τη βοήθεια του πίνακα δρομολόγησης. Το πρωτόκολλο IP προσδιορίζει το σημείο διεπαφής δικτύου που πρόκειται να χρησιμοποιήσει διαβάζοντας την αντίστοιχη γραμμή στον πίνακα, χρησιμοποιώντας ως κλειδί αναζήτησης την διεύθυνση δικτύου προορισμού. Η διεύθυνση δικτύου προορισμού όπως έχουμε ήδη πει προκύπτει από την IP διεύθυνση προορισμού. Ο πίνακας δρομολόγησης έχει μια εγγραφή (καταχώριση) για κάθε διαδρομή. Οι βασικές στήλες του πίνακα δρομολόγησης είναι:

- **Αριθμός Δικτύου IP** - Η διεύθυνση δικτύου προορισμού όπως προκύπτει από το IP προορισμού. Π.χ. για διεύθυνση IP 223.1.2.3 και μάσκα 255.255.255.0, το δίκτυο προορισμού είναι το 223.1.2
- **Αναγνωριστικό Άμεσης / Έμμεσης Δρομολόγησης** - Στη στήλη αυτή γράφεται αν η δρομολόγηση θα είναι άμεση (δηλ. ο προορισμός βρίσκεται στο ίδιο δίκτυο) ή έμμεση (θα παρεμβληθεί κάποιος δρομολογητής)
- **IP Διεύθυνση Δρομολογητή** - Στη στήλη αυτή γράφεται η IP διεύθυνση του δρομολογητή που θα χρησιμοποιηθεί - αν η δρομολόγηση είναι άμεση, το πεδίο αυτό παραμένει κενό.

- Αριθμός Διεπαφής Δικτύου** - Το βιβλίο δεν το διευκρινίζει, αλλά αναφέρεται στην κάρτα δικτύου από την οποία πρέπει να ξεκινήσει το πακέτο για να πάει στον προορισμό του. Προφανώς αυτό έχει νόημα αν ένας υπολογιστής διαθέτει περισσότερες από μια κάρτα δικτύου, και καθεμιά από αυτές είναι συνδεδεμένη σε διαφορετικό δίκτυο. Στην περίπτωση αυτή, το αυτοδύναμο πακέτο που δημιουργείται πρέπει να εξέλθει από τη σωστή κάρτα για να δρομολογηθεί. Αν όμως υπάρχει μόνο μία διεπαφή, αυτό το πεδίο θα έχει συνέχεια την ίδια τιμή π.χ. 1

Σημείωση εκτός βιβλίου: Στην πραγματικότητα ένας πίνακας δρομολόγησης μπορεί να έχει και έξι πεδία. Το πεδίο “Αριθμός Διεπαφής” είναι ένα μόνο από τρία προαιρετικά πεδία.

Για κάθε εξερχόμενο αυτοδύναμο πακέτο, το πρωτόκολλο IP συμβουλεύεται τον πίνακα δρομολόγησης. Έτσι αποφασίζει αν το πακέτο θα σταλεί με άμεση ή έμμεση δρομολόγηση, τον δρομολογητή ο οποίος θα το παραλάβει (αν πρόκειται για έμμεση δρομολόγηση) καθώς και τη διεπαφή δικτύου εξόδου – την κάρτα δικτύου στο χαμηλότερο επίπεδο η οποία θα το προωθήσει στο φυσικό μέσο. Ας πάρουμε για



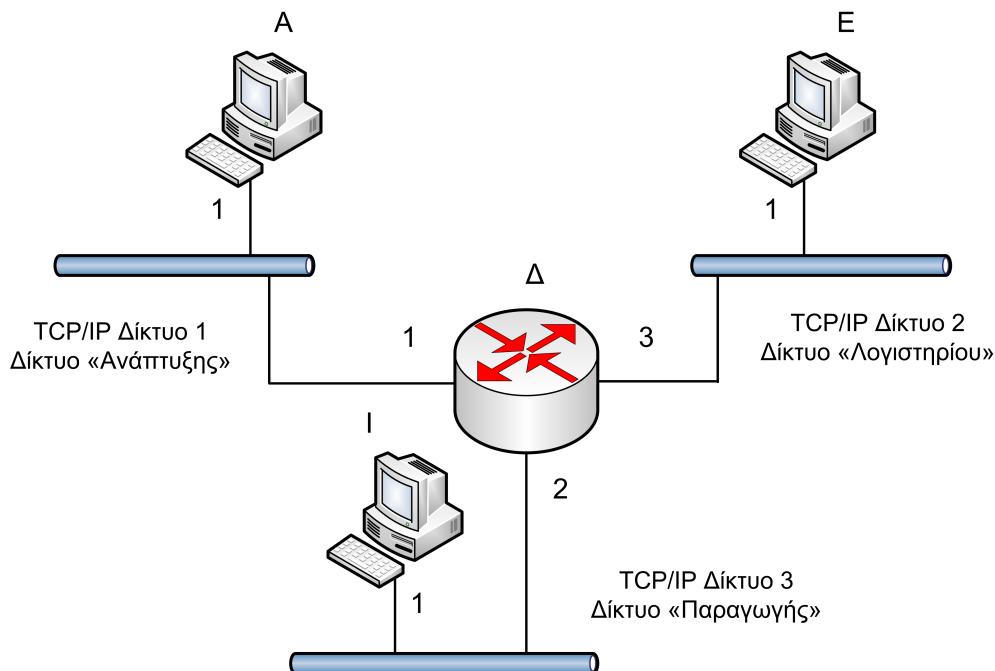
Σχήμα 7.34: Διεπαφές των υπολογιστών A,B,Γ TCP/IP δικτύου

παράδειγμα το δίκτυο του σχήματος 7.34. Όταν ο υπολογιστής A θέλει να στείλει ένα αυτοδύναμο IP πακέτο στον υπολογιστή B, αρχικά θα προσδιορίσει την διεύθυνση του υπολογιστή B. Αυτή είναι 223.1.2.2. Από την διεύθυνση αυτή προκύπτει

η διεύθυνση δικτύου 223.1.2 (Σημείωση: Για να το βρει αυτό στην πραγματικότητα χρειάζεται και τη μάσκα ή το πρόθεμα, αλλά το βιβλίο σας απλοποιεί υπερβολικά τα πράγματα). Ψάχνοντας στην πρώτη στήλη του πίνακα δρομολόγησης βρίσκει την αντίστοιχη διεύθυνση δικτύου και διαβάζει τα υπόλοιπα δεδομένα της ίδιας γραμμής. Στην περίπτωση μας ο πίνακας είναι ο παρακάτω:

Δίκτυο	Αναγνωριστικό Άμεσης ή Έμμεσης Δρομολόγησης	Δρομολογητής	Αριθμός Διεπαφής
Ανάπτυξης (223.1.2)	Άμεση	κενό	1

Αυτό απλά σημαίνει ότι ο υπολογιστής Β είναι στο ίδιο δίκτυο, άρα η δρομολόγηση θα είναι άμεση. Συνεπώς δεν παρεμβάλλεται δρομολογητής, έτσι το αντίστοιχο πεδίο είναι κενό. Τέλος θα χρησιμοποιηθεί η πρώτη (και πιθανόν μοναδική) διεπαφή που διαθέτει ο υπολογιστής για την ολοκλήρωση της επικοινωνίας. Έχοντας καθορίσει ότι η δρομολόγηση θα είναι άμεση και καθώς το δίκτυο είναι Ethernet, το επόμενο βήμα είναι η εύρεση της Ethernet διεύθυνσης του Β μέσω του πίνακα ARP και η αποστολή του πακέτου μέσω της διεπαφής 1. Στο σχήμα 7.35 μπορούμε να



Σχήμα 7.35: Διεπαφές των υπολογιστών A, Δ, E, I TCP/IP δικτύου με δρομολογητή

δούμε τι γίνεται στην περίπτωση έμμεσης δρομολόγησης. Όπως έχουμε ήδη αναφέρει, ο δρομολογητής Δ διαθέτει τρεις διαφορετικές διεπαφές (κάρτες δικτύου) και καθεμιά είναι συνδεδεμένη και σε ένα διαφορετικό δίκτυο. Ανάλογα με το δίκτυο

προορισμού του κάθε πακέτου που λαμβάνει μπορεί να χρησιμοποιήσει την κατάλληλη διεπαφή για να το στείλει. Στην πραγματικότητα ο πίνακας δρομολόγησης του υπολογιστή που βρίσκεται στο δίκτυο A θα περιέχει τις παρακάτω καταχωρίσεις που του επιτρέπουν να στείλει αυτοδύναμα IP πακέτα στους υπολογιστές των άλλων δύο δικτύων:

Δίκτυο	Αναγνωριστικό Άμεσης ή Έμμεσης Δρομολόγησης	Δρομολογητής	Αριθμός Διεπαφής
Ανάπτυξης (223.1.2)	Άμεση	κενό	1
Λογιστηρίου (223.1.3)	Έμμεση	Δ	1
Παραγωγής (223.1.4)	Έμμεση	Δ	1

Είναι αρκετά εύκολο να καταλάβουμε πως ο υπολογιστής A θα στείλει ένα πακέτο στον υπολογιστή E (που βρίσκεται στο τμήμα “Λογιστήριο”):

- Το πρωτόκολλο IP λαμβάνει τη διεύθυνση δικτύου του υπολογιστή E από την διεύθυνση IP του υπολογιστή E.
- Διερευνά τον πίνακα δρομολόγησης (πρώτη στήλη) και βρίσκει τη διεύθυνση δικτύου του E στη δεύτερη γραμμή του πίνακα.
- Από την ανάγνωση των δεδομένων της δεύτερης γραμμής του πίνακα αντιλαμβάνεται ότι θα χρησιμοποιηθεί έμμεση δρομολόγηση μέσω του δρομολογητή Δ.
- Από τον πίνακα ARP βρίσκεται η Ethernet διεύθυνση του δρομολογητή Δ και το πακέτο στέλνεται προς αυτόν (Όπως είπαμε στην προηγούμενη ενότητα, δεν αλλάζει η IP διεύθυνση προορισμού - αυτή εξακολουθεί να δείχνει στον υπολογιστή E. Βάζοντας όμως την Ethernet διεύθυνση προορισμού του Δ, το πακέτο θα παραληφθεί από το δρομολογητή)
- Το πακέτο φτάνει στο σημείο διεπαφής 1 (στην κάρτα δικτύου του A) και περνάει στο δίκτυο “Ανάπτυξης”. Παραλαμβάνεται από τον δρομολογητή Δ και φτάνει μέχρι το επίπεδο δικτύου του πρωτοκόλλου. Εκεί διαπιστώνεται ότι δεν προορίζεται πραγματικά για τον Δ, αφού η IP διεύθυνση προορισμού του δείχνει στον υπολογιστή E του “Λογιστηρίου”.
- Ο δρομολογητής Δ θα προωθήσει το πακέτο στο δίκτυο προορισμού του.

Είναι ενδιαφέρον να δούμε με ποιο τρόπο θα γίνει η προώθηση του πακέτου στο “Λογιστήριο”. Για να το καταλάβουμε θα πρέπει να ρίξουμε μια ματιά στον πίνακα δρομολόγησης που βρίσκεται μέσα στον ίδιο το δρομολογητή Δ.

Δίκτυο	Αναγνωριστικό Άμεσης ή Έμμεσης Δρομολόγησης	Δρομολογητής	Αριθμός Διεπαφής
Ανάπτυξης (223.1.2)	Άμεση	κενό	1
Λογιστηρίου (223.1.3)	Άμεση	κενό	3
Παραγωγής (223.1.4)	Άμεση	κενό	2

- Το πρωτόκολλο IP του δρομολογητή Δ βρίσκει την διεύθυνση δικτύου του υπολογιστή Ε, από την διεύθυνση IP προορισμού που περιέχεται στο πακέτο. Η διεύθυνση δικτύου είναι 223.1.3
- Ανιχνεύοντας την πρώτη στήλη του πίνακα, βρίσκει την διεύθυνση δικτύου του Ε στη δεύτερη γραμμή.
- Το αυτοδύναμο πακέτο IP στέλνεται με άμεση πλέον δρομολόγηση στον υπολογιστή Ε μέσω του σημείου διεπαφής 3.

Το αυτοδύναμο πακέτο που κατευθύνεται στον υπολογιστή Ε έχει ως IP και Ethernet διευθύνσεις προορισμού τις αντίστοιχες του Ε. Ο υπολογιστής Ε λαμβάνει το πακέτο, το οποίο φτάνει μέχρι το επίπεδο δικτύου όπου και διαπιστώνεται ότι η διεύθυνση IP προορισμού είναι ίδια με του Ε. Έτσι το πακέτο προωθείται προς τα υψηλότερα επίπεδα του πρωτοκόλλου.

7.11 Πρωτόκολλα Εφαρμογής

7.11.1 Γενικές Αρχές

Τα πρωτόκολλα που έχουμε εξετάσει μέχρι τώρα ανήκουν στα κατώτερα επίπεδα του μοντέλου TCP/IP. Έχουμε δει ότι έχουν δυνατότητες όπως:

- Να διασπούν την αρχική πληροφορία σε μικρότερα κομμάτια
- Να δημιουργούν αυτοδύναμα πακέτα που περιέχουν τη διεύθυνση αποστολέα και παραλήπτη
- Να δρομολογούν τα πακέτα μέχρι τον προορισμό τους
- Να συναρμολογούν τα πακέτα βάζοντας τα στη σωστή σειρά, ανασυνθέτοντας το αρχικό μήνυμα
- Να εξασφαλίζουν την ορθότητα της μετάδοσης κλπ.

Όλα αυτά και περισσότερα γίνονται από τα πρωτόκολλα TCP, IP και τα υπόλοιπα που εξετάσαμε στα επίπεδα Μεταφοράς, Δικτύου και Σύνδεσης Δικτύου (φυσικό). Όμως όλη η παραπάνω διαδικασία δεν αρκεί για να έχουμε μια πλήρης επικοινωνία.

Χρειαζόμαστε προφανώς και κάποιο τρόπο για να ζητήσουμε την εκτέλεση μιας συγκεκριμένης λειτουργίας.

Ας πάρουμε για παράδειγμα την περίπτωση που ένας χρήστης θέλει να ζητήσει τη μεταφορά ενός αρχείου από ένα απομακρυσμένο υπολογιστή στο δικό του. Θα πρέπει να υπάρχει κάποιος τρόπος ο χρήστης αυτός:

- Να ζητήσει την αποκατάσταση μιας σύνδεσης μεταξύ του υπολογιστή του και του απομακρυσμένου εξυπηρετητή
- Να παρέχει κάποιο όνομα και κωδικό που θα του επιτρέψει την πρόσβαση
- Να δει τη λίστα των διαθέσιμων αρχείων
- Να ζητήσει την αποστολή ενός συγκεκριμένου αρχείου

Είναι προφανές ότι δεν υπάρχει κάποιο πρωτόκολλο από αυτά που έχουμε εξετάσει μέχρι τώρα που να ικανοποιεί αυτές τις λειτουργίες. Προφανώς το πρωτόκολλο που χρειαζόμαστε εδώ είναι αρκετά πιο κοντά στις εφαρμογές και τη λογική που θα χρησιμοποιήσει ο χρήστης για να εκτελέσει την εργασία του, παρά στις τεχνικές λεπτομέρειες λειτουργίας της μετάδοσης μέσα από το φυσικό μέσο. Τα πρωτόκολλα που μας βοηθούν σε αυτή (και παρόμοιες εργασίες) ανήκουν στο υψηλότερο επίπεδο της οικογένειας TCP/IP, στα πρωτόκολλα εφαρμογής.

Σημείωση: Όσο πιο ψηλά βρίσκεται ένα πρωτόκολλο στην κορυφή, τόσο πιο κοντά είναι στον ανθρώπινο τρόπο σκέψης. Τα πρωτόκολλα στο επίπεδο εφαρμογής χρησιμοποιούν εντολές όπως “get”, “put”, “send”. Αντίθετα τα πρωτόκολλα που βρίσκονται στο τελευταίο επίπεδο (σύνδεσης δικτύου) ασχολούνται αποκλειστικά με δυαδικά δεδομένα.

Τα πρωτόκολλα εφαρμογών καθορίζουν τι στέλνεται μέσα από τη σύνδεση. Προσδιορίζουν με λίγα λόγια το σύνολο των εντολών που καταλαβαίνει η συγκεκριμένη εφαρμογή καθώς και τη δομή με την οποία πρέπει να σταλούν. Σε ένα πρωτόκολλο εφαρμογής αναμιγνύονται τα δεδομένα που στέλνονται ή λαμβάνονται με τις αντίστοιχες εντολές για τη διαχείριση της σύνδεσης. Όσο αφορά τις τεχνικές λεπτομέρειες της σύνδεσης (π.χ. τη δρομολόγηση ή τη δημιουργία πακέτων), το πρωτόκολλο εφαρμογής δεν ασχολείται καθόλου. Τα πρωτόκολλα που βρίσκονται κάτω από αυτό έχουν όπως έχουμε δει την αποκλειστική ευθύνη για όλα αυτά. Τα πρωτόκολλα εφαρμογής βλέπουν τη σύνδεση σαν να ήταν ένα καλώδιο που συνδέει απευθείας τους δύο υπολογιστές.

Ωστόσο τα πρωτόκολλα εφαρμογής έχουν να αντιμετωπίσουν διάφορες δυσκολίες, που έχουν να κάνουν με τον κοινό τρόπο παρουσίασης. Μερικά από τα προβλήματα που υπάρχουν:

- Δεν υπάρχει πάντα συμφωνία μεταξύ του συνόλου χαρακτήρων που χρησιμοποιείται από υπολογιστή σε υπολογιστή. Τυπικά χρησιμοποιείται το σύνολο χαρακτήρων ASCII ή το EBCDIC. Όμως πρόκειται για αρκετά περιορισμένο σύνολο χαρακτήρων στο οποίο υπάρχει πρόβλημα να κωδικοποιηθούν γλώσσες που περιέχουν διαφορετικά ή/και περισσότερα σύμβολα και γράμματα από αυτά του λατινικού αλφαριθμητικού. Τα πράγματα γίνονται ακόμα χειρότερα με γλώσσες που περιέχουν πάρα πολλά γράμματα ή για τις οποίες έχουν προταθεί περισσότερες από μία συμβάσεις κωδικοποίησης του αλφαριθμητικού τους.
- Υπάρχουν και άλλες ασυμφωνίες όπως για παράδειγμα τον χαρακτήρα που χρησιμοποιείται στην επικοινωνία για να δηλώσει το τέλος μιας γραμμής κειμένου. Πρόκειται για διαφορετική ακολουθία π.χ. σε μηχανήματα Windows και μηχανήματα UNIX.

Ο τρόπος παρουσίασης των δεδομένων (και επίλυσης των παραπάνω προβλημάτων) είναι αποκλειστικά ευθύνη των πρωτοκόλλων εφαρμογής. Πρωτόκολλα όπως το TCP και το IP δεν ασχολούνται καθόλου με αυτό το θέμα.

7.11.2 Βασικές και Προηγμένες Υπηρεσίες Διαδικτύου

Ακολουθεί μια σύντομη αναφορά στις πιο χαρακτηριστικές εφαρμογές που διατίθενται στο Διαδίκτυο και υποστηρίζονται από την τεχνολογία TCP/IP:

Ηλεκτρονικό Ταχυδρομείο

Το ηλεκτρονικό ταχυδρομείο ή *email* είναι η εφαρμογή που επιτρέπει την αποστολή μηνυμάτων (επιστολών) μεταξύ δύο ή περισσότερων χρηστών με ηλεκτρονικό τρόπο. Το ηλεκτρονικό ταχυδρομείο έχει σχεδόν μηδαμινό κόστος ενώ τα μηνύματα παραδίδονται ταχύτατα σε σχέση με το συμβατικό ταχυδρομείο. Τα σύγχρονα προγράμματα διαχείρισης *e-mail* είναι αρκετά φιλικά προς το χρήστη. Με τη χρήση του *e-mail* καταργείται στην ουσία η αναμονή σε ταχυδρομεία.

Τα τελευταία χρόνια, με την εξάπλωση και την ευρεία χρήση του Διαδικτύου, διακινείται μέσω *e-mail* μεγάλο τμήμα των εγγράφων που ανταλλάσσονται μεταξύ των υπηρεσιών και εταιριών. Καθώς τα προγράμματα είναι ιδιαίτερα φιλικά, δεν απαιτούνται εξειδικευμένες γνώσεις για το χειρισμό τους ο οποίος μπορεί να γίνει αρκετά καλά από απλούς χρήστες. Ανάμεσα στις δυνατότητες που παρέχονται είναι η παράδοση του ίδιου μηνύματος σε πολλούς παραλήπτες, ενημέρωση λήψης του μηνύματος στον αποστολέα, καθώς και αυτόματη διαχείριση και ταξινόμηση των εισερχόμενων μηνυμάτων ανά κατηγορία, περιεχόμενο, αποστολέα κ.λ.π. Να σημειώσουμε εδώ ότι δεν είναι απαραίτητο να είναι παρών ο παραλήπτης για τη λήψη

του μηνύματος, καθώς αυτό παραμένει στον απομακρυσμένο εξυπηρετητή αλληλογραφίας μέχρι να συνδεθεί ο χρήστης και να τα λάβει στον προσωπικό του υπολογιστή.

Πλεονεκτήματα

- Είναι πολύ γρήγορο. Ο τυπικός χρόνος λήψης ενός μηνύματος είναι γύρω στα δύο λεπτά. Ο χρόνος παράδοσης δεν εξαρτάται από την γεωγραφική θέση του παραλήπτη, αλλά από την ταχύτητα των συνδέσεων του δικτύου που παρεμβάλλονται μεταξύ αποστολέα και παραλήπτη. Ετσι για παράδειγμα ένα μήνυμα μπορεί να κάνει λιγότερο χρόνο να φτάσει σε ένα μακρινότερο προορισμό (π.χ. Αμερική) επειδή οι ενδιάμεσοι συνδέσεις είναι ταχύτερες.
- Ο χρήστης δεν χρειάζεται να παρακολουθεί τη μεταφορά του μηνύματος μέσω του e-mail (όπως για παράδειγμα γίνεται με το Fax ή το τηλέφωνο). Το μήνυμα παραδίδεται στον εξυπηρετητή προορισμού και ο παραλήπτης θα το λάβει μόλις ενεργοποιήσει τον υπολογιστή του και το πρόγραμμα ηλεκτρονικού ταχυδρομείου.
- Είναι πιο οικονομικό από το κοινό ταχυδρομείο. Μπορούμε να καθορίσουμε πολλαπλούς παραλήπτες σε ένα μήνυμα και να μεταδώσουμε μεγάλο αριθμό μηνυμάτων με μια απλή σύνδεση. Μπορούμε ακόμα να μεταδώσουμε εικόνες και ίχο εφόσον χρησιμοποιούμε το κατάλληλο πρόγραμμα.

