e-HellenicAirForce

www.e-haf.org

Οδηγός aDSL για το OpenFalcon

ΠΕΡΙΕΧΟΜΕΝΑ

Συντάκτης: Κωνσταντίνος "Cannon" Οικονομίδης
Έκδοση 1η – Ιούνιος 2007

1. ΓΕΝΙΚΑ

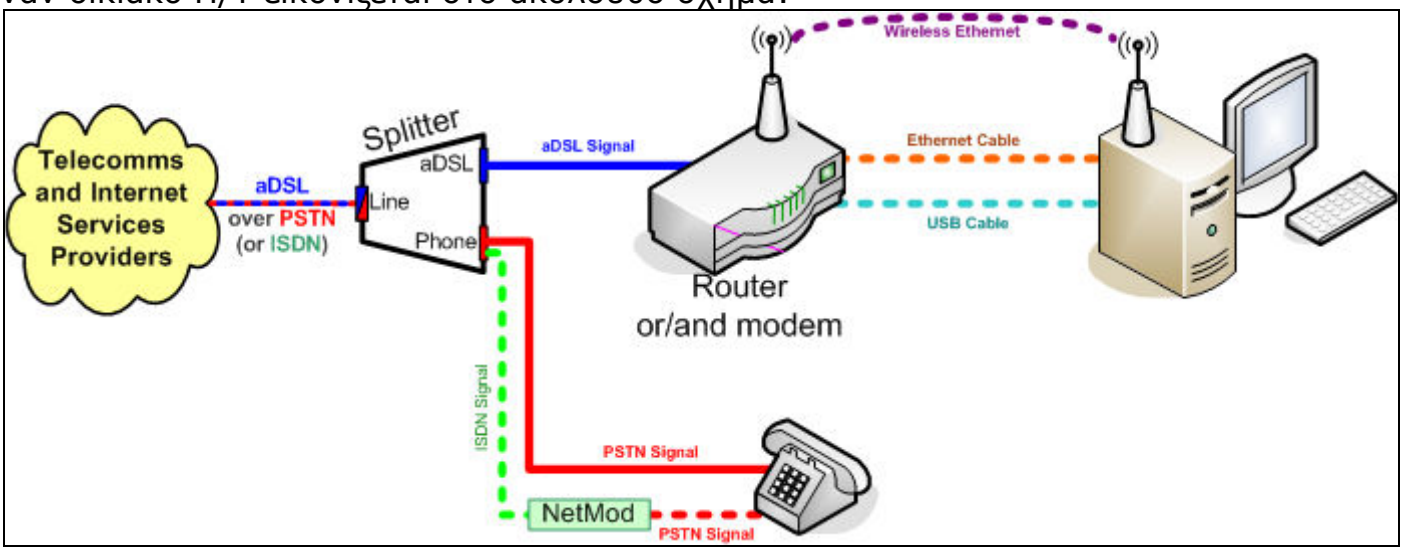
Σκοπός του παρόντος οδηγού είναι αφενός να δώσει με πολύ απλά λόγια μια σαφή εικόνα για το πώς υλοποιούνται aDSL συνδέσεις από τη μεριά του τελικού (οικιακού) χρήστη, και αφετέρου να γίνουν κατανοητές οι απαραίτητες ρυθμίσεις για την επιτυχή συνδεσιμότητα μεταξύ των μελών της e-HAF για τον εξομοιωτή OpenFalcon (OF). Τονίζεται, ότι τα παραδείγματα που χρησιμοποιούνται απευθύνονται στην πλειοψηφία του τρόπου με τον οποίο υλοποιούνται συνδέσεις aDSL στην Ελλάδα επί του παρόντος (και πιθανώς για αρκετό καιρό ακόμα). Τυχόν ιδιομορφίες κυρίως τοπικών LANs *(Local Area Networks)* πιθανώς να μην καλύπτονται πλήρως στο παρόν κείμενο.

Στις παραγράφους που ακολουθούν, εξηγούνται:

- Συνδεσμολογίες συσκευών από Η/Υ έως το Διαδίκτυο
- Σύνδεση με χρήση aDSL Modem
- Σύνδεση με χρήση aDSL Router
- Διευθυνσιοδότηση IP
- Network Address Translation (NAT)
- Port forwarding
- Firewalls
- Web interface των aDSL routers
- Χρησιμοποιούμενα ports του OF
- Απαραίτητες ρυθμίσεις συσκευών και Η/Υ για επιτυχή σύνδεση στο OF.

