Το RedHat Linux 6.x σαν Internet Gateway γιά σπιτικό δίκτυο

Paul Ramsey <pramsey@refractions.net> 22 Ιουνίου 2000

Ένα απλό διδακτικό κείμενο γιά τη ρύθμιση του RedHat 6 και παρομοίων εκδόσεων, γιά να δουλέψει σαν Internet gateway ς' ένα μικρό δίκτυο στο σπίτι ή στο γραφείο. Τα θέματα που καλύπτονται, περιλαμβάνουν το μασκάρισμα (masquerading), το DNS, το DHCP, και βασικές απαιτήσεις ασφάλειας.

Contents

1 Εισαγωγή **2**

1.1 Εκδόσεις . . . 2

1.2 Copyright . . . 3

2 Καλωδιώνοντας το σύστημα **3**

2.1 Με hub . . . 3

2.2 Χωρίς hub . . . 4

2.3 Με μόνο μία κάρτα δικτύου . . . 4

3 Ρυθμίζοντας τη δικτύωση **4**

3.1 Ρυθμίζοντας έναν driver δικτύου . . . 5

3.1.1 Δύο ακριβώς ίδιες κάρτες δικτύου . . . 6

3.2 Ρυθμίζοντας το εσωτερικό μέρος του δικτύου . . . 7

3.2.1 Η συσκευή δικτύου . . . 7

3.2.2 Ο DHCP server . . . 8

3.2.3 Οι client Η/Υ . . . 9

3.2.4 Ο DNS server . . . 10

3.2.5 Τεστάροντας το εσωτερικό δίκτυο . . . 11

3.3 Ρυθμίζοντας το εξωτερικό δίκτυο . . . 11

3.3.1 Με στατική διεύθυνση IP . . . 12

3.3.2 Με το DHCP . . . 12

3.3.3 Παραξενιές και ανωμαλίες . . . 12

3.3.4 Κοιτάζοντας τις ρυθμίσεις του δικτύου . . . 13

3.4 Ασφάλεια . . . 14

4 Ρυθμίσεις μασκαρίσματος (masquerading) **15**

5 Προβλήματα **16**

5.1 Το ICQ δεν δουλεύει 17

5.2 Έχω Caldera 2.x, όχι RedHat 6.x 17

5.3 Θέλω ένας από τους εσωτερικούς Η/Υ μου να γίνει ο Web server μου 17

1 Εισαγωγή

Αυτό το κείμενο περιέχει απλές συνταγές γιά τη ρύθμιση του RedHat 6.x σαν Internet gateway γιά ένα σπιτικό δίκτυο, ή δίκτυο ενός μικρού γραφείου. Οι οδηγίες είναι όσο γίνεται απλοποιημένες : Δεν συζητάμε γιά ειδικές περιπτώσεις, και θα κάνουμε μερικές υποθέσεις, όσον αφορά τις διευθύνσεις δικτύου που θα χρησιμοποιηθούν, Οι σημαντικότερες υποθέσεις μας είναι :

- Οτι διαθέτετε διαρκή καλωδιακή ή ADSL σύνδεση στο Internet.
- Οτι μπορείτε να εγκαταστήσετε με επιτυχία το *RedHat 6.x* σε τουλάχιστον έναν από τους Η/Υ σας. Σημειώστε ότι αυτές οι οδηγίες ισχύουν και γιά τα παράγωγα του RedHat, όπως το *Mandrake 6.x*, που διανέμεται από την MacMillan Publishing κάτω από μιά ποικιλία εμπορικών ετικετών.
- Οτι ο Η/Υ σας με το Linux έχει δύο κάρτες δικτύου εγκατεστημένες μέσα του, και είναι συμβατές με το Linux και οι δύο.
- Οτι διαθέτετε ένα ethernet hub, αν συνδέετε σε δίκτυο περισσότερους από έναν υπολογιστές, ή καλώδιο cross-over, αν συνδέετε μόνον έναν Η/Υ.
- Οτι γνωρίζετε πώς να επεξεργάζεστε αρχεία μορφής text σε Η/Υ με Linux.
- Οτι μπορείτε να μπείτε στον Η/Υ ως `root`. Οτι γνωρίζετε να εγκαθιστάτε πακέτα RPM από τα cd-roms του Linux.

Αν δεν πληρείτε αυτές τις προϋποθέσεις, τότε πιθανότατα αυτό το κείμενο να μην προορίζεται γιά σας.

Δεν υπάρχει κάτι το ασυνήθιστο, που πρέπει να κάνετε κατά τη διαδικασία εγκατάστασης. Απλά, διαλέξτε μιά εγκατάσταση που σας ταιριάζει, και ξεκινήστε την. Αυτό το κείμενο δίνει οδηγίες γιά να εγκαταστήσετε ο,τιδήποτε έχει σχέση με την προσπάθεια δικτύωσης που ξεκινάει από το μηδέν, γιά ν' αποφύγετε τις τυφλές υποθέσεις, ως προς το τί εγκαταστάθηκε ή ρυθμίστηκε κατά τη διάρκεια της εγκατάστασης αυτής. Γιά να βεβαιωθείτε πως το σύστημα δουλεύει και πως δεν υπάρχει σύγχυση ως προς το τί-πάει-πού, όλες οι ρυθμίσεις θα γίνουνε με κατευθείαν επέμβαση στα αρχεία ρυθμίσεων, παρά με χρήση των εργαλείων ρυθμίσεων κάτω από GUI's, τα οποία παρέχει το RedHat. Από τη μιά πλευρά, αυτός ο τρόπος είναι λιγάκι δυσκολότερος απ' ό,τι πρέπει. Από την άλλη, όμως, οι γνώσεις σας θα μπορούν να εφαρμοστούν πολύ εύκολα σε διαφορετικές διανομές του Linux, ή διαφορετικές καταστάσεις. (Πχ, σε φάση όπου τα X-Windows δεν δουλεύουν, ή αν στήνετε έναν headless server.)

1.1 Εκδόσεις

Η τελευταία έκδοση αυτού εδώ του κειμένου πάντα βρίσκεται στο *http://www.coastnet.com/˜pramsey/linux/homenet.html* (σε HTML), και στο *http://www.coastnet.com/˜pramsey/linux/homenet.sgml* (σε SGML).

- 21 Δεκεμβρίου 1999 : Πρώτη έκδοση.
- 2 Ιανουαρίου 2000 : Περιέλαβα υποδείξεις του John Mellor, γιά τις παραξενιές του εξωτερικού δικτύου.
- 22 Ιανουαρίου 2000 : Μικρή προσθήκη σχετικά με τις κάρτες δικτύου που είναι ακριβώς ίδιες, και πληροφορίες γιά το IP aliasing από τον Chris Lea.
- 16 Μαρτίου 2000 : Μερικές πληροφορίες σχετικές με την ασφάλεια του name server και σχετικά με την υποστήριξη του Caldera Linux, από τον Nelson Gibbs.
- 22 Ιουνίου 2000 : Τεκμηρίωση γιά τις παραξενιές της ρύθμισης του RedHat 6.2 . Περισσότερες πληροφορίες γιά το PPPoE (PPP over Ethernet), από τον Kerr First.

1.2 Copyright

2 Καλωδιώνοντας το σύστημα

Ανάλογα με το αν χρησιμοποιείτε hub ή όχι, η δικτυακή σας τοπολογία θα διαφέρει λιγάκι. Εδώ καλύπτω μονάχα την σύνδεση με καλώδιο RJ45 (αυτό που μοιάζει με τηλεφωνικό καλώδιο που πάχυνε, επειδή πήρε αναβολικά), και όχι την σύνδεση με λεπτό ομοαξονικό. Με το λεπτό ομοαξονικό μπορείτε να συνδέσετε πολλούς Η/Υ χωρίς να χρειαστεί hub, αλλά πρέπει να προσέχετε τον τερματισμό των συνδέσεων, κλπ. Αν ήδη γνωρίζετε από δικτύωση, οι οδηγίες αυτές θα σας φανούν σε μεγάλο βαθμό περιττές.

2.1 Με hub

Αν διαθέτετε hub, το δίκτυό σας θα μοιάζει μ' *αυτό εδώ* `<http://www.coastnet.com/~pramsey/linux/w_hub.gif>`.