Μειονεκτήματα

- Δεν υπάρχει απόλυτη εγγύηση ότι το μήνυμα θα ληφθεί

Σημείωση εκτός βιβλίου: Στην πραγματικότητα το email έχει άλλα σοβαρότερα μειονεκτήματα από αυτό – στην πράξη τα email χάνονται σπάνια. Άλλα μειονεκτήματα είναι:

- Δεν εξασφαλίζεται ότι ο αποστολέας είναι πράγματι αυτός που αναφέρεται στο μήνυμα. Για να γίνει αυτό θα πρέπει να χρησιμοποιηθεί κάποιο επιπλέον σύστημα, π.χ. ψηφιακές υπογραφές ή πιστοποιητικά (Για τις ψηφιακές υπογραφές θα μιλίσουμε στο επόμενο κεφάλαιο).
 - Πολλές φορές γίνεται διακίνηση ιών και κακόβουλων προγραμμάτων μέσω email.
 - Λαμβάνουμε πάρα πολλά ανεπιθύμητα μηνύματα – τα γνωστά spam.
 - Λαμβάνουμε παραπλανητικά μηνύματα (phishing) τα οποία έχουν σκοπό να μας οδηγήσουν να αποκαλύψουμε προσωπικά ή/και οικονομικά στοιχεία (αριθμούς πιστωτικών καρτών κλπ).
-

Το σύστημα του ηλεκτρονικού ταχυδρομείου αποτελείται από ένα συντάκτη κειμένου (κειμενογράφο) με το οποίο ο χρήστης γράφει τα μηνύματα του, και το σύστημα μεταφοράς το οποίο αναλαμβάνει να τα μεταφέρει στους παραλήπτες. Για τη μεταφορά του ηλεκτρονικού ταχυδρομείου χρησιμοποιείται στο σύστημα TCP/IP το *Πρωτόκολλο Μεταφοράς Απλού Ταχυδρομείου - Simple Mail Transfer Protocol* (Σημείωση: Η μετάφραση του βιβλίου είναι λάθος βέβαια - η λέξη "απλό" αναφέρεται στο πρωτόκολλο). Το πρωτόκολλο SMTP συνοπτικά δουλεύει ως εξής:

- Το SMTP θέτει κάποιες ερωτήσεις στον εξυπηρετητή ονομάτων (DNS). Πρέπει να προσδιορίσει ποιος είναι ο εξυπηρετητής ταχυδρομείου για τον τομέα στον οποίο ανήκει ο παραλήπτης. Για παράδειγμα, αν στέλνουμε ένα email στον user1@otenet.gr, το SMTP θα ρωτήσει ποιος είναι ο εξυπηρετητής ταχυδρομείου του τομέα otenet.gr και μόλις πάρει το όνομα, θα ρωτήσει τη διεύθυνση του εξυπηρετητή.
- Το SMTP θα ανοίξει μια σύνδεση με τον απομακρυσμένο εξυπηρετητή, χρησιμοποιώντας ως θύρα TCP προορισμού την 25. Η θύρα 25 είναι η προκαθορισμένη θύρα εξυπηρετητή για το Ηλεκτρονικό Ταχυδρομείο. Ο υπολογιστής που στέλνει το μήνυμα είναι ο SMTP πελάτης ενώ αυτός που το λαμβάνει είναι ο εξυπηρετητής.
- Μόλις γίνει αποκατάσταση της σύνδεσης, το SMTP αρχίζει να στέλνει μια σειρά από εντολές που καθορίζουν τον αποστολέα και τον παραλήπτη του μηνύματος. Ο εξυπηρετητής ανταποκρίνεται σε κάθε ένα από αυτά τα μηνύματα με απαντήσεις που δείχνουν ότι τα αιτήματα γίνονται δεκτά ή ότι υπάρχει κάποιο πρόβλημα (π.χ. ότι δεν βρέθηκε ο παραλήπτης). Με το τέλος αυτής της συνεννόησης, ο αποστολέας στέλνει μια εντολή (DATA) που δείχνει ότι αρχίζει να μεταδίδει το μήνυμα. Με τη λήξη του μηνύματος, στέλνεται ένας χαρακτήρας που δείχνει το τέλος και ειδοποιεί το πρόγραμμα του εξυπηρετητή να ερμηνεύει πάλι τα δεδομένα που λαμβάνει ως εντολές.

Πρωτόκολλο Μεταφοράς Αρχείων (FTP, File Transfer Protocol)

Το πρωτόκολλο μεταφοράς αρχείων, *FTP* επιτρέπει τη μεταφορά αρχείων μεταξύ υπολογιστών που χρησιμοποιούν την τεχνολογία TCP/IP. Το πρωτόκολλο αυτό χρησιμοποιεί το γνωστό μας μοντέλο πελάτη-εξυπηρετητή. Πελάτης είναι ο υπολογιστής που ξεκινάει την επικοινωνία και ζητάει να κατεβάσει κάποιο από τα αρχεία που διαθέτει ο εξυπηρετητής (μπορεί επίσης ανάλογα με τις ρυθμίσεις να έχει και δυνατότητα να ανεβάσει αρχεία). Ο εξυπηρετητής είναι ο υπολογιστής στον οποίο ζητάμε πρόσβαση. Το πρωτόκολλο FTP χρησιμοποιεί στο επίπεδο μεταφοράς το πρωτόκολλο TCP για την μεταφορά των δεδομένων του. Γνωρίζουμε ότι το TCP διασφαλίζει αξιόπιστη από άκρο σε άκρο επικοινωνία, κάτι το οποίο είναι απαραίτητο

καθώς δεν είναι αποδεκτό να λαμβάνουμε αρχεία που να περιέχουν λάθη. Ουσιαστικά το FTP μας επιτρέπει να δημιουργούμε αντίγραφα αρχείων ενός απομακρυσμένου εξυπηρετητή και μας επιτρέπει για παράδειγμα να δουλέψουμε στο σπίτι μας αφού λάβουμε το κατάλληλο αρχείο από τον εξυπηρετητή του γραφείου μας. Σημειώστε βέβαια ότι το FTP δεν έχει δυνατότητες συγχρονισμού - δεν μπορεί δηλ. να πάρει π.χ. τις διαφορές μεταξύ δύο εκδόσεων του ίδιου αρχείου, αλλά μονάχα ολόκληρο το αρχείο.

Για να εξασφαλιστεί η ασφάλεια του συστήματος και να επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες η πρόσβαση στα αρχεία ενός εξυπηρετητή, υλοποιείται ένα σύστημα ελέγχου εξουσιοδότησης. Το σύστημα αυτό βασίζεται στην χρήση ονόματος πρόσβασης και κωδικού τα οποία πρέπει να πληκτρολογήσει ο χρήστης για την είσοδο του στο σύστημα. Τα στοιχεία αυτά δημιουργούνται από το διαχειριστή του εξυπηρετητή FTP και ελέγχονται κάθε φορά. Να σημειώσουμε ότι όταν ένας χρήστης διαθέτει ένα λογαριασμό FTP σε ένα απομακρυσμένο σύστημα, δεν έχει πλήρη πρόσβαση στο σύστημα, το μόνο που μπορεί να κάνει είναι να αντιγράψει αρχεία (με λίγα λόγια, το FTP δέχεται ένα πολύ περιορισμένο σύνολο εντολών που έχουν να κάνουν με διαχείριση / αντιγραφή αρχείων και όχι το μεγάλο σύνολο εντολών που μπορεί κανείς να εκτελέσει μέσω ενός τερματικού του UNIX - για παράδειγμα μέσω ενός συστήματος απομακρυσμένης πρόσβασης).

Με την ολοκλήρωση της σύνδεσης και την επαλήθευση των στοιχείων του χρήστη, το σύστημα μας επιτρέπει να αντιγράψουμε ένα ή περισσότερα αρχεία στον υπολογιστή μας. Ο όρος “μεταφορά” στο FTP δηλώνει ότι το αρχείο μεταφέρεται από τον ένα υπολογιστή (εξυπηρετητή) στον άλλο (πελάτη). Ωστόσο το πρωτότυπο αρχείο δεν επηρεάζεται από αυτή τη διαδικασία (πρόκειται για αντιγραφή, και όχι για μετακίνηση).

Σημείωση: Το FTP στις μέρες μας δεν θεωρείται ασφαλές πρωτόκολλο, καθώς μεταφέρει το όνομα χρήστη και τον κωδικό μέσα από το δίκτυο ως απλό κείμενο, χωρίς καμιά κρυπτογράφηση. Για το λόγο αυτό αποφεύγεται η χρήση του. Το FTP ωστόσο παρέχει και τη δυνατότητα ανώνυμης πρόσβασης μέσω της οποίας ένας χρήστης έχει ελάχιστα δικαιώματα (βλέπει μόνο συγκεκριμένους καταλόγους και μπορεί μόνο να κατεβάσει αρχεία). Με αυτό τον τρόπο λειτουργίας χρησιμοποιείται και σήμερα για να κατεβάζουμε αρχεία τα οποία είναι δημόσια διαθέσιμα.

Η λειτουργία του FTP είναι κάπως πιο πολύπλοκη σε σχέση με τη λειτουργία του ηλεκτρονικού ταχυδρομείου SMTP που περιγράψαμε προηγουμένως. Το FTP συνδυάζει δύο διαφορετικές συνδέσεις. Στη μία σύνδεση (γνωστή και ως κανάλι εντολών) το FTP στέλνει εντολές για τις ενέργειες που θα γίνουν. Αρχικά, η επικοινωνία μοιάζει με αυτή του ηλεκτρονικού ταχυδρομείου με εντολές όπως “δώσε μου

πρόσβαση με όνομα χρήστη X” και “ο κωδικός μου είναι ο Y”. Μετά την επιτυχή αναγνώριση του χρήστη στέλνονται εντολές του τύπου “πήγαινε στον κατάλογο Z”, “δείξε μου τα αρχεία του καταλόγου” και τέλος “στείλε μου το αρχείο A”. Μια πλήρης τέτοια συνομιλία πελάτη - εξυπηρετητή φαίνεται παρακάτω:

```
[13:56:31][pulstar]$ ftp www.freebsdworld.gr
Connected to freebsdworld.gr.
220----- Welcome to Pure-FTPD [privsep] [TLS] -----
220-You are user number 2 of 50 allowed.
220-Local time is now 05:56. Server port: 21.
220 You will be disconnected after 15 minutes of inactivity.
Name (www.freebsdworld.gr:user1): user1
331 User user1 OK. Password required
Password:
230-User user1 has group access to: user1
230 OK. Current restricted directory is /
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
drwxr-x--- 12 user1 user1 4096 Nov  9 16:01 .
drwx--x--x 12 user1 user1 4096 Feb 12 15:54 ..
drwxr-xr-x  2 user1 user1 4096 Oct 26 08:53 etc
drwxr-x---  8 user1 user1 4096 Dec 17 00:20 mail
-rw-r--r--  1 user1 user1 39228 Oct 27 16:41 php.ini
drwxr-x---  3 user1 user1 4096 Oct 26 08:53 public_ftp
drwxr-x--- 12 user1 user1 4096 Nov  9 16:01 public_html
226 7 matches total
ftp> cd public_html
250 OK. Current directory is /public_html
drwxr-x--- 12 user1 user1 4096 Nov  9 16:01 .
drwx--x--x 12 user1 user1 4096 Feb 12 15:54 ..
drwxr-xr-x  2 user1 user1 4096 Sep 16 13:40 scripts
-rw-r--r--  1 user1 user1 31877 Oct 26 11:10 site-logo.png
226 4 matches total
ftp> get site-logo.png
local: site-logo.png remote: site-logo.png
229 Extended Passive mode OK (|||11932|)
150-Accepted data connection
150 31.1 kbytes to download
100% |*****| 31877 40.25 KiB/s
226-File successfully transferred
```

```
226 0.004 seconds (measured here), 7.90 Mbytes per second
31877 bytes received in 00:00 (40.23 KiB/s)
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 32 kbytes.
221 Logout.
```

Μετά τις εντολές για την αποστολή δεδομένων, ζεκινάει η δεύτερη σύνδεση για την μετάδοση των δεδομένων. Στο παραπάνω παράδειγμα βλέπουμε την επιτυχή εκκίνηση της δεύτερης σύνδεσης με το μήνυμα του εξυπηρετητή FTP “150-Accepted data connection”. Στο ηλεκτρονικό ταχυδρομείο τόσο η μεταφορά των δεδομένων όσο και των εντολών γίνεται από την ίδια σύνδεση. Στο πρωτόκολλο FTP, επειδή συνήθως η μεταφορά των αρχείων χρειάζεται περισσότερο χρόνο (τα email είναι συνήθως μικρά), οι σχεδιαστές του πρωτοκόλλου θέλησαν να δώσουν τη δυνατότητα στο χρήστη της υπηρεσίας να μπορεί να στέλνει εντολές την ώρα που ήδη εκτελείται κάποια μεταφορά. Για παράδειγμα, την ώρα που εκτελείται η μεταφορά μπορεί ο χρήστης να θέλει να υποβάλλει κάποια ερώτηση (π.χ. να δει τα περιεχόμενα ενός άλλου καταλόγου) ή ακόμα και να διακόψει (ακυρώσει) την μεταφορά. Σύμφωνα με το πρότυπο, για τις εντολές χρησιμοποιείται το TCP port 21 (command channel) ενώ για την μεταφορά των δεδομένων το TCP port 20 (data channel).

Σημείωση: Το πρωτόκολλο FTP υποστηρίζει ένα ακόμα τρόπο μετάδοσης δεδομένων στον οποίο το κανάλι δεδομένων επιλέγεται μετά από συνεννόηση μεταξύ πελάτη και εξυπηρετητή, και ονομάζεται *passive mode*. Φαίνεται και στο παράδειγμα που δώσαμε παραπάνω, καθώς υπάρχει το μήνυμα “229 Extended Passive mode OK”.

Εκτός από το πρωτόκολλο FTP, για την μεταφορά αρχείων υπάρχει και το *TFTP*, *Trivial File Transfer Protocol* ή *Πρωτόκολλο Απλής Μεταφοράς Αρχείων*. Είναι στην ουσία μια εξαιρετικά απλοποιημένη εκδοχή του FTP η οποία δεν διαθέτει κανένα είδος ασφάλειας ή εξουσιοδότησης και ουσιαστικά δεν προορίζεται για χρήση έξω από τοπικό δίκτυο. Το TFTP χρησιμοποιεί το UDP ως πρωτόκολλο στο επίπεδο μεταφοράς.

Απομακρυσμένη Σύνδεση - Telnet (Telecommunications Network ή Teletype Network)

Το πρόγραμμα *Απομακρυσμένης Σύνδεσης Telnet* επιτρέπει την προσπέλαση σε εφαρμογές που βρίσκονται εγκατεστημένες σε ένα υπολογιστή του δικτύου, από οποιοδήποτε άλλο υπολογιστή που είναι συνδεδεμένος σε αυτό το δίκτυο. Με το telnet

μπορεί ένας χρήστης που δουλεύει στον υπολογιστή του, να συνδεθεί με ένα απομακρυσμένο υπολογιστή και να τον χειρίζεται από το τερματικό του, σαν να βρισκόταν μπροστά στην κονσόλα του. Μπορεί πρακτικά να εκτελέσει οποιαδήποτε εφαρμογή βρίσκεται εγκατεστημένη στον απομακρυσμένο υπολογιστή εφόσον αυτή βασίζεται σε περιβάλλον κειμένου, καθώς και να εκτελέσει εντολές του λειτουργικού συστήματος του απομακρυσμένου υπολογιστή (το Telnet είναι μια υπηρεσία που κατά βάση παρέχεται σε υπολογιστές που εκτελούν συστήματα τύπου UNIX). Ο απομακρυσμένος υπολογιστής μπορεί να βρίσκεται οπουδήποτε, αρκεί να έχει δυνατότητα σύνδεσης με τον υπολογιστή που εκτελεί τον εξυπηρετητή telnet, ακόμα και μέσω του Internet.

Προφανώς για να είναι δυνατή η χρήση του εξυπηρετητή Telnet από κάποιο απομακρυσμένο χρήστη, ο χρήστης αυτός θα πρέπει να έχει δικαιώματα πρόσβασης (όνομα και κωδικό) στον εξυπηρετητή. Το όνομα και ο κωδικός ζητούνται στην αρχή της σύνδεσης και πρέπει να επαληθευτούν πριν ο χρήστης αρχίσει να εκτελεί εντολές και προγράμματα στον εξυπηρετητή.

Σημείωση: Όπως και με το FTP, έτσι και το telnet στέλνει το όνομα χρήστη και τον κωδικό ως απλό κείμενο (χωρίς κρυπτογράφηση) μέσα από το δίκτυο. Γενικά όλη η επικοινωνία γίνεται χωρίς κανένα είδος κρυπτογράφησης που σημαίνει ότι μπορεί να υποκλαπεί εύκολα όλη η “συνομιλία” από κάποιο ενδιάμεσο υπολογιστή. Για το λόγο αυτό το telnet πρακτικά δεν χρησιμοποιείται στις μέρες μας και έχει αντικατασταθεί από το πρωτόκολλο SSH, Secure Shell στο οποίο τα πάντα είναι κρυπτογραφημένα.

Επειδή οι εφαρμογές που εκτελούνται σε ένα υπολογιστή είναι ως ένα βαθμό εξαρτημένες από τον τύπο του υπολογιστή, θα πρέπει για την απομακρυσμένη σύνδεση να υπάρχει ένα πρωτόκολλο που θα εξασφαλίζει την επικοινωνία μεταξύ του τερματικού που χρησιμοποιεί ο χρήστης στον τοπικό του υπολογιστή με αυτό που διαθέτει ο απομακρυσμένος εξυπηρετητής και για το οποίο είναι γραμμένη η εφαρμογή.

Σημείωση: Στο UNIX η έννοια του τερματικού σχετίζεται μεταξύ άλλων και με τους ειδικούς χαρακτήρες ελέγχου που στέλνονται για να εκτελεσθούν λειτουργίες όπως αλλαγή χρωμάτων, καθαρισμός της οθόνης κλπ. Τα κλασικά τερματικά σε ένα UNIX σύστημα συνδέονται με σειριακές συνδέσεις στον κεντρικό υπολογιστή και υπάρχουν κάποια πρότυπα που ορίζουν ποιες εντολές καταλαβαίνουν. Για παράδειγμα, διαφορετικές εντολές καταλαβαίνει ένα τερματικό με δυνατότητα απεικόνισης χρωμάτων και άλλες ένα μονόχρωμο. Όταν το τερματικό μας δεν είναι πραγματικό, αλλά εικονικό όπως σε αυτή την περίπτωση θα πρέπει να συμπεριφέρεται με τον ίδιο τρόπο και να καταλαβαίνει τις ίδιες εντολές με κάποιο από τα έτοιμα πρό-

τυπα που αναγνωρίζει ο εξυπηρετητής Telnet. Τα περισσότερα προγράμματα telnet για πελάτες υποστηρίζουν εξομοίωση μεγάλου πλήθους τερματικών.

Η λειτουργία αυτή υποστηρίζεται από το πρωτόκολλο Telnet το οποίο υλοποιεί την ιδέα του εικονικού τερματικού στην τεχνολογία TCP/IP. Το εικονικό τερματικό αποτελεί τον ενδιάμεσο μεταξύ του τερματικού του εξυπηρετητή και του πελάτη telnet. Τα τερματικά εκτελούν την απαραίτητα αντιστοίχιση και μετατροπή των καταστάσεων σε αυτές του εικονικού τερματικού ώστε να υπάρχει μια κοινή γλώσσα επικοινωνίας. Έτσι π.χ. καθορίζονται μέσω του Telnet και οι παράμετροι επικοινωνίας και τα χαρακτηριστικά του τερματικού που πρέπει να χρησιμοποιούνται τόσο από τη μεριά του πελάτη όσο και από τη μεριά του εξυπηρετητή.

Το πρωτόκολλο Telnet όπως και τα FTP και SMTP ακολουθεί το μοντέλο πελάτη – εξυπηρετητή. Πελάτης είναι ο υπολογιστής ο οποίος ξεκινάει την επικοινωνία και εξυπηρετητής είναι ο απομακρυσμένο υπολογιστής που εκτελεί τον αντίστοιχο εξυπηρετητή Telnet και δέχεται τις εισερχόμενες συνδέσεις. Στο επίπεδο μεταφοράς, το Telnet χρησιμοποιεί το πρωτόκολλο TCP και χρησιμοποιεί για την επικοινωνία του το TCP port 23.

Όταν ξεκινά η εκτέλεση του προγράμματος, γίνεται αρχικά η ταυτοποίηση του χρήστη μέσω του ονόματος και του κωδικού που του έχει αποδοθεί. Οτιδήποτε γράφει ο χρήστης στο τερματικό του μεταφέρεται και εκτελείται στον εξυπηρετητή Telnet. Αντίστοιχα μεταφέρονται και τα αποτελέσματα (έξοδος) των εντολών του, από τον εξυπηρετητή στο τερματικό του. Είναι κυριολεκτικά σαν να βρίσκεται μπροστά στον εξυπηρετητή. Μεταξύ των δύο μηχανημάτων υπάρχει μόνο μια σύνδεση από την οποία μεταφέρονται εντολές και δεδομένα. Όταν ο χρήστης χρειάζεται να στείλει κάποια εντολή που να μην απευθύνεται στον απομακρυσμένο υπολογιστή αλλά για να εκτελέσει μια ρύθμιση του πρωτοκόλλου Telnet (π.χ. να αλλάξει τον τύπο του τερματικού ή κάποια επιλογή λειτουργίας) χρησιμοποιείται ένας ειδικός χαρακτήρας (χαρακτήρας διαφυγής) ο οποίος δηλώνει στο σύστημα ότι αυτό που ακολουθεί δεν είναι μια εντολή που πρέπει να ληφθεί από τον απομακρυσμένο υπολογιστή αλλά μια εντολή προς το πρωτόκολλο Telnet.

Παρακάτω φαίνεται μια ενδεικτική συνεδρία telnet:

```
[15:39:25] [sonic@pulstar:~]$ telnet pegasus
Trying 62.71.35.221...
Connected to pegasus.chania-lug.gr.
Escape character is '^]'.
```

FreeBSD/amd64 (pegasus.dyndns.org) (pts/3)

```

login: sonic
Password:
Last login: Mon Feb 15 15:39:14 from localhost
Copyright (c) 1992-2009 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

FreeBSD 8.0-RELEASE-p2 (PEGASUS) #1: Sat Jan 30 22:05:14 EET 2010

Welcome to FreeBSD!

[15:40:45] [sonic@pegasus:~]$ ls -d */
Desktop/      data/      html/      notes/
GNUstep/      diktia-new/  logos/     original/
UNIX/         external/   logs/     page/
bin/          fonts/     multimedia/ some/
books/        freebsd-book/ nethome/  tarballs/

logout
Connection closed by foreign host.

```

Παγκόσμιος Ιστός (World Wide Web, WWW)

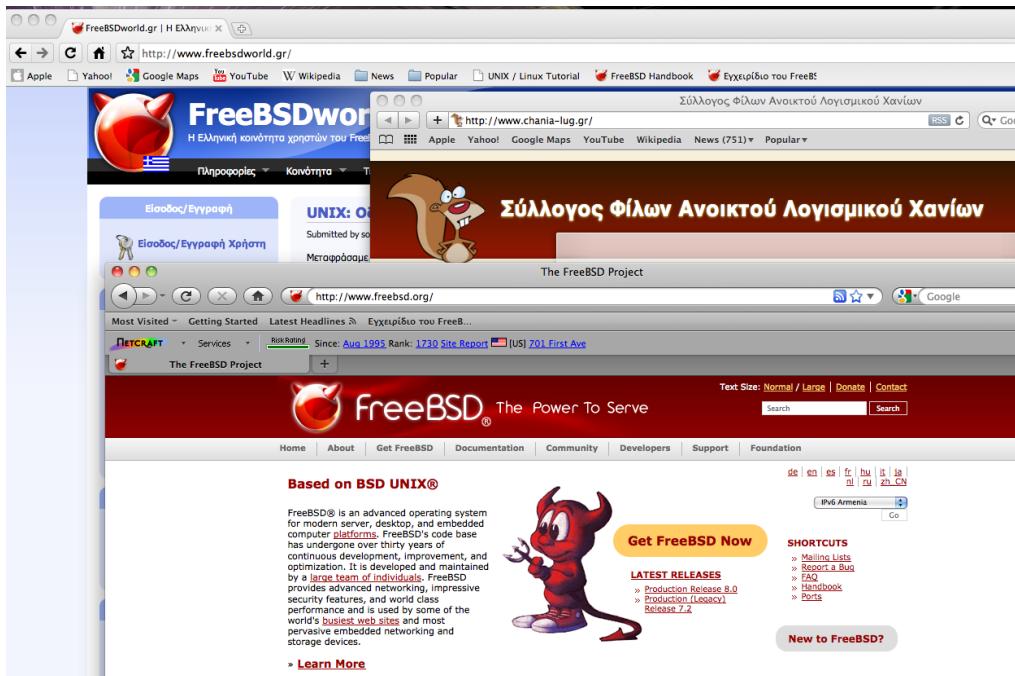
To *World Wide Web* ή *WWW* ή *Παγκόσμιος Ιστός* είναι ένα σύστημα που αρχικά δημιουργήθηκε για τη διακίνηση ακαδημαϊκών πληροφοριών μεταξύ ομάδων που βρίσκονταν σε απομακρυσμένες γεωγραφικά περιοχές. Το σύστημα του Παγκόσμιου Ιστού συνδυάζει τις τεχνικές ανάκλησης πληροφοριών με την τεχνολογία των υπερκειμένων για την δημιουργία ενός παγκόσμιου και εύκολου στη χρήση συστήματος πληροφοριών.