2. ΤΥΠΙΚΟΙ ΤΡΟΠΟΙ ΣΥΝΔΕΣΗΣ aDSL

Η πληθώρα των περιπτώσεων καλωδιακής συνδεσμολογίας μιας aDSL σύνδεσης με έναν οικιακό Η/Υ εικονίζεται στο ακόλουθο σχήμα:



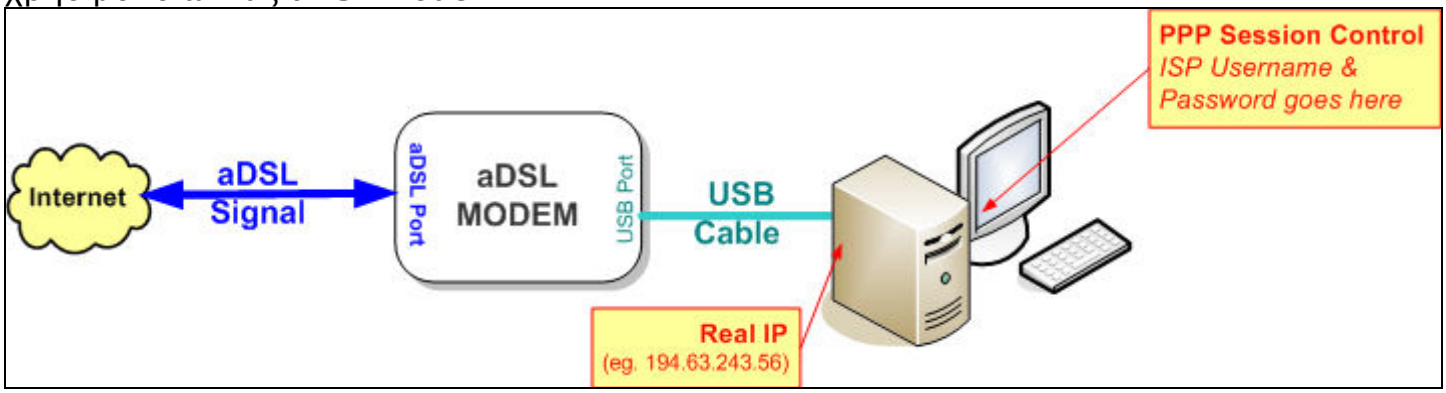
Εξηγώντας το σχήμα από αριστερά προς τα δεξιά, βλέπουμε ότι το ζεύγος του χάλκινου καλωδίου που έρχεται από τον Τηλεπικοινωνιακό Πάροχο (πχ. ΟΤΕ) προς την οικία μας, μεταφέρει σηματοδοσία aDSL καθώς και PSTN (ή ISDN). Το παθητικό φίλτρο (Splitter) αναλαμβάνει να διαχωρίσει τα δύο αυτά σήματα, κι έτσι στις δύο εξόδους του παίρνουμε διαχωρισμένα πλέον το aDSL σήμα στη μία, και στην άλλη το PSTN (ή ISDN). Για το PSTN/ISDN σήμα δεν χρειάζεται να γίνει ιδιαίτερος λόγος, καθώς μετά την έξοδο "Phone" από το splitter, μεταχειριζόμαστε τη γραμμή με τον συνήθη έως σήμερα τρόπο.

Από την έξοδο "aDSL" του splitter – η οποία και μας ενδιαφέρει- οδηγούμε αυτούσιο το aDSL σήμα σε μια συσκευή που μεσολαβεί για την τελική σύνδεση του Η/Υ μας με το Internet. Η συσκευή αυτή μπορεί να είναι Δρομολογητής (router) ή Modem. Από αυτή τη συσκευή, συνδέουμε τον Η/Υ μας είτε μέσω Ethernet (ενσύρματα ή ασύρματα) είτε μέσω USB *(Universal Serial Bus)*, ανάλογα του τί είναι διαθέσιμο και πόσο θέλουμε να επεκτείνουμε την aDSL σύνδεσή μας και με άλλους τοπικούς Η/Υ (δημιουργώντας έτσι ένα Private LAN με κοινή σύνδεση προς το Internet).

3. ΣΥΝΔΕΣΗ ΜΕ ΧΡΗΣΗ aDSL MODEM

3.1 Τοπολογία Συνδέσεων

Ο πιο απλός τρόπος σύνδεσης **ενός** Η/Υ με το Internet μέσω aDSL, είναι χρησιμοποιώντας aDSL Modem.



3.2 Διαδικασία σύνδεσης

Σε αυτή την περίπτωση το aDSL modem δρα ως ένας μετατροπέας σήματος aDSL σε σήμα USB, όπως γινόταν σε παλαιότερου τύπου συνδέσεις με αναλογικά modems που μετέτρεπαν το τηλεφωνικό σήμα σε σειριακή θύρα RS-232 ή USB. Δηλαδή, εγκαθιστούμε τους windows drivers της USB συσκευής στα Windows, δημιουργούμε εικονίδιο σύνδεσης και πληκτρολογούμε το username/password που έχουμε από τον ISP (OTEnet, Forthnet κτλ.). Η σύνδεσή μας με το Internet γίνεται κατά βούληση, όπως ακριβώς γίνεται και στα απλά αναλογικά (PSTN) ή ψηφιακά (ISDN) modems. Με άλλα λόγια, σε αυτόν τον τρόπο σύνδεσης **εμείς** καθορίζουμε πότε θα συνδεθούμε και πότε όχι με το Internet (PPP Session Control γίνεται από τα Windows με εντολή μας) μέσω του εικονιδίου σύνδεσης.

