ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΕΠΙΣΤΗΜΩΝ

Τ.Ε.Ι. ΚΡΗΤΗΣ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ Τ.Ε.

Πτυχιακή Εργασία

Ονοματεπώνυμο σπουδαστή: Μαυροειδής Αλέξανδρος

Α.Μ.: 4729

Θέμα: **Τεχνική Ανασκόπηση xDSL δρομολογητών με έμφαση στις τεχνολογίες ADSL & VDSL**

Επιβλέπων καθηγητής : Ιωάννης Μπαρμπουνάκης

Περίληψη

Σκοπός της παρούσας πτυχιακής εργασίας είναι η παρουσίαση των τεχνολογιών ADSL και VDSL, των τεχνικών χαρακτηριστικών τους και πως διασυνδέουν τον πάροχο με έναν καταναλωτή μέσω του ζεύγους χάλκινων αγωγών. Έπειτα εξηγείται τι είναι οι δρομολογητές (Router) και τα χαρακτηριστικά τους, από τι αποτελούνται οι συσκευές αυτές, τα πρωτόκολλα δρομολόγησης και μεταφοράς των πακέτων και η ασφάλειά τους, και τέλος συγκρίνουμε κάποια από τα μοντέλα δρομολογητών (Router) που κυκλοφορούν στην Ελληνική Αγορά.

Αναλυτικά, στο πρώτο κεφάλαιο παρουσιάζουμε τη τεχνολογία DSL και τα τεχνικά χαρακτηριστικά της, όπως ο μέγιστος ρυθμός μετάδοσης download/upload σε Mbps, ο σηματοθορυβικός λόγος (S/N) και η διάρθρωση μιας DSL σύνδεσης. Παρακάτω, αναφέρεται η τεχνική Orthogonal Frequency Division Multiplexing (OFDM) και ο τρόπος διαμόρφωσης Discrete MultiTone (DMT) που χρησιμοποιεί OFDM. Ακολουθεί σύντομη περιγραφή των τεχνολογιών FTTC, FTTB, FTTH και τέλος οι ασύμμετρες και συμμετρικές παραλλαγές της DSL.

Στο δεύτερο κεφάλαιο αναλύεται η τεχνολογία ADSL, εξηγείται η επίδραση της απόστασης στην ταχύτητα της ADSL και τα μειονεκτήματα/πλεονεκτήματά της. Παρακάτω ακολουθεί μία εξέλιξη της ADSL, που λέγεται VDSL και πλεονεκτεί ως προς την ADSL ως προς τον υψηλό ρυθμό μετάδοσης που επιτυγχάνει.

Στο τρίτο κεφάλαιο αναλύουμε τον δρομολογητή (router). Επίσης περιγράφουμε τα διάφορα είδη δρομολόγησης και τα συστήματα διευθυνσιοδότησης IP. Έπειτα περιγράφουμε τα multicast πρωτόκολλα δρομολόγησης που χρησιμοποιούν δύο τεχνικές για την προώθηση των πακέτων **Flooding** και **Reverse Path Forwarding.** Στη συνέχεια αναφέρουμε τις δρομολογήσεις MPLS, ATM. Τέλος, εξηγούμε τον όρο IP spoofing (Security) που αναφέρεται στην δημιουργία πακέτων με ψεύτικη διεύθυνση προέλευσης.

Στο τέταρτο κεφάλαιο στόχος μας είναι να παρουσιάσουμε τα χαρακτηριστικά ενός δρομολογητή (router): τείχος προστασίας (firewall), πρωτόκολλα επικοινωνίας και TCP/IP. Ακολουθεί, η περιγραφή του DHCP πρωτοκόλλου, και η εφαρμογή του. Τέλος, γίνεται μια αναφορά στα πρωτόκολλα Address Resolution Protocol (ARP), Network Address Translation (NAT) και Domain Name Service DNS.

Στο πέμπτο κεφάλαιο δείχνουμε το Virtual private network (VPN), τα χαρακτηριστικά του (π.χ. tunneling) και τις χρήσεις του. Ακολουθούν περιγραφές των πρωτοκόλλων IPsec, PPTP, L2F και L2TP. Το κεφάλαιο ολοκληρώνεται με την πιστοποίηση ταυτότητας του χρήστη με πρωτόκολλο chap σε σύνδεση PPP.

Τέλος στο έκτο κεφάλαιο συγκρίνουμε κάποια βασικά μοντέλα XDSL δρομολογητών της τοπικής αγοράς.

Summary

The purpose of the present thesis is the presentation of ADSL and VDSL technologies, their technical characteristics and the way they interconnect the provider to a consumer via a copper pair. Then, a description of the router and its features is given, what do these devices constitute of, packet routing and transport protocols and their safety, and finally a comparison is made regarding some of the xDSL router models adopted in the Greek Market.

Specifically, in the first chapter we present the DSL technology and its technical characteristics, such as maximum transmission rate of download / upload in Mbps, the signal-ratio (S/N) and the structure of a DSL connection. In the following, the Orthogonal Frequency Division Multiplexing (OFDM) technique is referred and how Discrete MultiTone modulation (DMT) makes use of OFDM. A brief description of technologies FTTC, FTTB, FTTH and finally the asymmetrical and symmetrical DSL variants, is given.

The second chapter analyzes the ADSL technology, the effect of the distance on the ADSL speed and its disadvantages/advantages are explained. An advancement of ADSL, called VDSL that achieves higher data rate transmission compared to ADSL, is finally presented.

In the third chapter we analyze the router. We also describe the different types of routing and IP addressing systems. Then we analyze the multicast routing protocols that use two techniques to forward packets, namely Packet Flooding and Reverse Path Forwarding. Then, we mention the routing procedures followed by MPLS and ATM networks. At the end of the chapter, we explain the term IP spoofing (Security) referred to a packet creation process with false source address.

In the fourth chapter, our aim is to present the characteristics of a router: firewall, communication protocols and TCP/IP. Here, the DHCP protocol and its implementation are described. Finally, a reference is made to protocols Address Resolution Protocol (ARP), Network Address Translation (NAT) and Domain Name Service DNS.

In the fifth chapter we show the Virtual private network (VPN), its characteristics (eg tunneling) and its uses. Descriptions of the IPsec protocols, PPTP, L2F and L2TP follow. The chapter concludes with the user authentication chap protocol under PPP.

Finally, in the sixth chapter, we attempt a comparison of some basic xDSL router models adopted in the local market.

ΠΕΡΙΕΧΟΜΕΝΑ

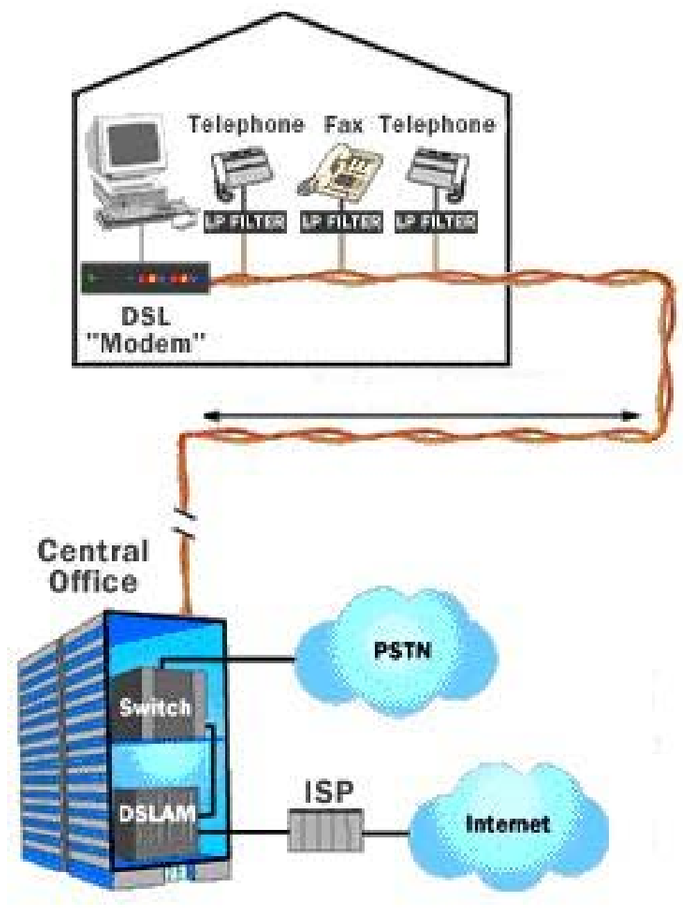
Κεφάλαιο 1: xDSL

Μία τεχνολογία η οποία χρησιμοποιείται τα τελευταία χρόνια στην Ελλάδα, είναι το DSL (Digital Subscriber Line-Ψηφιακή Γραμμή Συνδρομητή), το οποίο παρέχει πρόσβαση υψηλής ταχύτητας στο διαδίκτυο χρησιμοποιώντας τις κοινές τηλεφωνικές γραμμές. Στην ουσία αποτελεί μια τεχνολογία που μετατρέπει το απλό τηλεφωνικό καλώδιο σε ένα δίαυλο ψηφιακής επικοινωνίας μεγάλου εύρους ζώνης με τη χρήση ειδικών modems, τα οποία τοποθετούνται στις δυο άκρες της γραμμής.

Τα modems DSL χωρίζονται σε δύο κατηγορίες:

- Συμμετρικά DSL (Symmetric DSL), τα οποία προσφέρουν ταχύτητα upload ίδια με την ταχύτητα download.
- Ασύμμετρα DSL (Asymmetric DSL) τα οποία προσφέρουν ταχύτητα upload μικρότερη από την ταχύτητα download.

Η διάρθρωση ενός τυπικού δικτύου DSL φαίνεται στο ακόλουθο σχήμα:



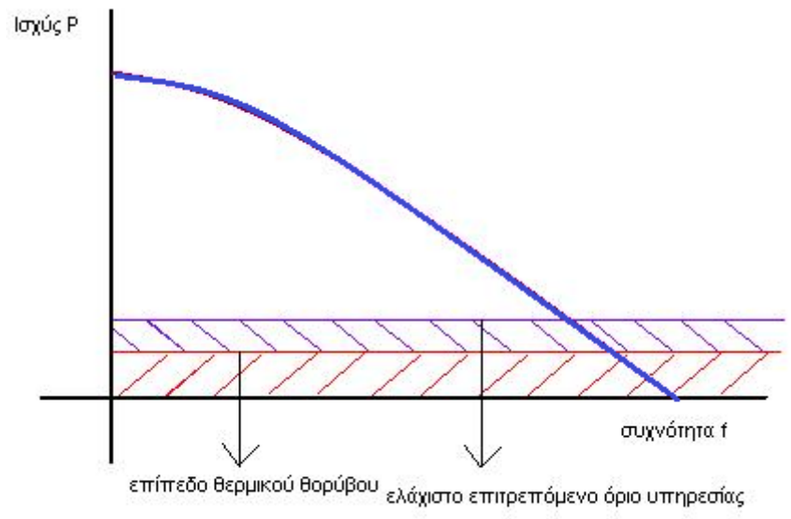
Από την πλευρά του παρόχου ISP (Internet Service Provider) υπάρχει το DSLAM (Digital Subscriber Line Access Multiplexer) το οποίο είναι μία συσκευή δικτύου που βρίσκεται κοντά στο συνδρομητή και η οποία συνδέει πολλές διαφορετικές γραμμές DSL συνδρομητών με το κεντρικό δίκτυο. Επίσης υπάρχει το Switch, το οποίο προσθέτει στο σήμα του ISP το σήμα της φωνής από την υπηρεσία τηλεφωνίας (POTS). Το σύνθετο αυτό σήμα οδηγείται στον συνδρομητή, όπου διαχωρίζεται με τη χρήση φίλτρων. Στις τηλεφωνικές συσκευές χρησιμοποιείται χαμηλοπερατό φίλτρο που αφήνει μόνο τις συχνότητες μέχρι 4kHz να περάσουν, οι οποίες είναι και οι συχνότητες που χρησιμοποιούνται από την υπηρεσία της τηλεφωνίας.

Σκοπός της DSL

Σκοπός της τεχνολογίας DSL είναι η χρησιμοποίηση όλης της δυναμικής περιοχής των καλωδίων χαλκού που χρησιμοποιούνται στα δίκτυα σταθερής τηλεφωνίας, ώστε εκτός από τη μετάδοση της φωνής με τις ήδη υπάρχουσες υπηρεσίες (POTS) να μεταδίδουμε ταυτόχρονα και δεδομένα με τη χρήση διαμορφωμένου ψηφιακού σήματος.

Προτού εξηγήσουμε τη λειτουργία της DSL θα πρέπει να έχουμε υπόψη, ότι το τηλεφωνικό δίκτυο του ΟΤΕ σχεδιάστηκε αποκλειστικά για τη μετάδοση φωνής. Η ανθρώπινη φωνή κυμαίνεται μεταξύ 300 Hz έως 4 KHz. Για να αποφευχθούν προβλήματα στην φωνητική επικοινωνία (παράσιτα), χρησιμοποιούνται φίλτρα, ώστε να αποκόπτονται οι «περιττές» συχνότητες (μεγαλύτερες των 4 KHz). Η DSL πολύ απλά κάνει χρήση του υπολοιπόμενου εύρους ζώνης (των αποκομμένων συχνοτήτων στις τηλεφωνικές γραμμές χαλκού) με αποτέλεσμα να έχουμε υψηλές ταχύτητες. Ο δίαυλος αυτός μεταφέρει ταυτόχρονα τις χαμηλές συχνότητες για τη μεταφορά του σήματος της φωνής και τις υψηλές συχνότητες για τα δεδομένα. Ανάλογα με το είδος του modem που θα συνδέσουμε πετυχαίνουμε και διαφορετικές επιδόσεις. Τα φυσικά χαρακτηριστικά του μέσου καθορίζουν και τη δυναμική περιοχή του, την οποία μπορούμε να εκμεταλλευτούμε για τη μετάδοση των δεδομένων.

Η δυναμική περιοχή καθορίζεται από την μέγιστη εκπεμπόμενη ισχύς και εξαρτάται από τη συχνότητα. Όσο μεγαλύτερη είναι η συχνότητα στη γραμμή μεταφοράς, τόσο μεγαλύτερες είναι οι απώλειες της γραμμής, άρα και οι απώλειες σε ισχύ στο σήμα που μεταδίδουμε, για μία δεδομένη ισχύ εκπομπής. Η ισχύς του σήματος πρέπει να είναι αρχικά πάνω από την ισχύ του θερμικού θορύβου. Ένα ακόμη μεγαλύτερο κατώφλι ισχύος, εκτός από αυτό που καθορίζεται από τον θερμικό θόρυβο είναι το κατώφλι που απαιτεί η εκάστοτε υπηρεσία ώστε να θεωρείται αξιόπιστη η μετάδοση των δεδομένων. Για παράδειγμα, το κατώφλι αυτό στο ADSL καθορίζεται στα 6dB SNR για κάθε bit μεταδιδόμενης πληροφορίας, οπότε υπολογίζοντας το επίπεδο ισχύος του θερμικού θορύβου, μπορούμε να προσδιορίσουμε και το κατώφλι ισχύος μιας αξιόπιστης υπηρεσίας.



Η δυναμική περιοχή που σημειώνεται στην παραπάνω εικόνα, καθορίζει τα όρια της υπηρεσίας. Όσο αυξάνεται το μήκος της γραμμής αυξάνεται και η απόσβεση που προκαλείται από το σήμα λόγω απωλειών της γραμμής. Οι απώλειες αυτές δεν πρέπει να είναι μεγαλύτερες από το όριο που καθορίζεται από τη δυναμική περιοχή, όπως περιγράφηκε και παραπάνω. Έτσι, με την αύξηση της απόστασης και των απωλειών όλο και χαμηλότερες συχνότητες μπορούν να χρησιμοποιηθούν, με αποτέλεσμα να μειώνεται διαρκώς η ταχύτητα μετάδοσης λόγω μεγαλύτερης απόσβεσης.

Η τεχνολογία DSL βασίζεται στην τεχνική της πολυπλεξίας στη συχνότητα. Η πολυπλεξία στη συχνότητα (FDM) είναι η αποτύπωση τμημάτων της μεταδιδόμενης πληροφορίας σε φέροντα διαφορετικής συχνότητας και η ανασύνθεσή τους στην πλευρά του δέκτη. Συγκεκριμένα, στο DSL χρησιμοποιείται η OFDM πολυπλεξία (Orthogonal Frequency Division Multiplexing) η οποία χρησιμοποιεί φέροντα που είναι όλα μεταξύ τους ορθογώνια.

Η διαφορά του OFDM από την κλασική πολυπλεξία στη συχνότητα είναι το γεγονός ότι η πολυπλεξία συνήθως χρησιμοποιείται για να μεταδώσει πολλά σήματα από διαφορετικές πηγές μέσα από ένα κανάλι ενώ η OFDM χρησιμοποιείται για να μοιράσει το ίδιο σήμα σε παράλληλες ροές και να το μεταδώσει διαμοιρασμένο μέσα από το κανάλι και στη συνέχεια να το επανασυνδέσει στο δέκτη.

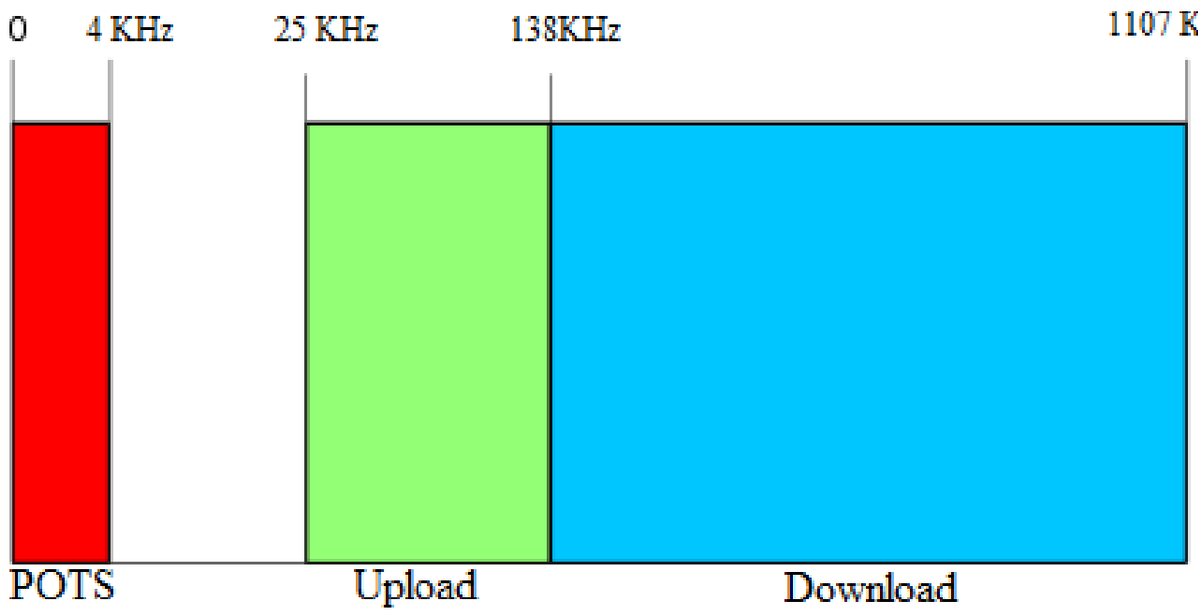
Σε μία απλή πολυπλεξία στη συχνότητα τα φέροντα συνήθως δεν είναι ορθογώνια μεταξύ τους. Έτσι είναι δυνατόν να υπάρχουν παρεμβολές από το ένα σήμα στο άλλο ειδικά στα φέροντα που βρίσκονται σε κοντινές συχνότητες. Ενώ στην OFDM τα φέροντα είναι ορθογώνια μεταξύ τους και αποφεύγει την παρεμβολή του ενός σήματος από το άλλο και επιτρέπει τη μετάδοσή τους σε ένα μικρό εύρος συχνοτήτων.

Το πλεονέκτημα της χρησιμοποίησης του OFDM έναντι ενός απλού φέροντος είναι το γεγονός ότι ο OFDM μπορεί να επιτύχει καλύτερη απόδοση σε διάφορες συνθήκες του καναλιού, π.χ. εξασθένηση σε μεγάλες συχνότητες σε ένα καλώδιο χαλκού. Για να είναι τα φέροντα ορθογώνια, πρέπει όλες οι συχνότητες των φερόντων να είναι ακέραια πολλαπλάσια της ίδιας συχνότητας.

1.1 Τεχνικές Λεπτομέρειες

Η τεχνολογία DSL στις περισσότερες μορφές της είναι συμβατή με τις προϋπάρχουσες τεχνολογίες και κυρίως με τη μετάδοση φωνής από τις κλασσικές ήδη υπάρχουσες τηλεφωνικές υπηρεσίες (POTS). Αυτό γίνεται με το διαχωρισμό του φάσματος στα εξής τμήματα:

Μία περιοχή στη βασική ζώνη η οποία χρησιμοποιείται για τη μετάδοση της φωνής στις υπηρεσίες τηλεφωνίας. Μία περιοχή υψηλών συχνοτήτων η οποία χρησιμοποιείται για τη μετάδοση ISP (Internet Service Provider) δεδομένων. Η περιοχή υψηλών συχνοτήτων χωρίζεται σε 2 μικρότερες η χαμηλότερη χρησιμοποιείται για το upload και η υψηλότερη για το download.



Το φάσμα συχνοτήτων συνοπτικά χωρίζεται:

- 0-4 KHz, φωνή
- 4-25 KHz, μη χρησιμοποιούμενο φάσμα.
- 25-138 KHz, 25 upload bins (7-31).
- 138-1107 KHz, 224 download bins (32-255).

Ο DMT (Discrete multitone modulation) τρόπος διαμόρφωσης χρησιμοποιεί OFDM (Orthogonal Frequency Division Mulitplexing) πολυπλεξία στη συχνότητα. Μοιράζει το σήμα σε 255 φέροντα (bins), κεντραρισμένα σε συχνότητες πολλαπλάσιες των 4.3125kHz. Ο DMT διαθέτει 224 downstream bins και έως και 31 upstream bins. Το bin 0 βρίσκεται στην DC συνιστώσα και δε μπορεί να χρησιμοποιηθεί. Όταν μεταδίδεται μέσα από την ίδια γραμμή και σήμα φωνής, το πρώτο bin που χρησιμοποιείται είναι το bin 7, ενώ οι κατώτερες συχνότητες αφήνονται κενές, ώστε να μεταδοθεί μέσα από αυτές το σήμα φωνής. Η κεντρική συχνότητα του N-καναλιού (bin) είναι (N x 4.3125) kHz. Το φάσμα κάθε καναλιού συμπίπτει εν μέρει με το φάσμα γειτονικών καναλιών και δεν περιορίζεται σε εύρος καναλιού 4.3125 KHz. Ωστόσο, αυτό είναι δυνατόν να συμβεί λόγω ότι τα φέροντα είναι ορθογώνια του OFDM.

Συνήθως, λίγα κανάλια γύρω στο 31^{o}-32^{o} bin δε χρησιμοποιούνται ώστε να αποφευχθεί η παρεμβολή μεταξύ του upstream και του downstream δεξιά και αριστερά της συχνότητας 138kHz. Αυτά τα μη χρησιμοποιούμενα bins σχηματίζουν μια περιοχή ασφαλείας.

Η χρήση του DMT τρόπου διαμόρφωσης επιτρέπει στον εξοπλισμό του τηλεπικοινωνιακού συστήματος να επιλέγει μόνο εκείνα τα κανάλια που μπορούν να χρησιμοποιηθούν στη γραμμή επιτυγχάνοντας έτσι το βέλτιστο BER. Καθώς οι συνθήκες στη γραμμή αλλάζουν με το χρόνο, το modem μπορεί να αναδιατάσσει τα bits μέσα στα κανάλια, ενώ κάθε κανάλι γίνεται περισσότερο ή λιγότερο ικανό να μεταφέρει πληροφορία. Αν η δυνατότητα αναδιάταξης μεταξύ των καναλιών είναι απενεργοποιημένη, το modem πρέπει να ξανά ρυθμιστεί έτσι ώστε να προσαρμόζεται στις νέες συνθήκες των καναλιών μετάδοσης.

Για την κωδικοποίηση των bits μέσα σε κάθε κανάλι, χρησιμοποιείται μια μέθοδος διαμόρφωσης QAM ή PSK. Αυτές οι μέθοδοι διαμόρφωσης επιτρέπουν τη βελτίωση του SNR, χαμηλώνοντας τα επίπεδα του θορύβου και επιτρέποντας πιο αξιόπιστη μετάδοση. Το κέρδος πέρα απ' τα επίπεδα του θορύβου μπορεί να είναι από 0.5-1.5 dB και αυτές οι μικρές ποσότητες σημαίνουν μεγάλη διαφορά όταν στέλνουμε σήματα μέσα από γραμμές χαλκού μήκους 6km και πάνω.

Η απόδοση της γραμμής στη συχνότητα του κάθε καναλιού (bin) καθορίζει τον αριθμό των bits που μπορούν να μεταδοθούν μέσα από κάθε κανάλι. Όπως σε όλες τις γραμμές αυτό εξαρτάται από την απόσβεση και από το SNR.

Το SNR διαφέρει από κανάλι σε κανάλι και αυτό παίζει καθοριστικό ρόλο στην απόφαση για τον αριθμό των bits που μπορούν να κωδικοποιηθούν αξιόπιστα σε κάθε κανάλι. Γενικότερα, μπορούμε ότι για κάθε 3 dB διαθέσιμα πάνω απ' το επίπεδο θορύβου μέσα σε ένα κανάλι μπορούμε να κωδικοποιήσουμε αξιόπιστα 1 bit. Για παράδειγμα, ένα bin με SNR=18 dB μπορεί να μεταφέρει 6 bits. Με βάση τα παραπάνω, και το γεγονός ότι ο ελάχιστος αριθμός bits που κωδικοποιούνται σε κάθε κανάλι είναι 2, το SNR κάθε σήματος δεν πρέπει να είναι χαμηλότερο από 6 dB .

Η πληροφορία, από μια ροή bits που είναι αρχικά, μετατρέπεται σε πολλές παράλληλες ροές, καθεμία από τις οποίες αντιστοιχεί σε ένα από τα επιμέρους φέροντα. Κάθε ένα από αυτά με τη σειρά του διαμορφώνεται σύμφωνα με μία από τις ήδη γνωστές μεθόδους διαμόρφωσης ψηφιακού σήματος με χαμηλό ρυθμό μετάδοσης συμβόλου (symbol rate), ώστε όταν αποστέλλονται συνολικά όλα τα φέροντα, να διατηρείται ο αντίστοιχος ρυθμός συμβόλων που θα μπορούσαμε να επιτύχουμε με τη μετάδοση της πληροφορίας με ένα μόνο φέρον χρησιμοποιώντας το ίδιο εύρος ζώνης.[1]

1.2 Τεχνολογίες δικτύου πρόσβασης FTT x

Οι τεχνολογίες FTTx είναι δικτυακές τεχνολογίες και η παράμετρος x υπονοεί το βαθμό διείσδυσης της οπτικής ίνας στο δίκτυο. Οι τεχνολογίες αυτές χωρίζονται σε :

- ✓ Fibre To The Cabinet or Curb (FFTC – ίνα μέχρι μία υπαίθρια καμπίνα).
- ✓ Fibre To The Building (FTTB – ίνα μέχρι την εισαγωγή του κτιρίου).
- ✓ Fibre To The Home (FTTH - ίνα μέχρι το διαμέρισμα του συνδρομητή).

Υπάρχουν και διάφορες παραλλαγές των τεχνολογιών αυτών όπως η FTTN – ίνα μέχρι τη γειτονιά, FTTO – ίνα μέχρι το γραφείο, FTTP – ίνα μέχρι το χώρο του συνδρομητή, FTTU – ίνα μέχρι το χρήστη και FTTD – ίνα μέχρι τη θέση εργασίας. Παρακάτω θα γίνει ανάλυση για τις τρεις κύριες τεχνολογίες του δικτύου πρόσβασης τις FTTC, FTTB και FTTH.

1.2.1 Τεχνολογία Δικτύου Πρόσβασης FTTC

FTTC σημαίνει «ίνα μέχρι την καμπίνα», δηλαδή η οπτική ίνα χρησιμοποιείται μέχρι μία υπαίθρια καμπίνα το KV όπου είναι τοποθετημένη στο πεζοδρόμιο και έχει χώρο για εξυπηρέτηση συνδρομητών από 50 έως 500 μέσω του απερχόμενου δικτύου χαλκού. Για την ανάπτυξη ενός δικτύου FTTC απαιτείτε η εγκατάσταση υπαίθριου κατανεμητή για την εγκατάσταση ενεργού εξοπλισμού. Η FTTC τεχνολογία είναι παρόμοια με την FTTN όπου είναι μία αρχιτεκτονική δικτύου τηλεπικοινωνιών που βασίζεται σε καλώδια οπτικών ινών και εξυπηρετούν μία γειτονιά. Η FTTC παρέχει ευρυζωνικές υπηρεσίες και γρήγορο internet. Στο καλώδιο χρησιμοποιούνται κάποια πρωτόκολλα επικοινωνίας ή κάποια μορφή DSL τεχνολογίας και ανάλογα με το πόσο κοντά είναι ο πελάτης στον υπαίθριο κατανεμητή τα πρωτόκολλα δεδομένων ποικίλουν. Τέλος η FTTC τεχνολογία κοστίζει λιγότερο για την ανάπτυξή της.

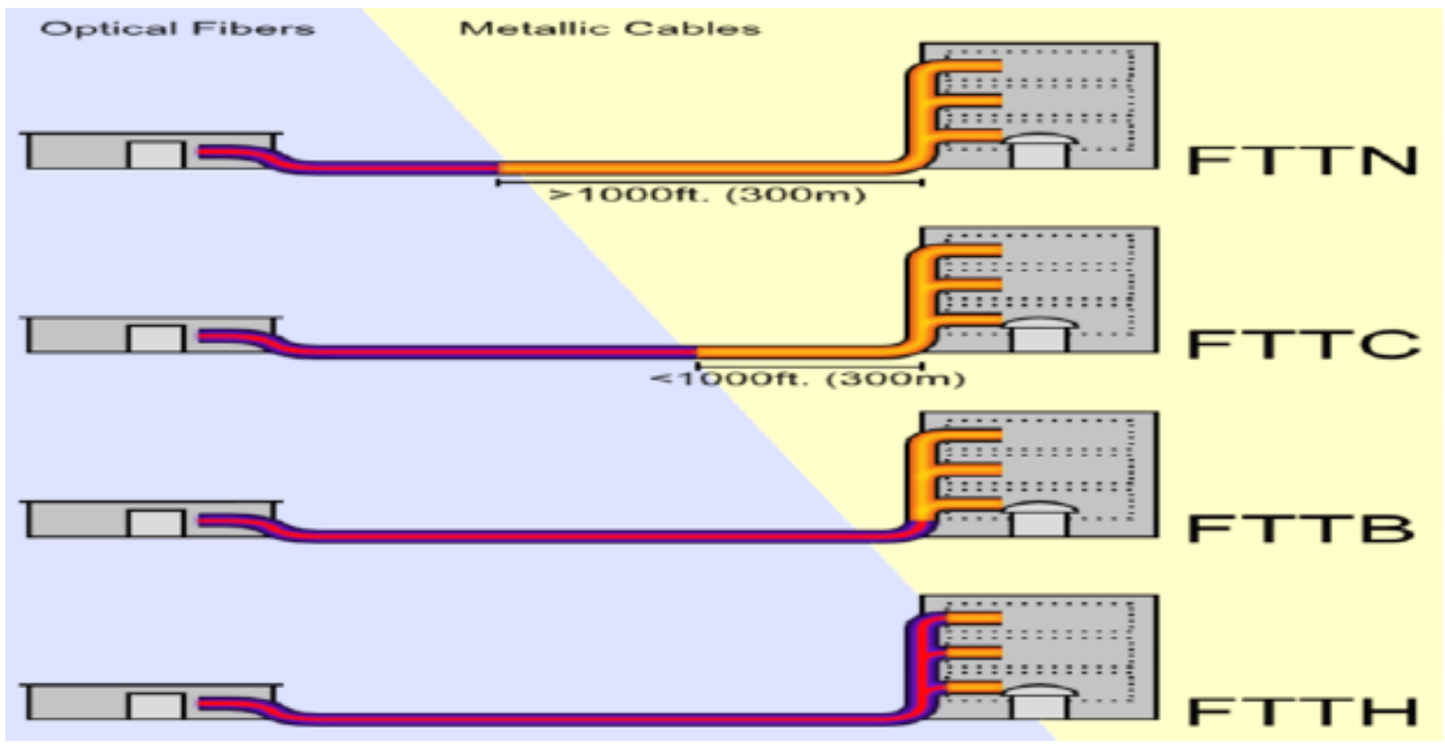
1.2.2 Τεχνολογία Δικτύου Πρόσβασης FTTB

Η τεχνολογία FTTB δηλαδή «ίνα μέχρι το κτίριο», είναι ένα μεταβατικό στάδιο στη διαδικασία σε ένα ολοκληρωμένο οπτικό δίκτυο πρόσβασης. Η τεχνολογία FTTB σημαίνει η οπτική ίνα που φτάνει μέχρι το κτίριο, δηλαδή σε ένα συγκρότημα διαμερισμάτων και όχι σε κάθε σπίτι ξεχωριστά. Για να υλοποιηθεί μία

τεχνολογία FTTB πρέπει κάθε κτίριο να συνδέεται μέσω καλωδίου οπτικών ινών στο αστικό κέντρο. Σε κάθε κτίριο χρησιμοποιούνται σημειακές και πολύ-σημειακές τοπολογίες οπού έχουν δύο ή τρία ζεύγη ινών. Οι οπτικές ίνες που εισέρχονται στο κτίριο τερματίζουν σε ένα μικρό κατανεμητή κοντά στο κουτί τερματισμού του χάλκινου συμβατικού δικτύου δηλαδή κοντά στον εσωτερικό χώρο του σπιτιού. Τέλος από άποψη κόστους η τεχνολογία FTTB έχει μεγαλύτερο σε σύγκριση με την FTTC. Υπάρχει μικρότερη χωρητικότητα του εξοπλισμού για την FTTB σε θύρες και έτσι αυξάνεται το κόστος ανά θύρα. Επίσης η παροχή υπηρεσιών DSL και η συντήρηση του εξοπλισμού γίνονται μέσα στο κτίριο και έτσι επιβαρύνεται το κόστος με μετακινήσεις του τεχνικού προσωπικού.

1.2.3 Τεχνολογία Δικτύου Πρόσβασης FTTH

Η τεχνολογία FTTH «ίνα μέχρι το σπίτι», είναι ο τελευταίος σταθμός στην εξελικτική διαδικασία των τεχνολογιών στο δίκτυο πρόσβασης. Η υλοποίηση της τεχνολογίας FTTH γίνεται σε κάθε διαμέρισμα ξεχωριστά εντός του κτιρίου και συνδέεται μέσω ενός ζεύγους οπτικών ινών. Σε αυτή την τεχνολογία χρησιμοποιούνται για τη σύνδεση τοπολογίες σημειακές και πολύ-σημειακές. Στο εσωτερικό του κτιρίου τερματίζει ένα οπτικό καλώδιο και αποτελεί το σημείο όπου ενώνει το εσωτερικό και το εξωτερικό δίκτυο. Ο ενεργός εξοπλισμός μιας τεχνολογίας FTTH είναι ένα οπτικό modem όπου παρέχει όλες τις διαθέσιμες τηλεπικοινωνιακές υπηρεσίες. Το κόστος είναι κυρίως δικτυακό ενώ το κόστος του ενεργού εξοπλισμού, δηλαδή το οπτικό modem επιβαρύνει τον συνδρομητή. Για αυτό σε σχέση με την τεχνολογία FTTC και FTTB το κόστος θεωρείται ελάχιστο για το λόγο ότι ο ενεργός εξοπλισμός δεν συντηρείται από την τηλεπικοινωνιακή εταιρεία. Τέλος όλες οι τεχνολογίες που αναλύθηκαν παραπάνω εξελίσσονται και στη παρακάτω εικόνα. [2]



1.3 Ασύμμετρες Παραλλαγές xDSL

Πρότυπο ADSL (ITU G.992.1)

Στις τηλεπικοινωνίες, το ITU G.992.1 (περισσότερο γνωστό ως G.DMT) είναι ένα πρότυπο ADSL της ITU που χρησιμοποιεί DMT (discrete multitone modulation). Το G.DMT full-rate ADSL διευρύνει το φάσμα που χρησιμοποιούν οι τηλεφωνικές γραμμές χαλκού, διανέμοντας υψηλής ταχύτητας μετάδοση δεδομένων με ταχύτητες άνω των 12 Mbit/s download και 1.3 Mbit/s upload. Το πρότυπο ITU G.992.1 αντιστοιχεί στην παραλλαγή ADSL και έχει περιγραφεί παραπάνω, στην ενότητα “τεχνικές λεπτομέρειες’’. Υπάρχουν 2 πρότυπα για το DMT ADSL - ANSI & DMT. Το πρότυπο ANSI T1.413 είναι το Βόρειο Αμερικανικό πρότυπο, ενώ το G.992.1 (DMT) είναι το ITU (United Nations Telecom committee) πρότυπο. Υπάρχουν διαφορές μεταξύ τους ως προς τον καθορισμό των καναλιών και επομένως η λάθος επιλογή προτύπου μπορεί να οδηγήσει σε λάθη “ευθυγράμμισης πλαισίου” κάθε 5 λεπτά. Τα λάθη διορθώνονται με κώδικες Reed-Solomon και επιπλέον με κωδικοποίηση Trellis και στις 2 άκρες της γραμμής.

Αυτή η παραλλαγή DSL είναι η πιο διαδεδομένη για χρήση τόσο από επιχειρήσεις όσο και από ιδιώτες. Είναι κατάλληλη για χρήστες που θέλουν γρήγορη πρόσβαση στο διαδίκτυο και γενικά για εφαρμογές όπου η ταχύτητα μεταφοράς δεδομένων από το δίκτυο προς το χρήστη είναι σημαντική. Η ADSL πλήρους ρυθμού καθορίζεται από το ITU-T Recommendation G.992.1 και το ANSI Standard T1.413-1998.

ADSL2

Το ITU G.992.3 είναι ένα πρότυπο της ITU το οποίο είναι περισσότερο γνωστό ως ADSL2. Η λειτουργία του επεκτείνει τις δυνατότητες του βασικού ADSL σε ταχύτητες που φτάνουν τα 12 Mbit/s download και 3.5 Mbit/s upload (με υποχρεωτικά κατώτερα όρια για τους ADSL2 πομπούς και δέκτες τα 8 Mbit/s download και 800 Kbit/s upload). Οι πραγματικές ταχύτητες ενδεχομένως να είναι μικρότερες, ανάλογα με την ποιότητα της γραμμής.

ADSL2+ ή ADSL2Plus

Το ITU G.992.5 είναι ένα πρότυπο της ITU το οποίο είναι περισσότερο γνωστό ως ADSL2+ ή ADSL2Plus. Η ADSL2+ επεκτείνει τις ιδιότητες του ADSL διπλασιάζοντας τον αριθμό των download bits. Οι ταχύτητες που μπορούν να επιτευχθούν είναι της τάξης των 24 Mbit/s download και 1 Mbit/s upload

ανάλογα με την απόσταση του συνδρομητή απ' τον πάροχο. Το ADSL2+ έχει τη δυνατότητα να διπλασιάζει τη περιοχή συχνοτήτων που χρησιμοποιούν οι τυπικές συνδέσεις ADSL, από 1.1 MHz σε 2.2 MHz. Αυτός ο διπλασιασμός έχει ως συνέπεια να διπλασιαστούν οι ταχύτητες download σε σχέση με το ADSL2 (πρόκειται για ταχύτητες άνω των 12 Mbit/s). Μία επιπλέον δυνατότητα του ADSL2+ είναι η χρήση περισσότερων ζευγών καλωδίων ταυτόχρονα. Αυτό σημαίνει πως αν για παράδειγμα 2 γραμμές στις οποίες μπορεί να αναπτυχθεί ταχύτητα 24 Mbit/s χρησιμοποιηθούν συνδυασμένα, το αποτέλεσμα θα ήταν να πετύχουμε διπλάσια ταχύτητα (48 Mbit/s).

Άλλες Ασύμμετρες παραλλαγές DSL

Οι ασύμμετρες παραλλαγές περιλαμβάνουν τις: ADSL, RADSL και VDSL. Οι τυποποιημένες μορφές της ADSL (Πρότυπα ITU G.992.1, G.992.2, και ANSI T1.413-Issue 2) χρησιμοποιούν όλες την ίδια τεχνολογία Discrete Multi Tone (DMT). Ακολούθως αναφέρονται οι παραλλαγές RADSL και VDSL.

RADSL

RADSL: (rate adaptive DSL – DSL προσαρμοζόμενου ρυθμού) Είναι μία non-standard έκδοση της ADSL. Αξίζει να σημειωθεί ότι το standard ADSL επιτρέπει στο ADSL μόντεμ να προσαρμόζει τις ταχύτητες μεταφοράς δεδομένων.

VDSL

Η VDSL (very high bit rate DSL – DSL πολύ υψηλού ρυθμού μεταφοράς bit) υποστηρίζει ταχύτητες μέχρι 50 Mb/s. Παρέχει πολύ γρήγορες συνδέσεις γιατί στις περισσότερες περιπτώσεις οι γραμμές VDSL εξυπηρετούνται από τοπικούς κατανεμητές, οι οποίοι συνδέονται με τις κεντρικές εγκαταστάσεις του παρόχου πρόσβασης μέσω οπτικών ινών. Είναι ιδιαίτερα χρήσιμο σε μεγάλους απομακρυσμένους πελάτες 'campus' όπως πανεπιστήμια και τεχνολογικά πάρκα. Το VDSL χρησιμοποιείται πλέον και για υπηρεσίες μετάδοσης βίντεο πάνω από υπάρχουσες τηλεφωνικές γραμμές. Το VDSL μπορεί επίσης να διαμορφωθεί σε συμμετρικό τρόπο λειτουργίας.

1.4 Συμμετρικές Παραλλαγές xDSL

Οι συμμετρικές παραλλαγές της DSL περιλαμβάνουν τα: SDSL, SHDSL, HDSL, HDSL-2 και IDSL. Οι ίσες ταχύτητες μεταφοράς δεδομένων από και προς το δίκτυο καθιστούν τη συμμετρική DSL ιδανική για πρόσβαση τοπικών δικτύων LANs (local area networks), βίντεο-συνδιάσκεψη και για τοποθεσίες οι οποίες φιλοξενούν τις δικές τους ιστοσελίδες.

SDSL

Η SDSL (symmetric DSL – συμμετρική DSL) είναι μια έκδοση που βασίζεται σε ιδιωτικές τεχνολογίες των κατασκευαστών και μπορεί να παρέχει ρυθμούς μεταφοράς δεδομένων από και προς τον χρήστη που κυμαίνονται από 128 kbps μέχρι 2.32 Mbps. Το SDSL είναι ένας γενικός όρος που καλύπτει έναν αριθμό από εφαρμογές συγκεκριμένες ανά κατασκευαστή, πάνω από ένα ζευγάρι καλωδίων χαλκού, που παρέχουν μεταβλητούς ρυθμούς μεταφοράς δεδομένων σε συμμετρική μορφή.

SHDSL

Η SHDSL είναι ένα βιομηχανικό πρότυπο αιχμής, συμμετρικής DSL. Ο εξοπλισμός SHDSL ακολουθεί την σύσταση G.991.2 της ITU, γνωστή επίσης ως G.SHDSL. Η SHDSL πετυχαίνει 20% καλύτερη πρόσβαση βρόχου σε σχέση με παλαιότερες εκδόσεις της συμμετρικής DSL, προκαλεί πολύ λιγότερη συνακρόαση σε άλλα συστήματα εκπομπής πάνω στο ίδιο καλώδιο και η λειτουργικότητα μεταξύ εξοπλισμού διάφορων κατασκευαστών διευκολύνεται από τη καθιέρωση αυτής της τεχνολογίας ως πρότυπο. Τα συστήματα SHDSL μπορεί να λειτουργούν σε διαφορετικούς ρυθμούς μεταφοράς δεδομένων από 192 kbps μέχρι 2.3 Mbps, μεγιστοποιώντας έτσι το ρυθμό μεταφοράς για κάθε χρήστη. Το G.SHDSL προδιαγράφει λειτουργία πάνω από ένα ζεύγος καλωδίων ή λειτουργία σε μακρύτερους βρόχους που μπορούν να χρησιμοποιηθούν με δύο ζεύγη. Για παράδειγμα, με δύο ζεύγη καλωδίου 1.2 Mbps μπορούν να σταλούν σε απόσταση πάνω από 6.000 μέτρα μέσω ενός καλωδίου. Η SHDSL είναι καταλληλότερη για εφαρμογές μεταφοράς μόνο δεδομένων οι οποίες χρειάζονται υψηλό ρυθμό μεταφοράς προς το δίκτυο. Ενώ η SHDSL δεν μεταφέρει φωνή όπως η ADSL, νέες τεχνικές μεταφοράς φωνής πάνω από DSL μπορεί να χρησιμοποιηθούν για να μεταφέρουν ψηφιοποιημένη φωνή και δεδομένα μέσω SHDSL. Η SHDSL αναπτύσσεται κυρίως για επιχειρήσεις.

HDSL

Η HDSL (high data rate DSL – DSL υψηλού ρυθμού μεταφοράς) παρέχει συμμετρική υπηρεσία σε ταχύτητες μέχρι 2.3 Mbps αμφίδρομα. Διαθέσιμη στα 1.5 ή 2.3 Mbps, αυτή η συμμετρική εφαρμογή σταθερού ρυθμού δεν παρέχει τυπική υπηρεσία τηλεφωνίας πάνω από την ίδια γραμμή και έχει ήδη γίνει πρότυπο από την ETSI και τον ITU (International Telecommunications Union). Χρησιμοποιεί ένα-δύο ή τρία ζεύγη συνεστραμμένου χαλκού.

HDSL2

Η HDSL2 (2nd generation HDSL – 2ης γενιας HDSL) εκδοχή παρέχει ταχύτητα 1.5 Mbps και προς τις δύο κατευθύνσεις, υποστηρίζει φωνή, δεδομένα και βίντεο και χρησιμοποιεί είτε ATM (asynchronous transfer mode) είτε frame relay πάνω από ένα ζεύγος χαλκού. Αυτό το πρότυπο του ANSI (American National Standards Institute) δίνει ένα σταθερό ρυθμό μεταφοράς δεδομένων 1.5 Mbps και προς τις δύο κατευθύνσεις. Η HDSL2 δεν παρέχει τυπική υπηρεσία τηλεφωνίας πάνω από το ίδιο ζεύγος καλωδίων. Η HSDL2 διαφέρει από την HDSL στο ότι η HDSL2 χρησιμοποιεί ένα ζεύγος καλωδίων για να μεταφέρει 1.5 Mbps ενώ η ANSI HDSL χρησιμοποιεί δύο ζεύγη.

PDSL

PDSL (Powerline Digital Subscriber Line), μια τεχνολογία που χρησιμοποιεί το δίκτυο του ηλεκτρικού ρεύματος.

IDSL

Η IDSL (integrated services digital network DSL – συμμετρικό δίκτυο ολοκληρωμένων υπηρεσιών DSL) είναι μια μορφή DSL που υποστηρίζει συμμετρικούς ρυθμούς μεταφοράς δεδομένων μέχρι 144 Kbps χρησιμοποιώντας τις υπάρχουσες τηλεφωνικές γραμμές. Η ιδιαιτερότητά του έγκειται στο ότι μπορεί να παρέχει υπηρεσίες μέσω ενός DLC (Digital Loop Carrier) σε μια απομακρυσμένη διάταξη η οποία τοποθετείται συχνά για να απλοποιήσει τη διανομή της καλωδίωσης από την τηλεφωνική εταιρία. Ενώ τα DLCs απλοποιούν τη διανομή παραδοσιακών υπηρεσιών φωνής που μπορούν να παρέχουν επίσης και η DSL. Η IDSL απευθύνεται σ’ αυτή την αγορά μαζί με την ADSL καθώς εφαρμόζονται απευθείας στα DLCs. Η IDSL διαφέρει από το συγγενές ISDN (integrated services digital network) στο ότι είναι μια υπηρεσία

συνεχώς διαθέσιμη, αλλά ικανή να χρησιμοποιεί τον ίδιο τερματικό προσαρμογέα ή μόντεμ που χρησιμοποιείται στο ISDN. [1]

Σύγκριση τεχνολογιών DSL

Τύπος	Μέγιστη Αποστολή Δεδομένων	Μέγιστη Λήψη Δεδομένων	Μέγιστη Απόσταση
VDSL	16 Mbps	52 Mbps	1,200 m
ADSL	3,5 Mbps	24Mbps	3,400 m
RADSL	1 Mbps	7 Mbps	5,500 m
SDSL	2,3 Mbps	2,3 Mbps	6,700 m
HDSL	1,54 Mbps	1,54 Mbps	9,650 m
IDSL	144 Kbps	144 Kbps	10,700 m

Κεφάλαιο 2: Τεχνολογία ADSL

Το Asymmetric Digital Subscriber Line (Ασύμμετρη Ψηφιακή Συνδρομητική Γραμμή) είναι μια μορφή DSL, δηλαδή μια τεχνολογία μετάδοσης δεδομένων που λειτουργεί πάνω σε παραδοσιακή τηλεφωνική γραμμή αλλά πετυχαίνει υψηλότερους ρυθμούς μεταφοράς από τα παραδοσιακά modem. Το απλό χάλκινο καλώδιο (γνωστό και ως τοπικός βρόχος, local loop) που συνδέει σχεδόν κάθε σπίτι με το τοπικό τηλεφωνικό κέντρο έχει πολύ περισσότερες δυνατότητες από την υποστήριξη της απλής τηλεφωνίας. Έτσι με χρήση ανώτερου τμήματος του εύρους ζώνης του βρόχου, εκείνου το οποίο μένει αναξιοποίητο από την κλασική τηλεφωνία (PSTN ή ISDN), επιτυγχάνονται υψηλές ταχύτητες μετάδοσης δεδομένων. Το γεγονός αυτό προσφέρει πλεονέκτημα ότι η παραδοσιακή τηλεφωνία και η μετάδοση δεδομένων μπορούν να λειτουργούν ταυτόχρονα και ανεξάρτητα η μία από την άλλη, εφόσον χρησιμοποιούν διαφορετικό φάσμα συχνοτήτων στην τηλεφωνική γραμμή. Ωστόσο οι συχνότητες που χρησιμοποιεί το ADSL εξασθενούν συντομότερα από αυτές της τηλεφωνίας, με αποτέλεσμα να μπορεί να λειτουργήσει σε αποστάσεις έως 5 Χλμ. από το τηλεφωνικό κέντρο. Επιπλέον όσο μεγαλώνει η απόσταση από το τηλεφωνικό κέντρο τόσο μειώνεται η ταχύτητα μετάδοσης δεδομένων που μπορεί να επιτευχθεί από το ADSL.

Χαρακτηριστικό του ADSL είναι το ότι οι ταχύτητες λήψης και αποστολής δεδομένων διαφέρουν, αυτό οφείλει και τη λέξη «ασύμμετρη» στο όνομά του. Η μέγιστη ταχύτητα που μπορεί να επιτύχει είναι τα 24 Mbps. Ένα επιπλέον χαρακτηριστικό είναι ότι η σύνδεση ADSL είναι μόνιμη και διαθέσιμη ανά πάσα στιγμή, δηλαδή δεν απαιτείται σύνδεση και αποσύνδεση από το δίκτυο όπως συμβαίνει με τις τηλεφωνικές κλήσεις. Εξελιγμένες εκδόσεις του ADSL είναι το ADSL2 και το ADSL2+, οι οποίες παρέχουν μεγαλύτερες ταχύτητες αξιοποιώντας διαφορετικά το εύρος ζώνης του καλωδίου. Η μέγιστη ταχύτητα που μπορεί να επιτύχει το ADSL2+ είναι τα 24/1 Mbps (ή τα 24/3,5 Mbps σε περίπτωση που υλοποιεί το πρότυπο ITU G.992.5) αλλά στην πράξη πολύ λίγοι χρήστες μπορούν να συνδεθούν σε αυτές τις ταχύτητες λόγω της απόστασής τους από το τηλεφωνικό κέντρο.