Συνδέστε την κάρτα δικτύου `eth0` του Η/Υ σας με το καλωδιακό (cable) modem, ή το κουτί της σύνδεσης ADSL, χρησιμοποιώντας το καλώδιο που σας έδωσε ο τεχνικός της σύνδεσης κατά την εγκατάσταση που έκανε. (Η, ένα καλώδιο που γνωρίζετε ότι θα δουλέψει μ' αυτή τη σύνδεση.) Αυτό το βήμα χρειάζεται προσοχή, επειδή μερικές φορές στα cable modems αρέσει η σύνδεση με crossover, και μερικές φορές η κατευθείαν σύνδεση με καλώδιο. Το καλώδιο που σας δίνει η εταιρία σύνδεσης, είναι αυτό ακριβώς που χρειάζεστε.

Συνδέστε την κάρτα δικτύου `eth1` του Η/Υ σας με το hub, κατευθείαν με καλώδιο. Κάντε το ίδιο και γιά τους άλλους Η/Υ σας.

2.2 Χωρίς hub

Ακόμη κι αν δεν έχετε hub, πάντα μπορείτε να συνδέσετε έναν Η/Υ επάνω στον Η/Υ σας που έχει Linux, με καλώδιο crossover. Η τοπολογία σας θα μοιάζει με *αυτήν εδώ* `<http://www.coastnet.com/~pramsey/linux/wo_hub.gif>`.

Συνδέστε την κάρτα δικτύου `eth0` με το cable modem, ή το κουτί της σύνδεσης ADSL, χρησιμοποιώντας το καλώδιο της συσκευασίας των συνδέσεων. Συνδέστε την κάρτα δικτύου `eth1` με τον άλλον Η/Υ, χρησιμοποιώντας καλώδιο crossover.

2.3 Με μόνο μία κάρτα δικτύου

Αυτό το στήσιμο δεν το συνιστώ. Μ' αυτόν τον τρόπο, το εσωτερικό και το εξωτερικό σας δίκτυο βρίσκονται επάνω στο ίδιο κομμάτι δικτύου, και άρα είναι πιο επιδεκτικά σε cracking (= ζημιές από κακόβουλους hackers). Στην πραγματικότητα, ο κίνδυνος αυτός είναι πιθανότατα ασήμαντος, αλλά *υπαρκτός*. Ανάλογα τί θα σας τύχει.

Ο πυρήνας του Linux περιλαμβάνει υποστήριξη γιά το "IP aliasing", η οποία επιτρέπει σε μία κάρτα δικτύου τύπου ethernet να υποστηρίζει δύο διευθύνσεις IP ταυτόχρονα. (Αυτό το χαρακτηριστικό είναι σύμφυτο στους πυρήνες που βρίσκονται στις διανομές της RedHat και της Mandrake.) Γιά να ρυθμίσετε μιά gateway με μόνο μία κάρτα ethernet, αντικαταστήστε σε όλα τα εφεξής παραδείγματα το `eth1` με το `eth0:0`.

Σε σύστημα μονής κάρτας δικτύου, *δεν* συνίσταται να τρέξετε έναν DHCP server.

Συνδέστε όλους τους Η/Υ σας και το cable modem σας (ή το κουτί της σύνδεσης ADSL) στο hub. Σταυρώστε τα δάχτυλά σας, και συνεχίζουμε.

3 Ρυθμίζοντας τη δικτύωση

Εντάξει λοιπόν, μέχρι τώρα έχετε εγκαταστήσει το Linux στον Η/Υ, που αποτελεί την gateway σας. Μπορεί ακόμη και να 'χετε ρυθμίσει μία από τις κάρτες δικτύου σας, και τη σύνδεση με το Internet. Ωστόσο, θ' αρχίσουμε από το μηδέν, και θα κάνουμε σα να μην έγινε καμμία ρύθμιση.

Κάντε login ως `root`. Όλες οι οδηγίες αυτού του κειμένου προϋποθέτουν ότι έχετε κάνει login ως root.

Ο πυρήνας του Linux αναφέρεται στις δύο ethernet κάρτες σας ως `eth0` και `eth1`, άρα με τον ίδιο τρόπο θ' αναφέρομαι κι εγώ ς' αυτές εις το εξής. Το πρόβλημα, όμως, είναι ότι δεν ξέρουμε ποια είναι ποια. Ορίστε ένας "απλός" τρόπος να το βρούμε, που δουλεύει εγγυημένα τουλάχιστον στο 50% των περιπτώσεων : Βάλτε τον Η/Υ σας επάνω στο γραφείο με τη motherboard σε οριζόντια θέση, και να βλέπετε το πίσω μέρος. (Σα να επρόκειτο να τον ανοίξετε, και να κάνετε κάποια εργασία στο εσωτερικό του.) Η `eth0` κάρτα είναι η πιο αριστερά - ίσως να θέλετε να σημειώσετε τη θέση της με μιά ετικέτα. Τώρα, σημειώστε ς' ένα φύλλο χαρτί τη μάρκα και το μοντέλο και της `eth0`, και της `eth1`.

Εντάξει, ας δούμε τώρα αν και την `eth0` και την `eth1` τις αναγνωρίζει αυτόματα ο πυρήνας. Δώστε : `ifconfig eth0` και : `ifconfig eth1`. Και στις δύο περιπτώσεις, αν ο πυρήνας αναγνωρίζει την αντίστοιχη κάρτα, πρέπει να δείτε ένα μήνυμα σαν το παρακάτω (με τα νούμερα και τα υπόλοιπα, βέβαια, να είναι διαφορετικά) :

```
eth0   Link encap: Ethernet   HWaddr 00:60:67:4A:02:0A
       inet addr:0.0.0.0  Bcast:0.0.0.0  Mask:255.255.255.255
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:466 errors:0 dropped:0 overruns:0 frame:0
       TX packets:448 errors:0 dropped:0 overruns:0 carrier:0
       collisions:85 txqueuelen:100
       Interrupt:10 Base address:0xe400
```

Αν ο πυρήνας δεν αναγνωρίζει την κάρτα δικτύου σας, θα δείτε ένα μήνυμα σαν το παρακάτω :

```
eth0: error fetching interface information: Device not found.
```

3.1 Ρυθμίζοντας έναν driver δικτύου

Αν το Linux βρει και τίς δύο κάρτες σας, πάτε την επόμενη ενότητα. Αλλιώς, διαβάστε αυτήν εδώ.

Ας πούμε ότι ο πυρήνας δεν αναγνωρίζει τη μία κάρτα, ή και τις δύο. Αυτό δεν είναι κανένα σπουδαίο πρόβλημα. Ο,τι πρέπει να κάνουμε, είναι να εξηγήσουμε στον πυρήνα πώς να βρει τις κάρτες. Υπάρχουν πολλά κόλπα εδώ, αλλά δεν θα τ' αναφέρω όλα. Μονάχα θυμηθείτε πως, όταν τα πράγματα δυσκολεύουν, υπάρχει και το *Ethernet HOWTO*. Ιδού, όμως, μερικές συμβουλές σε συντομία :

- *Διαθέτετε μιά PCI κάρτα δικτύου.* Και πιθανότατα έχετε ξενοιάσει, υποθέτοντας πως δεν είναι τόσο καινούργια, ώστε να μην υπάρχουν καθόλου drivers γι' αυτήν. Συχνά, όμως, μπορείτε να βρείτε πάρα πολλές πληροφορίες γιά τις κάρτες δικτύου σας (καθώς και γι' άλλα πράγματα), διαβάζοντας το `/proc/pci` και σημειώνοντας μάρκες και μοντέλα.
- *Διαθέτετε μιά ISA κάρτα δικτύου.* Είναι πιθανό να χρειαστεί να μάθετε τη βασική διεύθυνση IO και την IRQ της κάρτας. Η κάρτα έχει ένα εγχειρίδιο, σωστά; Αν δεν έχει, πρέπει να πάτε στο site του κατασκευαστή της, και να δείτε αν έχει on-line τίποτε κείμενα αναφοράς. Η, αν η κάρτα έχει μιά δισκέτα ρυθμίσεων στο DOS, ξεκινήστε με την δισκέτα αυτή και κοιτάξτε αν έχει πρόγραμμα ρυθμίσεων (το οποίο θα διαβάσει και θα ρυθμίσει τη διεύθυνση και την IRQ).
- *Διαθέτετε μιά ISA Plug'n'Play κάρτα δικτύου.* Πρώτα πρέπει να μάθετε πώς να τη ρυθμίζετε - διαβάστε το *Plug'n'Play HOWTO*. Ευτυχώς, αφού ρυθμίσετε μία φορά την κάρτα σας, θα γνωρίζετε ακριβώς ποιες είναι η βασική διεύθυνση IO και η IRQ της.