3.3 Διευθυνσιοδότηση IP

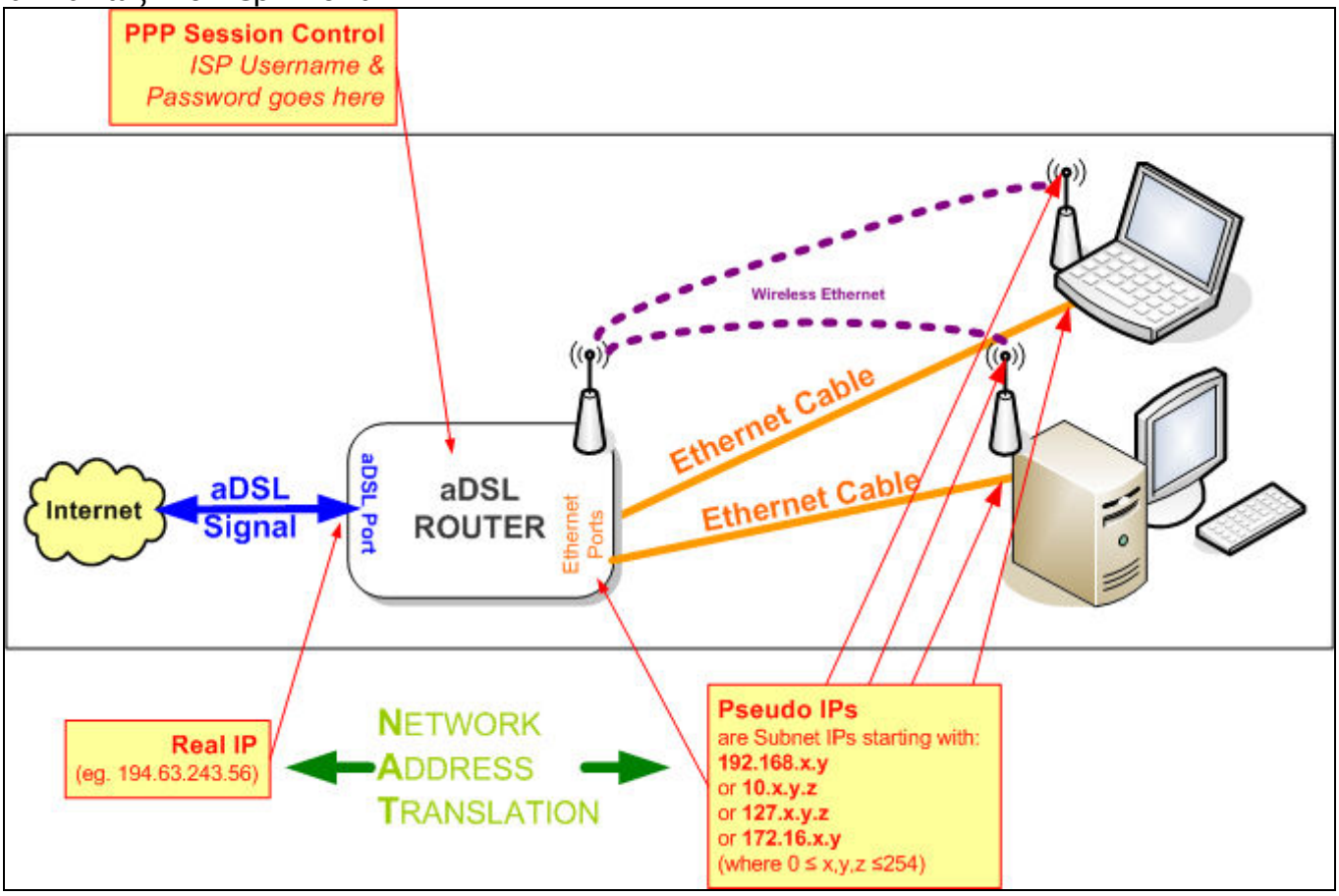
Είναι επίσης σημαντικό να κατανοήσουμε ότι στον Η/Υ μας σε αυτή την περίπτωση δίδεται από τον ISP μας με **δυναμικό** τρόπο μια IP address της μορφής x.y.z.w (πχ. 194.63.243.56), η οποία είναι μοναδική στο internet *(REAL IP)* και χαρακτηρίζει τον Η/Υ μας όση ώρα είναι συνδεδεμένος. Αν αποσυνδεθούμε ηθελημένα ή "πέσει" η σύνδεσή μας για οποιοδήποτε λόγο και επανασυνδεθούμε, τότε θα αποδοθεί εκ νέου μια IP, τις περισσότερες φορές διαφορετική από αυτή της τελευταίας σύνδεσής μας. Το ποιά IP έχει αποδοθεί στον Η/Υ μας όση ώρα είμαστε συνδεδεμένοι, μπορούμε να το διαπιστώσουμε με έναν από τους ακόλουθους τρόπους:

- Στα Windows: Έναρξη (Start)-> Εκτέλεση… (Run…) -> Πληκτρολογούμε cmd -> OK και στο παράθυρο της Γραμμής Εντολών δίνουμε ipconfig και Enter.
- Σε Internet Explorer δίνουμε τη διεύθυνση http://www.whatismyip.com και εμφανίζεται σχετική σελίδα με την IP address μας.

