Π Α Ν Ε Π Ι Σ Τ Η Μ Ι Ο Π Α Τ Ρ Ω Ν
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ε Ρ Γ Α Σ Ι Α Ε Ξ Α Μ Η Ν Ο Υ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ

&

ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ

ΠΡΩΤΟΚΟΛΛΟ DHCP ΚΑΙ ΑΝΑΛΥΣΗ ΤΗΣ ΜΕΘΟΔΟΥ NAT

ΜΟΣΧΟΓΙΑΝΝΙΔΟΥ ΙΩΑΝΝΑ

Α.Μ 5358

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2015

ΠΕΡΙΕΧΟΜΕΝΑ

1 ΕΙΣΑΓΩΓΗ

Είναι γεγονός ότι ζούμε στην εποχή που οι περισσότερες ηλεκτρονικές συσκευές μπορούν να συνδεθούν στο Ίντερνετ, είναι δηλαδή "IP-capable" [1]. Αυτό σημαίνει ότι οποιαδήποτε στιγμή συνδέσουμε μια συσκευή σε ένα δίκτυο, θα πρέπει να της ανατεθεί μια διεύθυνση IP. Από τα παραπάνω λοιπόν, προκύπτουν δύο βασικές ανάγκες:

1) ένας τρόπος ώστε να αρκούν οι διευθύνσεις για όλες τις συσκευές ανά πάσα στιγμή, και
2) ένας μηχανισμός ώστε μία συσκευή κάθε φορά που συνδέεται να μπορεί να αποκτάει μια IP διεύθυνση **αυτόματα**, χωρίς να χρειάζεται να επιβαρύνεται με αυτό το έργο ο διαχειριστής του δικτύου.

Όσο αφορά το πρώτο, στην παρούσα εργασία θα μελετήσουμε μία "βραχυπρόθεσμη" και έντονα αμφιλεγόμενη λύση, το Network Address Translation (NAT). Η βασική ιδέα είναι η δημιουργία ιδιωτικών (private) δικτύων τα οποία είναι συνδεδεμένα **έμμεσα** στο Ίντερνετ, μέσω NAT-enabled δρομολογητών οι οποίοι μεταφράζουν τις ιδιωτικές διευθύνσεις σε δημόσιες (απαραίτητα μοναδικές) και αντίστροφα.
Ο ακριβής μηχανισμός αυτής της λύσης, οι διάφορες κατηγορίες στις οποίες μπορεί να ταξινομηθεί, οι τρόποι να αντιμετωπιστούν τα διάφορα προβλήματα που προκύπτουν καθώς και τα πλεονεκτήματα και τα μειονεκτήματα θα αναλυθούν στη συνέχεια.

Το πρωτόκολλο που δίνει τη δυνατότητα να καλυφθεί η δεύτερη ανάγκη είναι γνωστό ως Dynamic Host Configuration Protocol (DHCP).

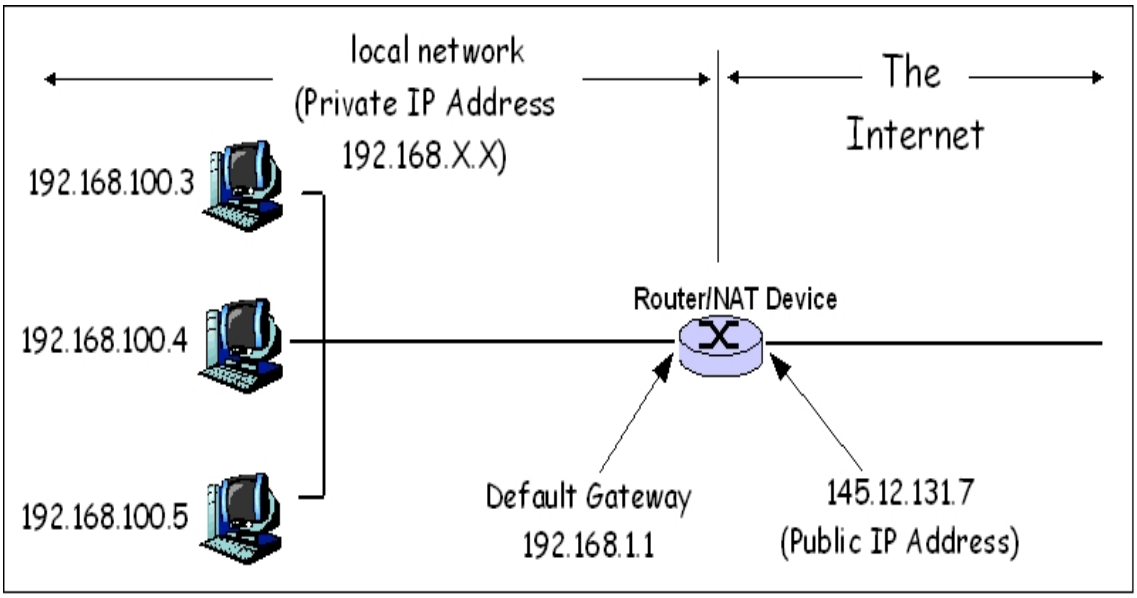
2 NETWORK ADDRESS TRANSLATION (NAT)

2.1 Τι είναι το NAT, για ποιο λόγο χρησιμοποιείται και πως λειτουργεί

Το NAT είναι ένα Internet standard το οποίο ορίστηκε αρχικά στο RFC 1631. Ο διάδοχός του, το RFC 3022, επεκτείνει και εισάγει κάποιες διορθώσεις στον ήδη υπάρχων μηχανισμό.

Καθώς πολλοί Small Office, Home Office (SOHO) χρήστες μπορεί να έχουν πολλαπλές δικτυακές συσκευές, η καθεμία από τις οποίες να πρέπει να τρέχει τις δικές της εφαρμογές [8], ένα εύρος από IP διευθύνσεις θα πρέπει να δεσμευτεί έτσι ώστε να τις καλύψει. Αυτό εισάγει έναν αριθμό από προβλήματα, μιας και ο IP χώρος διευθύνσεων είναι περιορισμένος και η απόκτηση ενός μεγάλου μπλοκ από καταχωρημένες διευθύνσεις είναι δύσκολη [2]. Η λύση είναι η χρήση ιδιωτικών διευθύνσεων (RFC 1918) εσωτερικά στο δίκτυο με τις οποίες όμως οι διάφορες συσκευές (hosts) δεν έχουν τρόπο να έχουν πρόσβαση στο Ίντερνετ (είτε για λόγους ιδιωτικότητας είτε επειδή δεν είναι έγκυρες έξω από το δίκτυο [8]). Εδώ έρχεται το NAT, που επιτρέπει τη μετάφραση των ιδιωτικών διευθύνσεων στις απαιτούμενες καθολικές και μοναδικές. Οι hosts εντός ενός ιδιωτικού δικτύου μπορούν έτσι με έναν *διαφανή* τρόπο να έχουν πρόσβαση στον "έξω κόσμο", έχοντας εξασφαλίσει την ιδιωτικότητα και τις λεπτομέρειες του δικτύου κρυφές.
Όλα αυτά προϋποθέτουν φυσικά την ύπαρξη ενός κατάλληλα ρυθμισμένου δρομολογητή, του λεγόμενου "NAT-enabled router". Ο δρομολογητής αυτός συμπεριφέρεται για οποιονδήποτε πέρα του δικτύου που ανήκει σαν *μία* συσκευή με *μία* IP. Την IP αυτή την αποκτάει μέσω του DHCP server (για τον οποίο θα μιλήσουμε αργότερα) του παροχέα υπηρεσιών διαδικτύου (ISP - Internet Service Provider) στον οποίο ανήκει, και έπειτα "γίνεται" ο ίδιος ένας DHCP server που παρέχει IP διευθύνσεις στις συσκευές εντός του δικτύου [1].

Παρακάτω δίνεται με τη βοήθεια ενός σχήματος ένα παράδειγμα χρήσης του NAT:



Βλέπουμε ότι το NAT-enabled router αποτελείται από μία ιδιωτική (private) διεύθυνση, την 192.168.1.1, και από μία δημόσια (public), την 145.12.131.7. Η κίνηση που φεύγει από το δρομολογητή (προερχόμενη από οποιοδήποτε υπολογιστή του δικτύου) με προορισμό το Ίντερνετ, όπως και η κίνηση που φτάνει στο δρομολογητή από το Ίντερνετ (με προορισμό οποιοδήποτε υπολογιστή του δικτύου) έχει IP πηγής (source address) και αντίστοιχα IP προορισμού (destination address) τη δημόσια IP διεύθυνση.
Όταν ένα διάγραμμα θα φτάσει στο δρομολογητή από έναν υπολογιστή του δικτύου (έστω αυτόν με IP 192.168.100.4), τότε αυτός θα αντικαταστήσει την source IP address με τη δική του δημόσια, θα του αναθέσει ένα καινούριο port number και αφού δημιουργήσει μία καταχώρηση στον πίνακα μετάφρασης (NAT translation table) που διαθέτει θα στείλει το διάγραμμα. Όταν αυτό θα φτάσει στον προορισμό του (και υποθέτοντας ότι περιέχει κάποιου είδους αίτηση, όπως για παράδειγμα για μία σελίδα από κάποιον Web server ο οποίος θα πρέπει να στείλει την αντίστοιχη απάντηση), αγνοώντας ότι το διάγραμμα έχει τροποποιηθεί από το NAT-enabled router θα στείλει την απάντηση με destination IP address και port number που αντιστοιχούν στο δρομολογητή. Φτάνοντας στο δρομολογητή, αυτός ελέγχει τον πίνακα μετάφρασης για να αποκτήσει την κατάλληλη IP διεύθυνση και port number για τον υπολογιστή που πρέπει να καταλήξει το διάγραμμα. Αφού τα βρει, τα αντικαθιστεί και προωθεί το διάγραμμα εντός του δικτύου.

2.2 Παραλλαγές του NAT

Ο πιο απλός τύπος NAT ονομάζεται **one-to-one** ή **Basic NAT** [7] Ο τύπος αυτός αλλάζει τις IP διευθύνσεις στην IP επικεφαλίδα και χρησιμοποιείται όταν υπάρχει επαρκής αριθμός από IP διευθύνσεις για one-to-one μετάφραση [2].
Το παράδειγμα που δόθηκε παραπάνω αφορά τον πιο συνηθισμένο τύπο NAT [6], που είναι γνωστός ως **one-to-many** NAT ή **NAPT** (Network Address Port Translation, [7]), αφού αντιστοιχίζει πολλαπλούς (ιδιωτικούς) hosts με μία δημόσια IP διεύθυνση και σε αντίθεση με το Basic NAT συμπεριλαμβάνει port translation (επιπέδου 2-transport). Χρησιμοποιείται όταν δεν υπάρχει επαρκής αριθμός από IP διευθύνσεις για να μεταφραστούν όλες οι εσωτερικές διευθύνσεις [2].

2.3 Τύποι του NAT

Όλοι οι τύποι του NAT εμπίπτουν σε δύο κατηγορίες: Το στατικό (**static**) NAT και το δυναμικό (**dynamic**) NAT.
Το static NAT είναι αυτό όπου οι διαχειριστές δημιουργούν και συντηρούν **χειροκίνητα** τις NAT αντιστοιχίσεις (mappings), ενώ στο dynamic NAT ο δρομολογητής δημιουργεί και συντηρεί τα mappings **αυτόματα** κατ' απαίτηση. Από τους παρακάτω τέσσερις τύπους, μόνο το full-cone NAT είναι static ενώ οι υπόλοιποι τρεις ανήκουν στην κατηγορία του dynamic NAT [4].

Full-cone
Σε ένα full-cone NAT όλες οι αιτήσεις από μία συγκεκριμένη **εσωτερική** IP διεύθυνση και port αντιστοιχίζονται σε μια ίδια/συγκεκριμένη **εξωτερική** IP διεύθυνση και port. Οποιοσδήποτε εξωτερικός host μπορεί να στείλει ένα πακέτο σε κάποιον εσωτερικό απευθύνοντας το πακέτο στην εξωτερική IP διεύθυνση [9].
Λόγω του ότι η υλοποίηση αυτή είναι απλή και περιορισμένων δυνατοτήτων, δε χρησιμοποιείται σε μεγάλης κλίμακας δίκτυα αλλά κυρίως σε παλιές συσκευές και σε χαμηλού επιπέδου home routers [3].

(Address)-restricted-cone
Σε ένα restricted cone NAT όλες οι αιτήσεις από μία συγκεκριμένη **εσωτερική** IP διεύθυνση και port αντιστοιχίζονται σε μια ίδια/συγκεκριμένη **εξωτερική** IP διεύθυνση και port. Αντίθετα όμως με το full-cone NAT, ένας εξωτερικός host με κάποια IP μπορεί να στείλει ένα πακέτο σε κάποιον εσωτερικό μόνο αν ο εσωτερικός είχε στείλει προηγουμένως κάποιο πακέτο σ αυτήν την IP [9].
Από τη σκοπιά της ασφάλειας αυτή η παραλλαγή του NAT είναι πολύ καλύτερη από ότι η full-cone, μιας και το NAT λειτουργεί ως τείχος προστασίας. Παρόλα αυτά από τη στιγμή που έχει γίνει το "δέσιμο" μεταξύ ενός εσωτερικού και ενός εξωτερικού host, οποιοδήποτε πακέτο που φτάνει με source IP διεύθυνση υπάρχουσα στη λίστα με τις επιτρεπόμενες, αφήνεται να περάσει και να προωθηθεί στον εσωτερικό host [3].

Port-restricted cone

Ένα port-restricted cone NAT είναι σαν ένα restricted-cone NAT, μόνο που ο περιορισμός που αναφέρθηκε συμπεριλαβάνει port numbers. Ειδικότερα, ένας εξωτερικός host με κάποια IP και port number μπορεί να στείλει ένα πακέτο σε κάποιον εσωτερικό μόνο αν ο εσωτερικός είχε στείλει προηγουμένως κάποιο πακέτο σ αυτήν την IP και port number [9].

Symmetric
Σε ένα symmetric NAT όλες οι αιτήσεις από μία συγκεκριμένη **εσωτερική** IP διεύθυνση και port σε μια συγκεκριμένη **εξωτερική** IP διεύθυνση και port αντιστοιχίζονται στην *ίδια* εξωτερική IP διεύθυνση και port. Αν ο εσωτερικός host στείλει ένα πακέτο σε διαφορετικό προορισμό, χρησιμοποιείται διαφορετική αντιστοίχηση (mapping). Επιπλέον, μόνο ένας εξωτερικός host που έχει λάβει πακέτο από έναν εσωτερικό μπορεί να του στείλει πίσω κάποιο πακέτο [9].
Τα Symmetric NAT, όπως περιγράφεται στο STUN [9], είναι τα πιο συνηθισμένα NAT που συναντάει κανείς σε μεγάλες επιχειρήσεις.

2.4 Hairpinning

Το hairpinning είναι μια τεχνική που επιτρέπει σε δύο host που ανήκουν στο ίδιο δίκτυο (και πίσω από ένα NAT) να επικοινωνήσουν χρησιμοποιώντας τη δημόσια IP διεύθυνση [3]. Η NAT συσκευή προωθεί τα πακέτα προερχόμενα από ένα host στο δίκτυο (έστω host A) πίσω σε κάποιον άλλο host (host B) μέσα στο ίδιο δίκτυο, όταν ανιχνεύσει ότι η δημόσια IP διεύθυνση του προορισμού του πακέτου είναι στην πραγματικότητα μία αντιστοιχισμένη IP διεύθυνση που δημιουργήθηκε για τον host (host B) [5].
Αυτή είναι μία πολύ επιθυμητή συμπεριφορά του NAT, την οποία όμως δεν υποστηρίζουν όλες οι NAT συσκευές [5].
Αν δεν υπήρχε αυτή η συμπεριφορά, δύο (εσωτερικοί) host πίσω από το ίδιο NAT δε θα μπορούσαν να επικοινωνήσουν ο ένας με τον άλλο αν αντάλλασσαν τις δημόσιες IP διευθύνσεις τους [5].

2.5 NAT traversal και port forwarding

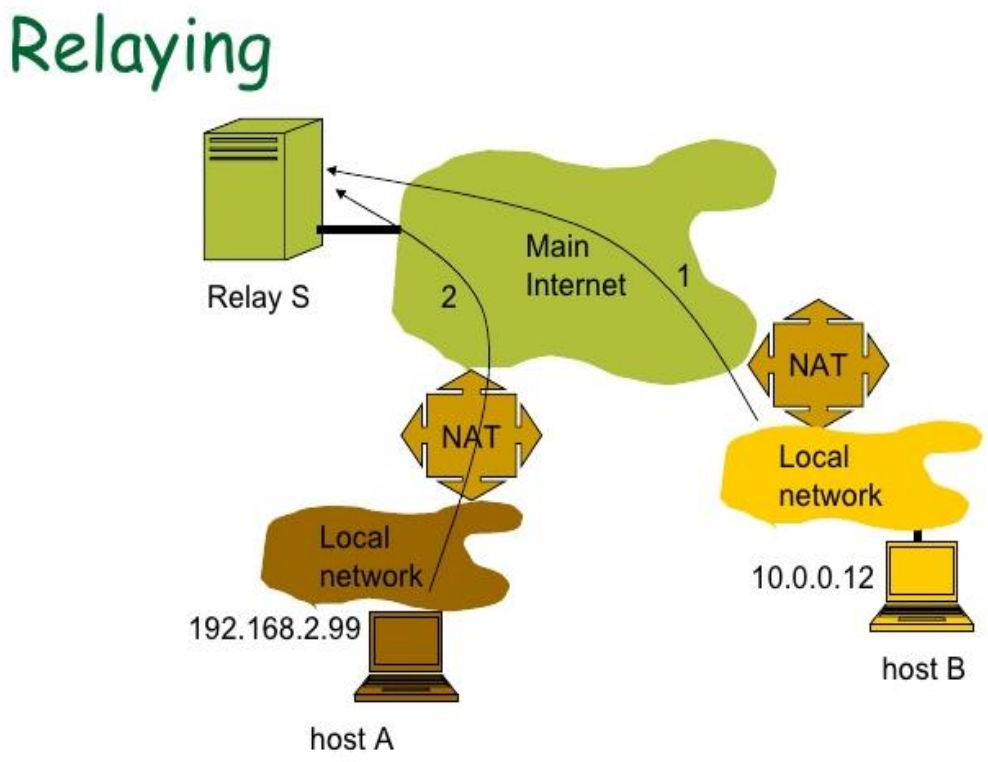
Σε ένα δίκτυο, κάθε host αναγνωρίζεται από μία IP διεύθυνση και είναι επομένως προσβάσιμος από οποιονδήποτε άλλο host. Με το NAT όμως, όλοι οι hosts "πίσω" του είναι προσβάσιμοι με μία (την ίδια) διεύθυνση. Αυτό δημιουργεί προβλήματα όταν ένας host που δεν βρίσκεται πίσω από ένα NAT θέλει να συνδεθεί με κάποιον που είναι. Το NAT δε θα ξέρει σε ποιον host να προωθήσει τα πακέτα [3].

Μία λύση σ αυτό είναι να ρυθμίσουμε χειροκίνητα τη συσκευή NAT ώστε να προωθεί εξωτερικές συνδέσεις σε καθορισμένα port στους host του δικτύου. Αυτή η τεχνική λέγεται **port forwarding**. Η λύση αυτή μπορεί να λειτουργεί, αλλά είναι δύσκολη ως προς τη διαχείριση ειδικά αν υπάρχουν πολλοί host πίσω από το NAT. Επιπλέον, κάτι τέτοιο απαιτείται από κάθε εφαρμογή σε κάθε ένα host, και αν η IP κάποιου υπολογιστή αλλάξει, τότε πρέπει να αλλάξουν και οι κανόνες του port forwarding [3].
Πέρα από το port forwarding υπάρχουν και άλλες τεχνικές για το λεγόμενο **NAT traversal**, κάποιες από τις οποίες θα αναλύσουμε στη συνέχεια.

2.6 Τεχνικές για NAT traversal

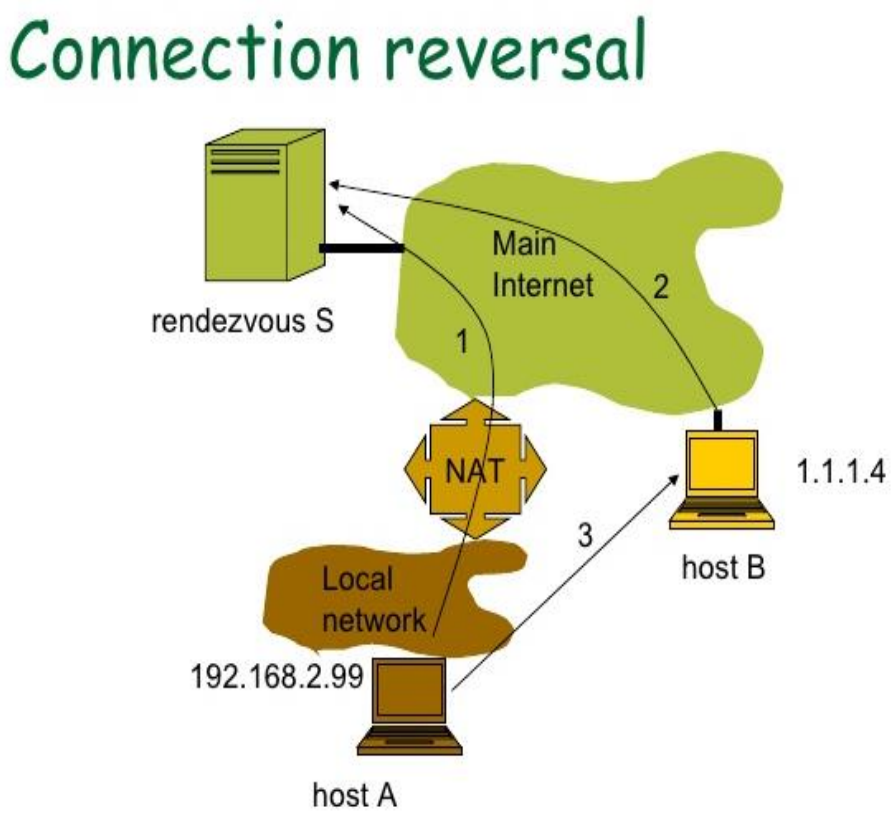
2.6.1 **RELAYING** [3]

Η πιο αξιόπιστη αλλά λιγότερη αποδοτική μέθοδος είναι το relaying. Απαιτεί την ύπαρξη ενός εξυπηρετητή που μπορεί να χειριστεί μεγάλο όγκο δεδομένων, καθώς όλη η κίνηση μεταξύ των host θα περνάει μέσα από αυτόν.
Για παράδειγμα, αν κάποιος peer (έστω peer A) θέλει να επικοινωνήσει με κάποιον άλλο (peer B) τότε πρέπει και οι δύο να ανοίξουν και να διατηρήσουν μία σύνδεση με τον relaying εξυπηρετητή που δεν είναι πίσω από NAT. Αφού έχει γίνει αυτό, ο peer A στέλνει τα δεδομένα του στον relaying εξυπηρετητή, ο οποίος θα τα μεταφέρει στον peer B. Όλα τα δεδομένα που στέλνονται από τους δύο peer θα περάσουν μέσω αυτού του εξυπηρετητή.
Το relaying υποστηρίζεται από όλους τους τύπους NAT (Full Cone, Address-Restricted Cone, Port-Restricted Cone και Symmetric), σε οποιαδήποτε αρχιτεκτονική δικτύου (χωρίς ή με NAT) καθώς είναι βασικά μια επικοινωνία τύπου πελάτη-εξυπηρετητή.
Το relaying έχει ένα μεγάλο μειονέκτημα: όλα τα δεδομένα μεταδίδονται μέσω ενός εξυπηρετητή, ο οποίος οπότε χρησιμοποιεί μεγάλο εύρος ζώνης και προσφέρει λίγη ασφάλεια καθώς ο κάτοχός του μπορεί να δει όλα τα μεταφερόμενα δεδομένα και ακόμα να τα φιλτράρει. Επιπλέον, αν ο εξυπηρετητής "πέσει", οι peer δεν μπορούν να συνδεθούν ώστε να στείλουν πακέτα.



2.6.2 **Connection Reversal** [3]

Η τεχνική αυτή είναι μια απλοποίηση της τεχνικής UDP/TCP hole punching υπό την έννοια ότι λειτουργεί μόνο όταν ο ένας peer δεν είναι πίσω από NAT.
Η βασική αρχή είναι ότι πρέπει ο peer που βρίσκεται πίσω από NAT (έστω peer A) να στείλει ένα πακέτο στον peer που δε βρίσκεται πίσω από NAT (peer B). Αυτό θα ανοίξει ένα port στο NAT του peer A και έτσι ο peer B θα μπορεί να περάσει μέσα από αυτήν την "τρύπα" (hole). Αλλά αυτό προϋποθέτει ότι ο peer A γνωρίζει την IP διεύθυνση και το TCP/UDP port του peer B ώστε να ξεκινήσει τη σύνδεση. Αυτό μπορεί να γίνει με τη βοήθεια ενός εξωτερικού εξυπηρετητή μέσω του οποίου οι peer μπορούν να μοιραστούν τις IP διευθύνσεις τους, ώστε ο peer A να έχει τη δυνατότητα να ανοίξει το απαιτούμενο κενό στο NAT του.
Αυτή η τεχνική λειτουργεί με όλους του τύπους του NAT επειδή η διαδικασία προσωμοιώνει μία σύνδεση πελάτη-εξυπηρετητή (ο πελάτης είναι ο peer πίσω από το NAT, ο οποίος κάνει όλες τις συνδέσεις).



2.7 Πλεονεκτήματα-Μειονεκτήματα

Το NAT έχει το μεγάλο πλεονέκτημα ότι μπορεί να εγκατασταθεί *σταδιακά,* χωρίς να χρειάζεται να γίνουν αλλαγές στους hosts και τους δρομολογητές.
Αν και πρόκειται για μία ευρέως χρησιμοποιούμενη τεχνική, έχει κάποια μειονεκτήματα.
Αρχικά, ενώ το NAT λειτουργεί μια χαρά για τυπικές πελάτη-εξυπηρετητή επικοινωνίες (όπως είναι το web και το e-mail), καθώς είναι ο πελάτης αυτός που ξεκινάει τη σύνδεση και δε χρειάζεται συνήθως να διατηρήσει τη σύνδεση για πολύ, η εγκατάσταση του NAT μπορεί να δημιουργήσει τεράστιο πρόβλημα στην peer-to-peer επικοινωνία, όπως για παράδειγμα το VoIP [5]. Το NAT λοιπόν παρεμβαίνει και δυσκολεύει τις peer-to-peer (P2P) εφαρμογές. Τεχνικές για να παρακαμθούν οι δυσκολίες που δημιουργούνται είναι μέσω του NAT traversal (ενότητα 2.6), όπου μεταξύ άλλων βρίσκουμε το relaying (υποενότητα 2.6.1), το connection reversal (υποενότητα 2.6.2) κλπ.
Ίσως το πιο βασικό είναι ότι παραβιάζει το λεγόμενο “end-to-end” επιχείρημα, όπου οι hosts θα έπρεπε να επικοινωνούν απ' ευθείας ο ένας με τον άλλο χωρίς να

τροποποιούν οι ενδιάμεσοι κόμβοι τις IP διευθύνσεις και τα port number [1], και στο οποίο επιχείρημα βασίζονται πολλά πρωτόκολλα και εφαρμογές του Ίντερνετ.

2.8 Συμπέρασμα

Το NAT δημιουργήθηκε για να αντιμετωπιστούν οι ελλείψεις του χώρου διευθύνσεων του πρωτοκόλου IP version 4. Μέχρις ότου λοιπόν άλλες, πιο εκτεταμένες λύσεις (όπως ίσως η πλήρης ανάπτυξη του IP version 6 στο οποίο δεν περιλαμβάνεται το NAT) είναι διαθέσιμες θα πρέπει να αρκεστούμε στο NAT, το οποίο όπως και να έχει αποτελεί μια σημαντική συνιστώσα του Ίντερνετ.

3 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

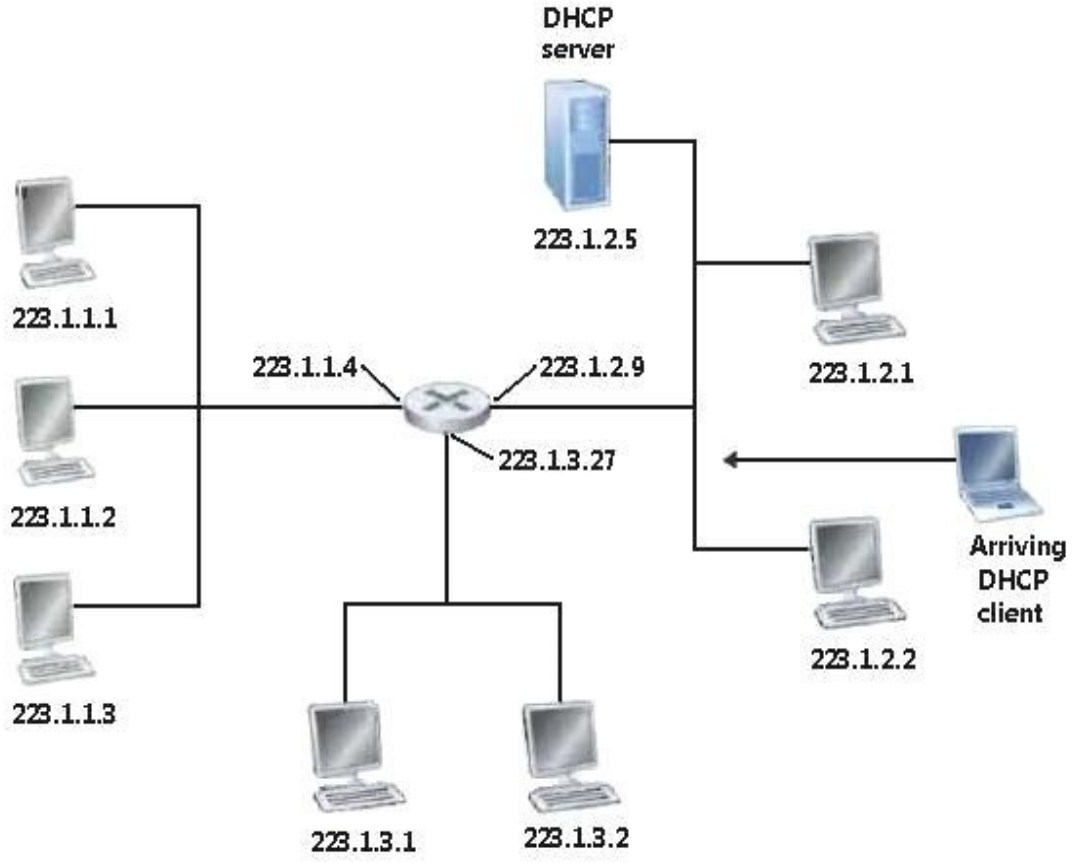
3.1 Εισαγωγή και μηχανισμοί του DHCP

Όπως έχουμε αναφέρει, κάθε συσκευή για να μπορεί να συνδεθεί στο Ίντερνετ χρειάζεται να έχει μία IP διεύθυνση. Η διεύθυνση αυτή μπορεί να ανατεθεί στη συσκευή είτε χειροκίνητα από το διαχειριστή του συστήματος, είτε αυτόματα μέσω του πρωτόλλου **DHCP**.
Το DHCP λοιπόν, επιτρέπει σε έναν πελάτη να αποκτήσει μια IP διεύθυνση αυτόματα και επίσης να μάθει επιπλέον πληροφορίες, όπως την διεύθυνση του δρομολογητή πρώτου άλματος (first hop router) καθώς και την διεύθυνση του DNS εξυπηρετητή του.

Το DHCP υποστηρίζει τρεις μηχανισμούς για την κατανομή (allocation) IP διευθύνσεων [10]. Στην "αυτόματη κατανομή" (automatic allocation), το DHCP αναθέτει μία **μόνιμη** διεύθυνση στον πελάτη. Στην "δυναμική κατανομή" (dynamic allocation), το DHCP αναθέτει μία IP διεύθυνση στον πελάτη για περιορισμένο χρονικό διάστημα (ή μέχρι ο πελάτης να "αφήσει" τη διεύθυνση). Τέλος, στην "χειροκίνητη κατανομή" (manual allocation) η IP διεύθυνση του πελάτη δίνεται από το διαχειριστή του δικτύου και το DHCP χρησιμοποιείται απλά για να του μεταφέρει τη διεύθυνση.
Οποιοδήποτε δίκτυο θα χρησιμοποιήσει ένα ή περισσότερους από αυτούς τους μηχανισμούς με βάση την πολιτική του υπεύθυνου διαχειριστή δικτύου.

Η δυναμική κατανομή είναι ο μόνος από τους τρεις μηχανισμούς που επιτρέπει την αυτόματη επαναχρησιμοποίηση μιας διεύθυνσης που δεν είναι πλέον απαραίτητη από τον πελάτη που του έχει ανατεθεί. Επιπλέον, η δυναμική κατανομή είναι ιδιαίτερα χρήσιμη για κάποιον πελάτη που θα είναι συνδεδεμένος στο δίκτυο προσωρινά ή για την περίπτωση που υπάρχει μικρός αριθμός από διαθέσιμες IP διευθύνσεις για ανάθεση και οι πελάτες δε χρειάζονται μόνιμες διευθύνσεις. Είναι μια καλή επιλογή ακόμα για κάποιον νέο πελάτη που είναι μόνιμα συνδεδεμένος σε ένα δίκτυο στο οποίο οι IP διευθύνσεις είναι σπάνιες και περιορισμένες και είναι ζωτικής σημασίας να επαναποκτηθούν αφού οι παλιοί πελάτες αποσυρθούν [10].

Το DHCP είναι ένα πρωτόκολλο πελάτη-εξυπηρετητή. Ο πελάτης είναι συνήθως ένας host που μόλις έχει "φτάσει" και θέλει να αποκτήσει κάποιες πληροφορίες για το δίκτυο συμπεριλαμβανομένης μιας IP διεύθυνσης [1].
Στην πιο απλή περίπτωση, κάθε υποδίκτυο θα περιέχει έναν DHCP εξυπηρετητή. Αν όχι, τότε απαιτείται ένας DHCP relay agent (παράγοντας που λειτουργεί εκ μέρους κάποιου DHCP εξυπηρετητή), συνήθως ένας δρομολογητής, που γνωρίζει την IP διεύθυνση του DHCP εξυπηρετητή για αυτό το δίκτυο [1].