Τώρα, μιά που ξέρετε τις μάρκες - μοντέλα των `eth0` και `eth1`, μπορείτε να πάτε στη *σελίδα συμβατότητας* του *Ethernet HOWTO*, και να ψάξετε γιά τις κάρτες σας. Σημειώστε τον συνιστώμενο driver, καθώς και κάθε πληροφορία γιά ειδικές ρυθμίσεις, που τυχόν απαιτούν οι κάρτες σας.

Έφτασε η στιγμή να επέμβουμε ς' ένα αρχείο ρυθμίσεων! Το αρχείο που θα διορθώσουμε, είναι το `/etc/conf.modules`. Ανοίξτε το με τον text editor της επιλογής σας. Επειδή υπάρχουν πολλές επιλογές και συνδυασμοί, που μπορούν να προστεθούν στο συγκεκριμένο αρχείο, θα σας δώσω σαν παράδειγμα τις ρυθμίσεις γιά τη δική μου gateway. Έχω μιά PCI κάρτα των 10/100 Mbps, που βασίζεται στο ολοκληρωμένο VIA Rhine, κι έναν τυπικότατο ISA κλώνο του προτύπου NE2000, στα 10 Mbps. Χρησιμοποιώ την κάρτα των 100 Mbps γιά το εσωτερικό δίκτυο, και την 10άρα γιά τη σύνδεση με το εξωτερικό δίκτυο. Το δικό μου `/etc/conf.modules` αρχείο είναι κάπως έτσι :

```
alias parport_lowlevel parport_pc
alias eth0 ne
options ne io=0x300 irq=10
alias eth1 via-rhine
```

Η εξήγηση των γραμμών του `conf.modules` αρχείου μου είναι η εξής :

- Η πρώτη γραμμή καθορίζει ότι η παράλληλη θύρα μου είναι γιά εκτυπώσεις. Πιθανότατα έχετε κι εσείς μιά τέτοια γραμμή, την οποία αφήστε την ως έχει.
- Η δεύτερη γραμμή (`alias eth0 ne`) λέει στον πυρήνα να χρησιμοποιήσει τον ne driver γιά τη συσκευή `eth0`.
- Η τρίτη γραμμή (`options ne io=0x300 irq=10`) λέει στον ne driver σε ποια διεύθυνση IO και σε ποια IRQ θα βρει την ISA κάρτα. Αν έχετε και σεις κάρτα ISA, πιθανότατα πρέπει να γράψετε μιά παρόμοια γραμμή στο αρχείο. Απλά, αντικαταστήστε τον driver και τις IO και irq με τα αντίστοιχα γιά την κάρτα σας.
- Η τέταρτη γραμμή (`alias eth1 via-rhine`) λέει στον πυρήνα να χρησιμοποιήσει στην κάρτα `eth1` τον driver γιά ολοκληρωμένα via-rhine. Επειδή, τώρα, η `eth1` κάρτα μου είναι PCI, δεν χρειάζεται να γράψω οδηγίες γιά τις io και irq : Το υποσύστημα PCI ρυθμίζει την κάρτα αυτόματα.

Πρέπει να βεβαιωθείτε ότι υπάρχουν γραμμές alias και γιά τις δυο κάρτες σας στο αρχείο `conf.modules` , και να βάλετε τις σωστές γραμμές επιλογών γιά όλες τις ISA κάρτες σας. Μπορεί και να υπάρχουν ήδη γραμμές στο `conf.modules`, γιά κάθε κάρτα ethernet που ρυθμίσατε κατά την εγκατάσταση

Όταν τελειώσετε τη διόρθωση του `conf.modules`, ξαναδοκιμάστε τις εντολές `ifconfig eth0` και `ifconfig eth1`. Ίσως σας χρειαστεί να κάνετε κάμποσες δοκιμές, αν σκαλίζετε τις διευθύνσεις IO και τις IRQs, χωρίς να κοιτάζετε το εγχειρίδιο του κατασκευαστή.

3.1.1 Δύο ακριβώς ίδιες κάρτες δικτύου

Εσείς ο ξύπνιος, που αγοράσατε δύο ακριβώς ίδιες κάρτες δικτύου, τώρα δεν μπορείτε να τις βάλετε να δουλέψουν μαζί; Μην ανησυχείτε, το ν' αναγκαστούν να συμβιώσουν είναι απλά θέμα σωστής σύνταξης των γραμμών του αρχείου `/etc/conf.modules`. Στο παράδειγμά μας, οι αριθμοί IO διευθύνσεων και IRQ's είναι απλά της φαντασίας μας, αλλά θα υποθέσω ότι αγοράσατε ένα ταιριασμένο ζευγάρι κλώνων του προτύπου NE2000 (πράγμα που είναι μιά συνηθισμένη επιλογή). Το δικό σας αρχείο `/etc/conf.modules` λογικά μοιάζει κάπως έτσι :

```
alias eth0 ne
alias eth1 ne
options ne io=0x330,0x360 irq=7,9
```

Οι παράμετροι διευθυνσιοδότησης δίδονται όλες στην ίδια γραμμή, και ο πρώτος αριθμός σε κάθε παράμετρο αναφέρεται στην eth0. Ο δεύτερος στην eth1.

3.2 Ρυθμίζοντας το εσωτερικό μέρος του δικτύου

Το "εσωτερικό" δίκτυο είναι αυτό, με το οποίο επικοινωνούν όλοι οι Η/Υ μας στο σπίτι ή στο γραφείο. Το "εξωτερικό" δίκτυο είναι το μεγάλο, τρομακτικό Internet, στην άλλη πλευρά του gateway Η/Υ μας. Γιά τον περισσότερο χρόνο, το εσωτερικό δίκτυο θα είναι πλήρως απομονωμένο από το εξωτερικό με τη βοήθεια του gateway Η/Υ, ο οποίος θα ενεργεί ως firewall μέτριας ισχύος.

3.2.1 Η συσκευή δικτύου

Μιά που οι drivers σας δουλεύουνε τώρα, και μπορείτε να δείτε και την eth0 και την eth1 με το ifconfig, ήρθε η στιγμή να ρυθμίσουμε το εσωτερικό δίκτυο. Υποθέτω ότι θα βάλετε το εσωτερικό σας δίκτυο στην eth1, και το εξωτερικό δίκτυο στην eth0.

Το εσωτερικό σας δίκτυο θα είναι ιδιωτικής χρήσης, και άρα πρέπει να το κάνουμε δίκτυο τέτοιας μορφής : 192.168.1.0. Αυτό επίσημα λέγεται "ιδιωτικό δίκτυο Τάξης C", σε περίπτωση που θέλετε να εντυπωσιάσετε τους φίλους σας.

Πρώτα, πρέπει να βεβαιωθούμε ότι έχει ενεργοποιηθεί η δικτύωση. Αλλάξτε το αρχείο /etc/sysconfig/network, και βεβαιωθείτε πως περιέχει τις εξής γραμμές :

```
NETWORKING=yes
FORWARD_IPV4=yes
```

Η πρώτη γραμμή λέει στο Linux πως επιθυμούμε η δικτύωση να ενεργοποιείται κατευθείαν με την εκκίνηση του Η/Υ. Η δεύτερη γραμμή λέει στο Linux να ενεργοποιήσει την προώθηση αριθμών IP (IP forwarding). Αυτή απαιτείται γιά τη ρύθμιση του μασκαρίσματος (masquerading), που θα πούμε στην ενότητα 4 του HowTo.

Σημείωση γιά το RedHat : Το RedHat 6.2 απαιτεί αλλαγές στο αρχείο /etc/sysctl.conf, γιά να υποστηρίξει σωστά το IP forwarding και το masquerading. Βεβαιωθείτε ότι υπάρχουν κι έχουν τις σωστές τιμές παραμέτρων οι ακόλουθες γραμμές :

```
net.ipv4.ip_forward = 1
net.ipv4.ip_always_defrag = 1
```

Όλες οι ρυθμίσεις δικτύου γιά το RedHat και τις παράγωγες διανομές του RedHat περιέχονται σε αρχεία, στο directory /etc/sysconfig/network-scripts directory. Κάντε cd ς' αυτό το directory, και φτιάξτε ένα νέο αρχείο, το ifcfg-eth1. Μέσα ς' αυτό γράψτε τα εξής :

```
DEVICE=eth1
IPADDR=192.168.1.1
ONBOOT=yes
```

Αυτός ο κώδικας λέει στα scripts δικτύου να ρυθμίσουν την eth1 κατά την εκκίνηση, και να της δώσουν μιά συγκεκριμένη διεύθυνση IP. Ενεργοποιείστε τις νέες ρυθμίσεις στο δίκτυό σας με την ακόλουθη εντολή : `/etc/rc.d/init.d/network restart`

3.2.2 O DHCP server

Ενας DHCP server αποδίδει αυτόματα διευθύνσεις IP στους Η/Υ που βρίσκονται συνδεδεμένοι στο σπιτικό σας δίκτυο. Είναι πολύ χρήσιμος, όταν έχουμε φορητούς Η/Υ : Μπορούμε απλά να συνδέσουμε τους φορητούς Η/Υ στο δίκτυο, και αμέσως να δικτυωθούν σωστά. Αν δεν θέλετε DHCP server στο εσωτερικό σας δίκτυο, να προχωρήσετε στην επόμενη ενότητα.