4. ΣΥΝΔΕΣΗ ΜΕ ΧΡΗΣΗ aDSL ROUTER

4.1 Τοπολογία Συνδέσεων

Ο aDSL Router (δρομολογητής) είναι μια συσκευή, η οποία αναλαμβάνει να συνδέσει **έναν ή περισσότερους** Η/Υ στο Internet, διαμοιράζοντας έτσι την aDSL σύνδεση που έχουμε από έναν ISP. Σε αυτού του τύπου συνδέσεις aDSL, τα πράγματα είναι κάπως πιο περίπλοκα:



4.2 Επικοινωνία Router με Internet

Όταν χρησιμοποιούμε router, στην ουσία συνδέουμε ένα τοπικό δίκτυο Η/Υ (private LAN) κάνοντας χρήση του πρωτοκόλλου Ethernet, δλδ καρτών δικτύου Ethernet (ενσύρματες ή ασύρματες) μεταξύ Η/Υ και Router.

Ο Router είναι μια συσκευή που χρειάζεται προγραμματισμό, καθώς είναι αυτή η οποία κάνει τη σύνδεση με τον ISP (και κατ' επέκταση με το Internet). Δηλαδή καταχωρούμε **στον router** μια φορά το username/password που έχουμε από τον ISP, και **αυτός διαχειρίζεται** την πρόσβαση των Η/Υ του τοπικού δικτύου στην aDSL σύνδεση με το Internet.

Είναι πολύ σημαντικό να κατανοήσουμε τί ακριβώς γίνεται με τις IP διευθύνσεις. Είναι δεδομένο ότι ο Router αρχικά επικοινωνεί μέσω της aDSL με τον ISP και αποστέλλει το username/password μας. Όταν πάρει το OK από τον ISP (δλδ. πιστοποιηθεί), τότε ο ISP αποδίδει **δυναμικά <u>ΜΙΑ</u>** IP address (Real IP, πχ. 194.63.243.56), την οποία κρατά ο router καταχωρημένη όση ώρα διαρκεί η σύνδεση. Η σύνδεση αυτή μπορεί να διακοπεί με έναν από τους παρακάτω τρόπους:

- Σβήνοντας ή κάνοντας Reset στον Router.
- Αποσυνδέοντας (ή κόβοντας) το καλώδιο του aDSL Signal
- Διακοπές στη σύνδεση από μέρους του Τηλεπικοινωνιακού Παρόχου ή του ISP.

Όταν κόβεται η aDSL σύνδεση για έναν από τους παραπάνω λόγους, η διαδικασία πιστοποίησης στοιχείων χρήστη που είναι καταχωρημένα στον router γίνεται εξ'αρχής, και αποδίδεται εκ νέου μια IP address (πολλές φορές διαφορετική από αυτή της τελευταίας φοράς).

4.3 Τοπικά Δίκτυα (Private LANs)

Το γεγονός του ότι ο ISP μας δίνει **<u>μία</u>** <u>πραγματική IP</u>, θέτει το πρόβλημα του πώς θα "πολλαπλασιάσουμε" αυτή την IP για να έχουμε περισσότερες, καθώς κάθε Η/Υ στο τοπικό δίκτυό μας χρειάζεται <u>απαραιτήτως</u> να έχει μια IP δηλωμένη στην Ethernet κάρτα δικτύου του για να ανταλλάσει πακέτα δεδομένων με άλλους Η/Υ στο Internet (αλλά και μεταξύ των άλλων Η/Υ του τοπικού μας δικτύου). Τη λύση σε αυτό το θέμα έρχονται να δώσουν οι Ψευδο-IPs (Private IPs), ή αλλιώς τα Ψευδο-δίκτυα (Private LANs).
Τα Private LANs είναι σύνολο από IP διευθύνσεις οι οποίες δεν δημοσιεύονται (δλδ, δεν είναι ορατές) στο Internet. Έχει συμφωνηθεί σε παγκόσμιο επίπεδο από τον διεθνή οργανισμό IANA αυτές οι IPs να είναι:

- Όλες αυτές που ξεκινούν από 10. (δλδ. 10.x.y.z, όπου $0 \leq x,y,z \leq 254$)
- Όλες αυτές που ξεκινούν από 192.168. (δλδ. 192.168.x.y, όπου $0 \leq x,y \leq 254$)
- Όλες αυτές που ξεκινούν από 127. (δλδ. 127.x.y.z, όπου $0 \leq x,y,z \leq 254$)
- Όλες αυτές που ξεκινούν από 172.16. (δλδ. 172.16.x.y, όπου $0 \leq x,y \leq 254$)

Έτσι λοιπόν, όποια Ethernet συσκευή έχουμε συνδέσει στο τοπικό δίκτυό μας θα πρέπει να της δώσουμε μια μοναδική ψευδο-IP, ξεκινώντας από τον router και προχωρώντας σε κάθε Η/Υ ξεχωριστά. Πρέπει απλά να φροντίζουμε να είναι από το ίδιο Subnet. Λέγοντας subnet στη γλώσσα των Δικτύων, εννοούμε Ομάδες IP που τις χαρακτηρίζει άμεσα η μάσκα Subnet (Subnet mask). Η θεωρία των subnets είναι αρκετά εκτενής, και πέραν του σκοπού του παρόντος οδηγού. Αρκεί όμως να έχουμε στο μυαλό μας το εξής:

Αν επιλέξουμε τις IPs που ξεκινούν με 10… και subnet mask 255.255.255.0 τότε μπορούμε να έχουμε 255 διαφορετικές IPs: 10.0.0.0, 10.0.0.1, 10.0.0.2,…,10.0.0.254. Σημείωση: Αποφεύγουμε να βάζουμε την IP που λήγει σε .0 (στο παράδειγμά μας την 10.0.0.0, καθώς αυτή χρησιμοποιείται για ειδικό σκοπό –*Broadcast IP*–).