Στην παραπάνω εικόνα ο DHCP εξυπηρετητής βρίσκεται στο υποδίκτυο 223.1.2/24 και ο δρομολογητής είναι ο relay agent για τους πελάτες που φτάνουν στα υποδίκτυα 223.1.1/24 και 223.1.3/24 [1].

3.2 Διαδικασία ανάθεσης IP διεύθυνσης

Για ένα νέο host η διαδικασία που ακολουθεί το DHCP μπορεί να αποδοθεί στα τέσσερα ακόλουθα βήματα [1]:

- Ανακάλυψη εξυπηρετητή DHCP (DHCP server discovery): Η πρώτη ενέργεια λοιπόν του host είναι η εύρεση ενός DHCP εξυπηρετητή με τον οποίο να αλληλεπιδράσει. Αυτό γίνεται μέσω ενός **DHCP μηνύματος ανακάλυψης** το οποίο

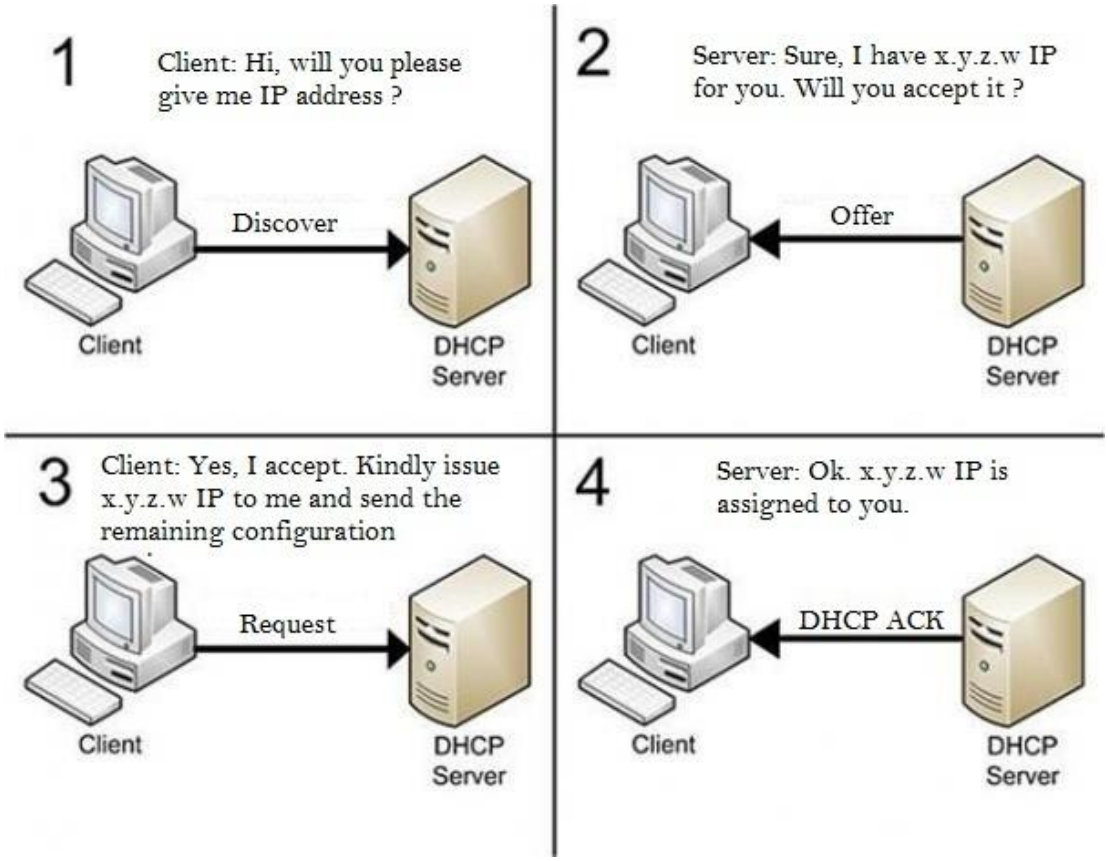
στέλνεται σε όλους τους κόμβους του δικτύου μέσω broadcast. Αυτό γίνεται γιατί ο host δε γνωρίζει ούτε την IP του δικτύου στο οποίο θέλει να συνδεθεί, πόσο μάλλον την IP κάποιου DHCP εξυπηρετητή.

- Προσφορά εξυπηρετητή DHCP (DHCP server offer): Ένας DHCP εξυπηρετητής ο οποίος λαμβάνει το DHCP μήνυμα ανακάλυψης θα απαντήσει στον host με ένα **DHCP μήνυμα προσφοράς**, το οποίο θα στείλει σε όλους τους κόμβους του δικτύου. Το μήνυμα αυτό περιέχει μεταξύ άλλων την προσφερόμενη IP διεύθυνση και το χρόνο για τον οποίο θα είναι έγκυρη. Δεδομένου ότι υπάρχει δυνατότητα να υπάρχουν περισσότεροι από ένας DHCP εξυπηρετητές στο δίκτυο οπότε και το DHCP μήνυμα ανακάλυψης να έχει ληφθεί από περισσότερους του ενός, ο πελάτης μπορεί να επιλέξει ανάμεσα σε πολλά DHCP μηνύματα προσφοράς.

- Αίτηση DHCP (DHCP request): Ο πελάτης θα επιλέξει μία από τις προσφορές και θα απαντήσει σ αυτήν με ένα **DHCP μήνυμα αίτησης.**

- Επιβεβαίωση λήψης DHCP (DHCP ACK): Ο εξυπηρετητής θα απαντήσει με ένα **DHCP μήνυμα επιβεβαίωσης**, επιβεβαιώνοντας έτσι τις παραμέτρους της ζητούμενης προσφοράς.

Αφού ο host λάβει το DHCP μήνυμα επιβεβαίωσης η αλληλεπίδραση έχει ολοκληρωθεί και μπορεί πλέον να χρησιμοποιήσει την IP διεύθυνση. Αν ο χρόνος εγκυρότητας της διεύθυνσης λήξει και ο host τη χρειάζεται ακόμα, το DHCP παρέχει ένα μηχανισμό που του επιτρέπει να ανανεώσει το χρόνο χρήσης της.



3.3 Πλεονεκτήματα-Μειονεκτήματα

Το DHCP χρησιμοποιείται ευρέως σε τοπικά και σε ασύρματα δίκτυα, όπου οι host εισέρχονται και εξέρχονται από το δίκτυο τακτικά.

Εξαιτίας της ικανότητας του DHCP να αυτοματοποιεί κάποιες ενέργειες της διαδικασίας σύνδεσης ενός host σε κάποιο δίκτυο, συχνά αναφέρεται ως ένα **plug-and-play** πρωτόκολλο [1]. Τα οφέλη αυτής του της ικανότητας είναι εμφανή, αν αναλογιστούμε ότι η εναλλακτική είναι η χειροκίνητη ρύθμιση της IP διεύθυνσης και η οποία θα ήταν για κάποιον host που θα μεταφερόταν διαρκώς σε διαφορετικά υποδίκτυα (και επομένως θα έπρεπε να του ανατίθεται ξανά και ξανά μια διεύθυνση) ή για τον διαχειριστή του συστήματος μια επίπονη τουλάχιστον διαδικασία.

Παρ όλα αυτά, αυτή η αυτοματοποίηση μπορεί να εισάγει έναν αριθμό από προβλήματα ασφαλείας. Έτσι, αν κάποιος μη εξουσιοδοτημένος DHCP εξυπηρετητής (γνωστός ως “rogue DHCP”) εισέλθει στο δίκτυο, τότε μπορεί να προσφέρει IP διευθύνσεις στους χρήστες. Ο χρήστης που θα συνδεθεί με έναν rogue DHCP, κινδυνεύει οι πληροφορίες που στέλνονται μέσω της σύνδεσης να υποκλαπούν (man-in-the-middle attack) [11]. Ο επιτιθέμενος μπορεί ακόμα να ανακατευθύνει την κίνηση του χρήστη μέσω του ιδίου, κάτι που μπορεί να έχει σοβαρές συνέπειες.

Ένα ακόμα πρόβλημα είναι ότι αν υπάρχει μόνο ένας διαθέσιμος DHCP εξυπηρετητής και σταματήσει να λειτουργεί, όσοι host δεν έχουν ήδη IP διεύθυνση θα προσπαθήσουν και θα αποτύχουν να αποκτήσουν μία. Αυτοί που έχουν όταν θα προσπαθήσουν να την ανανεώσουν, θα αναγκαστούν να τη χάσουν. Μέχρι να αποκατασταθεί η βλάβη και ο εξυπηρετητής να επανέλθει, οποιαδήποτε δικτυακή πρόσβαση θα είναι αδύνατη, με πιθανές επιπλοκές σε όσους χρειάζονται επικοινωνία με το δίκτυο [11].

3.4 Συμπέρασμα

Φτάνοντας λοιπόν προς το τέλος, είναι απαραίτητο να αναγνωρίσουμε πόσο πολύ έχει βοηθήσει τόσο το DHCP όσο και το NAT στην καθημερινή επαφή των χρηστών με τους ηλεκτρονικούς υπολογιστές και το διαδίκτυο. Από την αρχή της δημιουργίας των ηλεκτρονικών υπολογιστών έως την δημιουργία του διαδικτύου, και από την περιορισμένη χρήση τους έως την ευρέως διαδεδομένη και πλέον απαραίτητη χρήση τους από τον μέσο άνθρωπο, κάθε ανακάλυψη, κάθε νέο πρωτόκολλο, κάθε προσπάθεια για πρόοδο της τεχνολογίας γίνεται δίχως άλλο με σκοπό την διευκόλυνση του μέσου αλλά και του ειδικευμένου χρήστη. Ζούμε σε έναν κόσμο που η τεχνολογία έχει πρωταρχικό ρόλο, γι' αυτό και είναι εύλογο να αναμένουμε τόσο την ανάπτυξη των ήδη εφαρμόσιμων διαδικασιών όσο και την ανακάλυψη νέων και εξίσου βοηθητικών και πρωτοποριακών, που θα συνεχίσουν να μετατρέπουν το διαδίκτυο σε χώρο προσβάσιμο και εύχρηστο για τον καθένα.

Β Ι Β Λ Ι Ο Γ Ρ Α Φ Ι Α

Βιβλία:

[1] Computer Networking, James F.Kurose - Keith W.Ross, Pearson, SIXTH EDITION

URLs:

[2] http://www.cisco.com/networkers/nw00/pres/2211.pdf

[3] https://curve.carleton.ca/system/files/frp/27418.pdf

[4] http://think-like-a-computer.com/2011/09/16/types-of-nat/

[5] http://www.pjsip.org/pjnath/docs/html/group__nat__intro.htm

[6] Wikipedia *Network Address Translation*
http://en.wikipedia.org/wiki/Network_address_translation

[11] http://www.ehow.com/info_8760244_disadvantages-dhcp.html

Εικόνες:

- Εικόνα 1: http://en.wikibooks.org/wiki/Communication_Networks/NAT_and_PAT_Protocols
- Εικόνα 2, Εικόνα 3: http://www.slideshare.net/dadaista/nat-traversal
- Εικόνα 4: http://www.networkinginfoblog.com/post/130/obtaining-a-block-of-addresses/
- Εικόνα 5: http://techmightsolutions.blogspot.gr/2012/06/dynamic-host-configuration-protocol.html

Αναφορές:

[7] RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations
https://tools.ietf.org/html/rfc2663

[8] RFC 3022 - Traditional IP Network Address Translator (Traditional NAT)
https://tools.ietf.org/html/rfc3022

[9] RFC 3489 - STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
https://www.ietf.org/rfc/rfc3489.txt

[10] RFC 2131 - Dynamic Host Configuration Protocol
https://www.ietf.org/rfc/rfc2131.txt