Η στοίβα πρωτοκόλλων TCP/IP

Στρώμα	**Περιγραφή**	**Κάποια πρωτόκολλα που υλοποιούνται**
Εφαρμογής	Παρέχει το σημείο προσαρμογής για την αλληλεπίδραση του χρήστη με το δίκτυο.	**HTTP**: για τις ιστοσελίδες **SMTP, IMAP, POP3**: για τα e-mails **FTP**: για αποθήκευση αρχείων σε απομακρυσμένο φάκελο
Μεταφοράς	Επεξεργάζεται τη ροή δεδομένων που λαμβάνει από το στρώμα δικτύου, ώστε να τη φέρει σε κατάλληλη μορφή για χρήση από το στρώμα εφαρμογής.	**TCP**: Αξιόπιστη αλλά αργή μετάδοση: **UDP**: Αναξιόπιστη αλλά γρήγορη μετάδοση δεδομένων
Δικτύου	Χειρίζεται την κίνηση των πακέτων στο δίκτυο. Δεν ασχολείται με την αξιοπιστία της μετάδοσης δεδομένων.	**IP**: Πρωτόκολλο δρομολόγησης **ICMP**: Πρωτόκολλο για τον έλεγχο της μεταφοράς των πακέτων
Ζεύξης και ελέγχου πρόσβασης στο μέσο	Είναι το χαμηλότερο της στοίβας και είναι υπεύθυνο για την επικοινωνία με το πραγματικό μηχανικό μέρος του υπολογιστικού συστήματος. Στην ουσία, είναι το στρώμα στο οποίο βρίσκονται οι drivers του υπολογιστή.	**Ethernet, FDDI**

Σχόλια: Στα τερματικά υλοποιούνται και τα τέσσερα στρώματα, ενώ στους δρομολογητές μόνο τα δύο κατώτερα.

Στρώμα ζεύξης

Η ροή δεδομένων χωρίζεται σε πλαίσια.

- IEEE 802.3 (CSMA/CD)
  Ο τρόπος προσπέλασης του μέσου CSMA/CD χρησιμοποιείται κυρίως σε **δίκτυα τοπολογίας αρτηρίας**, όπου δηλαδή όλοι οι τερματικοί σταθμοί είναι συνδεδεμένοι στο ίδιο καλώδιο. Με αυτόν τον τρόπο διευθέτησης του μέσου είναι δυνατόν δύο σταθμοί να μεταδώσουν την ίδια στιγμή στο δίκτυο. Σ' αυτήν την περίπτωση, η πληροφορία και των δύο θα καταστραφεί. Γι' αυτό, ο τρόπος προσπέλασης του μέσου CSMA/CD καθορίζει ότι πριν τη μετάδοση πρέπει ο σταθμός να ελέγχει αν κάποιος άλλος σταθμός μεταδίδει. Αυτό το κάνει συγκρίνοντας το σήμα στο καλώδιο-αρτηρία με το σήμα που μεταδίδει.
- IEEE 802.4 (token)
  Στο πρότυπο αυτό γίνεται χρήση **τοπολογίας αρτηρίας και ελέγχου πρόσβασης στο μέσο με σκυτάλη**. Χρησιμοποιείται, δηλαδή, μια σκυτάλη ελέγχου άδειας που περνά από σταθμό σε σταθμό σύμφωνα με ένα σύνολο κανόνων που αποδέχονται όλοι οι σταθμοί. Ένας σταθμός μπορεί να μεταδώσει μόνο αν έχει τη σκυτάλη. Μόλις ολοκληρώσει τη μετάδοση του πλαισίου, παραδίδει τη σκυτάλη στον επόμενο σταθμό. Υπάρχει ένα μέγιστο χρονικό διάστημα για το οποίο μπορεί να κρατά τη σκυτάλη ο σταθμός. Αν μια μετάδοση διακοπεί υποχρεωτικά, λόγω του διαστήματος αυτού, προφανώς θα συνεχιστεί όταν ο σταθμός ξαναπάρει τη σκυτάλη.
- IEEE 802.5

Πρόκειται για συνδυασμό του πρότυπου IEEE 802.4 με **τοπολογία δακτυλίου**. Οι σταθμοί είναι σειριακά συνδεδεμένοι με το μέσο μεταφοράς (καλώδιο) και η σκυτάλη πάει κυκλικά από τον ένα σταθμό στον επόμενο. Το πρότυπο αυτό διαφέρει από τα προηγούμενα δύο στο ότι, τα bits σε κάθε πλαίσιο μεταδίδονται στο μέσο ξεκινώντας από το πιο σημαντικό ψηφίο.

- FDDI
  Είναι μια σειρά πρωτοκόλλων για τη μετάδοση ψηφιακών δεδομένων πάνω από **οπτική ίνα**. Τα δίκτυα FDDI είναι **δίκτυα με διπλό δακτύλιο** και γίνεται **έλεγχος πρόσβασης στο μέσο με σκυτάλη**. Το FDDI επιτρέπει παραπάνω από ένα πλαίσια να βρίσκονται ταυτόχρονα σε μετάδοση. Λόγω της τεράστιας ταχύτητας που προσφέρουν τα δίκτυα FDDI, μπορούν να χρησιμοποιηθούν ως **δίκτυα κορμού** για τη διασύνδεση άλλων τοπικών δικτύων.
- DSL (Digital Subscriber Line)
  Τα διάφορα είδη ψηφιακής συνδρομητικής τεχνολογίας χρησιμοποιούν ως μέσο τις **κοινές τηλεφωνικές γραμμές** και παρέχουν πρόσβαση υψηλής ταχύτητας στο διαδίκτυο. Εκμεταλλεύονται τις αχρησιμοποίητες υψηλότερες συχνότητες στα χάλκινα δισύρματα καλώδια του τηλεφωνικού δικτύου, για να παρέχουν ευρυζωνική πρόσβαση στους τελικούς χρήστες. Έχουν αναπτυχθεί διάφορες παραλλαγές της τεχνολογίας DSL και η βασικής τους διαφορά συνίσταται στη μέγιστη ταχύτητα μεταφοράς δεδομένων πάνω από δισύρματη γραμμή. Η τεχνολογία xDSL χωρίζεται σε δύο βασικές κατηγορίες: Στη μία απαιτείται η χρήση **διαχωριστή σήματος** (splitter) είτε εσωτερικά είτε εξωτερικά στο χώρο του συνδρομητή. Στη δεύτερη κατηγορία δεν πραγματοποιείται διαχωρισμός των δύο σημάτων, αλλά τοποθετείται κατάλληλο βαθυπερατό φίλτρο στην τηλεφωνική συσκευή. Τον διαχωρισμό του σήματος αναλαμβάνει, σ' αυτή τη περίπτωση, ο router (διαποδιαμορφωτής... ζντόιόιόιόινγκ!). Επίσης, οι τεχνολογίες xDSL κατηγοριοποιούνται στις συμμετρικές και τις ασύμμετρες. Ως **συμμετρικές** ορίζονται οι τεχνολογίες που προσφέρουν ίσο ρυθμό λήψης και αποστολής δεδομένων. Ενώ **ασύμμετρες** είναι εκείνες στις οποίες η ταχύτητα με την οποία ο χρήστης λαμβάνει δεδομένα είναι μεγαλύτερη από αυτή με την οποία στέλνει.

Στρώμα Δικτύου

Στα δίκτυα TCP/IP όλη η πληροφορία μεταφέρεται από το πρωτόκολλο IP, το οποίο είναι ένα πρωτόκολλο στρώματος δικτύου και παρέχει μια **χωρίς σύνδεση** (connectionless) υπηρεσία μεταφοράς δεδομένων. Η υπηρεσία αυτή πολλές φορές αναφέρεται και ως *μη αξιόπιστη* εφόσον δεν εγγυάται τη σωστή παράδοση των δεδομένων. Το πρωτόκολλο IP ορίζει τη μορφή που πρέπει να πάρουν τα πακέτα προκειμένου να μεταδοθούν. Η τελική μορφή του πακέτου ονομάζεται **IP-datagram**. Κάθε IP-datagram μεταδίδεται ανεξάρτητα από τα υπόλοιπα (εφόσον το IP παρέχει μια υπηρεσία χωρίς σύνδεση), επομένως πρέπει το καθένα να περιέχει τις πληροφορίες που απαιτούνται για τη δρομολόγησή του (π.χ. η διεύθυνση IP της πηγής και του προορισμού).