Στον router ουσιαστικά καθορίζουμε ποιο εύρος ψευδο-IP θα χρησιμοποιήσουμε, προγραμματίζοντάς του μια IP και ένα subnet mask. Συνήθως βάζουμε την πρώτη IP του subnet μας, χωρίς όμως αυτό να είναι δεσμευτικό. Στους Η/Υ προγραμματίζουμε στα TCP/IP properties της κάρτας δικτύου από μια IP, το κοινό subnet mask καθώς και το Default Gateway (προεπιλεγμένη πύλη). Η προεπιλεγμένη πύλη στους Η/Υ είναι <u>πάντα</u> η IP που έχουμε δώσει στον Router μας. Επίσης ο DNS server (στα TCP/IP properties) στους Η/Υ μπορεί και πάλι να είναι η IP του router μας, καθώς κατά τη σύνδεση του router με τον ISP καταχωρούνται στη μνήμη του Router οι πραγματικές IP διευθύνσεις των DNS servers του ISP μας.

Επίσης είναι δυνατό ο Router να δίνει αυτόματα δικτυακές ρυθμίσεις (IP, mask, Gateway IP, DNS server IP) σε κάθε υπολογιστή την ώρα που ανάβει ο υπολογιστής και

συνδέεται με φυσικό μέσο (καλώδιο δικτύου) στο router. Αυτό γίνεται αν στα TCP/IP properties της κάρτας δικτύου του Η/Υ επιλέξουμε "Αυτόματη απόδοση IP" και παράλληλα έχουμε ενεργοποιήσει τη λειτουργία DHCP Server *(Dynamic Host Configuration Protocol Server)* στον router μας. **Προτείνεται όμως,** σε περιπτώσεις ύπαρξης λίγων Η/Υ στο τοπικό δίκτυό μας (από 1 έως 10) να ΜΗΝ χρησιμοποιούμε αυτή τη μέθοδο, δλδ της αυτόματης απόδοσης IP, προγραμματίζοντας στον router μας DHCP server -> Disabled, και βάζοντας χειροκίνητα και εφάπαξ δικτυακές ρυθμίσεις στους Η/Υ μας.

4.4 Network Address Translation (NAT)

Δεδομένου ότι η αμφίδρομη ανταλλαγή πακέτων δεδομένων στο Internet γίνεται αποκλειστικά μεταξύ Η/Υ που έχουν πραγματικές IP, γεννάται το ερώτημα του πώς ένας Η/Υ του τοπικού δικτύου μας που έχει ψευδο-IP μπορεί και επικοινωνεί με τους servers του Internet παίρνοντας δεδομένα (σελίδες web, αρχεία κτλ); Απάντηση σε αυτό δίνει η λειτουργία NAT που εκτελεί ο Router. Δηλ. κάνει "μετάφραση" (ή μετατροπή) όλων των ψευδο-IP στη μία και μοναδική πραγματική IP που έχει αποδοθεί από τον ISP κατά την διαδικασία της aDSL σύνδεσης. Στη συνέχεια προωθεί το ερώτημα για λήψη δεδομένων από έναν Η/Υ του τοπικού μας δικτύου "καμουφλαρισμένο" με την πραγματική IP. Όταν έρθει το ζητούμενο πακέτο δεδομένων από έναν Η/Υ του Internet (πχ WebServer), τότε ο router "θυμάται" ποιος Η/Υ του τοπικού δικτύου (με την αντίστοιχη ψευδο-IP) το ζήτησε και του το προωθεί.

Επιγραμματικά και πολύ γενικά, ο τρόπος με τον οποίο "θυμάται" ο router ποιός Η/Υ (με ποια ψευδο-IP δηλαδή) ζήτησε δεδομένα από ποιόν Η/Υ του Internet είναι: δημιουργώντας έναν προσωρινό πίνακα αντιστοιχιών *(NAT Table)* του οποίου οι εγγραφές γράφονται και σβήνονται διαρκώς, κάθε φορά που ξεκινά η ζήτηση δεδομένων *(new NAT Table entries)*, που αυτή βρίσκεται σε εξέλιξη *(sustained NAT entries)*, και τελικά που ολοκληρώνεται ή δεν είναι εφικτή *(deleted NAT entries)*.