Πρώτα πρέπει να βεβαιωθείτε ότι ο DHCP server είναι εγκατεστημένος. Κάντε mount το CD του Linux σας, και εγκαταστήστε το πακέτο `dhcp` RPM. Τώρα, αλλάξτε το αρχείο `/etc/dhcpd.conf`, και προσθέστε τα εξής (και μόνον αυτά) :

```
subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.2 192.168.1.60;
default-lease-time 86400;
max-lease-time 86400;
option routers 192.168.1.1;
option ip-forwarding off;
option broadcast-address 192.168.1.255;
option subnet-mask 255.255.255.0;
}
```

Αν πρόκειται να στήσετε τον Linux Η/Υ σας σαν caching domain name server, δώστε την ακόλουθη επιλογή :

```
option domain-name-servers 192.168.1.1;
```

Εάν γνωρίζετε την εξωτερική DNS διεύθυνσή σας, και δεν πρόκειται να χρησιμοποιήσετε τον Linux Η/Υ γιά DNS, δώστε την ακόλουθη επιλογή (όπου x.x.x.x και y.y.y.y είναι αριθμοί IP των DNS servers) :

```
option domain-name-servers x.x.x.x, y.y.y.y;
```

Εάν πρόκειται να βάλετε την κοινή χρήση αρχείων με το πρότυπο Samba στον Linux Η/Υ σας (γιά χάρη των Η/Υ σας με Windows), προσθέστε τις ακόλουθες γραμμές, ώστε ο Linux Η/Υ να γίνει ο εξ ορισμού WINS και browsing server :

```
option netbios-name-servers 192.168.1.1;
option netbios-dd-server 192.168.1.1;
option netbios-node-type 8;
option netbios-scope "";
```

Οι ρυθμίσεις των Samba και WINS βρίσκονται πολύ έξω από τα όρια του παρόντος κειμένου. Αν χρειάζεστε κάποιες υποδείξεις, ξεκινήστε με το *SMB HOWTO*, και συνεχίστε από εκεί.

Υπάρχουν ακόμη λίγα βήματα. Τώρα, ανοίξτε το αρχείο `/etc/rc.d/init.d/dhcpd`, και ψάξτε να βρείτε την εξής γραμμή :

```
/sbin/route add -host 255.255.255.255 dev eth1
```

Οι DHCP clients με Windows απαιτούν εκπομπή μιας συγκεκριμένης διεύθυνσης στις αποκρίσεις DHCP, και η παραπάνω εντολή αναγκάζει τον TCP/IP stack του Linux να την παράγει. Εάν δεν μπορείτε να βρείτε αυτή τη γραμμή στο αρχείο αυτό, *προσθέστε την*. Αν *βρείτε* μιά παρόμοια γραμμή, βεβαιωθείτε ότι η συσκευή στην οποία αναφέρεται, είναι η `eth1`.

Το επόμενο βήμα είναι ν' αλλάξουμε το αρχείο `/etc/rc.d/init.d/dhcpd`, ώστε να δέχεται σαν default τη συσκευή `eth1`. Αντικαταστήστε τη γραμμή :

```
daemon /usr/sbin/dhcpd
```

με :

```
daemon /usr/sbin/dhcpd eth1
```

Τώρα είμαστε έτοιμοι να ξεκινήσουμε το DHCP. Πρώτα ξεκινάμε τον DHCP server, με την εντολή : `/etc/rc.d/init.d/dhcpd start`.

Τελικά, πρέπει να βεβαιωθούμε ότι ο DHCP server θα ξεκινήσει κατά την επανεκκίνηση. Μερικά πακέτα RPM του DHCP server δεν περιέχουν εντολές, που να σιγουρεύουν ότι ο server θα ξεκινάει κάθε φορά, άρα πρέπει να βεβαιωθούμε εμείς ότι ξεκινάει, δίνοντας την εντολή : `chkconfig dhcpd on`.

Αυτή η εντολή κάνει το RedHat να προσθέσει το script εκκίνησης του dhcp στα διάφορα directories των runlevels, κάτω από το `/etc/rc.d`. Ο DHCP server ξεκινάει στα runlevels 3 και 5 (multiuser κονσόλα και multiuser X). Στα runlevels 0, 1 και 6 (shutdown, μονοχρησία και reboot), ο DHCP server σταματάει.

3.2.3 Οι client Η/Υ

Αν έχετε ήδη ρυθμίσει το DHCP, είναι πολύ εύκολο να ρυθμίσετε και τους client Η/Υ σας : Απλά ενεργοποιείστε τη ρύθμιση του DHCP. Γιά Η/Υ με Windows, αυτό σημαίνει ν' ανοίξετε τον Πίνακα Ρυθμίσεων ("Control Panel"), και μετά την επιλογή δικτύωσης ("Networking"). Βρείτε το πρωτόκολλο "TCP/IP", και βάλτε Ρύθμιση ("Configure"). Κάντε τσεκάρισμα στο κουτάκι, που λέει να ρυθμίσουμε αυτόματα τη διεύθυνση TCP/IP ("Configure TCP/IP address automatically"), εφαρμόστε τις αλλαγές σας, και επανεκκινήστε.

Πριν επανεκκινήσετε, όμως, τον server, μπορείτε να δώσετε και την εξής εντολή : `tail -f /var/log/messages`. Αυτή παρακολουθεί συνεχώς τα logs στο Linux. Αν όλα πάνε καλά, με την επανεκκίνηση των Windows Η/Υ σας θα δείτε να ζητάνε διεύθυνση IP, και ο DHCP server ν' ανταποκρίνεται. (Η εντολή `tail -f` τερματίζεται, αν πατήσουμε Control-C.)

Αν δεν έχετε ρυθμίσει το DHCP, η ρύθμιση εξακολουθεί να παραμένει εύκολη. Ξανανοίξτε τη Δικτύωση ("Networking") του Πίνακα Ρυθμίσεων ("Control Panel"), και επιλέξτε τη ρύθμιση του πρωτοκόλλου TCP/IP. Μπορείτε να δώσετε στους client Η/Υ σας οποιαδήποτε διεύθυνση του δικτύου 192.168.1.0 , εκτός της 192.168.1.0 (δηλ. της διεύθυνσης του ίδιου του δικτύου), της 192.168.1.255 (δηλ. της διεύθυνσης broadcast), ή της 192.168.1.1 (της διεύθυνσης του Linux server Η/Υ). Ποτέ μη δώσετε την ίδια διεύθυνση IP σε δύο Η/Υ. Κάντε τη διεύθυνση "Gateway" 192.168.1.1, ώστε η κυκλοφορία προς το έξω δίκτυο να περνάει από τον gateway Η/Υ.

Το *IP Masquerading HOWTO* έχει λεπτομερείς πληροφορίες γιά τις ρυθμίσεις των clients, στο *κεφάλαιο των ρυθμίσεων*.

Γενικά, γιά να ρυθμίσουμε έναν client Η/Υ, είτε ενεργοποιούμε τη ρύθμιση DHCP, είτε της δίνουμε με το χέρι μιά διεύθυνση στην περιοχή 192.168.1.x, με gateway 192.168.1.1 . Ο DNS server πρέπει να είναι είτε ο 192.168.1.1, αν τρέχετε έναν caching DNS server (δες παρακάτω), ή να κατευθύνει το DNS στις διευθύνσεις που σας έδωσε ο Internet Provider σας.

3.2.4 Ο DNS server

Ρυθμίζοντας τον Linux Η/Υ σας σαν caching DNS server, θα καλυτερεύσει (ελαφρά) την ταχύτητα σερφαρίσματος, επειδή οι συχνής χρήσης διευθύνσεις DNS θα κασαριστούν μέσα στο δίκτυό σας, και δεν θα τις παίρνετε κάθε φορά απ' έξω.

Εάν ενδιαφέρεστε να υλοποιήσετε ένα πλήρες DNS, υπάρχουν πολλά σύνθετα πράγματα που πρέπει να μάθετε. Υπάρχει ένα *DNS HOWTO* διαθέσιμο, και το βιβλίο *DNS and BIND* αποτελεί μιά καλή (και πολύ κατανοητή) γραπτή πηγή αναφοράς.

Γιά να εκμεταλλευτούν τον caching server οι client Η/Υ σας, πρέπει να ρυθμιστούν, ώστε να χρησιμοποιήσουν τη Linux gateway ως τον πρωτεύοντα DNS server τους. Ένα τρόπος γιά να γίνει αυτό, είναι οι κατευθυντήριες εντολές γιά το DHCP, που δίδονται στην ενότητα 3.2.2 . Αν ρυθμίζετε με το χέρι τους client Η/Υ σας, μπορείτε ν' αλλάξετε τις ρυθμίσεις του DNS με τον ίδιο τρόπο που χρησιμοποιήσατε γιά να γράψετε τη διεύθυνση IP.

Γιά να εγκαταστήσετε τον DNS server, πρώτα εγκαταστήστε το πακέτο `bind` RPM, και μετά το `caching-nameserver` RPM. Σ' αυτό το σημείο, έχουμε σχεδόν τελειώσει.

Ο caching server θα δουλέψει μιά χαρά με τον τρόπο που τον εγκαταστήσαμε. Ωστόσο, αν γνωρίζετε τις διευθύνσεις IP των DNS servers του Internet Provider σας (στο εξής "ISP" - ς.τ.μ.), μπορείτε ν' αυξήσετε ακόμη λίγο την απόδοση, αλλάζοντας το αρχείο `/etc/named.conf`, και προσθέτοντας την εξής γραμμή μετά τη γραμμή `directory` (όπου x.x.x.x και y.y.y.y είναι αντίστοιχα ο πρωτεύων και ο δευτερεύων DNS servers) :

```
forwarders { x.x.x.x; y.y.y.y; };
```

Αυτή η αλλαγή κάνει τον DNS server πρώτα να ρωτάει τους DNS servers του ISP, πριν διασχίσει το Internet ψάχνοντας γιά μιά συγκεκριμένη διεύθυνση. Οι servers του ISP συνήθως έχουνε πάρα πολλές διευθύνσεις κασαρισμένες, και επομένως μπορούν να δώσουν ταχύτερη απάντηση απ' ό,τι θα μπορούσε ο δικός σας server.

Ο daemon `named` είχε κάποια προβλήματα ασφάλειας το προηγούμενο 12μηνο, άρα είναι πολύ σημαντικό το να έχετε την πλέον πρόσφατη έκδοση, και να κάνετε κάποιες αλλαγές στις εξ ορισμού ρυθμίσεις, ώστε ν' αυξήσετε την ασφάλεια του συστήματος.

1. Ελέγξτε την έκδοση του `bind` σας, και βεβαιωθείτε ότι είναι τουλάχιστον η 8.2.2. Πηγαίνετε στο site *Ανανεώσεις του RedHat*, ή στο *Ανανεώσεις του Mandrake*, ώστε να ψάξετε γιά την πιο πρόσφατη έκδοση.
2. Περιορίστε την πρόσβαση στον name server σας, ώστε να την έχει μόνο το τοπικό δίκτυο. Προσθέστε τη γραμμή `allow-query { 192.168.1/24; 127.0.0.1/32; };` στο αρχείο `/etc/named.conf`, μετά τη γραμμή `forwarders`.
3. Αποφύγετε να τρέχετε τον name server σας ως `root`. Εάν ο server τρέχει ως root, ένα χάκεμα του server θα δώσει στον χάκερ τα προνόμια του root. Αν τρέχετε τον server ως χρήστης χωρίς πολλά δικαιώματα, πχ σαν `nobody`, θα χαμηλώσετε το επίπεδο κινδύνου χακέματος του name server. Γιά να τρέξετε τον name server ως `nobody`, διορθώστε το αρχείο `/etc/rc.d/init.d/named`, και αλλάξτε τη γραμμή `daemon named` σε `daemon named -u nobody -g nobody`.

Βεβαιωθείτε ότι ο DNS server σας θα ενεργοποιηθεί με το bootάρισμα : `chkconfig named on`. Πάλι, αυτό σιγουρεύει ότι ο server θα ξεκινήσει στα συνηθισμένα runlevels (3 και 5) κατά το bootάρισμα.

Εντάξει, τώρα μπορείτε να ξεκινήσετε τον DNS server σας : `/etc/rc.d/init.d/named start`

3.2.5 Τεστάροντας το εσωτερικό δίκτυο

Το DNS δεν θα δουλέψει μέχρι να ρυθμίσουμε το εξωτερικό δίκτυο, (μιά που πρέπει να επικοινωνήσει με άλλους DNS servers επάνω στο Internet), αλλά με το πρόγραμμα `ping` μπορούμε να τεστάρουμε την βασική εσωτερική σύνδεση.

Ανοίξτε ένα παράθυρο τερματικού (MS-DOS) ς' έναν από τους client Η/Υ σας, και δώστε : `ping 192.168.1.1`. Αυτή η εντολή θα στέλνει σε τακτικά χρονικά διαστήματα πακέτα προς τον Linux Η/Υ σας, κι αυτός θα τα ξαναστέλνει πίσω. Αν όλα δουλεύουν σωστά, θα βλέπετε ένα σύνολο χρόνων επιστροφής των πακέτων.

3.3 Ρυθμίζοντας το εξωτερικό δίκτυο

Τώρα είμαστε έτοιμοι να ρυθμίσουμε το εξωτερικό δίκτυο. Μερικές φορές αυτό θα είναι δύσκολο, ανάλογα με το πόσο καλά υποστηρίζει το Linux ο ISP σας. Αν έχετε δυσκολίες, υπάρχει το *ADSL mini-HOWTO*, που καλύπτει τα θέματα της σύνδεσης ADSL αρκετά λεπτομερειακά. Εάν βρω και κανένα Cable Modem HOWTO, θα βάλω link και γι' αυτό.

Το κύριο πρόβλημα με τις περισσότερες εξωτερικές συνδέσεις είναι *το να πάρεις μιά διεύθυνση IP*. Μερικοί ISPs δίνουν στατικές διευθύνσεις IP σε συνδρομητές με σύνδεση cable (καλωδιακό) modem ή ADSL, και ς' αυτή την περίπτωση η ρύθμιση είναι εύκολη. Ωστόσο, οι περισσότεροι ISPs έχουνε πλέον προσανατολιστεί σε δυναμική σύνδεση μέσω (σωστά μαντέψατε!) DHCP. Αυτό σημαίνει ότι ο Linux Η/Υ σας θα είναι DHCP *server* στην κάρτα δικτύου `eth1` interface, και DHCP *client* στην κάρτα δικτύου `eth0`.

Επιπλέον, πολλοί ISPs παρέχουν τις υπηρεσίες τους με εξειδικευμένο τρόπο, που προϋποθέτει ότι οι πελάτες τους χρησιμοποιούν Windows. Μερικές απ' αυτές τις περιπτώσεις θα συζητηθούν στο τέλος της ενότητας 3.3.2. .

3.3.1 Με στατική διεύθυνση IP

Εάν ο ISP σας σας έδωσε στατική διεύθυνση IP, έχετε ξενοιάσει. Φτιάξτε ένα νέο αρχείο ρυθμίσεων της σύνδεσης, το `/etc/sysconfig/network-scripts/ifcfg-eth0`, και βάλτε τα εξής μέσα του :

```
DEVICE=eth0
IPADDR=x.x.x.x
NETMASK=y.y.y.y
ONBOOT=yes
```

Απλά αντικαταστήστε τα x.x.x.x και y.y.y.y με τις τιμές που σας έδωσε ο ISP. Τώρα, διορθώστε το αρχείο `/etc/resolv.conf`, και γράψτε τις ακόλουθες γραμμές :

```
search provider_domain_here
nameserver n.n.n.n
nameserver m.m.m.m
```

Το provider_domain πρέπει κανονικά να σας το δώσει ο ISP σας. Επίσης, βάλτε τους πρωτεύοντα και δευτερεύοντα DNS servers στις γραμμές n.n.n.n και m.m.m.m . Αν έχετε ρυθμίσει τον Linux Η/Υ σαν DNS server, προσθέστε μιά γραμμή πριν τις γραμμές γιά τους άλλους nameservers : `nameserver 127.0.0.1`. Αυτή θα κάνει τον Linux server να χρησιμοποιήσει τον caching server, πριν ζητήσει από τους εξωτερικούς servers πληροφορίες γιά DNS.

3.3.2 Με το DHCP

Αν ο ISP σας έχει ρυθμιστεί ως DHCP, πρέπει να φτιάξετε ένα νέο αρχείο ρυθμίσεων της σύνδεσης, το `/etc/sysconfig/network-scripts/ifcfg-eth0`, και προσθέστε του τα εξής :

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Τώρα, βεβαιωθείτε ότι ο dhcpcd client daemon είναι εγκατεστημένος στο σύστημά σας. Πηγαίνετε στα Linux CD σας, κι εγκαταστήστε το πακέτο `dhcpcd` RPM.

Έφτασε λοιπόν η στιγμή να δοκιμάσουμε τις ρυθμίσεις του νέου μας δικτύου. Απλά δίνουμε την εντολή `/etc/rc.d/init.d/network restart`. Μετά, με ping κάνουμε δοκιμή της εξωτερικής σύνδεσης. Κάνουμε ping ς' έναν Η/Υ στο Internet, σαν τον `www.yahoo.com`, και περιμένουμε μήπως επιστρέψει κάποιο πακέτο.

3.3.3 Παραξενιές και ανωμαλίες

Η κατάσταση με το δίκτυό σας μπορεί να είναι διαφορετική από τα απλά παραδείγματα που περιγράφονται παραπάνω. Ιδού μερικές σύντομες παρατηρήσεις επάνω στις διάφορες δυσκολίες, και links και διευθύνσεις προς περισσότερο έγκυρες πηγές. Ευχαριστώ τον John Mellor, που μου έδωσε τα links και την ώθηση να προσθέσω αυτήν την ενότητα.

ΠΠΠ επάνω σε Ετηερνετ (ΠΠΠοΕ) Μερικοί ADSL providers (πχ η Bell Atlantic) επιμένουν τελευταία να συνδέονται οι νέοι τους πελάτες μέσω του πρωτοκόλλου "PPP over Ethernet" (PPPoE). Γιά τον σκοπό αυτό, δίνουνε στους νέους συνδρομητές ένα client πρόγραμμα γιά Windows : κάτι όχι ιδιαίτερα χρήσιμο σε χρήστες Linux. Ευτυχώς, όμως, το PPPoE είναι ένα απλό πρωτόκολλο, και γίνονται ήδη πολλές προσπάθειες να υποστηριχθεί και από το Linux.

- Ο αναγνώστης Kerr First συνιστά ένθερμα το *Roaring Penguin PPPoE Client*.
- Υπάρχει και το *PPPoE on Linux for Bell Sympatico*,
- και τα *General Info* και *Linux Info*.

Χαζά κόλπα με το ΔΗΓΠ Ένα από τα αγαπημένα κόλπα των ISPs είναι το να σε συνδέουν μ' ένα και μοναδικό host name, ή ακόμη και με μία και μοναδική κάρτα πρόσβασης στο δίκτυο. Αυτό υποθετικά γίνεται γιά να ς' εμποδίσει να βάζεις πολλούς Η/Υ στο δίκτυό σου, με τη χρήση hub. (Φυσικά, με χρήση Linux και masquerading έχουμε το ίδιο αποτέλεσμα με καλύτερη ασφάλεια, και ο ISP δεν διαθέτει τρόπο να γνωρίζει αν έγινε αυτό!!)

Εάν ο ISP σας έδωσε ένα host name, και επέμεινε να δώσετε στον Windows Η/Υ σας αυτό το όνομα, ώστε να σας αφήσει να χρησιμοποιήσετε τη σύνδεση, τότε πρέπει να σιγουρευτείτε ότι ο Linux Η/Υ σας στέλνει πρώτα αυτό το host name, όταν ζητάει μιά διεύθυνση από τον DHCP server.

Όταν βάζετε dhcp στο BOOTPROTO, στο αρχείο ρυθμίσεων της σύνδεσης, καλείται μεν ο RedHat DHCP client, αλλά χωρίς ν' αναφέρεται σε κάποιο host name. Γιά να καλείτε το πρόγραμμα με host name στο RedHat 6.1, διορθώστε το αρχείο `/etc/sysconfig/network`, και αλλάξτε τη γραμμή :

`HOSTNAME=`

ώστε να γράφει :

`HOSTNAME=your_isp_assigned_name`

Αυτό μπορεί να μη δουλέψει σε μερικές παραλλαγές του RedHat. Αν δεν δουλέψει, ελέγξτε το `/sbin/ifup` script και κοιτάξτε αν οι κλήσεις των dhcpcd και pump περιλαμβάνουν μιά παράμετρο -h $HOSTNAME. Αν όχι, προσθέστε την, ώστε οι κλήσεις να γίνουν κάπως έτσι : `/sbin/dhcpcd -i $DEVICE -h $HOSTNAME` και `/sbin/pump -i $DEVICE -h $HOSTNAME`.

Η εταιρία Ροαδ Ρυννερ Η εταιρία καλωδιακών συνδέσεων Road Runner έχει μιά ειδική διαδικασία login, που πρέπει να τρέξει πριν χρησιμοποιηθεί ο server. Ευτυχώς, υπάρχει ένα λεπτομερές *Linux Road Runner HOWTO*.

3.3.4 Κοιτάζοντας τις ρυθμίσεις του δικτύου

Τώρα, μπορείτε να θαυμάσετε το έργο σας. Δώστε `ifconfig`, γιά να δείτε όλες τις ρυθμισμένες συσκευές σας. Στον δικό μου gateway Η/Υ, παίρνω τα εξής :

```
eth0  Link encap:Ethernet  HWaddr 00:60:67:4A:02:0A
      inet addr:24.65.182.43  Bcast:24.65.182.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
      RX packets:487167 errors:0 dropped:0 overruns:0 frame:0
```

```
      TX packets:467064 errors:0 dropped:0 overruns:0 carrier:0
      collisions:89 txqueuelen:100
      Interrupt:10 Base address:0xe400
eth1  Link encap:Ethernet  HWaddr 00:80:C8:D3:30:2C
      inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
      RX packets:284112 errors:0 dropped:0 overruns:0 frame:1
      TX packets:311533 errors:0 dropped:0 overruns:0 carrier:0
      collisions:37938 txqueuelen:100
      Interrupt:5 Base address:0xe800
lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      UP LOOPBACK RUNNING  MTU:3924  Metric:1
      RX packets:12598 errors:0 dropped:0 overruns:0 frame:0
      TX packets:12598 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
```

Σημειώστε ότι η κάρτα `eth0` έχει μιά εντυπωσιακή εξωτερική διεύθυνση IP, και η κάρτα `eth1` μιά ιδιωτική εσωτερική διεύθυνση.

Μπορείτε να δείτε τα routes του δικτύου, δίνοντας την εντολή `route`. Στον gateway Η/Υ μου, παίρνω ένα μήνυμα σαν αυτό :

```
Kernel IP routing table
Destination     Gateway      Genmask         Flags Metric Ref Use Iface
255.255.255.255 *            255.255.255.255 UH    0      0     0 eth1
192.168.1.0     *            255.255.255.0   U     0      0     0 eth1
24.65.182.0     *            255.255.255.0   U     0      0     0 eth0
127.0.0.0       *            255.0.0.0       U     0      0     0 lo
default         24.65.182.1  0.0.0.0         UG    0      0     0 eth0
```

Εδώ μπορούμε να δούμε ότι το εξωτερικό δίκτυο είναι ρυθμισμένο, το εσωτερικό δίκτυο είναι ρυθμισμένο, η τοπική συσκευή επίσης, η ειδική διεύθυνση broadcast 255.255.255.255 επίσης, και το default route είναι ρυθμισμένο να δείχνει την gateway του ISP. Τέλειο!

Τώρα έχουμε και τα έξω, και τα μέσα. Απομένει ν' ανοίξουμε την πόρτα μεταξύ τους. Ωστόσο, πρώτα πρέπει να βεβαιωθούμε ότι δεν μπορούν να μπουν μέσα τίποτε τέρατα απ' έξω.

3.4 Ασφάλεια

Ένα από τα μειονεκτήματα της μόνιμης σύνδεσης στο Internet μέσω ADSL ή καλωδιακού modem, είναι πως ο Η/Υ μας είναι εκτεθειμένος σε πιθανές απειλές της ασφάλειάς του 24 ώρες τη μέρα, 7 μέρες την εβδομάδα. Η χρήση του Linux ως gateway περιορίζει το ρίσκο, επειδή κρύβει όλους τους υπόλοιπους Η/Υ στο δίκτυό σας : Όσον αφορά το υπόλοιπο Internet, συνδεδεμένος είναι μόνον ο Linux Η/Υ σας. Αυτό σημαίνει ότι το δίκτυό σας μπορεί να είναι τόσο σίγουρο, όσο ο Linux Η/Υ σας, επομένως ς' αυτό το σημείο θα σας δώσω μερικές βασικές συμβουλές, γιά να τον κάνετε ασφαλέστερο.

Πρώτα, πρέπει να κλείσετε έξω όλους τους κακούς. Γιά να γίνει αυτό, διορθώστε το αρχείο /etc/hosts.deny, και βεβαιωθείτε ότι έγινε ακριβώς όπως παρακάτω :

```
#
# hosts.deny  \textgreek{Aut'o} \textgreek{to} \textgreek{arqe'io} \textgreek{perigr'afei} \textgreek{ta} \textgreek{on'omata} \textgreek{twn} host \textgreek{H}/\textgreek{U}, \textgreek{pou}
#             *\textgreek{den}* \textgreek{epitr'epetai} \textgreek{na} \textgreek{qrhsimopoio'un} \textgreek{tic} \textgreek{topik'ec} \textgreek{uphres'iec}
#             INET, \textgreek{'opwc} \textgreek{kajor'izetai} \textgreek{ap'o} \textgreek{ton} "/usr/sbin/tcpd" server.
#
#             \textgreek{H} \textgreek{gramm'h} \textgreek{gi'a} \textgreek{ton} portmap \textgreek{e'inai} \textgreek{peritt'h}, \textgreek{all'a} \textgreek{af'hnetai} \textgreek{gi'a}
#             \textgreek{na} \textgreek{sac} \textgreek{jum'izei} \textgreek{'oti} \textgreek{o} \textgreek{n'eoc} \textgreek{asfal'hc} portmap \textgreek{qrhsimopoie'i} \textgreek{to}
#             hosts.deny \textgreek{kai} \textgreek{to} hosts.allow . \textgreek{Eidik'otera}, \textgreek{ja} \textgreek{'eprepe} \textgreek{na}
#             \textgreek{gnwr'izete} \textgreek{'oti} \textgreek{to} NFS \textgreek{qrhsimopoie'i} \textgreek{ton} portmap!
ALL: ALL
```

Τα παραπάνω λένε στους "TCP wrappers" (οι οποίοι ελέγχουν το 95% των εισερχομένων συνδέσεων) να αρνηθούν κάθε σύνδεση από κάθε host Η/Υ. Αυτή είναι αρκετά καλή απαγόρευση! Αλλά επίσης θα σας εμποδίσει και να συνδεθείτε με τον Linux Η/Υ σας από το εσωτερικό σπιτικό σας δίκτυο, πράγμα ενοχλητικό. Επομένως, θα κάνουμε μιά εξαίρεση. Διορθώνουμε το αρχείο /etc/hosts.allow, και το κάνουμε ακριβώς έτσι :

```
#
# hosts.allow  \textgreek{Aut'o} \textgreek{to} \textgreek{arqe'io} \textgreek{perigr'afei} \textgreek{ta} \textgreek{on'omata} \textgreek{twn} host \textgreek{H}/\textgreek{U}, \textgreek{pou}
#              \textgreek{touc} \textgreek{epitr'epetai} \textgreek{na} \textgreek{qrhsimopoio'un} \textgreek{tic} \textgreek{topik'ec} \textgreek{uphres'iec}
#              INET, \textgreek{'opwc} \textgreek{kajor'izetai} \textgreek{ap'o} \textgreek{ton} "/usr/sbin/tcpd" server.
#
ALL: 127.0.0.1
ALL: 192.168.1.
```

Τα παραπάνω λένε στους "TCP wrappers" ότι μπορούν να επιτρέψουν συνδέσεις προς όλες τις υπηρεσίες της τοπικής συσκευής (local device, 127.0.0.1), και προς το σπιτικό δίκτυο (192.168.1.) .

Τώρα έχετε κλειδώσει τα τέρατα έξω, με ισχυρό λουκέτο. Αν θέλετε να βάλετε μπάρες και συναγερμούς, πρέπει να έχετε πολύ περισσότερες γνώσεις. Το *Security HOWTO* είναι ένα καλό μέρος γιά ν' αρχίσετε το διάβασμα, αν θέλετε να μάθετε περισσότερα γιά το πώς ν' ασφαλίζετε τον Linux Η/Υ σας.

4 Ρυθμίσεις μασκαρίσματος (masquerading)

Όλα καλά! Τα προκαταρκτικά τελειώσανε, κι εδώ ακριβώς αρχίζει η μαγεία. Το μασκάρισμα IP είναι μία από τις πραγματικά μαγικές ευκολίες του Linux. Υπάρχουν εμπορικά προϊόντα γιά τα Windows, που κάνουνε το ίδιο πράγμα, αλλά όχι τόσο αποτελεσματικά. Ενας αρχαίος 386 μπορεί μιά χαρά να κάνει μασκάρισμα IP γιά ένα ολόκληρο γραφείο μεσαίου μεγέθους, αλλά δεν μπορεί καν να τρέξει Windows 95 - ας αφήσουμε κατά μέρος το πρόγραμμα μασκαρίσματος γιά Windows. (Σαν υστερόγραφο, διάβασα σε πρόσφατες ειδήσεις ότι τα Windows 2000 θα υποστηρίζουν "κοινή χρήση συνδέσεων" χωρίς επιπρόσθετο software. Φαίνεται ότι οι εταιρίες που πουλούσαν προγράμματα κοινής χρήσης συνδέσεων, "αγκαλιάστηκαν από και πλάτυναν με τη βοήθεια της" MicroSoft. Ωστόσο, δεν θα συνιστούσα να δοκιμάσετε Windows 2000 επάνω σε 386.)

Το Linux διαθέτει μιά τρομερά ευέλικτη ικανότητα firewalling, την οποία και θα χρησιμοποιήσουμε εδώ με τον πλέον απλό και χονδροειδή τρόπο. Αν επιθυμείτε να κάνετε firewalling σαν ειδικός στο θέμα, πρέπει να διαβάσετε το *Firewalling HOWTO* γιά κατανόηση της θεωρίας, και το *IPChains HOWTO* γιά οδηγίες επάνω στο νέο εργαλείο firewalling, το `ipchains`, που πάει μαζί με τον πυρήνα 2.2.x του Linux (και, κατ' επέκταση, του RedHat 6.x). Επίσης, είναι διαθέσιμο σήμερα και το πολύ καλό *IP Masquerading HOWTO*, που καλύπτει με περισσότερες λεπτομέρειες τα κόλπα του μασκαρίσματος.

Είναι πάρα πολύ εύκολο το να ρυθμίσουμε ένα απλό μασκάρισμα, από τη στιγμή που θα δουλεύουν και το εσωτερικό και το εξωτερικό δίκτυο. Διορθώνουμε το αρχείο `/etc/rc.d/rc.local`, και προσθέτουμε τις εξής γραμμές στο τέλος του :

```
# 1) \textgreek{Adei'azoume} \textgreek{touc} \textgreek{p'inakec} \textgreek{kan'onwn}.
/sbin/ipchains -F input
/sbin/ipchains -F forward
/sbin/ipchains -F output
# 2) \textgreek{Or'izoume} \textgreek{touc} \textgreek{qronismo'uc} MASQ \textgreek{kai} \textgreek{epitr'epoume} \textgreek{na} \textgreek{mpoun} \textgreek{pak'eta} \textgreek{gi'a}
# \textgreek{r'ujmish} \textgreek{tou} DHCP.
/sbin/ipchains -M -S 7200 10 60
/sbin/ipchains -A input -j ACCEPT -i eth0 -s 0/0 68 -d 0/0 67 -p udp
# 3) \textgreek{Arno'umaste} \textgreek{thn} \textgreek{pro'wjhsh} \textgreek{'olwn} \textgreek{twn} \textgreek{pak'etwn}, \textgreek{ekt'oc} \textgreek{'oswn} \textgreek{e'inai} \textgreek{tou}
# \textgreek{topiko'u} \textgreek{dikt'uou}. \textgreek{Aut'a} \textgreek{ta} \textgreek{mask'aroume}.
/sbin/ipchains -P forward DENY
/sbin/ipchains -A forward -s 192.168.1.0/24 -j MASQ
# 4) \textgreek{Fort'wnoume} modules \textgreek{pro'wjhshc} \textgreek{gi'a} \textgreek{eidiko'uc} \textgreek{skopo'uc}.
/sbin/modprobe ip_masq_ftp
/sbin/modprobe ip_masq_raudio
```

Οι τελευταίες δύο γραμμές εισάγουν modules του πυρήνα, που επιτρέπουν να δουλεύουν το FTP και το RealAudio στους Η/Υ του εσωτερικού δικτύου. Υπάρχουν κι άλλα modules γιά ειδικές υπηρεσίες, που μπορείτε να τα σκαλίσετε, αν τα χρειαστείτε ποτέ :

- CUSeeMe (`/sbin/modprobe ip_masq_cuseeme`)
- Internet Relay Chat (`/sbin/modprobe ip_masq_irc`)
- Quake (`/sbin/modprobe ip_masq_quake`)
- VDOLive (`/sbin/modprobe ip_masq_vdolive`)

Τώρα είσαστε έτοιμοι να δοκιμάσετε το μασκάρισμα! Τρέξτε το `rc.local` script με την εντολή `/etc/rc.d/rc.local`, και φύγατε! Καθίστε σε κάποιον άλλον Η/Υ σας, και δοκιμάστε λίγο σερφάρισμα στο Internet. Με λίγη τύχη, όλα τώρα είναι κυριλέ!

5 Προβλήματα

Υπάρχουν ένα σωρό πράγματα που μπορεί να μην πάνε καλά με την εφαρμογή των οδηγιών ενός απλού κειμένου σαν αυτό εδώ, επειδή υπάρχουν πολλές ειδικές περιπτώσεις. Η πλειοψηφία των πιθανών προβλημάτων εστιάζεται στη ρύθμιση του εσωτερικού και του εξωτερικού δικτύου. Θα προσπαθήσω ν' απαντώ σε αναγνώστες με προβλήματα, να κατανοώ το τί δεν πήγε καλά, και να προσθέτω links εδώ στο τέλος, ώστε όσοι έχουνε ειδικής μορφής προβλήματα, να μπορούν να βρουν βοήθεια. Επικοινωνήστε ελεύθερα μαζί μου στο *pramsey@refractions.net*.

5.1 To ICQ δεν δουλεύει

Μερικά κομμάτια του ICQ δουλεύουν μιά χαρά με το μασκάρισμα. Κάποια άλλα δεν δουλεύουν καθόλου καλά. Ωστόσο, υπάρχει ένα *beta quality ICQ module* υπό ανάπτυξη, που ασχολείται με μερικές (αλλά όχι όλες) από τις ελλείψεις της λειτουργίας του ICQ μαζί με μασκάρισμα. Το αρχείο `README` μέσα στον κώδικα source, περιγράφει πώς να κάνετε compile το module. Αφού το κάνετε compile και το εγκαταστήσετε, καλέστε το : `/sbin/modprobe ip_masq_icq`.

5.2 Έχω Caldera 2.x, όχι RedHat 6.x

Λοιπόν, πρώτα τα συγχαρητήριά μου που τη σπάτε στη μόδα! Δεύτερον, ο Nelson Gibbs (ngibbs@pacbell.net) στέλνει καλά νέα, επειδή οι περισσότερες από τις οδηγίες εφαρμόζονται και στο δικό σας Linux. Ωστόσο, υπάρχουν μερικές σημαντικές αλλαγές που πρέπει να κάνετε :

1. Μιά δήλωση `GATEWAY=xxx.xxx.xxx.xxx` στο αρχείο `/etc/sysconfig/network-scripts/ifcfg-eth0` & `eth1` γιά τη σύνδεση (η τοπική σύνδεση χρησιμοποιεί τη διεύθυνση IP της μακρινής σύνδεσης, και η μακρινή σύνδεση χρησιμοποιεί το IP της gateway του ISP).

2. Βεβαιωθείτε ότι το `/etc/sysconfig/daemons/dhcpd` script δείχνει το `ROUTE_DEVICE` ως `eth1`, *όχι* `eth0`.

3. Το `/etc/dhcpd.conf` απαιτεί μιά δήλωση υποδικτύου (subnet) και γιά τις δύο κάρτες. Δεν ξέρω ακριβώς το γιατί, καθώς έκανα τη δεύτερη δήλωση : subnet 216.102.154.201 netmask 255.255.255.255 { } χωρίς άλλες παραμέτρους, και ο DHCP server ακούει και στέλνει στις eth0 και eth1, καθώς και στην επιστροφή (fallback). Ο DHCP server βγάζει μήνυμα σφάλματος, εάν ορίσουμε μόνο το ένα υποδίκτυο.

4. *Μην* προσθέσετε host route `255.255.255.255`, το `/etc/rc.d/init.d/dhcpd` script που χρησιμοποιεί η Caldera διορθώνει το πρόβλημα από μόνο του. *Βεβαιωθείτε* πως αλλάξατε όλες τις αναφορές στο `eth0` του script σε `eth1`.

5.3 Θέλω ένας από τους εσωτερικούς Η/Υ μου να γίνει ο Web server μου

Πανεύκολο! Ωστόσο, *πρέπει να έχετε στατική διεύθυνση IP*, γιά να έχουν αποτέλεσμα αυτές οι απλές οδηγίες. Εάν έχετε δυναμική διεύθυνση IP, θα χρειαστείτε ακόμη κάμποση δουλειά στα scripts, γιά να σιγουρέψετε το ότι η IP διεύθυνσή σας ανανεώνεται με τις εντολές προώθησης πακέτων, όταν η διεύθυνση αλλάζει.

Να θυμάστε ότι η προώθηση μιας εξωτερικής θύρας προς έναν εσωτερικό Η/Υ μετατρέπει τον "εσωτερικό" Η/Υ σε λιγότερο "εσωτερικό" απ' ό,τι πριν, αλλά μπορεί να γίνει διαφανώς και με ελάχιστη πτώση της απόδοσης. Ένα από τα πλεονεκτήματα του κώδικα μασκαρίσματος μέσα στον πυρήνα του Linux, είναι η ικανότητα να κάνουμε μερικά εντυπωσιακά πράγματα με τα πακέτα που φτάνουνε στο επίπεδο του δικτύου, και η utility `ipmasqadm` γράφτηκε γιά να εκμεταλλευτεί ακριβώς αυτά.

Γιά κάποιο λόγο, η `ipmasqadm` δεν συμπεριλαμβάνεται σε όλες τις παραλλαγές του RedHat και του Mandrake, άρα μάλλον πρέπει να την πάρουμε από το *web site* του προγραμματιστή της - υπάρχει ένα πακέτο *RPM* διαθέσιμο εκεί, καθώς και ο source κώδικας.

Αφού πάρετε το RPM, εγκαταστήστε το, και μετά προσθέστε τις εξής γραμμές στο `/etc/rc.d/rc.local` αρχείο σας :

```
/usr/sbin/ipmasqadm portfw -f
/usr/sbin/ipmasqadm portfw -a -P tcp -L x.x.x.x 80 -R 192.168.1.x 80
```

Η πρώτη εντολή αδειάζει τους κανόνες προώθησης θύρας (port forwarding rules), και η δεύτερη προσθέτει μιά προώθηση από τη θύρα 80 της εξωτερικής σύνδεσης προς τη θύρα 80 του εσωτερικού Η/Υ. Σημειώστε ότι η εξωτερική στατική διεύθυνση IP πάει στη θέση του x.x.x.x , και η διεύθυνση IP του εσωτερικού Η/Υ πάει στη θέση του 192.168.1.x .

Τώρα, οι εξωτερικές αιτήσεις γιά τη θύρα 80 θα σταλούν διαφανώς στη θύρα 80 του εσωτερικού μηχανήματος. Σημειώστε ότι δεν μπορείτε να το τεστάρετε αυτό με telnet, ή με σύνδεση στη θύρα 80 της gateway σας από έναν από τους εσωτερικούς Η/Υ σας : Ο προωθητής θύρας αποκρίνεται μόνο σε εισερχόμενες αιτήσεις προς την *εξωτερική* σύνδεση.