Η πληροφορία είναι δομημένη με μορφή υπερμέσων - *hypermedia* δηλ. περιλαμβάνει εκτός από κείμενο και εικόνες, ήχο και video ή γενικότερα οποιαδήποτε μορφή πολυμέσων. Ο παγκόσμιος ιστός είναι μια πλατφόρμα που υποστηρίζει την επικοινωνία πολυμέσων μέσω ενός γραφικού περιβάλλοντος επικοινωνίας με το χρήστη. Με άλλα λόγια, ο παγκόσμιος ιστός αποτελεί ένα γραφικό τρόπος απεικόνισης και μετάδοσης των πληροφοριών. Το περιβάλλον αυτό μας παρέχει την δυνατότητα να χρησιμοποιήσουμε τους δεσμούς ή *links* για να μετακινηθούμε μέσα στο Διαδίκτυο.

Το υπερκείμενο είναι μια μορφή παρουσίασης κειμένου στην οποία η διαδοχή των τμημάτων του δεν ακολουθεί αναγκαστικά τη σειρά παρουσίασης που επιβάλλεται

από τη σελιδοποίηση του. Οι αυτοτελείς ενότητες υπερκειμένου που προβάλλονται στην οθόνη ονομάζονται *ιστοσελίδες*. Σε μια ιστοσελίδα, τα τμήματα που παραπέμπουν σε άλλα τμήματα της ίδιας ή διαφορετικής ιστοσελίδας ονομάζονται *κόμβοι*. Οι αναφορές ή παραπομπές ενός τμήματος σε ένα άλλο ονομάζονται *δεσμοί* ή *σύνδεσμοι* (*links*).

Με τη χρήση των συνδέσμων, ο χρήστης/αναγνώστης της σελίδας δεν είναι υποχρεωμένος να διαβάζει απλά το κείμενο με τη σειρά που εμφανίζεται, αλλά μπορεί να περιηγηθεί στα διάφορα τμήματα της σελίδας (κόμβους) ή ακόμα και σε άλλες ιστοσελίδες ή δικτυακούς τόπους έξω από αυτόν που επισκέφτηκε αρχικά. Το γραφικό περιβάλλον επικοινωνίας επιτρέπει στο χρήστη να εντοπίσει εύκολα τα κομμάτια που αποτελούν συνδέσμους δείχνοντας τις ως λέξεις φωτισμένες, υπογραμμισμένες ή με διαφορετικό χρώμα (highlighted). Τα προγράμματα τα οποία χρησιμοποιούνται για την περιήγηση στον παγκόσμιο ιστό είναι γνωστά ως όργανα πλοιήγησης – περιήγησης, περιηγητές, φυλλομετρητές ή *browsers*. Ο όρος περιήγηση προέρχεται ακριβώς από τη δυνατότητα του χρήστη να διαβάζει το κείμενο με τη σειρά που αυτός επιθυμεί καθώς και να χρησιμοποιεί τους συνδέσμους για να μετακινείται σε διαφορετικά τμήματα του ή και άλλες ιστοσελίδες και τόπους.



Σχήμα 7.36: Τρεις γνωστοί *browsers*: Google Chrome, Mozilla Firefox, Apple Safari

Τα τελευταία χρόνια, με την εξέλιξη των πληροφοριακών συστημάτων αλλά και της ταχύτητας πρόσβασης των απλών οικιακών συνδέσεων, έγινε δυνατόν να συμπερι-

λαμβάνονται μέσα στο υπερκείμενο και στοιχεία πολυμέσων που απαιτούν αρκετά μεγαλύτερο όγκο πληροφοριών, όπως ήχος και κινούμενη εικόνα (video). Γενικά τα συστήματα υπερκειμένου που περιλαμβάνουν και άλλες μορφές μέσων εκτός από κείμενο ονομάζονται υπερμέσα (*hypermedia*).

Αν και μέσω του WWW μπορούμε να έχουμε πρόσβαση σε όλα σχεδόν τα πρωτόκολλα τεχνολογίας Διαδικτύου (εφαρμογών) όπως το FTP, κατά βάση το πρωτόκολλο που χρησιμοποιούμε για τη μεταφορά υπερκειμένου είναι το *Πρωτόκολλο Μεταφοράς Υπερκειμένου, HTTP, Hypertext Transfer Protocol*. Και αυτό το πρωτόκολλο βασίζεται στο μοντέλο πελάτη – εξυπηρετητή. Οι εξυπηρετητές του παγκόσμιου ιστού (γνωστοί και ως *Web Servers*) είναι μηχανήματα με μόνιμη σύνδεση στο Διαδίκτυο και φιλοξενούν τις ιστοσελίδες που είναι διαθέσιμες για πρόσβαση. Μέσω των σελίδων αυτών παρέχεται ένα σημείο παρουσίας στο Διαδίκτυο τόσο για οργανισμούς και επιχειρήσεις, όσο και για ιδιώτες.

Για την πρόσβαση σε αυτές τις σελίδες, χρειάζεται να χρησιμοποιήσουμε κάποια από τα προγράμματα – πελάτες που έχουν αναπτυχθεί και είναι όπως αναφέραμε οι *browsers*. Υπάρχουν *browsers* για κάθε πλατφόρμα και λειτουργικό σύστημα υπολογιστή. Κάποιοι γνωστοί *browsers* είναι σήμερα ο Mozilla Firefox, ο MS Internet Explorer και ο Opera.

Κάθε οργανισμός, επιχείρηση ή ιδιώτης μπορεί να κατασκευάσει το δικό του σημείο παρουσίας στο Διαδίκτυο. Αυτό συνήθως αποτελείται από ένα εξυπηρετητή συνδεδεμένο στο Διαδίκτυο σε μόνιμη βάση, ο οποίος και φιλοξενεί τις αντίστοιχες ιστοσελίδες. Οι μεγάλες επιχειρήσεις και οργανισμοί συνήθως διαθέτουν τους δικούς τους εξυπηρετητές αλλά μικρότεροι χρήστες μπορούν να φιλοξενήσουν τις σελίδες στους εξυπηρετητές των εταιριών παροχής υπηρεσιών Διαδικτύου (ISPs, Internet Service Providers). Οι εξυπηρετητές αυτοί είναι οργανωμένοι με τέτοιο τρόπο ώστε να μπορούν να φιλοξενήσουν πολλούς διαφορετικούς δικτυακούς τόπους από πολλούς χρήστες.

Σήμερα μέσω του παγκόσμιου ιστού μπορεί οποιοσδήποτε να έχει πρόσβαση σε διάφορες πληροφορίες από διάφορες πηγές σε διαφορετικά σημεία της γης. Η πρόσβαση είναι δυνατή μέσω της διεύθυνσης παγκόσμιου ιστού (διεύθυνση WWW). Σε κάθε θέση παγκόσμιου ιστού (web site) και κεντρική ιστοσελίδα εταιρίας ή οργανισμού (home page) ανατίθεται μια μοναδική διεύθυνση www. Λόγω του μεγάλου αριθμού των κεντρικών ιστοσελίδων, είναι αδύνατο να τις θυμόμαστε όλες. Για το σκοπό αυτό κάνουμε την περιήγηση μας σε αυτές συνήθως μέσω συνδέσμων από άλλες σελίδες ή χρησιμοποιούμε κάποια από τις μηχανές αναζήτησης για να τις εντοπίσουμε.

Οι μηχανές αναζήτησης είναι ειδικές τοποθεσίες που έχουν αναπτυχθεί στο Internet με σκοπό να μας βοηθήσουν να βρούμε ιστοσελίδες και τοποθεσίες σχετικές με τις πληροφορίες που ψάχνουμε. Οι μηχανές αναζήτησης ανακαλύπτουν και στη συ-

νέχεια ταξινομούν στη βάση δεδομένων που διαθέτουν κάθε νέα ιστοσελίδα. Σε μια δική μας αναζήτηση, συμβουλεύονται αυτή τη βάση για να μας παρέχουν μια σειρά από αποτελέσματα σχετικά με τις λέξεις – κλειδιά που χρησιμοποιήσαμε. Μερικά παραδείγματα γνωστών μηχανών αναζήτησης είναι το Google, το Google, το Google, το Bing, το Yahoo κλπ.

Η δημοτικότητα του παγκόσμιου ιστού είναι εκπληκτική: Το 1993 υπήρχαν 130 Web sites, το 1994 ξεπέρασαν τις 10000, το 1996 τις 100000 και το 1997 τις 650000. Το Δεκέμβρη του 2009 υπήρχαν περισσότερα από 200000000 (διακόσια εκατομμύρια!) sites. Όσο αφορά την κίνηση, το 1994 ο παγκόσμιος ιστός είχε το 6% της συνολικής κίνησης του Internet ενώ το 1995 το ποσοστό έφτασε το 24%. Ο αριθμός χρηστών του παγκόσμιου ιστού ήταν 5 εκατομμύρια το 1996, 22 εκατομμύρια το 1996 και περισσότερο από 1.5 δις. το 2009!

Σημείωση: Μπορείτε να βρείτε πολλά χρήσιμα στοιχεία και στατιστικά για το διαδίκτυο στην ιστοσελίδα της Netcraft, <http://www.netcraft.com>

Ασύρματο Διαδίκτυο

Η ανάπτυξη του Ασύρματου Πρωτοκόλλου Εφαρμογής, WAP, *Wireless Application Protocol* σε συνδυασμό με την παρουσίαση των πρώτων συσκευών (κινητών) που το υποστηρίζουν, δίνουν τη δυνατότητα στους χρήστες κινητών τηλεφώνων να έχουν ασύρματη διασύνδεση στο Internet. Σήμερα, μπορεί κανείς με το κινητό του τηλέφωνο να:

- Περιπλανηθεί στο Internet και να εκτελέσει συναλλαγές
- Αναζητήσει πληροφορίες από βάσεις δεδομένων
- Στέλνει και να δέχεται email
- Ενημερώνεται για τους τραπεζικούς του λογαριασμούς και να εκτελεί συναλλαγές με αυτούς (μεταφορά χρημάτων)
- Ενημερώνεται για την (χάλια) πορεία του Χρηματιστηρίου

Σημείωση: Σήμερα η τεχνολογία WAP στην οποία αναφέρεται το βιβλίο έχει αντικατασταθεί από πιο σύγχρονες με πολύ μεγαλύτερες ταχύτητες (3G, GPRS).

Ιδιωτικά Εσωτερικά Δίκτυα Τεχνολογίας TCP/IP (Intranets)

Τα τελευταία χρόνια αναπτύσσονται δίκτυα οργανισμών και επιχειρήσεων τα οποία χρησιμοποιούν τα πρωτόκολλα επικοινωνίας του Διαδικτύου αλλά και τα πρότυπα

περιεχομένων του Παγκόσμιου Ιστού. Τα δίκτυα αυτά ονομάζονται *Iδιωτικά Εσωτερικά Δίκτυα τεχνολογίας TCP/IP* ή απλώς *Intranets*. Σε σχέση με τα παραδοσιακά δίκτυα, οι εφαρμογές που χρησιμοποιούνται στα Intranets βασίζονται στην τεχνολογία του Web. Κατά βάση δηλ. η πρόσβαση στις πληροφορίες σε αυτά τα δίκτυα γίνεται μέσω προγραμμάτων περιήγησης (browsers). Στις πληροφορίες αυτές συνήθως έχουν πρόσβαση μόνο οι εργαζόμενοι και τα μέλη του προσωπικού των αντίστοιχων εταιριών.

Με άλλα λόγια, το Intranet είναι ένα δίκτυο τύπου Internet στο εσωτερικό μιας επιχείρησης. Οι υπολογιστές της επιχείρησης επικοινωνούν μεταξύ τους με τον ίδιο τρόπο που επικοινωνούν μεταξύ τους και οι υπολογιστές στο Διαδίκτυο. Ένα δίκτυο Intranet μπορεί να εκτείνεται πέρα από την περιορισμένη περιοχή ενός τοπικού δικτύου: μπορεί να καλύπτει για παράδειγμα όλα τα γραφεία του οργανισμού ή της επιχείρησης, άσχετα με τη γεωγραφική τους θέση. Επιτρέπει όμως πρόσβαση μόνο εσωτερικά στον οργανισμό (με απλά λόγια, μπορεί να χρησιμοποιεί το δημόσιο Internet για να μεταφέρει δεδομένα, αυτά όμως και πάλι δεν είναι προσβάσιμα παρά μόνο στους εργαζόμενους του).

Χαρακτηριστικές υπηρεσίες που μπορεί να προσφέρει ένα Intranet είναι:

- Ηλεκτρονικό ταχυδρομείο
- Πρόσβαση και αναζήτηση πληροφοριών με χρήση εργαλείων Web (είτε πληροφοριών που βρίσκονται εσωτερικά στον οργανισμό, είτε στο Διαδίκτυο)
- Ηλεκτρονική διακίνηση εγγράφων

Τα Intranets είναι εύκολα επεκτάσιμα και παρέχουν εύκολη αναζήτηση και πρόσβαση στις πληροφορίες (μέσω WWW clients, browsers). Είναι συμβατά σχεδόν με όλες τις υπολογιστικές πλατφόρμες και μπορούν να ενσωματώσουν εύκολα τις ήδη υπάρχουσες πηγές πληροφοριών της επιχείρησης ή οργανισμού.

Τηλεφωνία μέσω Διαδικτύου

Μέσω του Διαδικτύου μπορούμε να έχουμε μετάδοση φωνής, παρακάμπτοντας το σταθερό τηλεφωνικό δίκτυο. Για να επιτύχουμε τηλεφωνία μέσω Διαδικτύου χρειαζόμαστε ειδικό λογισμικό το οποίο θα εγκαταστήσουμε σε ένα προσωπικό υπολογιστή με δυνατότητες πολυμέσων. Χρειαζόμαστε δηλ. κάρτα ήχου, μικρόφωνο και ηχεία (και προφανώς σύνδεση στο Διαδίκτυο).

Το λογισμικό σε πολλές περιπτώσεις επιτρέπει επικοινωνία half-duplex δηλ. όχι πλήρως αμφίδρομη. Αυτό σημαίνει ότι κάθε φορά μόνο ένας μιλάει και ο άλλος ακούει. Ανάλογα με την ταχύτητα και την ποιότητα της σύνδεσης είναι πολλές φορές δυνατή η επικοινωνία διπλής κατεύθυνσης (full-duplex). Σε κάθε περίπτωση θα πρέπει

να χρησιμοποιείται συμβατό λογισμικό και από τις δύο μεριές (κατά προτίμηση το ίδιο).



Σχήμα 7.37: Το γνωστό πρόγραμμα επικοινωνίας Skype

Είτε σε half είτε σε full duplex, η μετάδοση φωνής στα δίκτυα μεταγωγής πακέτου μπορεί να παρουσιάζει κάποια προβλήματα. Καθώς η ταχύτητα και η καθυστέρηση του δικτύου δεν είναι εγγυημένα (και ταυτόχρονα δεν υπάρχει μόνιμη σύνδεση μεταξύ των συνδρομητών όπως στο τηλεφωνικό δίκτυο) δημιουργούνται αρκετές φορές προβλήματα στην επικοινωνία (π.χ. διακοπές). Τα προβλήματα αυτά εντείνονται περισσότερο αν σκεφτούμε ότι η μετάδοση φωνής έχει ιδιαίτερες απαιτήσεις (εύρος ζώνης, συγχρονισμός κλπ). Σε περίπτωση απώλειας πακέτων ή μεγάλων καθυστερήσεων η ποιότητα της επικοινωνίας είναι χαμηλή.

Άλλο πρόβλημα είναι ότι πρέπει και τα δύο μέλη που πρόκειται να χρησιμοποιήσουν την υπηρεσία να έχουν συνεννοηθεί από πριν για την ώρα της κλήσης, καθώς τις περισσότερες φορές τα προγράμματα δεν παρέχουν την δυνατότητα να στείλουν σήμα κουδουνισμού στον καλούμενο.

Σημείωση: Από την εποχή που γράφτηκε το βιβλίο σας πολλά από αυτά έχουν αλλάξει. Σήμερα έχουμε ολόκληρο κομμάτι των δικτύων που ασχολείται με την επικοινωνία φωνής μέσω της τεχνολογία TCP/IP – το γνωστό μας VoIP, Voice Over IP. Χάρις στις αυξημένες ταχύτητες του σημερινού Διαδικτύου, τα περισσότερα προβλήματα επικοινωνίας φωνής με τη βοήθεια λογισμικού έχουν περιοριστεί σημαντικά ή εξαφανιστεί. Η επικοινωνία μπορεί πλέον να είναι πάντα διπλής κατεύθυνσης και να συνδυάζεται με video (video κλήση). Ταυτόχρονα τα προγράμματα έχουν τη δυνατότητα να εκτελούν κλήσεις όπως το κανονικό τηλέφωνο και να στέλνουν σήμα κουδουνισμού στον καλούμενο.

Μετάδοση Εικόνας και Ήχου μέσω Διαδικτύου

Αρχικά, η μετάδοση δεδομένων εικόνας και ήχου μέσω του Διαδικτύου παρουσίαζε κάποιες ιδιαίτερες δυσκολίες. Για παράδειγμα, τα αρχεία video έχουν αρκετά μεγάλο μέγεθος και επίσης για να αναπαράγονται την ώρα που κατεβαίνουν (streaming), θα πρέπει η σύνδεση να διατηρείται σε μια συγκεκριμένη και σχετικά υψηλή ταχύτητα.

Για να γίνει δυνατή η μετάδοση video μέσω του Διαδικτύου, αναπτύχθηκαν κάποιες τεχνικές συμπίεσης και πρωτόκολλα τα οποία έχουν σκοπό να μειώσουν τόσο το τελικό μέγεθος του αρχείου, όσο και το ρυθμό μετάδοσης (bitrate) που απαιτείται για να αναπαραχθεί. Η συμπίεση ελαχιστοποιεί την πληροφορία που πρέπει να μεταδοθεί από το ένα καρέ στο επόμενο, ώστε να μειωθεί το εύρος ζώνης που απαιτείται για να παρακολουθήσουμε “ζωντανά” ένα video από το Διαδίκτυο. Ταυτόχρονα οι αλγόριθμοι συμπίεσης που χρησιμοποιούνται προσπαθούν να διασφαλίσουν ότι δεν μειώνεται (κατά το δυνατόν) η ποιότητα του video κατά τη διαδικασία αυτή.

Για τις τεχνικές συμπίεσης αναπτύχθηκαν τα συστήματα MPEG1 και MPEG2 ενώ για τη μετάδοση εικόνας και ήχου στο Διαδίκτυο, αναπτύχθηκε το πρωτόκολλο H.323. Η ποιότητα της μεταδιδόμενης εικόνας φτάνει τα 12-15 καρέ το δευτερόλεπτο, το οποίο δεν είναι ακόμα το επιθυμητό (25-30 καρέ το δευτερόλεπτο).

Η συμπίεση των αρχείων σε συνδυασμό με την εμφάνιση νέων τεχνικών μετάδοσης αλλά και την αύξηση του τοπικού αποθηκευτικού χώρου στους υπολογιστές των χρηστών συντελούν στον περιορισμό των προβλημάτων μετάδοσης. Σήμερα είναι δυνατόν οι χρήστες να συνδέονται και να ανταλλάσσουν μεταξύ τους αρχεία πολυμέσων. Είναι επίσης δυνατή η τηλεδιάσκεψη, όπου οι χρήστες μπορούν να συζητούν βλέποντας ταυτόχρονα ο ένας τον άλλο με τη βοήθεια κάμερας που συνδέεται στον υπολογιστή τους. Για να λειτουργεί ικανοποιητικά αυτό το σύστημα, θα πρέπει να έχουμε ταχύτητα σύνδεσης στο Internet τουλάχιστον 64Kbps.

Ένα παράδειγμα εφαρμογής για ομαδική επικοινωνία, είναι το πρόγραμμα CU - SeeMee που δημιουργήθηκε από ερευνητές στο Cornell University. Το πρόγραμμα αυτό επιτρέπει την επικοινωνία μέχρι 8-12 ατόμων ταυτόχρονα, με μετάδοση εικόνας και ήχου. Η εικόνα δεν μεταδίδεται συνέχεια, αλλά μόνο κάθε φορά που αυτή αλλάζει. Έτσι η μετάδοση εικόνας δεν είναι συνεχής (και εκλείπει σε φυσικότητα) αλλά τουλάχιστον είναι δυνατή.

Για την πραγματοποίηση τηλεδιάσκεψης μέσω διαδικτύου, απαιτείται υπολογιστής που προφανώς να διαθέτει ικανότητες πολυμέσων: κάρτα ήχου, μικρόφωνο, ηχεία και κάμερα. Φυσικά απαιτείται και το κατάλληλο λογισμικό, το οποίο πρέπει να χρησιμοποιείται (το ίδιο ή συμβατό) από όλους τους χρήστες της συγκεκριμένης επικοινωνίας.

Σημείωση: Όπως και προηγουμένως, η εξέλιξη της τεχνολογίας και της ταχύτητας των οικιακών συνδέσεων από την εποχή που γράφτηκε το σχολικό βιβλίο έχει καταστήσει τα περισσότερα από τα παραπάνω προβλήματα – και προγράμματα – ανύπαρκτα. Ένα βιβλίο που αναφέρει συγκεκριμένες τεχνικές και προγράμματα θα έπρεπε να αλλάζει κάθε σχολικό έτος, και αυτό έχει μάλλον κλείσει ήδη δεκαετία.

Συνομιλία Πραγματικού Χρόνου στο Διαδίκτυο με Μορφή Κειμένου

Μέσω του Διαδικτύου είναι δυνατόν να συζητάμε ανταλλάσσοντας με τους φίλους μας μηνύματα σε μορφή κειμένου, σε πραγματικό χρόνο. Τα μηνύματα και οι απαντήσεις που πληκτρολογούμε στον υπολογιστή μας, εμφανίζονται την ίδια στιγμή στις οθόνες όλων όσων συμμετέχουν στη συζήτηση μας.

Με τον τρόπο αυτό, μπορούμε να δημιουργήσουμε ομάδες χρηστών που συζητούν για συγκεκριμένα θέματα ειδικού ενδιαφέροντος. Ορίζονται έτσι χώροι (κανάλια) συζήτησης που καθένας μπορεί να πάρει μέρος ανάλογα με τα ενδιαφέροντα του. Τα προγράμματα χρησιμοποιούν το πρωτόκολλο TCP/IP και δεν χρειάζεται να αναπτυχθούν ειδικά πρωτόκολλα όπως στην περίπτωση μετάδοσης video. Για να συμμετέχουμε σε μια τέτοια συζήτηση, συνήθως απαιτούνται τα παρακάτω βήματα:

- Να εγκαταστήσουμε κατάλληλο λογισμικό στον υπολογιστή μας.
- Να συνδεθούμε στο Διαδίκτυο και να εκτελέσουμε το λογισμικό, δίνοντας και τη διεύθυνση του εξυπηρετητή ή του χρήστη με τον οποίο θα συνδεθούμε.
- Να περιμένουμε μέχρι να μας απαντήσει ο χρήστης ή κάποιος που βρίσκεται στην ομάδα συζήτησης ή το χώρο που συνδεθήκαμε.
- Μπορούμε έπειτα να ξεκινήσουμε την επικοινωνία μας. Σε πολλά προγράμματα εμφανίζονται σε διαφορετικά παράθυρα αυτά που πληκτρολογούμε εμείς

και αυτά που πληκτρολογούν οι άλλοι.