4.5 Port Forwarding

Με ποιο τρόπο όμως μπορεί να γίνει το αντίστροφο; Δηλαδή, αν συνδεόμαστε στο Internet από έναν Η/Υ ο οποίος έχει πραγματική IP, πώς μπορούμε να ζητήσουμε δεδομένα έναν Η/Υ που βρίσκεται σε ένα τοπικό δίκτυο ο οποίος έχει ψευδο-IP *(δεδομένου ότι η αμφίδρομη ανταλλαγή πακέτων δεδομένων στο Internet γίνεται αποκλειστικά μεταξύ Η/Υ που έχουν πραγματικές IP)*; Με απλά λόγια, το κλειδί στην υπόθεση αυτή είναι πως κάθε δικτυακή εφαρμογή που τρέχει σε έναν Η/Υ χρησιμοποιεί συγκεκριμένο port (ή ports) μέσω του οποίου τροφοδοτεί με δεδομένα άλλους δικτυακούς Η/Υ.

Τα διαθέσιμα ports ανά IP αριθμούν σε 65535, και μάλιστα είναι τόσα τύπου TCP *(Transport Control Protocol)* και άλλα τόσα τύπου UDP *(User Datagram Protocol).* Υπάρχουν ports που έχει συμφωνηθεί διεθνώς να χρησιμοποιούνται από γνωστές εφαρμογές (πχ. το 80 για web, το 23 για telnet, το 21 για FTP κτλ.), τα οποία είναι τα πρώτα 1024 (από 0 έως 1023). Αναλυτικός πίνακας υπάρχει στη διεύθυνση http://www.iana.org/assignments/port-numbers.

Έτσι λοιπόν, αν θέλουμε επί παραδείγματι ο Η/Υ του τοπικού μας δικτύου με IP 10.0.0.35 να είναι web server ορατός από το υπόλοιπο Internet (ώστε να μπορούν να πάρουν από αυτόν δεδομένα Η/Υ που είναι στο Internet), αρκεί να δηλώσουμε στον Router μας (που δρομολογεί ποιος θα πάρει τί και από ποιόν) ότι: "Οποιοσδήποτε Η/Υ του Internet ζητήσει δεδομένα τύπου web (port 80 TCP & UDP δλδ) από την πραγματική IP

που έχει ο router μας (που του αποδόθηκε δυναμικά από τον ISP μας κατά την aDSL σύνδεση), να προωθήσει το αίτημα κατ'ευθείαν στον Η/Υ που έχει την IP 10.0.0.35, και κατόπιν να στείλει την απάντηση (ή τα δεδομένα web) που ζητήθηκαν στον Η/Υ του Internet που τα ζήτησε".

5. FIREWALLS

Τα Firewalls είναι προγράμματα που εκτελούν μια σχετικά απλή διαδικασία: Κόβουν ή επιτρέπουν την διέλευση δεδομένων σε επίπεδο δικτυακού Port. Αυτό -και μόνο αυτό- μπορούν να κάνουν τα firewalls που τρέχουν σε aDSL Routers. Τα software firewalls όπως αυτό των Windows, κάνουν και κάτι παραπάνω: πέραν από τα ports που μπλοκάρουν (ή επιτρέπουν), μπορούν να μπλοκάρουν (ή να επιτρέψουν) και ports ανά εφαρμογή (δλδ αρχείο .exe).

Χαρακτηριστικό παράδειγμα για να γίνει κατανοητό το παραπάνω είναι το OpenFalcon. Το OpenFalcon για να επικοινωνήσει δικτυακά από τον Η/Υ μας με άλλη παρόμοια εφαρμογή άλλου Η/Υ (δλδ. OpenFalcon άλλου Η/Υ) χρειάζεται οι εφαρμογές F4-BMS.exe και voicesetup.exe να στέλνουν και να λαμβάνουν δεδομένα στα ports: από 2934 έως 2937, 7778, 28900 (όλα σε TCP **και** UDP). Έτσι:

α) Αν έχουμε firewall enabled στον Router, θα πρέπει να επιτρέψουμε τη διέλευση των παραπάνω Ports από και προς το τοπικό δίκτυό μας σε σχέση με το λοιπό Internet.

β) Αν έχουμε firewall στον Η/Υ (πχ windows firewall) κάνοντας απλά στην καρτέλλα "Exceptions" -> "Add Program…" τα F4-BMS.exe και voicesetup.exe, ελευθερώνεται όλο το εύρος των ports *(65535 ports)* για αυτά τα δύο .exe αρχεία -και μόνο-. Θα μπορούσαμε εναλλακτικά να δηλώσουμε στο firewall των windows να επιτρέπει τη διέλευση των παραπάνω ports ανεξαρτήτως εφαρμογής .exe κάνοντας στην καρτέλλα "Exceptrions" -> "Add Port…", αλλά αν σκεφτούμε ότι μπορεί να υπάρξει κάποιο κακόβουλο .exe που χρησιμοποιεί αυτά τα ports, η λύση αυτή είναι λιγότερο ασφαλής.

γ) Τελος, αν έχουμε firewall enabled στον router **και** windows firewall ενεργοποιημένο θα πρέπει να κάνουμε το (α) **και** το (β) για να μπορέσει να επικοινωνήσει τελικά το OpenFalcon.