Το πρωτόκολλο IP προσφέρει ένα σύνολο από βασικές λειτουργίες, οι οποίες είναι απαραίτητες για τη διασύνδεση δικτύων υπολογιστών, όπως:

- **Λειτουργίες κατάτμησης** των μηνυμάτων και επανένωσής τους προκειμένου αυτά να περάσουν από υποδίκτυα που υποστηρίζουν διαφορετικού μεγέθους πεδίο δεδομένων στο πλαίσιό τους.
- **Λειτουργίες δρομολόγησης** των IP-datagrams μέσω των κόμβων του δικτύου, προκειμένου να φτάσουν στον προορισμό τους.
- **Λειτουργίες αναφοράς σφαλμάτων** με σκοπό την ενημέρωση του κόμβου-πηγή για τη σχετική απώλεια, δεδομένου ότι είναι δυνατόν κάποια IP-datagrams να χαθούν.

Κλάσεις διευθύνσεων IP

Κάθε συσκευή που είναι συνδεδεμένη στο διαδίκτυο έχει τη δική της διεύθυνση IP. Για δική μας ευκολία, χωρίζουμε τον αριθμό σε τέσσερις οκτάδες (bytes) από bits, όπου κάθε μία αναπαριστά έναν δεκαδικό αριθμό από το 0 έως και το 255. Έτσι, οι IP διευθύνσεις μπορούν να γραφτούν ως τέσσερις τέτοιοι αριθμοί, χωρισμένοι από μία τελεία. Ο χωρισμός των διευθύνσεων σε οκτάδες χρησιμοποιείται για τη δημιουργία κλάσεων διευθύνσεων IP. Οι διευθύνσεις IP χωρίζονται σε δύο πεδία: το **αναγνωριστικό δικτύου (net_id)** [προσδιορίζει το δίκτυο στο οποίο είναι συνδεδεμένος ο χρήστης] και το **αναγνωριστικό κόμβου (host_id)** [προσδιορίζει τον συγκεκριμένο υπολογιστή μέσα σε ένα δίκτυο].

Οι κύριες κλάσεις διευθύνσεων είναι οι A, B και C, κάθε μία από τις οποίες χρησιμοποιείται σε δίκτυα διαφορετικού μεγέθους. Η κλάση στην οποία ανήκει κάθε δίκτυο μπορεί να αναγνωριστεί από τη θέση στην οποία βρίσκεται το πρώτο μηδενικό στα τέσσερα πρώτα bits της διεύθυνσης.

- Κλάση A: Το net_id καταλαμβάνει το πρώτο byte της διεύθυνσης IP και το host_id τα υπόλοιπα. Το πρώτο μηδενικό στα τέσσερα πρώτα bits της διεύθυνσης βρίσκεται στο πρώτο ψηφίο. Έτσι, σε δεκαδική γραφή, η πρώτη οκτάδα από bits έχει τιμή από το 0 έως και το 127. Όμως, οι διευθύνσεις δικτύων με πρώτη οκτάδα ίση με 0 ή 127 είναι κρατημένες, οπότε έχουμε μέχρι 126 σε πλήθος δίκτυα κλάσης A. Μπορούν στο εσωτερικό τους να έχουν μέχρι και 16 εκατομμύρια κόμβους το καθένα.
- Κλάση B: Το net_id καταλαμβάνει τα 2 πρώτα bytes της διεύθυνσης IP και το host_id τα υπόλοιπα. Το πρώτο μηδενικό στα τέσσερα πρώτα bits της διεύθυνσης βρίσκεται στο δεύτερο ψηφίο, δηλαδή οι διευθύνσεις IP αυτής της κλάσης ξεκινάνε πάντα με τον αριθμό 10. Έτσι, το εύρος του πρώτου δεκαδικού αριθμού είναι από 128 έως 191. Μπορούμε να έχουμε 16 χιλιάδες δίκτυα κλάσης B με 65 χιλιάδες κόμβους το καθένα στο εσωτερικό του. Πχ, το δίκτυο του ΕΜΠ είναι κλάσης B με net_id 147.102.
- Κλάση C: Το net_id καταλαμβάνει τα πρώτα 3 bytes της διεύθυνσης IP και το host_id το τέταρτο. Το πρώτο μηδενικό στα τέσσερα πρώτα bits της διεύθυνσης βρίσκεται στο τρίτο ψηφίο, δηλαδή οι διευθύνσεις IP αυτής της κλάσης ξεκινάνε πάντα με τον αριθμό 110. Το εύρος του πρώτου δεκαδικού αριθμού είναι από 192 έως 223. Έτσι, μπορούμε να έχουμε 2 εκατομμύρια δίκτυα κλάσης C με 256 κόμβους το καθένα.

Υποδίκτυα και μάσκες υποδικτύων

Αντί της ιεραρχίας δύο επιπέδων (net_id και host_id), με τις μάσκες υποδικτύων μπορούμε να έχουμε μια ιεράρχηση τριών επιπέδων. Η βασική ιδέα είναι ο διαχωρισμός του host_id σε δύο μέρη: το **αναγνωριστικό υποδικτύου (subnet_id)** και στον **αριθμό τερματικού σ' αυτό το υποδίκτυο (host_id)**. Οι μάσκες υποδικτύων γράφονται σε διάστικτη δεκαδική σημειογραφία (όπως οι διευθύνσεις IP) και αποτελούνται από 4 bytes. Δεν μπορούν να υπάρχουν ανεξάρτητα από τις διευθύνσεις IP. Αντιθέτως, συνοδεύουν μια διεύθυνση IP και οι δύο αριθμοί λειτουργούν μαζί.

Για να είναι μια μάσκα υποδικτύου έγκυρη θα πρέπει τα bits που προσδιορίζουν τα net_id και subnet_id να είναι όλα 1, ενώ τα bits που προσδιορίζουν το host_id να είναι όλα 0. Οι μάσκες υποδικτύων μπορούν να γραφτούν είτε σε δεκαδική μορφή είτε με έναν αριθμό ίσο με το πλήθος των άσσων. Για παράδειγμα,

- Οι διευθύνσεις 208.162.106.17 255.255.255.0 και 208.162.106.17/24 αναφέρονται και οι δύο σε διευθύνσεις κλάσης C με net_id 208.162.106.
- Τα πρώτα τέσσερα bits της διεύθυνσης 193.78.57.203 (1100) κατατάσσουν το δίκτυο στην κλάση C. Για τη δημιουργία υποδικτύων θα πρέπει παραπάνω από 24 bits να τεθούν στην τιμή 1. Έτσι, η μάσκα των 25 bits 255.255.255.128 (ή 192.78.57.203/25) χωρίζει το δίκτυο σε 4 υποδίκτυα. Το net_id είναι 192.78.57 και, ενώ χωρίς τη μάσκα υποδικτύου το host_id είναι 203 (σε δεκαδική μορφή 11001011), η μάσκα το χωρίζει σε net_id 1 και host_id 1001011 (σε δεκαδική μορφή, net_id 1 και host_id 75)

Δρομολόγηση IP

Η δρομολόγηση αναφέρεται στη μεταφορά ενός IP-datagram (πακέτο) από έναν κόμβο σε έναν άλλο του ίδιου ή άλλου δικτύου. Σε περίπτωση που ορίζεται **στατική δρομολόγηση** για κάποιο δίκτυο προορισμού, όλο το φορτίο με προορισμό το δίκτυο αυτό θα ακολουθήσει την ίδια διαδρομή ακόμα και αν υπάρχουν καλύτερες εναλλακτικές. Στη **δυναμική δρομολόγηση** τα μονοπάτια δρομολόγησης αλλάζουν συχνά καθώς αλλάζει το διαδικτυακό φορτίο ή η διαδικτυακή τοπολογία. Το πρωτόκολλο IP έχει σε κάθε δρομολογητή έναν **πίνακα δρομολόγησης**, στον οποίο ανατρέχει κάθε φορά που θέλει να στείλει ένα πακέτο. Η διαδικασία της δρομολόγησης γίνεται από δρομολογητή σε δρομολογητή. Ο κάθε δρομολογητής δεν γνωρίζει την πλήρη διαδρομή που ακολουθεί το πακέτο παρά μόνο τον επόμενο σταθμό του. Συνεπώς, η δρομολόγηση ουσιαστικά προμηθεύει το πακέτο κάθε δορά με τη διεύθυνση του επόμενο σταθμού του. Τα βήματα του δρομολογητή είναι τα εξής:

1. Αρχικά, ψάχνει στους πίνακες δρομολόγησης που έχει για να δει αν υπάρχει διεύθυνση προορισμού του πακέτου. Αν βρεθεί ολόκληρη η διεύθυνση, τότε στέλνει το πακέτο στον κατάλληλο επόμενο δρομολογητή ή στο υποδίκτυο, σύμφωνα με τον πίνακα δρομολόγησης.
2. Αν δεν βρεθεί, ψάχνει να βρει μόνο τη διεύθυνση του υποδικτύου. Αν τη βρει, προωθεί το πακέτο στον αντίστοιχο επόμενο δρομολογητή και αφήνει εκείνον να αποφασίσει για την τελική διεύθυνση.
3. Τέλος, αν δεν βρεθεί ούτε το υποδίκτυο, ψάχνει στον πίνακα να βρει αν υπάρχει κάποιος προεπιλεγμένος δρομολογητής και αν υπάρχει, το στέλνει εκεί. Αν όλα τα παραπάνω αποτύχουν, το πακέτο απορρίπτεται και επιστρέφεται κάποιο μήνυμα λάθους στην πηγή που έστειλε το πακέτο.

Πρωτόκολλο ARP

Η χρήση ενός δρομολογητή για τις περιπτώσεις επικοινωνίας δύο υπολογιστών που βρίσκονται στο ίδιο υποδίκτυο φορτώνει υπερβολικά το υποδίκτυο. Σε τέτοιες περιπτώσεις, αρκεί ο σταθμός -πηγή να γνωρίζει τη φυσική διεύθυνση του σταθμού-προορισμού, για να του προωθήσει το πακέτο IP. **Το πρωτόκολλο ARP διευκολύνει τη δρομολόγηση μέσα σε ένα υποδίκτυο αντιστοιχίζοντας τις διευθύνσεις IP σε αντίστοιχες φυσικές διευθύνσεις, διατηρώντας έναν πίνακα για την εκτέλεση της διαδικασίας αυτής**.

Πρωτόκολλο ICMP

Το πρωτόκολλο αυτό αποτελεί αναπόσταστο κομμάτι του IP και πρέπει να υλοποιείται από κάθε κόμβο. Χρησιμοποιείται για την αναφορά σφαλμάτων και όχι για να καταστήσει αξιόπιστο το πρωτόκολλο IP. Βασικές λειτουργίες είναι οι εξής:

- Αναφορά συμφόρησης στο δίκτυο (ο δρομολογητής αποθηκεύει πάρα πολλά πακέτα επειδή δεν προλαβαίνει να τα στείλει με τον ρυθμό που τα λαμβάνει)
- Αναφορά δικτυακών σφαλμάτων (μη προσβάσιμος τερματικός σταθμός)
- Αναφορά λήξης χρόνου (ο χρόνος ζωής ενός πακέτου τελειώνει, πριν αυτό φτάσει στον προορισμό του)
- Βοήθεια στην ανίχνευση προβλημάτων

Στρώμα μεταφοράς

Στο στρώμα μεταφοράς περιλαμβάνονται τα πρωτόκολλα **TCP**, το οποίο είναι μια *αξιόπιστη* υπηρεσία μεταφοράς *σε σύνδεση*, και **UDP**, που είναι *μη αξιόπιστη* και η μεταφορά γίνεται *χωρίς σύνδεση*. Θεωρούμε σαν τελικό προορισμό των δεδομένων σε κάθε μηχάνημα, όχι μια εφαρμογή, αλλά ένα σύνολο από νοητά σημεία προορισμού, που ονομάζουμε **θύρες** (ports) πρωτοκόλλου και καθένα από αυτά αναγνωρίζεται από ένα μοναδικό θετικό ακέραιο αριθμό.

TCP

Το TCP συμφέρει όταν δύο διαδικασίες ανταλλάσσουν μεγάλο όγκο δεδομένων. Το πρωτόκολλο αυτό περνά τα δεδομένα στον προορισμό με την ίδια σειρά που τα έστειλε η πηγή, εγκαθιστώντας πρώτα μια σύνδεση μεταξύ των δύο σταθμών εργασίας. Επειδή δύο σταθμοί εργασίας μπορεί να ανταλλάσσουν δεδομένα για διαφορετικές εφαρμογές, για κάθε εφαρμογή οι δύο σταθμοί λαμβάνουν τη θύρα στην οποία θα γίνεται η επικοινωνία. Η μεταφορά δεδομένων με TCP είναι **απολύτως αμφίδρομη**, δηλαδή μπορούμε να έχουμε ταυτόχρονη μεταφορά δεδομένων και προς τις δύο κατευθύνσεις. Το λογισμικό του TCP αποθηκεύει τα bytes που πρέπει να μεταφέρει, μέχρι να γεμίσει ένα IP-datagram.

Κάθε πακέτο TCP (μονάδα πληροφορίας αυτού του πρωτοκόλλου) έχει έναν μοναδικό αριθμό που το αναγνωρίζει σε σχέση με τα υπόλοιπα πακέτα. Με τον τρόπο αυτό, η διεργασία-προορισμός μόλις το λάβει στέλνει μια επιβεβαίωση στη διεργασία-πηγή, η οποία συνεχίζει την αποστολή πακέτων. Αν η πηγή δεν δεχτεί την επιβεβαίωση για κάποιο πακέτο εντός προκαθορισμένου χρονικού διαστήματος, τότε επαναμεταδίδει το μη επιβεβαιωμένο πακέτο. Αν ο προορισμός δεχτεί ένα πακέτο δεύτερη φορά, τότε το απορρίπτει. Έτσι, ξεπερνιούνται τα προβλήματα του μη αξιόπιστου πρωτοκόλλου IP.

Η αξιοπιστία εξασφαλίζεται χάρη στα παρακάτω χαρακτηριστικά:

- Τα δεδομένα προς μεταφορά αντιμετωπίζονται ως ένα ρεύμα από bytes. Η διεργασία-παραλήπτης λαμβάνει τα δεδομένα με την ίδια σειρά που τα μεταδίδει η διεργασία-αποστολέας.
- Γίνεται χρήση επιβεβαιώσεων για τα δεδομένα που μεταδίδονται. Δεδομένα, για τα οποία δεν έχει ληφθεί από τον αποστολέα επιβεβαίωση, αναμεταδίδονται.
- Πραγματοποιείται έλεγχος ροής. Με τη χρήση των επιβεβαιώσεων και ενός μηχανισμού κυλιόμενου παραθύρου, εξασφαλίζεται ότι ο αποστολέας δεν στέλνει δεδομένα ταχύτερα απ' όσο μπορεί να τα απορροφήσει ο παραλήπτης και ότι δεν θα εξαντληθεί ο χώρος ενταμίευσης.
- Πραγματοποιείται μεταφορά δεδομένων με σύνδεση. Η εγκατάσταση σύνδεσης αποτελεί προϋπόθεση για την υλοποίηση των παραπάνω μηχανισμών.
- Ο έλεγχος συμφόρησης αποβλέπει στην ομαλή ροή των δεδομένων στο δίκτυο και στην αποφυγή καταστάσεων συμφόρησης του δικτύου.

UDP

Το UDP επιτρέπει στις εφαρμογές να ανταλλάσσουν μονοσήμαντα ανεξάρτητα μηνύματα πληροφορίας. Προσφέρει μια μη αξιόπιστη υπηρεσία μεταφοράς χωρίς σύνδεση. Δεν χρησιμοποιεί επιβεβαιώσεις, δεν αριθμεί τα μηνύματα και δεν ελέγχει τη ροή τους. Επομένως, μια εφαρμογή που χρησιμοποιεί το UDP θα πρέπει η ίδια να λύσει το πρόβλημα της αξιοπιστίας. Κάθε μήνυμα UDP μεταφέρει μαζί με τα δεδομένα και την θύρα της πηγής και του προορισμού του μηνύματος.

Αν και τα μειονεκτήματα είναι αρκετά, υπάρχουν περιπτώσεις όπου το UDP θεωρείται καταλληλότερο από το TCP, για τους εξής λόγους:

- Δεν υπάρχει εγκατάσταση σύνδεσης πριν τη μετάδοση των δεδομένων, άρα ούτε και χρονική καθυστέρηση.
- Δεν διατηρεί κατάσταση σύνδεσης. Έτσι, ένας εξυπηρετητής (server) υπεύθυνος για μια εφαρμογή μπορεί να εξυπηρετήσει πολλούς παραπάνω ενεργούς clients.
- Το UDP-datagram έχει μικρή επικεφαλίδα.
- Ο ρυθμός μετάδοσης δεν περιορίζεται ούτε επιβαρύνεται λόγω ελέγχου των πακέτων. Ο περιορισμός του ρυθμού μετάδοσης μπορεί να έχει σοβαρές επιπτώσεις σε εφαρμογές πραγματικού χρόνου.

Πρωτόκολλα δρομολόγησης IP

Ένα αυτόνομο σύστημα αποτελείται από μια ομάδα δρομολογητών που βρίσκονται υπό τον έλεγχο της ίδιας διαχειριστικής αρχής και ανταλλάσσουν πληροφορίες χρησιμοποιώντας το ίδιο πρωτόκολλο δρομολόγησης. Τα Αυτόνομα Συτήματα (AS) μπορούν να ταξινομηθούν στις παρακάτω τρεις κατηγορίες:

- Ένα **αυτόνομο σύστημα stub** έχει μία και μόνο σύνδεση προς ένα άλλο AS. Δεδομένα τα οποία στέλνονται προς ή λαμβάνονται από διευθύνσεις εκτός του AS θα πρέπει να περάσουν από τη συγκεκριμένη σύνδεση.
- Ένα **αυτόνομο σύστημα διέλευσης** έχει πολλαπλές συνδέσεις με ένα ή παραπάνω AS. Γεγονός το οποίο επιτρέπει σε δεδομένα που δεν έχουν ως προορισμό του συγκεκριμένο AS να το διατρέξουν.
- Ένα **αυτόνομο σύστημα multihomed** έχει κι αυτό πολλαπλές συνδέσεις με ένα ή περισσότερα AS, αλλά δεν επιτρέπει σε δεδομένα που δεν έχουν ως προορισμό το συγκεκριμένο AS να το διατρέξουν. Με άλλα λόγια, δεν υπάρχει υπηρεσία διέλευσης προς άλλα AS.

Τα πρωτόκολλα δρομολόγησης IP χωρίζονται σε δύο κατηγορίες: στα **εσωτερικής δρομολόγησης** και στα **εξωτερικής δρομολόγησης**. Τα εσωτερικής δρομολόγησης (IGP) εκτελούν δρομολόγηση εντός αυτόνομων συστημάτων, ενώ τα εξωτερικής (EGP) χρησιμοποιούνται για την ανταλλαγή πληροφορίας δρομολόγησης μεταξύ διαφορετικών αυτόνομων συστημάτων. Επιπλέον, τα πρωτόκολλα δρομολόγησης διακρίνονται σε **πρωτόκολλα στατικής και δυναμικής δρομολόγησης**.

Στατική δρομολόγηση
Ο πίνακας δρομολόγησης δημιουργείται κάθε φορά που ενεργοποιείται μια διασύνδεση από τον διαχειριστή του κάθε σταθμού και παραμένει αναλλοίωτος, εκτός εξαιρέσεων, μέχρι την επόμενη ενημέρωση από τον διαχειριστή του συστήματος. Τα μονοπάτια, δηλαδή, που συνδέουν τους διάφορους κόμβους είναι στατικά.

Ο δρομολογητής έχει αρχικά στον πίνακα δρομολόγησης μόνο την προεπιλεγμένη εγγραφή δρομολόγησης. Με την πάροδο του χρόνου όμως, δημιουργεί έναν πίνακα δρομολόγησης χρησιμοποιώντας το πρωτόκολλο ICMP καθώς και πληροφορίες σχετικές με την τοπολογία του δικτύου από γειτονικούς δρομολογητές. Ένα πρόβλημα με τη μέθοδο αυτή είναι ότι για κάθε προορισμό δημιουργείται μια εγγραφή στον πίνακα δρομολόγησης. Οι διαδρομές που εγγράφονται στον πίνακα αφορούν μόνο προορισμούς τερματικών και όχι δικτύων. Έτσι, ακόμη και αν δυο τερματικά βρίσκονται στο ίδιο δίκτυο, δεν είναι δυνατόν να γίνει μία μόνο εγγραφή στον πίνακα δρομολόγησης. Το αποτέλεσμα είναι ότι οδηγούμαστε σε άσκοπη κατανάλωση μνήμης και αύξηση του χρόνου αναζήτησης των διευθύνσεων στον πίνακα. **Η στατική δρομολόγηση μπορεί να είναι αποτελεσματική στην περίπτωση μικρών δικτύων**.

Δυναμική δρομολόγηση
Ένας δρομολογητής που υλοποιεί δυναμική δρομολόγηση κατασκευάζει και ενημερώνει δυναμικά τους πίνακες δρομολόγησής του. Η ενημέρωση πραγματοποιείται με την περιοδική ή κατόπιν αιτήματος ανταλλαγή μηνυμάτων με τους γειτονικούς δρομολογητές. Ο μηχανισμός δρομολόγησης καθορίζει την «πολιτική» δρομολόγησης, αποφασίζοντας ποια είναι η βέλτιστη διαδρομή προς έναν προορισμό, την οποία και εγγράφει στον πίνακα δρομολόγησης. Η ικανότητα κλιμάκωσης ενός δικτύου και ανάκτησης από δικτυακά σφάλματα καθιστά τη δυναμική δρομολόγηση την καλύτερη επιλογή για μεσαία, μεγάλα και πολύ μεγάλα δίκτυα.

Τα πρωτόκολλα δυναμικής δρομολόγησης IP βασίζονται συνήθως στις παρακάτω τεχνολογίες:

- Πρωτόκολλα δρομολόγησης διανύσματος απόστασης
- Πρωτόκολλα δρομολόγησης κατάστασης ζεύξης

Αλγόριθμος δρομολόγησης κατάστασης ζεύξης
Ο αλγόριθμος είναι γνωστός ως **αλγόριθμος Dijkstra** και υπολογίζει το μονοπάτι ελάχιστου κόστους από έναν κόμβο προς όλους τους άλλους σε ένα δίκτυο. Περισσότερα στη Βικιπαίδεια ή στο βιβλίο (σελ 61).

RIP
Το πρωτόκολλο αυτό ανήκει στην κατηγορία πρωτοκόλλων **απόστασης διανύσματος** και χρησιμοποιεί τον **αλγόριθμο Bellman-Ford** για να υπολογίσει τις βέλτιστες διαδρομές. Κατά την εκκίνηση ενός συστήματος που χρησιμοποιεί το πρωτόκολλο RIP, το σύστημα αναζητά τις ενεργές διασυνδέσεις μεταξύ των δρομολογητών του. Κατόπιν, στέλνει πακέτα RIP ζητώντας τους πλήρεις πίνακες δρομολόγησης των γειτονικών δρομολογητών. Στη συνέχεια, το σύστημα που ζήτησε την πληροφορία ενημερώνει τον πίνακα δρομολόγησής του. Το πρωτόκολλο RIP ορίζει ένα χρονιστή ενημέρωσης, ο οποίος καθορίζει τη συχνότητα αποστολής των περιοδικών ενημερώσεων. Συνήθως, στον χρονιστή αυτό προστίθεται και ένας μικρός τυχαίος αριθμός κάθε φορά που αρχικοποιείται, ώστε να αποφευχθεί η πιθανή συμφόρηση στην περίπτωση που όλοι οι δρομολογητές προσπαθούσαν ταυτόχρονα να στείλουν ενημερώσεις στους γειτονικούς δρομολογητές. Εκτός από την ενημέρωση κατά τακτά χρονικά διαστήματα, υπάρχει και η εξαναγκασμένη ενημέρωση, η οποία πραγματοποιείται όταν αλλάζει η τοπολογία του δικτύου.

Το RIP, παρόλο που είναι πολύ απλό πρωτόκολλο, έχει σημαντικά μειονεκτήματα.
- Ο μέγιστος αριθμός δρομολογητών μέσω των οποίων μπορεί να διέλθει ένα μήνυμα είναι 15. Συνεπώς, δεν είναι δυνατή η χρήση του σε μεγάλα δίκτυα.
- Το πρωτόκολλο δεν περιέχει πληροφορία διευθυνσιοδότησης υποδικτύων. Έτσι, δεν είναι ικανό να διακρίνει αν μια διεύθυνση αντιστοιχεί σε υποδίκτυο ή σε τερματικό.
- Η κίνηση που προκαλεί καταναλώνει αρκετό εύρος ζώνης. Πολλές αλλαγές στη δικτυακή τοπολογία συνεπάγονται πολλές ενημερώσεις και κατά συνέπεια αύξηση της πιθανότητας συμφόρησης του δικτύου.
- Σημαντικό μειονέκτημα αποτελεί ο μεγάλος χρόνος που απαιτείται μέχρι να ισορροπήσει μετά την αστοχία ή την απενεργοποίηση μιας ζεύξης.
- Είναι δυνατόν, διαδρομή με λίγους κόμβους να αποτελείται από ζεύξεις χαμηλού ρυθμού διέλευσης και τα πακέτα να καθυστερούν περισσότερο απ' ότι αν ακολουθούσαν διαδρομή με περισσότερους κόμβους.
- Το πρωτόκολλο δεν προβλέπει εξισορρόπηση φορτίου σε περιπτώσεις ισοδύναμων διαδρομών, αφού στον πίνακα υπάρχει μόνο μια εγγραφή για κάθε προορισμό.

OSPF
Πρόκειται για πρωτόκολλο **δυναμικής δρομολόγησης** για μεγάλα δίκτυα και είναι πρωτόκολλο **κατάστασης ζεύξης**. Υλοποιεί δηλαδή τον αλγόριθμο του Dijkstra.

Από άκρο σε άκρο αποφυγή συμφόρησης

Μηχανισμός συρόμενου παραθύρου
Η τεχνική του συρόμενου παραθύρου επιτρέπει σε κάθε χρήστη του δικτύου να μεταδώσει έναν αριθμό πακέτων ίσο με το μέγεθος του παραθύρου, πριν περιμένει για τις επιβεβαιώσεις των πακέτων που έστειλε. Επίσης, δίνει τη δυνατότητα στον παραλήπτη να περιορίσει τον ρυθμό μετάδοσης μέχρι να αδειάσουν οι ενταμιευτές του.

Βασικοί ορισμοί, για την αναλυτική επεξήγηση του μηχανισμού:
- **Segment**: οποιοδήποτε πακέτο IP μεταφέρει δεδομένα TCP ή/και επιβεβαιώσεις.

- **Sender maximum segment size** (smss): Μέγιστο μήκος ενός πακέτου που μπορεί να μεταδώσει ένας αποστολέας.
- **Receiver maximum segment size** (rmss): Μέγισο μήκος ενός πακέτου που μπορεί να δεχτεί ο παραλήπτης.
- **Full size segment**: Ένα πακέτο μήκους smss bytes.
- **Receiver window** (rwnd): Το πιο πρόσφατο μήκος παραθύρου που ανακοίνωσε ο παραλήπτης στον αποστολέα.
- **Congestion window** (cwnd): Το μήκος του παραθύρου που χρησιμοποιεί ο αποστολέας για τη μετάδοση των δεδομένων. Πρέπει πάντα $cwnd \leq rwnd$.
- **Initial window** (IW): Η αρχική τιμή του cwnd, αμέσως μετά την εγκατάσταση της σύνδεσης.
- **Loss window** (LW): Το cwnd γίνεται ίσο με το LW, όταν ο αποστολέας αντιληφθεί απώλεια πακέτου με τη λήξη του χρονιστή επανεκπομπής.
- **Restart window** (RW): Το cwnd γίνεται ίσο με το RW, όταν ο αποστολέας ξεκινά τη μετάδοση μετά από περίοδο σιωπής.

Περισσότερα στο βιβλίο (σελ. 89)

Αργή έναρξη και αποφυγή συμφόρησης

Μια επιπλέον μεταβλητή που χρειάζεται είναι ένα κατώφλι αργής έναρξης, το **ssthresh**, που χρησιμοποιείται για να καθορίσει αν θα χρησιμοποιηθεί ο αλγόριθμος αργής έναρξης ή ο αλγόριθμος αποφυγής συμφόρησης. Ο αποστολέας συγκρίνει την τιμή του cwnd με το ssthresh:

- Αν cwnd<ssthresh, τότε επιλέγεται ο αλγόριθμος αργής έναρξης. Αυτός θέτει αρχικά μια μικρή τιμή στο cwnd, αλλά στη συνέχεια αυξάνει την τιμή του cwnd εκθετικά.
- Αν cwnd>ssthresh, τότε επιλέγεται ο αλγόριθμος αποφυγής συμφόρησης, ο οποίος προκαλεί γραμμική αύξηση του cwnd.
- Αν qwnd=ssthresh, επιλέγεται οποιοσδήποτε από τους δύο αλγόριθμους.

Ταχεία επανεκπομπή και ταχεία ανάρρωση

Ο αποστολέας θεωρεί ότι επικρατεί συμφόρηση στο δίκτυο, όταν αντιληφθεί απώλεια πακέτων (αν δε λάβει επιβεβαίωση εντός ορισμένου χρονικού διαστήματος ή αν λάβει δύο ή παραπάνω επιβεβαιώσεις για το ίδιο πακέτο). Η περίπτωση του timeout υποδηλώνει σοβαρό πρόβλημα συμφόρησης, καθώς έχει σταματήσει η ροή των πακέτων. Η περίπτωση των πολλαπλών όμοιων επιβεβαιώσεων υποδηλώνει ελαφρύτερη μορφή συμφόρησης: έχει χαθεί κάποιο πακέτα, όμως πακέτα μεταγενέστερα του χαμένου φτάνουν στον παραλήπτη και προκαλούν τις πολλαπλές όμοιες επιβεβαιώσεις.

- Αν συμβεί retransmission timeout, το cwnd γίνεται ίσο με LW. Επιπλέον ο αποστολέας πρέπει να θέσει το ssthresh σε μικρότερη τιμή. Αφού ο αποστολέας μεταδώσει ξανά το χαμένο πακέτο, χρησιμοποιεί τον αλγόριθμο αργής έναρξης.
- Αν ο αποστολέας λάβει τρεις όμοιες επιβεβαιώσεις, θέτει σε λειτουργία τον αλγόριθμο ταχείας επανεκπομπής, κατά τον οποίο με τη λήψη της τρίτης όμοιας επιβεβαίωσης, ο αποστολέας θα μεταδώσει το χαμένο πακέτο χωρίς να περιμένει τη λήξη του timer. Μετά την αναμετάδοση του χαμένου πακέτου, ο αποστολέας ενεργοποιεί τον αλγόριθμο ταχείας ανάρρωσης.

Η υποδομή δημόσιου κλειδιού (PKI)

Οι αλγόριθμοι κρυπτογράφησης χωρίζονται σε δύο βασικές κατηγορίες:

- **Αλγόριθμοι συμμετρικού κλειδιού**: προϋποθέτουν ότι χρησιμοποιείται το ίδιο μυστικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος. Αν ο αλγόριθμος συμμετρικού κλειδιού εφαρμόζεται σε ομάδες bit συγκεκριμένου μεγέθους, τότε ονομάζεται ομαδικός, ενώ στην περίπτωση που κρυπτογραφείται κάθε bit ξεχωριστά, ονομάζεται αλγόριθμος ροής.
- **Αλγόριθμοι ασύμμετρου κλειδιού**: χρησιμοποιούν διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος. Το κλειδί της κρυπτογράφησης είναι δημόσιο, ενώ της αποκρυπτογράφησης είναι ιδιωτικό, δηλαδή κρυφό. Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη και ο παραλήπτης είναι ο μοναδικός που μπορεί να αποκρυπτογραφήσει το μήνυμα με το ιδιωτικό του κλειδί.

Η υποδομή δημόσιου κλειδιού αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών ασύμμετρης κρυπτογραφίας και υπηρεσιών, ο οποίος πιστοποιεί την εγκυρότητα του κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή και παράλληλα προστατεύει την ασφάλεια κάθε συναλλαγής.

Βασικές λειτουργίες του PKI είναι:

- **Χορήγηση ψηφιακών πιστοποιητικών:** είναι η διαδικασία με την οποία συνδέουμε έναν ιδιώτη, μια εταιρία ή κάποια άλλη οντότητα με την τιμή ενός δημόσιου κλειδιού
- **Επαλήθευση**: είναι η διαδικασία επαλήθευσης ότι ένα πιστοποιητικό ισχύει ακόμα.

<u>Έκδοση πιστοποιητικών</u>
Ένα πιστοποιητικό είναι μια συλλογή πληροφοριών, οι οποίες έχουν υπογραφεί ηλεκτρονικά από τον εκδότη τους. Τα πιστοποιητικά, ανάλογα με το περιεχόμενό τους διακρίνονται σε τέσσερις κατηγορίες:

- **Προσωπικά πιστοποιητικά**, τα οποία δηλώνουν την ταυτότητα μιας οντότητας και τη συσχετίζουν με την τιμή ενός δημόσιου κλειδιού.
- **Πιστοποιητικά εξυπηρετητών**, τα οποία δηλώνουν την «ταυτότητα» εξυπηρετητών οι οποίοι επικοινωνούν με ασφάλεια με άλλους εξυπηρετητές μέσω πρωτοκόλλων επικοινωνίας όπως SSL.
- **Πιστοποιητικά αρχής πιστοποίησης**, τα οποία πιστοποιούν την ταυτότητα της αρχής πιστοποίησης. Περιέχουν πληροφορίες γι' αυτήν καθώς και το δημόσιο κλειδί της. Μπορεί να είναι υπογεγραμμένα από μια άλλη αρχή πιστοποίησης ή από την ίδια.
- **Πιστοποιητικά εταιριών λογισμικού**, τα οποία χρησιμοποιούνται για να πιστοποιούν προγράμματα που πωλούνται και διανέμονται.

Κύρια λειτουργία της αρχής έκδοσης πιστοποιητικών (Certification Authority) είναι να δέχεται αιτήσεις για πιστοποίηση της ταυτότητας διάφορων οντοτήτων και στη συνέχεια, με γνώμονα την πολιτική της, να εκδίδει ή όχι το πιστοποιητικό. Τα πιστοποιητικά που εκδίδει, τα καταχωρεί σε δημόσια ευρετήρια, από τα οποία μπορεί κάθε ενδιαφερόμενος να τα ανακτήσει προκειμένου να εξετάσει την ισχύ μιας ηλεκτρονικής υπογραφής ή να κρυπτογραφήσει ένα μήνυμα.

<u>Μοντέλα της υποδομής δημόσιου κλειδιού</u>

- PKI με μόνο μία CA
  Στο μοντέλο αυτό υπάρχει μία CA που εκδίδει πιστοποιητικά. Έτσι, αν δύο οντότητες Α και Β θέλουν να επικοινωνήσουν με ασφάλεια, αρκεί ο αποστολέας να έχει το δημόσιο

κλειδί της CA και η εμπιστοσύνη του αποστολέα προς την CA μεταβιβάζεται στον παραλήπτη. Ένα τέτοιο μοντέλο είναι εξυπηρετικό για έναν μικρό αριθμό χρηστών, καθώς όσο μεγαλύτερη είναι η ομάδα χρηστών τόσο δυσκολότερο για την CA να αντεπεξέλθει σε τεχνικό επίπεδο.

- Ιεραρχικό μοντέλο PKI
  Στο μοντέλο αυτό υπάρχουν πολλές CA και κάποιες από αυτές έχουν μεταξύ τους σχέση «προϊστάμενου – υφιστάμενου». Όλοι οι χρήστες εμπιστεύονται την ίδια ρίζα CA και αν δύο οντότητες θέλουν να επικοινωνήσουν μεταξύ τους, ο αποστολέας στέλνει ένα μήνυμα με το δημόσιο κλειδί της ρίζας CA και η εμπιστοσύνη μεταβιβάζεται από προϊστάμενη CA σε υφιστάμενη. Η ρίζα CA δεν εκδίδει πιστοποιητικά σε μεμονωμένους χρήστες, αλλά στις υφιστάμενες CA, οι οποίες μπορεί να εκδίδουν πιστοποιητικά σε χρήστες ή άλλες υφιστάμενες CA. Σ' αυτό το μοντέλο, η σχέση εμπιστοσύνης είναι μίας κατεύθυνσης (από την προϊστάμενη στην υφιστάμενη), Ένα τέτοιο μοντέλο είναι εύκολα επεκτάσιμο, αλλά ευάλωτο, αφού ένα πλήγμα στη ρίζα CA είναι αρκετό για να χάσει την αξιοπιστία του ολόκληρο το οικοδόμημα PKI.
- Μικτό μοντέλο PKI
  Εδώ οι CA εκδίδουν πιστοποιητικά για τους χρήστες τους, αλλά και μεταξύ τους, στα οποία περιγράφουν την αμφίδρομη σχέση εμπιστοσύνης ανάμεσά τους. Μπορεί εύκολα να προστεθεί στη δομή μια νέα CA: αρκεί μια υπάρχουσα CA να αναπτύξει σχέση εμπιστοσύνης με τη νέα. Επίσης, μια απώλεια στην αξιοπιστία μιας CA δεν οδηγεί στην κατάρρευση της PKI, αφού αυτή εύκολα μπορεί να απομονωθεί από τις υπόλοιπες.

Το πρωτόκολλο FTP

Το πρωτόκολλο αυτό χρησιμοποιείται για τη μεταφορά αρχείων από έναν υπολογιστή του Διαδικτύου σε κάποιον άλλο. Ο χρήστης έρχεται σε επαφή με το FTP μέσω μιας διεπαφής-χρήστη (FTP user interface), η οποία ουσιαστικά είναι κάποιο πρόγραμμα. Ο χρήστης παρέχει πρώτα το όνομα ή την IP διεύθυνση του απομακρυσμένου υπολογιστή, με αποτέλεσμα να εγκαθίσταται μια TCP σύνδεση μεταξύ των δύο υπολογιστών. Τότε, ο χρήστης παρέχει το username και το password.

Το FTP χρησιμοποιεί δύο παράλληλες συνδέσεις TCP για τη μεταφορά ενός αρχείου: μια **σύνδεση ελέγχου** και μια **σύνδεση δεδομένων**. Η πρώτη χρησιμοποιείται για τη μεταφορά πληροφοριών ελέγχου (όπως το username, το password, αλλαγή φακέλου, κλπ). Η δεύτερη χρησιμοποιείται για την πραγματική μεταφορά των αρχείων. Πρωτόκολλα που χρησιμοποιούν δύο TCP συνδέσεις λέμε ότι μεταφέρουν τις πληροφορίες ελέγχου **εκτός ζώνης**, ενώ γι' αυτά που χρησιμοποιούν μία σύνδεση λέμε ότι μεταφέρουν τις πληροφορίες ελέγχου εντός ζώνης.

Αρχικά, το FTP εγκαθιστά μια σύνδεση ελέγχου με τη θύρα 21 του απομακρυσμένου υπολογιστή. Όταν ο χρήστης ζητήσει τη μεταφορά ενός αρχείου, το FTP ανοίγει σύνδεση δεδομένων στη θύρα 20. Μέσω αυτής, στέλνεται ένα μόνο αρχείο και όταν τελειώσει η μεταφορά, η σύνδεση κλείνει. Αν ο χρήστης θέλει να μεταφέρει κι άλλα αρχεία, τότε ανοίγονται ξεχωριστές συνδέσεις δεδομένων. Επομένως, στο FTP η σύνδεση ελέγχου παραμένει ανοιχτή καθόλη τη διάρκεια της συνόδου, ενώ συνδέσεις δεδομένων ανοίγουν και κλείνουν ανάλογα με τα αρχεία που μεταφέρονται.

Το πρωτόκολλο DNS

Το DNS χρησιμοποιείται συχνά από άλλα πρωτόκολλα του στρώματος εφαρμογής, όπως το HTTP και το FTP, για τη μετάφραση των διευθύνσεων που δίνουν οι χρήστες σε IP διευθύνσεις. Το πρωτόκολλο αυτό χρησιμοποιεί το UDP στο στρώμα μεταφοράς και συγκεκριμένα τη θύρα 53. Για παράδειγμα, για να μπορέσει ο client να ανοίξει μια ιστοσελίδα, θα πρέπει να μάθει την IP διεύθυνση του server που φιλοξενεί αυτήν την ιστοσελίδα. Το μηχάνημα του χρήστη, που λειτουργεί ως DNS πελάτης, στέλνει μέσω ενός DNS ερωτήματος (query) την διεύθυνση της ιστοσελίδας και λαμβάνει απάντηση από τον DNS server την ζητούμενη διεύθυνση IP.

Το DNS εισάγει μια επιπλέον καθυστέρηση στις εφαρμογές που το χρησιμοποιούν. Για τη μείωση της καθυστέρησης αυτής, η επιθυμητή διεύθυνση IP συνήθως αποθηκεύεται προσωρινά σε κάποιον κοντινό εξυπηρετητή DNS. Αν και πρόκειται για πρωτόκολλο του στρώματος εφαρμογής, έχει μια βασικά διαφορά με τα υπόλοιπα: ο χρήστης δεν μπορεί να έρθει σε άμεση επαφή με το DNS. Το DNS το χρησιμοποιούν άλλες εφαρμογές και όχι ο ίδιο ο χρήστης.

Η δομή του DNS

Υπάρχουν τρία είδη DNS εξυπηρετητών.

- **Τοπικοί εξυπηρετητές ονομάτων**: Κάθε πάροχος (ISP) έχει έναν τοπικό DNS server, οποίος είναι και ο default. Όταν ένα host κάνει ένα DNS ερώτημα, τότε αυτό στέλνεται πρώτα απ' όλα στον τοπικό εξυπηρετητή.
- **Εξυπηρετητές ονομάτων δρομολόγησης**: Όταν ο τοπικός DNS server δεν μπορεί να απαντήσει στο query (επειδή δεν περιέχει εγγραφή για τη διεύθυνση για την οποία γίνεται το ερώτημα), τότε αυτός λειτουργεί ως DNS client και στέλνει query σε έναν εξυπηρετητή ονομάτων δρομολόγησης. Αν αυτός μπορεί να απαντήσει, τότε στέλνει την απάντηση στον τοπικό server και εκείνος με τη σειρά του τη στέλνει στον αρχικό client. Διαφορετικά, «απευθύνεται» στους επίσημους εξυπηρετητές ονομάτων.
- **Επίσημοι εξυπηρετητές ονομάτων**: Κάθε host είναι εγγεγραμμένος σε κάποιον επίσημο DNS server.

Η λειτουργία του DNS, όπως περιγράφηκε παραπάνω είναι **αναδρομική**. Το πρωτόκολλο DNS όμως επιτρέπει και επαναληπτικά ερωτήματα σε κάθε βήμα της αλυσίδας μεταξύ του αιτούντα host και του επίσημου DNS server. Όταν ο DNS server Α κάνει μια **επαναληπτική** ερώτηση στον DNS server Β, αν ο Β δεν μπορεί να απαντήσει στο ερώτημα, στέλνει στον Α μια DNS απόκριση, η οποία περιέχει τη διεύθυνση IP του επόμενου εξυπηρετητή ονομάτων στην αλυσίδα, έστω τον Γ. Έπειτα, ο Α στέλνει απευθείας στον Γ το ερώτημα. Στην αλυσίδα των ερωτήσεων, κάποιες μπορεί να είναι αναδρομικές και κάποιες άλλες επαναληπτικές.

Εγγραφές πόρων

Οι εξυπηρετητές ονομάτων, κρατούν μια βάση δεδομένων στην οποία αποθηκεύουν εγγραφές πόρων για τις αντιστοιχίες μεταξύ ονομάτων (domains) και IP διευθύνσεων. Μια εγγραφή είναι μια τετράδα (name, value, type, TTL). Το TTL δίνει τον χρόνο ζωής της εγγραφής, μετά τη λήξη του οποίου η εγγραφή πρέπει να διαγραφεί από την προσωρινή μνήμη. Η σημασία των name και value εξαρτάται από το πεδίο type:

- Αν type=A, τότε το name είναι το όνομα του host και το πεδίο value η διεύθυνση IP για το συγκεκριμένο όνομα host.
- Αν type=NS, τότε το πεδίο name είναι το όνομα της περιοχής domain και το πεδίο value το όνομα του εξυπηρετητή, που γνωρίζει πώς να ανακτά τις διευθύνσεις IP των hosts της ίδιας περιοχής.
- Αν type=CNAME, τότε το πεδίο value είναι το κανονικό όνομα για το ψευδώνυμο name. Οι εγγραφές αυτές χρησιμεύουν στη δημιουργία ψευδώνυμων για τα ονόματα των host του Διαδικτύου.
- Αν type=MX, τότε το πεδίο value είναι το όνομα ενός εξυπηρετητή ταχυδρομείου, ο οποίος έχει ψευδώνυμο name. Οι εγγραφές αυτές επιτρέπουν τα ονόματα των host των εξυπηρετητών ταχυδρομείου να έχουν απλά ψευδώνυμα.

Ηλεκτρονικό ταχυδρομείο

Τα τρία βασικά στοιχεία της αρχιτεκτονικής του ηλεκτρονικού ταχυδρομείου είναι:

- οι **αντιπρόσωποι χρηστών** (user agents): επιτρέπουν στους χρήστες να συνθέσουν, να διαβάσουν και να στείλουν e-mail.
- οι **εξυπηρετητές ταχυδρομείου** (mail servers): τα e-mails που στέλνονται, φτάνουν πρώτα εδώ και αποθηκεύονται σε μια εξερχόμενη ουρά μηνυμάτων
- το **πρωτόκολλο μεταφοράς** των μηνυμάτων.

Το σύστημα e-mail επιτελεί βασικά τις παρακάτω λειτουργίες:

- Σύνθεση (δηλαδή, δημιουργία) μηνυμάτων και απαντήσεων.
- Μεταφορά μηνυμάτων από την πηγή προς τον προορισμό.
- Αναφορά προς τον αποστολέα, για το αν το μήνυμα έφτασε στον τελικό του προορισμό, αν χάθηκε ή αν απορρίφθηκε.
- Παρουσίαση των περιεχομένων του μηνύματος
- Διευθέτηση, που αφορά το τι θα κάνει το μήνυμα ο παραλήπτης του, πχ μπορεί να το διαγράψει ή να το αποθηκεύσει.
- Πέρα από τα παραπάνω, που είναι οι βασικές λειτουργίες, οι αντιπρόσωποι χρηστών μπορεί να έχουν και πιο εξειδικευμένες, όπως προώθηση (fowarding) των μηνυμάτων, παραμετροποίηση του mailbox κλπ.

SMTP

Πρόκειται για πρωτόκολλο μεταφοράς μηνυμάτων ηλεκτρονικού ταχυδρομείου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP στο στρώμα μεταφοράς και τη θύρα 25. Ο εξυπηρετητής ταχυδρομείου του αποστολέα αποτελεί το **client side (πλευρά του πελάτη)**, ενώ αυτός του παραλήπτη

αποτελεί το **server side (πλευρά του εξυπηρετητή)**. Κάθε mail server μπορεί να παίξει και τις δύο πλευρές.

Αρχικά, λοιπόν, το SMTP ανοίγει μια TCP σύνδεση στη θύρα 25 μεταξύ των εξυπηρετητών ταχυδρομείου του αποστολέα και του παραλήπτη. Στη συνέχεια, πραγματοποιείται ένα είδος «χαιρετισμού», κατά τον οποίο οι δύο servers γνωστοποιούν ο ένας στον άλλο τη διεύθυνσή τους. Στη συνέχεια, το client side του εξυπηρετητή του αποστολέα γνωστοποιεί στο server side του εξυπηρετητή του παραλήπτη τις e-mail διευθύνσεις του αποστολέα και του παραλήπτη και τέλος, αποστέλλεται το ίδιο το μήνυμα. Σε περίπτωση που ο πελάτης έχει κι άλλα μηνύματα να στείλει προς τον ίδιο mail server, τότε τα στέλνει μέσω της ίδιας TCP σύνδεσης και έπειτα την κλείνει.

Το SMTP είναι ένα πρωτόκολλο με το οποίο ο πελάτης μπορεί να γράψει στον εξυπηρετητή, σε αντίθεση με την πλειονότητα των πρωτοκόλλων του στρώματος εφαρμογής (με εξαίρεση το FTP).

POP3
Το πρωτόκολλο αυτό είναι ένα απλό πρωτόκολλο μεταφοράς, που χρησιμοποιεί TCP σύνδεση στη θύρα 110 του εξυπηρετητή. Κατά την πρώτη φάση, ο user agent στέλνει ένα όνομα χρήστη (username) κι έναν κωδικό (password) στον εξυπηρετητή, τα οποία χρησιμοποιούνται για την πιστοποίηση του χρήστη. Σε δεύτερη φάση, ο user agent μπορεί σημειώσει τα μηνύματα προς διαγραφή ή να αφαιρέσει τα σημάδια διαγραφής από κάποια μηνύματα και να πάρει στατιστικά στοιχεία για τη χρήση του ηλεκτρονικού ταχυδρομείου. Κατά την τρίτη φάση, που εκτελείται όταν ο χρήστη δώσει την εντολή quit, για την τερματισμό του πρωτοκόλλου, διαγράφονται τα μηνύματα που είναι σημειωμένα για διαγραφή και τερματίζεται η σύνδεση.

Το POP3 δεν παρέχει άλλες υπηρεσίες.

IMAP
Αυτό το πρωτόκολλο παρέχει πολλές επιπλέον δυνατότητες από αυτές του POP3, όπως:

- οργάνωση των μηνυμάτων στο mailbox σαν να ήταν αρχεία του τοπικού συστήματος
- υποστήριξη πολλών καταλόγων (φακέλων) για την ταξινόμηση των μηνυμάτων
- αναζήτηση μηνυμάτων με βάση ορισμένα κριτήρια
- λήψη ενός μόνο τμήματος από ένα MIME μήνυμα που έχει κι άλλα τμήματα

Ο IMAP server βρίσκεται πάντα σε μία από τις ακόλουθες τέσσερις καταστάσεις και ανάλογα την κατάσταση του server γίνονται αποδεκτές και οι αντίστοιχες εντολές του πρωτοκόλλου.

- **Κατάσταση μη πιστοποίησης**, στην οποία βρίσκεται κατά την έναρξη της συνόδου. Στην κατάσταση αυτή, ζητείται από τον χρήστη το username και το password.
- Μετά την παροχή των στοιχείων αυτών από τον χρήστη, ο server μεταβαίνει σε **κατάσταση πιστοποίησης** και ζητά από τον χρήστη να επιλέξει έναν κατάλογο πριν από τις εντολές που σχετίζονται με τα μηνύματα
- Στην **κατάσταση επιλογής**, ο χρήστης μπορεί να δώσει εντολές που σχετίζονται με τα μηνύματα
- Τέλος, ο server βρίσκεται στην **κατάσταση εξόδου** κατά τον τερματισμό της συνόδου.

Το πρωτόκολλο HTTP

Το HTTP ανήκει στο στρώμα εφαρμογής του Διαδικτύου. Χρησιμοποιεί το TCP ως πρωτόκολλο μεταφοράς και εγκαθιστά σύνδεση στην θύρα 80 του server. Λόγω της χρήσης του TCP, το HTTP δεν χρειάζεται να ασχοληθεί με τη μεταφορά των δεδομένων. Το μόνο που πρέπει να κάνει είναι να στείλει τις αιτήσεις μέσω της TCP σύνδεσης και να περιμένει τις αποκρίσεις. Το TCP εγγυάται την αξιόπιστη μεταφορά των δεδομένων καθώς και τον έλεγχο της συμφόρησης. Το HTTP δεν κρατάει πληροφορία για την κατάσταση του πελάτη και γι' αυτό χαρακτηρίζεται **stateless**.

Το πρωτόκολλο αυτό μπορεί να χρησιμοποιεί είτε μόνιμες είτε μη μόνιμες συνδέσεις.

- Με τις **μη μόνιμες συνδέσεις**, για κάθε αντικείμενο μιας ιστοσελίδας (πχ, ένα html αρχείο ή ένα αρχείο εικόνας κλπ) ανοίγεται ξεχωριστή TCP σύνδεση. Οι συνδέσεις αυτές μπορούν να υλοποιηθούν **σειριακά** (μια σύνδεση ανοίγει αφού κλείσει η προηγούμενη), αλλά αν το υποστηρίζει ο browser μπορούν να υλοποιηθούν και **παράλληλα**.
- Στις μόνιμες συνδέσεις, ο εξυπηρετητής TCP δεν τερματίζει τη σύνδεση αμέσως μετά την αποστολή της απόκρισης. Αντίθετα, την τερματίζει μετά από κάποιο συγκεκριμένο χρονικό διάστημα, για το οποίο η σύνδεση παραμένει ανενεργή. Υπάρχουν δύο τύπου μόνιμες συνδέσεις:
  - Στην περίπτωση της μόνιμης σύνδεση **χωρίς pipelining**, ο πελάτης στέλνει μια καινούργια αίτηση μόνο μετά τη λήψη της προηγούμενης απάντησης.
  - Ο χρόνος απόκρισης μπορεί να βελτιωθεί με τη χρήση μόνιμων συνδέσεων **με pipelining**.

Proxy server

Πρόκειται για έναν εξυπηρετητή, ο οποίος ικανοποιεί τις HTTP αιτήσεις για λογαριασμό του πελάτη. Αποθηκεύει στον δικό του δίσκο όλα τα αντικείμενα που έλαβε πρόσφατα. Έτσι, αν ο χρήστης στείλει αίτηση για ένα αντικείμενο, το οποίο είχε πρόσφατα ξαναζητήσει, τότε θα το λάβει άμεσα από τον proxy server και δεν θα χρειαστεί να φτάσει η αίτηση στον αυθεντικό εξυπηρετητή και από κει να σταλεί ολόκληρο το αντικείμενο. Η χρήστη του proxy server έχει τρία πλεονεκτήματα:

- Μπορεί να μειωθεί ο χρόνος απόκρισης μιας αίτησης από τον πελάτη, ειδικά αν το σημείο συμφόρησης του δικτύου βρίσκεται μεταξύ του proxy server και του αυθεντικού εξυπηρετητή (που είναι η συνηθισμένη περίπτωση).
- Μειώνει το φορτίο μεταξύ του ISP και του Διαδικτύου, με αποτέλεσμα να χρειάζονται γραμμές μικρότερου εύρους ζώνης.
- Ο proxy server μειώνει γενικά το φορτίο του Διαδικτύου, αφού η κίνηση του Ιστού αποτελεί το μεγαλύτερο τμήμα της συνολικής κίνησης του Διαδικτύου.

Συνοπτικά:

Πρωτόκολλο εφαρμογής	**Πρωτόκολλο μεταφοράς και θύρα**	**Stateless**	**Μεταφορά πληροφοριών ελέγχου εκτός ζώνης**	**Σχόλια**
FTP	TCP/21	Όχι	Ναι	
DNS	UDP/53	Ναι	-	Μπορεί να κάνει αναδρομικά ή και επαναληπτικά ερωτήματα
SMTP	TCP/25	Όχι	Όχι	
POP3	TCP/110	Όχι	Όχι	
IMAP	TCP/143	Όχι	Όχι	Είναι για τον ίδιο σκοπό, αλλά δίνει περισσότερες δυνατότητες από το POP3
HTTP	TCP/80	Ναι	-	Οι συνδέσεις μπορεί να είναι μόνιμες (με ή χωρίς pipelining) ή μη μόνιμες