Υπάρχουν σήμερα πολλά προγράμματα που υποστηρίζουν την μετάδοση άμεσων μηνυμάτων και γραπτή συνομιλίας. Τα πλέον παλιά προγράμματα αναπτύχθηκαν για το UNIX, όπως για παράδειγμα το talk και η αντίστοιχη έκδοση Windows, wintalk. Ωστόσο σήμερα χρησιμοποιούνται πιο σύγχρονες εκδοχές. Ένα από τα πρώτα συστήματα επικοινωνίας με κανάλια και δυνατότητα άμεσης (ένας προς έναν) επικοινωνίας είναι το σύστημα *IRC, Internet Relay Chat*. Το σύστημα αυτό είναι ακόμα σε ευρεία χρήση και στις μέρες μας. Μερικά γνωστά προγράμματα για το IRC είναι το XChat, IRCII, miRC κ.α. Ταυτόχρονα σήμερα υπάρχουν πολλοί ακόμα τρόποι για συνομιλία κειμένου: MSN messenger, Google Talk, ακόμα και ιστοσελίδες που παρέχουν απευθείας αυτή τη δυνατότητα.

Ηλεκτρονικό Εμπόριο

Ο όρος “Ηλεκτρονικό Εμπόριο” αναφέρεται σε κάθε είδος εμπορικής δραστηριότητας που πραγματοποιείται με τη χρήση ηλεκτρονικών μέσων. Η χρήση τηλεπικοινωνιακών δικτύων προσφέρει την δυνατότητα πραγματοποίησης συναλλαγών από μακριά, χωρίς τη φυσική παρουσία του πελάτη, και χωρίς φυσικά την ανάγκη να υπάρχει πραγματικό μαγαζί! Οι συναλλαγές πραγματοποιούνται ηλεκτρονικά, χωρίς τη χρήση χαρτιού ή φαξ, αλλά με τη βοήθεια υπολογιστών που συνδέονται στο Internet.

Το ηλεκτρονικό εμπόριο δεν αναφέρεται σε κάποια συγκεκριμένη τεχνολογία, αλλά περιλαμβάνει όλους τους μηχανισμούς και τεχνολογίες που απαιτούνται για την ολοκλήρωση μιας εμπορικής συναλλαγής μέσω υπολογιστών. Ένα παράδειγμα τέτοιου μηχανισμού είναι η *Ηλεκτρονική Ανταλλαγή Δεδομένων, EDI, Electronic Data Interchange* που ορίζει μια τυποποιημένη μορφή ανταλλαγής πληροφοριών. Ένας άλλος μηχανισμός είναι το γνωστό μας email.

Μια εταιρία που επιθυμεί να παρέχει υπηρεσίες ηλεκτρονικού εμπορίου ακολουθεί συνήθως την παρακάτω πρακτική:

- Αρχικά δημιουργείται μια δικτυακή τοποθεσία (web site) στο Διαδίκτυο, στο οποίο υπάρχουν κατάλογοι με τα προϊόντα της εταιρίας.
- Μέσα από τις ιστοσελίδες, παρέχεται η δυνατότητα προς τους πελάτες να επικοινωνήσουν με την εταιρία για να κάνουν την παραγγελία τους. Η επικοινωνία μπορεί να γίνεται μέσω email ή τηλεφωνικά, ή ακόμα και απευθείας μέσω της σελίδας με τη βοήθεια της τεχνολογίας του *Καλαθιού Αγορών, Shopping Basket*.
- Αν η παραγγελία γίνεται τηλεφωνικά, ο πελάτης εξυπηρετείται από κάποιο αντιπρόσωπο που απαντάει στην κλήση. Σε περίπτωση πλήρους ηλεκτρονικής

παραγγελίας, το μήνυμα ή παραγγελία παραλαμβάνεται από τον αντίστοιχο υπεύθυνο για να γίνει η συγκέντρωση και αποστολή των προϊόντων.

- Τις περισσότερες φορές, η χρέωση του πελάτη γίνεται μέσω πιστωτικής κάρτας τα στοιχεία της οποίας υποβάλλονται μέσω του browser με τη βοήθεια ασφαλούς (κρυπτογραφημένης) σύνδεσης. Σε κάποιες περιπτώσεις είναι δυνατή η πληρωμή των προϊόντων κατά την παραλαβή τους.
- Τα προϊόντα αποστέλλονται στον πελάτη, είτε ηλεκτρονικά (αν είναι π.χ. λογισμικό το οποίο ο πελάτης μπορεί να συνδεθεί και να κατεβάσει) είτε μέσω μεταφορικής εταιρίας.

Αν και αρχικά υπήρχε η αντίληψη ότι το ηλεκτρονικό εμπόριο είναι κατάλληλο για συγκεκριμένες κατηγορίες προϊόντων (συνήθως βιβλία, εξαρτήματα υπολογιστών, μουσική, λογισμικό), σήμερα έχει επεκταθεί σε άλλους τομείς όπως έπιπλα, τρόφιμα, παιχνίδια, λουλούδια και σχεδόν οτιδήποτε πωλείται και μέσω του κλασικού εμπορίου. Τα τελευταία χρόνια το ηλεκτρονικό εμπόριο αναπτύσσεται με ταχύτατους ρυθμούς, αλλά υπάρχουν ακόμα κάποια ζητήματα όπως είναι η προστασία, η ασφάλεια των συναλλαγών και η νομική κάλυψη των εμπλεκόμενων πλευρών.

Κεφάλαιο 8

Διαχείριση και Ασφάλεια Δικτύου

Εισαγωγή

Καθώς σήμερα η ανάγκη δικτύωσης γίνεται όλο και πιο επιτακτική, οι περισσότερες επιχειρήσεις διαθέτουν κάποιο είδος τοπικού δικτύου. Οι μεγαλύτερες εταιρίες έχουν προχωρήσει στη διασύνδεση των απομακρυσμένων υποκαταστημάτων τους με τεχνολογίες WAN ή και απευθείας μέσω του Διαδικτύου και τεχνολογιών VLAN.

Οι δομές των παραπάνω δικτύων μπορούν να γίνουν αρκετά πολύπλοκες. Σε μεγάλες εταιρίες, ακόμα και το τοπικό δίκτυο μπορεί να περιέχει αρκετές δικτυακές συσκευές και να είναι ιδιαίτερα πολύπλοκο. Ειδικά όταν έχουμε δικτυακές συσκευές από διάφορους κατασκευαστές, αυξάνεται ακόμα περισσότερο η δυσκολία διαχείρισης του δικτύου.

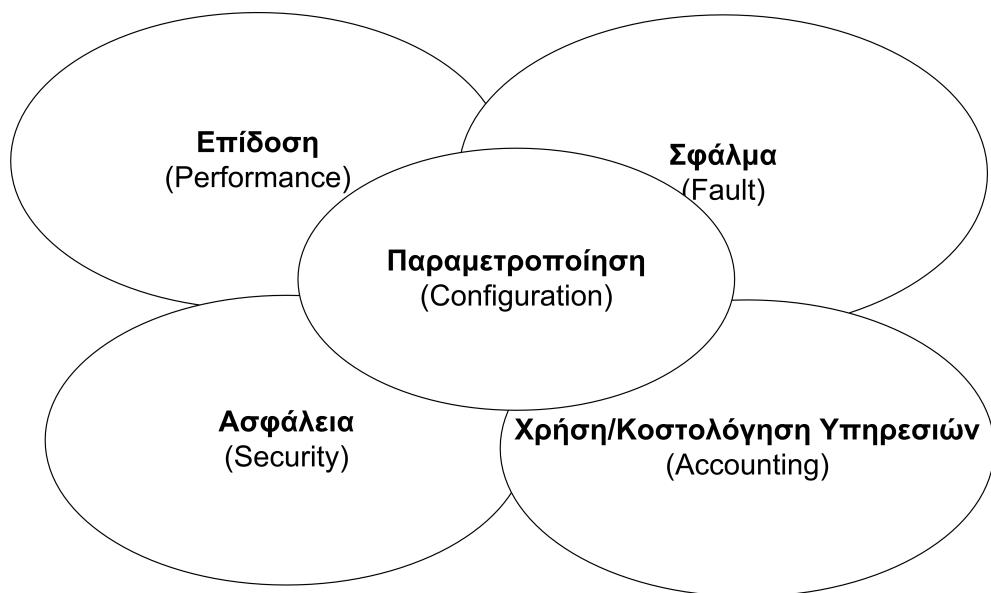
Είναι προφανές ότι υπάρχει ανάγκη για κεντρική διαχείριση σε κάθε πολύπλοκο ή/και κατανεμημένο δίκτυο. Η κεντρική διαχείριση μπορεί να παρουσιάζει δυσκολίες, καθώς συσκευές διαφορετικών κατασκευαστών μπορεί να υλοποιούν τους μηχανισμούς διαχείρισης με διαφορετικό τρόπο. Βρίσκεται και σήμερα σε εξέλιξη μια διαδικασία για τη δημιουργία προτύπων στον τομέα της διαχείρισης.

Ένα κομμάτι της διαχείρισης είναι και η ασφάλεια του δικτύου. Πρόκειται για ένα σύνθετο θέμα το οποίο περιλαμβάνει αρκετές παραμέτρους, και είναι πολύ σημαντικό να μπορούμε να τις ελέγχουμε κεντρικά. Και στον τομέα αυτό, γίνεται αυτή τη στιγμή προσπάθεια για τη δημιουργία προτύπων. Στις επόμενες ενότητες θα ασχοληθούμε με θέματα ασφάλειας και διαχείρισης δικτύων.

8.1 Διαχείριση Δικτύου

Ο Διεθνής Οργανισμός Πιστοποίησης (ISO, International Standards Organization) έχει ορίσει ένα πλαίσιο λειτουργιών (framework) που αφορά τη διαχείριση δικτύων και ανήκει στο μοντέλο του γνωστού μας OSI. Το μοντέλο αυτό ορίζει πέντε περιοχές διαχείρισης:

- Διαχείριση Παραμέτρων του Δικτύου (Configuration Management)
- Διαχείριση Επίδοσης του Δικτύου (Performance Management)
- Διαχείριση Σφαλμάτων (Fault Management)
- Διαχείριση Κόστους Υπηρεσιών (Accounting Management)
- Διαχείριση Ασφάλειας (Security Management)



Σχήμα 8.1: Η διαχείριση δικτύων κατά το μοντέλο OSI

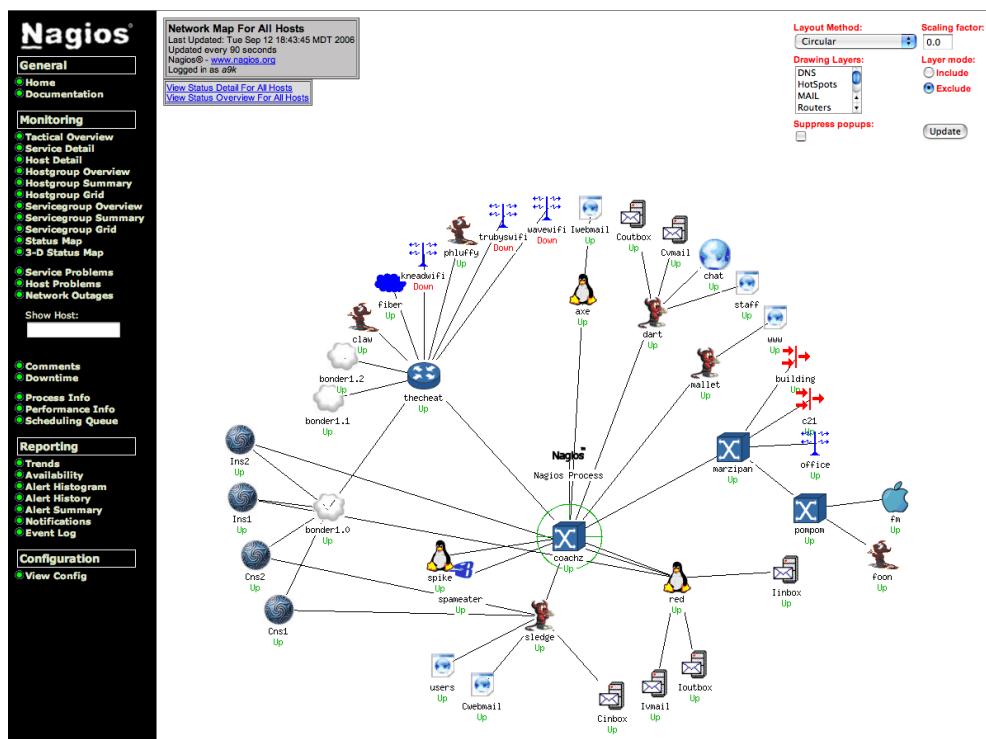
Θα εξετάσουμε αυτές τις πέντε περιοχές διαχείρισης παρακάτω.

8.1.1 Διαχείριση Παραμέτρων (Configuration Management)

Ο όρος διαχείριση παραμέτρων αναφέρεται στη διαδικασία αλλαγής της τοπολογίας του δικτύου και τη ρύθμιση των παραμέτρων των συσκευών. Οι ρυθμίσεις μπορούν να γίνονται στο επίπεδο του υλικού και του λογισμικού, προκειμένου το δίκτυο να

καλύπτει τις απαιτήσεις που έχουμε κάθε φορά. Η αρχική εγκατάσταση και ρύθμιση του δικτύου, δεν αποτελεί (σύμφωνα με τον επίσημο ορισμό του OSI) μέρος της διαχείρισης του. Ωστόσο τις περισσότερες φορές χρησιμοποιούμε τα ίδια εργαλεία (λογισμικό, εφαρμογές) και τεχνικές κατά την αρχική εγκατάσταση, όσο και μετέπειτα για τη συντήρηση του. Για το λόγο αυτό, η αρχική εγκατάσταση και διαμόρφωση ενός δικτύου θεωρείται από τους περισσότερους ως μέρος της διαχείρισης του.

Προκειμένου να είναι δυνατή η διαχείριση ενός δικτύου, ένα σημαντικό κομμάτι είναι η τεκμηρίωση (*documentation*). Τεκμηρίωση σε αυτή την περίπτωση είναι η καταγραφή των ρυθμίσεων και του τρόπου λειτουργίας κάθε συσκευής του δικτύου. Για παράδειγμα, μέρος της τεκμηρίωσης μπορεί να είναι τα πρωτόκολλα που χρησιμοποιούνται στο δίκτυο και οι ιδιαίτερες ρυθμίσεις τους σε κάθε συσκευή. Σε ένα switch μπορεί να είναι το πλήθος των θυρών που χρησιμοποιούνται και ποιο τμήμα του δικτύου είναι συνδεδεμένο σε ποια θύρα. Τέλος, για ένα μηχάνημα που έχει το ρόλο του *firewall* (τείχους προστασίας), η τεκμηρίωση θα αναφέρεται για παράδειγμα στις θύρες (TCP ports) που είναι ανοικτές. Η τεκμηρίωση επίσης αναφέρεται και σε γενικότερα θέματα, όπως η τοπολογία του δικτύου και ο τρόπος λειτουργίας του.



Σχήμα 8.2: Παράδειγμα προγράμματος διαχείρισης δικτύου

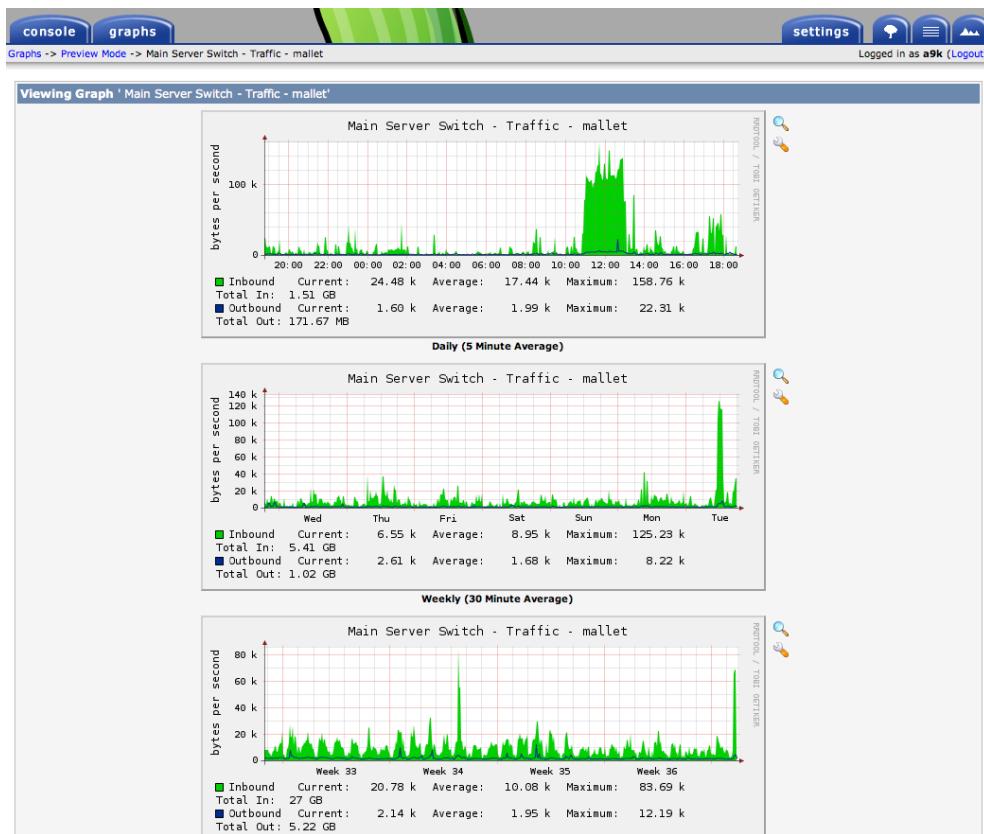
Η τεκμηρίωση μπορεί να βοηθηθεί αρκετά από την ύπαρξη λογισμικού που ανακαλύπτει και καταγράφει σε μια βάση δεδομένων καταλόγου υλικών (*inventory database*) όλες τις συσκευές ενός δικτύου και τον τρόπο διασύνδεσης τους. Προφανώς ένα τέτοιο πρόγραμμα μπορεί να ανακαλύψει μόνο ενεργές συσκευές ενός δικτύου (π.χ. δρομολογητές, υπολογιστές, switches κλπ). Το πρόγραμμα μπορεί επίσης να ανακαλύψει το είδος του τοπικού δικτύου (τμήματα ethernet, token ring κλπ) καθώς και τις όποιες γραμμές WAN ίσως υπάρχουν (μισθωμένες PPP, επιλεγόμενες dial-up / isdn, X.25, Frame Relay κλπ). Αν χρησιμοποιούμε λογισμικό που εκτελεί και λειτουργίες διαχείρισης δικτύου, τότε μπορεί να ανακαλύψει και υπολογιστές, εκτυπωτές και άλλες συσκευές. Οι εφαρμογές αυτές μπορούν συνήθως να αναπαραστήσουν γραφικά (δικτυακός χάρτης) τις συσκευές του δικτύου και την μεταξύ τους συνδεσμολογία.

8.1.2 Διαχείριση Επίδοσης του Δικτύου (Performance Management)

Για να διαχειριστούμε την απόδοση ενός δικτύου, πρέπει πρώτα να ορίσουμε ποια θα είναι τα μεγέθη που επιθυμούμε να μετρήσουμε. Έπειτα πρέπει να βρούμε τον τρόπο με τον οποίο θα γίνονται οι μετρήσεις μας και τέλος να τις υλοποιήσουμε. Τυπικά, σε ένα δίκτυο μετράμε ανά τακτά διαστήματα χαρακτηριστικά όπως τα παρακάτω:

- Το ποσοστό χρησιμοποίησης των γραμμών WAN ή τμημάτων του τοπικού δικτύου.
- Ανάλυση του ποσοστού κίνησης ανά πρωτόκολλο π.χ. TCP/IP, IPX, Netbios κλπ.
- Το ποσοστό λαθών σε σχέση με όλη την κίνηση.
- Το χρόνο καθυστέρησης σε διάφορα σημεία του δικτύου.
- Το χρόνο απόκρισης κάποιων συσκευών.
- Καθορισμένα κατώφλια (κρίσιμες μέγιστες ή ελάχιστες τιμές). Όταν οι τιμές των μετρούμενων παραμέτρων ξεφεύγουν από αυτά τα όρια, τότε εμφανίζονται κάποιοι συναγερμοί (alarms).

Οι μετρήσεις επίδοσης μπορεί να αποθηκεύονται για μελλοντική επεξεργασία και σύγκριση με επόμενες μετρήσεις. Υπεύθυνος για αυτή την επεξεργασία είναι ο διαχειριστής του δικτύου. Η ανάλυση των μετρήσεων μπορεί να καταδείξει τα σημεία που δημιουργούν προβληματική λειτουργία ή συμφόρηση του δικτύου. Με βάση τα συμπεράσματα των μετρήσεων μπορεί να γίνει ανασχεδίαση σημείων του δικτύου,



Σχήμα 8.3: Παρακολούθηση επιδόσεων δικτύου

αλλαγή υλικού ή ρυθμίσεων κλπ. Μετά τις αλλαγές, η σύγκριση με νέες μετρήσεις θα δείξει κατά πόσο ήταν επιτυχής η επίλυση του προβλήματος.

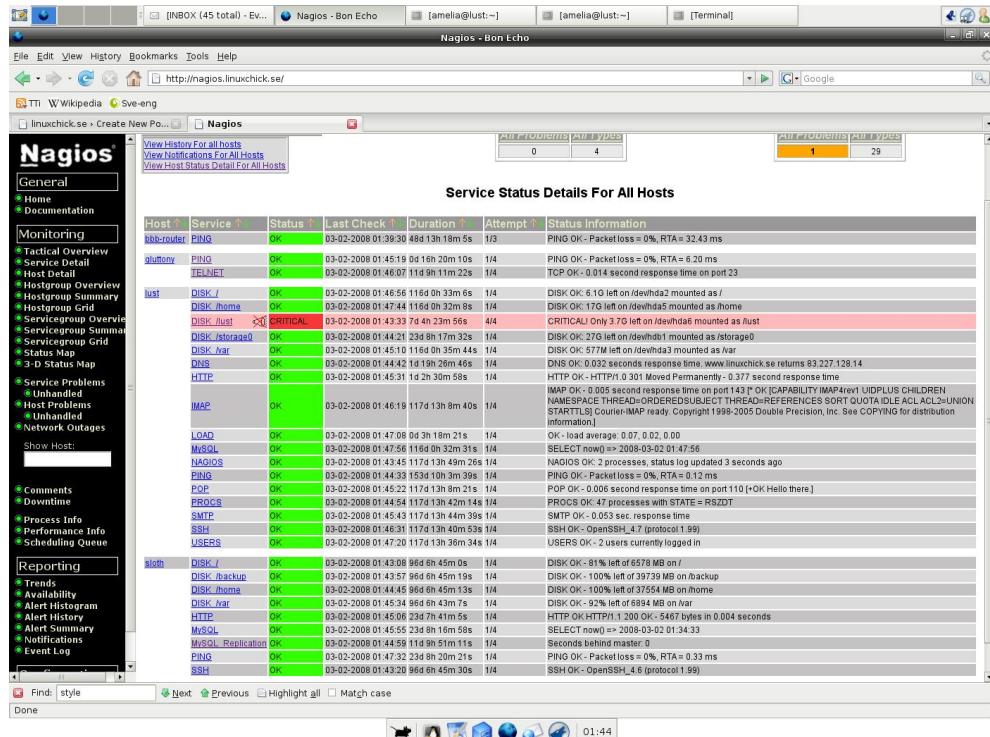
Τυπικά οι μετρούμενες τιμές καταγράφονται σε πίνακες και μπορούν επίσης να αναπαρίστανται με μορφή γραφημάτων (Σχήμα 8.3).

8.1.3 Διαχείριση Σφαλμάτων (Fault Management)

Με τη διαχείριση σφαλμάτων μπορούμε να εντοπίσουμε προβλήματα στη λειτουργία του δικτύου. Μπορούμε επίσης να βρούμε το σημείο στο δίκτυο που τα δημιουργεί και ενδεχομένως να το διορθώσουμε, αν πρόκειται απλώς για κάποια ρύθμιση. Σε περίπτωση που το πρόβλημα αφορά υλικό ή βρίσκεται εκτός της δικαιοδοσίας μας, μπορούμε να προωθήσουμε την περιγραφή του προβλήματος (να δημιουργήσουμε δηλ. κατάλληλη τεκμηρίωση) σε μια άλλη ομάδα που θα το αναλάβει.

Σε κάθε περίπτωση, γίνεται καταγραφή του προβλήματος καθώς και των βημάτων

που ακολουθήθηκαν για την επίλυση του, ώστε να υπάρχει έτοιμη λύση σε περίπτωση που το πρόβλημα εμφανιστεί ξανά στο μέλλον. Για κάποιες από τις συσκευές του δικτύου, ίσως να είναι χρήσιμο να τηρούνται στατιστικά σχετικά με το ποσοστό λαθών που εμφανίζουν.



Σχήμα 8.4: Παρακολούθηση σφαλμάτων

Μερικά προβλήματα μπορεί να είναι εύκολο να εντοπιστούν (χαλασμένη ή απενεργοποιημένη συσκευή). Ο σκοπός όμως της διαχείρισης είναι να μπορεί να προβλέψει προβλήματα πριν αυτά παρουσιαστούν και επηρεάσουν τους χρήστες του δικτύου. Η πρόβλεψη πιθανών προβλημάτων σχετίζεται άμεσα με τη διαχείριση επίδοσης του δικτύου.

Τα προβλήματα εμφανίζονται στο πρόγραμμα διαχείρισης με τη μορφή συναγερμών (alarms) και καταγράφονται συνήθως σε αρχεία καταγραφής (log files). Σε περίπτωση γραφικών απεικονίσεων, ενδεχομένως να απεικονίζονται οι προβληματικές συσκευές με διαφορετικό χρώμα. Ανάλογα με το πρόβλημα, μπορεί να χρειάζεται αποσύνδεση ή αντικατάσταση προβληματικών συσκευών από το δίκτυο ή αλλαγή των ρυθμίσεων στο λογισμικό των συσκευών.

8.1.4 Διαχείριση Κόστους (Accounting Management)

Το έργο της διαχείρισης κόστους του δικτύου περιλαμβάνει την παρακολούθηση της χρήσης των πόρων του δικτύου και την ανάλυση των διαθέσιμων ορίων χρήσης του δικτύου για συγκεκριμένες ομάδες χρηστών. Γίνεται ακόμα καταγραφή της χρήσης των πόρων του δικτύου ανά ομάδες χρηστών. Τέλος εξασφαλίζεται ότι οι χρήστες δεν χρησιμοποιούν υπηρεσίες που δεν είναι συμφωνημένες.

8.1.5 Διαχείριση Ασφάλειας (Security Management)

Η διαχείριση ασφάλειας περιλαμβάνει τον έλεγχο πρόσβασης σε συσκευές, δεδομένα και προγράμματα απέναντι σε κάθε μη-εξουσιοδοτημένη χρήση (ηθελημένη ή μη). Μπορούμε με αυτόν τον τρόπο να εντοπίσουμε τυχόν απόπειρες παραβίασης των κανόνων ασφαλείας του δικτύου και να λάβουμε τα απαραίτητα μέτρα. Το ζήτημα της ασφάλειας είναι αρκετά πολύπλοκο και θα το εξετάσουμε αναλυτικότερα σε επόμενες ενότητες.

Σε κάθε πληροφοριακό σύστημα που είναι κατανεμημένο, τα μέτρα ασφαλείας δεν πρέπει να εκτείνονται μόνο σε ένα ή μερικούς τομείς του, αλλά να καλύπτουν το σύνολο του. Ο οργανισμός ή εταιρία που χρησιμοποιεί ένα πληροφοριακό σύστημα, ουσιαστικά δεσμεύεται να οργανώσει και να τηρεί κανόνες ασφαλείας. Τα μέτρα ασφαλείας αφορούν:

- Τη φυσική προστασία των πόρων του συστήματος από μη-εξουσιοδοτημένη πρόσβαση. Αυτό τυπικά σημαίνει ότι τα κρίσιμα μηχανήματα του δικτύου βρίσκονται σε καλά φυλασσόμενο χώρο.
- Την ασφάλεια των συστημάτων που συνδέονται στο δίκτυο. Και αυτό το κομμάτι ανήκει στη διαχείριση ασφαλείας των συστημάτων (για παράδειγμα, μπορεί να υλοποιείται με τη βοήθεια των μηχανισμών ασφαλείας που παρέχει το λειτουργικό σύστημα που χρησιμοποιείται).
- Την ασφάλεια του δικτύου και την προστασία των δεδομένων που μεταφέρονται μέσα από αυτό.

8.3 Ασφάλεια Δικτύων

Με την ανάπτυξη των δικτύων αλλά και του Δημόσιου Internet (με το οποίο πλέον πραγματοποιείται μεγάλο μέρος συναλλαγών και διακίνηση κρίσιμων δεδομένων), είναι πλέον σαφής η ανάγκη για προστασία της πληροφορίας που μεταφέρεται και

αποθηκεύεται. Στην ενότητα αυτή θα εξετάσουμε τα διάφορα προβλήματα που εμφανίζονται στην ασφάλεια των δικτύων καθώς και διάφορους τρόπους για την αντιμετώπιση τους. Θα μιλήσουμε για συστήματα και τεχνικές ασφαλείας, για τους τρόπους με τους οποίους υλοποιούνται, καθώς και τις προϋποθέσεις για την ύπαρξη συστημάτων ασφαλείας.

8.3.1 Ασφάλεια Πληροφοριών

Η ασφάλεια ενός οποιουδήποτε συστήματος ασχολείται με την προστασία αντικειμένων που έχουν κάποια αξία, γενικά γνωστά ως αγαθά. Η αξία των αγαθών μειώνεται αν υποστούν ζημιά. Αν δεχτούμε ότι υπάρχουν κίνδυνοι που μπορούν να μειώσουν την αξία των αγαθών, θα πρέπει να λάβουμε τα αντίστοιχα μέτρα προστασίας τους. Τα μέτρα αυτά προφανώς θα έχουν κάποιο κόστος (χρηματικό και σε κόπο). Προφανώς θα πρέπει να σταθμίσουμε το κόστος προστασίας των αγαθών με το αντίστοιχο ρίσκο αλλά και με το κόστος των ίδιων των αγαθών. Αν λάβουμε μειωμένα (πλημμελή) μέτρα προστασίας, η ασφάλεια των αγαθών δεν θα είναι εξασφαλισμένη. Ο ιδιοκτήτης των αγαθών είναι υπεύθυνος να σταθμίσει το κόστος προστασίας ανάλογα με το κίνδυνο και την αξία των αγαθών, και να αποφασίσει ποιο είναι το σημείο ισορροπίας.

Σε ένα πληροφοριακό σύστημα, ως αγαθά θα πρέπει να θεωρήσουμε τα δεδομένα που διακινούνται και αποθηκεύονται σε αυτό, καθώς και τους υπολογιστικούς πόρους (εξοπλισμό) που το απαρτίζουν. Ο ιδιοκτήτης έχει τη δυνατότητα να καθορίσει ποιος μπορεί να έχει χρησιμοποιήσει, να μεταβάλλει, ή να διαθέσει το αγαθό. Εκτός από τους ιδιοκτήτες τα αγαθά μπορεί να χρησιμοποιούνται και από τους χρήστες, οι οποίοι μπορεί να έχουν διαφορετικούς βαθμούς πρόσβασης σε αυτά. Για παράδειγμα, ο χρήστης μιας ιστοσελίδας έχει δυνατότητα να διαβάσει το περιεχόμενο ή να “κατεβάσει” αρχεία, αλλά δεν μπορεί να αλλάξει το περιεχόμενο τους. Από το παράδειγμα μας είναι ήδη προφανές ότι ιδιοκτήτης και χρήστης ενός πληροφοριακού αγαθού, δεν είναι απαραίτητα το ίδιο άτομο. Η έννοια του χρήστη δεν αναφέρεται αναγκαστικά σε κάποιο φυσικό πρόσωπο: διεργασίες που εκτελούνται μέσα στο ίδιο το σύστημα και έχουν πρόσβαση στα δεδομένα θεωρούνται επίσης “χρήστες” των δεδομένων.

Σημείωση κατανόησης: Σε ένα σύστημα UNIX οι διεργασίες που εκτελούν λειτουργίες χωρίς την παρέμβαση χρηστών είναι γενικά γνωστές ως “δαίμονες” (daemons). Αντίστοιχα, σε συστήματα Windows είναι γνωστές ως “υπηρεσίες” (services). Γενικά στα σύγχρονα λειτουργικά συστήματα, η δυνατότητα κάποιου χρήστη να χρησιμοποιήσει ή να μεταβάλλει δεδομένα ή ρυθμίσεις ρυθμίζεται από το διαχειριστή ο οποίος παραχωρεί τα αντίστοιχα απαιτούμενα δικαιώματα. Θυμίζουμε ότι

ένας χρήστης αναγνωρίζεται τυπικά από κάποιο όνομα χρήστη και κωδικό.

Με τον ίδιο τρόπο που κάποιος πραγματικός χρήστης (άνθρωπος) διαθέτει δικαιώματα, το ίδιο και οι υπηρεσίες που εκτελούνται αυτόματα σε ένα σύστημα χρησιμοποιούν κάποιο λογαριασμό χρήστη στον οποίο έχουν παραχωρηθεί τα ελάχιστα απαραίτητα δικαιώματα που απαιτούνται για να διεκπεραιώσουν την εργασία που τους έχει ανατεθεί. Έτσι για παράδειγμα, μια διεργασία που αναλαμβάνει να εξυπηρετήσει ιστοσελίδες σε χρήστες (web server) έχει μόνο τη δυνατότητα να διαβάσει τα συγκεκριμένα αρχεία που χρειάζεται για αυτή τη λειτουργία (δηλ. τις html σελίδες που έχει αποθηκεύσει ο διαχειριστής σε κάποιους καταλόγους). Για το σκοπό αυτό δημιουργείται ένας λογαριασμός χρήστη με τα αντίστοιχα δικαιώματα και η διεργασία εξυπηρέτησης φαίνεται σαν να εκτελείται από το χρήστη αυτό.

Από τη στιγμή που υπάρχει η έννοια της ιδιοκτησίας, θα πρέπει να εισάγουμε και την έννοια της εξουσιοδότησης. Εξουσιοδότηση είναι η άδεια που παρέχει ο ιδιοκτήτης σε κάποιον τρίτο (χρήστη) για τη χρήση των δεδομένων ή/και των υπολογιστικών πόρων του δικτύου. Ένα από τα σημαντικότερα προβλήματα ασφάλειας είναι η εξασφάλιση ότι μόνο εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση στα δεδομένα. Ένα ακόμα πρόβλημα είναι ότι οι εξουσιοδοτημένοι χρήστες μπορεί να θελήσουν να χρησιμοποιήσουν την πρόσβαση τους για να αποκτήσουν περισσότερα δικαιώματα σε σημεία του συστήματος που δεν έχουν πρόσβαση. Για την εξασφάλιση της χρήσης των αγαθών από εξουσιοδοτημένους χρήστες, υπάρχουν τέσσερα ζητούμενα στα πλαίσια της πολιτικής ασφαλείας:

- **Αυθεντικότητα (authentication):** Η απόδειξη της ταυτότητας του χρήστη προκειμένου να του επιτραπεί η πρόσβαση στα αγαθά που παρέχει το σύστημα. Ένας γνωστός τρόπος είναι η χρήση του συνδυασμού ονόματος χρήστη/κωδικού πρόσβασης (username/password).
- **Ακεραιότητα (integrity):** Η διασφάλιση ότι τα δεδομένα δεν έχουν αλλοιωθεί ή ότι η όποια μεταβολή τους έχει επέλθει μόνο από εξουσιοδοτημένα άτομα.
- **Εμπιστευτικότητα (confidentiality):** Ο περιορισμός της πρόσβασης στα δεδομένα μόνο σε άτομα που επιτρέπεται να έχουν πρόσβαση σε αυτά.
- **Μη άρνηση ταυτότητας (non-repudiation):** Η δυνατότητα απόδοσης πράξεων (ευθυνών) σε κάποιο συγκεκριμένο χρήστη. Πολύ απλά, η δυνατότητα να δούμε ποιος έκανε οποιαδήποτε αλλαγή στο σύστημα.

Από τα τέσσερα παραπάνω μπορούμε ακόμα να ορίσουμε:

- **Εγκυρότητα (validity):** Την απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας. Η εγκυρότητα είναι συνδυασμός της Ακεραιότητας και της Αυθεντικότητας.

- **Διαθεσιμότητα Πληροφοριών (Information Availability):** Την αποφυγή προσωρινής ή μόνιμης απώλειας πρόσβασης στις πληροφορίες από εξουσιοδοτημένους χρήστες. Σε κάποιες περιπτώσεις, οι χρήστες μπορεί να πληρώνουν κάποιο αντίτιμο για να έχουν πρόσβαση στις πληροφορίες που παρέχει το σύστημα μας. Είναι απαραίτητο να εξασφαλίσουμε ότι η πρόσβαση σε αυτές τις πληροφορίες θα είναι αδιάλειπτη.

Μπορούμε τώρα να δώσουμε και τους παρακάτω ορισμούς:

- **Ασφάλεια (security):** Η προστασία της Διαθεσιμότητας, Ακεραιότητας και Εμπιστευτικότητας των πληροφοριών.
- **Ασφάλεια Πληροφοριών (information security):** Ο συνδυασμός της Εμπιστευτικότητας, Εγκυρότητας και Διαθεσιμότητας Πληροφοριών.
- **Παραβίαση Ασφαλείας (security violation):** Η παραβίαση ενός ή περισσότερων από τις παραπάνω ιδιότητες, όπως διαθεσιμότητα, εμπιστευτικότητα και εγκυρότητα.

Γενικά ένα πληροφοριακό σύστημα είναι εκτεθειμένο σε κινδύνους. Οι κίνδυνοι μπορούν να διαχωριστούν σε απειλές και αδυναμίες.

Με τον όρο “απειλές” (threats) αναφερόμαστε σε ενέργειες ή γεγονότα που μπορούν οδηγήσουν στην κατάρρευση κάποιου από τα χαρακτηριστικά ασφαλείας που ορίσαμε προηγουμένως. Οι απειλές μπορεί να οφείλονται σε τυχαία ή φυσικά γεγονότα (πυρκαγιά, πλημμύρα κλπ) ή σε ανθρώπινες ενέργειες (σκόπιμες ή μη).

Με τον όρο “αδυναμίες” (vulnerabilities) αναφερόμαστε σε σημεία του πληροφοριακού συστήματος τα οποία (ενδεχομένως λόγω κακού σχεδιασμού ή υλοποίησης) αφήνουν περιθώρια για παραβιάσεις. Σε πολλές περιπτώσεις οι αδυναμίες οφείλονται σε λάθη του λογισμικού ή σε ανεπαρκή παραμετροποίηση του από το προσωπικό που το εγκατέστησε και το συντηρεί.

Πριν προχωρήσουμε στη λήψη μέτρων ασφαλείας, θα πρέπει να εκτιμήσουμε και να υπολογίσουμε διάφορους παράγοντες. Θα πρέπει αρχικά να αξιολογήσουμε ποια είναι τα αγαθά που χρήζουν προστασίας και να εντοπίσουμε τους πιθανούς κινδύνους από τους οποίους θα πρέπει να προστατευθούν. Έπειτα θα πρέπει να προχωρήσουμε σε ένα αρχικό σχεδιασμό της αρχιτεκτονικής ασφαλείας που θα ακολουθήσουμε και να εκτιμήσουμε το κόστος του. Το συνολικό κόστος πρέπει να περιλαμβάνει το κόστος αγοράς εξοπλισμού και λογισμικού που θα χρησιμοποιήσουμε, το κόστος εγκατάστασης του από κατάλληλο προσωπικό, αλλά και το μόνιμο λειτουργικό κόστος που θα έχει η συντήρηση και αναβάθμιση του.

Αν το κόστος που υπολογίσουμε υπερβαίνει τα προβλεπόμενα όρια, θα πρέπει να κάνουμε κάποιες νέες παραδοχές ή συμβιβασμούς σχετικά με το τι προβλήματα ασφαλείας και σε τι βαθμό θα καλύπτει η πολιτική ασφαλείας. Με τον τρόπο αυτό

αποδεχόμαστε τους εναπομείναντες κινδύνους που δεν καλύπτονται από την τελική πολιτική ασφαλείας.

Στις επόμενες ενότητες θα εξετάσουμε τις τεχνικές μεθόδους που χρησιμοποιούνται για την επίτευξη των παραβιάσεων, αλλά και τα αντίμετρα που μπορούμε να υλοποιήσουμε για να προστατέψουμε ένα πληροφοριακό σύστημα.

8.3.2 Επεξήγηση Ορολογίας

Πριν προχωρήσουμε στις διάφορες τεχνικές ασφάλειας και μεθόδους παραβίασης, θα κάνουμε μια σύντομη αναφορά στην ορολογία που χρησιμοποιείται. Κάποιοι από τους όρους που θα παρουσιάσουμε εδώ, εξηγούνται καλύτερα παρακάτω σε συνδυασμό με τον αντίστοιχο τρόπο χρήση τους.

Οι πιο βασικοί όροι σε θέματα ασφάλειας πληροφοριακών συστημάτων είναι οι παρακάτω:

- **Κρυπτογράφηση (Encryption):** Η κρυπτογράφηση είναι η διαδικασία με την οποία μετατρέπονται τα αρχικά δεδομένα (γνωστά και ως *plaintext*) σε μορφή (κρυπτόγραμμα) η οποία δεν μπορεί πλέον να γίνει κατανοητή χωρίς να αποκρυπτογραφηθεί. Η κρυπτογράφηση γίνεται με τη βοήθεια αλγορίθμου, το αποτέλεσμα του οποίου μπορεί να αντιστραφεί ώστε να παράγει ξανά τα αρχικά δεδομένα εισόδου. Για την κρυπτογράφηση και την αποκρυπτογράφηση χρησιμοποιείται το κλειδί.
- **Αποκρυπτογράφηση (Decryption):** Προφανώς η αντίστροφη διαδικασία της κρυπτογράφησης. Ο αλγόριθμος δέχεται ως είσοδο τα κρυπτογραφημένα δεδομένα (κρυπτόγραμμα) και με τη βοήθεια του κλειδιού (το οποίο προφανώς είναι διαθέσιμο μόνο σε εξουσιοδοτημένα άτομα) τα μετατρέπει ξανά στα κανονικά δεδομένα. Τα δεδομένα πλέον δεν είναι κωδικοποιημένα και μπορούν να χρησιμοποιηθούν κανονικά.
- **Κλειδί (Key):** Στο πεδίο της κρυπτογράφησης, το κλειδί είναι ένας ψηφιακός κωδικός (ένας αριθμός από bits) ο οποίος χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση της πληροφορίας. Προφανώς το κλειδί φυλάσσεται σε ασφαλές μέρος και είναι διαθέσιμο μόνο στα μέρη που επιτρέπεται να έχουν πρόσβαση στα δεδομένα.
- **Δημόσιο Κλειδί (Public Key):** Στην ασυμμετρική κρυπτογράφηση, χρησιμοποιούνται για κάθε χρήστη δύο κλειδιά, το δημόσιο και το ιδιωτικό. Η βασική ιδέα είναι ότι το δημόσιο το γνωρίζει καθένας, ενώ το ιδιωτικό μόνο ο χρήστης. Το δημόσιο κλειδί χρησιμοποιείται για να “κλειδώνει” (κρυπτογραφεί) ενώ το ιδιωτικό ξεκλειδώνει. Όποιος θέλει να μας στείλει κρυπτογραφημένα δεδομένα, χρησιμοποιεί το δημόσιο μας κλειδί για να τα κλειδώσει.

Μετά από αυτό η αποκρυπτογράφηση γίνεται μόνο με το δικό μας ιδιωτικό κλειδί. Γενικά η ασυμμετρική κρυπτογράφηση θεωρείται πιο ασφαλής από τη συμμετρική, καθώς δεν γνωρίζει κανείς άλλο το ιδιωτικό μας κλειδί. (Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί και για τις δύο λειτουργίες, άρα πρέπει να το έχουν και τα δύο μέρη της επικοινωνίας)

- **Ιδιωτικό Κλειδί (Private Key):** Το ιδιωτικό κλειδί χρησιμοποιείται στην ασυμμετρική κρυπτογράφηση για να αποκρυπτογραφεί και να υπογράφει δεδομένα. ΠΡΟΣΟΧΗ: το σχολικό βιβλίο γράφει λανθασμένα ότι το ιδιωτικό κλειδί κρυπτογραφεί και ελέγχει υπογραφές - αυτά τα κάνει το δημόσιο κλειδί συνδυάζεται πάντα (σαν ζεύγος) με ένα αντίστοιχο δημόσιο. Η πλήρης διαδικασία εξηγείται σε επόμενη ενότητα.
- **Μυστικό Κλειδί (Secret Key):** Ψηφιακός κωδικός που είναι γνωστός και στα δύο μέρη προκειμένου να τον χρησιμοποιήσουν σε ανταλλαγή δεδομένων με χρήση κρυπτογράφησης / αποκρυπτογράφησης.
- **Λειτουργία (Συνάρτηση) Κατατεμαχισμού (Hash Function):** Μαθηματική συνάρτηση της οποίας η έξοδος δεν μπορεί με αντιστροφή (με κανένα τρόπο) να μας παράγει την αρχική είσοδο. Προφανώς δεν μπορεί να χρησιμοποιηθεί για κρυπτογράφηση, καθώς δεν μπορούμε μετά να αποκρυπτογραφήσουμε το κείμενο, αλλά χρησιμοποιείται για την παραγωγή συνόψεων (digests).
- **Σύνοψη Μηνύματος (Message Digest):** Η σύνοψη ενός μηνύματος είναι το αποτέλεσμα (έξοδος) της συνάρτησης κατατεμαχισμού. Η σύνοψη δεν έχει το ίδιο μέγεθος (είναι συνήθως μικρότερη) με το αρχικό μήνυμα – κάτι το οποίο έχει νόημα, γιατί όπως εξηγήσαμε δεν μπορούμε έτσι και αλλιώς να ξαναγυρίσουμε στο αρχικό μήνυμα. Οι αλγόριθμοι κατατεμαχισμού είναι φτιαγμένοι με τέτοιο τρόπο ώστε μια μικρή μεταβολή στα δεδομένα εισόδου (π.χ. ένα μόνο γράμμα ή ακόμα και ένα μόνο bit) να προκαλεί ολοκληρωτική αλλαγή στην έξοδο (πλήρης αλλαγή της σύνοψης). Για το λόγο αυτό η σύνοψη χρησιμοποιείται πολύ συχνά για να ελέγχουμε την ακεραιότητα κάποιου αρχείου που κατεβάσαμε π.χ. από το Internet. Σε μεγάλα downloads, μπορούμε συνήθως να κατεβάσουμε και ένα αρχείο CHECKSUM (αθροίσματος ελέγχου) που περιέχει μέσα την σύνοψη του μεγάλου αρχείου. Εκτελώντας τη συνάρτηση κατατεμαχισμού στο δικό μας μηχάνημα, μπορούμε να συγκρίνουμε τις συνόψεις: αν είναι ίδιες το αρχείο έχει κατέβει σωστά.
- **Ψηφιακή Υπογραφή (Digital Signature):** Η ψηφιακή υπογραφή είναι τυπικά ένας αριθμός από bit που προστίθεται στο τέλος κάποιου αρχείου και εξασφαλίζει την αυθεντικότητα (“το έστειλε πράγματι ο χρήστης A”) και την ακεραιότητα (“το έχουμε λάβει σωστά”) ενός μηνύματος.

8.3.3 Μέθοδοι Παραβίασης

Σε κάθε δίκτυο υπολογιστών μπορεί να υπάρχουν εμπιστευτικές πληροφορίες. Τυπικά, αυτές θα είναι αποθηκευμένες σε διάφορα αποθηκευτικά μέσα (σκληροί δίσκοι κλπ) ενώ κατά τη διάρκεια της επεξεργασίας τους θα βρίσκονται και στην κύρια μνήμη (RAM) των υπολογιστών. Οι πληροφορίες μεταδίδονται επίσης στο δίκτυο με τη μορφή πακέτων. Η ύπαρξη πληροφοριών σε αυτές τις καταστάσεις μπορεί να απειληθεί με διάφορους τρόπους από ενέργειες χρηστών, τόσο του εσωτερικού δικτύου, όσο και του Internet (εφόσον υπάρχει σύνδεση σε αυτό). Στην ενότητα αυτή θα αναφερθούμε στους συνηθισμένους τρόπους επιθέσεων που χρησιμοποιούνται για την παραβίαση της ασφάλειας ενός δικτύου υπολογιστών.

Επιθέσεις στους Κωδικούς Πρόσβασης (Password Attacks)

Οι κωδικοί πρόσβασης είναι ένας από τους πλέον συνηθισμένους μεθόδους ελέγχου πρόσβασης σε υπολογιστικά συστήματα. Γενικά υπάρχουν δύο είδη κωδικών:

- **Τα επαναχρησιμοποιούμενα passwords:** Πρόκειται για τον πλέον συνηθισμένο τύπο κωδικού πρόσβασης. Μπορεί να χρησιμοποιηθεί πολλές φορές για την εξακρίβωση των στοιχείων του χρήστη.
- **Τα passwords μια χρήσης, OTP (One Time Password):** Τα passwords αυτά αλλάζουν συνεχώς, καθένα είναι έγκυρο για μια και μοναδική χρήση.

Στα περισσότερα είδη λειτουργικών συστημάτων, όπως το UNIX και τα Windows, υποστηρίζεται η χρήση επαναχρησιμοποιούμενων κωδικών πρόσβασης. (Στο UNIX υποστηρίζονται και τα OTP, αλλά το βιβλίο σας ντρέπεται να το πει).

Με την εξέλιξη της τεχνολογίας (αλλά και με την άνοδο των τεχνικών “ψαρέματος” των χρηστών) η προστασία ενός υπολογιστικού συστήματος μόνο με τη χρήση κωδικών (και ειδικά επαναχρησιμοποιούμενων) θεωρείται πολύ ασθενής.

Για την παραβίαση κωδικών πρόσβασης υπάρχουν προγράμματα που σε μικρό χρονικό διάστημα μπορούν να δοκιμάσουν πολύ μεγάλο συνδυασμό χαρακτήρων και γραμμάτων (brute force attack). Ένας άλλος τρόπος παραβίασης είναι η παρακολούθηση των πλήκτρων (key stroke monitoring) με τη βοήθεια κάποιου προγράμματος (keylogger) που καταγράφει τα πλήκτρα που πιέζονται, ενδεχομένως σε κάποιο αρχείο. Προφανώς το πρόγραμμα αυτό πρέπει να εγκατασταθεί εν αγνοία του αρχικού χρήστη του συστήματος. Με την ανάλυση των στοιχείων που έχουν καταγραφεί στο αρχείο, μπορεί να αποκαλυφθεί ο κωδικός πρόσβασης (και ενδεχομένως και άλλες εμπιστευτικές πληροφορίες, π.χ. αριθμοί πιστωτικών καρτών κλπ).

Ένας άλλος ιδιαίτερα συνηθισμένος στις μέρες μας τρόπος ανάκτησης κωδικών πρόσβασης αναφέρεται ως *social engineering* και επικεντρώνει στην παραπλάνηση των

χρηστών για την απόκτηση πληροφοριών. Για παράδειγμα, φανταστείτε ότι σας καλεί στο τηλέφωνο κάποιος που υποτίθεται ότι ανήκει στο τεχνικό τμήμα του παροχέα σας υπηρεσιών Internet (ISP) και σας ζητάει να του δώσετε τον κωδικό σας γιατί θέλουν να κάνουν κάποιες αλλαγές ρυθμίσεων στα συστήματα τους. Πάρα πολλοί χρήστες το πιστεύουν αυτό και πραγματικά δίνουν τους κωδικούς τους. Γιατί άραγε ένας τεχνικός του ISP σας να θέλει τον κωδικό σας; Ο διαχειριστής ενός συστήματος έχει πλήρη πρόσβαση σε όλα τα στοιχεία και τους λογαριασμούς και δεν χρειάζεται ποτέ κανένα κωδικό χρήστη! Στην ίδια κατηγορία εντάσσεται και η δυνατότητα να δούμε τυχαία (shoulder surfing) τον κωδικό πρόσβασης ενός χρήστη την ώρα που τον πληκτρολογεί (αρκεί να περνάμε δίπλα του εκείνη τη στιγμή).

Υπάρχει προφανώς η πιθανότητα απόκτησης ενός κωδικού πρόσβασης και με τη χρήση φυσικής βίας. Οι περιπτώσεις φυσικής βίας μπορούν να ενταχθούν σε δύο κατηγορίες: στην εξωτερική και στην εσωτερική βία. Είναι προφανές ότι με την εξωτερική βία, ο χρήστης του οποίου απειλείται η σωματική ακεραιότητα θα αποκαλύψει ενδεχομένως τον κωδικό του. Με την εσωτερική βία, αναφερόμαστε στην περίπτωση όπου κάποιος αντιγράφει (νόμιμα ή παράνομα) κρυπτογραφημένα passwords και στη συνέχεια χρησιμοποιεί κάποιο πρόγραμμα crack για να προσπαθήσει να τα αποκρυπτογραφήσει.

Οι κωδικοί πρόσβασης δεν αποθηκεύονται απευθείας σε ένα σύστημα. Αντίθετα, περνούν από λειτουργία κατατεμαχισμού και αποθηκεύεται η σύνοψη τους (digest). Για τον έλεγχο έπειτα του κωδικού που εισάγει ο χρήστης, γίνεται ξανά η ίδια διαδικασία: παράγεται το digest και συγκρίνεται με το αποθηκευμένο. Αν είναι ίδιο, ο κωδικός που δίνει ο χρήστης είναι ο σωστός. Από τα παραπάνω, μπορούμε να αντιληφθούμε ότι δεν είναι δυνατόν να πάρουμε με κάποιο τρόπο τον αρχικό κωδικό με αποκρυπτογράφηση του αποθηκευμένου, καθώς έχει προέλθει από λειτουργία κατατεμαχισμού (που δεν αντιστρέφεται).

Ένα πρόγραμμα τύπου crack χρησιμοποιεί μια απλή μέθοδο: αν έχουμε αποκτήσει τα digests των κωδικών πρόσβασης (γνωστά και ως hashes) και γνωρίζουμε τον αλγόριθμο κατατεμαχισμού που έχει χρησιμοποιηθεί για την παραγωγή τους, μπορούμε να αρχίζουμε να δοκιμάζουμε τυχαίους συνδυασμούς γραμμάτων, μέχρι να παράγουμε το ίδιο digest. Τότε θα έχουμε βρει τον κωδικό πρόσβασης. Η μέθοδος αυτή είναι γνωστή ως *brute force attack*.

Τα πράγματα γίνονται πιο εύκολα αν αναλογιστούμε ότι οι περισσότεροι χρήστες (για ευκολία τους) χρησιμοποιούν μάλλον απλές λέξεις ως κωδικούς πρόσβασης. Ετσι, αντί να ψάχνουμε τυχαία γράμματα μπορούμε να ψάχνουμε για λέξεις. Τα περισσότερα προγράμματα crack διαθέτουν ένα λεξικό αγγλικών (συνήθως) λέξεων τις οποίες δοκιμάζουν. Ένα γνωστό τέτοιο πρόγραμμα για UNIX είναι το Jack the Ripper, το οποίο χρησιμοποιούν και οι διαχειριστές για να ελέγξουν αν ο κωδικός

κάποιου χρήστη είναι “ασθενής”.

Να σημειώσουμε βέβαια ότι πρόσβαση στο αρχείο των κρυπτογραφημένων κωδικών σε ένα UNIX σύστημα έχει μόνο ο διαχειριστής (root) και τα προγράμματα που εξασφαλίζουν την είσοδο των χρηστών και την αλλαγή των κωδικών (login και passwd αντίστοιχα). Αν το αρχείο αυτό έχει πέσει στα χέρια κάποιου άλλου, τα προβλήματα μας είναι συνήθως πολύ πιο σοβαρά από την απλή παραβίαση κωδικών...

Παρακολούθηση Δικτύου (Network Monitoring ή Network Packet Sniffing)

Όπως είναι γνωστό, τα δεδομένα μέσα σε ένα δίκτυο μεταφέρονται μεταξύ υπολογιστών με τη μορφή πακέτων. Σε αρκετές εφαρμογές (για παράδειγμα το telnet και το ftp για τα οποία έχουμε ήδη μιλήσει), τα δεδομένα αλλά και οι ίδιοι οι κωδικοί πρόσβασης μεταφέρονται με μορφή απλού κειμένου, χωρίς κανένα είδος κρυπτογράφησης (clear text). Είναι φανερό, ότι κάποιος με τα κατάλληλα τεχνικά μέσα και γνώσεις μπορεί να λάβει τα πακέτα, να τα συναρμολογήσει και να παράγει έτσι το σύνολο των πληροφοριών που παρέχονται σε αυτά, συμπεριλαμβανομένων και τυχόν κωδικών.

Τα προγράμματα που κάνουν ανίχνευση πακέτων (packet sniffing) χρησιμοποιούν την κάρτα δικτύου του υπολογιστή σε κατάσταση λειτουργίας promiscuous. Στο promiscuous mode η κάρτα δικτύου λαμβάνει όλα τα πακέτα που κυκλοφορούν στο δίκτυο, και όχι μόνο αυτά που απευθύνονται σε αυτήν. Τα προγράμματα για packet sniffing μπορούν να χρησιμοποιηθούν για επίλυση προβλημάτων δικτύου από τους διαχειριστές συστημάτων, αλλά αποτελούν και ένα πολύ ισχυρό εργαλείο για επίδοξους εισβολείς. Τα προγράμματα αυτά μπορούν να συλλέξουν εμπιστευτικές πληροφορίες την ώρα που διέρχονται μέσα από τις γραμμές του δικτύου και πιθανόν και κωδικούς που μεταδίδονται σε μορφή κειμένου. Η αποκάλυψη passwords με αυτό τον τρόπο είναι γνωστή και ως επίθεση *Man-in-the-Middle*. Είναι φανερό ότι η παρακολούθηση δικτύου μπορεί να χρησιμοποιηθεί και για την παραβίαση κωδικών πρόσβασης.

Μεταμφίεση (Masquerade)

Η επίθεση με μεταμφίεση παρατηρείται όταν ο επιτιθέμενος που βρίσκεται σε δίκτυο έξω από το δικό μας, προσποιείται ότι βρίσκεται στο δικό μας. Ειδικά για τα πρωτόκολλα TCP/IP, το παραπάνω είναι γνωστό και ως *IP Spoofing* καθώς ο επιτιθέμενος αλλάζει την διεύθυνση IP των πακέτων του ώστε να φαίνεται ότι προέρχονται από το εσωτερικό μας δίκτυο (ότι ανήκουν δηλ. στο εύρος των δικών μας IP διευθύνσεων). Η μέθοδος αυτή χρησιμοποιείται κυρίως για να ξεγελάσει ο επιτιθέμενος το

firewall που συνδέει το εσωτερικό μας δίκτυο με τον έξω κόσμο (το Internet ή γενικά με δίκτυο που δεν θεωρείται έμπιστο (trusted)). Τυπικά, το IP spoofing περιορίζεται στο να εισάγει δεδομένα ή εντολές σε υπάρχον πακέτο δεδομένων σε επικοινωνίες τύπου client – server ή σημείου προς σημείο (point to point).

Για να είναι δυνατή η αμφίδρομη επικοινωνία (τη στιγμή που η διεύθυνση αφετηρίας δεν είναι η πραγματική του εισβολέα), θα πρέπει ο εισβολέας να έχει αλλάξει κατάλληλα τους πίνακες δρομολόγησης που δείχνουν προς τη διεύθυνση που έχει προσποιηθεί ότι βρίσκεται, ώστε να κατευθύνουν τα δεδομένα προς την πραγματική του διεύθυνση. Έτσι θα λαμβάνει όλα τα πακέτα που κατευθύνονται προς την “ψεύτικη” διεύθυνση. Στην περίπτωση αυτή, ενδέχεται να λάβει και πακέτα που περιέχουν κωδικούς πρόσβασης. Μπορεί επίσης να στέλνει emails προς το εσωτερικό μας δίκτυο, στους πελάτες ή τους συνεργάτες μας και να χρησιμοποιήσει τεχνικές social engineering που αναφέραμε προηγουμένως για να ανακτήσει κωδικούς.

Άρνηση Παροχής Υπηρεσίας (Denial of Service)

Αυτή η κατηγορία επιθέσεων διαφοροποιείται από αυτές που έχουμε περιγράψει ως τώρα, καθώς δεν προσπαθεί να αποσπάσει τους κωδικούς από το δίκτυο μας, αλλά έχει ως στόχο την διαθεσιμότητα των δεδομένων μας. Σκοπός μιας τέτοιας επίθεσης είναι να φτάσει το δικτυακό εξοπλισμό (ή την υπολογιστική ισχύ) στα όρια, ώστε να μην μπορούν να εξυπηρετηθούν πλέον οι νόμιμοι χρήστες του δικτύου. Η επίθεση γίνεται συνήθως με εξάντληση των ορίων των πόρων του δικτύου (π.χ. μέγιστος αριθμός πακέτων ανά δευτερόλεπτο που μπορεί να αντέξει το δίκτυο μας, μέγιστος αριθμός πακέτων ανά δευτερόλεπτο σε κάποιο δρομολογητή ή και μέγιστος αριθμός διεργασιών κάποιου εξυπηρετητή κλπ).

Οι επιθέσεις του παραπάνω τύπου είναι διαδεδομένες ειδικά σε γνωστά και μεγάλα sites στο Internet (Yahoo, CNN, twitter κλπ). Επειδή δεν είναι γενικά δυνατόν να παράγονται και να αποστέλλονται όλα αυτά τα πακέτα της επίθεσης από ένα μόνο υπολογιστή, τυπικά χρησιμοποιούνται μηχανήματα γνωστά ως zombies που ανήκουν σε κάποιο botnet.

Σημείωση: Ένας υπολογιστής που έχει μολυνθεί με κατάλληλο κακόβουλο πρόγραμμα (malware) μπορεί να δίνει τη δυνατότητα σε κάποιον να τον κατευθύνει από μακριά. Ένας τέτοιος υπολογιστής ονομάζεται zombie. Πολλοί υπολογιστές που έχουν μολυνθεί από το ίδιο πρόγραμμα και τους χειρίζεται το ίδιο άτομο ταυτόχρονα, αποτελούν ένα botnet. Ο “χειριστής” του botnet μπορεί να στείλει εντολή σε όλα τα zombies που το αποτελούν να αρχίσουν να στέλνουν πακέτα προς μια συγκεκριμένη διεύθυνση δικτύου, δημιουργώντας έτσι μια επίθεση τύπου Denial Of Service. Μάλιστα, επειδή η επίθεση αυτή δεν προέρχεται από ένα μόνο μηχάνημα και διεύ-

θυνση IP (ένα botnet μπορεί να περιέχει υπολογιστές σε κάθε σημείο του κόσμου), ονομάζεται κατανεμημένη (Distributed Denial of Service Attack, ή DDOS) και είναι αρκετά πιο δύσκολο να αντιμετωπιστεί από το απλό Denial of Service.

Σε σχέση με τις άλλες επιθέσεις που αναφέραμε, οι τεχνικές τύπου Denial of Service δεν απαιτούν ειδικές γνώσεις. Είναι πάντως πιο αποτελεσματικές αν υπάρχει γνώση της εσωτερικής δομής του δικτύου στο οποίο πρόκειται να γίνει η επίθεση.

Επιθέσεις στο Επίπεδο Εφαρμογών (Application-Layer Attacks)

Ορισμένες εφαρμογές όπως το HTTP, ActiveX, Telnet, FTP κλπ. παρουσιάζουν αδυναμίες σε συγκεκριμένα σημεία της ασφάλειας τους, που οφείλονται πολλές φορές σε αδυναμίες στον κώδικα τους (γνωστές και ως τρύπες, holes). Οι γνώστες αυτών των αδυναμιών μπορούν να τις εκμεταλλευθούν για να αποκτήσουν πρόσβαση στο σύστημα με απότερο σκοπό τη δημιουργία προβλημάτων ή τη συλλογή πληροφοριών.

8.3.4 Τεχνικές Ασφάλειας

Ο τομέας της ασφάλειας δεδομένων σε κατανεμημένα πληροφοριακά συστήματα είναι από τους πιο ραγδαία αναπτυσσόμενους σήμερα, με συνεχή παρουσίαση νέων τεχνολογιών και προϊόντων σε θέματα ασφάλειας από διάφορες εταιρίες. Στην ενότητα αυτή θα παρουσιάσουμε κάποιες βασικές τεχνικές ασφάλειας πληροφοριών που χρησιμοποιούνται σε σύγχρονα δίκτυα.

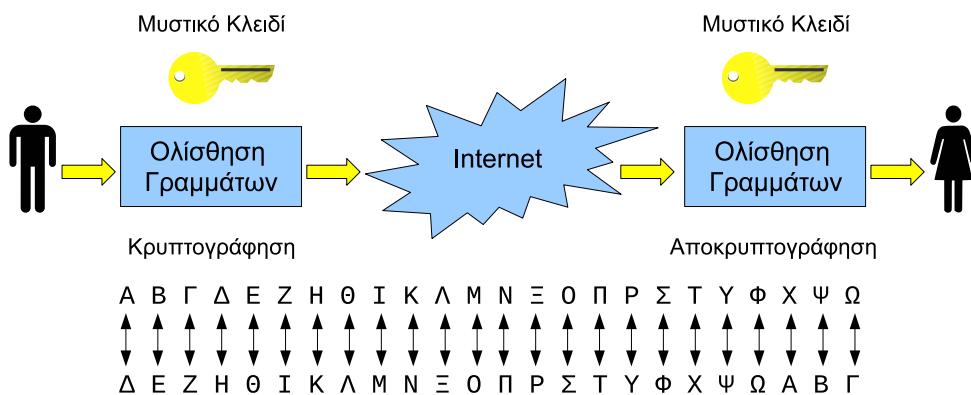
Συμμετρική Κρυπτογράφηση

Η συμμετρική κρυπτογράφηση (ή κρυπτογράφηση συμμετρικού κλειδιού όπως αναφέρεται συχνά) αποτελεί μια μέθοδο για την εξασφάλιση της εμπιστευτικότητας κατά τη μετάδοση πληροφοριών πάνω από ένα κανάλι επικοινωνίας.

Ας υποθέσουμε ότι έχουμε δύο χρήστες A και B που θέλουν να επικοινωνήσουν μεταξύ τους με ασφάλεια. Η κρυπτογράφηση που περιγράφουμε ονομάζεται συμμετρική επειδή χρησιμοποιείται το ίδιο ακριβώς κλειδί τόσο για την κρυπτογράφηση (παραγωγή του κρυπτογραφημένου μηνύματος από το απλό κείμενο εισόδου) όσο και για την αποκρυπτογράφηση (εξαγωγή του αρχικού μηνύματος από το κρυπτογραφημένο). Προφανώς, για να είναι εφικτή η επικοινωνία του A με τον B, θα πρέπει:

- Να χρησιμοποιούν και οι δύο το ίδιο κλειδί, το οποίο πρέπει να έχουν από πριν συμφωνήσει (και για το οποίο είναι βέβαιοι ότι δεν το έχει υποκλέψει και κάποιος τρίτος).
- Να έχουν συμφωνήσει σε ένα κοινό αλγόριθμο κρυπτογράφησης.

Ένας απλοϊκός αλγόριθμος κρυπτογράφησης, είναι ο Caesar Cipher που φαίνεται στο σχήμα 8.5. Στον αλγόριθμο αυτό, γίνεται αντικατάσταση κάθε γράμματος του



Σχήμα 8.5: Επικοινωνία με χρήση συμμετρικής κρυπτογράφησης

μηνύματος με ένα άλλο που βρίσκεται μερικές θέσεις πιο κάτω στο αλφάριθμο. Για παράδειγμα, μπορούμε να συμφωνήσουμε ότι θα μετακινούμε κάθε γράμμα κατά τρεις θέσεις, έτσι για παράδειγμα το Α γίνεται Δ, το Β γίνεται Ε κ.ο.κ. Προφανώς εδώ το κλειδί είναι στην πραγματικότητα το πόσες θέσεις έχουμε κάνει τη μετακίνηση. Ο αλγόριθμος ολισθαίνει τα γράμματα δεξιά όταν γίνεται κρυπτογράφηση και αριστερά (πάντα τον ίδιο αριθμό από θέσεις) όταν γίνεται αποκρυπτογράφηση. Καθώς ο αλγόριθμος δεν είναι σύνθετος, είναι πολύ εύκολο να γίνει αποκρυπτογράφηση ακόμα και αν δεν διαθέτουμε το κλειδί: με ένα υπολογιστή είναι πολύ εύκολο να δοκιμάσουμε όλες τις πιθανές τιμές θέσεων, μέχρι να βρούμε κάποια που το αποκρυπτογραφημένο κείμενο να βγάζει νόημα. Οι πιθανές θέσεις είναι πολύ λίγες (θεωρώντας κεφαλαία ελληνικά, μόνο 24) και έτσι δεν έχει νόημα να χρησιμοποιήσουμε πρακτικά πουθενά αυτό τον αλγόριθμο.

Υπάρχουν προγράμματα που προσπαθούν – με διάφορες μεθόδους – να αποκρυπτογράφήσουν μηνύματα δοκιμάζοντας διάφορους αλγόριθμους ώστε να ανακτήσουν το μήνυμα χωρίς να διαθέτουν το κλειδί. Εάν ο αλγόριθμος είναι πολύπλοκος, το σπάσιμο του (ακόμα και σε μηχανήματα με τεράστια υπολογιστική ισχύ) μπορεί να διαρκέσει πάρα πολύ χρόνο (χρόνια ως και αιώνες ακόμα!) σε σημείο που ακόμα και αν τελικά επιτευχθεί να μην προστατεύει πλέον κάποια πληροφορία με αξία.

Έχουν αναπτυχθεί πολλοί αλγόριθμοι κρυπτογράφησης που βασίζονται σε πολύπλοκα μαθηματικά μοντέλα και σύνθετη λογική. Ορισμένοι από αυτούς δεν είναι καν τεκμηριωμένοι, ενώ άλλοι φυλάσσονται ως κρατικά μυστικά και η εξαγωγή τους σε τρίτες χώρες απαγορεύεται. Μάλιστα, αν χρησιμοποιούνται σε προϊόντα εταιριών, η εξαγωγή της πλήρης έκδοσης τους σε άλλες χώρες μπορεί να γίνεται μόνο μετά από χορήγηση σχετικής άδειας.

Σημείωση: Άσχετα με αυτά που γράφει το βιβλίο σας παραπάνω, έχει αποδειχθεί και είναι πλέον κοινά αποδεκτό ότι οι μόνοι αλγόριθμοι κρυπτογράφησης που παρέχουν αρκετή ασφάλεια είναι οι ανοικτού κώδικα. Σε αυτούς καθένας μπορεί να δει πως λειτουργούν και να τους βελτιώσει ή να βρει τυχόν προβλήματα που μπορούν να οδηγήσουν σε ασθενή κρυπτογράφηση. Για το λόγο αυτό η βελτίωση τους είναι συνεχής. Αντίθετα οι περισσότεροι κλειδωμένοι και κρυφοί αλγόριθμοι έχουν σπάσει: CSS (κρυπτογράφηση ταινιών DVD), A5/1 (κρυπτογράφηση δεδομένων φωνής σε κινητά τηλέφωνα GSM), κρυπτογράφηση Blue-Ray κλπ.

Μερικοί από τους πιο διαδεδομένους αλγόριθμους κρυπτογράφησης είναι:

- DES, Data Encryption Standard, Πρότυπο Κρυπτογράφησης Δεδομένων
- 3DES, Triple DES
- IDEA, International Data Encryption Algorithm, Διεθνής Αλγόριθμος Κρυπτογράφησης Δεδομένων.

Οι παραπάνω αλγόριθμοι δέχονται ως είσοδο μηνύματα μεγέθους 64 bits. Αν το μήνυμα είναι μεγαλύτερο από 64 bits, θα πρέπει να σπάσει σε κομμάτια των 64 bits.

Όπως αναφέραμε, η συμμετρική κρυπτογράφηση προσφέρει κυρίως εμπιστευτικότητα στην επικοινωνία. Αν και μπορεί να χρησιμοποιηθεί και για την εξασφάλιση της αυθεντικότητας και της ακεραιότητας, υπάρχουν αρκετά καλύτερες τεχνικές για αυτούς τους σκοπούς. Συγκεκριμένα, η συμμετρική κρυπτογράφηση έχει το σημαντικό μειονέκτημα ότι πρέπει με κάποιο ασφαλή τρόπο να γνωστοποιήσουμε το κλειδί στην άλλη μεριά προκειμένου να αποκρυπτογραφήσει το μήνυμα. Προφανώς, δεν μπορούμε να χρησιμοποιήσουμε για αυτό το σκοπό κάποιο μη-έμπιστο μέσο (π.χ. το Διαδίκτυο) γιατί υπάρχει κίνδυνος υποκλοπής του. Ωστόσο γίνονται κάποιες προσπάθειες και σε αυτό τον τομέα: για παράδειγμα, ο αλγόριθμος Diffie Hellman επιτρέπει τη διανομή ενός συμμετρικού κλειδιού με ασφάλεια σε κάποιο απομακρυσμένο παραλήπτη, ακόμα και μέσω του Διαδικτύου.

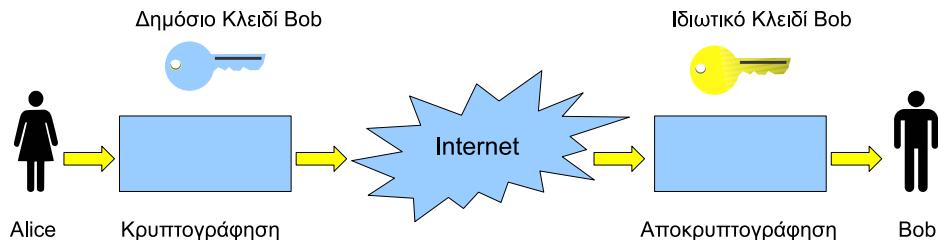
Ασυμμετρική Κρυπτογράφηση

Η ασυμμετρική κρυπτογράφηση ονομάζεται συχνά και κρυπτογράφηση δημόσιου κλειδιού. Σε αντίθεση με την συμμετρική κρυπτογράφηση που περιγράψαμε προηγουμένως, η ασυμμετρική χρησιμοποιεί διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση – για το λόγο αυτό άλλωστε ονομάζεται και ασυμμετρική.

Συνηθισμένες χρήσης της ασυμμετρικής κρυπτογράφησης είναι:

- Εξασφάλιση εμπιστευτικότητας στη μεταδιδόμενη πληροφορία
- Εξασφάλιση αυθεντικότητας

Για να δούμε με ποιο τρόπο διασφαλίζονται η εμπιστευτικότητα και η αυθεντικότητα, θα αναλύσουμε βήμα προς βήμα μια επικοινωνία ανάμεσα στα δύο μέρη A και B (στην διεθνή βιβλιογραφία χρησιμοποιούνται πάντα ως παραδείγματα για την κρυπτογράφηση ο Bob και η Alice!).



Σχήμα 8.6: Εμπιστευτικότητα δεδομένων με χρήση δημόσιου κλειδιού

Για να ξεκινήσει η επικοινωνία μεταξύ του Bob και της Alice, πρέπει πρώτα να διαθέτει ο καθένας από ένα ζεύγος κλειδιών, ιδιωτικό και δημόσιο. Το ιδιωτικό κλειδί ονομάζεται έτσι ακριβώς επειδή δεν πρέπει ποτέ να γνωστοποιηθεί πουθενά, προσρίζεται μόνο για τον κάτοχο του. Αντίθετα, το δημόσιο κλειδί γίνεται διαθέσιμο σε οποιονδήποτε (πρακτικά, τα δημόσια κλειδιά μεταφορτώνονται σε ειδικούς εξυπηρετητές, τους λεγόμενους *keyservers* όπου μπορεί όποιος θέλει να τα αναζητήσει και να τα ανακτήσει). Η δημιουργία του ζεύγους κλειδιών είναι μια απλή διαδικασία και μπορεί να γίνει από κάθε χρήστη που το επιθυμεί.

Στην ασυμμετρική κρυπτογράφηση, η διαδικασία της κρυπτογράφησης γίνεται με τη βοήθεια του δημόσιου κλειδιού, ενώ της αποκρυπτογράφησης με τη βοήθεια του ιδιωτικού. Αυτό σημαίνει ότι για να στείλει η Alice ένα κρυπτογραφημένο μήνυμα στον Bob θα πρέπει:

- Να ανακτήσει το δημόσιο κλειδί του Bob.

- Να χρησιμοποιήσει το δημόσιο κλειδί του Bob για να κρυπτογραφήσει το μήνυμα που θέλει να στείλει.

Από τη μεριά του, ο Bob θα πρέπει:

- Να λάβει το κρυπτογραφημένο μήνυμα από την Alice.
- Να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει.

Γενικά, στην ασυμμετρική κρυπτογράφηση, ο ένας χρήστης χρειάζεται πάντα το δημόσιο κλειδί του άλλου προκειμένου είτε να του στείλει κάποιο κρυπτογραφημένο μήνυμα ή να ελέγξει την ψηφιακή υπογραφή (θα δούμε αργότερα) ενός μηνύματος που έλαβε από αυτόν. Καθώς το δημόσιο κλειδί διανέμεται μέσω μη έμπιστου δικτύου, τίθεται επίσης θέμα πως θα γίνει ο διαμοιρασμός του.

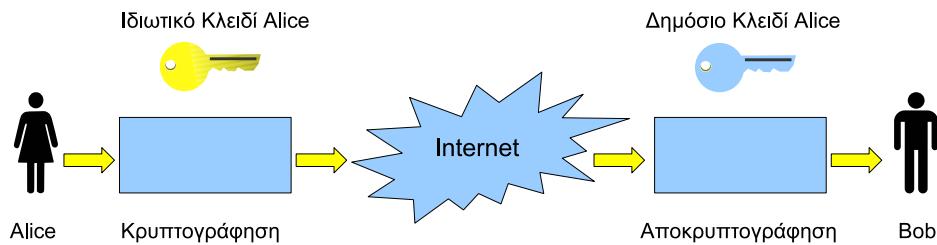
Σημείωση: Φυσικά το βιβλίο εδώ έχει λάθος: δεν υπάρχει θέμα διαμοιρασμού του δημοσίου κλειδιού. Τη στιγμή που είναι δημόσιο, είναι διαθέσιμο σε όλους και μπορούμε να το στείλουμε από μη έμπιστο δίκτυο. Το πραγματικό πρόβλημα είναι πως γνωρίζουμε ότι ένα δημόσιο κλειδί που κατεβάσαμε, ανήκει πραγματικά στο άτομο στο οποίο θέλουμε να στείλουμε το μήνυμα, και όχι σε κάποιο τρίτο που επιθυμεί να το υποκλέψει. Για το λόγο αυτό, κάθε κλειδί είναι επίσης εφοδιασμένο με μια τιμή γνωστή ως δακτυλικό αποτύπωμα (*fingerprint*), που είναι μοναδική και μπορούμε να τη δούμε. Μετά, αν θέλουμε, μπορούμε να επικοινωνήσουμε (με συμβατικό τρόπο, π.χ. τηλέφωνο) με τον κάτοχο του κλειδιού για να επιβεβαιώσουμε ότι πράγματι πρόκειται για το δικό του κλειδί.

Γενικά λοιπόν, η κρυπτογράφηση ενός μηνύματος απαιτεί τη χρήση από τον αποστολέα του δημοσίου κλειδιού **του παραλήπτη**, ώστε η αποκρυπτογράφηση να μπορεί να γίνει μόνο από τον παραλήπτη με τη χρήση του δικού του, καλά προστατευμένου, ιδιωτικού κλειδιού.

Θα δούμε τώρα πως μπορεί να εξασφαλιστεί η αυθεντικότητα ενός μηνύματος κατά την επικοινωνία του Bob και της Alice. Να θυμίσουμε εδώ ότι αυθεντικότητα είναι η δυνατότητα επαλήθευσης της ταυτότητας του χρήστη. Άρα όταν λέμε για εξασφάλιση αυθεντικότητας ενός μηνύματος που προέρχεται από τον Bob, σημαίνει ότι μπορούμε να επαληθεύσουμε ότι έρχεται πραγματικά από τον Bob και όχι από οποιοδήποτε άλλο πρόσωπο. Να σημειώσουμε εδώ ότι για παράδειγμα το απλό email δεν παρέχει καμιά εξασφάλιση αυθεντικότητας, αφού μπορούμε να προσποιηθούμε ότι έχει γίνει αποστολή του από οποιονδήποτε θέλουμε.

Ας υποθέσουμε ότι η Alice στέλνει ένα μήνυμα στον Bob και επιθυμεί να έχει ο Bob την δυνατότητα να ελέγξει ότι η Alice είναι πράγματι ο αποστολέας. Στην περίπτωση αυτή, ακολουθείται η παρακάτω διαδικασία:

- Η Alice δημιουργεί το μήνυμα και το κρυπτογραφεί με το ιδιωτικό της κλειδί.



Σχήμα 8.7: Αυθεντικοποίηση αποστολέα με χρήση ασυμμετρικής κρυπτογράφησης

- Ο Bob λαμβάνει το μήνυμα και το αποκρυπτογραφεί με το δημόσιο κλειδί της Alice (το οποίο φυσικά πρέπει να έχει ανακτήσει από πριν).
- Αν η αποκρυπτογράφηση είναι σωστή το μήνυμα έχει πράγματι προέλθει από την Alice και δεν έχει αλλοιωθεί (τυχαία ή εσκεμμένα) στη διαδρομή. Σε κάθε άλλη περίπτωση η διαδικασία θα αποτύχει.

Σημείωση: Όταν κρυπτογραφούμε κάτι με ένα δημόσιο κλειδί, αυτό αποκρυπτογραφείται μόνο με το αντίστοιχο ιδιωτικό. Αυτό σημαίνει ότι η αποκρυπτογράφηση του μπορεί να γίνει μόνο από ένα άτομο. Αντίθετα, όταν κρυπτογραφούμε κάτι με το ιδιωτικό κλειδί, η αποκρυπτογράφηση μπορεί να γίνει από τον καθένα. Προφανώς ο λόγος για να κάνουμε μια τέτοια κρυπτογράφηση δεν είναι για να προστατεύσουμε τα δεδομένα: καθένας μπορεί να τα αποκρυπτογραφήσει. Όμως εξασφαλίζουμε την αυθεντικότητα των δεδομένων, δηλ. την ταυτότητα του αποστολέα. Σε αυτό βασίζεται και η λειτουργία της ψηφιακής υπογραφής που περιγράφεται στην επόμενη ενότητα.

8.3.4.1 Ψηφιακές Υπογραφές

Η ψηφιακή υπογραφή είναι σύνοψη ενός μηνύματος, η οποία προσκολλάται στο τέλος του ηλεκτρονικού εγγράφου. Η ψηφιακή υπογραφή χρησιμοποιείται για την απόδειξη της ταυτότητας του αποστολέα (αυθεντικοποίηση) καθώς και για την απόδειξη της ακεραιότητας των δεδομένων.

Οι ψηφιακές υπογραφές προκύπτουν από το συνδυασμό ενός αλγόριθμου ασυμμετρικής κρυπτογράφησης και ενός αλγόριθμου κατατεμαχισμού (hash). Οι αλγόριθμοι κατατεμαχισμού συνήθως δέχονται ως είσοδο μηνύματα τυχαίου μήκους και δίνουν στην έξοδο τους μια σύνοψη (digest) συγκεκριμένου μήκους. Γνωστοί αλγόριθμοι κατατεμαχισμού είναι οι *MD4, Message Digest 4, MD5, Message Digest 5* και *SHA, Secure Hash Algorithm* και οι παραλλαγές τους (π.χ. *SHA1, SHA256*).

Η διαδικασία δημιουργίας και επαλήθευσης μιας ψηφιακής υπογραφής, περιγράφεται παρακάτω:

- Αρχικά πρέπει τα δύο μέρη της επικοινωνίας (π.χ. ο Bob και η Alice) να έχουν συμφωνήσει σε κάποιο αλγόριθμο δημοσίου κλειδιού (ασυμμετρικής κρυπτογράφησης, π.χ. PGP, Digital Signature Standard κλπ) και κάποιο αλγόριθμο κατατεμαχισμού (π.χ. MD5).
- Και τα δύο μέρη πρέπει να έχουν ζευγάρια δημοσίων και ιδιωτικών κλειδών σύμφωνα με τον αλγόριθμο που επέλεξαν προηγουμένως. Θα πρέπει να ανταλλάξουν μεταξύ τους τα δημόσια κλειδιά τους.
- Ας υποθέσουμε ότι η Alice θέλει να στείλει στον Bob ένα υπογεγραμμένο μήνυμα. Αρχικά θα περάσει το μήνυμα από τον αλγόριθμο κατατεμαχισμού ο οποίος θα παράγει μια σύνοψη (digest).
- Θα κρυπτογραφήσει τη σύνοψη με το ιδιωτικό της κλειδί, και θα προσθέσει την κρυπτογραφημένη εκδοχή της στο τέλος του εγγράφου. Θα αποστείλει στον Bob το τελικό αυτό έγγραφο.
- Ο Bob θα εξάγει τη κρυπτογραφημένη σύνοψη από το τέλος του εγγράφου και θα την αποκρυπτογραφήσει χρησιμοποιώντας το δημόσιο κλειδί της Alice. Εφόσον η αποκρυπτογράφηση γίνει σωστά, γνωρίζουμε ότι η σύνοψη δεν έχει αλλοιωθεί. Επειτα, θα πάρει το μήνυμα, θα το περάσει από τον αλγόριθμο κατατεμαχισμού και θα συγκρίνει τη σύνοψη που υπολόγισε ο ίδιος με τη σύνοψη που έλαβε από την Alice. Αν οι συνόψεις είναι ίδιες τότε γνωρίζει ότι το αρχικό μήνυμα δεν έχει αλλοιωθεί.

Με τον παραπάνω τρόπο, έχουμε εξασφαλίσει τόσο την αυθεντικότητα (ελέγχοντας ότι γίνεται σωστά η αποκρυπτογράφηση της σύνοψης) όσο και την ακεραιότητα (συγκρίνοντας τη σύνοψη που λάβαμε με αυτήν που υπολογίζουμε) του μηνύματος. Έτσι είμαστε σίγουροι και για την ταυτότητα του παραλήπτη και για τη μη-αλλοίωση του περιεχομένου του μηνύματος.

Εργαστηριακή Επίδειξη: Μπορείτε να χρησιμοποιήσετε το πρόγραμμα GPG σε περιβάλλον Linux/FreeBSD (και Windows) για να δείτε στην πράξη τις βασικές έννοιες της κρυπτογράφησης και υπογραφής με τη χρήση τεχνολογιών δημοσίου κλειδιού. Θα γίνει μια σύντομη επίδειξη στο εργαστήριο σχετικά με τη χρήση αυτού του προγράμματος.

8.3.5 Τεχνολογίες Ασφάλειας

Όπως αναφέραμε σε προηγούμενη ενότητα, υπάρχει πλήθος τεχνικών που εξασφαλίζουν λύσεις για τα βασικά στοιχεία μιας πολιτικής ασφαλείας. Στην αγορά υπάρχει μεγάλο πλήθος προϊόντων ασφάλειας. Μερικές από τις πιο δημοφιλείς λύσεις για την εμπιστευτικότητα των δεδομένων και την πιστοποίηση των χρηστών αναφέρονται επιγραμματικά παρακάτω:

- **Σταθερά passwords και passwords μιας χρήσης (One Time Passwords, OTP):** για πιστοποίηση χρηστών.
- **SSL / SSH / SOCKS:** Κρυπτογράφηση δεδομένων για εξασφάλιση ακεραιότητας και εμπιστευτικότητας.
- **Radius / Tacacs:** Συστήματα για πιστοποίηση dial-up χρηστών και εκχώρηση συγκεκριμένων δικαιωμάτων.
- **PAP / CHAP:** Συστήματα για πιστοποίηση δικτυακών συσκευών σε συνδέσεις point to point (το βιβλίο γράφει ότι δεν χρησιμοποιούνται για πιστοποίηση χρηστών, αλλά είναι λάθος).
- **Single Sign On:** Βασίζεται σε πιστοποίησεις ενός παράγοντα και είναι συνήθως λιγότερο ασφαλές από τη χρήση πολλαπλών passwords. Single Sign On ουσιαστικά σημαίνει ότι ένας χρήστης μπορεί να εισέλθει με το όνομα και τον κωδικό του σε ένα σύστημα και να χρησιμοποιήσει έπειτα όλες τις υπηρεσίες που του παρέχει το δίκτυο, χωρίς να χρειαστεί επιπλέον αυθεντικοποίηση.
- **Κέρβερος:** Κρυπτογράφηση για τη διασφάλιση της εμπιστευτικότητας των δεδομένων και πιστοποίηση των χρηστών.
- **IPSec (IP Security):** Το Internet Protocol Security είναι ένα αναπτυσσόμενο πρότυπο για ασφάλεια στο επίπεδο δικτύου. Πριν την ανάπτυξη του, η ασφάλεια συνήθως εστιάζονταν στο επίπεδο εφαρμογής με βάση το μοντέλο OSI. Το IPSec παρέχει δύο επιλογές ασφάλειας:
 - **Αυθεντικότητα της επικεφαλίδας των IP πακέτων:** παρέχεται η δυνατότητα αυθεντικοποίησης του αποστολέα των πακέτων.
 - **ESP, Encapsulation Security Payload:** υποστηρίζεται η αυθεντικότητα τόσο της επικεφαλίδα των πακέτων όσο και των δεδομένων που μεταφέρουν.

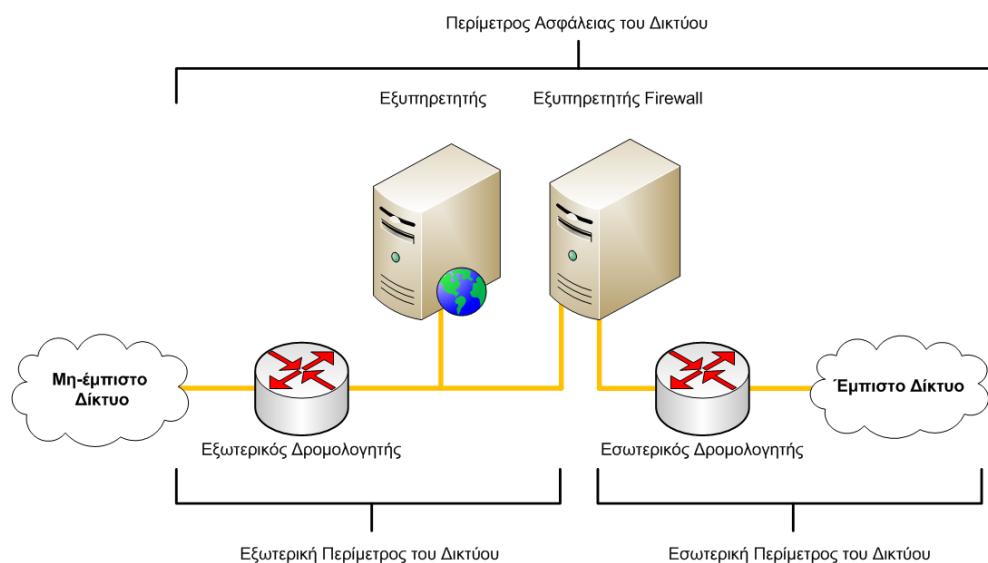
Το IPSec είναι ιδιαίτερα χρήσιμο για δίκτυα VPN (εικονικά ιδιωτικά δίκτυα, Virtual Private Networks) όσο και για χρήστες που συνδέονται στο δίκτυο μέσω επιλεγομένων τηλεφωνικών γραμμών (dial up).

- **Firewall ή τείχος προστασίας:** Το εξηγούμε παρακάτω.

Firewall

Η έννοια αναφέρεται στο σύνολο των προγραμμάτων και φίλτρων που έχουμε εγκαταστήσει στις πύλες (gateways, τα σημεία στο δίκτυο που μας συνδέουν με κάποιο εξωτερικό μη-έμπιστο δίκτυο, π.χ. το Internet και γενικά δίκτυα που δεν ελέγχονται από εμάς). Τα προγράμματα και τα φίλτρα που συνιστούν το firewall, εγκαθίστανται σε δρομολογητές και σε υπολογιστές που τυπικά αναλαμβάνουν αποκλειστικά αυτό το ρόλο.

Στο σχήμα 8.8 βλέπουμε το διαχωρισμό του δίκτυου της επιχείρησης με τα υπόλοιπα δίκτυα με τη βοήθεια αρχιτεκτονικής που βασίζεται σε δρομολογητές και εξυπηρετητές. Ο εξωτερικός δρομολογητής συνδέει το εξωτερικό μη-έμπιστο δίκτυο (συνήθως το Internet) με το εσωτερικό μας δίκτυο. Η σύνδεση δεν γίνεται απευθείας, αφού παρεμβάλλεται το μηχάνημα που στο σχήμα φαίνεται ως “εξυπηρετητής firewall”. Ο εξωτερικός δρομολογητής μπορεί να περιέχει ένα πρόγραμμα φίλτρου που κόβει από την αρχή πακέτα που γνωρίζουμε ότι δεν μπορεί να είναι έγκυρα για το δίκτυο μας (π.χ. που απευθύνονται σε ports ή μηχανήματα που δεν παρέχουν τις αντίστοιχες υπηρεσίες).



Σχήμα 8.8: Παράδειγμα δικτύου με χρήση firewall

Ο υπολογιστής που βρίσκεται στην εξωτερική περίμετρο του δικτύου, αμέσως μετά τον εξωτερικό δρομολογητή, αναλαμβάνει τυπικά να παρέχει κάποιες υπηρεσίες σε όσους συνδέονται στο δίκτυο της εταιρίας από το μη έμπιστο δίκτυο. Π.χ. μπορεί να είναι ένας web server που να περιέχει τον δικτυακό τόπο (ιστοσελίδες) της εταιρίας.

Τα πακέτα που κατευθύνονται προς το εσωτερικό δίκτυο της εταιρίας, εφόσον περάσουν από το πρώτο φίλτρο στον εξωτερικό δρομολογητή, εισέρχονται στο μηχάνημα firewall. Εκεί διευκρινίζεται σε ποιο εσωτερικό μηχάνημα και port κατευθύνονται και ανάλογα τους επιτρέπεται ή τους απαγορεύεται η είσοδος. Τυπικά, τα πακέτα στα οποία δεν επιτρέπεται να περάσουν απλώς απορρίπτονται. Το firewall μπορεί να επιτρέψει πακέτα τα οποία έρχονται ως απάντηση σε μια επικοινωνία που ξεκίνησε ένας χρήστης από το εσωτερικό δίκτυο (π.χ. ένας υπάλληλος που διαβάζει μια ιστοσελίδα στο Διαδίκτυο), αλλά απαγορεύει την είσοδο πακέτων που δεν κατευθύνονται σε κάποια ενεργή υπηρεσία. Μπορεί να επιτρέπεται επίσης πρόσβαση σε συγκεκριμένες IP (μηχανήματα) του εσωτερικού δικτύου ή σε συγκεκριμένες ports που εκτελούνται υπηρεσίες (π.χ. HTTP), αλλά να απαγορεύεται σε άλλες που προορίζονται μόνο για εσωτερική χρήση (π.χ. telnet, rlogin κλπ).

Το φιλτράρισμα γίνεται με βάση τον αριθμό της πόρτας (TCP ή UDP port) στην οποία κατευθύνεται το πακέτο. Για το σκοπό αυτό εξετάζεται η επικεφαλίδα των πακέτων και απορρίπτονται όσα κατευθύνονται σε απαγορευμένες διευθύνσεις ή ports. Μετά τον εξυπηρετητή firewall, επιπλέον πακέτα μπορούν να απορριφθούν και στο δεύτερο (εσωτερικό) δρομολογητή εφόσον εκτελεί και αυτός κάποιο πρόγραμμα φίλτρου.

Γενικά υπάρχουν πολλές διαφορετικές αρχιτεκτονικές στην τοπολογία διασύνδεσης δρομολογητών και εξυπηρετητών που απαρτίζουν ένα firewall. Όσο πιο πολύπλοκη είναι η αρχιτεκτονική (κάτι που συνήθως επιτυγχάνεται με πολλαπλά στρώματα προστασίας το ένα μετά το άλλο), τόσο πιο δύσκολο είναι να παραβιαστεί η ασφάλεια του εσωτερικού δικτύου της επιχείρησης.

8.3.6 Αποφυγή Καταστροφών

Το πληροφοριακό σύστημα μιας εταιρίας είναι πολύ σημαντικό στην εύρυθμη λειτουργία της. Ουσιαστικά σήμερα οι εταιρίες βασίζονται στα πληροφοριακά τους συστήματα για την καθημερινή τους εργασία – σε περίπτωση βλάβης η απώλειας δεδομένων, η εταιρία συνήθως δεν μπορεί να λειτουργήσει καθόλου. Είναι πολύ σημαντικό η εταιρία να είναι προετοιμασμένη να επιλύσει προβλήματα που ίσως παρουσιαστούν στο συντομότερο δυνατό χρονικό διάστημα.

Τα προβλήματα ενός μοντέρνου, κατανευμένου πληροφοριακού συστήματος εντοπίζονται συνήθως σε κάποιον από τους παρακάτω τομείς:

- Βλάβες ενεργού εξοπλισμού (σκληροί δίσκοι, τροφοδοτικά, μητρικές κάρτες, δρομολογητές κλπ), παθητικού εξοπλισμού (καλωδιώσεις, racks κλπ).
- Δυσλειτουργίες λειτουργικών συστημάτων και εφαρμογών που μπορεί να οφείλονται σε προβληματικές ρυθμίσεις ή εγγενή προβλήματα τους (bugs).

- Δυσλειτουργίες πρωτοκόλλων επικοινωνίας.
- Δυσλειτουργίες που οφείλονται στα δεδομένα (π.χ. προβληματικά (corrupted) δεδομένα προκαλούν την κατάρρευση κάποιας εφαρμογής).
- Φυσικές καταστροφές (φωτιές, πλημμύρες κλπ).
- Επιθέσεις από κακόβουλα άτομα (crackers, και παρακαλώ να μην το μπερδεύουμε με τους hackers όπως κάνει το σχολικό βιβλίο).

Κάθε επιχείρηση που σέβεται το όνομα της και τους πελάτες της, θα πρέπει να είναι σε θέση να αντεπεξέλθει σε οποιαδήποτε από τις παραπάνω καταστάσεις, στο συντομότερο χρονικό διάστημα και με τις λιγότερες πιθανές επιπτώσεις, τόσο για την ίδια όσο και για τους πελάτες της. Φανταστείτε για παράδειγμα τι πλήγμα είναι για μια χρηματιστηριακή εταιρία ή τράπεζα να μην μπορεί να εξυπηρετήσει για μεγάλο διάστημα τους πελάτες της για λόγους τεχνικών προβλημάτων. Η ύπαρξη σχεδίου αποφυγής καταστροφών (και ανάκαμψης από αυτές) είναι απαραίτητη.

Κάποιες έννοιες που σχετίζονται με το σχεδιασμό αποφυγής καταστροφών είναι οι παρακάτω:

- **Ανάκαμψη (recovery):** Η αποκατάσταση της λειτουργίας του συστήματος μετά από κάποια δυσλειτουργία.
- **Σχέδιο Συνέχειας (Continuity Plan):** Η πλήρης λεπτομερή περιγραφή των βημάτων που πρέπει να πραγματοποιηθούν για να ανακάμψει το σύστημα μετά από μια σοβαρή παραβίαση.
- **Εφεδρικό Αντίγραφο Πληροφοριών (Information Backup):** Η τήρηση πλήρους αντίγραφου των πληροφοριών που μπορεί να χρησιμοποιηθεί για ανάκαμψη ακόμα και από πλήρη απώλεια. Υπάρχουν περιπτώσεις που χρειάζεται να έχουμε ανάκαμψη σε μηδενικό χρόνο, δηλ. να μην υπάρχει καμιά καθυστέρηση όταν έχουμε μια σοβαρή βλάβη. Ουσιαστικά αυτό σημαίνει ότι η λειτουργία του πληροφοριακού συστήματος δεν σταματά ποτέ. Για να γίνει αυτό, πρέπει να έχουμε περισσότερα από ένα πληροφοριακά συστήματα που να λειτουργούν παράλληλα χρησιμοποιώντας τα ίδια δεδομένα (τα δεδομένα πρέπει να είναι συνέχεια σε συγχρονισμό μεταξύ των δύο συστημάτων). Πρόκειται πρακτικά για κλωνοποίηση του αρχικού συστήματος και της δομής του δικτύου. Μπορεί το παραπάνω να φαίνεται υπερβολικό και είναι γεγονός ότι έχει μεγάλο κόστος, ωστόσο σε ορισμένες περιπτώσεις εταιριών (που βασίζουν όλο το μοντέλο λειτουργίας τους στο πληροφοριακό τους σύστημα) δεν υπάρχει άλλη λύση.

Προφανώς κάθε επιχείρηση θα πρέπει να αναλύσει τους κινδύνους που διατρέχει κάθε τμήμα του πληροφοριακού της συστήματος και να αποφασίσει πόσο κρίσιμοι είναι και μέχρι ποιο σημείο είναι διατεθειμένη να το προστατεύσει. Η λύση θα πρέπει

να λαμβάνει υπόψη το κόστος υλοποίησης σε συνάρτηση με την κρισιμότητα των δεδομένων που προστατεύει ή το πόσο εύκολο είναι να αναδημιουργηθούν αυτά τα δεδομένα. Γενικά, τα περισσότερα πληροφοριακά συστήματα σήμερα βασίζονται σε αρχιτεκτονικές πελάτη – εξυπηρετητή (client – server). Σε τέτοια συστήματα, το πιο κρίσιμο σημείο είναι το κτήριο που στεγάζει τους βασικούς υπολογιστές (servers), γνωστό ως main site. Αρκετές εταιρίες και οργανισμοί μεγάλου μεγέθους και με κρίσιμα δεδομένα, επιλέγουν να υλοποιήσουν δύο main sites, ώστε σε περίπτωση καταστροφής του ενός να αναλάβει αυτόματα το δεύτερο. Τα δύο αυτά κεντρικά sites πρέπει προφανώς να είναι αρκετά απομονωμένα μεταξύ τους ώστε να μην επηρεαστούν και τα δύο από την ίδια φυσική καταστροφή (π.χ. φωτιά, πλημμύρα).

Η ύπαρξη δυο κεντρικών site προϋποθέτει και την ύπαρξη δύο ουσιαστικά ισοδύναμων υπολογιστικών συστημάτων καθώς και της απαραίτητης τηλεπικοινωνιακής υποδομής μεταξύ τους ώστε να γίνεται συνέχεια συγχρονισμός των δεδομένων. Τα κεντρικά site θα πρέπει να περιλαμβάνουν πρόβλεψη για επαλληλία των κεντρικών δικτυακών συσκευών (δρομολογητών, switches κλπ). Πρακτικά, αυτό σημαίνει ότι για κάθε τέτοια συσκευή θα πρέπει να υπάρχει μια εναλλακτική έτοιμη να αναλάβει (ενδεχομένως αυτόματα) σε περίπτωση βλάβης της πρώτης. Πρέπει επίσης να υπάρχει εναλλακτικότητα στη διασύνδεση των διάφορων εσωτερικών τοπικών δικτύων (LANs). Αυτό σημαίνει ότι αν για παράδειγμα χαλάσει ένας δρομολογητής που ενώνει δύο εσωτερικά δίκτυα και δεν μπορεί να αντικατασταθεί άμεσα, να υπάρχει κάποια εναλλακτική διαδρομή μέσω άλλων δρομολογητών ώστε τα δίκτυα αυτά να συνεχίσουν να είναι συνδεδεμένα (έστω και με πιο αργή ταχύτητα).

Πέρα φυσικά από τις παραπάνω προβλέψεις εναλλακτικότητας και επαλληλίας, θα πρέπει να υπάρχει και αντίστοιχο σχέδιο για εφεδρικές λύσεις τόσο για τον εξοπλισμό του πληροφοριακού συστήματος όσο και για τις εφαρμογές και τα δεδομένα (π.χ. πολιτική τήρησης αντιγράφων ασφαλείας – backup. Συνηθίζεται να τηρούνται περισσότερα από ένα αντιγραφα ασφαλείας, με ένα πάντα να φυλάσσεται σε προστατευμένο χώρο εκτός του main site ώστε να μην επηρεαστεί από τυχόν καταστροφή του).

Γενικά δεν υπάρχει καθιερωμένη λύση για τη μορφή του σχεδίου αποφυγής και αντιμετώπισης καταστροφών μιας επιχείρησης. Η λύση διαφέρει ανάλογα με τη δομή του συστήματος, την σπουδαιότητα και κρισιμότητα των δεδομένων, το χρόνο που μπορούμε να ανεχθούμε μέχρι την ανάκαμψη της λειτουργίας και φυσικά τα χρήματα που είναι η επιχείρηση διατεθειμένη να ξοδέψει. Σίγουρα πρόκειται για ένα πολύ σοβαρό έργο, το οποίο δεν μπορεί να αναβληθεί ή να μην σχεδιαστεί σωστά από την αρχή, καθώς αυτό θα αποδειχθεί κάποια στιγμή μοιραίο για την επιχείρηση.

Μέρος II

Παραρτήματα

Παράρτημα Α

Θέματα Προηγούμενων Ετών

Θεματα 2009

Θέμα 10

- A.** Στον παρακάτω πίνακα, η Στήλη Α περιέχει τις τεχνολογίες δικτύων ευρείας περιοχής (ΔΕΠ) και η Στήλη Β περιέχει τα πλεονεκτήματα ή τα μειονεκτήματα τους. Να γράψετε στο τετράδιο σας τους αριθμούς της στήλης Α και δίπλα τα γράμματα της στήλης Β που αντιστοιχούν σ' αυτούς.

ΣΤΗΛΗ Α	ΣΤΗΛΗ Β
1. ψηφιακό δίκτυο ενοποιημένων υπηρεσιών (ISDN) – πλεονέκτημα	α. πολύ υψηλές ταχύτητες
2. ψηφιακή συνδρομητική γραμμή (xDSL) – πλεονέκτημα	β. μικρή ταχύτητα
3. επιλεγόμενες τηλεφωνικές γραμμές – μειονέκτημα	γ. γρήγορη εγκαθίδρυση σύνδεσης
4. ψηφιακή συνδρομητική γραμμή (xDSL) – μειονέκτημα	δ. μικρή απόσταση

Μονάδες 8

- B.** Να γράψετε στο τετράδιό σας τον αριθμό καθεμιάς από τις παρακάτω προτάσεις και δίπλα τη λέξη ΣΩΣΤΟ αν είναι σωστή ή τη λέξη ΛΑΘΟΣ, αν είναι λανθασμένη.

- Οι διάφορες παραλλαγές της ψηφιακής συνδρομητικής γραμμής (xDSL) υποστηρίζουν μόνο συμμετρική μετάδοση δεδομένων.
- Στο μοντέλο OSI υπάρχουν τέσσερα επίπεδα, ενώ στο μοντέλο TCP/IP επτά επίπεδα.
- Η μάσκα υποδικτύου χρησιμοποιείται για το διαχωρισμό των διευθύνσεων IP στα τμήματα δικτύου και υπολογιστή.
- Το σύστημα ονομάτων περιοχών (DNS) είναι μηχανισμός απεικόνισης των IP διευθύνσεων σε ονόματα και το αντίστροφο.

Μονάδες 8

- Γ.** Να μεταφέρετε στο τετράδιό σας τον αριθμό των παρακάτω επιλογών και δίπλα το γράμμα της σωστής απάντησης.

- Ποιο πρωτόκολλο βρίσκεται στο επίπεδο μεταφοράς του μοντέλου TCP/IP;
 - Το πρωτόκολλο απλού ταχυδρομείου (SMTP).
 - Το πρωτόκολλο αυτοδύναμου πακέτου (UDP).
 - Το πρωτόκολλο διαδικτύου (IP).

- δ.** Το πρωτόκολλο μηνύματος και ελέγχου διαδικτύου (ICMP).
2. Ποια από τις παρακάτω επιλογές είναι μαθηματική συνάρτηση, της οποίας το αποτέλεσμα δεν μπορεί με αναστροφή να μας παράγει την αρχική είσοδο.
 - α.** Το μυστικό κλειδί
 - β.** Η κρυπτογράφηση
 - γ.** Η λειτουργία κατατεμαχισμού
 - δ.** Η μεταμφίεση

Μονάδες 9

Θέμα 2ο

- A.** Ποιο είναι το σημαντικό πλεονέκτημα της ομάδας πρωτοκόλλων TCP/IP;

Μονάδες 15

- B.** Δίνεται η IP διεύθυνση: 150.23.05.0/22

1. Ποιο είναι το πρόθεμα;

Μονάδες 5

2. Τι προσδιορίζει το πρόθεμα;

Μονάδες 5

Θέμα 3ο

- A.** Έστω ότι οι υπολογιστές A και B συνδέονται στο ίδιο φυσικό δίκτυο. Ο υπολογιστής A θέλει να στείλει δεδομένα στον υπολογιστή B και γνωρίζει μόνο τη διεύθυνση IP του υπολογιστή B.

Να τοποθετήσετε στη σωστή σειρά την παρακάτω ακολουθία ενεργειών, για να ολοκληρωθεί η αποστολή των δεδομένων από τον υπολογιστή A στον υπολογιστή B.

1. Μετατρέπεται η IP διεύθυνση στην αντίστοιχη Ethernet με βάση τον ενημερωμένο ARP πίνακα.
2. Λαμβάνεται η ARP απάντηση και μία νέα εγγραφή καταχωρείται στον ARP πίνακα.
3. Το IP αυτοδύναμο πακέτο βγαίνει από την ουρά αναμονής, σχηματίζεται ένα Ethernet πακέτο και μεταδίδεται στο δίκτυο.

4. Δημιουργείται η ARP ερώτηση.
5. Το IP αυτοδύναμο πακέτο μπαίνει σε ουρά αναμονής.

Μονάδες 10

- B.** Να αναφέρετε, ονομαστικά, τις πέντε (5) περιοχές διαχείρισης που έχουν οριστεί με βάση το μοντέλο OSI.

Μονάδες 5

- Γ.** Δίνονται:

Η IP διεύθυνση:

11010001.10101010.01010101.00001111

Η μάσκα υποδικτύου:

11111111.11111111.11110000.00000000

1. Από πόσα bits αποτελείται το τμήμα δικτύου;

Μονάδες 4

2. Να προσδιορίσετε τη διεύθυνση υποδικτύου.

Μονάδες 6**Θέμα 4ο**

- A.** Ένα IP αυτοδύναμο πακέτο 2000 bytes δεδομένων και 20 bytes επικεφαλίδας μεταδίδεται μέσω φυσικού δικτύου που υποστηρίζει πακέτα συνολικού μήκους 820 bytes (800 bytes δεδομένα και 20 bytes επικεφαλίδα). Να συμπληρώσετε τον παρακάτω πίνακα αιτιολογώντας την τιμή κάθε κελιού.

	1ο κομμάτι	2ο κομμάτι	3ο κομμάτι
DF			
Συνολικό μήκος			
MF			
Δείκτης Εντοπισμού Τμήματος			

Να θεωρήσετε ότι η επικεφαλίδα όλων των νέων αυτοδύναμων πακέτων (κομματών), που προέκυψαν από την διάσπαση του αρχικού αυτοδύναμου πακέτου, αποτελείται μόνο από το σταθερό της τμήμα των 20 bytes.

Μονάδες 16

- B.** Έστω ότι δύο χρήστες A και B έχουν συμφωνήσει να χρησιμοποιήσουν αλγόριθμο δημοσίου κλειδιού τον digital signature standard και αλγόριθμο κατατεμαχισμού τον MD5. Να υποθέσετε ότι οι A και B χρήστες έχουν δημιουργήσει επιτυχώς το ζευγάρι δημόσιου – ιδιωτικού κλειδιού και έχουν ανταλλάξει τα δημόσια κλειδιά τους. Να περιγράψετε **μόνο** τη διαδικασία που θα ακολουθηθεί, ώστε ο χρήστης A να στείλει ψηφιακά υπογεγραμμένο έγγραφο στο χρήστη B.

Μονάδες 9

Θέματα 2010

Θέμα A

- A1.** Να γράψετε στο τετράδιό σας τον αριθμό καθεμιάς από τις παρακάτω προτάσεις και δίπλα τη λέξη ΣΩΣΤΟ, αν είναι σωστή ή τη λέξη ΛΑΘΟΣ, αν είναι λανθασμένη.
- α.** Ένα από τα μειονεκτήματα του xDSL είναι το χαμηλό κόστος εγκατάστασης και λειτουργίας.
 - β.** Στην αρχιτεκτονική TCP/IP το επίπεδο πρόσβασης δικτύου παρέχει την πρόσβαση στο φυσικό μέσο.
 - γ.** Το πρωτόκολλο ελέγχου μετάδοσης (Transmission Control Protocol, TCP) είναι το βασικό πρωτόκολλο του επιπέδου δικτύου της τεχνολογίας TCP/IP.
 - δ.** Η εξασφάλιση αυθεντικότητας είναι μία από τις πιο κοινές χρήσεις της ασυμμετρικής κρυπτογράφησης.

Μονάδες 8

- A2.** Να μεταφέρετε στο τετράδιο σας το γράμμα της σωστής απάντησης.

Ο εξυπηρετητής του ηλεκτρονικού ταχυδρομείου χρησιμοποιεί:

- α.** To TCP port 20.
- β.** To TCP port 21.
- γ.** To TCP port 23.
- δ.** To TCP port 25.

Μονάδες 5

- A3.** Να αντιστοιχίσετε κάθε στοιχείο της στήλης A με ένα στοιχείο της στήλης B.

ΣΤΗΛΗ Α	ΣΤΗΛΗ Β
1. διεπαφή βασικού ρυθμού (BRI)	α. λέξεις των 32bits
2. διεπαφή πρωτεύοντος ρυθμού (PRI)	β. διευθύνσεις 32bits
3. πεδίο μήκος επικεφαλίδας	γ. δύο κανάλια B των 64 Kbps
4. η τεχνολογία TCP/IP χρησιμοποιεί	δ. 30 κανάλια των 64 Kbps

Μονάδες 8

- A4** Ποια είναι τα πλεονεκτήματα και τα μειονεκτήματα των επιλεγόμενων τηλεφωνικών γραμμών;

Μονάδες 4

Θέμα Β

B1. Τι είναι η ψηφιακή υπογραφή;

Μονάδες 5

B2. Τι είναι το δημόσιο κλειδί;

Μονάδες 5

B3. Ποιες είναι οι βασικές στήλες του πίνακα δρομολόγησης;

Μονάδες 8

B4. Σε ποιες περιπτώσεις χρησιμοποιείται η μέθοδος της μεταμφίεσης;

Μονάδες 7

Θέμα Γ

Γ1. Τι ονομάζεται Αριθμός Σειράς των τμημάτων της επικεφαλίδας του πρωτοκόλλου TCP;

Μονάδες 4

Γ2. Τι ονομάζεται Έλεγχος Ροής του πρωτοκόλλου TCP;

Μονάδες 5

Γ3. Να μεταφέρετε στο τετράδιό σας τον παρακάτω πίνακα και να τον συμπληρώσετε με τις κλάσεις IP διευθύνσεων.

Class A		
Class B		
Class C		
Class D		

Μονάδες 16

Θέμα Δ

Δ1. Στην επικεφαλίδα ενός TCP τμήματος το πεδίο παράθυρο έχει τεθεί σε 2.000 οκτάδες και το πεδίο επιβεβαίωσης σε 10.000 οκτάδες. Σε ποια περιοχή οκτάδων μπορεί να δεχθεί το άκρο που έχει δηλώσει αυτές τις τιμές;

Μονάδες 10

- Δ2.** Ένα IP αυτοδύναμο πακέτο 2.400 bytes δεδομένων και 20 bytes επικεφαλίδας μεταδίδεται μέσω φυσικού δικτύου που υποστηρίζει πακέτα συνολικού μήκους 620 bytes. Να συμπληρώσετε τον παρακάτω πίνακα, αφού πρώτα εντοπίσετε σε πόσα κομμάτια διασπάται το αρχικό IP αυτοδύναμο πακέτο.

	1ο κομμάτι
πεδίο Αναγνώρισης				
πεδίο Μήκος Επικεφαλίδας				
DF				
Συνολικό Μήκος				
MF				
Δείκτης Εντοπισμού Τμήματος				

Να θεωρήσετε ότι η επικεφαλίδα όλων των νέων αυτοδύναμων πακέτων (κομματιών), που προέκυψαν από τη διάσπαση του αρχικού IP αυτοδύναμου πακέτου, αποτελείται μόνο από το σταθερό της τμήμα των 20 bytes.

Μονάδες 15