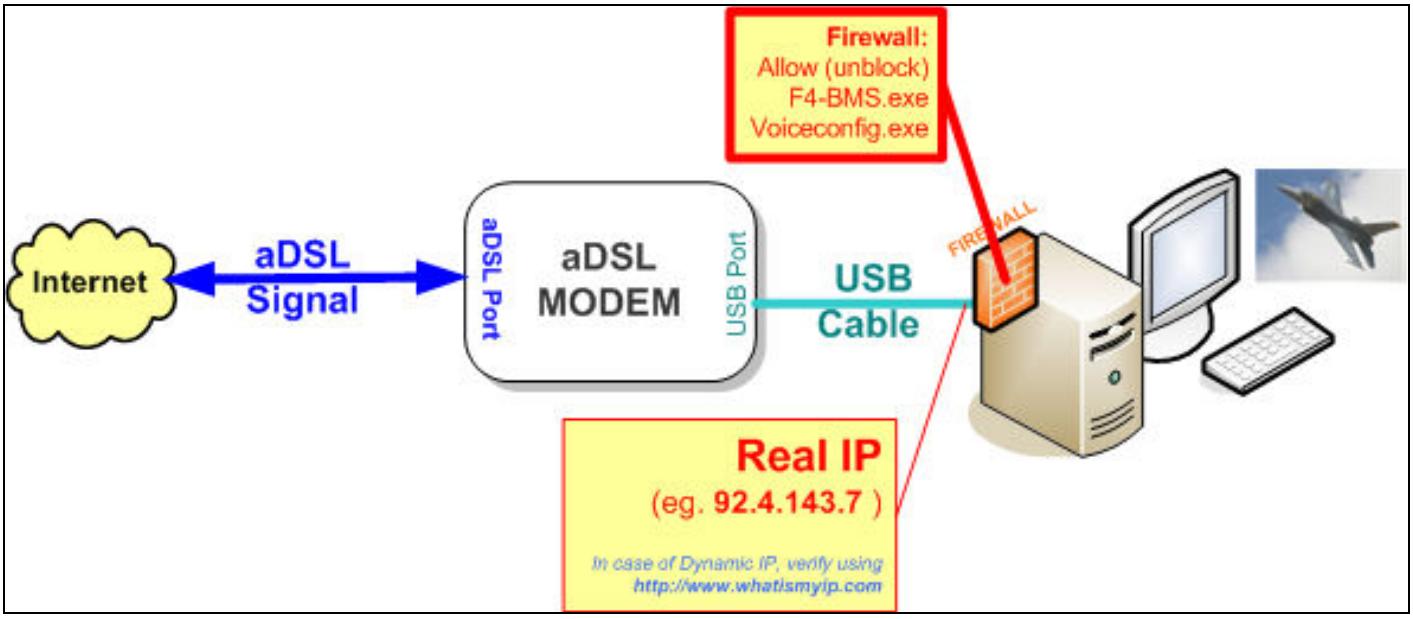
Γενικά πάντως για οικιακή χρήση και σε πλήθος υπολογιστών όχι πάνω από 5-6 πρέπει να αποφασίζουμε από την αρχή τί σχήμα firewalling θέλουμε να τηρήσουμε, και μια καλή πρακτική θεωρώ πως είναι να τρέχει firewall μόνο στους Η/Υ (πχ windows firewall). Επειδή, ειδικά για την περίπτωση του OpenFalcon πρέπει να γίνει και port forwarding για τα ports που χρησιμοποιεί, θα γίνει περίπλοκη η κατάσταση για τον μέσο χρήστη αν κάνει **και** firewalling στον Router.

6. WEB INTERFACE ΤΩΝ ADSL ROUTERS

Στους περισσότερους -αν όχι, όλους- aDSL routers, όλες οι ρυθμίσεις και ο απαραίτητος προγραμματισμός τους που περιγράφθηκαν στις προηγούμενες παραγράφους, γίνεται από το λεγόμενο web interface. Δηλαδή, ο router είναι και ένας mini webserver, ο οποίος παρουσιάζει μια σελίδα ρυθμίσεων αν ανοίξουμε έναν Internet Explorer και δώσουμε ως διεύθυνση ιστοσελίδας την ψευδο-IP που έχει ο router (ή αλλιώς, είναι η Gateway IP του Η/Υ που είναι στο τοπικό δίκτυο). Κάθε κατασκευαστής router, ακολουθεί τη δική του φιλοσοφία οργάνωσης απεικόνισης των ρυθμίσεων. Οι ρυθμίσεις αυτές τις περισσότερες φορές χρησιμοποιούν την κοινή ορολογία που

περιγράφθηκε παραπάνω. Μια καλή πηγή πληροφοριών (πέραν του εγχειριδίου χρήσης που συνοδεύει τον κάθε router) είναι και η ιστοσελίδα http://www.adslgr.com.

