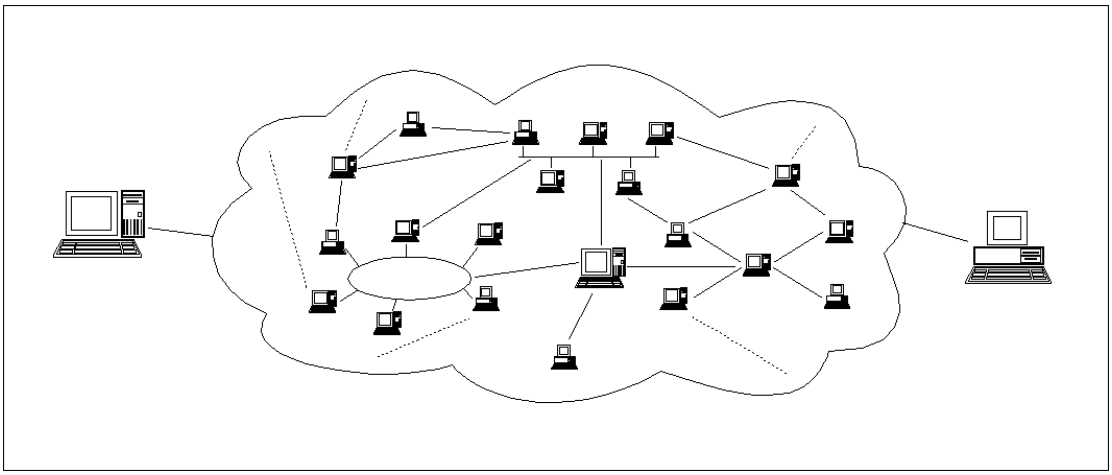
Πρωτόκολλα Επικοινωνίας

Στην καθημερινή μας ζωή, πρωτόκολλο είναι ένα σύνολο από συμβάσεις που καθορίζουν το πώς πρέπει να πραγματοποιηθεί κάποια διαδικασία. Στον κόσμο των δικτύων, **πρωτόκολλο** είναι ένα σύνολο από συμβάσεις που καθορίζουν το πώς ανταλλάσσουν μεταξύ τους δεδομένα οι υπολογιστές του δικτύου. Το πρωτόκολλο είναι αυτό που καθορίζει το πώς διακινούνται τα δεδομένα, το πώς γίνεται ο έλεγχος και ο χειρισμός των λαθών, κλπ. Το Internet δεν είναι ένα απλό δίκτυο, αλλά ένα διαδίκτυο. 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 Internet τρέχουν το πρωτόκολλο TCP/IP κι έτσι **μιλούν μια κοινή γλώσσα** που τους επιτρέπει να συνεννοούνται παρά τις διαφορές τους.

Τι κάνει το TCP / IP :

Ας υποθέσουμε ότι θέλουμε να μεταφέρουμε δεδομένα από έναν υπολογιστή που είναι συνδεδεμένος στο Internet και βρίσκεται π.χ. στην Αμερική, στο MIT, σε έναν άλλον που είναι επίσης συνδεδεμένος στο Internet και βρίσκεται π.χ. στην Ελλάδα, στο Πανεπιστήμιο Θεσσαλίας. Μεταξύ των δύο υπολογιστών παρεμβάλλεται το "σύννεφο" του Internet, δηλ. ένα πλέγμα από συνδέσεις και ενδιάμεσους υπολογιστές.



Το Internet 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 Internet αντιστοιχίζεται μία διεύθυνση που ονομάζεται διεύθυνση IP (περισσότερα γι αυτές τις διευθύνσεις στην επόμενη παράγραφο).

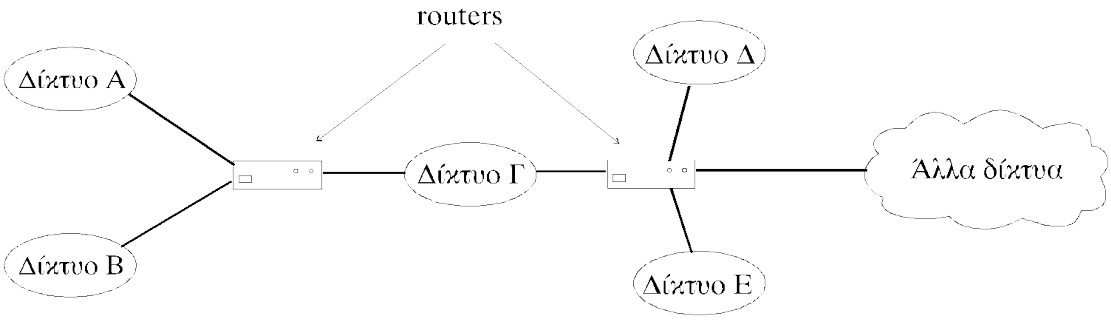
Το πρωτόκολλο IP είναι υπεύθυνο για το πέρασμα του πακέτου από υπολογιστή σε υπολογιστή μέσα από το "σύννεφο" των συνδέσεων. Καθώς το IP δρομολογεί το κάθε πακέτο μέσα στο δίκτυο, προσπαθεί να το παραδώσει, αλλά δεν μπορεί να εγγυηθεί ούτε ότι το πακέτο θα φτάσει στον προορισμό του ούτε ότι τα διάφορα πακέτα που αποτελούν τα αρχικά δεδομένα θα φτάσουν με τη σειρά με την οποία στάλθηκαν ούτε 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, αλλά όχι οι ενδιάμεσοι υπολογιστές, 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 αναμετάδοση 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.

Τώρα λοιπόν που γνωρίσαμε το TCP/IP μπορούμε να δώσουμε έναν πιο "επίσημο" ορισμό του Internet: ένα δίκτυο αποτελούμενο από δίκτυα υπολογιστών που επικοινωνούν χρησιμοποιώντας το πρωτόκολλο TCP/IP. Όπως θα δούμε παρακάτω, η διαδρομή που ακολουθεί ένα πακέτο μέσα από το "σύννεφο" των συνδέσεων δεν είναι προκαθορισμένη.

Η δρομολόγηση των πακέτων

Το πρωτόκολλο IP είναι υπεύθυνο για το πέρασμα ενός πακέτου δεδομένων από υπολογιστή σε υπολογιστή. Όλα τα δίκτυα που συνδέονται στο Internet "καταλαβαίνουν" τη γλώσσα IP κι έτσι μπορούν να συνεννοούνται και να ανταλλάσσουν δεδομένα με ομοιόμορφο τρόπο.
Τα δίκτυα του Internet συνδέονται μεταξύ τους με ειδικούς υπολογιστές που ονομάζονται δρομολογητές (routers) ή πύλες (gateways). Ένας router είναι λοιπόν ένας υπολογιστής που συνδέει δύο ή περισσότερα δίκτυα (που μπορεί να είναι διαφορετικού τύπου) και έτσι ανήκει σε δύο ή περισσότερα δίκτυα ταυτόχρονα .



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

Ας θεωρήσουμε πάλι ότι ένας υπολογιστής που βρίσκεται κάπου στο Internet 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 στον router που είναι συνδεμένος με το δίκτυο. Ο router 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 router, κ.ο.κ. μέχρις ότου το πακέτο προωθηθεί τελικά στον router που είναι συνδεδεμένος στο ίδιο δίκτυο με τον παραλήπτη. Το πακέτο μπορεί έτσι να περάσει από πολλούς routers μέχρις ότου φτάσει στον προορισμό του.

Οι routers 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 router στον οποίο θα πρέπει να προωθήσουν το πακέτο. Κάθε φορά, 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 routers μπορούν να επιλέγουν εναλλακτικούς δρόμους για ένα πακέτο σε περίπτωση που μια συγκεκριμένη σύνδεση του δικτύου παρουσιάζει πρόβλημα και βρίσκεται προσωρινά σε αχρηστία.

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 (initialisation) 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 ενημερωμένες 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.

Αντιστοίχηση IP διευθύνσεων

Το DCHP υποστηρίζει 3 μηχανισμούς για να αντιστοιχίζει διευθύνσεις. Αυτοί είναι:

- ✓ Αυτόματη αντιστοίχηση (με αντιστοίχηση μόνιμης διεύθυνσης)
- ✓ Δυναμική αντιστοίχηση (με διεύθυνση με ημερομηνία λήξης)
- ✓ Χειροκίνητη αντιστοίχηση (ο διαχειριστής κανονίζει ότι θεωρεί καλύτερο)

Η εφαρμογή του πρωτοκόλλου

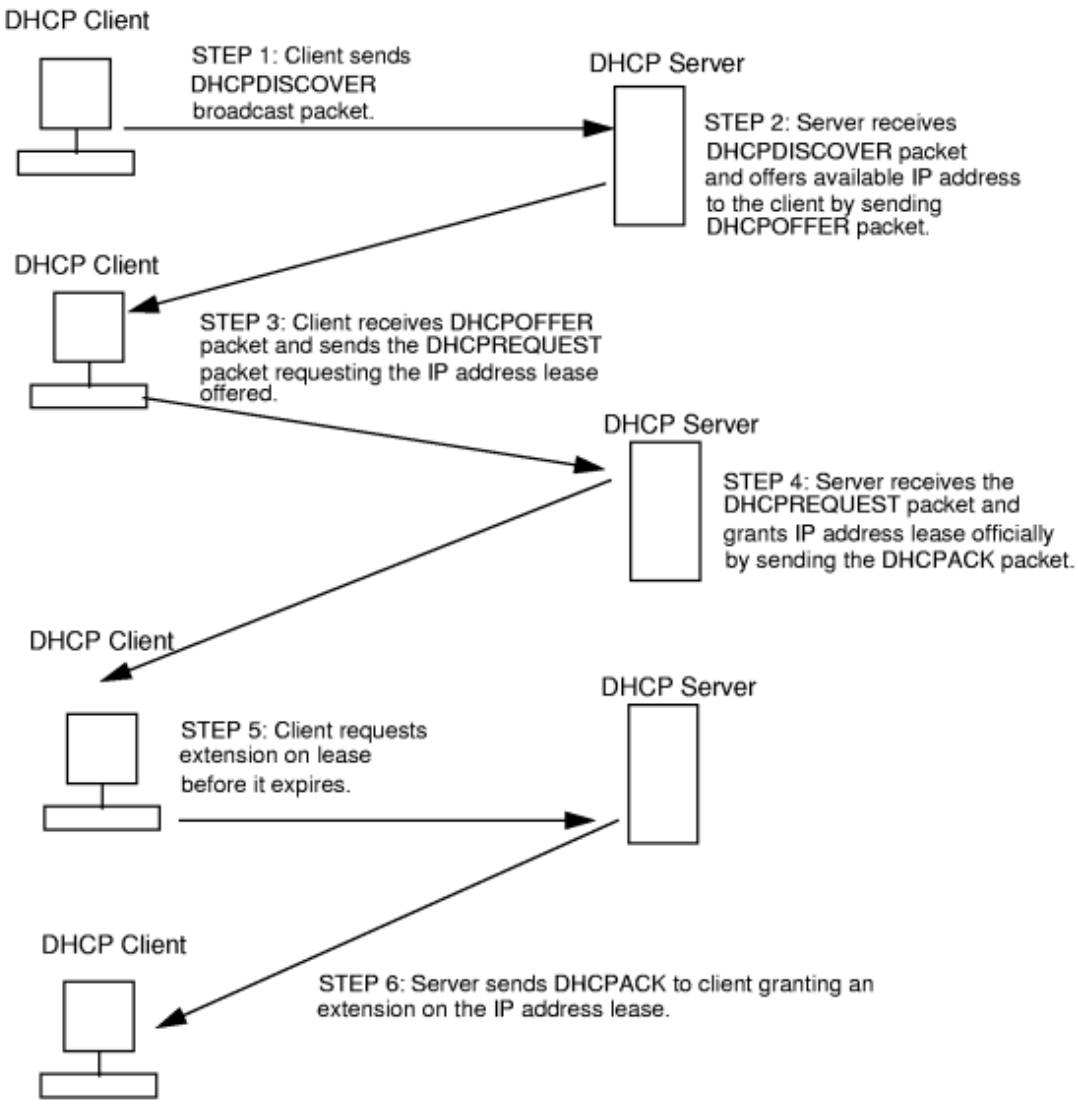
Σε ορισμένες περιπτώσεις και όταν αυτό είναι αναγκαίο μπορούμε να αποδώσουμε στους υπολογιστές του δικτύου διευθύνσεις IP οι οποίες δεν είναι στατικές αλλά δυναμικές . Αυτό σημαίνει πώς ο κάθε υπολογιστής δε θα έχει τη δική του σταθερή διεύθυνση αλλά κάθε φορά που θα συνδέεται στο δίκτυο θα ζητά να του 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 , λαμβάνει χώρα ως μια αρχιτεκτονική πελάτη διακομιστή (client server) στην οποία ο υπολογιστής που 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 BOOTR . Ένα σημαντικό πλεονέκτημα του πρωτοκόλλου DHCP έναντι του πρωτοκόλλου BOOTR 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 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 BOOTR , 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 BOOTR το οποίο χρησιμοποιεί μόνο δύο τέτοια μηνύματα (request & reply) .

Η λειτουργία του πρωτοκόλλου

Όταν ένας υπολογιστής συνδέεται στο δίκτυο , εκπέμπει (broadcast) ένα ειδικό πλαίσιο ελέγχου (control frame) ου 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 άλλο υπολογιστή . Αυτός ο έλεγχος γίνεται με τη βοήθεια ειδικών πρωτοκόλλων όπως είναι το **ARP** (address resolution protocol) και το **ICMP** (interface control message 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 .

Address Resolution Protocol

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 χώρα εκπομπή σε 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 . Η εντολή arp καλείται στις πιο συνηθισμένες περιπτώσεις με την παράμετρο –a η οποία εμφανίζει τα περιεχόμενα του πίνακα arp (arp table) ο οποίος περιέχει την παραπάνω αντιστοιχία διευθύνσεων .

Network Address Translation - Εισαγωγή

Είναι γνωστό ότι όταν κάποιος υπολογιστής είναι συνδεδεμένος στο Internet (ή σε οποιοδήποτε IP δίκτυο), 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 – 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:

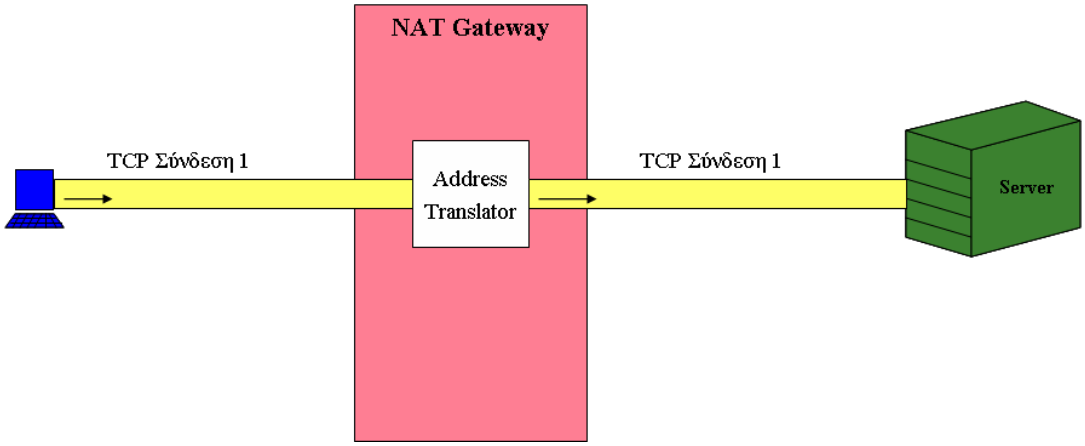
- 10.0.0.0 - 10.255.255.255 (Class A)
- 172.16.0.0 - 172.31.255.255 (Class B)
- 192.168.0.0 - 192.168.255.255 (Class C)

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 – θα 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 – στο 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).

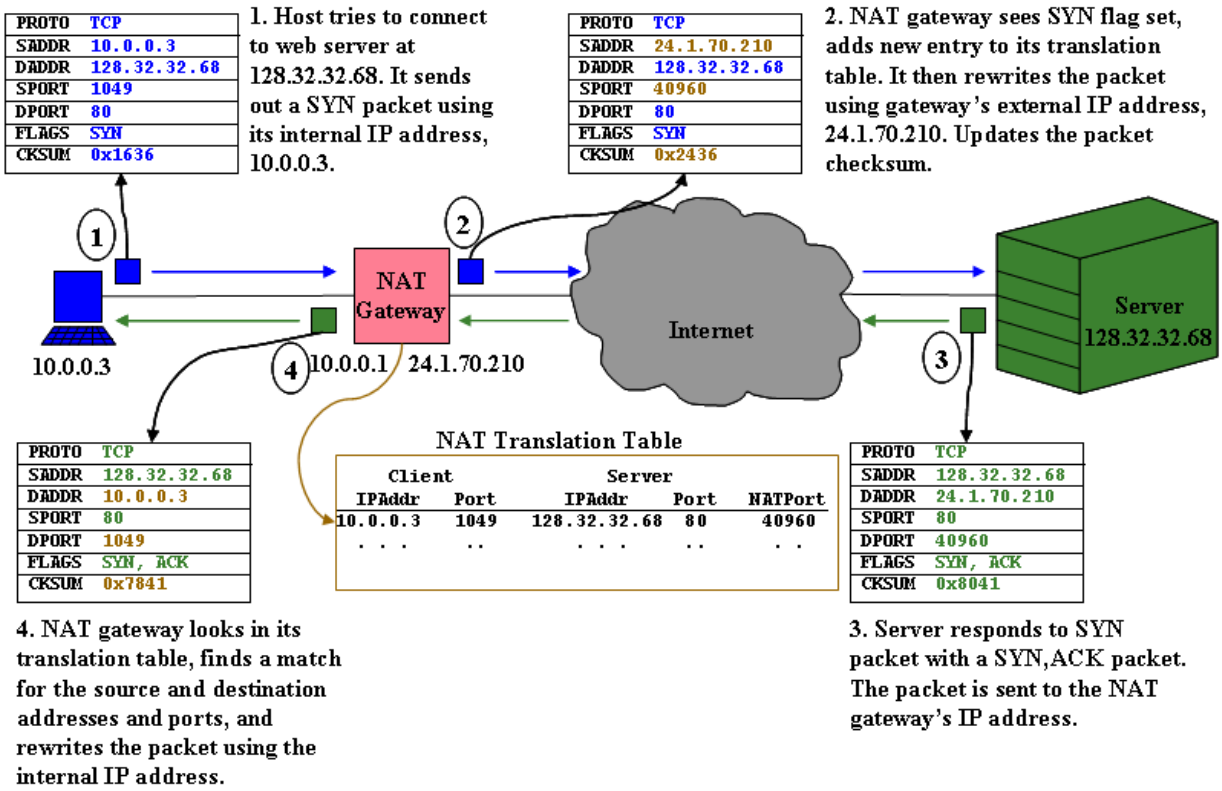
Το πρωτόκολλο Network Address Translation

Το NAT (Network Address Translation) είναι ειδικό πρωτόκολλο που εκτελούν οι πύλες (gateways) 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 (gateway ή firewall)) για να πάρει μία νέα διεύθυνση. Ο NAT διαθέτει ένα σύνολο διαθέσιμων IP διευθύνσεων («address pool») και μία από αυτές τις αναθέτει στον υπολογιστή. Ταυτόχρονα, κρατάει μία βάση δεδομένων στην οποία καταγράφει τη διεύθυνση που απέδωσε σε κάθε υπολογιστή (διαδικασία MAP). Έτσι, κάθε πακέτο που φεύγει από τον υπολογιστή του ιδιωτικού δικτύου και «ταξιδεύει» στο Internet 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. Τα παραπάνω απεικονίζονται στο σχήμα – όπου η διαδικασία Exlude υποδηλώνει το γεγονός ότι κάποιες διευθύνσεις κάποιες φορές δεν χρειάζεται να αλλάξουν (να «μεταγλωτιστούν») σε κάποια άλλη (π.χ. αν αντιστοιχούν σε κάποιον mail server).



Για να γίνει ακόμα πιο σαφής η διαδικασία του NAT, ας δούμε αναλυτικά το ακόλουθο παράδειγμα

Στάδιο 1. Ένας υπολογιστής εντός ιδιωτικού δικτύου με διεύθυνση 10.0.0.3 θέλει να συνδεθεί με ένα απομακρυσμένο υπολογιστή (server – π.χ ένας ftp server) που έχει διεύθυνση 128.32.32.68. Παρακολουθούμε τα πεδία από το TCP/IP πλαίσιο που μας ενδιαφέρουν: τα SADDR, DADDR είναι οι διευθύνσεις αποστολέα και προορισμού αντίστοιχα. Τα SPORT, DPORT είναι οι TCP θύρες αποστολέα και προορισμού αντίστοιχα και σχετίζονται κυρίως με την εφαρμογή που αιτείται ο χρήστης (τα νούμερα στο σχήμα είναι τυχαία). Το CKSUM είναι το πεδίο εκείνο του TPC/IP πλαίσιου που υπολογίζεται με σκοπό την ανίχνευση σφάλματος – δηλαδή εκτελεί μια συνάρτηση κατακεματισμού πάνω σε όλο το υπόλοιπο πακέτο και η τιμή που υπολογίζεται είναι αυτή που μπαίνει στο CKSUM (επίσης τυχαία η τιμή που αναγράφεται στο σχήμα).

Στάδιο 2. Ο NAT μεταβάλλει τη διεύθυνση του υπολογιστή. Στο συγκεκριμένο παράδειγμα την κάνει 24.1.70.210 (οπότε και αλλάζει η τιμή του πεδίου SADDR στο TCP/IP πακέτο). Αντίστοιχα αλλάζει και η τιμή του SPORT (επίσης τυχαία η τιμή του σχήματος), ενώ προφανώς, αφού 2 πεδία του πακέτου έχουν μεταβληθεί, αναγκαστικά θα αλλάξει και η τιμή του CKSUM. Ταυτόχρονα, ο NAT ενημερώνει τον πίνακά του σχετικά με την αλλαγή στη IP διεύθυνση που πραγματοποίησε (διαδικασία MAP, όπως αναφέρθηκε νωρίτερα). Η νέα καταχώρηση που τοποθετείται στον πίνακα περιέχει την αρχική IP διεύθυνση και TCP θύρα του υπολογιστή, την IP διεύθυνση και TCP θύρα του υπολογιστή-προορισμού, καθώς και την TPC θύρα του NAT.

Στάδιο 3. Παρατηρούμε τώρα το TCP/IP πακέτο-απάντηση που στέλνει ο απομακρυσμένος υπολογιστής. Προφανώς, η τιμή του SADDR είναι η διεύθυνση του υπολογιστή αυτού – δηλαδή 128.32.32.68. Η τιμή του DADDR είναι η διεύθυνση του αρχικού υπολογιστή που «βλέπει» ο 128.32.32.68 – δηλαδή, η νέα διεύθυνση 24.1.70.210. Οι τιμές του SPORT και DPORT είναι προφανώς 80 και 40960 – δηλαδή, εναλλάσονται οι αντίστοιχες τιμές του πακέτου που είχαμε στο στάδιο 2. Και, τέλος, επισημαίνεται ότι φυσικά η τιμή του CKSUM είναι διαφορετική από όλες τις προηγούμενες (αφού το εν λόγω IP πακέτο δεν είναι ίδιο με κανένα από τα προηγούμενα).

Στάδιο 4. Ο NAT κοιτάει το πακέτο που λαμβάνει (αυτό του σταδίου 3) και ψάχνει τον πίνακά του να βρει καταχώρηση που να έχει ως NAT θύρα τη 40960 (δηλαδή το DPORT του πακέτου που έλαβε), ως διεύθυνση προορισμού την 128.32.32.68 (που είναι η SADDR του πακέτου που έλαβε) και ως θύρα προορισμού την 80. Στο συγκεκριμένο παράδειγμα βρίσκει την καταχώρηση, η οποία σαν διεύθυνση και TCP θύρα αποστολέα έχει τις 10.0.0.3 και 1049 αντίστοιχα. Άρα, ξέρει σε ποιον υπολογιστή εντός του ιδιωτικού δικτύου να προωθήσει το πακέτο. Προσέξτε τα πεδία του προωθημένου αυτού πακέτου: πρέπει ο ο υπολογιστής 10.0.0.3 να μην αντιλαμβάνεται τον NAT, συνεπώς δεν φαίνεται πουθενά ούτε η διεύθυνση που απέδωσε ο NAT ούτε η θύρα του. Με άλλο λόγια, οι τιμές των πεδίων του πακέτου 4 είναι οι αντίστροφες αυτών του σταδίου 1 (δηλαδή η DADDR του σταδίου 1 γίνεται SADDR του σταδίου 4 κ.ο.κ). Και, βέβαια, πάλι έχουμε μια διαφορετική τιμή του CKSUM, σε σχέση με όλες τις προηγούμενες.

Όταν σε έναν υπολογιστή ανατίθεται πάντα μία νέα συγκεκριμένη IP διεύθυνση, μιλάμε για στατική μεταγλώττιση διεύθυνσης – διαφορετικά, αν κάθε φορά του αποδίδεται διαφορετική διεύθυνση, τότε αναφερόμαστε σε δυναμική μεταγλώττιση (που είναι και η συνηθέστερη περίπτωση). Πρέπει να σημειωθεί ότι το NAT, όπως περιγράφηκε παραπάνω, έχει τον ίδιο περιορισμό με τον Proxy server ως προς το ότι λειτουργεί μόνο πάνω σε TCP.

N.A.T. & PORT FORWARDING

Ένα πρότυπο που βρίσκει εφαρμογή σε τοπικά δίκτυα των οποίων οι υπολογιστές μοιράζονται μια κοινή σύνδεση Internet. Το NAT, ορίζει σε κάθε ηλεκτρονικό υπολογιστή του τοπικού δικτύου μια διαφορετική εσωτερική διεύθυνση IP, της μορφής 192.168.x.x ή 10.1.x.x και μια κοινή εξωτερική IP με την οποία αναγνωρίζονται από άλλα συστήματα συνδεμένα στο Internet. Το NAT βρίσκει εφαρμογή σε ιδιωτικά και εταιρικά δίκτυα που συνδέονται στο Internet μέσω routers και συνδέσεων ADSL ή μισθωμένων γραμμών. Πολλές φορές ο διαχειριστής των δικτύων αυτών θα πρέπει να ρυθμίσει κατάλληλα τους κανόνες NAT, ώστε να είναι εφικτή η πρόσβαση από το Internet σε υπηρεσίες και εφαρμογές που εκτελούνται σε συγκεκριμένο υπολογιστή του εσωτερικού δικτύου. Η ρύθμιση αυτή ονομάζεται και port forwarding. Επειδή όλοι οι ηλεκτρονικοί υπολογιστές εμφανίζονται στο διαδίκτυο με την ίδια διεύθυνση IP, ένας κανόνας NAT ή port forwarding καθορίζει σε ποιον από όλους θα πρέπει να αναζητηθεί μια συγκεκριμένη υπηρεσία. Αυτό γίνεται με την αντιστοίχηση του port της εν λόγω υπηρεσίας (π.χ. port 80 για HTTP server) στην εσωτερική διεύθυνση του υπολογιστή του τοπικού δικτύου όπου αυτή εκτελείται.

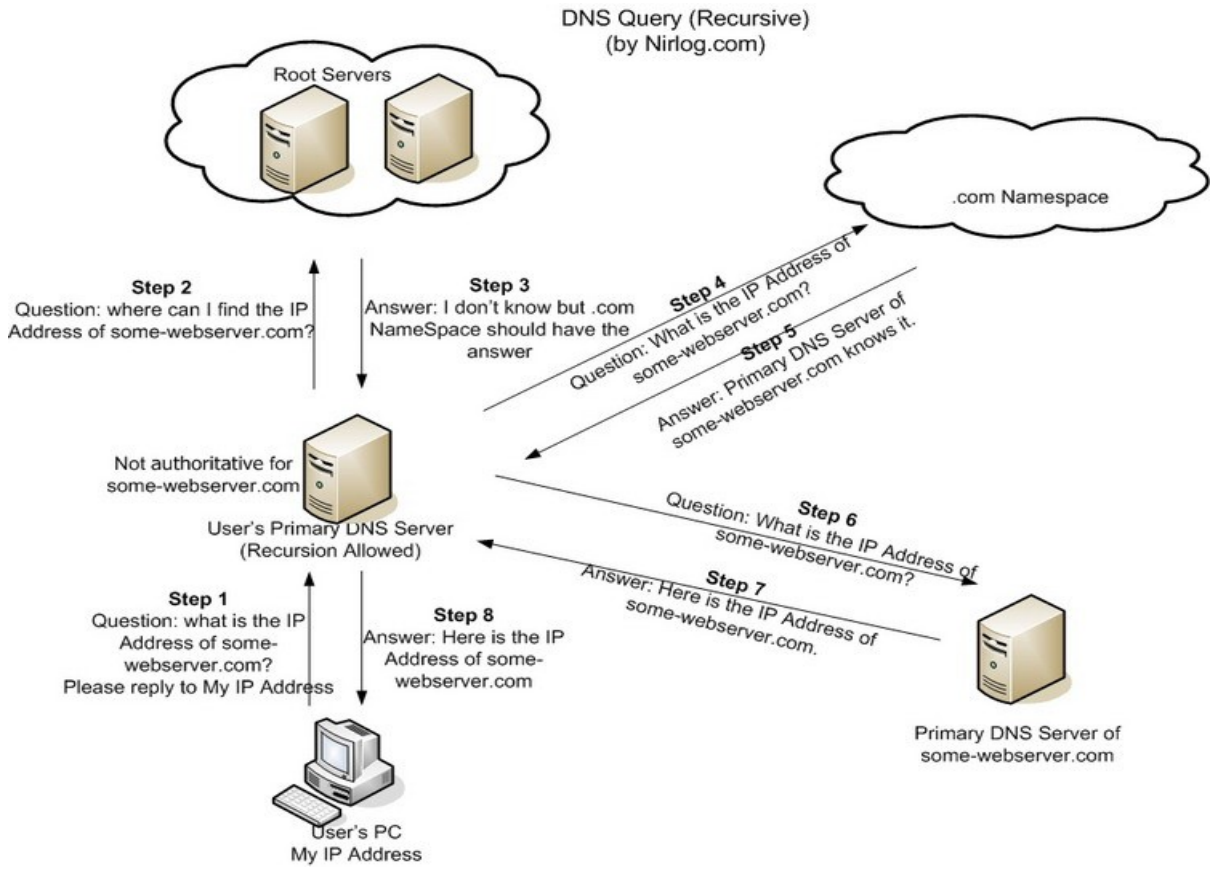
Η υπηρεσία UPnP (Universal Plug and Play) που υποστηρίζεται σήμερα από πολλές εφαρμογές, λειτουργικά συστήματα και routers έχει περιορίσει σημαντικά την ανάγκη καθορισμού κανόνων NAT, χωρίς όμως να την έχει εξαλείψει πλήρως.

Domain Name Service

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.teiath.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 .

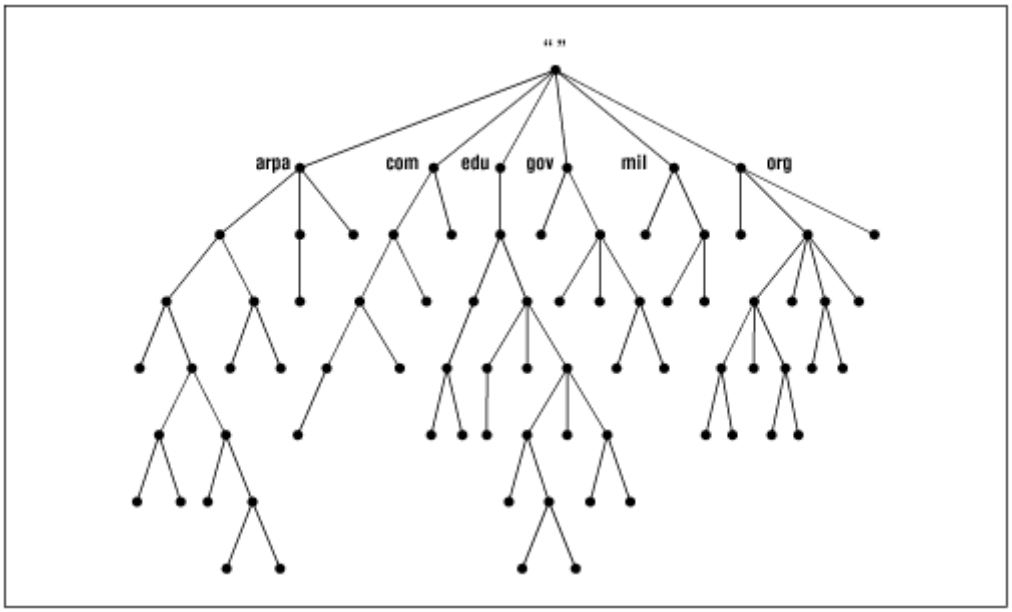
Πως είναι δυνατόν ο μηχανισμός DNS γνωρίζει ποια είναι η συμβολική διεύθυνση που αντιστοιχεί σε κάποια διεύθυνση IP . Η απάντηση είναι ότι υπάρχουν διασκορπισμένες σε όλο τον κόσμο τεράστιες βάσεις δεδομένων , οι οποίες περιέχουν ζεύγη της μορφής (συμβολική διεύθυνση – πραγματική διεύθυνση) . Όταν λοιπόν ο μηχανισμός DNS δέχεται ως είσοδο κάποια διεύθυνση IP , συνδέεται σε κάποια από αυτές τις βάσεις , 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 Internet. Κάθε δρομολογητής και κάθε υπολογιστής στο Internet 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)



Σε ένα δίκτυο που εξυπηρετεί αρκετούς υπολογιστές κάτω από το ίδιο όνομα δικτύου πρέπει να λειτουργεί ένας DNS server που θα δίνει τη διεύθυνση του προς τον DNS server του αμέσως ανώτερου επιπέδου . Αυτό επαναλαμβάνεται έως ότου καλυφθεί ολόκληρη η ιεραρχία ονομάτων. Οι διάφορες εφαρμογές στο διαδίκτυο όπως FTP , SMTP ,Telnet ή www για να εντοπίσουν μια διεύθυνση απευθύνουν ένα ερώτημα προς τον DNS server ο οποίος είτε δίνει την απάντηση από τους πίνακες καταχωρήσεων που διαθέτει είτε παραπέμπει προς τη διεύθυνση του DNS server που έχει την απάντηση . Εάν ο ίδιος ο DNS server δώσει την απάντηση , αυτή μπορεί να προέρχεται είτε από τους δικούς του πίνακες καταχωρήσεων είτε από άλλους DNS servers που ψάχνει για λογαριασμό της εφαρμογής .