2.1 Λειτουργία του ADSL

Στις απλές τηλεφωνικές συνδέσεις με χάλκινο καλώδιο χρησιμοποιείται μόνο η περιοχή συχνοτήτων 0-4 KHz για τη μετάδοση της φωνής. Αυτό δίνει τη δυνατότητα να χρησιμοποιηθούν οι μεγαλύτερες συχνότητες για τη μετάδοση άλλων δεδομένων. Επειδή το εύρος είναι περιορισμένο και οι συνηθισμένοι οικιακοί χρήστες έχουν μεγαλύτερο όγκο στο κατέβασμα παρά στο ανέβασμα χρησιμοποιείται μεγαλύτερο

εύρος συχνοτήτων για την αποστολή από τον πάροχο προς τον τελικό χρήστη από το εύρος συχνοτήτων που χρησιμοποιείται για την αποστολή από τον τελικό χρήστη προς τον πάροχο.

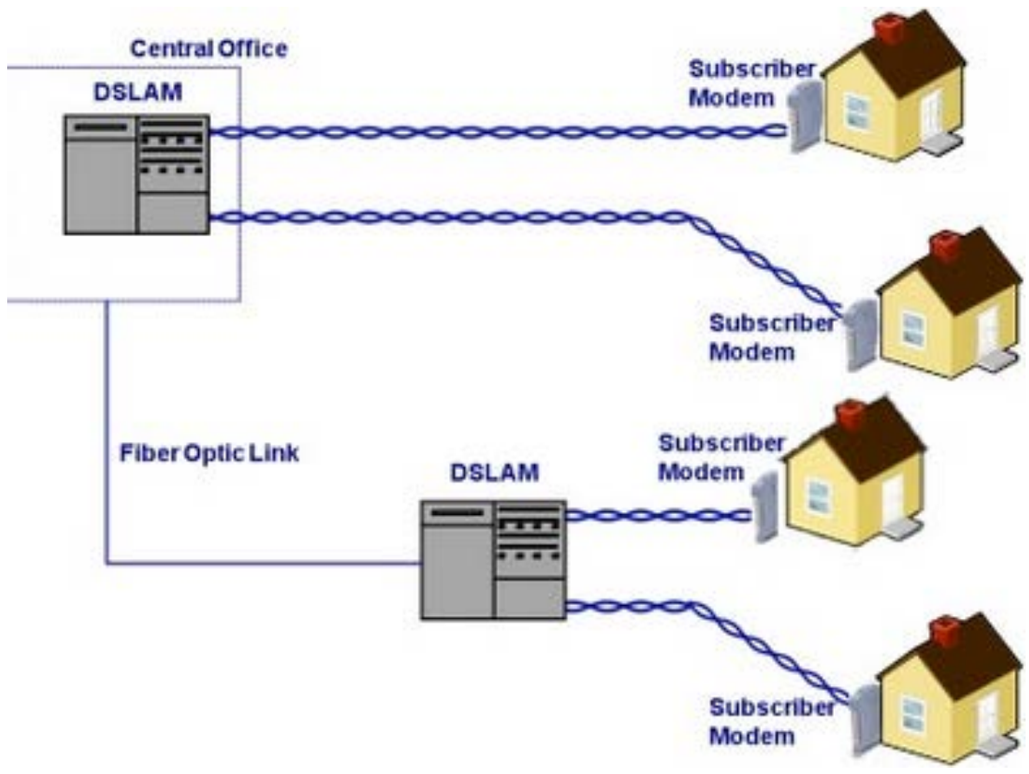
Αυτές οι συχνότητες υποδιαιρούνται σε ακόμα μικρότερες περιοχές των 4.3125 KHz. Συνήθως τα modem κατά την έναρξη της επικοινωνίας ελέγχουν ξεχωριστά κάθε τέτοια περιοχή για να καθορίσουν ποιες από αυτές τις περιοχές μπορούν να χρησιμοποιηθούν. Αυτή η σύνδεση χρησιμοποιείται για τη μεταφορά από τον τελικό χρήστη μέχρι το αντίστοιχο τηλεφωνικό κέντρο της περιοχής. Στο τηλεφωνικό κέντρο της περιοχής η μετάδοση των δεδομένων διακλαδώνεται μέσω των DSLAM και μεταβιβάζεται (συνήθως) με γραμμές πολύ μεγαλύτερης ταχύτητας στον αντίστοιχο πάροχο δεδομένων.

Για να συνδεθούμε στο Internet μέσω ADSL η τηλεφωνική γραμμή που ξεκινάει από το σπίτι μας καταλήγει με μια συσκευή δικτύου που ονομάζεται Digital Subscriber Line Access Multiplexer (DSLAM), είναι ο πολυπλέκτης / αποπολυπλέκτης των ψηφιακών συνδρομητικών γραμμών DSL (*Digital Subscriber Line*). Είναι μια συσκευή που τοποθετείται είτε στο Κέντρο Τηλεπικοινωνιακών Παρόχων, είτε σε καμπίνες στο δρόμο, είτε αντικαθιστούν τους Κατανεμητές καλωδίων (ΚΑ-ΦΑΟΥ που προέρχεται από τη γερμανική λέξη Kabelverteiler ή KV), είτε μέσα σε πολυκατοικίες.

2.2 Λειτουργία του DSLAM

Ο ρόλος του DSLAM συγκεντρώνει το traffic των δεδομένων αλλά και της φωνής από πολλαπλούς συνδρομητές και τα συνδυάζει σε ένα περίπλοκο "σήμα" με τη διαδικασία του multiplexing. Από εκεί και πέρα το σήμα από το DSLAM μεταφέρεται μέσω του πρωτοκόλλου Asynchronous Transfer Mode (PPP over ATM, PPPoA) ή Ethernet (PPP over Ethernet, PPPoE) στο δίκτυο του ISP, που μας δίνει πρόσβαση στο Internet.

Το DSLAM λειτουργεί όπως ένα απλό switch, στέλνοντας τα κατάλληλα δεδομένα στον κατάλληλο συνδρομητή, ταυτόχρονα όμως ένα DSLAM εμπεριέχει πολλαπλά κυκλώματα τύπου modem τα οποία αναφέρονται ως ports, για την ακρίβεια περιέχει ένα μοναδικό modem (port) για κάθε συνδρομητή που συνδέεται σε αυτό.



Κάθε κάρτα στο DSLAM τυπικά έχει 24 ports, και βεβαίως μπορούν να εγκατασταθούν πολλαπλές κάρτες για να καλύψουν ολόκληρες περιοχές. Στη παρακάτω εικόνα είναι ένα τυπικό DSLAM.

Όταν συνδέσουμε και ενεργοποιήσουμε το δρομολογητή το πρώτο πράγμα που κάνει είναι να συνδεθεί με το port του DSLAM που μας αντιστοιχεί. Αυτή η διαδικασία σύνδεσης μεταξύ των δύο modem ονομάζεται "συγχρονισμός", και συνήθως έχει ειδικό λαμπάκι με την ονομασία ADSL, line ή sync που δείχνει πως έγινε με επιτυχία.

2.3 Ταχύτητα και απόσταση

Το ADSL χρησιμοποιεί καλώδια του υπάρχοντος τηλεφωνικού δικτύου (Plain Old Telephone Service, POTS). Έτσι δεν χρειάζεται να περιμένουμε να στρώσουν νέα καλώδια ή οπτικές ίνες μέχρι το σπίτι μας. Για να μην μπλέκεται η μεταφορά δεδομένων του ADSL με την ομιλία στην απλή τηλεφωνική γραμμή, το ADSL χρησιμοποιεί υψηλότερες συχνότητες. Το πρόβλημα όμως είναι πως στα χάλκινα καλώδια του τηλεφωνικού δικτύου όσο μεγαλύτερο είναι το μήκος του καλωδίου τόσο μεγαλύτερη είναι η απώλεια (Attenuation) στις υψηλότερες συχνότητες.

Ως εκ τούτου, όσο μεγαλώνει η απόσταση ανάμεσα στο σπίτι μας και το DSLAM τόσο χαμηλότερο είναι το εύρος των συχνοτήτων που μπορεί να χρησιμοποιηθεί και κατά συνέπεια τόσο χαμηλότερη η μέγιστη

ταχύτητα συγχρονισμού. Ο παρακάτω πίνακας δείχνει στο περίπου τη μέγιστη ταχύτητα που μπορεί να επιτευχθεί σε ADSL2+ με βάση το μήκος του καλωδίου από το σπίτι μας μέχρι το DSLAM:

300 μέτρα =>25Mbps	2,1 χλμ =>16Mbps
600 μέτρα =>24Mbps	3,0 χλμ => 8Mbps
900 μέτρα =>23Mbps	3,5 χλμ -> 6Mbps
1,2 χλμ => 22Mbps	4,0 χλμ => 4Mbps
1,5 χλμ => 21Mbps	4,5 χλμ => 1,5Mbps
1,8 χλμ => 19Mbps	5,2 χλμ => 800Kbps

Συμπέρασμα ότι τα 2 χιλιόμετρα υπάρχουν και άλλοι παράγοντες στη γραμμή που επηρεάζουν την ταχύτητα γι' αυτό υπάρχει και η μεγαλύτερη πτώση. Αυτό λοιπόν σημαίνει πως αν το σπίτι μας μέχρι το DSLAM υπάρχουν 2 χιλιόμετρα καλωδίου, τα 24Mbps θα συγχρονίζονται περίπου στα 18Mbps.

2.4 Πλεονεκτήματα και μειονεκτήματα του ADSL

Πλεονεκτήματα

- Μεγαλύτερο εύρος ζώνης / μεγαλύτερη ταχύτητα download
- Πολύ γρήγορη σύνδεση
- Η σύνδεση του κάθε χρήστη είναι μοναδική και η ταχύτητα δεν επηρεάζεται σημαντικά από το πόσοι χρήστες είναι συνδεδεμένοι.
- Η ταχύτητα του ADSL είναι σταθερή

Μειονεκτήματα

- Τόσο αξιόπιστο όσο και οι τηλεφωνικές γραμμές. Για παράδειγμα μία κακοκαιρία μπορεί να δημιουργήσει προβλήματα
- Υψηλότερο κόστος για περιστασιακούς χρήστες
- Δεν είναι πάντα διαθέσιμο για όλους τους χρήστες
- Παρέχεται χαμηλότερη ταχύτητα για upload

2.5 Τεχνολογία VDSL

Το 2008 ο ΟΤΕ κάνει μια νέα επένδυση στην τεχνολογία VDSL όπου οι ταχύτητες να φτάνουν τα 30 Mbps / 2,5 Mbps download και τα 50 / 5Mbps upload. Μέχρι και το 2016 έχουν γίνει εγκαταστάσεις οπτικής ίνας σε πάρα πολλές περιοχές της χώρας.

Το VDSL (Very high-bitrate/high speed DSL) είναι το πιο γρήγορο ασύμμετρο DSL (υπάρχει και συμμετρικό DSL) και αποτελεί έναν συνδυασμό των χάλκινων καλωδίων του τοπικού βρόχου με την λεγόμενη οπτική ίνα στο πεζοδρόμιο που εξυπηρετεί μερικές δεκάδες σπίτια στη γειτονιά και θεωρείται μια σχετικά καλή μέθοδος για να περάσει κανείς από το ADSL στα δίκτυα επόμενης γενιάς. Το VDSL επιτρέπει την παροχή υπηρεσιών που απαιτούν υψηλό εύρος ζώνης, όπως η τηλεόραση υψηλής ανάλυσης, το ψηφιακό βίντεο ή η διασύνδεση απομακρυσμένων εταιρικών δικτύων.

Από το 2010 και μετά ο ΟΤΕ δημιουργεί ένα δικό του δίκτυο νέας γενιάς το NGA (New Generation Access) όπου παρέχει στους τελικούς χρήστες ευρυζωνικές υπηρεσίες πάρα πολύ υψηλών ταχυτήτων με βελτιωμένα ποιοτικά χαρακτηριστικά. Το δίκτυο του χαλκού που προϋπήρχε από το κέντρο του ΟΤΕ έως τα KV (καφάο) τώρα θα αντικατασταθεί από τις οπτικές ίνες. Το νέο αυτό δίκτυο είναι τύπου FTTC (Fiber to the Cabinet) όπου θα δίνει ταχύτητες για VDSL και VDSL2.

Τις χρονιές από το 2010 έως το 2012 ο ΟΤΕ φέρνει τις οπτικές ίνες πιο κοντά στα σπίτια των καταναλωτών. Από το δίκτυο του ΟΤΕ όπου οι οπτικές ίνες ξεπερνούσαν τα 35.000 χιλιόμετρα σε όλη την Ελλάδα και οι βασικοί κόμβοι συνδέονται μεταξύ τους με κυκλώματα των 10 Gbps τώρα δημιουργούνται υποδομές οπτικών ινών νέας γενιάς. Με τη διαδικασία αυτή ο ΟΤΕ προσφέρει ταχύτητες έως 50 Mbps.

2.6 Ταχύτητα και απόσταση

Η ταχύτητα που προσφέρει η VDSL τεχνολογία και η ιδανική απόσταση που θα πρέπει να έχει όπως οι άλλες ευρυζωνικές τεχνολογίες έτσι και στην VDSL η ταχύτητα στο τελικό χρήστη εξαρτάται από την απόσταση της σύνδεσης έως τον τοπικό βρόχο της εταιρίας που την παρέχει. Σύμφωνα με αυτή τη λογική οι μικρότερες αποστάσεις θα έχουν πιο μεγάλους ρυθμούς και οι μεγαλύτερες αποστάσεις θα έχουν χαμηλότερους ρυθμούς.

Για να λειτουργήσει μία VDSL τεχνολογία θα πρέπει το μήκος του βρόχου να είναι ιδανικά λιγότερο από 300 μέτρα και το πολύ έως 1200. Οι μέγιστες ταχύτητες που παρέχει το VDSL είναι συμμετρικά 26 Mbps και ασύμμετρα 52/12 Mbps όπου οι μέγιστες ταχύτητες επιτυγχάνονται μόνο για τις αποστάσεις έως 300

μέτρα. Η παροχής VDSL αντικαθιστούν τις παλιές γραμμές χαλκού από τις γραμμές οπτικών ινών. Αυτό έχει ως συνέπεια ένα τμήμα της γραμμής από τον τελικό χρήστη προς τον πάροχο να είναι με οπτικές ίνες και το άλλο χαλκός. Το πρόβλημα της απόστασης από το χρήστη μέχρι τον παροχέα λύνεται με τον εξής τρόπο. Το σήμα μεταφράζεται από αναλογικό που βρίσκεται στο χαλκό σε ψηφιακό όταν βρίσκεται στις οπτικές ίνες και το αντίστροφο. Αυτές οι μεταφράσεις γίνονται μέσω μιας συσκευής VDSL geteway – DSLAM όπου είναι τοποθετημένη στο σημείο που συναντιούνται τα καλώδια του χαλκού με τις οπτικές ίνες. Η συσκευή αυτή επίσης μετατρέπει το σήμα VDSL που περνάει από τα καλώδια χαλκού σε παλμούς φωτός για να μπορέσει να συνεχίσει τη διαδρομή του μέσα από τις οπτικές ίνες. Με τον ίδιο τρόπο ο πάροχος στέλνει μέσα από τις οπτικές ίνες το σήμα του έως το σημείο που ο χαλκούς συνδέετε με το χρήστη. Για να μην υπάρξει όμως πρόβλημα με απώλειες στην ταχύτητα θα πρέπει το μήκος του χαλκού να είναι μικρό. Έτσι και το μήκος του καλωδίου από το modem του τελικού χρήστη έως το KV (ΚΑΦΑΟ) που ο πάροχος έχει τις συσκευές VDSL gateway πρέπει να είναι το πολύ 1200 μέτρα.

Αναλυτικός Πίνακας Ρυθμού Μετάδοσης σε σχέση με την Απόσταση

Ταχύτητες (Mbps)	Απόσταση (m)
12,96-13,8	1500
25,92-27,6	1000
51,84-55,2	300

2.7 Στόχος της VDSL τεχνολογίας

Η νέα γενιά internet είναι το VDSL με στόχο να ολοκληρώσει «integrated» υπηρεσίες τηλεφωνίας και διασκέδασης από το σπίτι. Με τις αναβαθμισμένες δυνατότητες της νέας τεχνολογίας VDSL μπορούν να αλλάξουν την καθημερινή εμπειρία του διαδικτύου. Ο στόχος λοιπόν της VDSL τεχνολογίας είτε για ψυχαγωγικούς είτε για επαγγελματικούς λόγους είναι να πετύχει τις παρακάτω εφαρμογές :

- Εξαιρετικά γρήγορο downloading αρχείων
- Εξαιρετικά High Definition video – streaming χωρίς διακοπές
- Άμεσο uploading και sharing φωτογραφιών και video

- On line σύνδεση πολλών συσκευών ταυτόχρονα, χωρίς προβλήματα όπως laptops, smartphone, tablets κονσόλες παιχνιδιών, κλπ.
- Καλύτερη απόδοση στο online gaming.

2.8 Πλεονεκτήματα και Μειονεκτήματα της τεχνολογίας VDSL

Όπως όλες οι τεχνολογίες xDSL έτσι και στην τεχνολογία VDSL υπάρχουν κάποια πλεονεκτήματα και κάποια μειονεκτήματα. Το βασικότερο πλεονέκτημα της τεχνολογίας VDSL είναι πως παρέχει υψηλές ταχύτητες με αποτέλεσμα να προσφέρει νέες υπηρεσίες και εφαρμογές όπου έχουν μεγάλες απαιτήσεις. Δηλαδή το πρότυπο VDSL προσφέρει πακέτα ολοκληρωμένων υπηρεσιών όπως ψηφιακή τηλεόραση, ψηφιακό video, ψηφιακή τηλεφωνία και μεταφορά πληροφοριών όλα αυτά με χαμηλότερο κόστος. Όλες αυτές οι υπηρεσίες ελέγχονται από τον υπολογιστή γιατί η σύνδεση θα επιτρέπει ταυτόχρονη διαχείριση των πληροφοριών τους.

Όσον αφορά τα μειονεκτήματα της VDSL τεχνολογίας είναι τα εξής:

- Στην αρχή χρησιμοποίησαν κάποια φορτισμένα πηνία για να βελτιώσουν την ποιότητα του ήχου στις τηλεφωνικές γραμμές. Τώρα όμως τα συγκεκριμένα πηνία λειτουργούν σαν φίλτρα στις υψηλές συχνότητες.
- Η VDSL τεχνολογία εξαρτάται από το μήκος της γραμμής, αυτό έχει ως συνέπεια για να επιτύχει ρυθμούς υψηλούς, το μήκος της γραμμής θα πρέπει να είναι αρκετά μικρό. Αυτό είναι ένα σημαντικό μειονέκτημα.
- Η απόδοση της VDSL τεχνολογίας επηρεάζεται από το θόρυβο που προκαλείται από την παρουσία των Bridged taps (μια μέθοδος που χρησιμοποιείται από καλωδίωση για τηλεφωνικές γραμμές). Ένα ζεύγος καλωδίων που τοποθετείται σε διάφορες θέσεις τερματικών. Η κάθε τηλεφωνική εταιρία χρησιμοποιεί ένα τέτοιο ζεύγος σε κάθε συνδρομητή κοντά στις τελικές θέσεις. Σε αυτή την περίπτωση όταν υπάρχει βλάβη γίνεται αλλαγή ζεύγους.
- Η τεχνολογία VDSL δεν αποτελεί την καταλληλότερη λύση για μη αστικές ή αραιοκατοικημένες περιοχές. Ο λόγος είναι πως οι αποστάσεις των σπιτιών των καταναλωτών μέχρι τις υποδομές των τηλεπικοινωνιακών φορέων είναι πολύ μεγάλες.

- Τέλος οι γραμμές VDSL εξυπηρετούνται μόνο από τοπικούς κατανεμητές ανά γειτονιά, οι οποίοι συνδέονται με κεντρικές εγκαταστάσεις του φορέα πρόσβασης μέσω οπτικών ινών.

2.9 Διαφορές ADSL με VDSL

Η τεχνολογία VDSL είναι μία βελτιωμένη έκδοση της τεχνολογίας ADSL. Είναι δύο διαφορετικές τεχνολογίες στον τρόπο εφαρμογής τους γιατί δεν μπορούν να χρησιμοποιήσουν τον εξοπλισμό της μίας για την άλλη. Η σημαντικότερη διαφορά των δύο τεχνολογιών είναι η ταχύτητα. Η τεχνολογία ADSL μπορεί να φτάσει τη μέγιστη ταχύτητα download των 24 Mbps και upload του 1 Mbps ενώ η VDSL τεχνολογία μπορεί να φτάσει τη μέγιστη ταχύτητα download των 50 Mbps και upload των 12. Η τεχνολογία VDSL προσφέρει υψηλές ταχύτητες και έτσι είναι μία καλή τεχνολογία για την υποδοχή εφαρμογών υψηλού εύρους ζώνης που η τεχνολογία ADSL δεν έχει την ικανότητα να προσφέρει.

Άλλο ένα χαρακτηριστικό της τεχνολογίας VDSL είναι η χρησιμοποίηση 7 διαφορετικών ζωνών συχνοτήτων για να διαβιβάσει τα δεδομένα. Έτσι με τον τρόπο αυτό το VDSL modem έχει τη δυνατότητα να προσαρμόζεται στην κάθε ζώνη συχνοτήτων που χρησιμοποιεί για λήψη ή αποστολή δεδομένων. Ακόμη μία σημαντική διαφορά που λειτουργεί σαν μειονέκτημα για τη VDSL τεχνολογία είναι η απόσταση από το τηλεφωνικό κέντρο (μήκος τοπικού βρόχου). Σε μεγάλες αποστάσεις από το κέντρο του παρόχου η τεχνολογία VDSL υφίσταται εξασθένιση του σήματος περισσότερο από την ADSL τεχνολογία. Για το λόγο αυτό, η ADSL τεχνολογία χρησιμοποιείται πιο πολύ σε χρήστες που διαμένουν μακριά από το τηλεφωνικό κέντρο του παρόχου π.χ. ΟΤΕ. Οι περισσότεροι χρήστες της VDSL τεχνολογίας είναι εταιρείες που χρειάζονται μια δικτυακή σύνδεση υψηλού ρυθμού μετάδοσης.

Τέλος, λόγω των περιορισμών της VDSL τεχνολογίας και του υψηλού κόστους δεν είναι τόσο εμπορική όσο η ADSL τεχνολογία. Η VDSL δεν είναι πολύ διαδεδομένη στις περισσότερες χώρες, με εξαίρεση τη Νότια Κορέα και την Ιαπωνία. Η ADSL τεχνολογία χρησιμοποιείται ευρέως από τις περισσότερες χώρες που προσφέρουν ευρυζωνικές συνδέσεις στο διαδίκτυο.[2]

Κεφάλαιο 3: Δρομολογητής (router)

Ο δρομολογητής (router) είναι μια ηλεκτρονική συσκευή η οποία αναλαμβάνει την προώθηση πακέτων δεδομένων μεταξύ ενός ή περισσοτέρων διακομιστών και πελατών, με την βοήθεια και άλλων δρομολογητών κατά μήκος πολλαπλών δικτύων (δρομολόγηση). Η δρομολόγηση, δηλαδή η διαδικασία μεταφοράς δεδομένων από ένα κόμβο του δικτύου σε έναν άλλο αποτελεί βασική λειτουργία του επιπέδου δικτύου. Η δρομολόγηση πραγματοποιείται με βάση διάφορα κριτήρια και τελικώς επιλέγεται η βέλτιστη ανάμεσα σε διάφορες πιθανές διαδρομές.

Κάθε δρομολογητής χρησιμοποιεί ένα ή περισσότερα πρωτόκολλα δρομολόγησης. Με βάση αυτά τα πρωτόκολλα ο δρομολογητής καθορίζει ποιος ή ποιοι δρομολογητές είναι οι επόμενοι καταλληλότεροι αποδέκτες των πακέτων δεδομένων κάθε χρονική στιγμή και δρομολογεί τα πακέτα δεδομένων προς αυτούς.

Ορισμένα πολύ γνωστά πρωτόκολλα δρομολόγησης είναι τα:

- RIP
- OSPF
- BGP
- IS-IS

Παρόλο που μεταξύ τους διαφέρουν, όλοι οι δρομολογητές έχουν κάποια κοινά χαρακτηριστικά:

- CPU (Κεντρική Μονάδα Επεξεργασίας): ένας ή περισσότεροι επεξεργαστές υπεύθυνοι για την εκτέλεση εντολών του λειτουργικού συστήματος, λειτουργιών αρχικοποίησης, δρομολόγησης πακέτων και ελέγχου δικτυακής διασύνδεσης.[3]

- Η RAM (Μνήμη τυχαίας προσπέλασης) που διατηρεί τους πίνακες δρομολόγησης (routing tables) και χάνει τα δεδομένα της κάθε φορά που κλείνει ή κάνει επανεκκίνηση ο router.

- Η NVRAM (Nom Volatile RAM) που κρατάει ένα αντίγραφο της διαμόρφωσης του δρομολογητή ώστε να μην χρειάζεται εκ νέου ρύθμιση κάθε φορά που κάνουμε επανεκκίνηση.

- Flash μνήμη για την αποθήκευση του λειτουργικού συστήματος.

- ROM (Μνήμη μόνο για ανάγνωση) χρησιμοποιείται κατά την εκκίνηση του δρομολογητή για να του δώσει τις πρώτες εντολές που θα εκτελεστούν. Τα δεδομένα που περιέχονται στην μνήμη ROM είναι αμετάβλητα, δεν μπορούν να αλλαχθούν.

3.1 Δρομολόγηση

Η δρομολόγηση κατευθύνει και προωθεί, τα λογικά διευθυνσιοδοτημένα πακέτα από την πηγή τους προς τον προορισμό τους μέσω ενδιάμεσων κόμβων (που λέγονται δρομολογητές). Η διαδικασία της δρομολόγησης κατευθύνει προωθώντας τα δεδομένα με βάση πίνακες δρομολόγησης που βρίσκονται στους δρομολογητές οι οποίοι διατηρούν μια εγγραφή για την καλύτερη διαδρομή για κάθε κατεύθυνση στο δίκτυο. Κατά συνέπεια η κατασκευή των πινάκων δρομολόγησης είναι πολύ σημαντική για αποτελεσματική δρομολόγηση.

Τα περισσότερα δημόσια τηλεφωνικά δίκτυα μεταγωγής (PSTN) χρησιμοποιούν προ-υπολογισμένους πίνακες δρομολόγησης, με εφεδρικές διαδρομές ώστε αν μπλοκαριστεί η πιο σύντομη διαδρομή να χρησιμοποιήσουν την πρώτη εφεδρική. Η δυναμική δρομολόγηση προσπαθεί να λύσει αυτό το πρόβλημα κατασκευάζοντας τους πίνακες δρομολόγησης αυτόματα, βασιζόμενη στις πληροφορίες που μεταφέρονται από τα πρωτόκολλα δρομολόγησης, και αφήνει το δίκτυο να ενεργεί σχεδόν αυτόνομα στο να αποφεύγει βλάβες και μπλοκαρίσματα.

Η δυναμική δρομολόγηση κυριαρχεί στο διαδίκτυο όμως η ρύθμιση των πρωτοκόλλων δρομολόγησης απαιτεί ικανότητες που δεν θα πρέπει κάποιος να θεωρεί δεδομένες χωρίς ειδική εκπαίδευση δεδομένου ότι η τεχνολογία των δικτύων δεν έχει εξελιχθεί μέχρι το σημείο της πλήρους αυτοματοποίησης.

Τα δίκτυα μεταγωγής πακέτων (packet-switched networks) όπως το διαδίκτυο, χωρίζουν τα δεδομένα σε πακέτα που το καθένα περιέχει πληροφορίες για τον προορισμό του και τα δρομολογούν ξεχωριστά. Τα δίκτυα μεταγωγής κυκλώματος όπως τα τηλεφωνικά δίκτυα εκτελούν και αυτά δρομολόγηση με σκοπό να βρίσκουν διαδρομές για κυκλώματα (όπως τηλεφωνικές κλήσεις) πάνω από τις οποίες να μπορούν να στείλουν μεγάλες ποσότητες δεδομένων χωρίς να επαναλαμβάνουν συνεχώς την διεύθυνση του προορισμού.

Το υλικό που χρησιμοποιείται στα δίκτυα περιλαμβάνει συγκεντρωτές, μεταγωγείς, και δρομολογητές.[4]

3.1.1 Δρομολόγηση και μεταγωγή

Η λειτουργία που επιτελεί ένα δίκτυο είναι η σύνδεση υπολογιστών και περιφερειακών συσκευών χρησιμοποιώντας δύο τύπους δικτυακού εξοπλισμού, τους μεταγωγείς και τους δρομολογητές. Και οι δύο αυτές συσκευές επιτρέπουν στις τερματικές συσκευές που είναι συνδεδεμένες στο δίκτυό τους την επικοινωνία μεταξύ τους καθώς και με άλλα δίκτυα. Παρόλο που μοιάζουν αρκετά ως συσκευές οι μεταγωγείς και οι δρομολογητές εκτελούν διαφορετικές λειτουργίες σε ένα δίκτυο.

Οι μεταγωγείς χρησιμοποιούνται για τη σύνδεση πολλών συσκευών στο ίδιο τοπικό δίκτυο εντός ενός κτιρίου ή ενός ευρύτερου χώρου (π.χ. πανεπιστήμιο). Για παράδειγμα, ένας μεταγωγέας μπορεί να συνδέει τους υπολογιστές, τους εκτυπωτές και τους διακομιστές, δημιουργώντας ένα δίκτυο κοινόχρηστων πόρων. Ο μεταγωγέας εκτελεί χρέη ελεγκτή, επιτρέποντας στις διάφορες συσκευές την κοινή χρήση πληροφοριών και την επικοινωνία μεταξύ τους. Μέσω της κοινής χρήσης πληροφοριών και της κατανομής πόρων, οι μεταγωγείς μπορούν να συμβάλλουν στην εξοικονόμηση πόρων και στην αύξηση της παραγωγικότητας.

Υπάρχουν δύο βασικοί τύποι μεταγωγέων: διαχειριζόμενοι (managed) και μη (unmanaged).

- Ένας μη διαχειριζόμενος μεταγωγέας χρησιμοποιείται απευθείας όπως παραδίδεται από τον κατασκευαστή και δεν επιτρέπει καμία τροποποίηση. Οι εξοπλισμοί οικιακής δικτύωσης έχουν συνήθως μη διαχειριζόμενους μεταγωγείς.
- Ένας διαχειριζόμενος μεταγωγέας παρέχει δυνατότητα πρόσβασης και αλλαγής ρυθμίσεων. Αυτό προσφέρει μεγαλύτερη ευελιξία, καθώς ο μεταγωγέας μπορεί να παρακολουθείται και να προσαρμόζεται τοπικά ή απομακρυσμένα επιτρέποντας τον έλεγχο της κυκλοφορίας και της πρόσβασης χρηστών στο δίκτυο.

Οι δρομολογητές χρησιμοποιούνται για τη σύνδεση πολλών δικτύων. Για παράδειγμα, μπορείτε να χρησιμοποιήσετε ένα δρομολογητή για να συνδέσετε τους υπολογιστές του δικτύου σας στο διαδίκτυο και έτσι να επιτρέψετε την κοινή χρήση μιας σύνδεσης Internet από πολλούς χρήστες. Συνδέουν τους οικιακούς και εταιρικούς χρήστες με το διαδίκτυο, συμβάλλουν στην προστασία των πληροφοριών από απειλές ασφαλείας και μπορούν ακόμα και να αποφασίσουν ποιοι υπολογιστές θα αποκτούν προτεραιότητα έναντι άλλων.

3.2 Είδη δρομολόγησης-Δυναμική δρομολόγηση

Η δρομολόγηση προσαρμόζεται δυναμικά στις αλλαγές στην τοπολογία του δικτύου, μέσω της αποστολής των routing update μηνυμάτων. Δηλαδή, οι δρομολογητές επικοινωνούν μεταξύ τους και πρέπει να ενημερώνουν ο ένας τον άλλο για την περιοχή ευθύνης τους, δηλαδή ποιό δίκτυο χειρίζεται ο ένας και ποιό ο άλλος.

Αν μια συγκεκριμένη διαδρομή γίνει μη διαθέσιμη, οι υπάρχοντες κόμβοι πρέπει να αποφασίσουν μια εναλλακτική διαδρομή που θα χρησιμοποιήσουν να στείλουν τα δεδομένα στον προορισμό τους. Συχνά το πετυχαίνουν αυτό μέσω της χρήσης πρωτοκόλλων δρομολόγησης τα οποία χρησιμοποιούν μία από τις δυο ευρείες κλάσεις αλγορίθμων δρομολόγησης:

- ✓ αλγορίθμους διανύσματος απόστασης
- ✓ αλγορίθμους κατάστασης συνδέσμων

οι οποίες περιέχουν σχεδόν τον κάθε αλγόριθμο δρομολόγησης που χρησιμοποιείται σήμερα στο διαδίκτυο. Η δυναμική δρομολόγηση είναι σχεδόν επιβεβλημένη σε μεγάλα δίκτυα.

Εκτός της δυναμική έχουμε και την άμεση/έμμεση δρομολόγηση, άμεση έχουμε όταν κάποιος κόμβος στέλνει IP πακέτα δεδομένων σε κόμβο του ίδιου υπο-δικτύου (π.χ. του ίδιου Ethernet segment). Τότε με κατάλληλα μηνύματα (ARP) μπορεί να πληροφορηθεί την φυσική διεύθυνση του άλλου κόμβου, να τοποθετήσει το datagram σε ένα MAC πλαίσιο με τη φυσική διεύθυνση αυτή, και να το μεταδώσει. Στην έμμεση δρομολόγηση (indirect), κάποιος κόμβος στέλνει IP πακέτα δεδομένων σε κόμβο διαφορετικού δικτύου χρησιμοποιώντας κατάλληλους ενδιάμεσους κόμβους, οι οποίοι είναι οι δρομολογητές. Όταν κάποιος κόμβος αναγνωρίσει ότι ένα IP datagram κατευθύνεται σε κόμβο διαφορετικού δικτύου, τότε μέσα από ένα μικρό πίνακα δρομολόγησης που διαθέτει επιλέγει τον κατάλληλο δρομολογητή. Με ένα ARP μήνυμα μαθαίνει την φυσική διεύθυνση του δρομολογητή αυτού και του στέλνει το IP datagram με ένα MAC πλαίσιο. Σε περίπτωση που ο δρομολογητής είναι συνδεδεμένος στο δίκτυο προορισμού τότε πληροφορείται με παρόμοιο τρόπο την φυσική διεύθυνση του κόμβου προορισμού και του στέλνει το IP datagram. Σε αντίθετη περίπτωση, βρίσκει ένα δεύτερο δρομολογητή στην φυσική διεύθυνση του οποίου στέλνεται το datagram, και με την σειρά του θα εκτελέσει τις ίδιες λειτουργίες. Οι δρομολογητές παίρνουν αποφάσεις με βάση το δίκτυο προορισμού και όχι με βάση τον σταθμό προορισμού. Αυτό σημαίνει ότι

εξετάζουν αν είναι συνδεδεμένοι με δίκτυο το οποίο έχει το ίδιο netid με το κόμβο προορισμού, διαφορετικά στέλνουν το datagram σε άλλο δρομολογητή, ο οποίος θα καθορίσει τη συνέχεια της διαδρομής.

3.2.1 Στατική

Η διαμόρφωση του δρομολογητή λέγεται στατική δρομολόγηση (static routing).

- Πλεονέκτημα της στατικής δρομολόγησης είναι ότι είναι το πιο απλό είδος δρομολόγησης και δεν επιβαρύνει τον δρομολογητή και τις διεπαφές του.
- Μειονέκτημα της μεθόδου είναι ότι αν συμβεί κάποια μεγάλη αλλαγή στο δίκτυο τότε πρέπει ο διαχειριστής του δρομολογητή να κάνει ο ίδιος την αλλαγή στη δρομολόγηση.

Η στατική δρομολόγηση περιγράφεται στη διαμόρφωση του δρομολογητή. Κάθε εγγραφή στατικής δρομολόγησης περιγράφει ένα υποδίκτυο και οι διεπαφές από το οποίο θα προωθηθεί ένα πακέτο για να φτάσει στο συγκεκριμένο υποδίκτυο. Μπορεί για ένα υποδίκτυο να έχουμε δύο εγγραφές δρομολόγησης στη διαμόρφωση του δρομολογητή. Σε αυτή την περίπτωση χρησιμοποιείται ή έννοια του βάρους (metric) το οποίο είναι ένας αριθμός από το 0 έως το 255. Ορίζεται δηλαδή ένα είδος ποιότητας της διαδρομής με την ποιότητα της διαδρομής να αυξάνεται όσο ο αριθμός μικραίνει. Μια διαδρομή μπορεί να έχει βάρος από 0 (άριστη) έως 254 (χείριστη) ενώ βάρος 255 έχει μια διαδρομή όταν (π.χ. λόγω βλάβης της γραμμής) δεν λειτουργεί. Όταν μια διαδρομή έχει βάρος 255, τότε κανένα πακέτο δεν θα δρομολογείται πάνω από αυτήν (αφού η συγκεκριμένη είναι "κομμένη").

3.3 Διεύθυνση και εκδόσεις της IP

Μία διεύθυνση IP είναι ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές για τη μεταξύ τους αναγνώριση και συνεννόηση σε ένα δίκτυο υπολογιστών που χρησιμοποιεί το Internet Protocol. Κάθε συσκευή που ανήκει στο δίκτυο όπως οι δρομολογητές, οι υπολογιστές, οι εκτυπωτές, οι μηχανές για fax μέσω Internet, και ορισμένα τηλέφωνα πρέπει να έχει τη δική της μοναδική διεύθυνση. Μία διεύθυνση IP μπορεί να θεωρηθεί το αντίστοιχο μιας διεύθυνσης κατοικίας ή ενός αριθμού τηλεφώνου για έναν υπολογιστή ή άλλη συσκευή δικτύου στο διαδίκτυο. Όπως κάθε διεύθυνση κατοικίας και αριθμός

τηλεφώνου αντιστοιχούν σε ένα και μοναδικό κτίριο ή τηλέφωνο, μια IP διεύθυνση χρησιμοποιείται για τη μοναδική αναγνώριση ενός υπολογιστή ή άλλης συσκευής που συνδέεται στο δίκτυο.

Μια διεύθυνση IP μπορεί να "μοιράζεται" σε πολλές συσκευές-πελάτες είτε επειδή αυτές είναι μέρος ενός shared hosting web server environment, είτε λόγω ενός proxy server (π.χ. ενός Παροχέα Υπηρεσιών διαδικτύου (ISP) ή μιας υπηρεσίας για εξασφάλιση ανωνυμίας) που λειτουργούν ως μεσολαβητές. Στην τελευταία περίπτωση (για χρήση διακομιστή μεσολάβησης) η πραγματική διεύθυνση IP μπορεί να αποκρύπτεται από το διακομιστή που δέχεται αίτηση. Η αναλογία στα τηλεφωνικά συστήματα θα ήταν η χρήση διεθνών ή τοπικών αριθμών κλήσης (proxy) και επεκτάσεων (shared).

Το Πρωτόκολλο Διαδικτύου έχει δύο κύριες εκδόσεις σε χρήση, την IPv4 και την IPv6. Κάθε έκδοση έχει το δικό της ορισμό για την διεύθυνση IP. Λόγω της επικράτησής της, ο όρος «διεύθυνση IP» τυπικά αναφέρεται σε εκείνες που ορίζονται στο IPv4.

Οι διευθύνσεις IP που ορίζονται είναι αριθμοί της μορφής xxx.xxx.xxx.xxx (IPv4), όπου xxx ένας αριθμός από 0 εώς 255 ή xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.xxx.xxx.xxx.xxx (IPv6). Σε ένα δίκτυο υπολογιστών όπως είναι και το Διαδίκτυο ο κάθε υπολογιστής στέλνει ορισμένα πακέτα πληροφοριών, τα οποία ονομάζονται IP Packets.

3.3.1 Διεύθυνση IPv4

Το IPv4 χρησιμοποιεί διευθύνσεις των 32-bit (4 byte), που περιορίζουν το πλήθος διευθύνσεων σε 4.294.967.296 (232) πιθανές μοναδικές διευθύνσεις. Πολλές παρακρατούνται για ειδικούς λόγους, όπως για χρήση σε ιδιωτικά δίκτυα (18 εκατομμύρια) ή διευθύνσεις πολυδιανομής (1 εκατομμύριο). Κατά αυτόν τον τρόπο, μειώνεται ο αριθμός που μπορεί να διατεθεί για δημόσιες διευθύνσεις διαδικτύου και καθώς ο αριθμός διαθέσιμων διευθύνσεων καταναλώνεται, η έλλειψη εμφανίζεται να είναι αναπόφευκτη μακροπρόθεσμα. Αυτός ο περιορισμός έχει συντελέσει στη στροφή προς το IPv6, που είναι αυτήν την περίοδο σε αρχικά στάδια επέκτασης και ο μόνος υποψήφιος αντικαταστάτης του IPv4.

3.3.2 Διεύθυνση IPv6

Πρίν την έκδοση της IPv6 ένα πειραματικό πρωτόκολλο ήταν το IPv5**.** Σύμφωνα με τις πρότυπες συμβάσεις για κάθε διανομή UNIX, όλες οι περιττά αριθμημένες εκδόσεις θεωρούνται πειραματικές. Αυτή η έκδοση δεν προορίστηκε ποτέ για υλοποίηση και εφαρμογή και το πρωτόκολλο εγκαταλείφθηκε. Το RSVP το έχει αντικαταστήσει ως έναν ορισμένο βαθμό.

Η διεύθυνση της Έκδοσης 6 του Πρωτοκόλλου, που στο εξής θα την αναφέρουμε σαν διεύθυνση IPv6 είναι μία αριθμητική ετικέτα η οποία χρησιμοποιείται για τον προσδιορισμό της διασύνδεσης δικτύου (network interface) ενός υπολογιστή ή άλλου κόμβου δικτύου (network node) που συμμετέχει σε ένα δίκτυο υπολογιστών IPv6. Ο σκοπός μίας διεύθυνσης IP είναι να προσδιορίζει με μοναδικό τρόπο την δικτυακή διασύνδεση μιας δικτυακής συσκευής, εντοπίζοντας τη θέση της στο δίκτυο, δίνοντας έτσι τη δυνατότητα της δρομολόγησης των πακέτων μεταξύ τους. Για να είναι δυνατή η δρομολόγηση πακέτων ανάμεσα σε δύο δικτυακές συσκευές, στις επικεφαλίδες των πακέτων οι IP είναι ενσωματωμένες οι διευθύνσεις προέλευσης και προορισμού. Το IPv6 είναι ο διάδοχος της Έκδοσης 4 του Πρωτοκόλλου του Internet (του IPv4). Στο IPv4 οι διευθύνσεις IP ήταν 32bit, ενώ στο IPv6 είναι 128 bit. Έτσι η περιοχή διευθύνσεων του IPv6 είναι πάρα πολύ μεγαλύτερη από την περιοχή διευθύνσεων του IPv4.

Τάξεις διευθύνσεων IPv6

Οι διευθύνσεις IPv6, ταξινομούνται με βάση τις μεθόδους διευθυνσιοδότησης και δρομολόγησης που συνηθίζονται στα δίκτυα. Έτσι έχουμε διευθύνσεις **unicast**, διευθύνσεις **anycast** και διευθύνσεις **multicast**.

Μία διεύθυνση **unicast** προσδιορίζει μία συγκεκριμένη διασύνδεση δικτύου. Το πρωτόκολλο Internet παραδίδει τα πακέτα που στέλνονται σε μία unicast διεύθυνση, μόνο στη συγκεκριμένη διεύθυνση δικτύου.

Μία διεύθυνση **anycast** αποδίδεται σε μία ομάδα διασυνδέσεων, που συνήθως ανήκουν σε διαφορετικούς κόμβους. Ένα πακέτο που στέλνεται σε μία διεύθυνση anycast παραδίδεται μόνο σε μία από τις διασυνδέσεις της ομάδας, τυπικά στην πλησιέστερη, σύμφωνα με τον ορισμό της απόστασης που χρησιμοποιεί το πρωτόκολλο δρομολόγησης.

Μία διεύθυνση **multicast** χρησιμοποιείται από πολλές διασυνδέσεις. Αυτές παίρνουν τη multicast διεύθυνση συμμετέχοντας σε πρωτόκολλα διανομής διευθύνσεων multicast ανάμεσα στους δρομολογητές του δικτύου. Ένα πακέτο το οποίο στέλνεται σε μία διεύθυνση multicast, διανέμεται σε όλες τις διασυνδέσεις που συμετέχουν στην αντίστοιχη multicast ομάδα.

✓ Το πρωτόκολλο IPv6 δεν υλοποιεί διευθύνσεις τύπου broadcast.

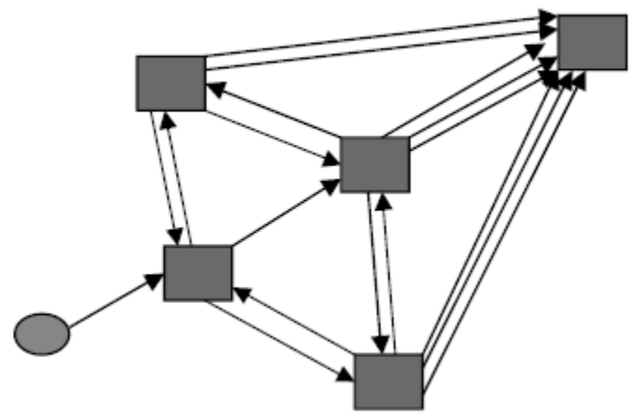
3.4 Τεχνικές δρομολόγησης

Τα multicast πρωτόκολλα δρομολόγησης χρησιμοποιούν δύο τεχνικές για την προώθηση των πακέτων:

1. Flooding
2. Reverse Path Forwarding

Flooding

Στην τεχνική Flooding ο δρομολογητής δεν απαιτείται να έχει καμιά πληροφορία δρομολόγησης. Ένα πακέτο που φτάνει στις διεπαφές προωθείται σε όλα τις υπόλοιπες διεπαφές εκτός αυτού από το οποίο ήρθε. Η τελευταία ενέργεια μπορεί να οδηγήσει σε loops δρομολόγηση (εικόνα 1) . Για να περιοριστεί το πρόβλημα των routing loops, ορίζεται ένας αριθμός σε hops τον οποίο όταν υπερβεί το πακέτο, αυτό απορρίπτεται.

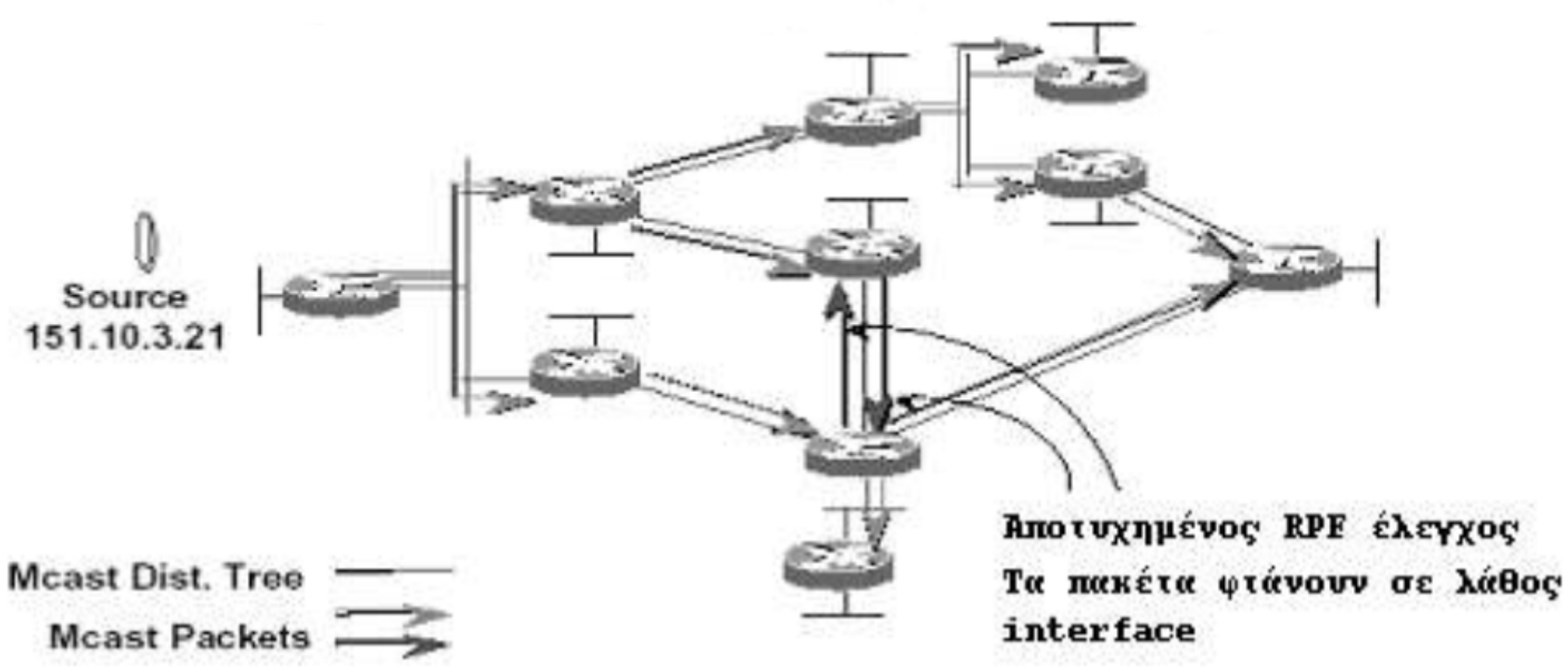


εικόνα 1

Η τεχνική flooding έχει τα εξής πλεονεκτήματα: είναι εύκολη στη διαχείριση και οι δρομολογητές δεν απαιτείται να έχουν πίνακες δρομολόγησης. Μειονεκτήματα του flooding αποτελούν: το γεγονός ότι αρκετές φορές δημιουργούνται routing loops και επομένως η συμφόρηση που δημιουργείται στο δίκτυο είναι μεγάλη.

Reverse Path Forwarding (RPF)

Το Reverse Path Forwarding (RPF) είναι μια δεύτερη τεχνική που χρησιμοποιούν οι δρομολογητές για να προωθήσουν multicast πακέτα. Με αυτή την τεχνική, όταν ένα πακέτο φτάσει σε μία από τις διεπαφές κάποιου δρομολογητή, εκείνος πραγματοποιεί ένα RPF έλεγχο για να διαπιστώσει αν το πακέτο έφτασε στο σωστό interface. Κατά τον έλεγχο αυτό εξετάζεται αν ο δρομολογητής θα χρησιμοποιούσε τις διεπαφές για να προωθήσει unicast πληροφορία στην πηγή, δηλαδή αν θα επέλεγε την αντίθετη διαδρομή (Reverse Path). Αν ο έλεγχος γίνει με επιτυχία, δηλαδή η παραπάνω υπόθεση ελεγχθεί ότι ισχύει, το πακέτο στέλνεται από όλες τις εξερχόμενες διεπαφές, αλλά όχι από το RPF interface, δηλαδή από το οποίο έφτασε το πακέτο. Αν ο έλεγχος δεν είναι επιτυχής, το πακέτο απορρίπτεται.

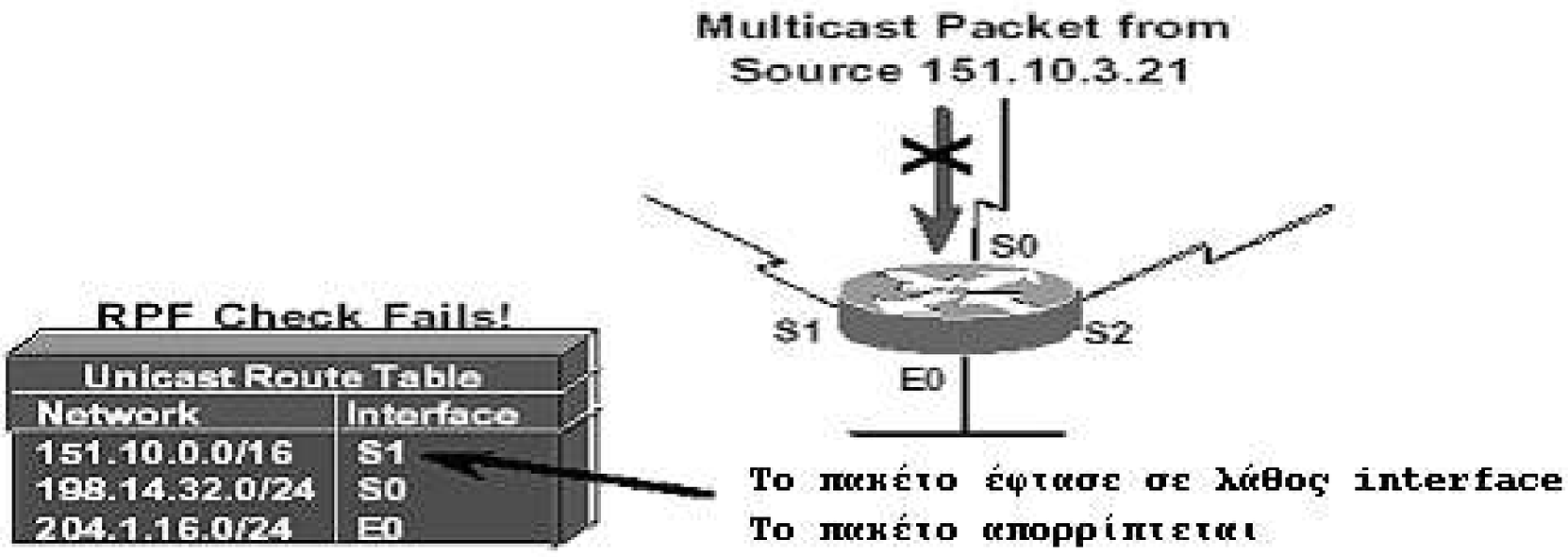


εικόνα 2: RPF Checking

Η εικόνα 2 δείχνει ένα χαρακτηριστικό παράδειγμα του RPF, το οποίο έχει ως εξής: Η πηγή προωθεί στο δίκτυο multicast δεδομένα. Κάθε δρομολογητής του σχήματος, βάσει του πίνακα δρομολόγησής του, έχει μια διαεπαφή (RPF) το οποίο είναι το σωστό για να δεχτεί τα πακέτα από τη συγκεκριμένη πηγή. Οι δρομολογητές λαμβάνουν τα multicast πακέτα σε μία ή σε περισσότερες διεπαφές, όμως με την εκτέλεση

RPF ελέγχου αποτρέπονται τα routing loops. Στο παράδειγμά μας, ένας από τους δρομολογητές μετά από RPF έλεγχο απέρριψε την προώθηση πακέτων που έφταναν σε διαφορετικό από το RPF interface.

Παράδειγμα RPF ελέγχου



εικόνα 3

Στην εικόνα 3 βλέπουμε με μια πιο κοντινή ματιά πώς γίνεται ο RPF έλεγχος. Ο δρομολογητής μπορεί να δεχτεί τα multicast δεδομένα που έρχονται από την πηγή 151.10.3.21 μόνο από το διεπαφή S1, γιατί ο unicast πίνακας δρομολόγησής του για το δίκτυο 151.10.0.0/16 έχει ως μία εξερχόμενη διεπαφή το S1. Τα δεδομένα που φτάνουν στη διεπαφή S0 απορρίπτονται.

Παράδειγμα επιτυχημένου RPF ελέγχο

εικόνα 4

Αντίθετα η εικόνα 4 δείχνει έναν επιτυχημένο RPF έλεγχο, οπότε τα δεδομένα προωθούνται από τις εξερχόμενες διεπαφές S0 και E0.

3.5 Σχεδιασμοί δρομολόγησης-CIDR

Ως CIDR (Classless inter-domain routing) ορίζουμε την δυνατότητα ή άρνηση προσθήκης επιτρεπόμενων IP διευθύνσεων. Αυτές μπορούν να εισαχθούν μεμονομένα μία-μία, ή απευθείας ολόκληρες εμβέλειες (subnets) IP διευθύνσεων.

Για να γίνει προσθήκη subnet δικτυακών διευθύνσεων, αυτές πρέπει να εισαχθούν σύμφωνα με τη μέθοδο CIDR, π.χ. 192.168.1.0/24. Αυτό προσθέτει όλες τις διευθύνσεις στην εμβέλεια από 192.168.1.1 έως 192.168.1.254.

Το CIDR εμπεριέχει τις εξής βασικές ιδέες:

- Ιεραρχημένη διευθυνσιοδότηση
- Απόδοση διευθύνσεων σε κομμάτια μεταβλητού μεγέθους (Classless Address Allocation).
- Άθροιση διαδρομών (Route Aggregation)

Μια βασική απαίτηση για την εφαρμογή του CIDR είναι η ύπαρξη ιεραρχημένης διευθυνσιοδότησης. Ένα είδος ιεραρχίας είναι η απόδοση διευθύνσεων ανάλογα με την γεωγραφική θέση του δικτύου, πολλές φορές αυτός ο διαχωρισμός δεν είναι εφικτός γιατί πολλά δίκτυα παρόχων διαδικτύου αλλά και εταιριών απλώνονται ακόμα και σε διαφορετικές ηπείρους. Μια πιο λειτουργική προσέγγιση είναι η απόδοση μεγάλων κομματιών του χώρου διευθύνσεων στους παρόχους διαδικτύου. Κάθε νέο δίκτυο λοιπόν που συνδέετε στο διαδίκτυο μέσω ενός παρόχου χρησιμοποιεί ένα κομμάτι διευθύνσεων που του παραχωρεί ο πάροχός του.

Αξίζει να σημειωθεί ότι πλέον οι διευθύνσεις ενός δικτύου παραχωρούνται από τον πάροχο και για την σωστή λειτουργία του CIDR θα πρέπει να επιστρέφονται σε περίπτωση αλλαγής παρόχου και να αποδίδεται στο δίκτυο καινούργιο κομμάτι διευθύνσεων από των χώρο διευθυνσιοδότησης του νέου παρόχου. Η διαδικασία που μόλις περιγράψαμε είναι γνωστή και ως address renumbering ή απλά renumbering.

Το CIDR καταργεί τις τάξεις διευθύνσεων που χρησιμοποιούν μάσκες σταθερού μήκους και χρησιμοποιεί μάσκες μεταβλητού μήκους (Variable Length Masks-VLM). Με αυτό τον τρόπο χρησιμοποιώντας το ζευγάρι Αρχική διεύθυνση / Μάσκα δικτύου είναι δυνατό να καθορίσουμε ένα κομμάτι διευθύνσεων. Το ζευγάρι Αρχική διεύθυνση / Μάσκα δικτύου ονομάζεται πρόθεμα IP διεύθυνσης (IPAddress Prefix) γιατί εάν πραγματοποιήσουμε την λογική πράξη αρχική διεύθυνση ΚΑΙ μάσκα δικτύου θα πάρουμε σαν αποτέλεσμα το κοινό μέρος που μοιράζονται όλες οι διευθύνσεις του κομματιού αυτού.

3.6 MPLS - ATM Δρομολόγηση

Το πρωτόκολλο MPLS είναι μια τεχνολογία που έχει καθοριστεί από την IETF (Internet Engineering Task Force) και προβλέπει τον αποδοτικό προσδιορισμό, τη δρομολόγηση, τη προώθηση, και μεταγωγή της ροής της κυκλοφορίας μέσα στο δίκτυο.

Στο MPLS, η μεταγωγή δεδομένων πραγματοποιείται με ετικέτες (Label switched paths - LSPs). Τα LSPs είναι μια ακολουθία ετικετών σε όλους τους κόμβους που μεσολαβούν κατά μήκος του μονοπατιού από την πηγή στον προορισμό. Τα LSPs εγκαθίστανται είτε πριν από τη μετάδοση δεδομένων (control - driven) είτε μετά την ανίχνευση μιας ορισμένης ροής δεδομένων (data - driven). Οι ετικέτες, οι οποίες ταυτοποιούν συγκεκριμένα πρωτόκολλα, διανέμονται χρησιμοποιώντας το πρωτόκολλο διανομής ετικετών (LDP) ή το RSVP ή με το να κάθονται πάνω σε πρωτόκολλα δρομολόγησης όπως το BGP και το OSPF.

Κάθε πακέτο δεδομένων τοποθετεί και μεταφέρει τις ετικέτες κατά τη διάρκεια της διαδρομής τους από την πηγή στον προορισμό. Η υψηλής ταχύτητας μεταγωγή δεδομένων είναι δυνατή επειδή οι καθορισμένου μήκους ετικέτες εισάγονται στην αρχή του πακέτου ή του κελιού και μπορούν χρησιμοποιηθούν από το υλικό για να μεταγάγουν τα πακέτα γρήγορα μεταξύ των συνδέσμων.

Το ATM είναι μια ενιαία μέθοδος για μεταφορά, πολυπλεξία και μεταγωγή (switching) πληροφορίας πολλών ειδών (data,video, audio) με υψηλές ταχύτητες μέσω ενός απλού μηχανισμού μετάδοσης και μεταγωγής (switching). Το βασικό του χαρακτηριστικό που το κάνει να διαφέρει από τις άλλες τεχνολογίες που διαχειρίζονται δεδομένα (data) είναι η επέκτασή του από τα τοπικά δίκτυα LAN στα δίκτυα ευρείας περιοχής WAN καθώς και από τη backbone υποδομή ενός δικτύου στο desktop.

3.7 IP spoofing (Security)

Ο όρος IP spoofing στην επιστήμη των υπολογιστών αναφέρεται στην δημιουργία πακέτων IP με ψεύτικη διεύθυνση προέλευσης ώστε να συγκαλυφθεί η ταυτότητα του αποστολέα του πακέτου και ο παραλήπτης να νομίζει ότι προήλθε από άλλον υπολογιστή.

Το βασικό πρωτόκολλο που χρησιμοποιείται στο διαδίκτυο για την αποστολή και λήψη δεδομένων είναι το IP - Internet Protocol. Κάθε πακέτο IP περιέχει εκτός των δεδομένων και μία κεφαλίδα (header) στην οποία καταγράφεται οι διευθύνσεις IP του αποστολέα και του παραλήπτη του πακέτου. Ένας κακόβουλος χρήστης μπορεί να στείλει ένα πακέτο IP του οποίου η κεφαλίδα να γράφει κάποια άλλη διεύθυνση και όχι την δικιά του. Με τον τρόπο αυτό μπορεί να ξεγελάσει τον παραλήπτη και να τον κάνει να πιστέψει ότι το πακέτο προήλθε από κάποιον άλλο υπολογιστή.

Ο υπολογιστής που λαμβάνει αυτό το πακέτο IP δεν γνωρίζει ότι η διεύθυνση του αποστολέα που αναγράφεται στην κεφαλίδα είναι πλαστογραφημένη, οπότε απαντάει στέλνοντας πακέτα IP στην ψεύτικη διεύθυνση. Αυτή η τεχνική χρησιμοποιείται κυρίως από χάκερ, οι οποίοι αφενός δεν θέλουν να αποκαλύψουν την ταυτότητά τους και αφετέρου στις περισσότερες περιπτώσεις το IP spoofing χρησιμοποιείται κυρίως σε επιθέσεις άρνησης υπηρεσιών (DOS - Denial of Service). Οι επιθέσεις αυτού του είδους έχουν ως στόχο να γεμίσουν τον υπολογιστή-θύμα με πολλά πακέτα ώστε να τον αναγκάσουν να περιέλθει σε δυσλειτουργία και να μην μπορεί να εξυπηρετήσει σωστά τους νόμιμους χρήστες του. Σε τέτοιες περιπτώσεις ο επιτιθέμενος δεν ενδιαφέρεται να λάβει απάντηση στα πακέτα που στέλνει, οπότε

συνήθως χρησιμοποιεί την τεχνική IP spoofing ώστε να κατευθύνει τις απαντήσεις του θύματος προς κάποιον άλλο υπολογιστή. Όπως ειπώθηκε και προηγουμένως, η τεχνική αυτή προσφέρει ακόμη ένα πλεονέκτημα: Κρύβει την πραγματική ταυτότητα του επιτιθέμενου.

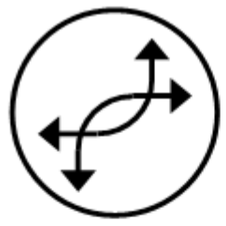
Ο επιτιθέμενος στις περισσότερες περιπτώσεις διαλέγει μία τυχαία IP διεύθυνση για να τοποθετηθεί στην κεφαλίδα του IP πακέτου, προσέχοντας όμως η διεύθυνση αυτή να μην είναι σε απαγορευμένη περιοχή (πχ 127.0.0.0, 192.168.0.1).

Μία άλλη χρήση του IP spoofing είναι για το σπάσιμο των μηχανισμών ασφαλείας δικτύων υπολογιστών. Σε πολλά εταιρικά δίκτυα είναι συνηθισμένο η αναγνώριση των χρηστών να γίνεται μέσω των IP διευθύνσεών τους. Για παράδειγμα ενδέχεται ένας υπολογιστής να είναι ρυθμισμένος ώστε να επιτρέπει την πρόσβαση χωρίς username και password όταν διαπιστώσει ότι η σύνδεση προέρχεται από κάποια συγκεκριμένη IP (πχ. την IP του υπολογιστή που χρησιμοποιεί ο διευθυντής). Αυτό όμως συνιστά τρύπα ασφαλείας, αφού οποιοσδήποτε εργαζόμενος μπορεί να χρησιμοποιήσει την τεχνική IP spoofing για να κατασκευάσει πακέτα IP με ψεύτικη διεύθυνση προέλευσης και έτσι να αποκτήσει πρόσβαση στον εν λόγω υπολογιστή.

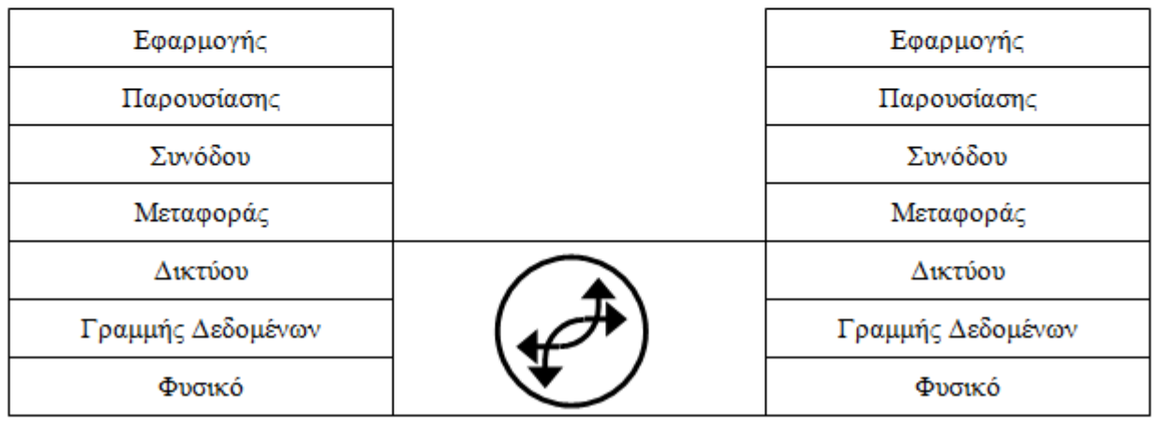
3.8 Διαφορές/βελτιώσεις σε σχέση με την γέφυρα.

Η δρομολόγηση διαφέρει από τη γεφύρωση στην υπόθεσή της ότι οι δομές διευθύνσεων υπονοούν την εγγύτητα των παρόμοιων διευθύνσεων μέσα στο δίκτυο, επιτρέποντας κατά συνέπεια σε έναν πίνακα δρομολόγησης εισόδου να αντιπροσωπεύσει τη διαδρομή προς μια ομάδα διευθύνσεων. Για αυτό και η δρομολόγηση ξεπερνά την γεφύρωση σε μεγάλα δίκτυα, και έχει γίνει κυρίαρχος τρόπος εύρεσης διαδρομής (path-discovery) στο διαδίκτυο.

Επίσης, μια σημαντική διαφορά των δρομολογητών από τις γέφυρες είναι ότι οι δρομολογητές λειτουργούν επίσης και στο επίπεδο δικτύου του OSI, (Οι γέφυρες λειτουργούν στο φυσικό επίπεδο και στο επίπεδο γραμμής δεδομένων, ενώ οι πιο απλές συσκευές όπως οι διανομείς λειτουργούν στο φυσικό επίπεδο).



Σύμβολο Δρομολογητή

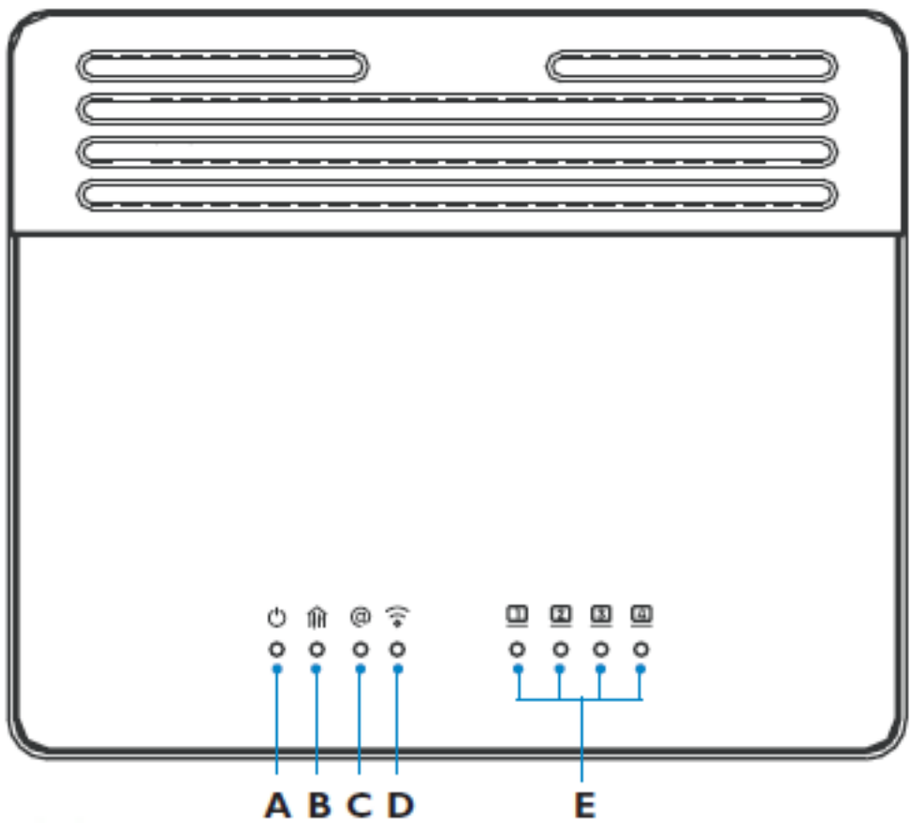


εικόνα: Επίπεδα Λειτουργίας Δρομολογητών

Ακόμα μια διαφορά με τις γέφυρες, είναι ότι οι δρομολογητές υποστηρίζουν αρκετά πιο πολύπλοκες διατάξεις (τοπολογίες) δικτύων στις οποίες είναι πιθανόν δύο σημεία του δικτύου να ενώνονται με περισσότερες από μία διαδρομές. Για παράδειγμα, στο διαδίκτυο (το οποίο δεν θα μπορούσε να λειτουργήσει χωρίς δρομολογητές) μεταξύ δύο κόμβων (π.χ. του υπολογιστή σας στο σπίτι και μιας δικτυακής τοποθεσία που επισκέπτεστε τη δεδομένη στιγμή), υπάρχουν πολλές διαδρομές τις οποίες μπορούν να ακολουθήσουν τα πακέτα κατά την μεταφορά τους. Μάλιστα αν υποθέσουμε ότι βλέπετε μια σελίδα στο διαδίκτυο ή κατεβάζετε ένα αρχείο, δεν είναι καν σίγουρο ότι όλα τα πακέτα από τα οποία αποτελείται έχουν ακολουθήσει την ίδια διαδρομή για να φτάσουν στον υπολογιστή σας.[4]

Γενικά οι δρομολογητές επειδή στην ουσία είναι εξειδικευμένοι υπολογιστές είναι αρκετά ακριβότεροι από τις γέφυρες αλλά προσφέρουν πολύ περισσότερα πλεονεκτήματα. Μπορούν να διασυνδέσουν μεταξύ τους διαφορετικά είδη δικτύων τόσο τα παραδοσιακά όσο και υψηλών επιδόσεων και ακόμα χρησιμοποιούνται ευρύτατα για την διασύνδεση τοπικών δικτύων με δίκτυα ευρείας περιοχής. Ευτυχώς, ολοένα αυξανόμενη ισχύς των μικροεπεξεργαστών, η πτώση τιμών και η ραγδαία αύξηση της τεχνολογίας κάνουν ολοένα και πιο οικονομική την χρήση των δρομολογητών. Οι δρομολογητές που κυκλοφορούν σήμερα στην αγορά έχουν πολλές δυνατότητες όπως η υποστήριξη πολλαπλών πρωτοκόλλων του επιπέδου δικτύου ενώ πολλοί έχουν και ενσωματωμένα χαρακτηριστικά γέφυρας (multi protocol bridge – router). [5]

ΚΕΦΑΛΑΙΟ 4: Βασικά χαρακτηριστικά του δρομολογητή



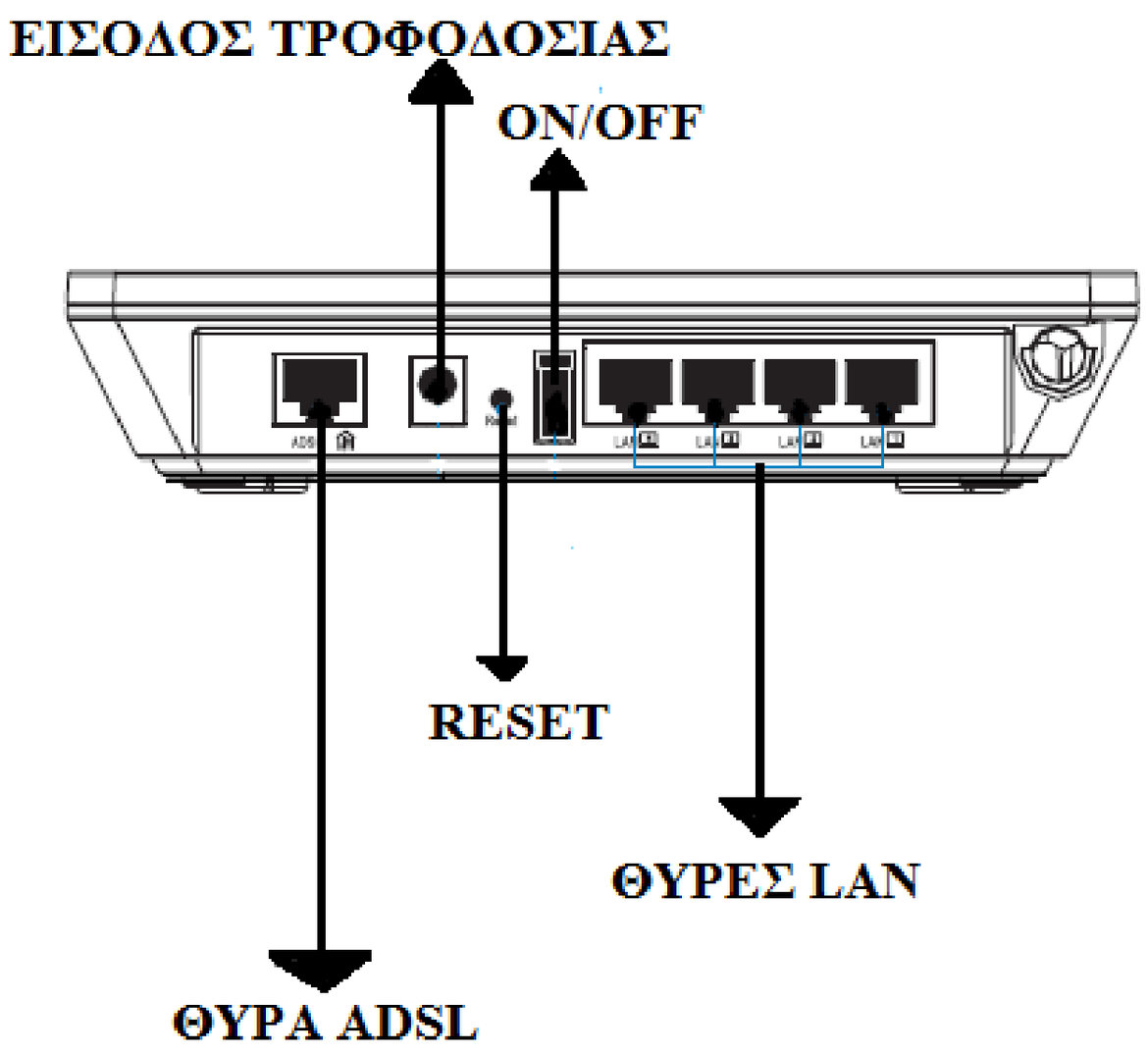
A
ON: Ενεργοποιημένο, κανονική λειτουργία
OFF: Απενεργοποιημένο ή βλάβη

B
ON: Ο βρόχος ADSL τίθεται σε λειτουργία
Αναβοσβήνει: Εκκίνηση
OFF: Ο βρόχος ADSL είναι εκτός λειτουργίας

C
ON: Η σύνδεση με το Διαδίκτυο έχει ενεργοποιηθεί
OFF: Μη μεταφορά δεδομένων

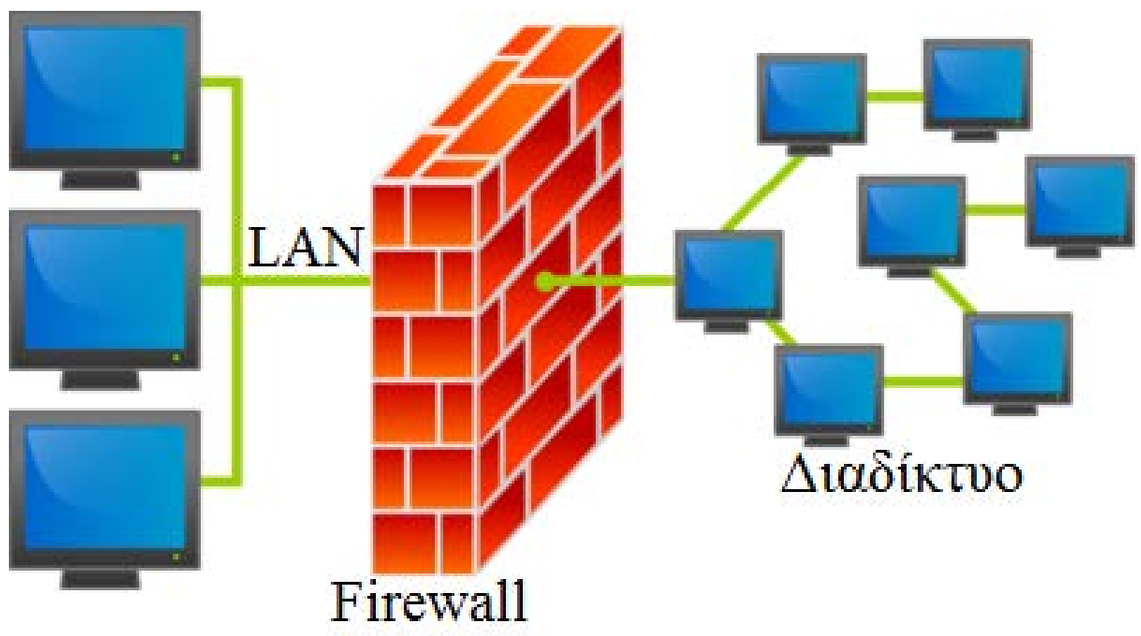
D
ON: Η ασύρματη σύνδεση έχει ενεργοποιηθεί
Αναβοσβήνει: Αποστολή/Λήψη δεδομένων
OFF: Μη μεταφορά δεδομένων

E
ON: Η σύνδεση Ethernet έχει εδραιωθεί
Αναβοσβήνει: Αποστολή/Λήψη δεδομένων
OFF: Χωρίς σύνδεση



4.1 Τεχνικά Χαρακτηριστικά -Τείχος Προστασίας (Firewall)

Το τείχος προστασίας βρίσκεται μεταξύ ενός ασφαλούς τοπικού δικτύου (LAN), όπως ισχύει για το ασφαλές ενσύρματο/ασύρματο δίκτυο ενός οικιακού χρήστη και του διαδικτύου. Σκοπός του είναι να ελέγχει τις επικοινωνίες μεταξύ τοπικού δικτύου και διαδικτύου με την ανάλυση των πακέτων δεδομένων και τον προσδιορισμό τους. Το τείχος προστασίας είναι πολύ χρήσιμο για τη παρεμπόδιση χάκερς που χρησιμοποιούν διάφορες τεχνικές για να επιτεθούν και να «μολύνουν» τους ηλεκτρονικούς υπολογιστές.



Ένα τείχος προστασίας μπορεί να υλοποιείται είτε μέσω λογισμικού (που συχνά αποκαλείται «προσωπικό firewall») είτε μέσω υλικού με εξειδικευμένη συσκευή δικτύου. Τα περισσότερα σύγχρονα λειτουργικά συστήματα, όπως Windows, linux έχουν ενσωματωμένο ένα βασικό προσωπικό firewall τουλάχιστον.[6]

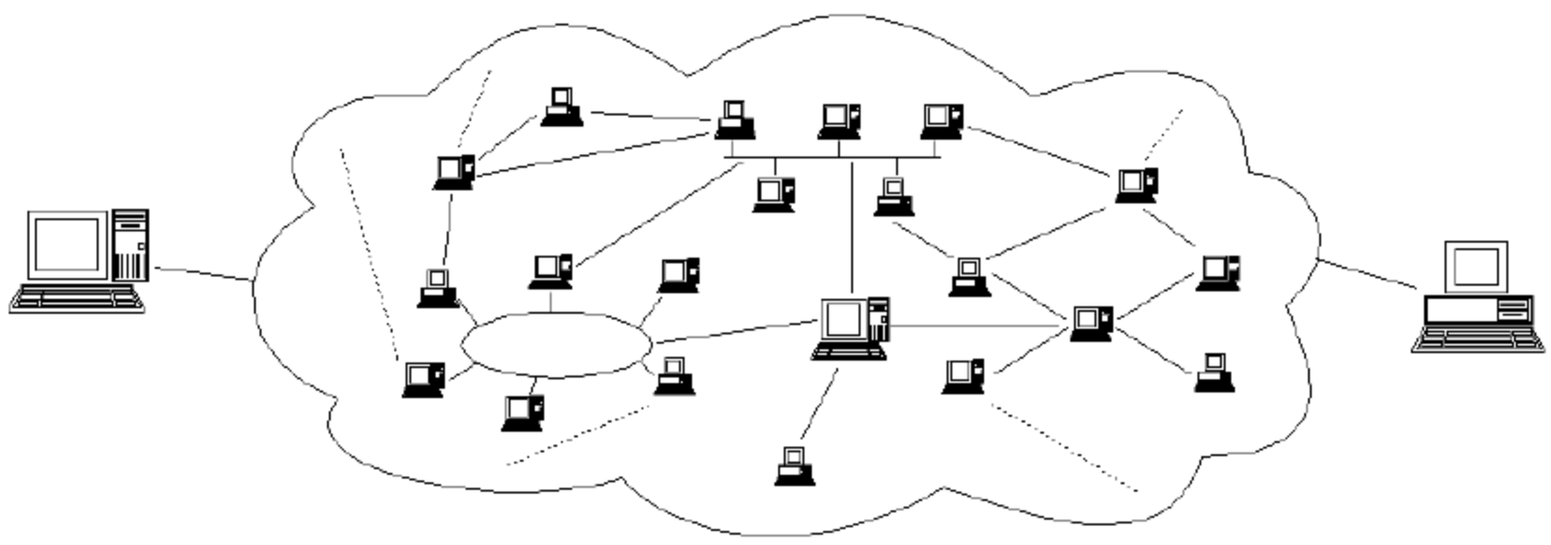
4.2 Πρωτόκολλα Επικοινωνίας

Στην καθημερινή μας ζωή, πρωτόκολλο είναι ένα σύνολο από συμβάσεις που καθορίζουν πως πρέπει να πραγματοποιείται κάποια διαδικασία. Στον κόσμο των δικτύων πρωτόκολλο είναι ένα σύνολο από συμβάσεις που καθορίζουν πως ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές του δικτύου. Το πρωτόκολλο είναι αυτό που καθορίζει πως διακινούνται τα δεδομένα, πως γίνεται ο έλεγχος και ο χειρισμός των λαθών, κλπ. Το διαδίκτυο δεν είναι ένα απλό δίκτυο, αλλά το δίκτυο όλων των δικτύων. Χρειάζεται επομένως ένα σύνολο από συμβάσεις που να καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα υπολογιστές που μπορεί να είναι διαφορετικού τύπου και να ανήκουν σε διαφορετικά δίκτυα. Ακριβώς αυτό το σύνολο συμβάσεων προσφέρει το TCP/IP. Όλοι οι υπολογιστές που είναι συνδεδεμένοι

στα χιλιάδες μικρότερα δίκτυα του διαδικτύου τρέχουν το πρωτόκολλο TCP/IP κι έτσι μιλούν μια κοινή γλώσσα που τους επιτρέπει να συνεννοούνται παρά τις διαφορές τους.

4.3 Γνωριμία του TCP/IP

Ας υποθέσουμε ότι θέλουμε να μεταφέρουμε δεδομένα από έναν υπολογιστή που είναι συνδεδεμένος στο διαδίκτυο και βρίσκεται π.χ. στην Αμερική, στη Βοστώνη, σε έναν άλλον που είναι επίσης συνδεδεμένος στο διαδίκτυο και βρίσκεται π.χ. στην Ελλάδα, στα Χανιά. Μεταξύ των δύο υπολογιστών παρεμβάλλεται το “σύννεφο” του διαδικτύου, δηλαδή ένα πλέγμα από συνδέσεις και δρομολογητές.



Το διαδίκτυο χρησιμοποιεί την τεχνολογία μεταγωγής πακέτων για τη μεταφορά των δεδομένων. Τα δεδομένα κόβονται σε κομμάτια που ονομάζονται πακέτα και σε κάθε πακέτο μπαίνει μια “επικεφαλίδα” με τις διευθύνσεις του υπολογιστή -αποστολέα και του υπολογιστή –παραλήπτη. Σημειώνουμε ότι σε κάθε υπολογιστή του διαδικτύου αντιστοιχίζεται μία διεύθυνση που ονομάζεται διεύθυνση IP.

Το πρωτόκολλο IP είναι υπεύθυνο για το πέρασμα του πακέτου από υπολογιστή σε υπολογιστή μέσα από το “σύννεφο” των συνδέσεων. Καθώς το IP δρομολογεί το κάθε πακέτο μέσα στο δίκτυο, προσπαθεί να το παραδώσει, αλλά δεν μπορεί να εγγυηθεί ούτε

- ότι το πακέτο θα φτάσει στον προορισμό του
- ότι τα διάφορα πακέτα που αποτελούν τα αρχικά δεδομένα θα φτάσουν με τη σειρά με την οποία στάλθηκαν

- ότι το περιεχόμενο των πακέτων θα φτάσει αναλλοίωτο.

Το TCP προσφέρει ένα αξιόπιστο πρωτόκολλο πάνω από το IP. Εγγυάται

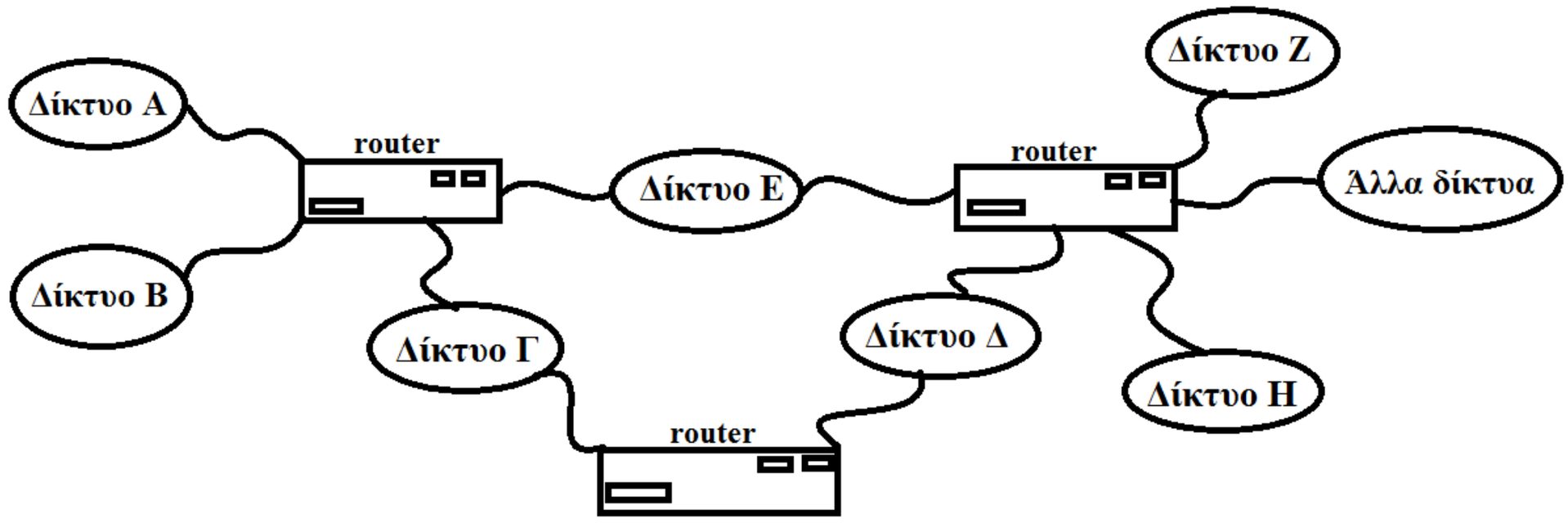
- ότι τα πακέτα θα παραδοθούν στον προορισμό τους,
- ότι θα φτάσουν με τη σειρά με την οποία στάλθηκαν και ότι τα περιεχόμενα των πακέτων θα φτάσουν αναλλοίωτα (δηλ. όπως στάλθηκαν).

Το TCP δουλεύει ως εξής: το κάθε πακέτο δεδομένων αριθμείται. Ο υπολογιστής - παραλήπτης και ο υπολογιστής – αποστολέας παρακολουθούν τους αριθμούς των πακέτων και ανταλλάσσουν μεταξύ τους πληροφορίες. Ο παραλήπτης λαμβάνει το πρώτο πακέτο, το δεύτερο, κλπ. Σε περίπτωση που παρουσιαστεί κάποιο πρόβλημα στο δίκτυο, είτε χαθεί κάποιο πακέτο κατά τη διάρκεια της μετάδοσης, το ξαναζητάει και ο αποστολέας είναι υπεύθυνος για την αναμετάδοσή του. Ο παραλήπτης ελέγχει επίσης αν το περιεχόμενο των πακέτων φτάνει σωστά.

Η μέθοδος αυτή εξασφαλίζει αξιοπιστία και ταχύτητα διότι οι ενδιάμεσοι υπολογιστές δεν εκτελούν ελέγχους. Συνεπώς, το διαδίκτυο (Internet) δεν είναι τίποτα άλλο παρά ένα δίκτυο αποτελούμενο από πολλά δίκτυα υπολογιστών που επικοινωνούν χρησιμοποιώντας το πρωτόκολλο TCP/IP.

4.4 Η δρομολόγηση των πακέτων

Όπως βλέπουμε στη παρακάτω εικόνα, η διαδρομή που ακολουθεί ένα πακέτο μέσα από το “σύννεφο” των συνδέσεων δεν είναι προκαθορισμένη. Το πρωτόκολλο IP είναι υπεύθυνο για τη μετάδοση ενός πακέτου δεδομένων από υπολογιστή σε υπολογιστή. Τα δίκτυα συνδέονται μεταξύ τους με δρομολογητές (routers) ή πύλες (gateways). Ένας δρομολογητής συνδέει δύο ή περισσότερα δίκτυα (που μπορεί να είναι διαφορετικού τύπου) και έτσι ανήκει σε δύο ή περισσότερα δίκτυα ταυτόχρονα.



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

Ας θεωρήσουμε πάλι ότι ένας υπολογιστής που βρίσκεται κάπου στο διαδίκτυο θέλει να στείλει δεδομένα σε κάποιον άλλον υπολογιστή. Τα δεδομένα κόβονται σε πακέτα και το IP που εκτελείται στον υπολογιστή - αποστολέα ετοιμάζεται να στείλει το κάθε πακέτο. Εισάγει λοιπόν στην επικεφαλίδα του πακέτου τις IP διευθύνσεις του αποστολέα και του παραλήπτη και κατόπιν βάσει των διευθύνσεων αυτών ελέγχει αν ο παραλήπτης βρίσκεται στο ίδιο δίκτυο με τον αποστολέα.

Εάν ναι, το πακέτο στέλνεται κατευθείαν στον παραλήπτη χωρίς να χρειαστεί να διαβεί τα όρια του δικτύου. Εάν όχι, προωθείται στο δρομολογητή που είναι συνδεμένος με το δίκτυο. Ο δρομολογητής με τη σειρά του ελέγχει αν ο παραλήπτης βρίσκεται σε κάποιο από τα υπόλοιπα δίκτυα με τα οποία είναι συνδεδεμένος. Εάν ναι, το πακέτο στέλνεται κατευθείαν στον παραλήπτη στο δίκτυο αυτό. Εάν όχι, το πακέτο προωθείται στον επόμενο δρομολογητή μέχρις ότου το πακέτο προωθηθεί τελικά στο δρομολογητή που είναι συνδεδεμένος στο ίδιο δίκτυο με τον παραλήπτη.Το πακέτο μπορεί έτσι να περάσει από πολλούς δρομολογητές μέχρις ότου φτάσει στον προορισμό του.

Οι δρομολογητές διατηρούν πίνακες που προσδιορίζουν την κατεύθυνση που πρέπει να πάρει ένα πακέτο προκειμένου να φτάσει στον προορισμό του. Βάσει αυτών των πινάκων αποφασίζουν ποιος θα είναι ο επόμενος δρομολογητής στον οποίο θα πρέπει να προωθήσουν το πακέτο. Κάθε φορά που το πακέτο μετακινείται όλο και πιο κοντά προς τον προορισμό του έως ότου τελικά τον φτάσει. Ένα μεγάλο πλεονέκτημα αυτής της μεθόδου είναι ότι η διαδρομή που ακολουθεί ένα πακέτο δεν είναι προκαθορισμένη, αλλά επιλέγεται δυναμικά. Έτσι, οι δρομολογητές μπορούν να επιλέγουν εναλλακτικούς

δρόμους για ένα πακέτο σε περίπτωση που μια συγκεκριμένη σύνδεση του δικτύου παρουσιάζει πρόβλημα και βρίσκεται προσωρινά εκτός λειτουργίας.

4.5 Το πρωτόκολλο DHCP

Με τον όρο DHCP (Dynamic Host Configuration Protocol) αναφερόμαστε σε ένα μηχανισμό διαχείρισης TCP/IP πρωτοκόλλων.Το πρωτόκολλο είναι ουσιαστικά ένα λογισμικό που τρέχει σε έναν υπολογιστή και κανονίζει όλα τα θέματα επικοινωνίας με αυτόν τον υπολογιστή και άλλους που χρησιμοποιούν αυτό το πρωτόκολλο ως γλώσσα. Για να δουλέψει το ίδιο λογισμικό σε τόσους πολλούς υπολογιστές υπάρχει η ανάγκη να το ξεκινήσουμε σε κάθε υπολογιστή με τις αντίστοιχες παραμέτρους για αυτόν και για τη θέση του στο δίκτυο. Η αρχικοποίηση αυτή μπορεί να γίνει κατά τη διάρκεια του φορτώματος (αν το πρωτόκολλο είναι συγχωνευμένο στο λειτουργικό σύστημα) ή με την κλήση του πρωτοκόλλου από κάποια εφαρμογή (αν το πρωτόκολλο υπάρχει στην εφαρμογή). Οι παράμετροι αυτές μπορούν να οριστούν τοπικά, για κάθε υπολογιστή ξεχωριστά. Κάτι τέτοιο όμως δημιουργεί αρκετά προβλήματα . Χρειάζεται πάρα πολύ εργασία από τον διαχειριστή του δικτύου η οποία είναι χρονοβόρα και επιρρεπής σε λάθη.

Το να διατηρούνται οι παράμετροι ενημερωμένοι χρειάζεται συνεχή δουλειά η οποία αυξάνεται γεωμετρικά με τις αλλαγές που συμβαίνουν στο δίκτυο, ειδικά αν υπάρχουν υπολογιστές που αλλάζουν συνεχώς θέση (π.χ. φορητοί Η/Υ) . Η αλλαγή μίας παραμέτρου κοινής για τους υπολογιστές σε ένα subnet (π.χ. τοπική διεύθυνση ενός router) απαιτεί αλλαγές σε κάθε υπολογιστή . Μερικά μηχανήματα μπορεί να λειτουργούν ως τερματικά. Κάτι τέτοιο σημαίνει ότι δεν έχουν αποθηκευτικό χώρο για να κρατήσουν τις ρυθμίσεις . Σε περιπτώσεις έλλειψης διευθύνσεων ή ενός δικτύου που αλλάζει συνέχεια είναι χάσιμο χρόνου να δίνουμε σε έναν μη σταθερό υπολογιστή μόνιμη διεύθυνση.

Μία καλύτερη προσέγγιση θα ήταν να χρησιμοποιούνται ομάδες διευθύνσεων από ομάδες υπολογιστών. Η «χειροκίνητη» ρύθμιση τέτοιου είδους δεν παρέχει εύκολο τρόπο για να γίνει αυτό . Όλοι αυτοί οι λόγοι οδήγησαν στην ανάγκη για έναν αυτόματο μηχανισμό διαχείρισης των TCP/IP πρωτοκόλλων. Ο DHCP είναι αυτή τη στιγμή ο πιο προηγμένος μηχανισμός για να γίνεται αυτό.

4.5.1 Η εφαρμογή του πρωτοκόλλου

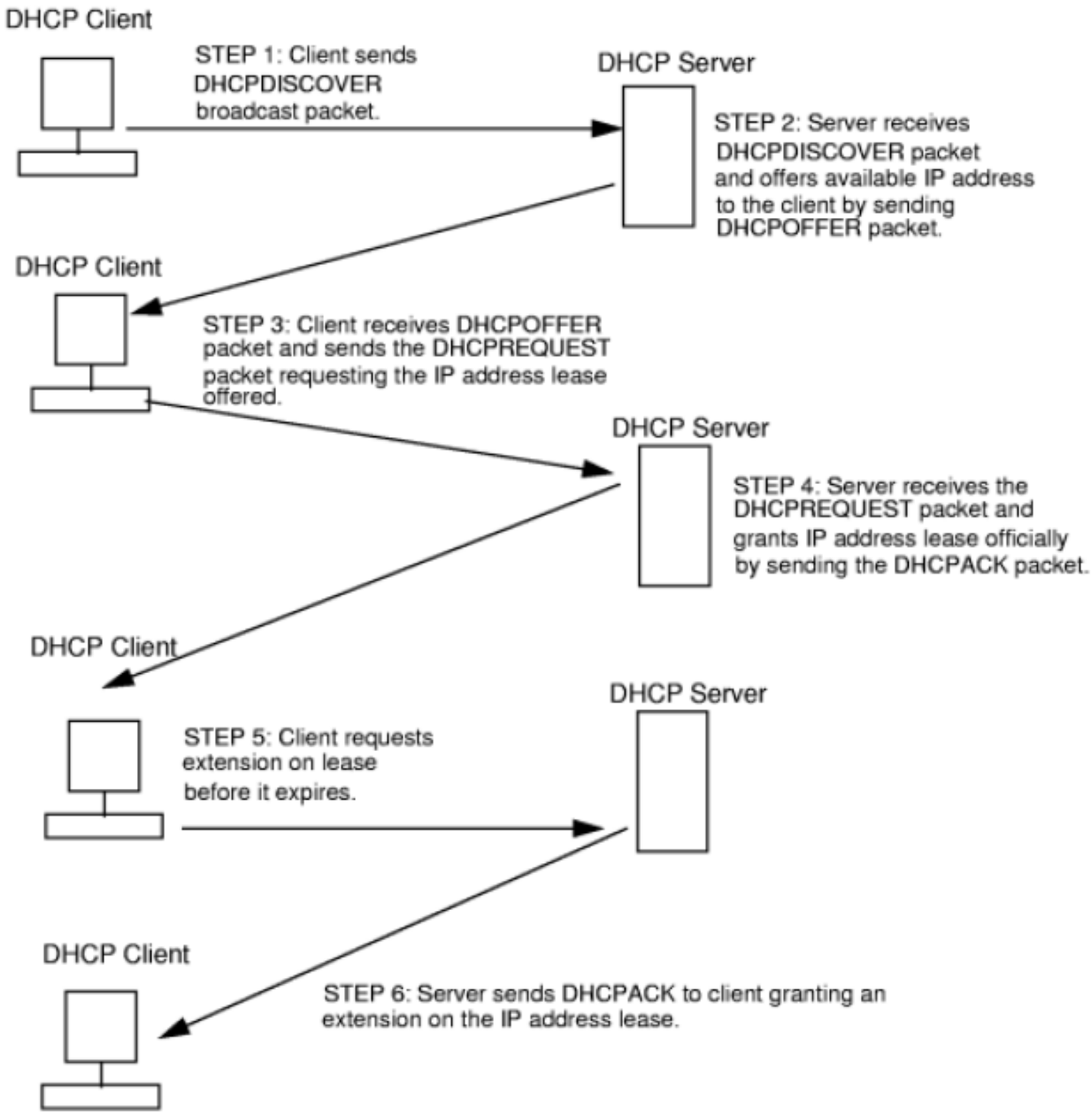
Σε ορισμένες περιπτώσεις και όταν αυτό είναι αναγκαίο μπορούμε να αποδώσουμε στους υπολογιστές του δικτύου διευθύνσεις IP οι οποίες δεν είναι στατικές αλλά δυναμικές . Αυτό σημαίνει πώς ο κάθε υπολογιστής δε θα έχει τη δική του σταθερή διεύθυνση αλλά κάθε φορά που θα συνδέεται στο δίκτυο θα ζητά να του χορηγηθεί μια ελεύθερη IP διεύθυνση από το σύνολο διευθύνσεων το οποίο είναι καθορισμένο εκ των προτέρων. Αυτή είναι και η ουσία του πρωτοκόλλου DHCP.

Η εφαρμογή του πρωτοκόλλου DHCP σε ένα δίκτυο ο διακομιστής (client-server) στο οποίο ο υπολογιστής που του ζητά να του χορηγηθεί μια δυναμική IP διεύθυνση είναι ο υπολογιστής πελάτης (DHCP client) ενώ ο υπολογιστής που θα του χορηγήσει τη διεύθυνση είναι ο διακομιστής (DHCP server) της υπηρεσίας. Ας σημειωθεί πως το πρωτόκολλο DHCP δεν είναι το μόνο πρωτόκολλο αυτού του είδους αλλά έρχεται να αντικαταστήσει παλαιότερα πρωτόκολλα απόδοσης IP διευθύνσεων με χαρακτηριστικό παράδειγμα το πρωτόκολλο BOOTR . Αν και υπάρχει συμβατότητα ανάμεσα στα δύο πρωτόκολλα που σημαίνει πως ένας υπολογιστής με πρωτόκολλο BOOTR μπορεί να ζητήσει IP διεύθυνση από έναν DHCP server , εν τούτοις το DHCP παρέχει πολλές βελτιώσεις έναντι του πρωτοκόλλου BOOTP .

Ένα σημαντικό πλεονέκτημα του πρωτοκόλλου DHCP έναντι του πρωτοκόλλου BOOTP είναι πως μια IP διεύθυνση μπορεί να χορηγηθεί σε έναν υπολογιστή του δικτύου για συγκεκριμένο χρονικό διάστημα . Αυτή η δυνατότητα είναι πολύ χρήσιμη σε περιπτώσεις που οι υπολογιστές του δικτύου είναι περισσότεροι από τις IP δικτύου που διαθέτουμε καθώς αποδίδοντας μια IP διεύθυνση σε έναν υπολογιστή για πεπερασμένο χρόνο, δεν κινδυνεύουμε να μείνουμε χωρίς ελεύθερες διευθύνσεις. Από την άλλη πλευρά, εάν οι διευθύνσεις που διαθέτουμε είναι περισσότερες από τους υπολογιστές του δικτύου, μπορούμε να αποδώσουμε διευθύνσεις σε κάποιους από αυτούς για απεριόριστο χρόνο. Ένα άλλο πλεονέκτημα του πρωτοκόλλου DHCP έναντι του πρωτοκόλλου BOOTP, είναι πως το πρώτο είναι πιο ευέλικτο όσον αφορά την επικοινωνία ανάμεσα στον DHCP client και στον DHCP server. Έτσι στο πρωτόκολλο DHCP αυτή η επικοινωνία πραγματοποιείται με τη χρήση επτά διαφορετικών τύπων μηνυμάτων σε αντίθεση με το πρωτόκολλο BOOTP το οποίο χρησιμοποιεί μόνο δύο τέτοια μηνύματα (request & reply).

4.5.2 Η λειτουργία του πρωτοκόλλου

Όταν ένας υπολογιστής συνδέεται στο δίκτυο, εκπέμπει (broadcast) ένα ειδικό πλαίσιο ελέγχου (control frame) που ονομάζεται DHCPDISCOVER και έχει ως στόχο να εντοπίσει τους διαθέσιμους DHCP servers που είναι συνδεδεμένοι στο τοπικό δίκτυο οι οποίοι μπορεί να είναι περισσότεροι από ένας. Κάθε φορά που ένας DHCP server δέχεται ένα τέτοιο μήνυμα ανταποκρίνεται στέλνοντας στον υπολογιστή πελάτη ένα μήνυμα που ονομάζεται DHCPOFFER και περιλαμβάνει μια ελεύθερη IP διεύθυνση και ένα σύνολο παραμέτρων διαμόρφωσης (configuration parameters) οι οποίες είναι και οι πιο κατάλληλες για αυτόν τον πελάτη. Σε ορισμένες περιπτώσεις ο DHCP server πριν αποδώσει την IP διεύθυνση στον DHCP client πραγματοποιεί έναν έλεγχο για να διαπιστώσει εάν αυτή η διεύθυνση χρησιμοποιείται ήδη από κάποιον άλλον υπολογιστή. Αυτός ο έλεγχος γίνεται με τη βοήθεια ειδικών πρωτοκόλλων όπως είναι το ARP (address resolution protocol).



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

4.6 Address Resolution Protocol (ARP)

Ο τρόπος που λειτουργεί το πρωτόκολλο ARP είναι εξαιρετικά απλός. Κάθε φορά που πρέπει να γίνει γνωστή η διεύθυνση MAC που αντιστοιχεί σε κάποια συγκεκριμένη διεύθυνση IP, λαμβάνει όλους τους υπολογιστές (broadcasting) ενός πακέτου δεδομένων που περιέχει τη διεύθυνση IP που θέλουμε να μεταφράσουμε. Ο κάθε ένας από τους υπολογιστές του δικτύου, παραλαμβάνει αυτό το πακέτο, συγκρίνει τη διεύθυνση IP που περιέχει, με τη δική του διεύθυνση IP και εάν οι δύο διευθύνσεις είναι οι ίδιες, αποστέλλει μια απάντηση στον υπολογιστή που υπέβαλλε το ερώτημα. Η απάντηση αυτή περιέχει τη MAC διεύθυνση του υπολογιστή αποστολέα η οποία ταυτοποιείται , απομονώνεται και αποθηκεύεται σε μια ειδική μνήμη ARP cache, έτσι ώστε να μπορεί να χρησιμοποιηθεί στο μέλλον.

Η μνήμη αυτή ανανεώνεται σε τακτά χρονικά διαστήματα, διότι τα περιεχόμενα της μπορούν σε κάποια χρονική στιγμή να μεταβληθούν, όπως συμβαίνει για παράδειγμα σε περιπτώσεις κατά τις οποίες αντικαθιστούμε την κάρτα δικτύου του υπολογιστή με κάποια άλλη η οποία έχει τη δική της MAC address.

4.7 Network Address Translation (NAT)

Είναι γνωστό ότι όταν κάποιος υπολογιστής είναι συνδεδεμένος στο διαδίκτυο του έχει αποδοθεί μία μοναδική IP διεύθυνση (ένας 32-bit αριθμός). Το πρωτόκολλο που εκτελείται για την απόδοση IP διευθύνσεων είναι το DHCP (Dynamic Host Control Protocol). Γενικά δεν μπορεί να αποδοθεί αυθαίρετα ένας οποιοσδήποτε 32-bit αριθμός σε έναν υπολογιστή επειδή υπάρχουν διάφορες κλάσεις IP

διευθύνσεων και ο κάθε υπολογιστής μπορεί να έχει ως διεύθυνση κάποιον αριθμό της κλάσης στην οποία ανήκει μόνο. Ειδικά για τα ιδιωτικά δίκτυα όπου ο αριθμός τους ανά τον κόσμο είναι συντριπτικά μεγάλος (ας αναλογιστούμε για παράδειγμα ότι σε κάθε απλό εργαστήριο Πληροφορικής σε ένα σχολείο υπάρχει ένα τοπικό ιδιωτικό δίκτυο), οι IP διευθύνσεις που μπορούν να έχουν οι υπολογιστές μπορούν να ανήκουν μόνο σε κάποια από τις τρεις επόμενες κλάσεις:

10.0.0.0 - 10.255.255.255 (Class A)

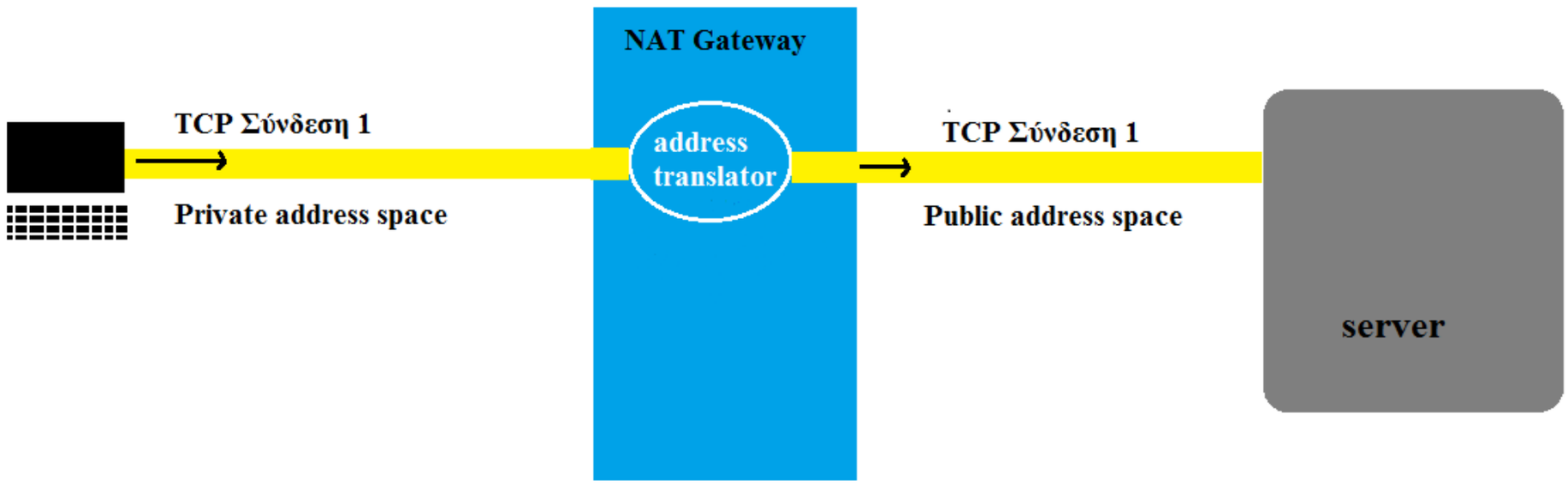
172.16.0.0 - 172.31.255.255 (Class B)

192.168.0.0 - 192.168.255.255 (Class C)

Έτσι, μπορούν ταυτόχρονα δύο διαφορετικοί υπολογιστές που ανήκουν σε διαφορετικά δίκτυα να έχουν την ίδια IP διεύθυνση (στο τοπικό ιδιωτικό του δίκτυο ο καθένας). Αυτό είναι απόλυτα θετικό να ήταν αδύνατον κάθε φορά που δημιουργούσαμε ένα τοπικό δίκτυο και αποδίδαμε διευθύνσεις στους υπολογιστές του, να εξετάζαμε αν σε κάποιο άλλο δίκτυο στον κόσμο υπάρχει κάποια κοινή διεύθυνση. Από την άλλη πλευρά όμως, αυτό το χαρακτηριστικό γίνεται μειονέκτημα όταν χρειαστεί να συνδεθούν δύο τέτοια δίκτυα σε νέο μεγαλύτερο δίκτυο που δημιουργείται, είναι πιθανό να βρεθούν δύο υπολογιστές με την ίδια IP διεύθυνση, αυτό βέβαια δεν πρέπει να επιτραπεί να συμβεί. Το παραπάνω λοιπόν είναι ένα πρόβλημα που συναντά κανείς κατά τη διασύνδεση δύο τοπικών δικτύων για την υλοποίηση ενός μεγαλύτερου VPN. Δύο είναι οι βασικοί τρόποι να αντιμετωπιστεί: η χρήση proxy server ή το πρωτόκολλο Network Address Translation (NAT).

4.7.1 Το πρωτόκολλο Network Address Translation

Το NAT (Network Address Translation) είναι ειδικό πρωτόκολλο που εκτελούν οι δρομολογητές και έχει σαν αποτέλεσμα να αλλάζει την IP διεύθυνση ενός πακέτου που ξεκινά από έναν υπολογιστή εντός του τοπικού δικτύου και προωθείται εκτός του δικτύου. Δεν δημιουργείται μία νέα TCP σύνδεση από τον Network Translator , βλέπε το ακόλουθο σχήμα:



Πιο συγκεκριμένα, το NAT δουλεύει ως εξής:

Κάθε υπολογιστής ενός ιδιωτικού δικτύου που ζητάει να συνδεθεί με κάποιον εκτός δικτύου, κάνει αίτηση στον Network Address Translator (που υπάρχει στην πύλη) για να πάρει μία νέα διεύθυνση. Ο NAT διαθέτει ένα σύνολο δημόσιων IP διευθύνσεων και μια από αυτές την αναθέτει στον υπολογιστή. Ταυτόχρονα, διατηρεί μία βάση δεδομένων στην οποία καταγράφει τη διεύθυνση που απέδωσε σε κάθε υπολογιστή. Έτσι κάθε πακέτο που φεύγει από τον υπολογιστή του ιδιωτικού δικτύου και «μεταδίδεται» στο διαδίκτυο έχει σαν διεύθυνση αποστολέα τη νέα αυτή διεύθυνση. Αντίστροφα κάθε υπολογιστής που θέλει να στείλει δεδομένα στον συγκεκριμένο υπολογιστή του ιδιωτικού δικτύου, στέλνει πακέτα με διεύθυνση παραλήπτη τη νέα διεύθυνση. Ο NAT είναι πάλι υπεύθυνος σε αυτήν την περίπτωση για να παραλάβει ο υπολογιστής τα πακέτα που προορίζονται για αυτόν. Συγκεκριμένα ο NAT κοιτάει τη βάση δεδομένων και βλέπει ποια είναι η πραγματική IP διεύθυνση του υπολογιστή (δηλαδή η διεύθυνση που έχει στο ιδιωτικό του δίκτυο) και με βάση αυτήν την πληροφορία, δρομολογεί τα εισερχόμενα πακέτα.

4.8 Domain Name Service (DNS)

Η μεγάλη διάδοση των δικτύων υπολογιστών τα τελευταία χρόνια, έκανε επιτακτική την ανάγκη δημιουργίας μιας διαφορετικής μορφής διευθύνσεων οι οποίες να είναι πιο εύκολες στη χρήση τους .Είναι πολύ πιο δύσκολο για κάποιον να απομνημονεύσει μια διεύθυνση της μορφής 196.109.82.61 , όλοι όμως μπορούν να μάθουν τη διεύθυνση **www.chania.teicrete.gr**. Για αυτό το λόγο πολύ σπάνια

χρησιμοποιούμε τη διεύθυνση IP στη δεκαδική της μορφή και σχεδόν πάντοτε επικοινωνούμε με τους άλλους υπολογιστές δίνοντας μια συμβολική διεύθυνση που είναι πιο εύκολο να απομνημονευθεί.

Το πρωτόκολλο IP φυσικά δε γνωρίζει τίποτα για αυτές τις συμβολικές διευθύνσεις και χρησιμοποιεί για τη λειτουργία του τις δεκαδικές διευθύνσεις IP. Θα πρέπει λοιπόν να υπάρχει ένας μηχανισμός, ο οποίος να δέχεται ως είσοδο τη συμβολική διεύθυνση του υπολογιστή στον οποίο θέλουμε να συνδεθούμε και να τη μεταφράζει στην αντίστοιχη δεκαδική διεύθυνση και αντίστροφα. Πράγματι ο μηχανισμός αυτός υπάρχει και είναι γνωστός με το όνομα Domain Name Service (DNS). Επομένως μέσω της υπηρεσίας αυτής είναι δυνατή η πρόσβαση στο δίκτυο με ένα πιο εύκολο και ταυτόχρονα πιο αποδοτικό τρόπο. Ένα εύλογο ερώτημα που θα μπορούσε να υποβληθεί στο σημείο αυτό αφορά τον τρόπο μετάφρασης των πραγματικών σε συμβολικές διευθύνσεις και αντίστροφα.

Πως είναι δυνατόν ο μηχανισμός DNS να γνωρίζει ποια είναι η συμβολική διεύθυνση που αντιστοιχεί σε κάποια διεύθυνση IP? Η απάντηση είναι ότι υπάρχουν διασκορπισμένες σε όλο τον κόσμο τεράστιες βάσεις δεδομένων, οι οποίες περιέχουν ζεύγη της μορφής (συμβολική διεύθυνση – πραγματική διεύθυνση). Όταν λοιπόν ο μηχανισμός DNS δέχεται ως είσοδο κάποια διεύθυνση IP, συνδέεται σε κάποια από αυτές τις βάσεις και αναζητά σε αυτή το ζεύγος που περιλαμβάνει τη διεύθυνση IP που του έχει δοθεί και εμφανίζει την αντίστοιχη συμβολική διεύθυνση. Το ίδιο ακριβώς συμβαίνει και κατά τη μετάφραση μιας συμβολικής διεύθυνσης σε διεύθυνση IP. Οι τεράστιες αυτές αποθηκευμένες σε ειδικούς υπολογιστές με αποθηκευτικές διατάξεις μεγάλης χωρητικότητας οι οποίοι ονομάζονται DNS servers. Ως υπολογιστές του δικτύου θα έχουν και αυτοί τη δική τους διεύθυνση IP η οποία επομένως θα πρέπει να δηλωθεί στο λειτουργικό σύστημα προκειμένου αυτό να γνωρίζει που να αναζητεί αυτούς τους υπολογιστές έτσι ώστε να συνδεθεί μαζί τους. Συνήθως καθορίζουμε δύο ή περισσότερες τέτοιες διευθύνσεις (primary DNS και secondary DNS) έτσι ώστε όταν ο ένας από τους υπολογιστές αυτούς δε μπορεί να μας εξυπηρετήσει για κάποιο λόγο να απευθυνόμαστε σε κάποιον άλλο υπολογιστή .

Με λίγα λόγια θα μπορούσαμε να πούμε ότι το Domain Name Service αποτελεί μια υπηρεσία μετάφρασης μεταξύ ονομάτων και IP διευθύνσεων στο διαδίκτυο. Κάθε δρομολογητής και κάθε υπολογιστής στο διαδίκτυο διαθέτει ένα όνομα. Η ιεραρχία ονομάτων περιλαμβάνει ονόματα υπολογιστών, εταιριών, δικτύων χωρών ή και ευρύτερων περιοχών (domain).

Για παράδειγμα το υποθετικό όνομα του εταιρικού δικτύου artemis.otenet.gr ακολουθεί την ιεραρχία της εταιρίας (artemis) , του δικτύου που την εξυπηρετεί (otenet) και της ευρύτερης περιοχής (gr). Το τελευταίο συστατικό του ονόματος χαρακτηρίζει το υψηλότερο επίπεδο ομαδοποίησης που διακρίνεται σε δύο μεγάλες κατηγορίες, τα γενικού τύπου domain και τα γεωγραφικά.

Τα γενικού τύπου domain είναι:

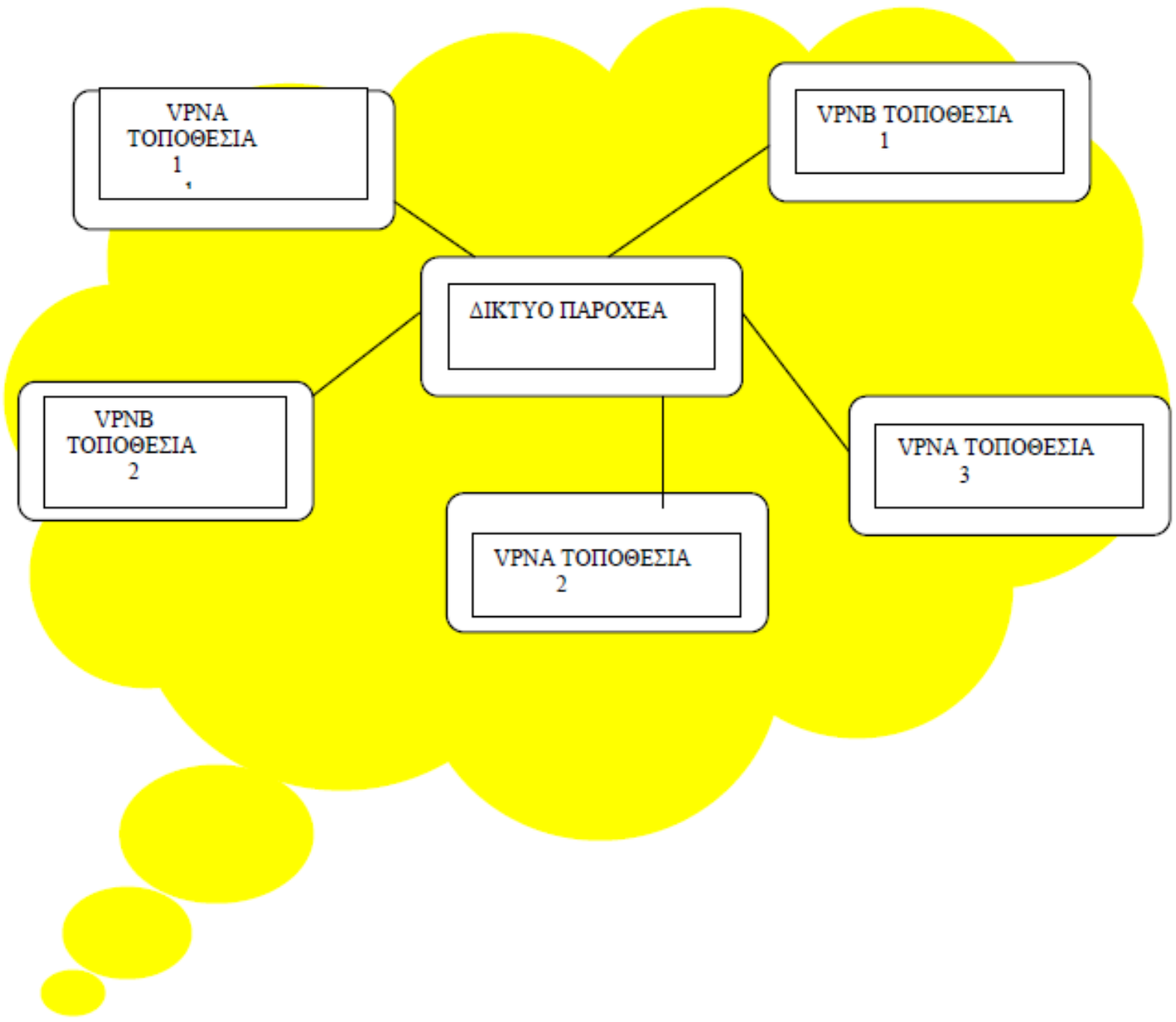
- Com (commercial – εμπορικά)
- Edu (educational – ακαδημαϊκά)
- Org (organizational – οργανισμοί μη κερδοσκοπικού χαρακτήρα)
- Net (network providers – πάροχοι δικτύου)
- Mil (military – κυρίες Αμερικάνικες στρατιωτικές υπηρεσίες)
- Gov (government – Αμερικάνικες κυβερνητικές υπηρεσίες)
- Int (international – διεθνείς οργανισμοί) [7]

Κεφαλαιο 5: VPN

Ως ιδεατό ιδιωτικό δίκτυο VPN (Virtual Private Network) ορίζεται ένα δίκτυο που διασυνδέει διαφορετικά απομακρυσμένα δίκτυα πάνω από κοινή υποδομή (π.χ. ίντερνετ), παρέχοντας το ίδιο επίπεδο ασφαλείας, διαχείρισης και απόδοσης με ένα ιδιωτικό δίκτυο. Τα ιδεατά ιδιωτικά δίκτυα υλοποιούν την λογική διασύνδεση πολλών απομακρυσμένων δικτύων, έτσι ώστε όλα μαζί να αποτελούν ένα ενιαίο δίκτυο ανεξάρτητα από την τοποθεσία τους.

Για να κατανοήσουμε καλύτερα την έννοια του ιδεατού ιδιωτικού δικτύου ας θεωρήσουμε μια επιχείρηση που διαθέτει ένα σύνολο από γεωγραφικά κατανεμημένα υποκαταστήματα. Για την επικοινωνία αυτών των υποκαταστημάτων η επιχείρηση χρειάζεται να υλοποιήσει ένα δίκτυο. Το δίκτυο αυτό είναι ιδιωτικό (private) με την έννοια ότι η δρομολόγηση της πληροφορίας και το πλάνο διευθυνσιοδότησης των συσκευών μέσα στο δίκτυο, είναι εντελώς ανεξάρτητα από την δρομολόγηση και το πλάνο διευθυνσιοδότησης που χρησιμοποιούνται σε άλλα δίκτυα. Το δίκτυο αυτό είναι ιδεατό με την έννοια ότι οι εγκαταστάσεις που χρησιμοποιούνται τόσο για την λειτουργία όσο και για την διαχείριση αυτού, μπορεί να μην είναι αφιερωμένες αποκλειστικά σε αυτήν την επιχείρηση, αλλά μπορεί και να μοιράζονται και με άλλες επιχειρήσεις που επιθυμούν και αυτές το δικό τους δίκτυο VPN.

Οι εγκαταστάσεις και τα μέσα μετάδοσης που απαιτούνται για την υποδομή ενός τέτοιου δικτύου παρέχονται συνήθως από κάποιον πάροχο ο οποίος καλείται πάροχος υπηρεσιών VPN (VPN Service Provider), ενώ η επιχείρηση ή ο οργανισμός ή ο ιδιώτης οποιασδήποτε νομικής μορφής που χρησιμοποιεί αυτό το δίκτυο καλείται πελάτης VPN (VPN CUSTOMER).



Στην παραπάνω εικόνα το δίκτυο του πάροχου μπορεί να υποστηρίξει μέσα από την ίδια υποδομή δύο δίκτυα VPN που ανήκουν σε διαφορετικούς πελάτες. Επίσης είναι δυνατή και η επικοινωνία των δύο πελατών μεταξύ τους.

Ένα δίκτυο VPN καθορίζεται από ένα σύνολο διεργασιών οι οποίες ελέγχουν τόσο τις διασυνδέσεις σε φυσικό και λογικό επίπεδο, όσο και το επίπεδο της παρερχόμενης ποιότητας υπηρεσίας (QoS) μεταξύ των διαφορετικών υπηρεσιών.

Τα δίκτυα VPN αποτελούν εξέλιξη των ιδιωτικών δικτύων δεδομένων (Private Networks) που είχαν αναπτύξει πολλές επιχειρήσεις στο παρελθόν, όπως για παράδειγμα οι τραπεζικοί οργανισμοί τα οποία στηρίζονται στη μίσθωση γραμμών μεταφοράς και στη χρήση των πρωτοκόλλων Frame Relay και ATM για την μεταφορά της πληροφορίας. Το κόστος υλοποίησης και συντήρησης αυτών των δικτύων είναι αρκετά υψηλό ανάλογα βέβαια και με το μέγεθός τους. Σήμερα τα VPN παρέχουν υψηλή διαθεσιμότητα και κλιμάκωση, ενώ υποστηρίζουν πολλά πρωτόκολλα δρομολόγησης και μεταφοράς δεδομένων (IP, Frame Relay , ATM).[8]

5.1 TUNNELING

Το tunneling είναι το κυριότερο χαρακτηριστικό των VPNs. Τα περισσότερα VPN βασίζονται σε αυτήν την διαδικασία προκειμένου να επικοινωνούν μεταξύ τους μέσω του διαδικτύου. Πρόκειται για τη διαδικασία κατά την οποία δημιουργείται μια ειδική σύνδεση μεταξύ δύο σημείων. Ο αποστολέας κάνοντας χρήση ειδικού εξοπλισμού ενσωματώνει τα IP πακέτα σε άλλα πακέτα (μια διαδικασία που καλείται encapsulation) και με αυτόν τον τρόπο ταξιδεύουν μέσω του διαδικτύου. Τα μεγαλύτερα αυτά πακέτα έχουν νέο IP header και κρυπτογράφηση. Όταν τελικά τα πακέτα φτάσουν στον προορισμό τους ο παραλήπτης τα δέχεται γίνεται η αποκρυπτογράφηση και παραδίδεται το αρχικό πακέτο. Κατά τη στιγμή που ο παραλήπτης τα δέχεται, αφαιρείται η πρόσθετη επικεφαλίδα, γίνεται η αποκρυπτογράφηση και παραδίδεται το αρχικό πακέτο.

Υπάρχουν δύο κύριες αρχιτεκτονικές στη διαδικασία tunneling:

- Client-initiated: Η περίπτωση αυτή απαιτεί ειδικό λογισμικό και από τα δύο σημεία επικοινωνίας τον client και τον server (ή gateway). Ο client ανοίγει το tunnel το οποίο και τερματίζεται στην πλευρά της επιχείρησης. Ο ISP δεν μετέχει στο tunneling. Χρησιμοποιείται πιστοποίηση (authentication) με IDs και passwords ή με άλλου είδους ψηφιακές υπογραφές. Από τη στιγμή όμως που δημιουργείται το tunnel ο Internet Service Provider είναι σαν να μην υπάρχει καθόλου.

- Client-transparent: Εδώ ο ISP παίζει ενεργό ρόλο αντίθετα με την πρώτη περίπτωση καθώς θα πρέπει να έχει ειδικούς servers ή δρομολογητές που να υποστηρίζουν ειδικά πρωτόκολλα tunneling. Η διαδικασία έχει ως εξής: Ο client συνδέεται με τον ISP δηλώνοντας ότι επιθυμεί να συνδεθεί με συγκεκριμένη τοποθεσία και με ειδική σύνδεση δηλ. tunneling (αυτό μπορεί να γίνει και αυτόματα βάση στοιχείων που εμπεριέχονται στο user-ID). Στη συνέχεια ο Network Access Server NAS εγκαθιστά σύνοδο (session) με τον tunnel server στην επιχείρηση. Εδώ υπάρχει το πλεονέκτημα ότι δεν είναι απαραίτητο ο client να έχει ειδικό λογισμικό εγκατεστημένο.

Το tunneling απαιτεί τρία διαφορετικά πρωτόκολλα:

- Carrier Protocol – Το πρωτόκολλο που χρησιμοποιείται από το δίκτυο επιβεβαιώνοντας πως η πληροφορία ταξιδεύει
- Encapsulating Protocol – Το πρωτόκολλο (GRE, IPSec, L2F, PPTP, L2TP) το οποίο είναι τυλιγμένο γύρω από τα αρχικά δεδομένα
- Passenger Protocol – Τα πραγματικά δεδομένα (IP) τα οποία μεταφέρονται.

Παρόλο που η τεχνολογία VPN είναι σχετικά καινούργια υπάρχουν ήδη αρκετά πρωτόκολλα που λειτουργούν κυρίως στο δεύτερο, τρίτο και πέμπτο επίπεδο του μοντέλου OSI. Επίσης παρόλο που χωρίζονται σε πρωτόκολλα που ασχολούνται με το tunneling και την ασφάλεια και σε πρωτόκολλα που ασχολούνται με τη διαχείριση του δικτύου η διάκριση αυτή δεν είναι απόλυτη καθότι στη διαχείριση εμπλέκονται διαδικασίες κρυπτογράφησης και authentication.

Σε ένα VPN απομακρυσμένης πρόσβασης, το tunneling κανονικά λαμβάνει χώρα με την βοήθεια του PPP (Point to Point Protocol). Μέρος της δέσμης TCP/IP, το PPP είναι ο μεταφορέας για άλλα πρωτόκολλα IP όταν υπάρχει επικοινωνία πάνω στο δίκτυο μεταξύ του υπολογιστή που φιλοξενεί και το απομακρυσμένο σύστημα. Το Remote-access VPN tunneling βασίζεται στο PPP.

Όλα τα παρακάτω πρωτόκολλα χτίστηκαν χρησιμοποιώντας την βασική δομή του PPP και χρησιμοποιούνται από τα remote-access VPNs.

5.2 Το πρωτόκολλο IPSec

Θεωρείται το πιο πλήρες και ολοκληρωμένο πρωτόκολλο αφού τα άλλα (PPTP και L2TP) χρησιμοποιούν μέρη από το IPSec, αλλά επίσης γιατί έχει εφαρμογή σε LAN-to-LAN και client-to-LAN δίκτυα.

Η ανάπτυξή του ξεκίνησε γιατί διαπιστώθηκε αδυναμία των TCP/IP στον τομέα της ασφάλειας που όμως είναι πολύ σημαντική. Το IP packet είναι το βασικό συστατικό στα IP δίκτυα γιατί περιλαμβάνει πληροφορίες για την πηγή, τον προορισμό και το είδος των δεδομένων που μεταφέρει.

Το IPSec ορίζει δύο νέες επικεφαλίδες (headers) σε κάθε IP πακέτο:

- Μια επικεφαλίδα για την πιστοποίηση (Authentication Header-AH).
- Μια επικεφαλίδα για την ενθυλάκωση (Encapsulating Security Payload-ESP).

Τρία βασικά χαρακτηριστικά του είναι:

1. Ενώσεις Ασφαλείας (Security Association) SA: Πιο συγκεκριμένα καθορίζονται τα εξής:

- Ο τρόπος που χρησιμοποιείται ο αλγόριθμος κρυπτογράφησης (encryption) στο Encapsulating Security Payload (ESP) και τα κλειδιά του.
- Το είδος των αλγόριθμων και τα κλειδιά που χρησιμοποιούνται για πιστοποίηση και κρυπτογράφηση
- Η συχνότητα ανταλλαγής και τροποποίησης των κλειδιών αυτών
- Ο χρόνος ζωής τους
- Ο χρόνος ζωής ολόκληρου του SA
- Ο τρόπος που χρησιμοποιείται ο αλγόριθμος πιστοποίησης (authentication) στο Authentication Header (AH) και τα κλειδιά του.
- Η παρουσία και το μέγεθος κάθε άλλου τρόπου κρυπτογράφησης που χρησιμοποιείται μαζί με τον αλγόριθμο

Το SA μπορούμε να το φανταστούμε σαν ένα είδος σύμβασης μεταξύ δύο μελών για τη μεταξύ τους ανταλλαγή δεδομένων. Σε περιπτώσεις που μία επιχείρηση με δικό της VPN συνδέεται με μία άλλη που επίσης έχει VPN με το SA καθορίζεται ποιος έχει πρόσβαση σε ποιους πόρους του δικτύου. Επίσης υπάρχουν διαφορετικά sets SA για τους υπαλλήλους τους πωλητές ή ακόμα για διαφορετικά τμήματα της επιχείρησης. Για επιπρόσθετη ασφάλεια, κάθε Security Association (SA) δεν ισχύει για αμφίδρομη επικοινωνία αλλά για μια κατεύθυνση αποστολέα-παραλήπτη. Για να συμβεί και το αντίστροφο πρέπει να συμφωνηθεί ακόμα ένα SA.

2. Authentication Header (AH): Σχεδιάστηκε για να εξυπηρετήσει υπηρεσίες πιστοποίησης (Authentication) στα IP data και περιέχει ελέγχους κρυπτογράφησης. Μπαίνει ανάμεσα στο IP header και τα πακέτα με τα δεδομένα (payload) χωρίς να τα τροποποιεί. Περιλαμβάνει πέντε πεδία:

- το πεδίο με το Next Header
- το μήκος του payload
- το Security Parameter Index

- τον αριθμό ακολουθίας
- authentication data

Τα σημαντικά είναι το Security Parameter Index που καθορίζει ποιο είδος από πρωτόκολλα χρησιμοποιούνται και βεβαίως η πιστοποίηση των δεδομένων (authentication data). Για να αποτραπεί η υποκλοπή των δεδομένων κατά τη διάρκεια της αναμετάδοσης στο AH υπάρχει μηχανισμός antireplay που βοηθά τον μετρητή πακέτων.

3. Encapsulating Security Payload (ESP): Είναι υπεύθυνο για την κρυπτογράφηση των πακέτων. Το ESP header μπαίνει ανάμεσα στην IP header και των πακέτων με τα δεδομένα τα οποία όμως και τα τροποποιεί. Περιλαμβάνει τα εξής πεδία:

- το Security Parameter Index που δηλώνει στον δέκτη ποια ένωση ασφαλείας είναι SA είναι καταλληλότερη για το συγκεκριμένο πακέτο
- τον αριθμό ακολουθίας, που προσφέρει προστασία από υποκλοπή κατά τη μετάδοση και αποτρέπει σύγχυση κατά την παραλαβή.
- authentication data

Συνοψίζοντας για το IPSec Protocol θα σημειώναμε ότι θεωρείται ένας πλήρες πρωτόκολλο αφού περιλαμβάνει έναν αριθμό από αλγορίθμους πιστοποίησης και κρυπτογράφησης καθώς επίσης είναι έτοιμο για μελλοντικές τροποποιήσεις (flexibility, scalability).

5.3 Το πρωτόκολλο PPTP

Το **P**oint-to-**P**oint **T**unneling **P**rotocol **(PPTP)** δημιουργήθηκε από ομάδα εταιριών που ονομάστηκε PPTP Forum. Συμμετείχαν η Microsoft, η 3Com, η US Robotics και η Ascend Communications. Η βασική ιδέα ήταν να δημιουργηθούν οι προϋποθέσεις για την εύκολη και με ασφάλεια πρόσβαση απομακρυσμένων χρηστών με τα εταιρικά τους δίκτυα, μέσω τοπικού ISP. Βασίστηκε στο PPP που χρησιμοποιείται ευρέως

στο διαδίκτυο. Τα PPP πακέτα ενσωματώνονται με τη βοήθεια ενός άλλου πρωτοκόλλου του **G**eneric **R**outing **E**ncapsulation **GRE**).

Το PPTP περιμένει από το PPP να κάνει τις εξής ενέργειες:

- Σύνδεση και τερματισμό της φυσικής σύνδεσης.
- Πιστοποίηση ταυτότητας χρήστη
- Δημιουργία PPP datagrams

Αμέσως μετά το PPTP κάνει την ενθυλάκωση και ορίζει δύο διαφορετικούς τύπους πακέτων τα control packets και τα data packets και τα στέλνει με διαφορετικά κανάλια τα πρώτα μέσω TCP και τα δεύτερα μέσω IP. Τα data πακέτα περιέχουν τα δεδομένα ενώ τα control πακέτα περιέχουν στοιχεία για τη σύνδεση ή πληροφορίες για την διαχείριση (management) και τη διαμόρφωση (configuration) μεταξύ των δύο συνδεδεμένων άκρων. Υπάρχει η δυνατότητα για τη δημιουργία διαφορετικών τύπων tunnels ανάλογα με τη δυνατότητα του client και του ISP. Έχει ευκολία στη διαχείριση και υποστήριξη πολλών διαφορετικών πλατφόρμων λειτουργικών στους απομακρυσμένους χρήστες. Άλλο σημαντικό του στοιχείο είναι ότι χρησιμοποιώντας RADIUS servers από την πλευρά του ISP προσφέρει αρκετά καλή ασφάλεια που πάντα είναι ζητούμενο.

Το πρωτόκολλο L2F

Το 1996 η Cisco έκανε τη δική της πρόταση, το πρωτόκολλο **L**ayer **T**wo **F**orwarding **(L2F)**. Για τη χρήση του χρειάζεται την ύπαρξη Access Server και Router (δρομολογητή). Επίσης πρέπει ο εξοπλισμός του ISP να το υποστηρίζει. Επιτρέπει πάνω από μία ταυτόχρονες συνδέσεις κατά τη δημιουργία των tunnel. Χρησιμοποιεί το PPP για την πιστοποίηση ταυτότητας του χρήστη. Έχει δύο επίπεδα πιστοποίησης: το πρώτο από το ISP όταν δημιουργεί το tunnel και το δεύτερο όταν γίνεται η σύνδεση με την επιχείρηση.

5.4 Το πρωτόκολλο L2TP

Τα δύο πρωτόκολλα PPTP και L2F και ύστερα από συμφωνία των εταιριών που τα ανέπτυξαν ενώθηκαν δημιουργώντας το **L**ayer **T**wo **T**unneling **P**rotocol **(L2TP)**. Θεωρείται το νέο όπλο στα VPNs.

Συνδυάζει πολλά χαρακτηριστικά και πλεονεκτήματα άλλων πρωτοκόλλων και επίσης την υποστήριξη μεγάλων εταιριών. Βασίζεται στο PPTP και L2F. Είναι ευέλικτο μιας και λειτουργεί στο Δεύτερο επίπεδο του μοντέλου OSI , δίνει τη δυνατότητα χρήσης στο ATM και Frame Relay.

Επειδή χρησιμοποιεί PPP για τις dial-up συνδέσεις συμπεριλαμβάνει τους μηχανισμούς του για την πιστοποίηση καθώς επίσης και άλλους επιπρόσθετους όπως το IPSec. Η διαδικασία έχει ως εξής: το PPP είναι αυτό που αναλαμβάνει να γίνει η σύνδεση , εκτελεί την πρώτη φάση πιστοποίησης του χρήστη και δημιουργεί τα datagrams. Εδώ αναλαμβάνει το L2TP, αρχικά επιβεβαιώνει ότι ο εταιρικός server πιστοποιεί την ταυτότητα του remote user και ότι του επιτρέπει τη δημιουργία του tunnel. Όταν το tunnel δημιουργηθεί κάνει ενθυλάκωση των PPP πακέτων που μεταδίδονται μέσω του ISP. Επειδή υπάρχει η δυνατότητα για παράλληλη ύπαρξη πολλών συνδέσεων στο ίδιο tunnel, κάθε πακέτο εφοδιάζεται με ένα Call ID που τοποθετείται στην επικεφαλίδα του και χρησιμεύει σαν αναγνωριστικό. Αν πάλι δημιουργηθούν πολλά παράλληλα tunnels τότε επίσης μπαίνει κάποιο αναγνωριστικό που βοηθά τον server της επιχείρησης και αποτρέπει τα λάθη παραλαβής πακέτων.

Όμοια με το PPTP ορίζει δύο διαφορετικούς τύπους πακέτων τα control packets και τα data packets τα στέλνει όμως με ίδιο κανάλι. Τα data πακέτα περιέχουν τα δεδομένα είναι δηλαδή τα αυθεντικά PPP πακέτα του αλλά έχουν και πληροφορίες για το μέσο μετάδοσης (Ethernet, frame relay, ATM) ενώ τα control πακέτα περιέχουν στοιχεία για τη σύνδεση ή πληροφορίες για διαχείριση (management) και διαμόρφωση (configuration) μεταξύ των δύο συνδεδεμένων άκρων.

Το L2TP δίνει τη δυνατότητα δημιουργίας δύο τρόπων tunneling.

- **Voluntary tunnels:** Τα voluntary tunnels δημιουργούνται από τον τελικό χρήστη. Ο χρήστης μπορεί ταυτόχρονα να ανοίξει και άλλη σύνδεση χωρίς tunneling με TCP/IP για το διαδίκτυο.

- **Mandatory tunnels:** Τα mandatory tunnels είναι user transparent δημιουργούνται δηλαδή εν’ αγνοία του χρήστη κατά τη διάρκεια της σύνδεσης με τον ISP. Οι συνδέσεις αυτές όμως έχουν προκαθορισμένα άκρα και ως εκ τούτου ο client δεν μπορεί να περιηγηθεί στο Internet. Έχουν το πλεονέκτημα της εύκολης διαχείρισης και της μη φόρτωσης του εσωτερικού δικτύου αλλά και το μειονέκτημα της ασφάλειας αφού το Secure tunnel αρχίζει από τον ISP και μετά.

Συμπερασματικά θα σημειώναμε πως το L2TP ή το πρωτόκολλο του μέλλοντος για τα VPNs όπως το ονομάζουν συγκεντρώνει τα καλύτερα χαρακτηριστικά των PPTP και L2F. Σημαντικό του πλεονέκτημα είναι πως μπορεί να εφαρμοστεί πάνω σε πολλά δίκτυα όπως Frame Relay, ή ATM έτσι προσφέρει ευελιξία στον σχεδιασμό και επίσης στην ασφάλεια επειδή

Το L2TP μπορεί να χρησιμοποιηθεί ως πρωτόκολλο tunneling για Εικονικά Ιδιωτικά Δίκτυα τύπου site-to-site καθώς επίσης ως remote-access VPNs. Ακριβέστερα, το L2TP μπορεί να δημιουργήσει tunnel μεταξύ:

- Πελάτη και δρομολογητή
- Δρομολογητή και δρομολογητή [9]

5.5 Ασφάλεια των δρομολογητών για τη πιστοποίηση ταυτότητας χρήστη chap με ppp

Η ταυτοποίηση χρησιμοποιείται στα VPNs για να εξασφαλίσει τα μέρη που επικοινωνούν και ανταλλάσουν πληροφορίες με το σωστό χρήστη ή μηχάνημα. Τα περισσότερα συστήματα ταυτοποίησης που χρησιμοποιούνται βασίζονται στο σύστημα διαμοίρασης κλειδιού (shared key). Αυτά τα κλειδιά περνούν από ένα αλγόριθμο κωδικοποίησης σύνοψης (one way hash algorithm) και προκύπτει μία τιμή σύνοψης (hash value) η οποία αποστέλλεται στον αποδέκτη. Ο αποδέκτης που έχει στην κατοχή του τον αλγόριθμο κωδικοποίησης θα παράγει μία τιμή σύνοψης (hash value) και θα την συγκρίνει με αυτήν που στάλθηκε από τον αποστολέα. Το αποτέλεσμα της κωδικοποίησης σύνοψης (hash value) το οποίο στάλθηκε μέσω του διαδικτύου δεν έχει αξία για τον πιθανό εξωτερικό παρατηρητή οπότε διασφαλίζεται η ταυτοποίηση της επικοινωνίας. Η ταυτοποίηση τυπικά γίνεται στην αρχή της συνεδρίας και ύστερα σε τυχαίες χρονικές στιγμές κατά την διάρκεια της συνεδρίας, ώστε να εξασφαλίσει ότι κάποιος εισβολέας δεν εισχώρησε στην επικοινωνία . Ένα τυπικό παράδειγμα μεθόδου ταυτοποίησης είναι το CHAP (Challenge Handshake Authentication Protocol).[10]

Συμπέρασμα ότι τα πρωτόκολλα PPTP και L2F επιτρέπουν να χρησιμοποιηθεί όποια μέθοδος ταυτοποίησης χρησιμοποιεί και το PPP , συμπεριλαμβανομένων των PAP και CHAP. Το πρωτόκολλο L2TP μπορεί να χρησιμοποιηθεί στη θέση των PPTP και L2F και μπορεί να εφαρμόσει τις ίδιες μεθόδους ταυτοποίησης ενώ σαν μέθοδος κρυπτογράφησης προτιμάται το IPSec.

Κεφάλαιο 6: Δρομολογητές xDSL

Το Wireless D-Link GO-DSL-N150 Router είναι μια συσκευή που χρησιμοποιεί ADSL2 / 2 + σύνδεση. Ο δρομολογητής παρέχει τείχος προστασίας για πρόσθετη ασφάλεια, και Quality of Service (QoS) για ομαλό online gaming, media streaming και φωνητική επικοινωνία με πρωτόκολλα μεταφοράς δεδομένων PPTP,L2TP,IPsec.

Το Belkin Surf N150 F9J1001AS έχει τη δυνατότητα επέκτασης χρήσης του ασύρματου δικτύου με ταχύτητα έως 150Mbps. Διαθέτει τείχος προστασίας και έχει πρωτόκολλο δρομολόγησης static IP, πρωτόκολλο μεταφοράς δεδομένων IPsec, L2TP, PPTP, TCP/IP και άλλο ένα χαρακτηριστικό του είναι πως υποστηρίζει Network Address Translation(NAT).

Ο δρομολογητής TP-Link AC1750 Wireless Dual Band διαθέτει 2 θύρες USB 2.0 για την σύνδεση στο τοπικό δίκτυο και κοινόχρηστων συσκευών, όπως εκτυπωτές. Οι χρήστες μπορούν να έχουν 10 φορές μεγαλύτερη ταχύτητα σε ενσύρματο δίκτυο και μέχρι και 4 φορές μεγαλύτερη ταχύτητα σε ασύρματο δίκτυο. Παρέχει πρωτόκολλο δρομολόγησης Dynamic IP/Static IP, L2TP/PPTP, πρωτόκολλο μεταφοράς δεδομένων TCP/IP, PPTP, L2TP, IPsec, DHCP, DNS. Τέλος υποστηρίζει Dynamic Host Configuration Protocol(DHCP), Network Address Translation(NAT), Virtual Private Network(VPN) και διαθέτει συνολικά 6 ξεχωριστές κεραίες, 3 εξωτερικές των 5dBi για το ασύρματο δίκτυο 5GHz και 3 εσωτερικές για το ασύρματο δίκτυο 2.4GHz, οι χρήστες μπορούν να συνδεθούν σε όποιο ασύρματο δίκτυο υποστηρίζουν χωρίς παρεμβολές.[11]

6.1 Σύγκριση δρομολογητών

Δρομολογητές	**1)D-Link GO-DSL-N150**	**2)Belkin Surf N150 F9J1001AS**	**3)TP-Link AC1750 Wireless Dual Band**
Πρωτόκολλο δρομολόγησης	**Static IP**	**Static IP**	**Dynamic IP/Static IP,**
Πρωτόκολλο μεταφοράς δεδομένων	**TCP/IP, PPTP, L2TP, IPsec**	**IPsec, L2TP, PPTP, TCP/IP**	**TCP/IP, PPTP, L2TP, IPsec, DNS**
Άλλα Χαρακτηριστικά		**NAT support**	**Firewall, DHCP support, NAT support, VPN** ✓ **Διαθέτει Dual Band, 3 εξωτερικές κεραίες των 5GHz και 3 εσωτερικές για τα 2.4GHz**

Επίλογος

Κατά την εκπόνηση της πτυχιακής μου εργασίας κατανόησα την τεχνολογία xDSL που χωρίζεται σε δυο κατηγορίες, τα συμμετρικά και ασύμμετρα DSL, από τι αποτελείται και τα τεχνικά χαρακτηριστικά της. Κατόπιν γνώρισα καλύτερα τις τεχνολογίες ADSL & VDSL, το πως λειτουργούν και τη δομή τους από τον πάροχο έως το σπίτι. Ανέλυσα την σχέση του ρυθμού μετάδοσης σε Mbps που έχει η κάθε τεχνολογία ως προς την απόσταση από τον πάροχο και έπειτα σύγκρινα την VDSL με την ADSL σε πλεονεκτήματα και μειονεκτήματα. Στη συνέχεια της πτυχιακής, επεξεργάστηκα το εσωτερικό του δρομολογητή και ανέλυσα τις τεχνικές της δρομολόγησης, τις διευθύνσεις IP και υπηρεσίες σαν το τείχος προστασίας που προστατεύουν από κακόβουλα λογισμικά κ.τ.λ. Επικεντρώθηκα στα πρωτόκολλα επικοινωνίας, την εφαρμογή τους, τη λειτουργία τους και ανέλυσα ενδεικτικά το Point-to-Point Tunneling Protocol (PPTP),το Layer Two Forwarding (L2F), το Layer Two Tunneling Protocol (L2TP). Προς το τέλος έκανα μία αναφορά στη διαιδκασία πιστοποίησης χρηστών στους δρομολογητές μέσω μηχανισμού chap σε πρωτόκολλο ppp. Η πτυχιακή μου εργασία ολκληρώθηκε με μια συνοπτική σύγκριση συγκεκριμένων μοντέλων δρομολογητών που χρησιμοποιούνται αυτή την περίοδο στην Ελληνική Αγορά.

ΒΙΒΛΙΟΓΡΑΦΙΕΣ-ΔΙΑΔΙΚΤΥΑΚΕΣ ΠΗΓΕΣ

[1] http://brain.ee.auth.gr/dokuwiki/doku.php?id=dsl:dsl

[2] ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ <<ΜΕΛΕΤΗ ΣΥΓΧΡΟΝΗΣ ΤΕΧΝΟΛΟΓΙΑΣ VDSL>>. Τ.Ε.Ι. ΗΠΕΙΡΟΥ, Ονοματεπώνυμο Φοιτητή: ΖΕΡΒΑ ΑΛΕΞΑΝΔΡΑ, Ονοματεπώνυμο Καθηγητή: ΒΑΣΙΛΕΙΑΔΗΣ ΔΗΜΗΤΡΙΟΣ.

[3]https://el.wikipedia.org/wiki/%CE%94%CF%81%CE%BF%CE%BC%CE%BF%CE%BB%CE%BF%CE%B3%CE%B7%CF%84%CE%AE%CF%82

[4] Δυναμική δρομολόγηση. Εργασία στα πλαίσια του μαθήματος <<Δίκτυα Δημόσιας Χρήσης και Διασύνδεση Δικτύων>>. Πανεπιστήμιο Πάτρας, Ονοματεπώνυμο Φοιτητή: Κόνδης Βλάσιος - Κουτρόπουλος Παναγιώτης

[5] http://thebook.homeunix.com/node108.html

[6]https://el.wikipedia.org/wiki/Firewall

[7]http://diktia.weebly.com/uploads/6/4/5/1/6451366/_protokolla_epikoinonias.pdf

[8] ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ << ΑΣΦΑΛΗΣ ΜΕΤΑΦΟΡΑ ΔΕΔΟΜΕΝΩΝ ΜΕ ΤΗΝ ΧΡΗΣΗ ΙΔΕΑΤΩΝ ΙΔΙΩΤΙΚΩΝ ΔΙΚΤΥΩΝ>>. Τ.Ε.Ι. ΗΠΕΙΡΟΥ. ΑΘΗΝΑ 25/09/2006,Ονοματεπώνυμο Φοιτητή: ΣΚΟΡΔΑ ΧΡΙΣΤΙΝΑ-ΓΙΑΝΝΑΚΟΥΔΑΚΗΣ ΝΙΚΟΛΑΟΣ,Ονοματεπώνυμο Καθηγητή: ΤΣΙΑΝΤΗΣ ΛΕΩΝΙΔΑΣ

[9] ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ << Διαχείριση κινητικότητας και ασφάλειας σε ασύρματα Εικονικά Ιδιωτικά Δίκτυα>>. ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ. Αθήνα, Ιούλιος 2004, Ονοματεπώνυμο Φοιτητή: ΚΩΝΣΤΑΝΤΙΝΙΔΗΣ Χ. ΑΡΙΣΤΟΤΕΛΗΣ-RONY J. EL ALAM, Ονοματεπώνυμο Καθηγητή: Μιχαήλ Θεολόγου

[10] ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ Τεχνολογίες ψηφιακών ραδιο-δικτύων υψηλής ταχύτητας IEEE 802.11 <<Διασύνδεση και ασφάλεια υπολογιστών>>, ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ. Ονοματεπώνυμο Φοιτητή: Νούκας Κωνσταντίνος – Παππή Χρίστο, Ονοματεπώνυμο Καθηγητή: Δημήτρης Μητράκος, ΘΕΣΣΑΛΟΝΙΚΗ 2006

[11]http://www.public.gr/product/perifereiaka/networking/access-points-routers-wi-fi-extenders/tp-link-ac1750-wireless-dual-band-gigabit-router-asyrmato-royter/prod6270034pp/