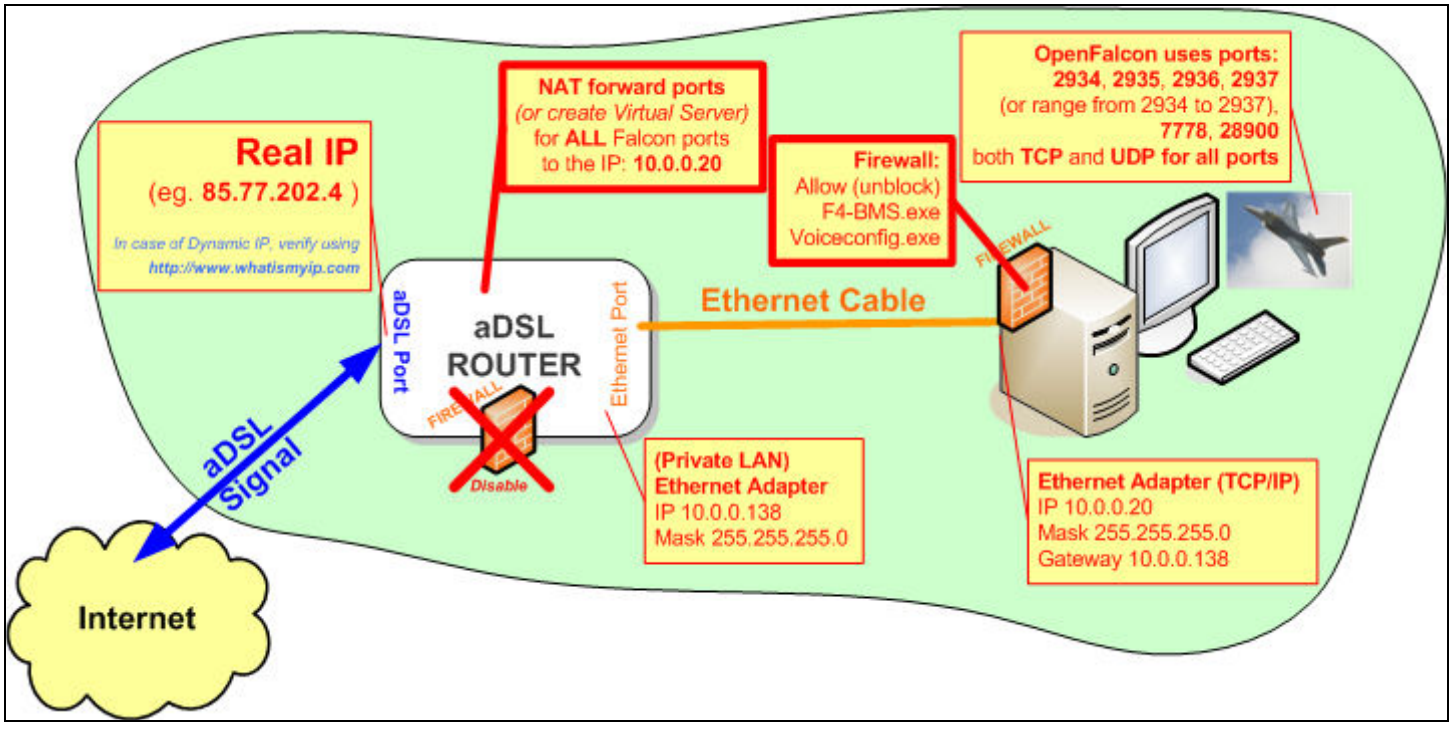
6. ΡΥΘΜΙΣΕΙΣ ΓΙΑ ΤΟ OPENFALCON ΜΕ ΣΥΝΔΕΣΗ aDSL MODEM



Στην περίπτωση σύνδεσης με aDSL Modem, τα πράγματα είναι απλά:

- Προσθέτουμε στις εξαιρέσεις του firewall το F4-BMS.exe και το Voiceconfig.exe
- Πριν συνδεθούμε με τους διαδικτυακούς e-wingmen, ελέγχουμε την πραγματική IP address που μας αποδόθηκε από τον ISP (με ipconfig ή whatismyip.com) και αλλάζουμε καταλλήλως το windows shortcut Target του OpenFalcon.

7. ΡΥΘΜΙΣΕΙΣ ΓΙΑ ΤΟ OPENFALCON ΜΕ ΣΥΝΔΕΣΗ aDSL Router



Στο παραπάνω σχηματικό παράδειγμα έχουμε κάνει τα εξής:

- Στον aDSL router (μόνιμες ρυθμίσεις),
  - Δηλώσαμε το τοπικό δίκτυο ότι θα είναι το 10.0.0.x, βάζοντας Private LAN IP την 10.0.0.138 και Subnet mask 255.255.255.0.
  - Disable στο ενσωματωμένο Firewall
  - Port forwarding στα ports του OpenFalcon προς την IP 10.0.0.20
  - Username/password μας που έχουμε από τον ISP μας (aDSL συνδρομή)
- Στον Η/Υ που είναι εγκατεστημένο το OpenFalcon:
  - Προσθέτουμε στις εξαιρέσεις του firewall το F4-BMS.exe και το Voiceconfig.exe
  - Πριν συνδεθούμε με τους διαδικτυακούς e-wingmen, ελέγχουμε την πραγματική IP address που μας αποδόθηκε από τον ISP (μέσω του whatismyip.com **μόνο**) και αλλάζουμε καταλλήλως το windows shortcut Target του OpenFalcon.

ΠΑΡΑΔΕΙΓΜΑ ΣΥΝΔΕΣΗΣ ΔΥΟ vPILOTS: