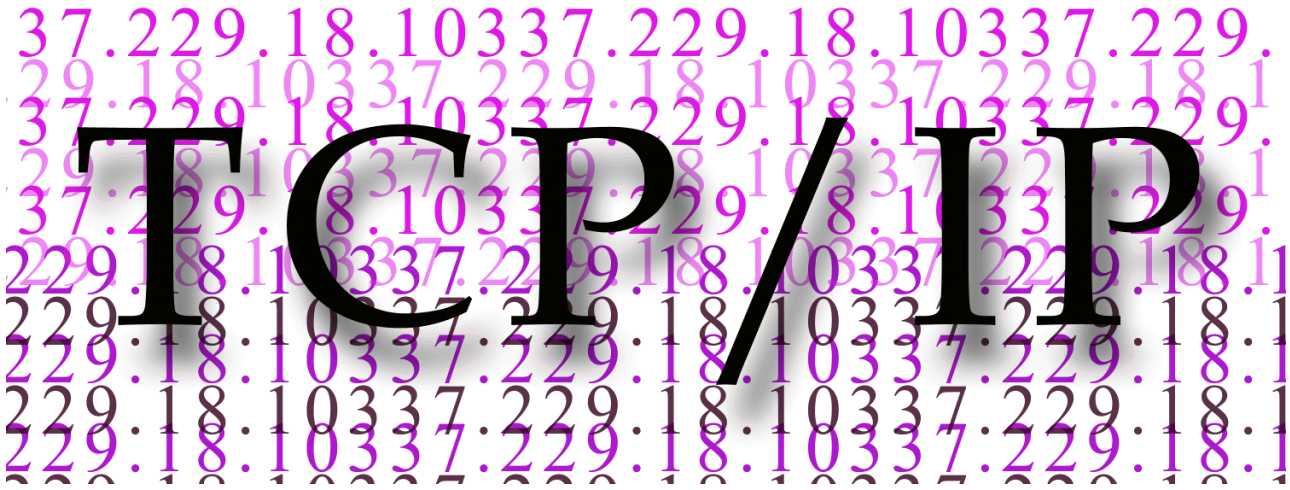
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΤΕΙ ΗΠΕΙΡΟΥ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΩΜΑΣ ΣΩΤ. ΤΣΙΓΑΡΑΣ
ΑΜ: 5864

<<ΠΡΩΤΟΚΟΛΛΟ TCP/IP>>



Επιβλέπουσα καθηγήτρια: Πηνελόπη Δράκου

ΣΕΠΤΕΜΒΡΙΟΣ 2008
ΑΡΤΑ

Περιεχόμενα

1 ΕΙΣΑΓΩΓΗ

1.1 ΜΙΑ ΣΥΝΤΟΜΗ ΙΣΤΟΡΙΑ

Ένα δίκτυο είναι μία ομάδα συνδεδεμένων συσκευών που επικοινωνούν μεταξύ τους, όπως υπολογιστές και εκτυπωτές. Ένα διαδίκτυο (internet) είναι δύο ή περισσότερα δίκτυα που μπορούν να επικοινωνούν μεταξύ τους. Το πιο αξιοσημείωτο διαδίκτυο είναι το Internet, το οποίο αποτελείται από εκατοντάδες χιλιάδες συνδεδεμένα δίκτυα. Ιδιώτες όπως και διάφοροι οργανισμοί, όπως κυβερνητικά κλιμάκια, σχολεία, ερευνητικά κέντρα, εταιρίες και βιβλιοθήκες, σε περισσότερες από 100 χώρες, χρησιμοποιούν το Internet. Εκατομμύρια άνθρωποι είναι χρήστες. Κι όμως, αυτό το ασυνήθιστο σύστημα επικοινωνίας γεννήθηκε μόλις το 1969.

1.1.1 Γέννηση του Internet

Το 1972, οι Vint Cerf και Bob Kahn, οι οποίοι ήταν μέλη της βασικής ομάδας του ARPANET (ένα μικρό δίκτυο συνδεδεμένων υπολογιστών), συνεργάστηκαν για να διεκπεραιώσουν αυτό που ονόμασαν διαδικτυακό έργο (internetting project). Ήθελαν να συνδέσουν διαφορετικά δίκτυα ώστε ένας κεντρικός υπολογιστής ενός δικτύου να επικοινωνούσε με τον κεντρικό υπολογιστή άλλου δικτύου. Υπήρχαν πολλά προβλήματα που έπρεπε να ξεπεραστούν: διάφορα μεγέθη πακέτων, διάφορες διεπαφές, διάφοροι ρυθμοί μετάδοσης και διάφορες απαιτήσεις αξιοπιστίας. Ο Cerf και ο Kahn επινόησαν την ιδέα μίας συσκευής που ονομάζεται gateway (θύρα εξόδου) που εξυπηρετούσε ως ενδιάμεσο υλικό που μετέδιδε δεδομένα από ένα δίκτυο σε άλλο.

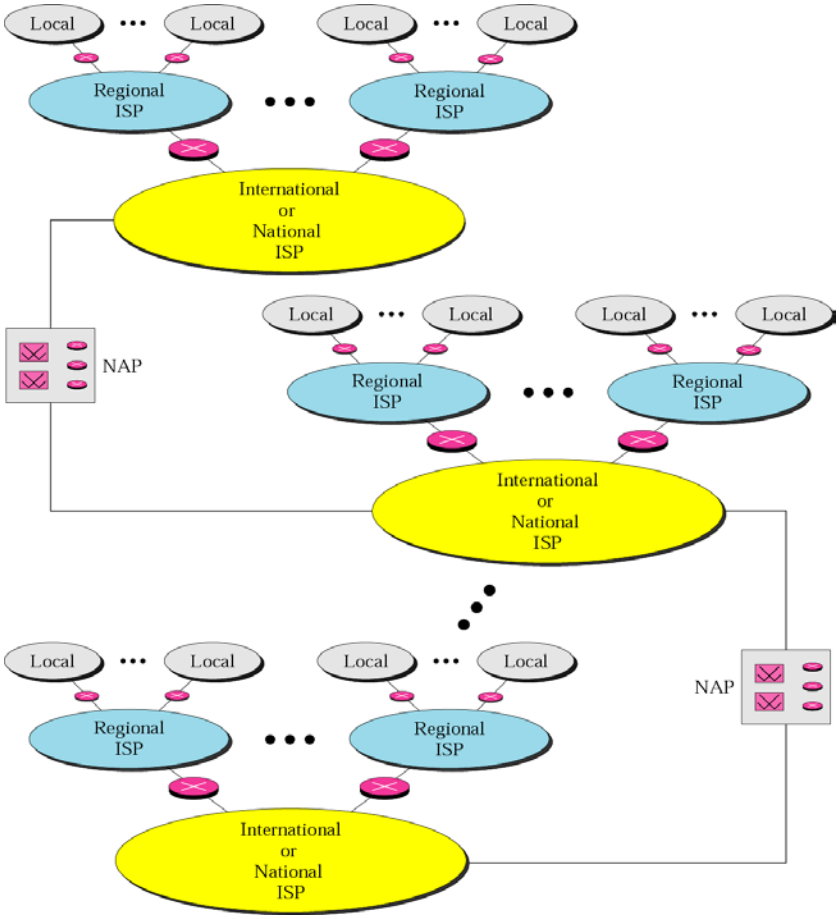
1.1.2 Transmission Control Protocol / Internetworking Protocol (TCP/IP)

Η εργασία-ορόσημο των δύο ερευνητών που εκδόθηκε το 1973, περίγραφε τα πρωτόκολλα που θα χρησιμοποιούνταν για την επίτευξη της διανομής των δεδομένων. Επρόκειτο για μία νέα έκδοση του NCP (Network Control Protocol). Αυτή η εργασία για το πρωτόκολλο ελέγχου μετάδοσης Transmission Control Protocol (TCP) περιλάμβανε έννοιες όπως συμπύκνωση, διάγραμμα δεδομένων και λειτουργίες της θύρας εξόδου. Μία ριζοσπαστική ιδέα ήταν η μεταφορά της ευθύνης για τη διόρθωση των λαθών από το IMP (interface message processor) στον κεντρικό υπολογιστή. Αυτό το ARPA (Advanced Research Projects Agency) Internet έγινε η εστία όλης της προσπάθειας για την επίτευξη της επικοινωνίας. Εκείνη την εποχή, η

ευθύνη για το ARPANET εκχωρήθηκε στην υπηρεσία επικοινωνίας και άμυνας (Defence Communication Agency). Τον Οκτώβριο του 1977 παρουσιάστηκε με επιτυχία ένα διαδίκτυο που αποτελούταν από τρία διαφορετικά δίκτυα (ARPANET, ραδιοφωνικό δίκτυο και δορυφορικό δίκτυο). Η επικοινωνία μεταξύ δικτύων κατέστη δυνατή.
Λίγο αργότερα, οι αρχές αποφάσισαν να διαχωρίσουν το TCP σε δύο πρωτόκολλα: Transmission Control Protocol (TCP) και Internetworking Protocol (IP). Το IP θα διαχειριζόταν τα διαγράμματα δεδομένων και το TCP θα ήταν υπεύθυνο για τις λειτουργίες υψηλότερου επιπέδου, όπως την κατάτμηση, την ανασυγκρότηση και την ανίχνευση σφαλμάτων. Το διαδικτυακό πρωτόκολλο ονομάστηκε TCP/IP.
Το 1981, μετά από μία σύμβαση DARPA, το Πανεπιστήμιο του Μπέρκλεϋ τροποποίησε το λειτουργικό σύστημα UNIX ώστε να συμπεριλαμβάνει το TCP/IP. Αυτή η προσθήκη λογισμικού δικτύου σε ένα δημοφιλές λειτουργικό σύστημα συντέλεσε τα μέγιστα στην περαιτέρω εξάπλωση των δικτύων. Η ανοιχτή (όχι δηλαδή η περιορισμένη από τον κατασκευαστή) υλοποίηση στο UNIX πρόσφερε σε κάθε κατασκευαστή ένα βασικό λειτουργικό κώδικα, επί του οποίου θα μπορούσαν να αναπτύξουν τα προϊόντα τους.
Το 1983, οι αρχές κατήργησαν τα αρχικά πρωτόκολλα ARPANET και το TCP/IP έγινε το επίσημο πρωτόκολλο για το ARPANET. Αυτοί που ήθελαν να χρησιμοποιήσουν το Internet για να προσπελαύνουν ένα διαφορετικό δίκτυο, έπρεπε να εκτελούν το TCP/IP.

1.1.3 Το Internet σήμερα

Το Internet σήμερα δεν είναι μία ιεραρχική δομή. Αποτελείται από πολλά μεγάλα και από πολλά τοπικά δίκτυα που συνδέονται μέσω συσκευών και σταθμών διακλάδωσης. Είναι δύσκολο να αποδώσουμε μία ακριβή αναπαράσταση του Internet επειδή αλλάζει διαρκώς -νέα δίκτυα προτίθενται, τα υπάρχοντα χρειάζονται περισσότερες διευθύνσεις και τα δίκτυα μη λειτουργουσών εταιριών πρέπει να απομακρύνονται. Σήμερα, οι περισσότεροι τελικοί χρήστες που θέλουν σύνδεση με το Internet, χρησιμοποιούν τις υπηρεσίες εταιριών παροχής Internet (ISP). Υπάρχουν διεθνείς εταιρίες, εθνικοί φορείς, περιφερειακοί φορείς και τοπικοί φορείς. Το Internet σήμερα διαχειρίζεται από ιδιωτικές εταιρίες και όχι από κυβερνητικούς φορείς. **Στην εικόνα παρακάτω** μπορούμε να δούμε μία θεμελιώδη, αν και όχι γεωγραφική, άποψη του Internet.



Το Internet σήμερα

Διεθνείς ISP

Στην κορυφή της ιεραρχίας βρίσκονται οι διεθνείς ISP που συνδέουν τα κράτη μεταξύ τους.

Εθνικοί ISP

Οι εθνικοί ISP είναι σπονδυλικά δίκτυα που δημιουργούνται και διατηρούνται από εξειδικευμένες εταιρίες. Για να παρέχουν σύνδεση μεταξύ των τελικών χρηστών, αυτά τα σπονδυλικά δίκτυα συνδέονται με σύνθετους σταθμούς διακλάδωσης (που συνήθως τους διαχειρίζονται τρίτοι), οι οποίοι ονομάζονται σημεία προσπέλασης δικτύου (network access points, NAP). Μερικά δίκτυα εθνικών ISP συνδέονται μεταξύ τους και με ιδιωτικούς σταθμούς διακλάδωσης που ονομάζονται ομότιμα σημεία (peering points). Οι εθνικοί ISP λειτουργούν σε υψηλές ταχύτητες μετάδοσης δεδομένων (έως 600 Mbps).

Περιφερειακοί ISP

Οι περιφερειακοί ISP είναι μικροί ISP που συνδέονται με έναν ή περισσότερους εθνικούς ISP. Βρίσκονται στο τρίτο επίπεδο της ιεραρχίας, με μικρότερες ταχύτητες μετάδοσης δεδομένων.

Τοπικοί ISP

Οι τοπικοί ISP παρέχουν απευθείας υπηρεσίες στους τελικούς χρήστες. Οι τοπικοί ISP μπορούν να συνδέονται με τους περιφερειακούς ISP ή απευθείας με τους εθνικούς ISP. Οι περισσότεροι τελικοί χρήστες συνδέονται με τοπικούς ISP. Σημειώνουμε ότι υπό αυτή την έννοια, ένας τοπικός ISP μπορεί να είναι μία εταιρία που απλά παρέχει υπηρεσίες Internet, μία εταιρία που διαθέτει δίκτυο για να παρέχει υπηρεσίες στους δικούς της υπαλλήλους ή ένα μη κερδοσκοπικό οργανισμό, όπως ένα πανεπιστήμιο, το οποίο λειτουργεί το δικό του δίκτυο. Κάθε ένας από τους παραπάνω φορείς μπορεί να συνδέεται με έναν περιφερειακό ή εθνικό ISP.

1.1.4 Ανάπτυξη του Internet

Το Internet έχει αναπτυχθεί τρομακτικά. Μόλις σε λίγες δεκαετίες, ο αριθμός των δικτύων αυξήθηκε από δεκάδες σε εκατοντάδες. Παράλληλα, ο αριθμός των υπολογιστών που συνδέονται με το Internet έχει αυξηθεί από εκατοντάδες σε εκατοντάδες εκατομμύρια. Το Internet εξακολουθεί να αυξάνεται. Οι παράγοντες που επηρεάζουν αυτήν την αύξηση είναι μεταξύ άλλων οι εξής:

- **Νέα πρωτόκολλα.** Νέα πρωτόκολλα πρέπει να προστεθούν και απαρχαιωμένα πρωτόκολλα πρέπει να απομακρυνθούν. Για παράδειγμα, έχει εγκριθεί ως βασικό πρωτόκολλο ένα πρωτόκολλο που είναι σαφώς ανώτερο του IPv4, το οποίο όμως δεν έχει ακόμα υλοποιηθεί πλήρως.
- **Νέες τεχνολογίες.** Αναπτύσσονται νέες τεχνολογίες που θα αυξήσουν τη χωρητικότητα των δικτύων και θα παρέχουν μεγαλύτερο εύρος ζώνης στους χρήστες του Internet.
- **Αυξανόμενη χρήση των πολυμέσων.** Προβλέπεται ότι το Internet, που κάποτε ήταν απλώς ένα μέσο με το οποίο διάφοροι φορείς μοιράζονταν δεδομένα, θα χρησιμοποιείται όλο και περισσότερο για πολυμέσα (ήχος και εικόνα).

1.2 ΠΡΩΤΟΚΟΛΛΑ ΚΑΙ ΠΡΟΤΥΠΑ

Σε αυτήν την ενότητα θα ορίσουμε δύο ευρέως χρησιμοποιημένους όρους: πρωτόκολλα και πρότυπα. Πρώτα θα ορίσουμε τον όρο πρωτόκολλο, ο οποίος είναι συνώνυμος του <<κανόνα>>. Μετά θα συζητήσουμε για τα πρότυπα, τα οποία είναι σύμφωνα με τους κανόνες.

Πρωτόκολλα

Στα δίκτυα υπολογιστών, η επικοινωνία συμβαίνει μεταξύ οντοτήτων σε διαφορετικά συστήματα. Μία οντότητα είναι οτιδήποτε είναι ικανό να στέλνει ή να λαμβάνει πληροφορίες. Δύο οντότητες όμως δεν μπορούν απλά να στέλνουν bit πληροφοριών η μία στην άλλη και να περιμένουν ότι έτσι απλά θα γίνουν κατανοητές. Για να επιτευχθεί η επικοινωνία, οι οντότητες πρέπει να συμφωνήσουν σε ένα πρωτόκολλο. Ένα πρωτόκολλο είναι ένα σύνολο κανόνων που διαχειρίζεται την επικοινωνία δεδομένων. Ένα πρωτόκολλο ορίζει τις πληροφορίες που μεταφέρονται, τον τρόπο που μεταφέρονται και το πότε μεταφέρονται. Τα σημαντικά στοιχεία ενός πρωτοκόλλου είναι το συντακτικό, η σημασιολογία και ο χρονισμός.

- **Συντακτικό.** Το συντακτικό αναφέρεται στη δομή ή τη μορφή των δεδομένων, στη σειρά δηλαδή με την οποία αναφέρονται. Για παράδειγμα, ένα απλό πρωτόκολλο μπορεί να αναμένει τα πρώτα 8 bits δεδομένων να είναι η διεύθυνση του αποστολέα, τα δεύτερα 8 η διεύθυνση του παραλήπτη και το υπόλοιπο της ροής να είναι το μήνυμα.
- **Σημασιολογία.** Η σημασιολογία αναφέρεται στη σημασία κάθε τμήματος bits. Δηλαδή τον τρόπο με τον οποίο ερμηνεύεται ένα συγκεκριμένο μοτίβο και τις ενέργειες που θα γίνουν βάσει αυτής της ερμηνείας. Για παράδειγμα, μία διεύθυνση αναγνωρίζει τη διαδρομή που πρέπει να γίνει ή τον τελικό προορισμό του μηνύματος ;
- **Χρονισμός.** Ο χρονισμός αναφέρεται σε δύο χαρακτηριστικά: πότε πρέπει να στέλνονται τα δεδομένα και πόσο γρήγορα μπορούν να σταλούν. Για παράδειγμα, αν ο αποστολέας παράγει δεδομένα με ρυθμό 100 Mbps αλλά ο παραλήπτης μπορεί να επεξεργαστεί δεδομένα με ρυθμό μόλις 1 Mbps, η μετάδοση θα υπερφορτώσει τον παραλήπτη και τα δεδομένα κατά ένα μεγάλο μέρος θα χαθούν.

Πρότυπα

Τα πρότυπα είναι απαραίτητα στη δημιουργία και διατήρηση μίας ανοιχτής και ανταγωνιστικής αγοράς για κατασκευαστές εξοπλισμού και στην εγγύηση της εθνικής και διεθνούς διαλειτουργικότητας δεδομένων και τεχνολογίας και διαδικασιών τηλεπικοινωνιών. Παρέχουν κατευθυντήριες γραμμές στους κατασκευαστές, στους πωλητές, στους κυβερνητικούς φορείς και σε άλλους φορείς παροχής υπηρεσιών, ώστε να εξασφαλίζεται το είδος

της απαραίτητης διασύνδεσης στις σημερινές αγορές και στις διεθνείς επικοινωνίες. Τα πρότυπα της επικοινωνίας δεδομένων ταξινομούνται σε δύο κατηγορίες: de facto (δηλαδή <<εξ των πραγμάτων>>, ή <<πραγματικός >>) και de jure (δηλαδή <<εκ νόμου>>, ή <<βάσει κανόνα>>).

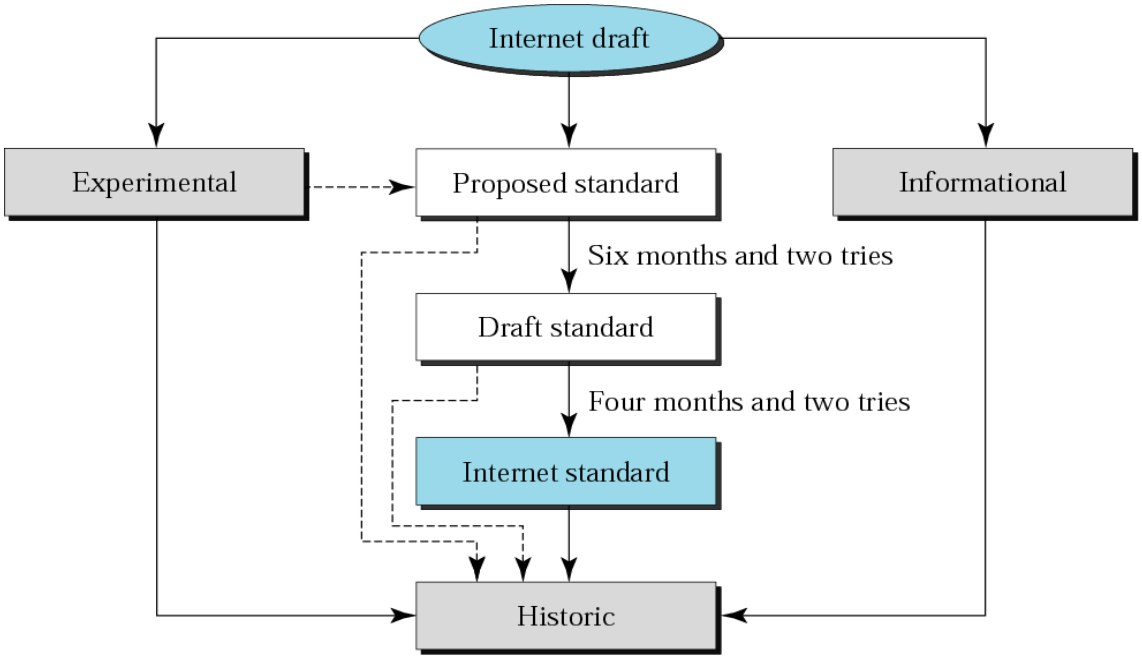
- **De facto**. Τα πρότυπα που δεν έχουν εγκριθεί από κάποιον οργανωμένο φορέα αλλά έχουν υιοθετηθεί ως πρότυπα μέσω ευρείας χρήσης είναι τα εκ των πραγμάτων (de facto) πρότυπα. Αυτά τα πρότυπα συχνά εγκαινιάζονται από κατασκευαστές που επιθυμούν να ορίσουν τις λειτουργίες ενός νέου προϊόντος ή μίας νέας τεχνολογίας.
- **De jure.** Τα πρότυπα εκ νόμου (de jure) που έχουν θεσμοθετηθεί από κάποιον επίσημο, αναγνωρισμένο φορέα.

1.3 ΠΡΟΤΥΠΑ ΤΟΥ INTERNET

Ένα πρότυπο του Internet είναι μία διεξοδικά ελεγμένη προδιαγραφή που είναι χρήσιμη και εφαρμόζεται από όσους ασχολούνται με το Internet. Είναι ένας μορφοποιημένος κανονισμός που πρέπει να ακολουθείται. Υπάρχει μία αυστηρή διαδικασία, βάσει της οποίας μία προδιαγραφή καθίσταται πρότυπο του Internet. Ένα σχέδιο του Internet είναι ένα έγγραφο εργασίας (μία εργασία σε εξέλιξη) με κανένα επίσημο κύρος και με διάρκεια ζωής έξι μήνες. Αφού αποκτήσει σύσταση από τις αρχές του Internet, ένα πρόχειρο μπορεί να εκδοθεί ως αίτημα για σχόλιο. Κάθε τέτοιο αίτημα τυγχάνει επεξεργασίας, του εκχωρείται ένας αριθμός και καθίσταται διαθέσιμο σε όλα τα ενδιαφερόμενα μέρη.
Τα αιτήματα περνάνε από επίπεδα ωριμότητας και κατηγοριοποιούνται σύμφωνα με το δικό τους επίπεδο απαίτησης.

1.3.1 Επίπεδα ωριμότητας

Ένα αίτημα, κατά τη διάρκεια της ζωής του περνάει από έξι επίπεδα ωριμότητας : προτεινόμενο πρότυπο, πρόχειρο πρότυπο, πρότυπο Internet, ιστορικό, πειραματικό και πληροφοριακό (**δείτε την εικόνα παρακάτω**).



Επίπεδα ωριμότητας ενός αιτήματος για σχόλιο

Προτεινόμενο πρότυπο

Ένα προτεινόμενο πρότυπο είναι μία προδιαγραφή που είναι σταθερή, κατανοητή και αφορά πολλούς χρήστες του Internet. Σε αυτό το επίπεδο, η προδιαγραφή συνήθως ελέγχεται και υλοποιείται από αρκετές διαφορετικές ομάδες.

Πρόχειρο πρότυπο

Ένα προτεινόμενο πρότυπο προάγεται σε πρόχειρο πρότυπο μετά από τουλάχιστον δύο επιτυχείς, ανεξάρτητες και διαλειτουργικές υλοποιήσεις. Παρά τις δυσκολίες, ένα πρόχειρο πρότυπο, με κάποιες τροποποιήσεις αν παρουσιαστούν συγκεκριμένα προβλήματα, φυσιολογικά γίνεται ένα πρότυπο του Internet.

Πρότυπο του Internet

Ένα πρόχειρο πρότυπο γίνεται πρόχειρο του Internet μετά από επιδείξεις επιτυχούς υλοποίησης.

Ιστορικό

Τα ιστορικά αιτήματα είναι σημαντικά από μία ιστορική άποψη. Είτε έχουν παραγκωνιστεί από νεώτερες προδιαγραφές, είτε ποτέ δεν πέρασαν τα απαραίτητα επίπεδα ωριμότητας για να γίνουν πρότυπα του Internet.

Πειραματικό

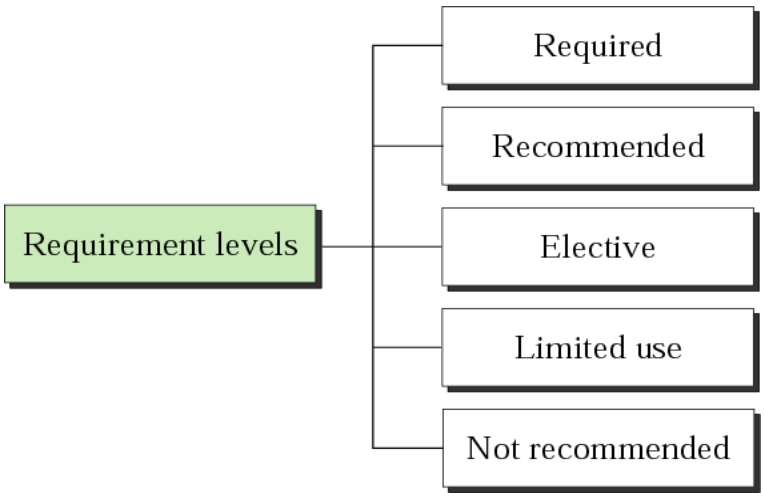
Ένα αίτημα που ονομάζεται πειραματικό περιγράφει την εργασία που σχετίζεται με μία πειραματική κατάσταση που δεν επηρεάζει τη λειτουργία του Internet. Ένα τέτοιο αίτημα δεν θα πρέπει να υλοποιείται σε καμία λειτουργική υπηρεσία του Internet.

Πληροφοριακό

Ένα αίτημα που ονομάζεται πληροφοριακό περιέχει γενικές, ιστορικές ή εκπαιδευτικές πληροφορίες που σχετίζονται με το Internet. Συνήθως συντάσσεται από κάποιον που δεν ανήκει σε οργανισμό που σχετίζεται με το Internet, όπως από έναν έμπορο.

1.3.2 Επίπεδα απαίτησης

Τα αιτήματα χωρίζονται σε πέντε επίπεδα απαίτησης: απαιτούμενο, προτεινόμενο, προαιρετικό, περιορισμένης χρήσης και μη προτεινόμενο (**δείτε την εικόνα παρακάτω**).



Επίπεδα απαίτησης ενός αιτήματος

Απαιτούμενο

Ένα αίτημα ονομάζεται απαιτούμενο αν πρέπει να υλοποιηθεί από όλα τα συστήματα του Internet για να επιτευχθεί η ελάχιστη συμμόρφωση. Για παράδειγμα, τα IP και ICMP είναι απαιτούμενα πρωτόκολλα.

Προτεινόμενο

Ένα αίτημα ονομάζεται προτεινόμενο αν δεν απαιτείται για την ελάχιστη συμμόρφωση και ονομάζεται έτσι χάρη στη χρησιμότητά του. Για παράδειγμα, τα FTP και TELNET είναι προτεινόμενα.

Προαιρετικό

Ένα αίτημα ονομάζεται προαιρετικό αν δεν απαιτείται και δεν προτείνεται. Μπορεί όμως να χρησιμοποιηθεί προς όφελος του υπολογιστή που το χρησιμοποιεί.

Περιορισμένης χρήσης

Ένα αίτημα που ονομάζεται περιορισμένης χρήσης θα πρέπει να χρησιμοποιείται μόνο σε συγκεκριμένες, λίγες περιπτώσεις. Τα περισσότερα πειραματικά αιτήματα ανήκουν σε αυτήν την κατηγορία.

Μη προτεινόμενο

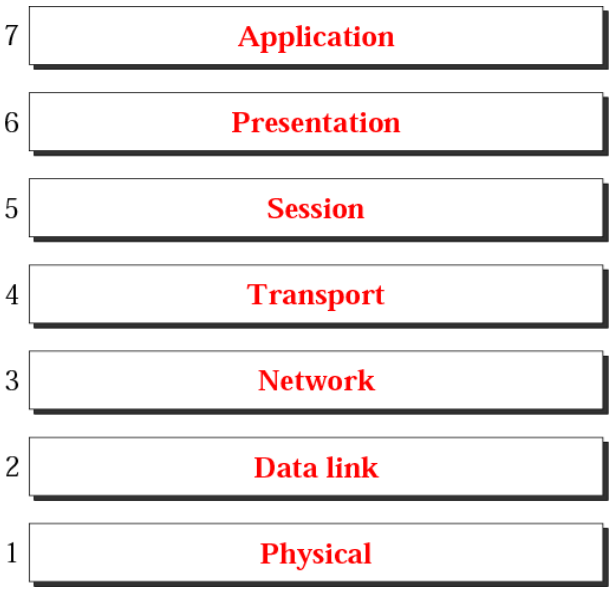
Ένα αίτημα που ονομάζεται μη προτεινόμενο είναι ακατάλληλο για γενική χρήση. Φυσιολογικά σε αυτήν την κατηγορία ανήκουν τα ιστορικά αιτήματα.

2 Το μοντέλο OSI και το πρωτόκολλο TCP/IP

2.1 ΤΟ ΜΟΝΤΕΛΟ OSI

Ο οργανισμός International Standards Organization (ISO) ιδρύθηκε το 1947 και αποτελεί ένα πολυεθνικό σώμα που αφιερώνεται στην παγκόσμια συμφωνία επί των διεθνών προτύπων. Ένα πρότυπο ISO που καλύπτει όλες τις πτυχές των επικοινωνιών δικτύων είναι το μοντέλο Open systems interconnection (OSI). Παρουσιάστηκε πρώτη φορά στα τέλη της δεκαετίας του 1970. Ένα ανοιχτό σύστημα (open system) είναι ένα σύνολο πρωτοκόλλων που επιτρέπει σε δύο διαφορετικά συστήματα να επικοινωνούν ανεξάρτητα από την υποκειμενική αρχιτεκτονική τους. Ο σκοπός του μοντέλου OSI είναι η διευκόλυνση της επικοινωνίας μεταξύ διαφορετικών συστημάτων χωρίς να απαιτούνται αλλαγές στη λογική του υποκείμενου υλικού και λογισμικού. Το μοντέλο OSI δεν είναι πρωτόκολλο αλλά είναι ένα μοντέλο για την κατανόηση και σχεδίαση μίας αρχιτεκτονικής δικτύου που είναι ευέλικτη, στιβαρή και διαλειτουργική. Το ISO είναι ο οργανισμός. Το OSI είναι το μοντέλο.

Το μοντέλο OSI είναι ένα διαστρωματωμένο πλαίσιο εργασίας για τη σχεδίαση συστημάτων δικτύων που επιτρέπει την επικοινωνία μεταξύ όλων των τύπων των υπολογιστικών συστημάτων. Αποτελείται από επτά ξεχωριστά αλλά σχετιζόμενα επίπεδα, κάθε ένα από τα οποία ορίζει ένα μέρος της διαδικασίας μεταφοράς πληροφοριών σε ένα δίκτυο. (**δείτε την εικόνα παρακάτω**)**.** Η κατανόηση των βασικών αρχών του μοντέλου OSI αποτελεί μία στέρεα βάση για την περαιτέρω εξερεύνηση των επικοινωνιών δεδομένων.

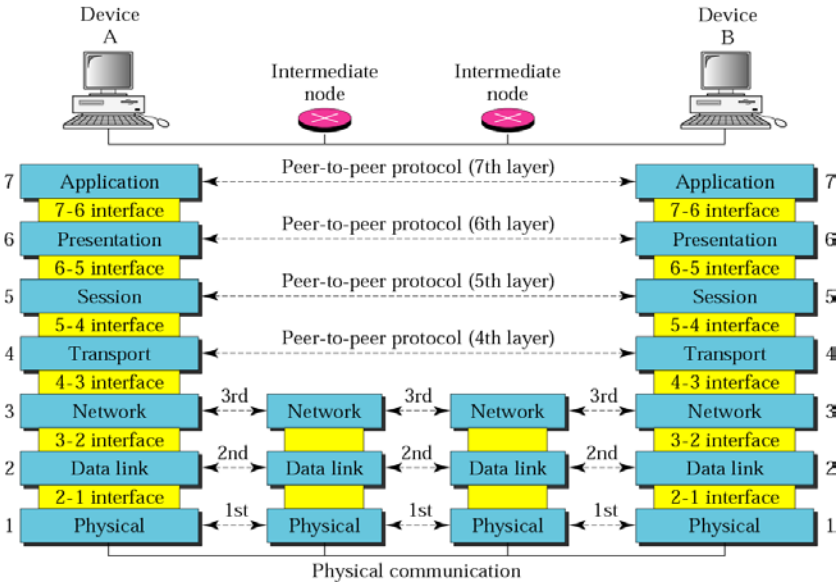


Το μοντέλο OSI

2.1.1 Αρχιτεκτονική σε επίπεδα

Το μοντέλο OSI αποτελείται από επτά διατεταγμένα επίπεδα: φυσικό επίπεδο (επίπεδο 1), σύνδεση δεδομένων (επίπεδο 2), δικτύου (επίπεδο 3), μετάδοσης (επίπεδο 4), συνόδου (επίπεδο 5), παρουσίασης (επίπεδο 6) και εφαρμογής (επίπεδο 7). **Στην εικόνα παρακάτω** μπορούμε να δούμε τα επίπεδα που εμπλέκονται στην αντιμετώπιση ενός μηνύματος που στέλνεται από τη συσκευή Α στη συσκευή Β. Όταν το μήνυμα ταξιδεύει από την Α στη Β, ίσως περάσει μέσα από αρκετούς ενδιάμεσους κόμβους. Αυτοί οι ενδιάμεσοι κόμβοι απασχολούν συνήθως μόνο τα τρία πρώτα επίπεδα του μοντέλου OSI. Κατά την ανάπτυξη του μοντέλου, οι σχεδιαστές διύλισαν τη διαδικασία της μετάδοσης δεδομένων στα πιο θεμελιώδη στοιχεία της. Αναγνώρισαν ποιες λειτουργίες δικτύου είχαν σχετικές χρήσεις και συνέλεξαν αυτές τις λειτουργίες σε διακριτές ομάδες που έγιναν επίπεδα. Κάθε επίπεδο ορίζει μία οικογένεια λειτουργιών διαφορετικών από εκείνες άλλων επιπέδων. Ορίζοντας και περιορίζοντας τις λειτουργίες με αυτόν τον τρόπο, οι σχεδιαστές δημιούργησαν μία αρχιτεκτονική που είναι κατανοητή και ευέλικτη. Το πιο σημαντικό είναι ότι το μοντέλο OSI επιτρέπει πλήρη διαλειτουργικότητα μεταξύ –σε άλλες περιπτώσεις- εντελώς ασύμβατων συστημάτων.
Μέσα σε έναν υπολογιστή, κάθε επίπεδο χρησιμοποιεί τις υπηρεσίες τού ακριβώς από κάτω επιπέδου. Το επίπεδο 3 για παράδειγμα, χρησιμοποιεί τις υπηρεσίες που παρέχονται από το επίπεδο 2 και παρέχει υπηρεσίες στο επίπεδο 4. Μεταξύ υπολογιστών, το επίπεδο χ ενός υπολογιστή επικοινωνεί με το επίπεδο χ άλλου υπολογιστή. Αυτή την επικοινωνία διαχειρίζεται μία προσυμφωνημένη σειρά κανόνων και συμβάσεων που ονομάζεται πρωτόκολλο. Οι διαδικασίες σε κάθε υπολογιστή που επικοινωνεί σε ένα

δεδομένο επίπεδο ονομάζονται ομότιμες διαδικασίες. Η επικοινωνία μεταξύ υπολογιστών είναι κατά συνέπεια μία ομότιμη διαδικασία που χρησιμοποιεί τα κατάλληλα πρωτόκολλα σε ένα δεδομένο επίπεδο.



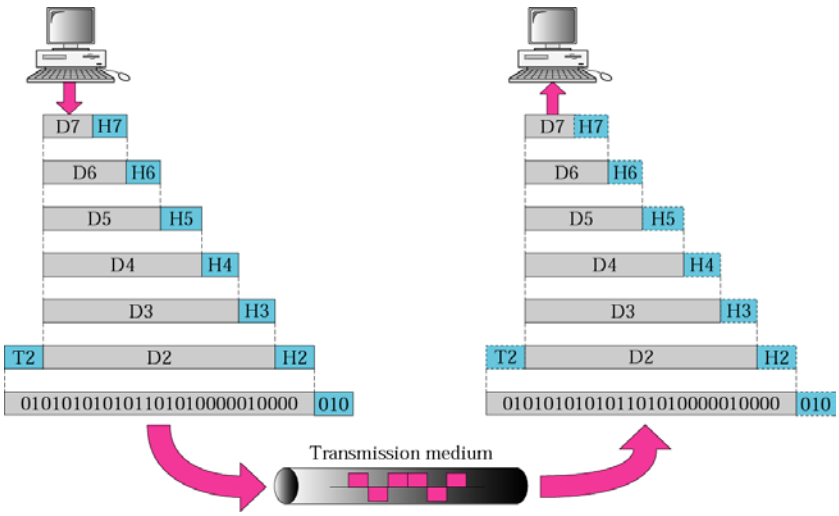
Επίπεδα OSI

2.1.2 Ομότιμες διαδικασίες

Στο φυσικό επίπεδο, η επικοινωνία είναι απευθείας: **στην Εικόνα παραπάνω**, η συσκευή Α στέλνει μία ροή bits στη συσκευή Β (μέσω ενδιάμεσων κόμβων). Σε υψηλότερα επίπεδα όμως, η επικοινωνία πρέπει να κινηθεί προς τα κάτω, μέσω των επιπέδων στη συσκευή Α, προς τη συσκευή Β και μετά προς τα πάνω. Κάθε επίπεδο στη συσκευή που στέλνει τις πληροφορίες προσθέτει τις δικές του πληροφορίες στο μήνυμα που λαμβάνει από το πάνω επίπεδο και περνάει όλο το πακέτο στο κάτω επίπεδο.
Στο επίπεδο 1, όλο το πακέτο μετατρέπεται σε μία φόρμα που μπορεί να μεταφερθεί στη λαμβάνουσα συσκευή. Στη λαμβάνουσα συσκευή, το μήνυμα απαλλάσσεται σε κάθε επίπεδο από τις επιπλέον πληροφορίες που πρόσθεσε κάθε επίπεδο της αποστέλλουσας συσκευής και κάθε διαδικασία λαμβάνει και απομακρύνει τα δεδομένα που προορίζονται για αυτήν. Για παράδειγμα, το επίπεδο 2 αφαιρεί τα δεδομένα που προορίζονται γι΄ αυτό και περνάει τα υπόλοιπα στο επίπεδο 3. Το επίπεδο 3 αφαιρεί με τη σειρά του τα δικά του δεδομένα και περνάει τα υπόλοιπα στο επίπεδο 4 και ούτω καθ΄ εξής.

2.1.3 Διεπαφές μεταξύ επιπέδων

Το πέρασμα των δεδομένων και των πληροφοριών δικτύου μέσω των επιπέδων της αποστέλλουσας συσκευής προς τα κάτω και προς τα πάνω στη λαμβάνουσα συσκευή καθίσταται εφικτό μέσω μίας διεπαφής μεταξύ κάθε ζεύγους γειτονικών επιπέδων. Κάθε διεπαφή ορίζει τις πληροφορίες και τις υπηρεσίες που πρέπει να παρέχει ένα επίπεδο στο από πάνω του επίπεδο. Οι καλά ορισμένες διεπαφές και οι λειτουργίες επιπέδου παρέχουν αρθρωτές δυνατότητες σε ένα δίκτυο. Όσο ένα επίπεδο παρέχει τις αναμενόμενες υπηρεσίες στο από πάνω του επίπεδο, η συγκεκριμένη υλοποίηση των λειτουργιών του μπορεί να τροποποιηθεί ή να αντικατασταθεί χωρίς να απαιτούνται αλλαγές στα γειτονικά επίπεδα. **Στην Εικόνα παρακάτω**, η οποία παρέχει μία συνολική εικόνα των επιπέδων OSI, τα δεδομένα D7 είναι η μονάδα δεδομένων στο επίπεδο 7, τα δεδομένα D6 είναι τα δεδομένα στο επίπεδο 6 και ούτω καθ΄ εξής. Η διαδικασία ξεκινάει στο επίπεδο 7 (το επίπεδο εφαρμογής), και στη συνέχεια κινείται από το ένα επίπεδο στο άλλο σε φθίνουσα σειρά. Σε κάθε επίπεδο, μπορεί να προστεθεί μία κεφαλίδα στη μονάδα των δεδομένων. Στο επίπεδο 2, ίσως προστεθεί και μία ετικέτα με τη μορφή υποσέλιδου. Όταν τα μορφοποιημένα δεδομένα περάσουν από το φυσικό επίπεδο (επίπεδο 1), μετατρέπονται σε ηλεκτρομαγνητικό σήμα και μεταδίδονται μέσω μίας φυσικής ζεύξης. Φτάνοντας στον προορισμό του, το σήμα περνάει στο επίπεδο 1, και μεταφέρεται πίσω με ψηφιακή μορφή. Οι μονάδες δεδομένων μετακινούνται μετά προς τα πάνω μέσω των επιπέδων OSI. Όπως κάθε μπλοκ δεδομένων φτάνει στο επόμενο υψηλότερο επίπεδο, τα πακέτα που έχουν επισυναφθεί σε αυτό από το αντίστοιχο αποστέλλον επίπεδο αφαιρούνται και γίνονται ενέργειες κατάλληλες για το εκάστοτε επίπεδο. Μέχρι να φτάσει στο επίπεδο 7, το μήνυμα έχει πάρει μορφή κατάλληλη για την εφαρμογή και γίνεται διαθέσιμο στον παραλήπτη.



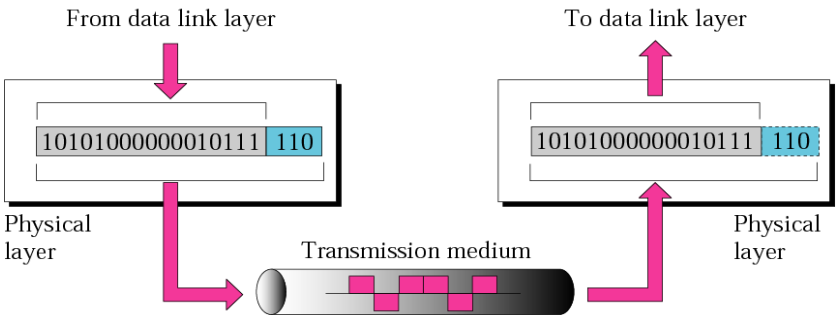
Μία ανταλλαγή με το μοντέλο OSI

2.2 ΤΑ ΕΠΙΠΕΔΑ ΣΤΟ ΜΟΝΤΕΛΟ OSI

Σε αυτήν την ενότητα θα συζητήσουμε εν συντομία τις λειτουργίες κάθε επιπέδου στο μοντέλο OSI.

Φυσικό επίπεδο

Το φυσικό επίπεδο συντονίζει τις λειτουργίες που απαιτούνται για τη μεταφορά μίας ροής bit μέσω ενός φυσικού μέσου. Ασχολείται με τις μηχανικές και ηλεκτρολογικές προδιαγραφές της διεπαφής και του μέσου μετάδοσης. Ορίζει επίσης τις διαδικασίες και τις λειτουργίες που πρέπει να εκτελούν οι φυσικές συσκευές και οι διεπαφές για να επιτευχθεί η μετάδοση. **Η Εικόνα παρακάτω** δείχνει τη θέση του φυσικού επιπέδου σε σχέση με το μέσο μετάδοσης και το επίπεδο σύνδεσης δεδομένων.



Φυσικό επίπεδο

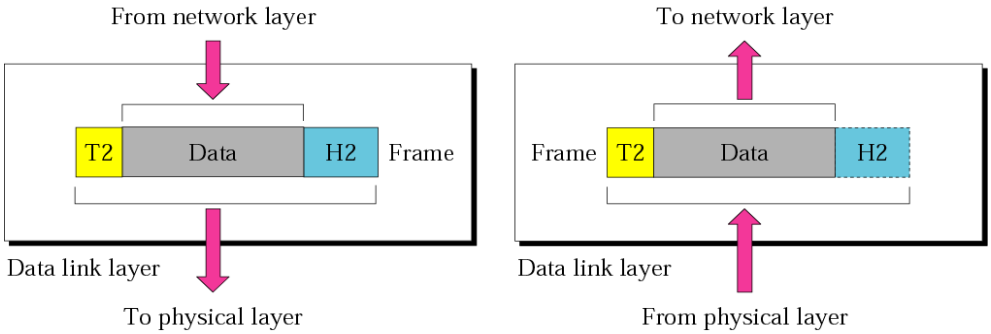
Το φυσικό επίπεδο είναι υπεύθυνο για κινήσεις μεμονωμένων bits από έναν κόμβο στον επόμενο.
Το φυσικό επίπεδο ασχολείται και με τα παρακάτω:

- **Φυσικά χαρακτηριστικά των διεπαφών και των μέσων.** Το φυσικό επίπεδο ορίζει τα χαρακτηριστικά της διεπαφής μεταξύ των συσκευών και του μέσου μετάδοσης. Ορίζει επίσης τον τύπο του μέσου μετάδοσης.
- **Αναπαράσταση των bits.** Τα δεδομένα του φυσικού επιπέδου αποτελούνται από μία ροή bits (ακολουθίες μηδενικών και άσων) χωρίς καμία ερμηνεία. Για να μεταδοθούν τα bits, πρέπει να έχουν κωδικοποιηθεί σε σήματα –ηλεκτρικά ή οπτικά. Το φυσικό επίπεδο ορίζει τον τύπο της κωδικοποίησης (πώς τα μηδενικά και οι άσσοι γίνονται σήματα).
- **Συγχρονισμός των bits.** Ο αποστολέας και ο παραλήπτης όχι απλά πρέπει να χρησιμοποιούν τον ίδιο αριθμό bit αλλά πρέπει επίσης να συγχρονίζονται στο επίπεδο bit. Με άλλα λόγια, πρέπει να συγχρονιστούν τα ρολόγια του αποστολέα και του παραλήπτη.

- **Διαμόρφωση γραμμής.** Το φυσικό επίπεδο ασχολείται με τη σύνδεση των συσκευών με το μέσο. Σε μία ρύθμιση σημείο προς σημείο, δύο συσκευές συνδέονται μέσω μίας αφιερωμένης γραμμής. Σε μία ρύθμιση πολλών σημείων, μία γραμμή χρησιμοποιείται από κοινού από αρκετές συσκευές.
- **Φυσική τοπολογία.** Η φυσική τοπολογία ορίζει το πώς συνδέονται οι συσκευές για να δημιουργήσουν δίκτυο. Οι συσκευές μπορεί να συνδέονται χρησιμοποιώντας τοπολογία πλέγματος (κάθε συσκευή συνδέεται με όλες τις άλλες), τοπολογία αστεριού (οι συσκευές συνδέονται μέσω μίας κεντρικής συσκευής), τοπολογία δακτυλίου (κάθε συσκευή συνδέεται με την επόμενη, σχηματίζοντας έναν δακτύλιο**)** ή τοπολογία δίαυλου (κάθε συσκευή σε μία κοινή γραμμή).
- **Κατάσταση μετάδοσης.** Το φυσικό επίπεδο ορίζει επίσης την κατεύθυνση της μετάδοσης μεταξύ δύο συσκευών: μονή, διπλή κατά το ήμισυ και διπλή. Στην απλή κατάσταση, μόνο μία συσκευή μπορεί να στέλνει και η άλλη μπορεί μόνο να λαμβάνει. Η απλή κατάσταση είναι μία μονόδρομη επικοινωνία. Στη διπλή κατά το ήμισυ κατάσταση, οι δύο συσκευές μπορούν να στέλνουν και να λαμβάνουν αλλά όχι ταυτόχρονα. Σε μία διπλή κατάσταση, μπορούν να στέλνουν και να λαμβάνουν και οι δύο συσκευές ταυτόχρονα.

Επίπεδο σύνδεσης δεδομένων

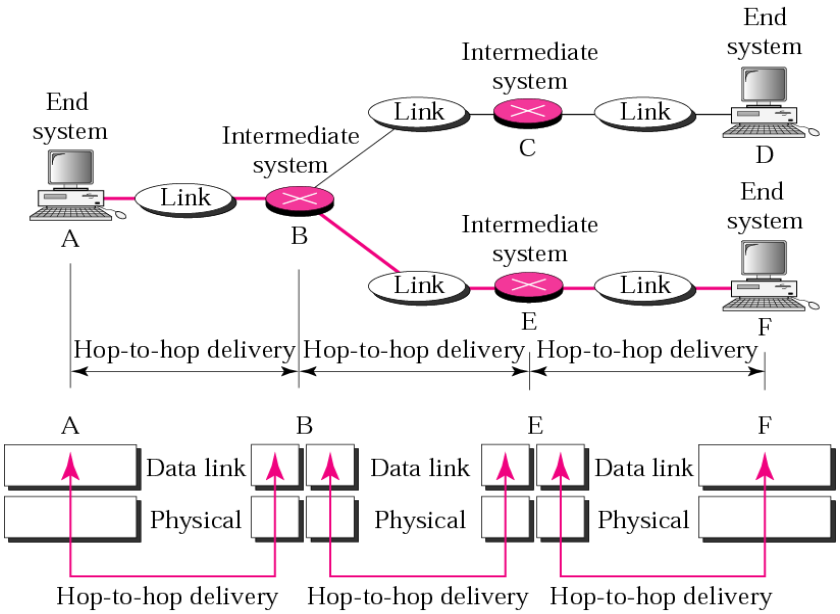
Το επίπεδο σύνδεσης δεδομένων μετατρέπει το φυσικό επίπεδο που κάνει μόνο τη μετάδοση, σε μία αξιόπιστη σύνδεση. Κάνει ό,τι πρέπει για να εμφανίζεται το φυσικό επίπεδο χωρίς λάθη στο ανώτερο επίπεδο (το επίπεδου δικτύου). **Η Εικόνα παρακάτω** δείχνει τη σχέση του επιπέδου σύνδεσης δεδομένων με το φυσικό επίπεδο και το επίπεδο δικτύου.



Επίπεδο σύνδεσης δεδομένων

Το επίπεδο σύνδεσης δεδομένων είναι υπεύθυνο για τη μεταφορά καρέ από έναν κόμβο στον επόμενο.
Άλλοι τομείς ευθύνης του επιπέδου σύνδεσης δεδομένων είναι οι εξής:

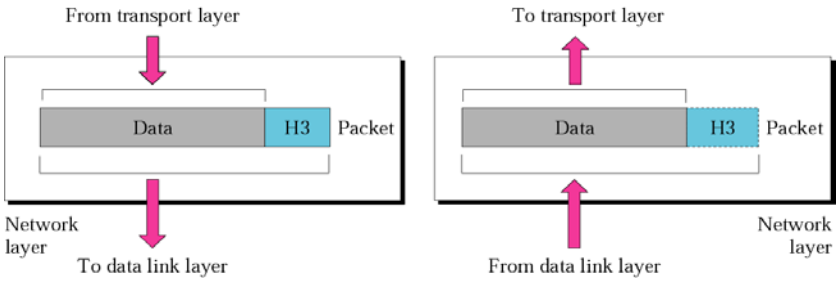
- **Δημιουργία πλαισίων.** Το επίπεδο σύνδεσης δεδομένων χωρίζει τη ροή των bits που λαμβάνονται από το επίπεδο δικτύου σε διαχειρίσιμες μονάδες δεδομένων που ονομάζονται πλαίσια.
- **Φυσική διευθυνσιοδότηση.** Αν τα πλαίσια πρέπει να κατανεμηθούν σε διαφορετικά συστήματα στο δίκτυο, το επίπεδο σύνδεσης δεδομένων προσθέτει μία κεφαλίδα στο πλαίσιο για να ορίζει τον αποστολέα και τον παραλήπτη του πλαισίου. Αν το πλαίσιο προοριζόταν για κάποιον υπολογιστή έξω από το δίκτυο του αποστολέα, η διεύθυνση του παραλήπτη είναι η διεύθυνση της συσκευής που συνδέει το δίκτυο με το επόμενο.
- **Έλεγχος ροής.** Αν ο ρυθμός με τον οποίο απορροφώνται τα δεδομένα από τον παραλήπτη είναι μικρότερος από τον ρυθμό που παράγονται από τον αποστολέα, το επίπεδο σύνδεσης δεδομένων επιβάλλει ένα μηχανισμό ελέγχου ροής για να αποτραπεί η υπερφόρτωση του παραλήπτη.
- **Έλεγχος λαθών.** Το επίπεδο σύνδεσης δεδομένων προσθέτει αξιοπιστία στο φυσικό επίπεδο προσθέτοντας μηχανισμούς ανίχνευσης και αναμετάδοσης κατεστραμμένων ή χαμένων πλαισίων. Χρησιμοποιεί επίσης ένα μηχανισμό που αναγνωρίζει τα διπλά πλαίσια. Ο έλεγχος λαθών επιτυγχάνεται συνήθως μέσω μίας πληροφορίας υποσέλιδου που προστίθεται στο τέλος του πλαισίου.
- **Έλεγχος πρόσβασης.** Όταν δύο ή περισσότερες συσκευές συνδέονται στην ίδια γραμμή, τα πρωτόκολλα του επιπέδου σύνδεσης δεδομένων είναι απαραίτητα για να καθοριστεί η συσκευή που έχει έλεγχο επί της γραμμής κάποια συγκεκριμένη στιγμή. **Η Εικόνα παρακάτω** δείχνει τη διανομή από κόμβο σε κόμβο που εκτελεί το επίπεδο σύνδεσης δεδομένων.



Διανομή από κόμβο σε κόμβο

Επίπεδο δικτύου

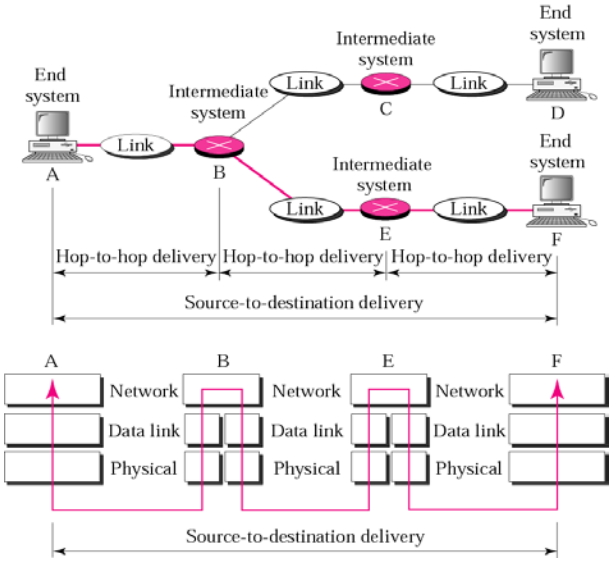
Το επίπεδο δικτύου είναι υπεύθυνο για τη διανομή από την πηγή στον προορισμό ενός πακέτου, πιθανότατα μέσω πολλών δικτύων (γραμμές). Ενώ το επίπεδο σύνδεσης δεδομένων επιβλέπει τη διανομή του πακέτου μεταξύ δύο συστημάτων του ίδιου δικτύου (γραμμές), το επίπεδο δικτύου εξασφαλίζει ότι κάθε πακέτο φτάνει από την πηγή του στον τελικό προορισμό του.
Αν δύο συστήματα είναι συνδεδεμένα στην ίδια γραμμή, συνήθως δεν υπάρχει ανάγκη για το επίπεδο δικτύου. Αν όμως δύο συστήματα επισυνάπτονται σε διαφορετικά δίκτυα με συνδετικές συσκευές μεταξύ των δικτύων, παρουσιάζεται συχνά η ανάγκη ύπαρξης επιπέδου δικτύου για να επιτευχθεί η διανομή από την πηγή στον προορισμό. **Η Εικόνα παρακάτω** δείχνει τη σχέση του επιπέδου δικτύου με τα επίπεδα σύνδεσης δεδομένων και μετάδοσης.



Επίπεδο δικτύου

Άλλες ευθύνες του επιπέδου δικτύου είναι οι εξής:

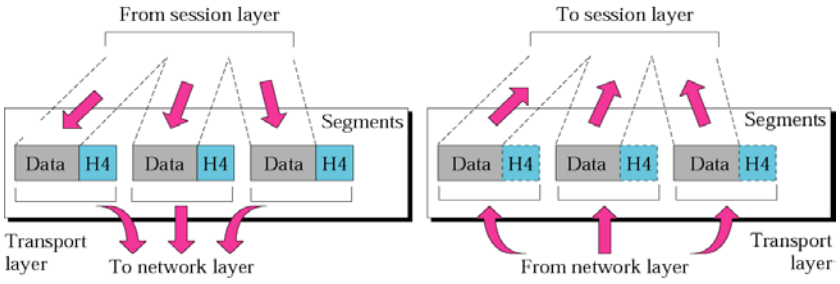
- **Λογική διευθυνσιοδότηση.** Η φυσική διευθυνσιοδότηση που υλοποιείται από το επίπεδο σύνδεσης δεδομένων χειρίζεται το πρόβλημα της διευθυνσιοδότησης τοπικά. Αν ένα πακέτο περάσει τα όρια του δικτύου, χρειαζόμαστε ακόμα ένα σύστημα διευθυνσιοδότησης που θα βοηθά στο διαχωρισμό των συστημάτων πηγής και προορισμού. Το επίπεδο δικτύου προσθέτει μία κεφαλίδα στο πακέτο που έρχεται από το ανώτερο επίπεδο, το οποίο, μεταξύ άλλων, περιέχει τις λογικές διευθύνσεις του αποστολέα και του παραλήπτη.
- **Δρομολόγηση.** Όταν συνδέονται ανεξάρτητα δίκτυα ή συνδέσεις για να δημιουργηθούν διαδίκτυα ή ένα μεγάλο δίκτυο, οι συνδετικές συσκευές (ονομάζονται δρομολογητές ή διακλαδωτές) δρομολογούν ή διακλαδώνουν τα πακέτα προς τον τελικό προορισμό τους. Μία από τις λειτουργίες του επιπέδου δικτύου είναι η παροχή αυτού του μηχανισμού. **Στην Εικόνα παρακάτω** μπορούμε να δούμε τη διανομή από άκρο σε άκρο που εκτελεί το επίπεδο δικτύου.



Διανομή από την πηγή στον προορισμό

Επίπεδο μετάδοσης

Το επίπεδο μετάδοσης είναι υπεύθυνο για τη διανομή από επεξεργασία σε επεξεργασία όλου του μηνύματος. Η διαδικασία είναι μία εφαρμογή που εκτελείται στον κεντρικό υπολογιστή. Ενώ το επίπεδο δικτύου επιβλέπει τη διανομή από την πηγή στον προορισμό μεμονωμένων πακέτων, δεν αναγνωρίζει καμία σχέση μεταξύ αυτών των πακέτων. Μεταχειρίζεται κάθε ένα ξεχωριστά, σαν κάθε πακέτο να ανήκει σε διαφορετικό μήνυμα, είτε αυτό συμβαίνει είτε όχι. Το επίπεδο μετάδοσης από την άλλη πλευρά, εξασφαλίζει ότι όλο το μήνυμα φτάνει ανέπαφο και στη σωστή σειρά, επιβλέποντας τον έλεγχο λαθών και τον έλεγχο ροής στο επίπεδο από την πηγή προς τον προορισμό. **Στην Εικόνα παρακάτω** βλέπουμε τη σχέση του επιπέδου μετάδοσης στα επίπεδα δικτύου και συνόδου.



Επίπεδο μετάδοσης

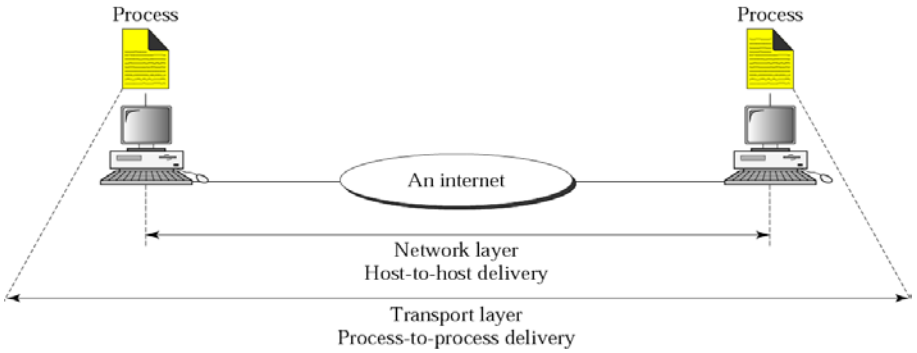
Άλλες ευθύνες του επιπέδου μετάδοσης είναι οι παρακάτω:

- **Διευθυνσιοδότηση σημείου εξυπηρέτησης.** Οι υπολογιστές συχνά εκτελούν πολλά προγράμματα ταυτόχρονα. Γι' αυτό το λόγο η διανομή από

την πηγή στον προορισμό σημαίνει διανομή όχι μόνο από έναν υπολογιστή στον επόμενο αλλά και από μία συγκεκριμένη διαδικασία σε έναν υπολογιστή και από μία άλλη συγκεκριμένη διαδικασία στον άλλο υπολογιστή. Η κεφαλίδα του επιπέδου μετάδοσης πρέπει επομένως να συμπεριλαμβάνει ένα είδος διεύθυνσης που ονομάζεται διεύθυνση σημείου εξυπηρέτησης (ή διεύθυνση θύρας). Το επίπεδο δικτύου μεταφέρει κάθε πακέτο στο σωστό υπολογιστή και το επίπεδο μετάδοσης μεταφέρει όλο το μήνυμα στη σωστή διαδικασία στον εν λόγω υπολογιστή.

- **Κατάτμηση και ανασύσταση.** Ένα μήνυμα χωρίζεται σε μεταδιδόμενα τμήματα –κάθε τμήμα περιέχει έναν αριθμό σειράς. Αυτοί οι αριθμοί δίνουν τη δυνατότητα στο επίπεδο μετάδοσης να ανασυστήσει το μήνυμα σωστά κατά την άφιξή του στον προορισμό και να αναγνωρίσει και αντικαταστήσει τα πακέτα που χάθηκαν κατά τη μετάδοση.
- **Έλεγχος σύνδεσης.** Το επίπεδο μετάδοσης μπορεί να είναι ασύνδετο ή συνδεδεμένο. Ένα ασύνδετο επίπεδο μετάδοσης μεταχειρίζεται κάθε τμήμα ως ανεξάρτητο πακέτο και το διανέμει στο επίπεδο μετάδοσης στον προορισμό. Ένα συνδεδεμένο επίπεδο μετάδοσης πραγματοποιεί μία σύνδεση με το επίπεδο μετάδοσης στον προορισμό πρώτα, πριν παραδώσει τα πακέτα. Μετά τη μεταφορά όλων των δεδομένων, η σύνδεση κλείνει.
- **Έλεγχος ροής.** Όπως το επίπεδο σύνδεσης δεδομένων, έτσι και το επίπεδο μετάδοσης είναι υπεύθυνο για τον έλεγχο ροής. Ο έλεγχος ροής ωστόσο σε αυτό το επίπεδο εκτελείται από άκρο σε άκρο και όχι επί μίας απλής σύνδεσης.
- **Έλεγχος λαθών.** Όπως το επίπεδο σύνδεσης δεδομένων, έτσι και το επίπεδο μετάδοσης είναι υπεύθυνο για τον έλεγχο λαθών. Ο έλεγχος λαθών ωστόσο σε αυτό το επίπεδο εκτελείται από διαδικασία σε διαδικασία και όχι επί μίας απλής σύνδεσης. Το επίπεδο μετάδοσης που στέλνει, εξασφαλίζει ότι όλο το μήνυμα φτάνει στο επίπεδο μετάδοσης που λαμβάνει, χωρίς λάθος (καταστροφή, απώλεια ή επανάληψη). Η διόρθωση λαθών επιτυγχάνεται συνήθως μέσω αναμετάδοσης.

Η Εικόνα παρακάτω παρουσιάζει τη διανομή από επεξεργασία σε επεξεργασία από το επίπεδο μετάδοσης.



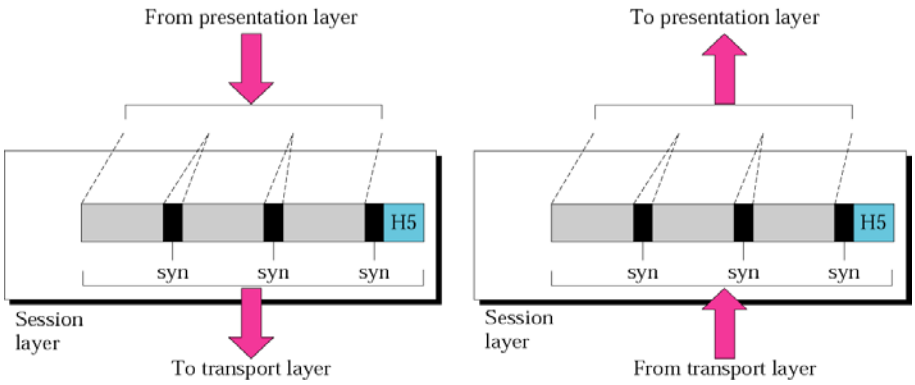
Αξιόπιστη διανομή από επεξεργασία σε επεξεργασία ενός μηνύματος

Επίπεδο συνόδου

Οι υπηρεσίες που παρέχονται από τα τρία πρώτα επίπεδα (φυσικό, σύνδεσης δεδομένων και δικτύου) δεν είναι επαρκείς για κάποιες επεξεργασίες. Το επίπεδο συνόδου είναι ο ελεγκτής επικοινωνίας του δικτύου. Εγκαθιστά, διατηρεί και συγχρονίζει την επικοινωνία μεταξύ των συστημάτων που επικοινωνούν.
Μεταξύ των ευθυνών του επιπέδου συνόδου είναι τα εξής:

- **Έλεγχος επικοινωνίας.** Το επίπεδο συνόδου επιτρέπει σε δύο συστήματα να εισέλθουν σε σύνοδο. Επιτρέπει την επικοινωνία μεταξύ δύο διαδικασιών, μονόδρομα ή αμφίδρομα.
- **Συγχρονισμός.** Το επίπεδο συνόδου επιτρέπει σε μία διαδικασία να προσθέτει σημεία ελέγχου (σημεία συγχρονισμού) στη ροή δεδομένων. Για παράδειγμα, αν ένα σύστημα στέλνει ένα αρχείο 2000 σελίδων, προτείνεται η εισαγωγή σημείων ελέγχου κάθε 100 σελίδες για να εξασφαλιστεί ότι κάθε μονάδα 100 σελίδων λαμβάνεται και επιβεβαιώνεται ανεξάρτητα. Σε αυτήν την περίπτωση, αν παρουσιαστεί διακοπή κατά τη μετάδοση της σελίδας 523, οι σελίδες που θα πρέπει να σταλούν ξανά μετά την αποκατάσταση της επικοινωνίας είναι μόνο οι σελίδες 501 ως 523. Οι σελίδες πριν την 501 δεν χρειάζεται να σταλούν ξανά. **Στην Εικόνα παρακάτω** μπορούμε να δούμε τη σχέση του επιπέδου συνόδου με τα επίπεδα μετάδοσης και παρουσίασης.

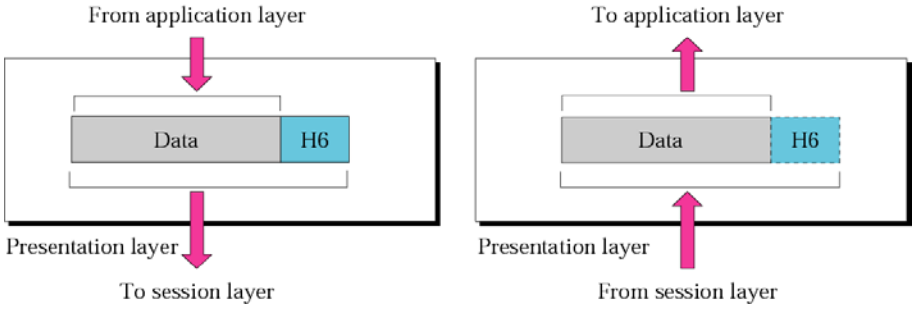
Το επίπεδο συνόδου είναι υπεύθυνο για τον έλεγχο επικοινωνίας και συγχρονισμού.



Επίπεδο συνόδου

Επίπεδο παρουσίασης.

Το επίπεδο παρουσίασης ασχολείται με το συντακτικό και τη σημασιολογία των πληροφοριών που ανταλλάσσονται μεταξύ δύο συστημάτων. **Η Εικόνα παρακάτω** δείχνει τη σχέση μεταξύ του επιπέδου παρουσίασης και των επιπέδων εφαρμογής και συνόδου.



Επίπεδο παρουσίασης

Μεταξύ των ευθυνών του επιπέδου παρουσίασης είναι τα εξής:

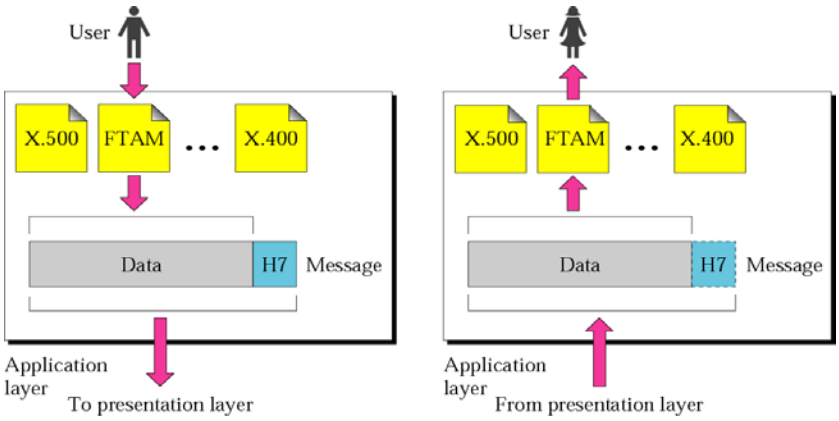
- **Μετάφραση.** Οι διαδικασίες (τα υπό εκτέλεση προγράμματα) σε δύο συστήματα ανταλλάσσουν πληροφορίες υπό τη μορφή συμβολοσειρών χαρακτήρων, αριθμών και άλλων στοιχείων. Οι πληροφορίες θα πρέπει να μετατρέπονται σε ροές bits πριν μεταδοθούν. Επειδή οι διάφοροι υπολογιστές χρησιμοποιούν διάφορα συστήματα κωδικοποίησης, το επίπεδο παρουσίασης είναι υπεύθυνο για τη διαλειτουργικότητα μεταξύ αυτών των διαφορετικών μεθόδων κωδικοποίησης. Το επίπεδο παρουσίασης στον αποστολέα αλλάζει τις πληροφορίες από τη μορφή που καθορίζει ο αποστολέας σε μία κοινή μορφή. Το επίπεδο παρουσίασης στην λαμβάνουσα μηχανή αλλάζει την κοινή μορφή στη μορφή που είναι συμβατή με το δέκτη.
- **Κρυπτογράφηση.** Για να μεταφερθούν ευαίσθητες πληροφορίες μέσω ενός συστήματος, αυτό πρέπει να εξασφαλίζει τη μυστικότητα. Η κρυπτογράφηση σημαίνει ότι ο αποστολέας μεταφέρει τις αρχικές πληροφορίες σε άλλη μορφή και στέλνει το προκύπτον μήνυμα στο δίκτυο. Η αποκρυπτογράφηση αντιστρέφει την αρχική διαδικασία για να επαναφέρει το μήνυμα στην αρχική του μορφή.
- **Συμπίεση.** Η συμπίεση δεδομένων μειώνει τον αριθμό των bits που περιέχονται στις πληροφορίες. Η συμπίεση δεδομένων γίνεται ιδιαίτερα σημαντική στη μετάδοση πολυμέσων όπως κείμενο, ήχο και βίντεο.

Επίπεδο εφαρμογής

Το επίπεδο εφαρμογής δίνει τη δυνατότητα στο χρήστη, είτε είναι άνθρωπος είτε είναι πρόγραμμα, να προσπελαύνει το δίκτυο. Παρέχει διεπαφές χρήστη και υποστήριξη για υπηρεσίες όπως ηλεκτρονική αλληλογραφία, προσπέλαση και μεταφορά αρχείων εξ αποστάσεως, από κοινού διαχείριση βάσεων δεδομένων και άλλους τύπους κατανεμημένων υπηρεσιών πληροφοριών.

Στην Εικόνα παρακάτω μπορούμε να δούμε τη σχέση του επιπέδου εφαρμογής με το χρήστη και το επίπεδο παρουσίασης. Από τις πολλές διαθέσιμες υπηρεσίες εφαρμογών, η εικόνα παρουσιάζει μόνο τρεις: X.400 (υπηρεσίες διαχείρισης μηνυμάτων), X.500 (υπηρεσίες καταλόγου) και μεταφορά, προσπέλαση και διαχείριση αρχείων (FTAM). Ο χρήστης σε αυτό

το παράδειγμα χρησιμοποιεί X.400 για να στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου.



Επίπεδο εφαρμογής

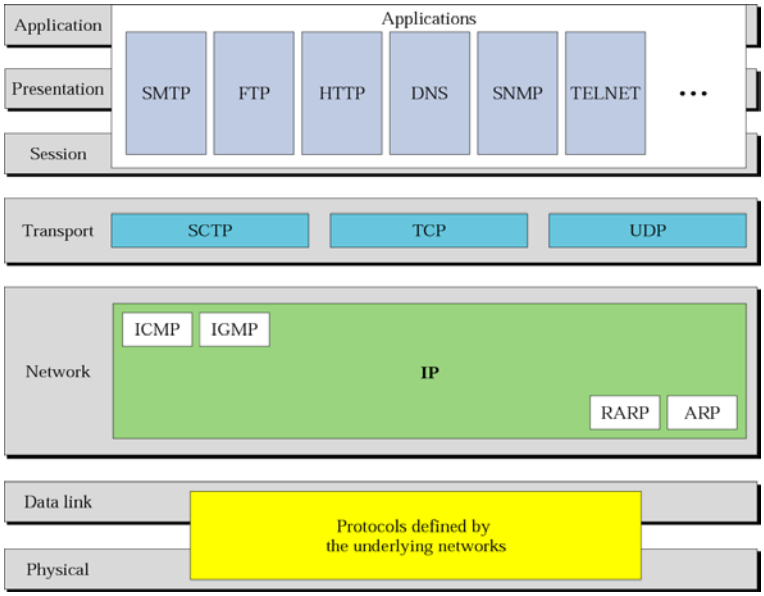
Μεταξύ των ευθυνών του επιπέδου εφαρμογής είναι οι εξής:

- **Εικονικό τερματικό δικτύου.** Ένα εικονικό τερματικό δικτύου είναι μία προγραμματιστική έκδοση ενός φυσικού τερματικού και επιτρέπει στους χρήστες να συνδέονται σε έναν απομακρυσμένο κεντρικό υπολογιστή. Για να επιτευχθεί αυτό, η εφαρμογή δημιουργεί μία προγραμματιστική εξομοίωση τερματικού, η οποία, με τη σειρά της, επικοινωνεί με τον κεντρικό υπολογιστή και αντιστρόφως. Ο απομακρυσμένος κεντρικός υπολογιστής πιστεύει ότι επικοινωνεί με ένα από τα δικά του τερματικά και μας επιτρέπει να συνδεθούμε.
- **Μεταφορά, προσπέλαση και διαχείριση αρχείων (FTAM).** Αυτή η εφαρμογή επιτρέπει σε ένα χρήστη να προσπελαύνει αρχεία σε έναν απομακρυσμένο κεντρικό υπολογιστή (για τροποποίηση ή ανάγνωση δεδομένων), να ανακτήσει αρχεία από έναν απομακρυσμένο υπολογιστή για χρήση στον τοπικό υπολογιστή και να διαχειριστεί ή να ελέγξει τοπικά τα αρχεία ενός απομακρυσμένου υπολογιστή.
- **Υπηρεσίες ταχυδρομείου.** Αυτή η εφαρμογή παρέχει τη βάση για την προώθηση και την αποθήκευση ηλεκτρονικής αλληλογραφίας.
- **Υπηρεσίες καταλόγου.** Αυτή η εφαρμογή παρέχει κατανεμημένους πόρους βάσεων δεδομένων και πρόσβαση για καθολικές πληροφορίες για διάφορες υπηρεσίες και αντικείμενα.

2.3 ΠΡΩΤΟΚΟΛΛΟ TCP/IP

Το πρωτόκολλο TCP/IP αναπτύχθηκε πριν από το μοντέλο OSI και επομένως, τα επίπεδα του πρωτοκόλλου TCP/IP δεν ταυτίζονται ακριβώς με εκείνα του μοντέλου OSI. Το πρωτόκολλο TCP/IP αποτελείται από πέντε

επίπεδα: φυσικό, σύνδεσης δεδομένων, δικτύου, μεταφοράς και εφαρμογής. Τα πρώτα τέσσερα παρέχουν φυσικά πρότυπα, διεπαφή δικτύου, υπηρεσίες διαδικτύου και λειτουργίες μεταφοράς που αντιστοιχούν στα πρώτα τέσσερα επίπεδα του μοντέλου OSI. Τα ανώτερα τρία επίπεδα του μοντέλου OSI όμως, εκπροσωπούνται στο TCP/IP από ένα μόνο επίπεδο που ονομάζεται επίπεδο εφαρμογής (**δείτε την Εικόνα παρακάτω**).



TCP/IP και μοντέλο OSI

Το TCP/IP είναι ένα ιεραρχικό πρωτόκολλο που αποτελείται από διαλογικές μονάδες, κάθε μία εκ των οποίων παρέχει ένα συγκεκριμένο πακέτο λειτουργιών, οι μονάδες όμως δεν είναι απαραίτητα αλληλένδετες. Ενώ το μοντέλο OSI ορίζει συγκεκριμένα ποιες λειτουργίες ανήκουν σε κάθε επίπεδο, τα επίπεδα στο πρωτόκολλο TCP/IP περιέχουν σχετικά ανεξάρτητα πρωτόκολλα που μπορούν να αναμειχθούν και να ταυτιστούν ανάλογα με τις ανάγκες του συστήματος. Ο όρος ιεραρχικό σημαίνει ότι κάθε ανώτερο πρωτόκολλο υποστηρίζεται από ένα ή περισσότερα πρωτόκολλα χαμηλότερου επιπέδου.
Στο επίπεδο μεταφοράς, το TCP/IP ορίζει τρία πρωτόκολλα: πρωτόκολλο ελέγχου μετάδοσης (TCP), πρωτόκολλο διαγράμματος δεδομένων χρήστη (UDP) και πρωτόκολλο μετάδοσης ελέγχου ροής (SCTP). Στο επίπεδο δικτύου, το κύριο πρωτόκολλο που ορίζεται από το TCP/IP είναι το πρωτόκολλο διαδικτύου (IP), αν και υπάρχουν μερικά ακόμα πρωτόκολλα που υποστηρίζουν μετακίνηση δεδομένων σε αυτό το επίπεδο.

Φυσικό επίπεδο και επίπεδο σύνδεσης δεδομένων

Στο φυσικό επίπεδο και στο επίπεδο σύνδεσης δεδομένων, το TCP/IP δεν ορίζει συγκεκριμένο πρωτόκολλο. Υποστηρίζει όλα τα βασικά και ιδιόκτητα

πρωτόκολλα. Ένα δίκτυο σε ένα διαδίκτυο TCP/IP μπορεί να είναι ένα τοπικό LAN ή ένα ευρείας περιοχής WAN.

Επίπεδο δικτύου

Στο επίπεδο δικτύου (ή ακριβέστερα στο επίπεδο διαδικτύου), το TCP/IP υποστηρίζει το πρωτόκολλο διαδικτύου IP. Το IP με τη σειρά του χρησιμοποιεί τέσσερα υποστηριζόμενα πρωτόκολλα: ARP, RARP, ICMP, IGMP.

Πρωτόκολλο διαδικτύου (IP)

Το πρωτόκολλο διαδικτύου (IP) είναι ένας μηχανισμός μετάδοσης που χρησιμοποιείται από τα πρωτόκολλα TCP/IP. Είναι ένα αξιόπιστο και ασύνδετο πρωτόκολλο –μία υπηρεσία βέλτιστης αποτελεσματικότητας διανομής. Ο όρος βέλτιστη αποτελεσματικότητα σημαίνει ότι το IP δεν παρέχει έλεγχο λαθών ή παρακολούθηση. Το IP θεωρεί δεδομένη την αναξιοπιστία των υποκείμενων επιπέδων και κάνει ό,τι μπορεί καλύτερο για να φτάσει η μετάδοση στον προορισμό της, χωρίς όμως εγγυήσεις.
Το IP μεταφέρει δεδομένα σε πακέτα που ονομάζονται διαγράμματα δεδομένων (datagrams), κάθε ένα από τα οποία μεταφέρεται χωριστά. Αυτά τα διαγράμματα δεδομένων μπορούν να ταξιδέψουν σε διαφορετικές διαδρομές και να φτάσουν χωρίς σειρά ή να φτάσουν δύο φορές το καθένα. Το IP δεν παρακολουθεί τις διαδρομές και δεν προσφέρει υπηρεσία ανασύνταξης των διαγραμμάτων όταν φτάσουν στον προορισμό τους.
Οι περιορισμένες λειτουργίες του IP δεν θα πρέπει να θεωρούνται αδυναμία. Το IP παρέχει ασύνδετες μεταξύ τους λειτουργίες μετάδοσης που επιτρέπουν στο χρήστη να χρησιμοποιεί μόνο τις υπηρεσίες που του είναι απαραίτητες για μία δεδομένη εφαρμογή και συνεπώς προσφέρεται για μέγιστη αποτελεσματικότητα.

Πρωτόκολλο ανάλυσης διεύθυνσης (ARP)

Το πρωτόκολλο ανάλυσης διεύθυνσης (ARP) χρησιμοποιείται για τη συσχέτιση μίας διεύθυνσης IP με τη φυσική διεύθυνση. Σε ένα τυπικό φυσικό δίκτυο, όπως ένα LAN, κάθε συσκευή σε μία γραμμή αναγνωρίζεται από μία φυσική διεύθυνση ή διεύθυνση σταθμού που συνήθως εντυπώνεται στην κάρτα διεπαφής του δικτύου (NIC). Το ARP χρησιμοποιείται για να βρει τη φυσική διεύθυνση του κόμβου όταν η διεύθυνση Internet είναι γνωστή.

Πρωτόκολλο αντίστροφης ανάλυσης διεύθυνσης (RARP)

Το πρωτόκολλο αντίστροφης ανάλυσης διεύθυνσης (RARP) επιτρέπει σε έναν κεντρικό υπολογιστή να βρει την διεύθυνση Internet του όταν γνωρίζει τη φυσική διεύθυνσή του. Χρησιμοποιείται όταν ένας υπολογιστής συνδέεται

στο δίκτυο για πρώτη φορά ή όταν ανοίγει ένας υπολογιστής χωρίς δίσκο. Το RARP είναι το αντίθετο του ARP. Το ARP χρησιμοποιείται όταν είναι γνωστή η IP διεύθυνση, αλλά δεν είναι η φυσική διεύθυνση. Το RARP χρησιμοποιείται όταν είναι γνωστή η φυσική διεύθυνση, αλλά η IP διεύθυνση δεν είναι.

Πρωτόκολλο μηνυμάτων ελέγχου Internet (ICMP)

Το πρωτόκολλο μηνυμάτων ελέγχου Internet (ICMP) είναι ένας μηχανισμός που χρησιμοποιείται από κεντρικούς υπολογιστές και θύρες εξόδου και ενημερώνει τον αποστολέα για προβλήματα που παρουσιάζονται στα διαγράμματα δεδομένων. Το ICMP στέλνει μηνύματα ερωτημάτων και αναφοράς λαθών. Το πρωτόκολλο IP δεν διαθέτει μηχανισμό αναφοράς λαθών ή διόρθωσης λαθών. Τι συμβαίνει αν κάτι πάει στραβά; Τι συμβαίνει αν ένας δρομολογητής πρέπει να απορρίψει ένα διάγραμμα δεδομένων επειδή δεν μπορεί να βρει ένα δρομολογητή στον τελικό προορισμό, ή επειδή το πεδίο χρόνου ζωής έχει μηδενική τιμή; Τι συμβαίνει αν ο κεντρικός υπολογιστής στον τελικό προορισμό πρέπει να απορρίψει όλα τα τμήματα ενός διαγράμματος δεδομένων επειδή δεν έχει δεχθεί όλα τα τμήματα μέσα σε προκαθορισμένο χρόνο; Αυτά είναι παραδείγματα περιπτώσεων όπου έχει συμβεί κάποιο λάθος και το πρωτόκολλο IP δεν διαθέτει ενσωματωμένο μηχανισμό για να ενημερώσει τον αρχικό κεντρικό υπολογιστή. Το πρωτόκολλο IP δεν διαθέτει επίσης μηχανισμό για ερωτήματα στον κεντρικό υπολογιστή και ερωτήματα διαχείρισης. Ένας κεντρικός υπολογιστής μερικές φορές πρέπει να διαπιστώσει αν ένας δρομολογητής ή ένας άλλος κεντρικός υπολογιστής είναι ενεργός. Και μερικές φορές ένας διαχειριστής δικτύου χρειάζεται πληροφορίες από άλλον κεντρικό υπολογιστή ή δρομολογητή. Το ICMP έχει σχεδιαστεί για να διορθώνει τα δύο παραπάνω μειονεκτήματα. Είναι σύντροφος του πρωτοκόλλου IP.

Πρωτόκολλο μηνυμάτων ομάδας Internet (IGMP)

Το πρωτόκολλο μηνυμάτων ομάδας Internet (IGMP) χρησιμοποιείται για να διευκολύνει την ταυτόχρονη μετάδοσης ενός μηνύματος σε μία ομάδα παραληπτών. Το πρωτόκολλο IP μπορεί να εμπλέκεται σε δύο τύπους επικοινωνίας: unicasting και multicasting. Unicasting είναι η επικοινωνία μεταξύ ενός αποστολέα και ενός παραλήπτη –είναι μία επικοινωνία ενός με έναν. Μερικές διαδικασίες όμως, μερικές φορές πρέπει να στείλουν το ίδιο μήνυμα σε πολλούς παραλήπτες ταυτόχρονα. Αυτό ονομάζεται multicasting, μία επικοινωνία ενός με πολλούς. Η επικοινωνία multicasting έχει πολλές εφαρμογές: Για παράδειγμα, πολλοί χρηματιστές μπορούν ταυτόχρονα να ενημερώνονται για την αλλαγή της τιμής μίας μετοχής ή ταξιδιωτικοί πράκτορες μπορούν να ενημερώνονται για την ακύρωση ενός ταξιδιού. Μερικές άλλες εφαρμογές είναι η εκμάθηση εξ αποστάσεως και τα βίντεο κατ’ απαίτηση. Το πρωτόκολλο IGMP είναι ένα από τα απαραίτητα αλλά όχι επαρκή πρωτόκολλα που εμπλέκονται στο multicasting.

Επίπεδο μεταφοράς

Το επίπεδο μεταφοράς παραδοσιακά εκπροσωπείτο στο TCP/IP από δύο πρωτόκολλα: το TCP και το UDP. Το IP είναι ένα πρωτόκολλο από υπολογιστή σε υπολογιστή, που σημαίνει ότι μπορεί να παραδώσει ένα πακέτο από μία φυσική συσκευή σε άλλη. Τα UDP και TCP είναι πρωτόκολλα επιπέδου μεταφοράς, υπεύθυνα για τη διανομή ενός μηνύματος από μία διαδικασία (εκτελούμενο πρόγραμμα) σε άλλη διαδικασία. Ένα νέο πρωτόκολλο επιπέδου μεταφοράς, το SCTP, έχει επινοηθεί για να ικανοποιήσει τις ανάγκες μερικών νέων εφαρμογών.

Πρωτόκολλο διαγραμμάτων δεδομένων χρήστη (UDP)

Το πρωτόκολλο διαγραμμάτων δεδομένων χρήστη (UDP) είναι το πιο απλό από τα δύο βασικά πρωτόκολλα μεταφοράς του TCP/IP. Είναι ένα πρωτόκολλο επεξεργασίας προς επεξεργασία που προσθέτει μόνο διευθύνσεις θυρών, έλεγχο λαθών αθροίσματος και πληροφορίες μήκους για τα δεδομένα που έρχονται από το ανώτερο επίπεδο.

Πρωτόκολλο ελέγχου μετάδοσης (TCP)

Το πρωτόκολλο ελέγχου μετάδοσης (TCP) παρέχει όλες τις υπηρεσίες του επιπέδου μεταφοράς σε εφαρμογές. Το TCP είναι ένα αξιόπιστο πρωτόκολλο μεταφοράς ροής. Ο όρος ροή στο συγκεκριμένο πλαίσιο σχετίζεται με τη σύνδεση: μία σύνδεση πρέπει να υπάρχει μεταξύ των δύο άκρων μίας μετάδοσης για να γίνει εφικτή η μεταφορά δεδομένων.
Στην πλευρά του αποστολέα κάθε μετάδοσης, το TCP χωρίζει μία ροή δεδομένων σε μικρότερες μονάδες που ονομάζονται τμήματα. Κάθε τμήμα περιλαμβάνει ένα σειριακό αριθμό που βοηθά στην ανασύνταξη μετά τη λήψη, μαζί με έναν αριθμό επιβεβαίωσης για τα τμήματα που ελήφθησαν. Τα τμήματα μεταφέρονται μέσω ενός διαδικτύου μέσα σε διαγράμματα δεδομένων IP. Στην πλευρά του λήπτη, το TCP συλλέγει κάθε διάγραμμα δεδομένων καθώς λαμβάνεται και το βάζει στη θέση του σύμφωνα με το σειριακό αριθμό.

Πρωτόκολλο μετάδοσης ελέγχου ροής (SCTP)

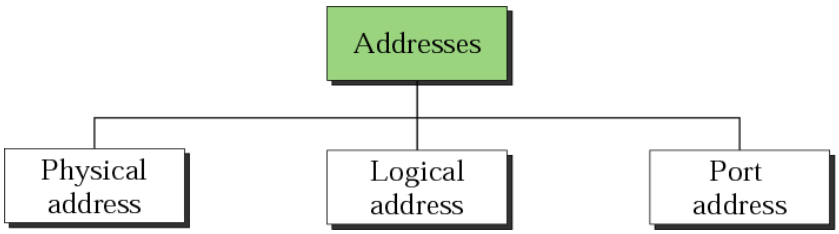
Το πρωτόκολλο μετάδοσης ελέγχου ροής (SCTP) παρέχει πλήρη υποστήριξη για νέες εφαρμογές όπως την τεχνολογία IP. Είναι ένα πρωτόκολλο επιπέδου μεταφοράς που συνδυάζει τα καλά στοιχεία των UDP και TCP. Το SCTP είναι ένα αξιόπιστο πρωτόκολλο που βασίζεται σε μηνύματα. Διατηρεί τα όρια του μηνύματος και ταυτόχρονα ανιχνεύει χαμένα δεδομένα, διπλά δεδομένα και δεδομένα εκτός σειράς. Διαθέτει επίσης μηχανισμούς ελέγχου συμφόρησης και ελέγχου ροής.

Επίπεδο εφαρμογής

Το επίπεδο εφαρμογής στο TCP/IP είναι ισοδύναμο με τα επίπεδα συνόδου, παρουσίασης και εφαρμογής του μοντέλου OSI.

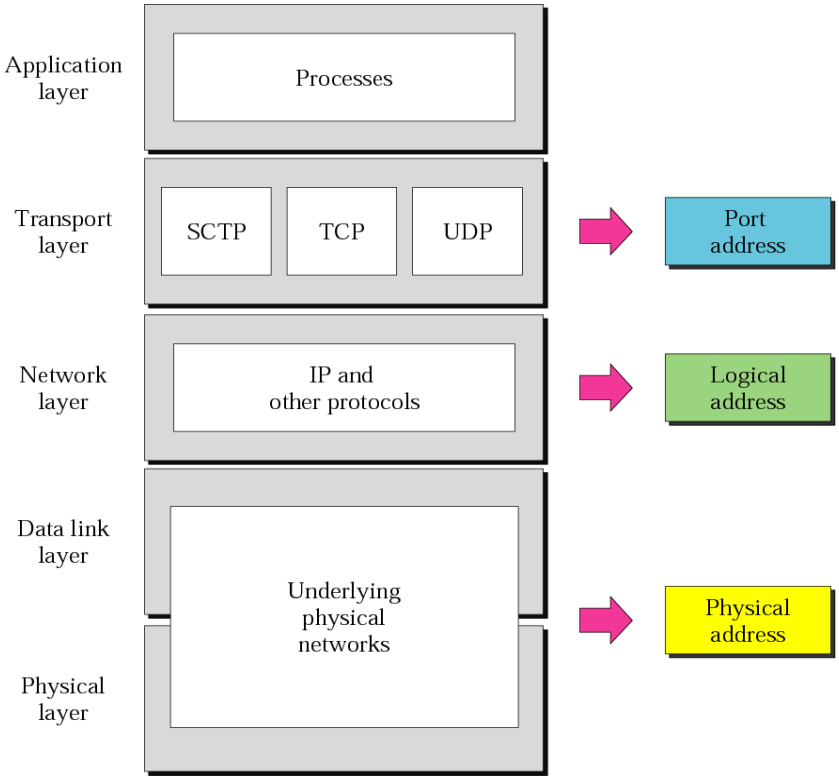
2.4 ΔΙΕΥΘΥΝΣΙΟΔΟΤΗΣΗ

Τρία επίπεδα διευθύνσεων χρησιμοποιούνται σε ένα διαδίκτυο που χρησιμοποιεί τα πρωτόκολλα TCP/IP: φυσική διεύθυνση (σύνδεση), λογική διεύθυνση (IP) και διεύθυνση θύρας. (**δείτε την Εικόνα παρακάτω**).



Διευθύνσεις στο TCP/IP

Κάθε διεύθυνση ανήκει σε ένα συγκεκριμένο επίπεδο της αρχιτεκτονικής TCP/IP, όπως φαίνεται στην **εικόνα παρακάτω**.



Σχέση επιπέδων και διευθύνσεων στο TCP/IP

Φυσική διεύθυνση

Η φυσική διεύθυνση, γνωστή και ως διεύθυνση σύνδεσης, είναι η διεύθυνση ενός κόμβου όπως ορίζεται από το LAN ή το WAN. Περιλαμβάνεται στο πλαίσιο που χρησιμοποιείται από το επίπεδο σύνδεσης δεδομένων. Είναι η διεύθυνση χαμηλότερου επιπέδου.
Οι φυσικές διευθύνσεις ασκούν εξουσία στο δίκτυο (LAN ή WAN). Το μέγεθος και η μορφή αυτών των διευθύνσεων ποικίλλουν ανάλογα με το δίκτυο. Για παράδειγμα, το Ethernet χρησιμοποιεί μία φυσική διεύθυνση των 6 bytes (48 bits) που εντυπώνεται στην κάρτα διεπαφής δικτύου (NIC). Το LocalTalk (Apple) ωστόσο, έχει μία δυναμική διεύθυνση του 1 byte που αλλάζει κάθε φορά που εμφανίζεται ο σταθμός.

Unicast, Multicast και Broadcast φυσικές διευθύνσεις

Οι φυσικές διευθύνσεις μπορεί να είναι unicast (ένας παραλήπτης), multicast (πολλοί παραλήπτες), ή broadcast (όταν λαμβάνεται από όλα τα συστήματα σε ένα δίκτυο). Μερικά δίκτυα υποστηρίζουν και τις τρεις διευθύνσεις. Για παράδειγμα, το Ethernet υποστηρίζει τις unicast φυσικές διευθύνσεις (6 bytes), τις διευθύνσεις multicast και τις διευθύνσεις broadcast. Μερικά δίκτυα δεν υποστηρίζουν τις multicast ή τις broadcast φυσικές διευθύνσεις. Αν ένα πλαίσιο πρέπει να σταλεί σε μία ομάδα παραληπτών ή σε όλα τα συστήματα, οι διευθύνσεις multicast ή broadcast πρέπει να εξομοιώνονται με

χρήση unicast διευθύνσεων. Αυτό σημαίνει ότι στέλνονται πολλά πακέτα που χρησιμοποιούν διευθύνσεις unicast.

Λογική διεύθυνση

Οι λογικές διευθύνσεις είναι απαραίτητες για παγκόσμιες υπηρεσίες επικοινωνίας που είναι ανεξάρτητες των υποκείμενων φυσικών δικτύων. Οι φυσικές διευθύνσεις δεν είναι επαρκείς σε ένα διαδικτυακό περιβάλλον όπου διαφορετικά δίκτυα μπορούν να έχουν διαφορετικές μορφές διευθύνσεων. Απαιτείται ένα παγκόσμιο σύστημα διευθυνσιοδότησης στο οποίο κάθε υπολογιστής μπορεί να αναγνωριστεί μοναδικά, ανεξάρτητα από το υποκείμενο φυσικό δίκτυο. Οι λογικές διευθύνσεις έχουν σχεδιαστεί για αυτόν το σκοπό. Μία λογική διεύθυνση στο Internet είναι τώρα μία διεύθυνση με 32 bits που μπορεί να ορίσει μοναδικά έναν κεντρικό υπολογιστή που συνδέεται στο Internet. Δεν είναι δυνατόν δύο κεντρικοί υπολογιστές που έχουν δημόσια διεύθυνση και εμφανίζονται στο Internet να έχουν την ίδια διεύθυνση IP.

Unicast, multicast και broadcast διευθύνσεις

Οι λογικές διευθύνσεις μπορούν να είναι unicast (ένας παραλήπτης), multicast (πολλοί παραλήπτες), ή broadcast (όλα τα συστήματα στο δίκτυο). Υπάρχουν περιορισμοί στις διευθύνσεις broadcast.

Διεύθυνση θύρας

Η διεύθυνση IP και η φυσική διεύθυνση είναι απαραίτητες για να ταξιδέψει μία ποσότητα δεδομένων από μία πηγή σε έναν προορισμό. Η άφιξη όμως στον προορισμό δεν είναι ο τελικός αντικειμενικός στόχος της επικοινωνίας δεδομένων στο Internet. Ένα σύστημα που δεν στέλνει τίποτα εκτός από δεδομένα από έναν υπολογιστή σε άλλον δεν είναι πλήρες. Σήμερα οι υπολογιστές είναι συσκευές που μπορούν να εκτελούν πολλές διαδικασίες παράλληλα. Ο τελικός στόχος της επικοινωνίας στο Internet είναι μία διαδικασία που επικοινωνεί με άλλη διαδικασία. Για παράδειγμα, ο υπολογιστής Α μπορεί να επικοινωνεί με τον υπολογιστή C χρησιμοποιώντας το TELNET. Παράλληλα, ο Α επικοινωνεί με τον Β χρησιμοποιώντας το FTP. Για να συμβαίνουν αυτές οι διαδικασίες ταυτόχρονα, πρέπει να έχουμε μία μέθοδο για την αναγνώριση των διαφορετικών διαδικασιών. Με άλλα λόγια, πρέπει να τους αποδώσουμε διευθύνσεις. Στην αρχιτεκτονική TCP/IP, το αναγνωριστικό που αποδίδεται σε κάθε διαδικασία ονομάζεται διεύθυνση θύρας. Μία διεύθυνση θύρας στο TCP/IP έχει μήκος 16 bits.

3 ΔΙΕΥΘΥΝΣΕΙΣ IP: ΔΙΕΥΘΥΝΣΙΟΔΟΤΗΣΗ ΜΕ ΚΛΑΣΕΙΣ

3.1 ΕΙΣΑΓΩΓΗ

Το αναγνωριστικό που χρησιμοποιείται στο επίπεδο IP του πρωτοκόλλου TCP/IP για την αναγνώριση κάθε συσκευής που συνδέεται στο Internet ονομάζεται διεύθυνση Internet ή διεύθυνση IP. Μία διεύθυνση IP είναι μία διεύθυνση με 32 bits που μοναδικά και παγκόσμια ορίζει τη σύνδεση ενός κεντρικού υπολογιστή ή ενός δρομολογητή στο Internet. Οι διευθύνσεις IP είναι μοναδικές. Είναι μοναδικές με την έννοια ότι κάθε διεύθυνση ορίζει μία και μόνο μία σύνδεση στο Internet. Δύο συσκευές στο Internet ποτέ δεν μπορεί να έχουν την ίδια διεύθυνση. Αν όμως μία συσκευή έχει δύο συνδέσεις στο Internet, μέσω δύο δικτύων, έχει δύο διευθύνσεις IP. Οι διευθύνσεις IP είναι παγκόσμιες με την έννοια ότι το σύστημα διευθυνσιοδότησης πρέπει να γίνεται αποδεκτό από κάθε κεντρικό υπολογιστή που θέλει να συνδεθεί στο Internet.

Χώρος διευθύνσεων

Ένα πρωτόκολλο όπως το IP που ορίζει διευθύνσεις έχει ένα χώρο διευθύνσεων. Ένας χώρος διευθύνσεων είναι ο συνολικός αριθμός των διευθύνσεων που χρησιμοποιούνται από το πρωτόκολλο. Αν ένα πρωτόκολλο χρησιμοποιεί N bits για να ορίσει μία διεύθυνση, ο χώρος διευθύνσεων είναι 2^N επειδή κάθε bit μπορεί να έχει δύο διαφορετικές τιμές (0 ή 1) και τα N bits μπορούν να έχουν 2^N τιμές.

Τρόπος γραφής

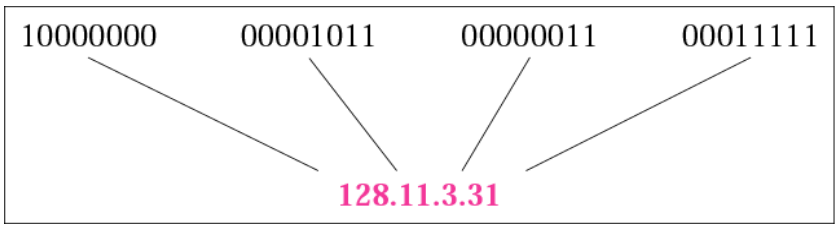
Υπάρχουν τρεις κοινοί τρόποι γραφής μίας διεύθυνσης IP: δυαδικός, δεκαδικός με τελείες και δεκαεξαδικός.

Δυαδικός τρόπος γραφής

Στο δυαδικό τρόπο γραφής, η διεύθυνση IP εμφανίζεται με 32 bits. Για να είναι πιο ευανάγνωστη, εισάγονται ένα ή περισσότερα κενά μεταξύ κάθε οκτάδας. Κάθε οκτάδα είναι ένα byte. Πολλές φορές λοιπόν θα ακούσουμε μία διεύθυνση IP να ονομάζεται διεύθυνση 32 bits, 4 οκτάδων ή 4 bytes.

Δεκαδικός με τελείες

Για να γίνει μία διεύθυνση IP πιο συμπυκνωμένη και πιο ευανάγνωστη, οι διευθύνσεις Internet συχνά γράφονται σε δεκαδική μορφή με μία τελεία να χωρίζει τα bits. **Στην Εικόνα παρακάτω** βλέπουμε μία διεύθυνση IP σε αυτήν τη μορφή. Σημειώνουμε ότι επειδή κάθε byte (οκτάδα) έχει μόνο 8 bits, κάθε αριθμός σε αυτήν τη μορφή είναι μεταξύ του 0 και του 255.



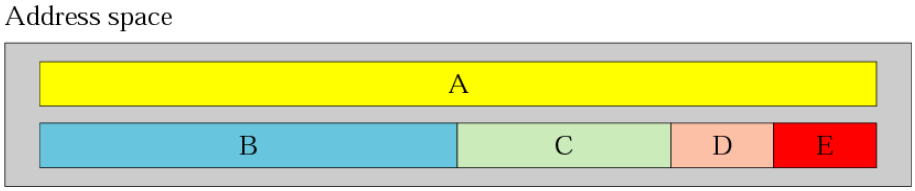
Δεκαδικός με τελείες

Δεκαεξαδικός τρόπος γραφής

Μερικές φορές βλέπουμε μία διεύθυνση IP σε δεκαεξαδική μορφή. Κάθε δεκαεξαδικό ψηφίο αντιστοιχεί σε 4 bits. Αυτό σημαίνει ότι μία διεύθυνση των 32 bits έχει 8 δεκαεξαδικά ψηφία. Αυτός ο τρόπος γραφής χρησιμοποιείται συχνά στον προγραμματισμό δικτύων.

3.2 ΔΙΕΥΘΥΝΣΙΟΔΟΤΗΣΗ ΜΕ ΚΛΑΣΕΙΣ

Στη διευθυνσιοδότηση με κλάσεις, ο χώρος διευθύνσεων IP χωρίζεται σε πέντε κλάσεις: A, B, C, D και E. Κάθε κλάση καταλαμβάνει μέρος του χώρου διευθύνσεων. **Στην Εικόνα παρακάτω** μπορούμε να δούμε τι καταλαμβάνει κάθε κλάση στο χώρο διευθύνσεων (κατά προσέγγιση).



Κατάληψη του χώρου διευθύνσεων

Μπορούμε να δούμε από την εικόνα ότι η κλάση A καλύπτει το μισό χώρο διευθύνσεων, κάτι που είναι ένα σοβαρό σχεδιαστικό λάθος. Η κλάση C καλύπτει το 1/4 του χώρου διευθύνσεων και οι κλάσεις D και E καλύπτουν το 1/16 του χώρου. **Ο Πίνακας παρακάτω** παρουσιάζει τον αριθμό των διευθύνσεων σε κάθε κλάση.

Class	*Number of Addresses*	*Percentage*
A	$2^{31} = 2,147,483,648$	50%
B	$2^{30} = 1,073,741,824$	25%
C	$2^{29} = 536,870,912$	12.5%
D	$2^{28} = 268,435,456$	6.25%
E	$2^{28} = 268,435,456$	6.25%

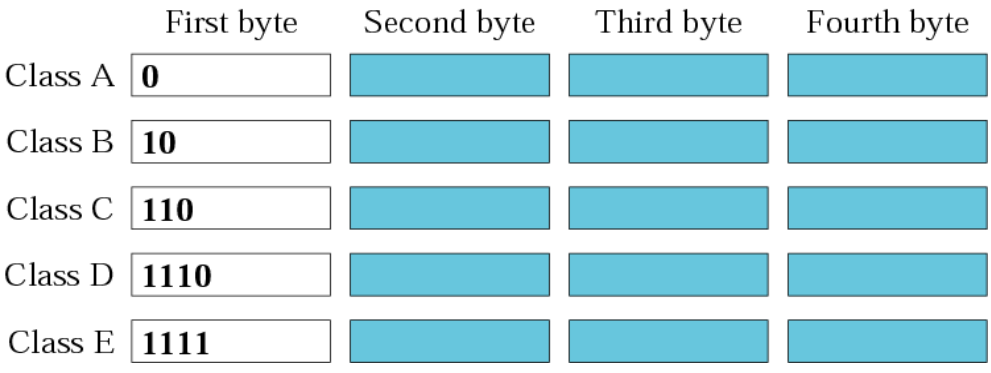
Διευθύνσεις ανά κλάση

Αναγνώριση κλάσεων

Μπορούμε να βρούμε την κλάση μίας διεύθυνσης όταν η διεύθυνση δίνεται με δυαδικό τρόπο γραφής ή με δεκαδικό με τελείες.

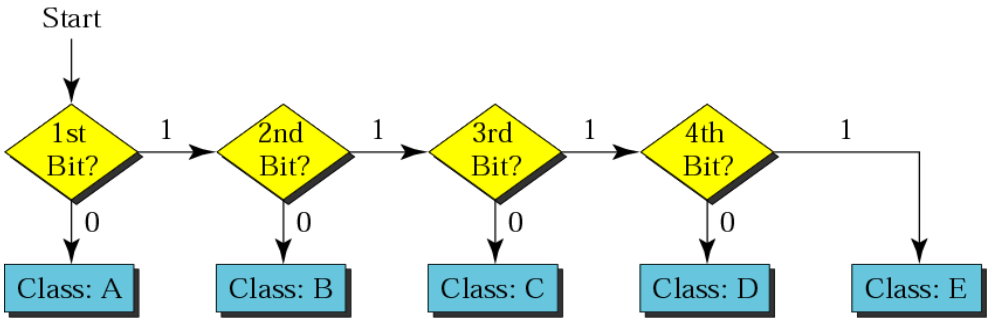
Εύρεση της κλάσης σε δυαδικό τρόπο γραφής

Αν η διεύθυνση δίνεται σε δυαδική μορφή, τα πρώτα bits μπορούν αμέσως να μας δείξουν την κλάση της διεύθυνσης όπως βλέπουμε στην **Εικόνα παρακάτω.**



Εύρεση της κλάσης σε δυαδική μορφή

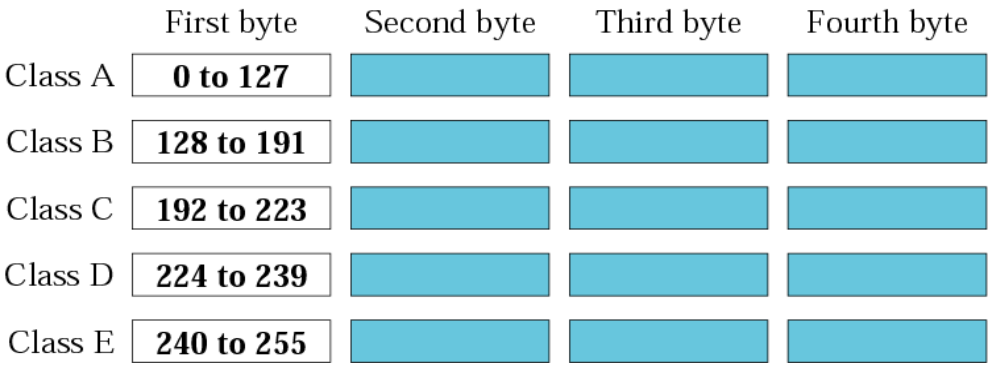
Μπορούμε να ακολουθήσουμε τη διαδικασία που βλέπουμε στην **Εικόνα παρακάτω** για να ελέγξουμε συστηματικά τα bits και να βρούμε την κλάση. Η διαδικασία μπορεί εύκολα να προγραμματιστεί σε κάθε γλώσσα.



Εύρεση της κλάσης της διεύθυνσης

Εύρεση της κλάσης σε δεκαδικό με τελείες

Όταν η διεύθυνση δίνεται σε δεκαδική μορφή με τελείες, αρκεί να παρατηρήσουμε μόνο το πρώτο byte (αριθμό) για να διαπιστώσουμε την κλάση της διεύθυνσης. Κάθε κλάση έχει ένα συγκεκριμένο εύρος αριθμών. **Η Εικόνα παρακάτω** δείχνει αυτό που λέμε.

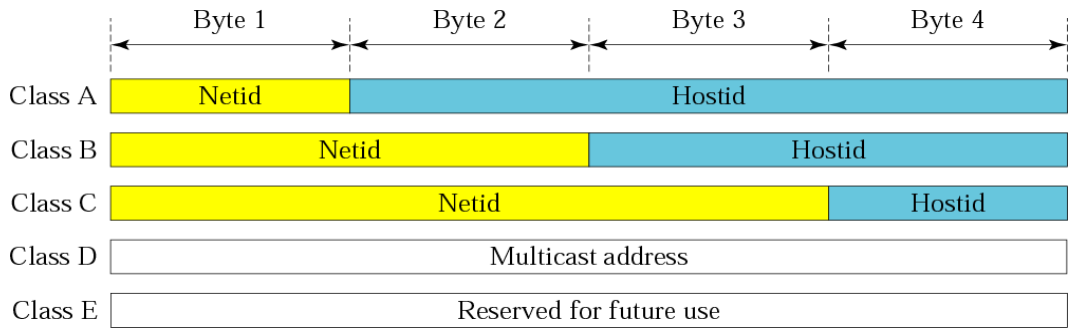


Εύρεση της κλάσης σε δεκαδική μορφή

Αυτό σημαίνει ότι αν το πρώτο byte (σε δεκαδική μορφή) είναι μεταξύ 0 και 127, η κλάση είναι A. Αν το πρώτο byte είναι μεταξύ 128 και 191 η κλάση είναι B και ούτω καθ' εξής.

Netid και Hostid

Στην διευθυνσιοδότηση με κλάσεις, μία διεύθυνση IP στις κλάσεις A, B και C χωρίζεται σε netid και hostid. Αυτά τα κομμάτια είναι μεταβλητού μήκους, ανάλογα με την κλάση της διεύθυνσης. Η **Εικόνα παρακάτω** δείχνει τα bytes netid και hostid. Σημειώνουμε ότι οι κλάσεις D και E δεν χωρίζονται σε netid και hostid.
Στην κλάση A, 1 byte ορίζει το netid και 3 bytes ορίζουν το hostid. Στην κλάση B, 2 bytes ορίζουν το netid και 2 bytes το hostid. Στην κλάση C, 3 bytes ορίζουν το netid και 1 byte το hostid.



Netid και hostid

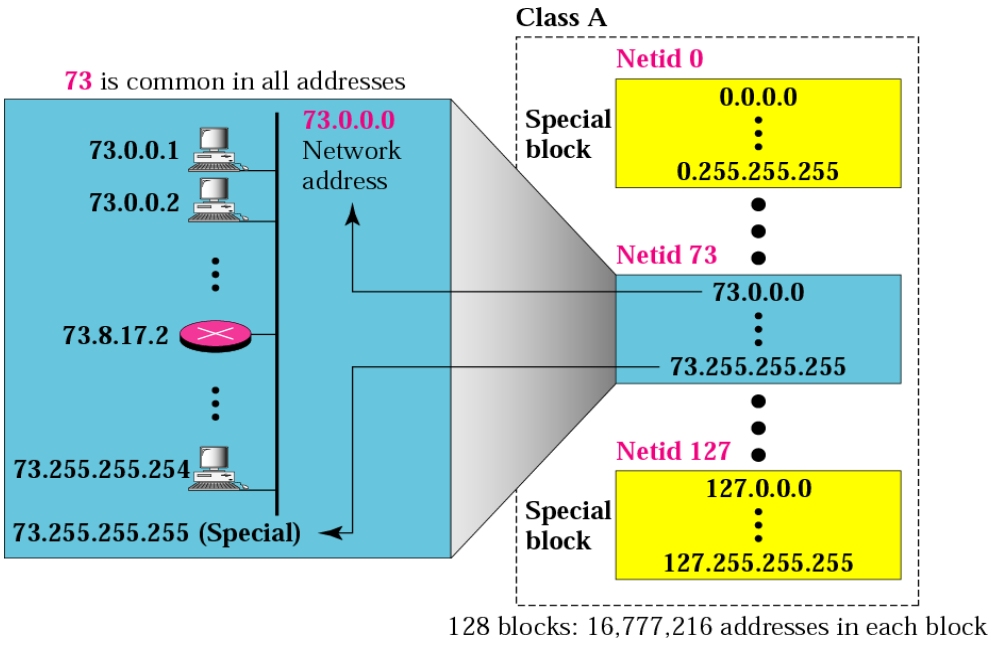
Κλάσεις και μπλοκ

Ένα πρόβλημα με τη διευθυνσιοδότηση με κλάσεις είναι ότι κάθε κλάση χωρίζεται σε ένα σταθερό αριθμό μπλοκ, με κάθε μπλοκ να έχει σταθερό μέγεθος. Ας εξετάσουμε κάθε κλάση.

Κλάση Α

Η κλάση Α χωρίζεται σε 128 μπλοκ με κάθε μπλοκ να έχει διαφορετικό netid. Το πρώτο μπλοκ καλύπτει διευθύνσεις από 0.0.0.0 έως 0.255.255.255 (netid 0). Το δεύτερο μπλοκ καλύπτει διευθύνσεις από 1.0.0.0 έως 1.255.255.255 (netid 1). Το τελευταίο μπλοκ καλύπτει διευθύνσεις από 127.0.0.0 έως 127.255.255.255 (netid 127). Σημειώνουμε ότι για κάθε μπλοκ διευθύνσεων, το πρώτο byte (netid) είναι ίδιο αλλά τα άλλα τρία bytes (hostid) μπορούν να πάρουν οποιαδήποτε τιμή στο δεδομένο εύρος.
Το πρώτο και το τελευταίο μπλοκ σε αυτήν την κλάση δεσμεύονται για ειδικούς σκοπούς. Επιπλέον, ένα μπλοκ (netid 10) χρησιμοποιείται για ιδιωτικές διευθύνσεις. Τα υπόλοιπα 125 μπλοκ μπορούν να εκχωρηθούν σε οργανισμούς. Αυτό σημαίνει ότι ο συνολικός αριθμός οργανισμών που μπορούν να έχουν διευθύνσεις κλάσης Α είναι μόνο 125. Κάθε μπλοκ όμως σε αυτήν την κλάση περιέχει 16.777.216 διευθύνσεις, που σημαίνει ότι ο οργανισμός θα πρέπει να είναι πολύ μεγάλος για να χρησιμοποιήσει όλες αυτές τις διευθύνσεις. Στην Εικόνα 4.7 βλέπουμε τα μπλοκ στην κλάση Α.
Η **Εικόνα παρακάτω** δείχνει επίσης πώς ένας οργανισμός στον οποίο εκχωρείται ένα μπλοκ με netid 73 χρησιμοποιεί τις διευθύνσεις του. Η πρώτη διεύθυνση στο μπλοκ χρησιμοποιείται για την αναγνώριση του οργανισμού στο υπόλοιπο Internet. Αυτή η διεύθυνση ονομάζεται διεύθυνση δικτύου. Ορίζει το δίκτυο του οργανισμού και όχι μεμονωμένους κεντρικούς υπολογιστές. Ο οργανισμός δεν επιτρέπεται να χρησιμοποιεί την τελευταία διεύθυνση καθώς αυτή δεσμεύεται για ειδικούς σκοπούς.
Οι διευθύνσεις της κλάσης Α σχεδιάστηκαν για μεγάλους οργανισμούς με μεγάλο αριθμό κεντρικών υπολογιστών ή δρομολογητών που επισυνάπτονται στα δίκτυά τους. Ο αριθμός όμως των διευθύνσεων σε κάθε μπλοκ,

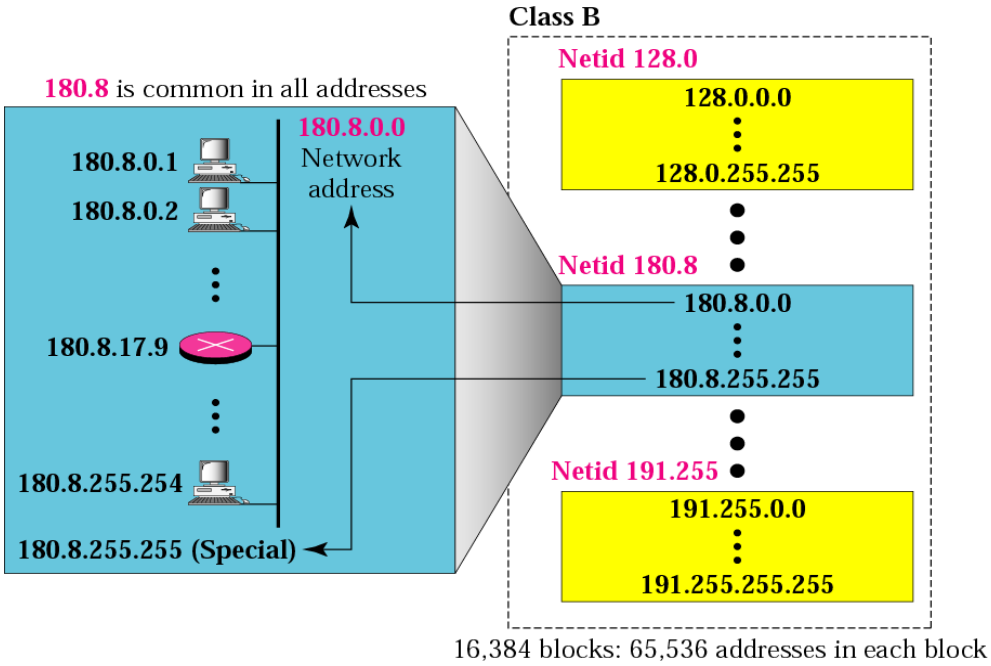
16.777.216, είναι πιθανώς μεγαλύτερος από τις ανάγκες όλων σχεδόν των οργανισμών. Πολλές διευθύνσεις χάνονται σε αυτήν την κλάση.



Μπλοκ στην κλάση Α

Κλάση Β

Η κλάση Β διαιρείται σε 16.384 μπλοκ με κάθε ένα να έχει διαφορετικό netid. Δεκαέξι μπλοκ δεσμεύονται για ιδιωτικές διευθύνσεις, αφήνοντας 16.368 μπλοκ να αποδοθούν σε οργανισμούς. Το πρώτο μπλοκ καλύπτει διευθύνσεις από 128.0.0.0 έως 128.0.255.255 (netid 128.0). Το δεύτερο μπλοκ καλύπτει διευθύνσεις από 191.255.0.0 έως 191.255.255.255 (netid 191.255). Σημειώνουμε ότι για κάθε μπλοκ διευθύνσεων, τα δύο πρώτα bytes (netid) είναι τα ίδια αλλά τα άλλα 2 (hostid) μπορούν να πάρουν οποιαδήποτε τιμή από το δεδομένο εύρος.
Υπάρχουν 16.368 μπλοκ που μπορούν να εκχωρηθούν. Αυτό σημαίνει ότι ο συνολικός αριθμός οργανισμών που μπορούν να έχουν διεύθυνση κλάσης Β είναι 16.368. Επειδή όμως κάθε μπλοκ σε αυτήν την κλάση περιέχει 65.536 διευθύνσεις, ο οργανισμός θα πρέπει να είναι αρκετά μεγάλος για να χρησιμοποιήσει όλες αυτές τις διευθύνσεις. Η **Εικόνα παρακάτω** δείχνει τα μπλοκ στην κλάση Β.

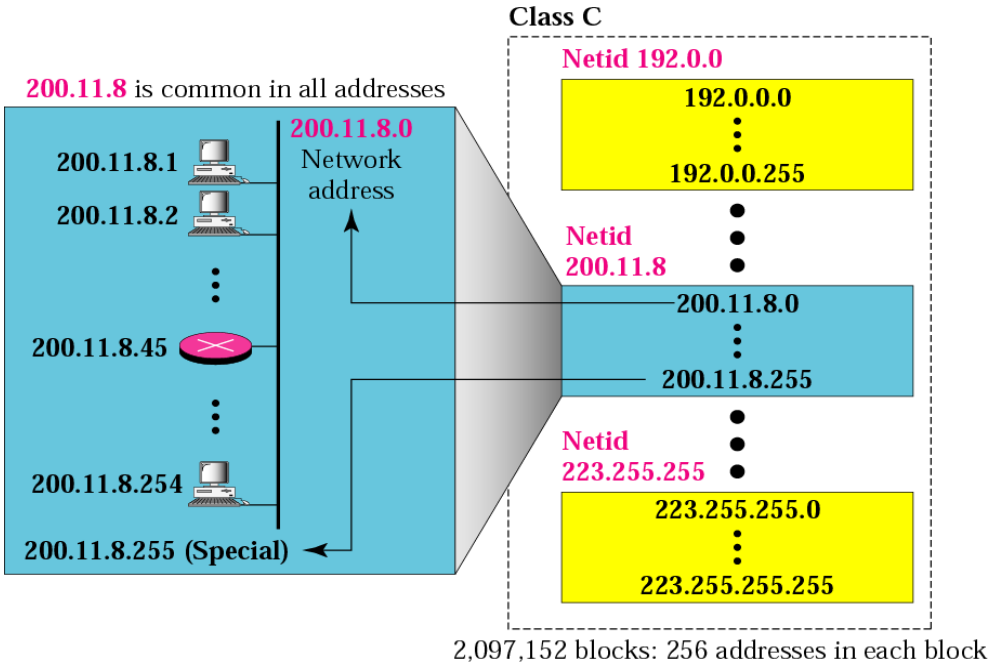


Μπλοκ στην κλάση Β

Η **Εικόνα παραπάνω** δείχνει επίσης πώς ένας οργανισμός στον οποίο εκχωρείται ένα μπλοκ με netid 180.8 χρησιμοποιεί τις διευθύνσεις του. Η πρώτη διεύθυνση είναι η διεύθυνση δικτύου και η τελευταία δεσμεύεται για ένα ειδικό σκοπό.
Οι διευθύνσεις της κλάσης Β σχεδιάστηκαν για οργανισμούς μεσαίου μεγέθους που έχουν μερικές δεκάδες χιλιάδες κεντρικούς υπολογιστές ή δρομολογητές στα δίκτυά τους. Ο αριθμός όμως των διευθύνσεων σε κάθε μπλοκ (65.536) είναι μεγαλύτερος από τις ανάγκες των περισσότερων οργανισμών μεσαίου μεγέθους και επομένως, πολλές διευθύνσεις χάνονται.

Κλάση C

Η κλάση C χωρίζεται σε 2.097.152 μπλοκ με κάθε ένα μπλοκ να έχει διαφορετικό netid. 256 μπλοκ χρησιμοποιούνται για ιδιωτικές διευθύνσεις, αφήνοντας έτσι 2.096.896 μπλοκ για να αποδοθούν σε οργανισμούς. Το πρώτο μπλοκ καλύπτει διευθύνσεις από 192.0.0.0 έως 192.0.0.255 (netid 192.0.0). Το τελευταίο μπλοκ καλύπτει διευθύνσεις από 223.255.255.0 έως 223.255.255.255 (netid 223.255.255). Σημειώνουμε ότι για κάθε μπλοκ διευθύνσεων τα πρώτα 3 bytes (netid) είναι ίδια αλλά αυτό που μένει (hostid) μπορεί να πάρει οποιαδήποτε τιμή από το δεδομένο εύρος.
Υπάρχουν 2.096.896 μπλοκ που μπορούν να αποδοθούν. Αυτό σημαίνει ότι ο συνολικός αριθμός οργανισμών που μπορούν να έχουν διεύθυνση κλάσης C είναι 2.096.896. Κάθε μπλοκ όμως σε αυτήν την κλάση περιέχει 256 διευθύνσεις, που σημαίνει ότι ο οργανισμός θα πρέπει να είναι αρκετά μικρός ώστε να χρειάζεται λιγότερες από 256 διευθύνσεις. **Η Εικόνα παρακάτω** δείχνει τα μπλοκ στην κλάση C.



Μπλοκ στην κλάση C

Η Εικόνα **παραπάνω** δείχνει επίσης πώς χρησιμοποιεί τις διευθύνσεις ένας οργανισμός στον οποίο εκχωρείται ένα μπλοκ με netid 200.11.8. Η πρώτη διεύθυνση είναι η διεύθυνση δικτύου και η τελευταία διεύθυνση δεσμεύεται για έναν ειδικό σκοπό. Οι διευθύνσεις της κλάσης C σχεδιάστηκαν για μικρούς οργανισμούς με ένα μικρό αριθμό κεντρικών υπολογιστών ή δρομολογητών που υπάρχουν στα δίκτυά τους. Ο αριθμός των διευθύνσεων σε κάθε μπλοκ είναι τόσο περιορισμένος ώστε οι περισσότεροι οργανισμοί δεν θα θέλουν ένα μπλοκ σε αυτήν την κλάση.

Κλάση D

Υπάρχει μόνο ένα μπλοκ στις διευθύνσεις της κλάσης D. Κάθε διεύθυνση σε αυτήν την κλάση χρησιμοποιείται για τον ορισμό μίας ομάδας κεντρικών υπολογιστών στο Internet. Όταν σε μία ομάδα εκχωρείται μία διεύθυνση σε αυτήν την κλάση, κάθε κεντρικός υπολογιστής που είναι μέλος αυτής της ομάδας θα έχει μία πολλαπλή διεύθυνση εκτός από την κανονική του διεύθυνση.

Κλάση E

Υπάρχει μόνο ένα μπλοκ στις διευθύνσεις της κλάσης E. Σχεδιάστηκε για να χρησιμοποιηθεί ως δεσμευμένες διευθύνσεις. Οι διευθύνσεις της κλάσης E δεσμεύονται για μελλοντικές χρήσεις –το μεγαλύτερο μέρος του μπλοκ χάνεται.

Διευθύνσεις δικτύου

Οι διευθύνσεις δικτύου παίζουν πολύ σημαντικό ρόλο στη διευθυνσιοδότηση με κλάσεις. Μία διεύθυνση δικτύου έχει αρκετές ιδιότητες:

- Η διεύθυνση δικτύου είναι η πρώτη διεύθυνση στο μπλοκ.
- Η διεύθυνση δικτύου ορίζει το δίκτυο για το υπόλοιπο Internet.
- Αν έχουμε τη διεύθυνση δικτύου μπορούμε να βρούμε την κλάση της διεύθυνσης, το μπλοκ και το εύρος των διευθύνσεων στο μπλοκ.

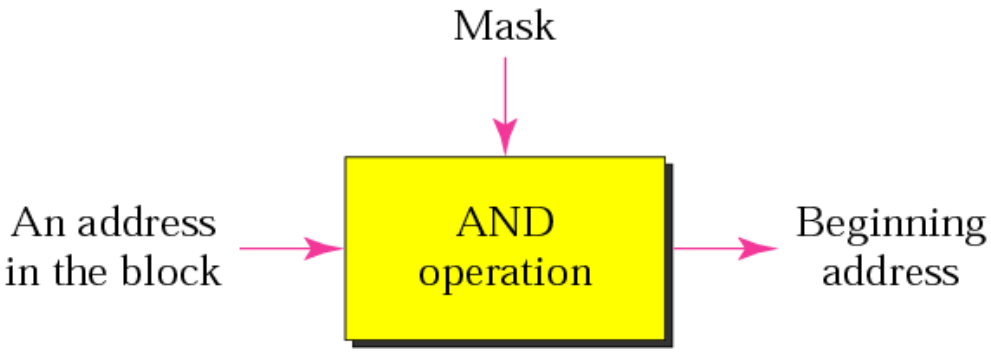
Στη διευθυνσιοδότηση με κλάσεις, η διεύθυνση δικτύου (η πρώτη διεύθυνση στο μπλοκ) είναι αυτή που εκχωρείται στον οργανισμό. Το εύρος των διευθύνσεων μπορεί αυτόματα να διαπιστωθεί από τη διεύθυνση δικτύου.

Μάσκα

Στην προηγούμενη ενότητα είπαμε ότι αν έχουμε τη διεύθυνση δικτύου, μπορούμε να βρούμε το μπλοκ και το εύρος των διευθύνσεων στο μπλοκ. Μπορεί να γίνει το αντίστροφο; Αν έχουμε μία διεύθυνση, μπορούμε να βρούμε τη διεύθυνση δικτύου (την αρχική διεύθυνση στο μπλοκ); Αυτό είναι σημαντικό επειδή για να δρομολογήσουμε ένα πακέτο στο σωστό δίκτυο, ένας δρομολογητής πρέπει να εξάγει μία διεύθυνση δικτύου από τη διεύθυνση προορισμού (μία διεύθυνση κεντρικού υπολογιστή) στην κεφαλίδα του πακέτου.
Ένας τρόπος να βρούμε τη διεύθυνση δικτύου είναι να βρούμε πρώτα την κλάση της διεύθυνσης και το netid. Μετά ορίζουμε το hostid ως μηδέν για να βρούμε τη διεύθυνση δικτύου. Για παράδειγμα, αν έχουμε την διεύθυνση 134.45.78.2, μπορούμε αμέσως να πούμε ότι η διεύθυνση ανήκει στην κλάση B. Το netid είναι 134.45 (2 bytes) και η διεύθυνση δικτύου είναι 134.45.0.0.
Η παραπάνω μέθοδος είναι εφικτή αν δεν έχουμε χωρίσει το δίκτυο σε δευτερεύοντα δίκτυα. Μία γενική διαδικασία που μπορεί να χρησιμοποιηθεί εμπλέκει μία μάσκα στην εύρεση της διεύθυνσης δικτύου από μία δεδομένη διεύθυνση.

Έννοια

Μία μάσκα είναι ένας αριθμός με 32 bits που δίνει την πρώτη διεύθυνση στο μπλοκ (τη διεύθυνση δικτύου) όταν εκτελέσουμε σε αυτόν την λογική πράξη AND μαζί με μία διεύθυνση στο μπλοκ. **Η Εικόνα παρακάτω** δείχνει την έννοια της μάσκας.



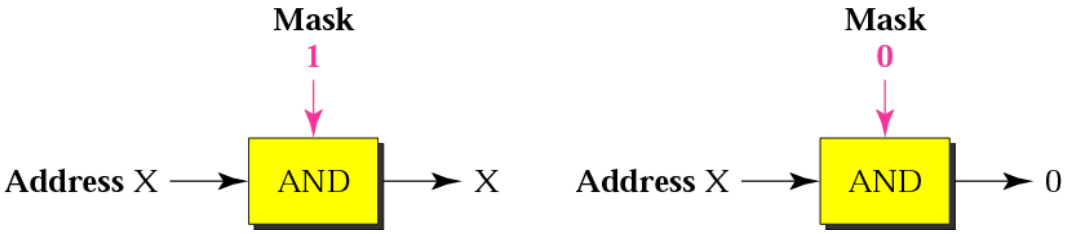
Έννοια της μάσκας

Πράξη AND

Η μάσκα χρησιμοποιεί τη λογική πράξη AND που ορίζεται στην επιστήμη των υπολογιστών. Η πράξη εφαρμόζεται bit προς bit στη διεύθυνση και τη μάσκα. Για το σκοπό μας είναι αρκετό να γνωρίζουμε ότι η πράξη AND κάνει τα εξής:

- Αν το bit στη μάσκα είναι 1, το αντίστοιχο bit στη διεύθυνση διατηρείται στην έξοδο (καμία αλλαγή).
- Αν το bit στη μάσκα είναι 0, το αποτέλεσμα στην έξοδο είναι 0 bit.

Με άλλα λόγια, τα bits στη διεύθυνση που αντιστοιχούν στους άσσους στη μάσκα διατηρούνται (παραμένουν 0 ή 1, ως είχαν) και τα bits που αντιστοιχούν στα μηδενικά στη μάσκα αλλάζουν σε 0. Η **Εικόνα παρακάτω** δείχνει τις δύο περιπτώσεις.



Πράξη AND

Προκαθορισμένες μάσκες

Στην πράξη AND για διευθυνσιοδότηση με κλάσεις, υπάρχουν τρεις μάσκες, μία για κάθε κλάση. Ο Πίνακας 4.2 δείχνει τη μάσκα για κάθε κλάση. Για την κλάση A, η μάσκα είναι 8 άσσοι και 24 μηδενικά. Για την κλάση B, η μάσκα είναι 16 άσσοι και 16 μηδενικά. Για την κλάση C, η μάσκα είναι 24 άσσοι και 8 μηδενικά. Οι άσσοι διατηρούν το netid και τα μηδενικά ορίζουν το hostid σε μηδέν. Η διεύθυνση δικτύου σε οποιαδήποτε κλάση είναι το netid με το hostid έχει μόνο μηδενικά. **Ο Πίνακας παρακάτω** δείχνει την προκαθορισμένη μάσκα για κάθε κλάση.

Class	*Mask in binary*	*Mask in dotted-decimal*
A	**11111111** 00000000 00000000 00000000	**255.**0.0.0
B	**11111111 11111111** 00000000 00000000	**255.255.**0.0
C	**11111111 11111111 11111111** 00000000	**255.255.255.**0

Προκαθορισμένες μάσκες

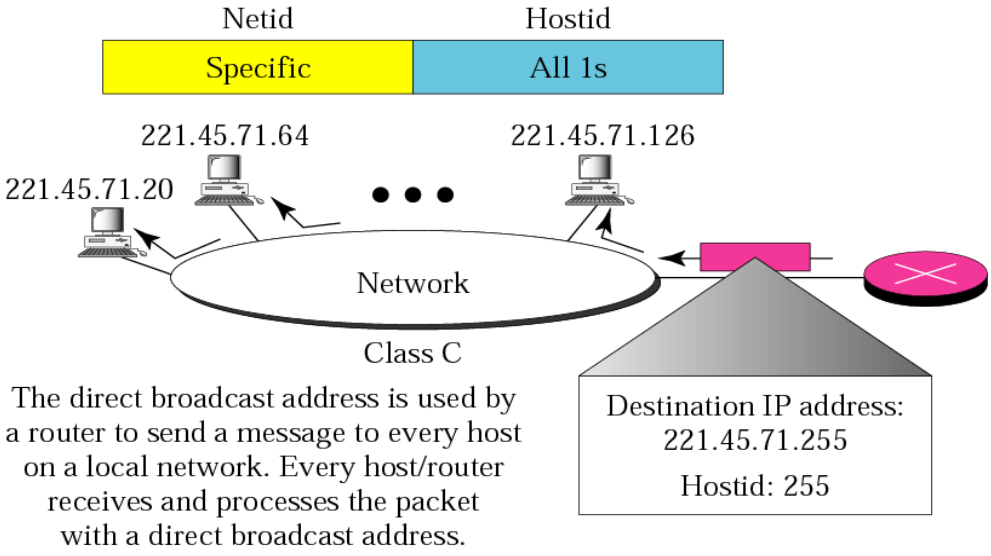
Ο αριθμός των άσσων σε κάθε κλάση ταυτίζεται με τον αριθμό των bits στο netid και ο αριθμός των μηδενικών ταυτίζεται με τον αριθμό των bits στο hostid. Με άλλα λόγια, όταν εκτελείται η AND σε μία μάσκα και μία διεύθυνση, το netid και το hostid είναι μηδέν.

3.3 Ειδικές διευθύνσεις

Μερικά μέρη του χώρου διευθύνσεων χρησιμοποιούνται για ειδικές διευθύνσεις.

Διεύθυνση απευθείας μετάδοσης

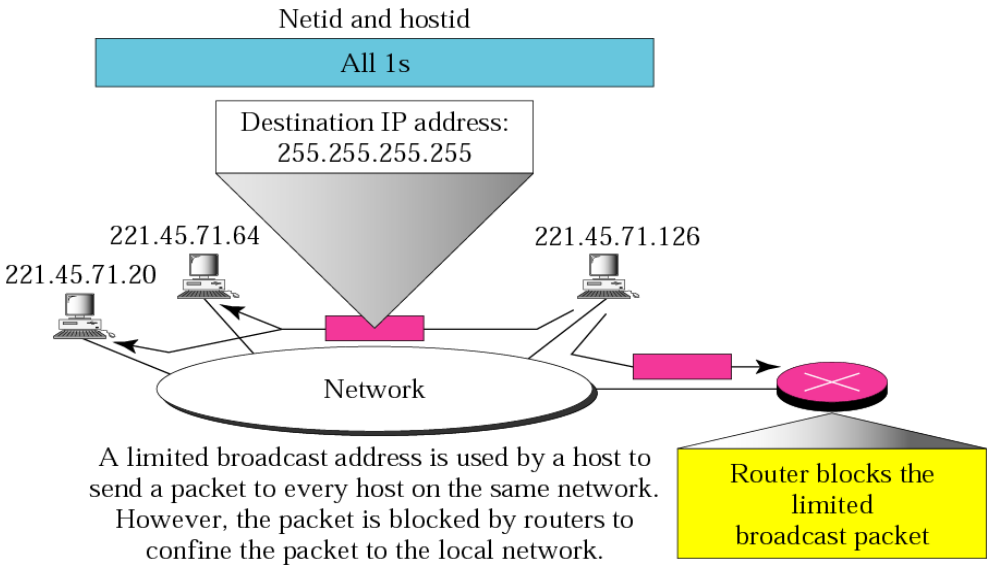
Στις κλάσεις A, B και C, αν το hostid έχει μόνο άσσους, η διεύθυνση ονομάζεται διεύθυνση απευθείας μετάδοσης. Χρησιμοποιείται από ένα δρομολογητή για να στείλει ένα πακέτο σε όλους τους υπολογιστές σε ένα συγκεκριμένο δίκτυο. Όλοι οι υπολογιστές θα δεχθούν ένα πακέτο που έχει αυτό το είδος διεύθυνσης προορισμού. Σημειώνουμε ότι αυτή η διεύθυνση μπορεί να χρησιμοποιηθεί μόνο ως διεύθυνση προορισμού σε ένα πακέτο IP. Σημειώνουμε επίσης ότι αυτή η ειδική διεύθυνση μειώνει τον αριθμό των διαθέσιμων hostid για κάθε netid στις κλάσεις A, B και C. **Στην Εικόνα παρακάτω**, ο δρομολογητής στέλνει ένα διάγραμμα δεδομένων χρησιμοποιώντας μία διεύθυνση IP προορισμού με ένα hostid που έχει όλο άσσους. Όλες οι συσκευές σε αυτό το δίκτυο λαμβάνουν και επεξεργάζονται το διάγραμμα δεδομένων.



Παράδειγμα διεύθυνσης απευθείας μετάδοσης

Διεύθυνση περιορισμένης μετάδοσης

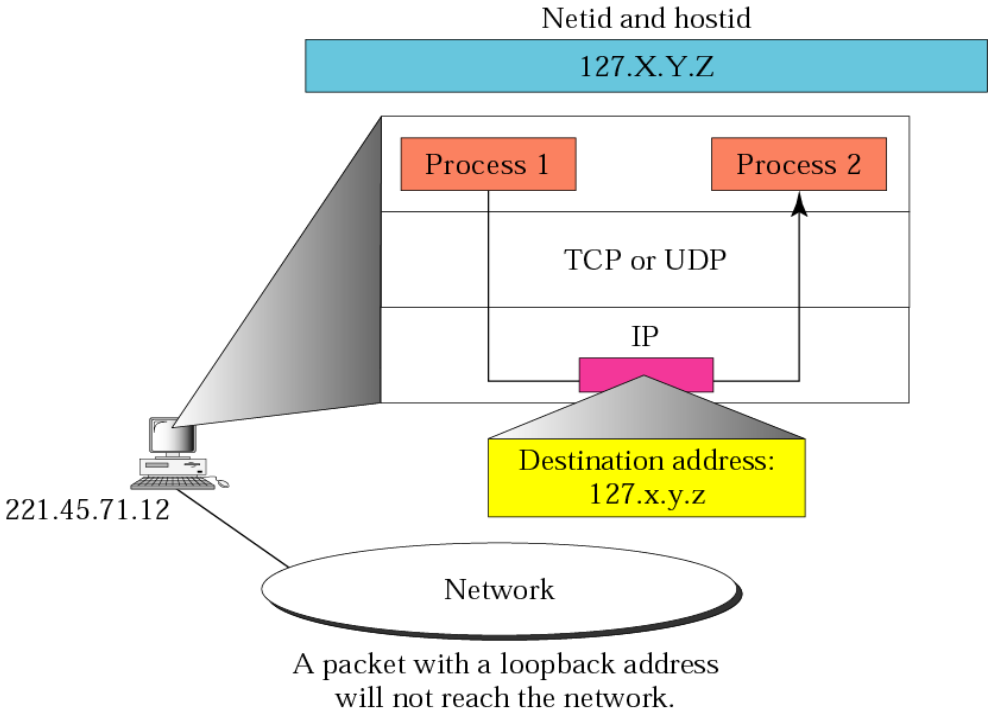
Στις κλάσεις A, B και C, μία διεύθυνση μόνο με άσσους για τα netid και hostid (32 bits) ορίζει μία διεύθυνση broadcast στο τρέχον δίκτυο. Ένας κεντρικός υπολογιστής που θέλει να στείλει ένα μήνυμα σε όλους τους άλλους κεντρικούς υπολογιστές μπορεί να χρησιμοποιήσει αυτήν τη διεύθυνση ως διεύθυνση προορισμού σε ένα πακέτο IP. Ένας δρομολογητής όμως θα μπλοκάρει ένα πακέτο που έχει αυτόν τον τύπο διεύθυνσης για να περιορίσει τη μετάδοση στο τοπικό δίκτυο. Σημειώνουμε ότι αυτή η διεύθυνση ανήκει στην κλάση E. **Στην Εικόνα παρακάτω** ένας υπολογιστής στέλνει ένα διάγραμμα δεδομένων χρησιμοποιώντας μία διεύθυνση IP που αποτελείται μόνο από άσσους. Όλες οι συσκευές σε αυτό το δίκτυο λαμβάνουν και επεξεργάζονται αυτό το διάγραμμα.



Παράδειγμα διεύθυνσης περιορισμένης μετάδοσης

Διεύθυνση επιστροφής

Η διεύθυνση IP με το πρώτο byte να είναι ίσο με 127 χρησιμοποιείται για τη διεύθυνση επιστροφής, η οποία είναι μία διεύθυνση που χρησιμοποιείται για να ελέγχει το λογισμικό σε έναν υπολογιστή. Όταν χρησιμοποιείται αυτή η διεύθυνση, ένα πακέτο ποτέ δεν φεύγει από τον υπολογιστή αλλά απλά επιστρέφει στο λογισμικό του πρωτοκόλλου. Μπορεί να χρησιμοποιηθεί για τον έλεγχο του λογισμικού IP. Για παράδειγμα, μία εφαρμογή όπως η <<ping>> μπορεί να στείλει ένα πακέτο με μία διεύθυνση επιστροφής ως διεύθυνση προορισμού για να δει αν το λογισμικό IP είναι ικανό να δεχθεί και να επεξεργαστεί ένα πακέτο. Επίσης, η διεύθυνση επιστροφής μπορεί να χρησιμοποιηθεί ως διαδικασία client (ένα πρόγραμμα εφαρμογής υπό εκτέλεση) για να στείλει μήνυμα σε μία διαδικασία server στον ίδιο υπολογιστή. Σημειώνουμε ότι αυτό μπορεί να χρησιμοποιηθεί μόνο ως διεύθυνση προορισμού σε ένα πακέτο IP. Σημειώνουμε επίσης ότι πρόκειται για διεύθυνση κλάσης Α που μειώνει τον αριθμό των μπλοκ στην κλάση Α κατά 1 (**δείτε την Εικόνα παρακάτω**).



Παράδειγμα της διεύθυνσης επιστροφής

4 Παράδοση, προώθηση και δρομολόγηση πακέτων IP

4.1 ΠΑΡΑΔΟΣΗ

Το επίπεδο δικτύου εποπτεύει το χειρισμό των πακέτων από τα υποκείμενα φυσικά δίκτυα. Ορίζουμε αυτόν τον χειρισμό ως παράδοση του πακέτου. Δύο σημαντικές έννοιες είναι ο τύπος της σύνδεσης και η απευθείας σε σχέση με την έμμεση παράδοση.

Τύποι σύνδεσης

Η παράδοση ενός πακέτου στο επίπεδο δικτύου επιτυγχάνεται αν χρησιμοποιούμε μία υπηρεσία με σύνδεση ή χωρίς σύνδεση.

Υπηρεσία με σύνδεση

Σε μία υπηρεσία με σύνδεση, το πρωτόκολλο του τοπικού επιπέδου δικτύου κάνει μία σύνδεση αρχικά με το πρωτόκολλο του επιπέδου δικτύου στην απομακρυσμένη τοποθεσία πριν στείλει ένα πακέτο δεδομένων. Όταν γίνει η σύνδεση, μία σειρά πακέτων από την πηγή ως τον προορισμό μπορεί να σταλεί, το ένα μετά το άλλο. Σε αυτήν την περίπτωση, υπάρχει μία σχέση μεταξύ των πακέτων. Στέλνονται μέσω της ίδιας διαδρομής σε σειρά. Ένα πακέτο είναι λογικά συνδεδεμένο με το πακέτο που ταξιδεύει πριν από αυτό και με αυτό που ταξιδεύει μετά από αυτό. Όταν όλα τα πακέτα ενός μηνύματος έχουν παραδοθεί, η σύνδεση τερματίζεται.
Σε μία υπηρεσία με σύνδεση, η απόφαση για τη διαδρομή που θα ακολουθήσει μία σειρά πακέτων με τις ίδιες διευθύνσεις πηγής και προορισμού μπορεί να γίνει μόνο μία φορά, όταν γίνει η σύνδεση. Οι δρομολογητές δεν υπολογίζουν εκ νέου τη διαδρομή για κάθε μεμονωμένο πακέτο.

Υπηρεσία χωρίς σύνδεση

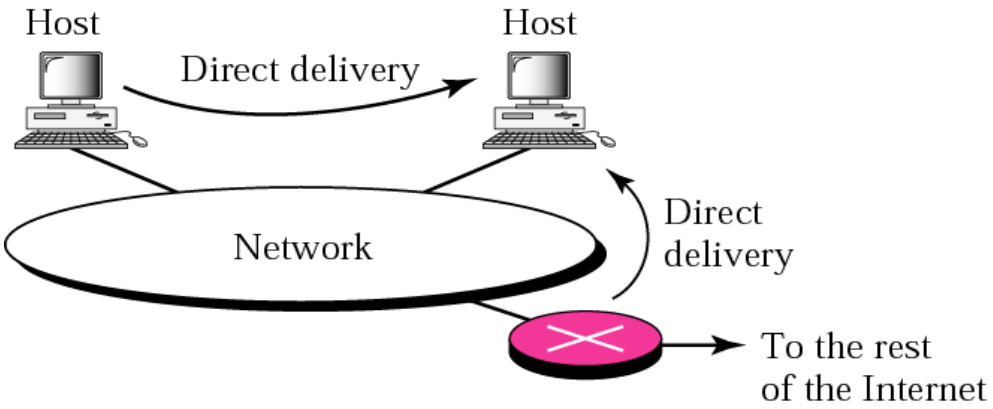
Σε μία υπηρεσία χωρίς σύνδεση, το πρωτόκολλο του επιπέδου δικτύου μεταχειρίζεται κάθε πακέτο ανεξάρτητα, με κάθε πακέτο να μην έχει σχέση με τα υπόλοιπα. Τα πακέτα σε ένα μήνυμα μπορεί να ταξιδεύουν ή όχι στην ίδια διαδρομή προς τον προορισμό τους. Σε μία υπηρεσία χωρίς σύνδεση, η απόφαση για τη διαδρομή ενός πακέτου γίνεται μεμονωμένα από κάθε δρομολογητή. Το πρωτόκολλο IP είναι ένα πρωτόκολλο χωρίς σύνδεση και παρέχει μία υπηρεσία χωρίς σύνδεση.

Άμεση εναντίον έμμεσης παράδοσης

Η παράδοση ενός πακέτου στον τελικό προορισμό του επιτυγχάνεται μέσω δύο διαφορετικών μεθόδων παράδοσης: άμεση και έμμεση.

Άμεση παράδοση

Σε μία άμεση παράδοση, ο τελικός προορισμός του πακέτου είναι ένας κεντρικός υπολογιστής που συνδέεται στο ίδιο φυσικό δίκτυο με την υπηρεσία παράδοσης. Η άμεση παράδοση συμβαίνει όταν η πηγή και ο προορισμός του πακέτου βρίσκονται στο ίδιο φυσικό δίκτυο ή αν η παράδοση είναι μεταξύ του τελευταίου δρομολογητή και του υπολογιστή προορισμού (**δείτε την Εικόνα παρακάτω**).



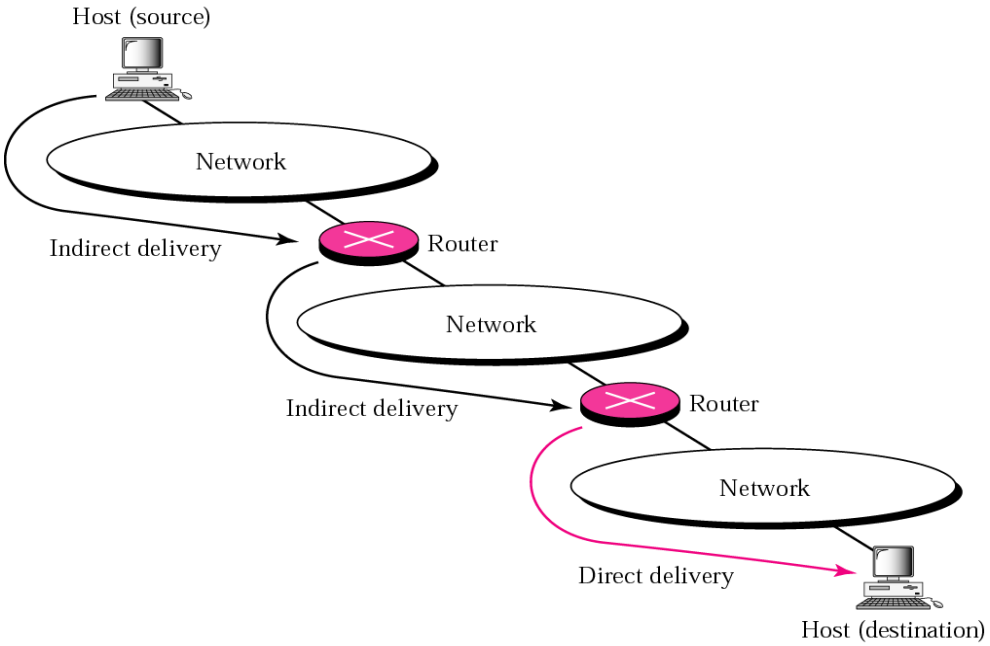
Άμεση παράδοση

Ο αποστολέας μπορεί εύκολα να αποφασίσει αν η παράδοση είναι άμεση. Μπορεί να εξάγει τη διεύθυνση δικτύου του προορισμού (χρησιμοποιώντας τη μάσκα) και να συγκρίνει αυτήν τη διεύθυνση με τις διευθύνσεις των δικτύων στα οποία είναι συνδεδεμένος. Αν βρεθεί μία ταύτιση, η παράδοση είναι άμεση.
Στην άμεση παράδοση, ο αποστολέας χρησιμοποιεί τη διεύθυνση IP του προορισμού για να βρει τη φυσική διεύθυνση προορισμού. Το λογισμικό IP δίνει μετά τη διεύθυνση IP του προορισμού μαζί με τη φυσική διεύθυνση προορισμού στο επίπεδο σύνδεσης δεδομένων για την πραγματική παράδοση. Αυτή η διαδικασία ονομάζεται αντιστοίχιση της διεύθυνσης IP στη φυσική διεύθυνση.

Έμμεση παράδοση

Αν ο υπολογιστής προορισμού δεν βρίσκεται στο ίδιο δίκτυο με τον αποστολέα, το πακέτο παραδίδεται έμμεσα. Σε μία έμμεση παράδοση, το

πακέτο πηγαίνει από δρομολογητή σε δρομολογητή μέχρι να φτάσει σε αυτόν που συνδέεται στο ίδιο φυσικό δίκτυο με τον τελικό προορισμό (**δείτε την Εικόνα παρακάτω**).



Έμμεση παράδοση

Σημειώνουμε ότι μία παράδοση πάντα περιέχει μία άμεση παράδοση αλλά καμία ή περισσότερες έμμεσες. Σημειώνουμε επίσης ότι η τελευταία παράδοση είναι πάντα άμεση.
Σε μία έμμεση παράδοση, ο αποστολέας χρησιμοποιεί τη διεύθυνση IP προορισμού και έναν πίνακα δρομολόγησης για να βρει τη διεύθυνση IP του επόμενου δρομολογητή στον οποίο πρέπει να παραδοθεί το πακέτο. Ο αποστολέας χρησιμοποιεί μετά το ARP για να βρει τη φυσική διεύθυνση του επόμενου δρομολογητή. Σημειώνουμε ότι στην άμεση παράδοση, η αντιστοίχιση διεύθυνσης βρίσκεται μεταξύ της διεύθυνσης IP του τελικού προορισμού και της φυσικής διεύθυνσης του τελικού προορισμού. Σε μία έμμεση παράδοση, η αντιστοίχιση διεύθυνσης βρίσκεται μεταξύ της διεύθυνσης IP του επόμενου δρομολογητή και της φυσικής διεύθυνσης του επόμενου δρομολογητή.

4.2 ΠΡΟΩΘΗΣΗ

Προώθηση είναι η τοποθέτηση του πακέτου στη διαδρομή του προς τον προορισμό του. Η προώθηση απαιτεί από έναν κεντρικό υπολογιστή ή ένα δρομολογητή να έχει έναν πίνακα δρομολόγησης. Όταν ένας υπολογιστής

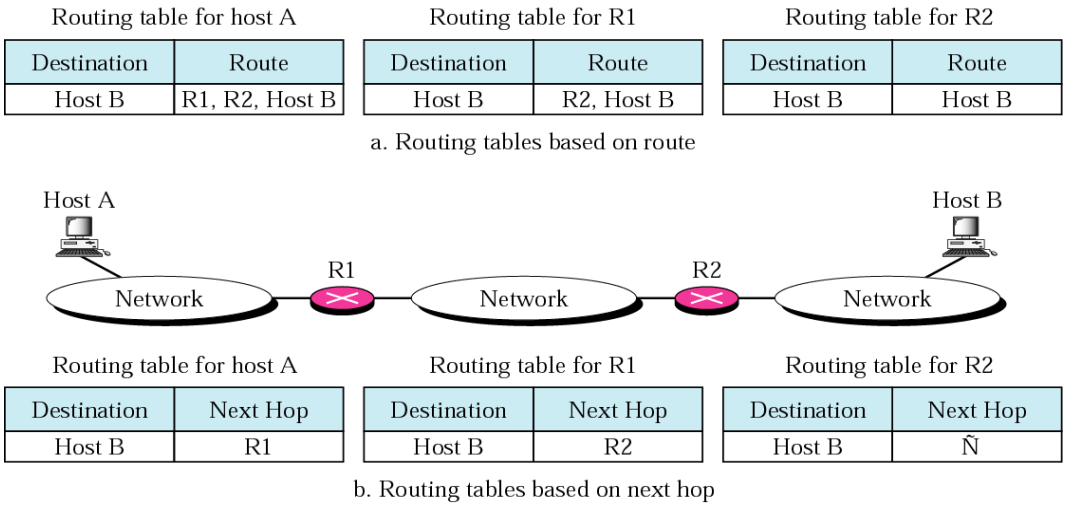
πρέπει να στείλει ένα πακέτο ή όταν ένας δρομολογητής δέχεται ένα πακέτο που πρέπει να προωθηθεί, παρατηρεί τον πίνακα για να βρει τη διαδρομή προς τον τελικό προορισμό. Αυτή η απλή λύση όμως δεν είναι δυνατή σήμερα σε ένα διαδίκτυο όπως το Internet επειδή ο αριθμός των εγγράφων που χρειάζονται στον πίνακα δρομολόγησης θα καθιστούσαν τις αναζητήσεις στον πίνακα ανεπαρκείς.

Τεχνικές προώθησης

Αρκετές τεχνικές μπορούν να καταστήσουν διαχειρήσιμο το μέγεθος του πίνακα δρομολόγησης και μπορούν επίσης να χειριστούν θέματα όπως η ασφάλεια. Θα εξετάσουμε εν συντομία αυτές τις μεθόδους παρακάτω.

Μέθοδος επόμενης μεταπήδησης

Μία τεχνική μείωσης των περιεχομένων ενός πίνακα δρομολόγησης ονομάζεται μέθοδος επόμενης μεταπήδησης. Σε αυτήν την τεχνική, ο πίνακας δρομολόγησης περιέχει μόνο τη διεύθυνση της επόμενης μεταπήδησης και όχι πληροφορίες για όλη τη διαδρομή. Οι εγγραφές ενός πίνακα δρομολόγησης πρέπει να συμβαδίζουν μεταξύ τους. **Η Εικόνα παρακάτω** δείχνει πώς μπορούν να απλοποιηθούν οι πίνακες μέσω αυτής της τεχνικής.

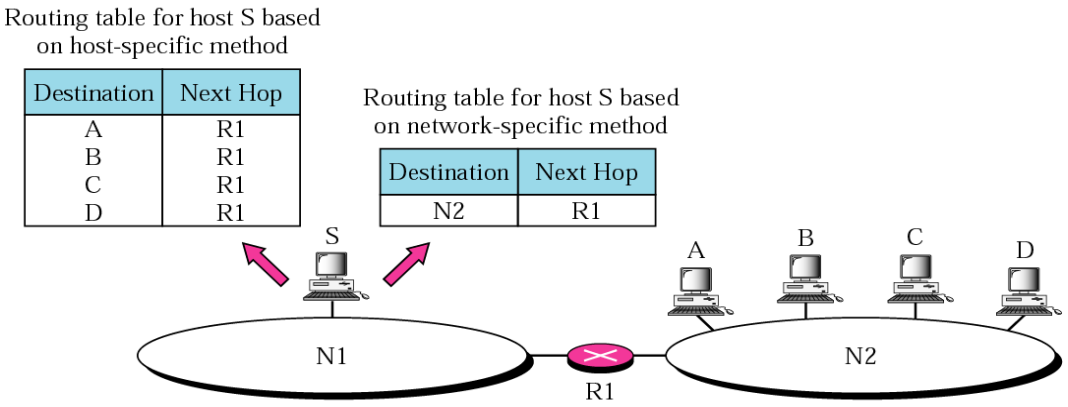


Μέθοδος επόμενου σταθμού

Μέθοδος συγκεκριμένου δικτύου

Μία δεύτερη τεχνική μείωσης του πίνακα δρομολόγησης και απλοποίησης της διαδικασίας αναζήτησης ονομάζεται μέθοδος συγκεκριμένου δικτύου. Εδώ, αντί να έχουμε μία εγγραφή για κάθε υπολογιστή προορισμού που συνδέεται στο ίδιο φυσικό δίκτυο, έχουμε μόνο μία εγγραφή που ορίζει τη

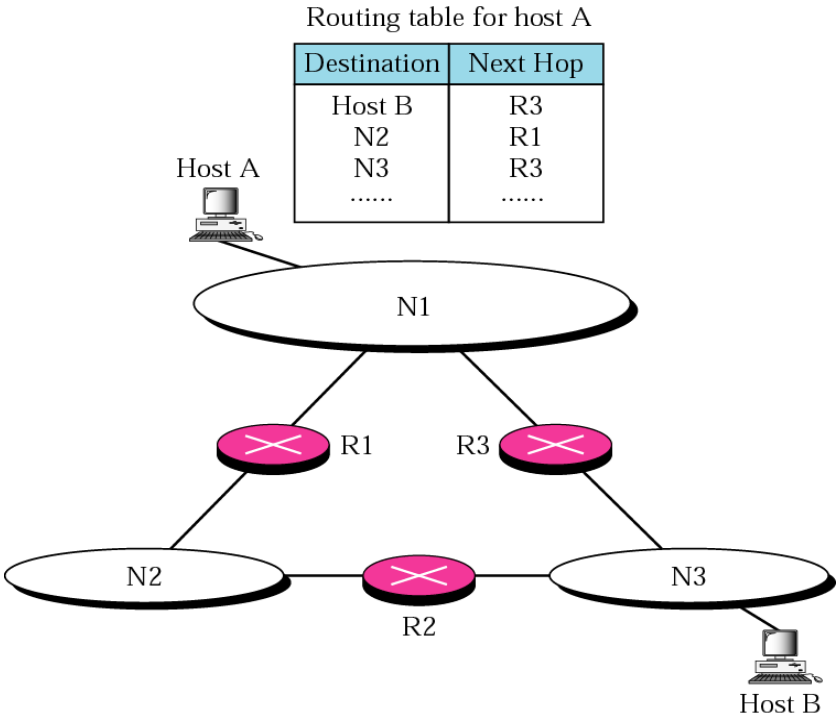
διεύθυνση του ίδιου του δικτύου προορισμού. Με άλλα λόγια, αντιμετωπίζουμε όλους τους υπολογιστές που συνδέονται στο δίκτυο ως μία εγγραφή. Για παράδειγμα, αν 1000 υπολογιστές βρίσκονται στο ίδιο δίκτυο, υπάρχει μόνο μία εγγραφή στον πίνακα δρομολόγησης και όχι 1000. **Η Εικόνα παρακάτω** δείχνει αυτό που εννοούμε.



Μέθοδος συγκεκριμένου δικτύου

Μέθοδος συγκεκριμένου υπολογιστή

Στη μέθοδο συγκεκριμένου υπολογιστή, η διεύθυνση του υπολογιστή προορισμού δίνεται στον πίνακα δρομολόγησης. Η λογική πίσω από αυτήν τη μέθοδο είναι η αντίστροφη της μεθόδου συγκεκριμένου δικτύου. Εδώ θυσιάζεται η αποδοτικότητα υπέρ άλλων πλεονεκτημάτων: αν και δεν είναι αποδοτικό να τοποθετούμε τη διεύθυνση υπολογιστή στον πίνακα δρομολόγησης, υπάρχουν περιπτώσεις όπου ο διαχειριστής θέλει να έχει περισσότερο έλεγχο επί της δρομολόγησης. Για παράδειγμα, **στην Εικόνα παρακάτω** αν ο διαχειριστής θέλει όλα τα πακέτα που φτάνουν για τον υπολογιστή B να παραδίδονται στον δρομολογητή R3 αντί του R1, μία μόνο εγγραφή στον πίνακα δρομολόγησης του υπολογιστή A μπορεί να ορίσει ρητά τη διαδρομή.

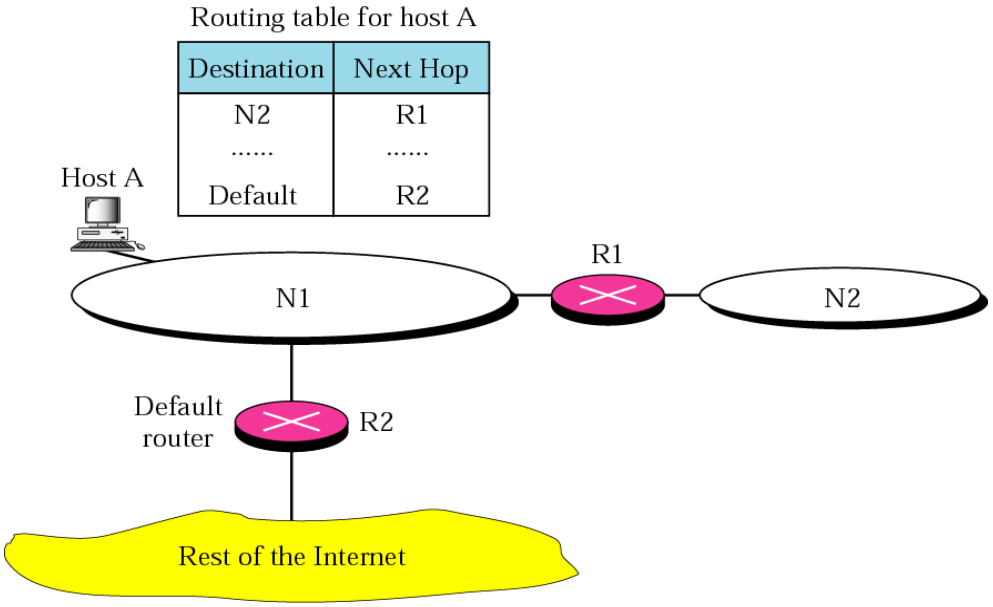


Μέθοδος συγκεκριμένου υπολογιστή

Η δρομολόγηση συγκεκριμένου υπολογιστή χρησιμοποιείται για λόγους ελέγχου της διαδρομής ή παροχής μέτρων ασφαλείας.

Προκαθορισμένη μέθοδος

Μία άλλη τεχνική απλοποίησης της δρομολόγησης ονομάζεται προκαθορισμένη μέθοδος. Στην **Εικόνα παρακάτω** ο υπολογιστής Α συνδέεται σε ένα δίκτυο με δύο δρομολογητές. Ο δρομολογητής R1 προωθεί τα πακέτα σε υπολογιστές που συνδέονται στο δίκτυο N2. Για το υπόλοιπο Internet όμως, χρησιμοποιείται ο δρομολογητής R2. Αντί λοιπόν να τοποθετεί στον πίνακα όλα τα δίκτυα για όλο το Internet, ο υπολογιστής Α μπορεί να έχει μόνο μία εγγραφή που ονομάζεται προκαθορισμένη (ορίζεται κανονικά ως διεύθυνση δικτύου 0.0.0.0).



Πίνακας δρομολόγησης για τον υπολογιστή Α

4.3 ΔΡΟΜΟΛΟΓΗΣΗ

Η δρομολόγηση αντιμετωπίζει τα θέματα της δημιουργίας και συντήρησης των πινάκων δρομολόγησης.

Πίνακες στατικής δρομολόγησης εναντίον πινάκων δυναμικής δρομολόγησης.

Ένας υπολογιστής ή ένας δρομολογητής έχει έναν πίνακα δρομολόγησης με μία εγγραφή ανά προορισμό ή ένα συνδυασμό προορισμών για να δρομολογεί πακέτα IP. Ο πίνακας δρομολόγησης μπορεί να είναι στατικός ή δυναμικός.

Στατικός πίνακας δρομολόγησης

Ένας στατικός πίνακας δρομολόγησης περιέχει πληροφορίες που εισάγονται μηχανικά. Ο διαχειριστής εισάγει τη διαδρομή για κάθε προορισμό μέσα στον πίνακα. Όταν δημιουργείται ένας πίνακας, δεν μπορεί να ενημερωθεί αυτόματα όταν υπάρχει αλλαγή στο Internet. Ο πίνακας μπορεί να αλλάξει μηχανικά από το διαχειριστή. Ένας στατικός πίνακας δρομολόγησης μπορεί να χρησιμοποιηθεί σε ένα μικρό διαδίκτυο που δεν αλλάζει συχνά ή σε ένα πειραματικό διαδίκτυο για αντιμετώπιση προβλημάτων. Δεν είναι καλή στρατηγική να χρησιμοποιούμε έναν στατικό πίνακα δρομολόγησης σε ένα μεγάλο διαδίκτυο όπως είναι το Internet.

Δυναμικός πίνακας δρομολόγησης

Ένας δυναμικός πίνακας δρομολόγησης ενημερώνεται τακτικά χρησιμοποιώντας ένα από τα πρωτόκολλα δυναμικής δρομολόγησης όπως τα RIP, OSPF και BGP. Κάθε φορά που υπάρχει μία αλλαγή στο Internet, όπως το κλείσιμο ενός δρομολογητή ή η διακοπή μίας γραμμής, τα πρωτόκολλα δυναμικής δρομολόγησης ενημερώνουν όλους τους πίνακες στους δρομολογητές (και σταδιακά στον υπολογιστή) αυτόματα.
Οι δρομολογητές σε ένα μεγάλο διαδίκτυο όπως το Internet πρέπει να ενημερώνονται δυναμικά για αποτελεσματική παράδοση των πακέτων IP.

Πίνακας δρομολόγησης

Μερικοί σύγχρονοι δρομολογητές έχουν αρκετές στήλες. Θα πρέπει να γνωρίζουμε ότι ο αριθμός των στηλών εξαρτάται από τον κατασκευαστή του λογισμικού και δεν έχουν όλοι οι δρομολογητές ίδιο αριθμό στηλών. Η **Εικόνα παρακάτω** δείχνει μερικές κοινές στήλες στους σύγχρονους δρομολογητές.

Mask	Network address	Next-hop address	Interface	Flags	Reference count	Use
.....	.....	.....	.....	.....	.....	.....

Κοινά πεδία σε έναν πίνακα δρομολόγησης

- **Μάσκα.** Αυτό το πεδίο ορίζει τη μάσκα που εφαρμόζεται για την εγγραφή.
- **Διεύθυνση δικτύου.** Αυτό το πεδίο ορίζει τη διεύθυνση δικτύου στην οποία παραδίδεται τελικά το πακέτο. Στην περίπτωση της δρομολόγησης συγκεκριμένου υπολογιστή, αυτό το πεδίο ορίζει τη διεύθυνση του υπολογιστή προορισμού.
- **Διεύθυνση επόμενου σταθμού.** Αυτό το πεδίο ορίζει τη διεύθυνση του επόμενου σταθμού στο οποίο παραδίδεται το πακέτο.
- **Διεπαφή.** Αυτό το πεδίο δείχνει το όνομα της διεπαφής.
- **Σημαίες.** Αυτό το πεδίο ορίζει έως και πέντε σημαίες. Οι σημαίες είναι διακόπτες on/off που δηλώνουν παρουσία ή απουσία. Οι πέντε σημαίες είναι U (πάνω), G (θύρα εξόδου), H (συγκεκριμένος υπολογιστής), D (προστίθεται από ανακατεύθυνση) και M (τροποποιείται από ανακατεύθυνση).

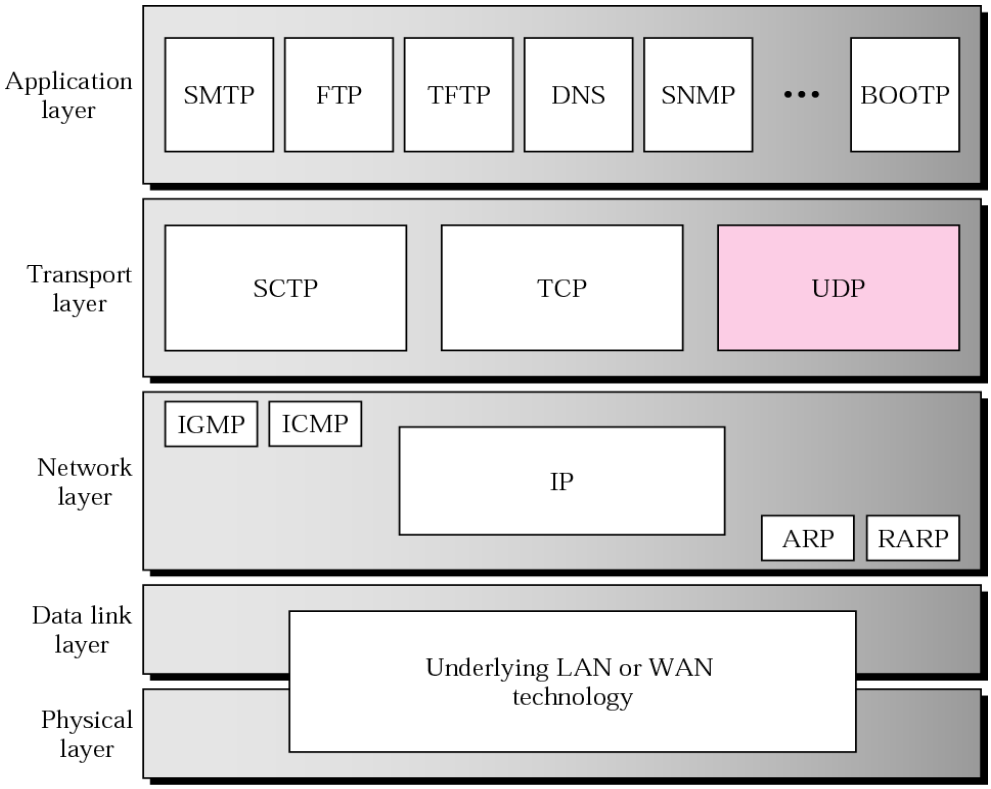
α. U (πάνω). Η σημαία U δηλώνει ότι ο δρομολογητής εκτελείται. Αν αυτή η σημαία δεν υπάρχει, αυτό σημαίνει ότι ο δρομολογητής δεν λειτουργεί. Το πακέτο δεν μπορεί να προωθηθεί και απορρίπτεται.

β. G (θύρα εξόδου). Η σημαία G σημαίνει ότι ο προορισμός βρίσκεται σε άλλο δίκτυο. Το πακέτο παραδίδεται στο δρομολογητή του επόμενου σταθμού προς παράδοση (έμμεση παράδοση). Όταν η σημαία λείπει, σημαίνει ότι ο προορισμός βρίσκεται στο ίδιο δίκτυο (άμεση παράδοση).
γ. Η (συγκεκριμένος υπολογιστής). Η σημαία Η δείχνει ότι η εγγραφή στο πεδίο διεύθυνσης δικτύου είναι μία διεύθυνση συγκεκριμένου υπολογιστή. Όταν λείπει, αυτό σημαίνει ότι η διεύθυνση είναι μόνο η διεύθυνση δικτύου του προορισμού.
δ. D (προστίθεται από ανακατεύθυνση). Η σημαία D δείχνει ότι έχουν προστεθεί πληροφορίες για αυτόν τον προορισμό στον πίνακα δρομολόγησης του υπολογιστή από ένα μήνυμα ανακατεύθυνσης από το ICMP.
ε. Μ (τροποποιείται από ανακατεύθυνση). Η σημαία Μ δείχνει ότι έχουν τροποποιηθεί πληροφορίες για αυτόν τον προορισμό στον πίνακα δρομολόγησης του υπολογιστή από ένα μήνυμα ανακατεύθυνσης από το ICMP.

- **Μετρητής αναφορών.** Αυτό το πεδίο δίνει τον αριθμό των χρηστών που χρησιμοποιούν αυτήν την διαδρομή την παρούσα στιγμή. Για παράδειγμα, αν πέντε χρήστες είναι συνδεδεμένοι ταυτόχρονα με τον ίδιο υπολογιστή από αυτόν το δρομολογητή, η τιμή σε αυτήν τη στήλη είναι 5.
- **Χρήση.** Αυτό το πεδίο δείχνει τον αριθμό των πακέτων που μεταδίδονται μέσω αυτού του δρομολογητή για τον αντίστοιχο προορισμό.

5 User Datagram Protocol (UDP)

Η Εικόνα παρακάτω παρουσιάζει τη σχέση του UDP με τα άλλα πρωτόκολλα και επίπεδα του πακέτου TCP/IP: το UDP βρίσκεται μεταξύ του επιπέδου εφαρμογής και του επιπέδου IP και όπως και το TCP, εξυπηρετεί ως ενδιάμεσος μεταξύ των προγραμμάτων εφαρμογής και των λειτουργιών του δικτύου.



Θέση του UDP στα πρωτόκολλα TCP/IP

Ένα πρωτόκολλο επιπέδου μεταφοράς έχει συνήθως αρκετές ευθύνες. Μία είναι η δημιουργία μίας επικοινωνίας από διαδικασία σε διαδικασία (μία διαδικασία είναι ένα τρέχον πρόγραμμα εφαρμογής). Το UDP χρησιμοποιεί αριθμούς θυρών για να το επιτύχει. Μία άλλη ευθύνη είναι η παροχή μηχανισμών ελέγχου στο επίπεδο μεταφοράς. Το UDP εκτελεί αυτήν την ενέργεια σε πολύ ελάχιστο βαθμό. Δεν υπάρχει μηχανισμός ελέγχου ροής και δεν υπάρχει επιβεβαίωση για τα ληφθέντα πακέτα. Το UDP όμως, παρέχει έλεγχο λαθών σε κάποιο βαθμό. Αν το UDP ανιχνεύσει ένα λάθος στο ληφθέν πακέτο, το απομακρύνει σιωπηρά.

Το επίπεδο μεταφοράς επίσης παρέχει ένα μηχανισμό σύνδεσης για τις διαδικασίες. Οι διαδικασίες πρέπει να μπορούν να στέλνουν ροές δεδομένων στο επίπεδο μεταφοράς. Είναι ευθύνη του επιπέδου μεταφοράς στο σταθμό που στέλνει τα δεδομένα να κάνει τη σύνδεση με τον παραλήπτη, να κόψει τη

ροή σε μονάδες μεταφοράς, να τις αριθμήσει και να τις στείλει τη μία μετά την άλλη. Είναι ευθύνη του επιπέδου μεταφοράς στον παραλήπτη να περιμένει μέχρι όλες οι διαφορετικές μονάδες που ανήκουν στην ίδια διαδικασία να φτάσουν, να ελεγχθούν και να περάσουν μόνο αυτές που δεν έχουν λάθη και τέλος, να παραδοθούν στον παραλήπτη ως ροή. Αφού σταλεί όλη η ροή, το επίπεδο μεταφοράς κλείνει τη σύνδεση. Το UDP δεν κάνει τίποτα από τα παραπάνω. Μπορεί να λάβει μόνο μία μονάδα δεδομένων από τις διαδικασίες και να τις παραδώσει, αναξιόπιστα στον παραλήπτη. Η μονάδα δεδομένων πρέπει να είναι αρκετά μικρή για να χωράει σε ένα πακέτο UDP.

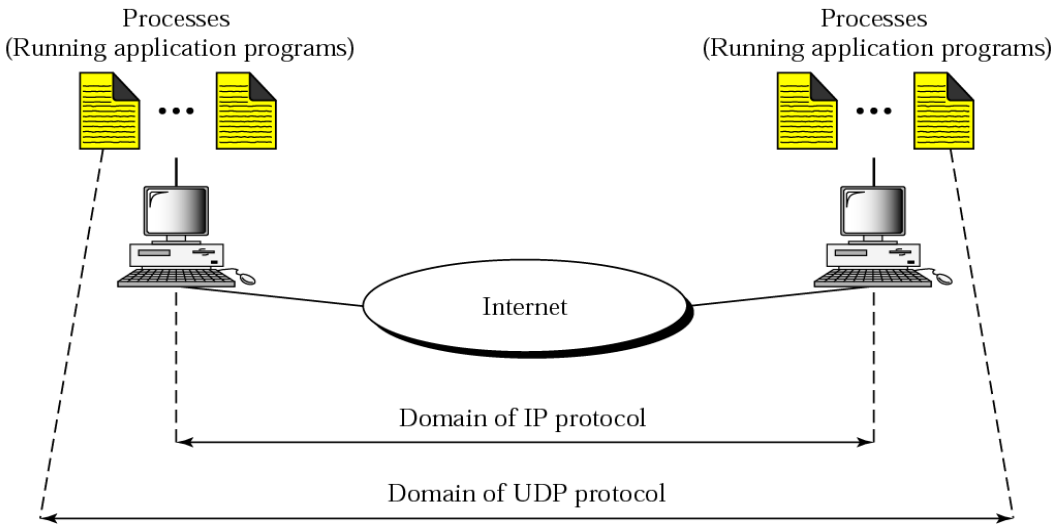
Το UDP ονομάζεται χωρίς σύνδεση, αναξιόπιστο πρωτόκολλο μεταφοράς. Δεν προσθέτει τίποτα στις υπηρεσίες του IP εκτός από την παροχή επικοινωνίας από διαδικασία σε διαδικασία αντί της επικοινωνίας από κεντρικό υπολογιστή σε κεντρικό υπολογιστή. Επίσης, εκτελεί πολύ περιορισμένο έλεγχο λαθών.

Αν το UDP είναι τόσο ανίσχυρο, γιατί να το χρησιμοποιεί μία διαδικασία; Με τα μειονεκτήματα προκύπτουν και κάποια πλεονεκτήματα. Το UDP είναι ένα πολύ απλό πρωτόκολλο, το οποίο επιφέρει ελάχιστη επιβάρυνση. Αν μία διαδικασία θέλει να στείλει ένα μικρό μήνυμα και δεν ενδιαφέρεται για αξιοπιστία, μπορεί να χρησιμοποιήσει το UDP. Η αποστολή ενός μικρού μηνύματος μέσω UDP προκαλεί ελάχιστες αλληλεπιδράσεις μεταξύ αποστολέα και παραλήπτη σε σχέση με το TCP.

5.1 ΕΠΙΚΟΙΝΩΝΙΑ ΑΠΟ ΔΙΑΔΙΚΑΣΙΑ ΣΕ ΔΙΑΔΙΚΑΣΙΑ

Πριν εξετάσουμε το UDP, πρέπει πρώτα να καταλάβουμε την επικοινωνία κεντρικού υπολογιστή με κεντρικό υπολογιστή και την επικοινωνία από διαδικασία σε διαδικασία και τη διαφορά μεταξύ τους.

Το IP είναι υπεύθυνο για την επικοινωνία στο επίπεδο υπολογιστών (επικοινωνία κεντρικού υπολογιστή με κεντρικό υπολογιστή). Ως ένα πρωτόκολλο επιπέδου δικτύου, το IP μπορεί να παραδώσει το μήνυμα μόνο στον υπολογιστή προορισμού. Αυτή όμως η παράδοση είναι ανολοκλήρωτη. Το μήνυμα πρέπει να παραδοθεί στη σωστή διαδικασία. Εδώ αναλαμβάνει ένα πρωτόκολλο επιπέδου μεταφοράς όπως το UDP. Το UDP είναι υπεύθυνο για την παράδοση του μηνύματος στην κατάλληλη διαδικασία. **Η Εικόνα παρακάτω** παρουσιάζει τους τομείς των IP και UDP.



UDP εναντίον IP

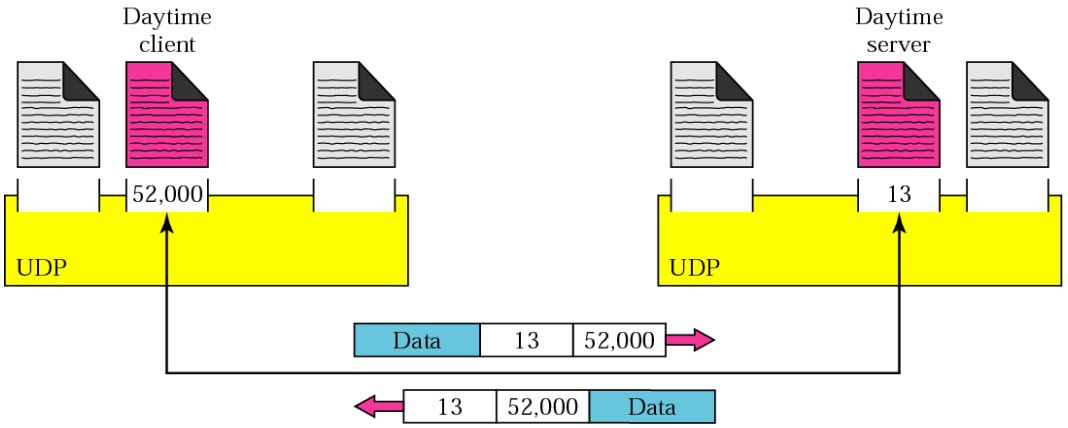
Αριθμοί θυρών

Αν και υπάρχουν αρκετοί τρόποι για να επιτευχθεί επικοινωνία από διαδικασία σε διαδικασία, ο πιο γνωστός είναι το σχήμα client-server (εξυπηρετούμενος-εξυπηρέτης). Μία διαδικασία στον τοπικό κεντρικό υπολογιστή, η οποία ονομάζεται client, χρειάζεται υπηρεσίες από μία διαδικασία που βρίσκεται συνήθως στον απομακρυσμένο κεντρικό υπολογιστή και η οποία ονομάζεται server.
Και οι δύο διαδικασίες (client και server) έχουν το ίδιο όνομα. Για παράδειγμα, για να πάρουμε την ημέρα και την ώρα από έναν απομακρυσμένο υπολογιστή, πρέπει να εκτελείται η διαδικασία client Daytime στον τοπικό κεντρικό υπολογιστή και η διαδικασία server Daytime στον απομακρυσμένο υπολογιστή. Τα λειτουργικά συστήματα όμως πλέον, υποστηρίζουν τα περιβάλλοντα πολλών χρηστών και πολλών προγραμμάτων. Ένας απομακρυσμένος υπολογιστής μπορεί να εκτελεί πολλά προγράμματα server ταυτόχρονα, όπως και αρκετοί τοπικοί υπολογιστές μπορούν να εκτελούν ένα ή περισσότερα προγράμματα client ταυτόχρονα. Για την επικοινωνία πρέπει να ορίσουμε τα εξής:

- Τοπικός κεντρικός υπολογιστής
- Τοπική διαδικασία
- Απομακρυσμένος κεντρικός υπολογιστής
- Απομακρυσμένη διαδικασία

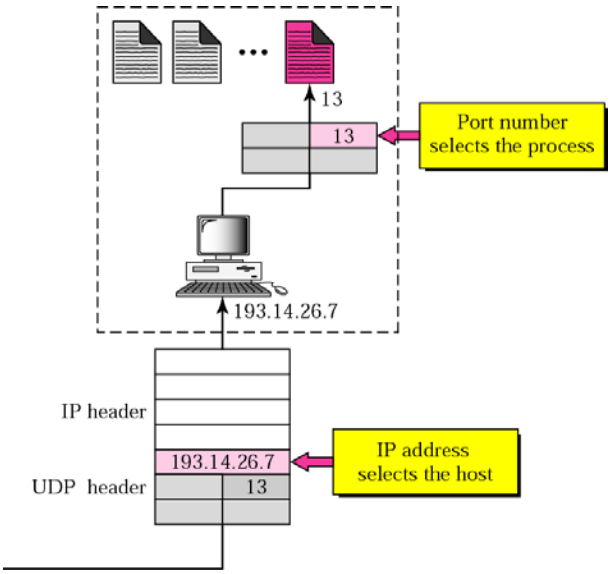
Ο τοπικός κεντρικός υπολογιστής και ο απομακρυσμένος κεντρικός υπολογιστής ορίζεται μέσα από διευθύνσεις IP. Για να οριστούν οι διαδικασίες, πρέπει να έχουμε ένα δεύτερο αναγνωριστικό, τους αριθμούς θυρών. Στα πρωτόκολλα TCP/IP, οι αριθμοί θυρών είναι ακέραιοι μεταξύ 0 και 65.535. Το πρόγραμμα client ορίζει τον εαυτό του με έναν αριθμό θύρας, τον εφήμερο αριθμό θύρας. Η λέξη εφήμερος σημαίνει με περιορισμένο χρόνο ζωής και χρησιμοποιείται επειδή η ζωή ενός client είναι συνήθως

μικρή. Ένας εφήμερος αριθμός θύρας θα πρέπει να είναι μεγαλύτερος από 1023 για κάποια προγράμματα client/server για να λειτουργούν κανονικά.
Η διαδικασία server πρέπει επίσης να ορίζει τον εαυτό της με έναν αριθμό θύρας. Αυτός ο αριθμός θύρας όμως, δεν μπορεί να επιλεχθεί τυχαία. Αν ο υπολογιστής στο server εκτελεί μία διαδικασία server και εκχωρεί έναν τυχαίο αριθμό ως αριθμό θύρας, η διαδικασία στο client που θέλει να προσπελάσει αυτό το server και να χρησιμοποιήσει τις υπηρεσίες του, δεν θα γνωρίζει τον αριθμό θύρας. Μία λύση θα ήταν να στέλνει ένα ειδικό πακέτο και να αιτείται τον αριθμό θύρας ενός συγκεκριμένου server, αυτό όμως δημιουργεί μεγαλύτερη επιβάρυνση. Το TCP/IP έχει αποφασίσει να χρησιμοποιεί καθολικούς αριθμούς θυρών για τους servers, οι οποίοι ονομάζονται γνωστοί αριθμοί θυρών. Υπάρχουν μερικές εξαιρέσεις σε αυτόν τον κανόνα, όπως για παράδειγμα, υπάρχουν clients στους οποίους έχουν αποδοθεί γνωστοί αριθμοί θυρών. Κάθε διαδικασία client γνωρίζει το γνωστό αριθμό θύρας της αντίστοιχης διαδικασίας server. Για παράδειγμα, ενώ η διαδικασία client Daytime, που αναφέραμε παραπάνω, μπορεί να χρησιμοποιήσει τον εφήμερο (προσωρινό) αριθμό θύρας 52.000 για να αναγνωρίσει τον εαυτό της, η διαδικασία server Daytime πρέπει να χρησιμοποιήσει το γνωστό (μόνιμο) αριθμό θύρας 13. **Η Εικόνα παρακάτω** παρουσιάζει αυτήν την έννοια.



Αριθμοί θυρών

Πρέπει να έχει καταστεί σαφές ότι οι διευθύνσεις IP και οι αριθμοί θυρών παίζουν διαφορετικό ρόλο στην επιλογή του τελικού προορισμού των δεδομένων. Η διεύθυνση προορισμού IP ορίζει τον κεντρικό υπολογιστή μεταξύ των διαφορετικών κεντρικών υπολογιστών στον κόσμο. Αφού επιλεχθεί ο κεντρικός υπολογιστής, ο αριθμός θύρας ορίζει μία από τις διαδικασίες σε αυτόν το συγκεκριμένο κεντρικό υπολογιστή. (**δείτε την εικόνα παρακάτω**).



Διευθύνσεις IP εναντίον αριθμών θυρών

Γνωστές θύρες για το UDP

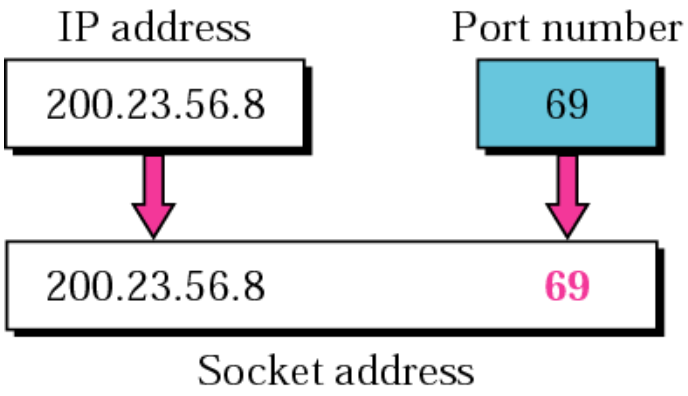
Ο πίνακας παρακάτω παρουσιάζει μερικούς γνωστούς αριθμούς θυρών που χρησιμοποιούνται από το UDP. Μερικοί αριθμοί θυρών μπορούν να χρησιμοποιούνται από το UDP και από το TCP.

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
67	Bootps	Server port to download bootstrap information
68	Bootpc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

Γνωστές θύρες που χρησιμοποιούνται με το UDP

Διευθύνσεις υποδοχών

Όπως έχουμε δει, το UDP χρειάζεται δύο αναγνωριστικά, τη διεύθυνση IP και τον αριθμό θύρας, σε κάθε άκρο για να κάνει μία σύνδεση. Ο συνδυασμός μίας διεύθυνσης IP και ενός αριθμού θύρας ονομάζεται διεύθυνση υποδοχής. Η διεύθυνση υποδοχής client ορίζει τη διαδικασία client μοναδικά, όπως η διεύθυνση υποδοχής server ορίζει τη διαδικασία server μοναδικά (δείτε την Εικόνα παρακάτω).

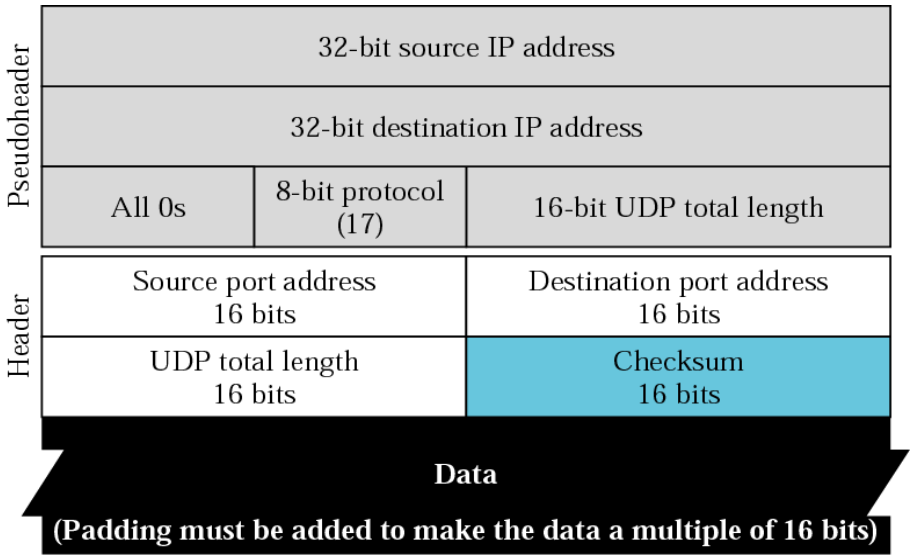


Διεύθυνση υποδοχής

Για να χρησιμοποιήσουμε τις υπηρεσίες του UDP, χρειαζόμαστε ένα ζευγάρι διευθύνσεων υποδοχών: τη διεύθυνση υποδοχής client και τη διεύθυνση υποδοχής server. Αυτές οι τέσσερις πληροφορίες είναι μέρος της κεφαλίδας IP και της κεφαλίδας UDP. Η κεφαλίδα IP περιέχει τις διευθύνσεις IP και η κεφαλίδα UDP περιέχει τους αριθμούς θυρών.

5.2 ΑΘΡΟΙΣΜΑ ΕΛΕΓΧΟΥ

Ο έλεγχος του αθροίσματος ελέγχου στο UDP είναι διαφορετικός από τα IP και ICMP. Εδώ το άθροισμα ελέγχου συμπεριλαμβάνει τρία τμήματα: μία ψευδοκεφαλίδα, την κεφαλίδα UDP και τα δεδομένα που προέρχονται από το επίπεδο εφαρμογής.
Η ψευδοκεφαλίδα είναι το τμήμα της κεφαλίδας του πακέτου IP στο οποίο το διάγραμμα δεδομένων χρήστη πρέπει να ενσωματωθεί με μερικά πεδία που συμπληρώνονται με μηδενικά (δείτε την Εικόνα παρακάτω).



Ψευδοκεφαλίδα για υπολογισμό αθροίσματος ελέγχου

Αν το άθροισμα ελέγχου δεν συμπεριλαμβάνει την ψευδοκεφαλίδα, ένα διάγραμμα δεδομένων χρήστη μπορεί να φτάσει σώο και ασφαλές. Αν όμως η κεφαλίδα IP αλλοιωθεί, μπορεί να παραδοθεί σε λάθος κεντρικό υπολογιστή.
Το πεδίο πρωτοκόλλου προστίθεται για να εξασφαλιστεί ότι το πακέτο ανήκει στο UDP και όχι στο TCP. Θα δούμε αργότερα ότι αν μία διαδικασία μπορεί να χρησιμοποιήσει ένα από τα UDP και TCP, ο αριθμός θύρας προορισμού μπορεί να είναι ο ίδιος. Η τιμή του πεδίου πρωτοκόλλου για το UDP είναι 17. Αν αυτή η τιμή αλλάξει κατά τη μετάδοση, ο υπολογισμός

αθροίσματος ελέγχου στον παραλήπτη θα την ανιχνεύσει και το UDP θα διώξει το πακέτο. Δεν θα παραδοθεί έτσι σε λάθος πρωτόκολλο.

Υπολογισμός αθροίσματος ελέγχου στον αποστολέα

Ο αποστολέας ακολουθεί τα παρακάτω 8 βήματα για να υπολογίζει το άθροισμα ελέγχου:

1. Προσθέτει την ψευδοκεφαλίδα στο διάγραμμα δεδομένων χρήστη UDP.
2. Συμπληρώνει το πεδίο αθροίσματος ελέγχου με μηδενικά.
3. Χωρίζει όλα τα bits σε λέξεις των 16 bits (2 bytes).
4. Αν ο συνολικός αριθμός των bytes δεν είναι άρτιος, προσθέτει ένα byte γεμίσματος (όλα μηδενικά). Το γέμισμα είναι μόνο για να υπολογιστεί το άθροισμα ελέγχου και θα απομακρυνθεί αμέσως μετά.
5. Προσθέτει όλα τα τμήματα των 16 bits χρησιμοποιώντας αριθμητική συμπληρώματος του ένα.
6. Συμπληρώνει το αποτέλεσμα (αλλάζει όλα τα μηδενικά σε άσσους και όλους τους άσσους σε μηδενικά), το οποίο είναι ένας αριθμός με 16 bits και το εισάγει στο πεδίο αθροίσματος ελέγχου.
7. Αφαιρεί την ψευδοκεφαλίδα και το γέμισμα που ενδεχομένως προστέθηκε.
8. Παραδίδει το διάγραμμα δεδομένων χρήστη UDP στο λογισμικό IP για ενσωμάτωση.

Σημειώνουμε ότι η σειρά των γραμμών στην ψευδοκεφαλίδα δεν αλλάζει κάτι στον υπολογισμό του αθροίσματος ελέγχου. Επίσης, η πρόσθεση μηδενικών δεν αλλάζει το αποτέλεσμα. Γι' αυτό και το λογισμικό που υπολογίζει το άθροισμα ελέγχου μπορεί να προσθέσει εύκολα όλη την κεφαλίδα IP (20 bytes) στο διάγραμμα δεδομένων UDP, να κάνει τα πρώτα bytes μηδέν, το πεδίο TTL μηδέν, να αντικαταστήσει το άθροισμα ελέγχου IP με το μήκος UDP και να υπολογίσει το άθροισμα ελέγχου. Το αποτέλεσμα θα είναι το ίδιο.

Υπολογισμός αθροίσματος ελέγχου στον παραλήπτη

Ο παραλήπτης ακολουθεί τα παρακάτω 6 βήματα για να υπολογίσει το άθροισμα ελέγχου:

1. Προσθέτει την ψευδοκεφαλίδα στο διάγραμμα δεδομένων χρήστη UDP.
2. Προσθέτει γέμισμα αν χρειάζεται.
3. Διαιρεί το σύνολο των bits σε τμήματα των 16 bits.
4. Προσθέτει όλα τα τμήματα των 16 bits χρησιμοποιώντας αριθμητική συμπληρώματος του ένα.
5. Συμπληρώνει το αποτέλεσμα.

6. Αν στο αποτέλεσμα είναι όλα μηδενικά, διώχνει την ψευδοκεφαλίδα και τυχόν επιπλέον γέμισμα και δέχεται το διάγραμμα δεδομένων χρήστη. Αν το αποτέλεσμα είναι κάτι άλλο, απορρίπτει το διάγραμμα δεδομένων χρήστη.

Προαιρετική χρήση του αθροίσματος ελέγχου

Ο υπολογισμός του αθροίσματος ελέγχου και η συμπερίληψή του σε ένα διάγραμμα δεδομένων χρήστη είναι προαιρετική. Αν το άθροισμα ελέγχου δεν υπολογίζεται, το πεδίο συμπληρώνεται μα μηδενικά. Κάποιος ίσως αναρωτηθεί, όταν το λογισμικό UDP στον υπολογιστή προορισμού λαμβάνει ένα διάγραμμα δεδομένων χρήστη με μία τιμή αθροίσματος ελέγχου μηδέν, πώς μπορεί να προσδιορίσει αν το άθροισμα ελέγχου δεν χρησιμοποιήθηκε ή αν χρησιμοποιήθηκε και το αποτέλεσμα έτυχε να είναι μόνο μηδέν; Η απάντηση είναι πολύ απλή. Αν η πηγή υπολογίζει το άθροισμα ελέγχου και το αποτέλεσμα τύχει να είναι μόνο μηδενικά, πρέπει να συμπληρωθεί. Αυτό λοιπόν που στέλνεται είναι μόνο άσσοι. Σημειώνουμε ότι ένα υπολογισμένο άθροισμα ελέγχου μπορεί να μην είναι ποτέ μόνο μηδενικά επειδή αυτό σημαίνει ότι το άθροισμα είναι μόνο άσσοι, κάτι που είναι αδύνατο στην αριθμητική συμπληρώματος του δύο.

5.3 ΛΕΙΤΟΥΡΓΙΑ UDP

Το UDP χρησιμοποιεί έννοιες που είναι ικανές με το επίπεδο μεταφοράς. Αυτές οι έννοιες θα συζητηθούν εδώ εν συντομία και θα επεκταθούμε περισσότερο στο επόμενο κεφάλαιο για το πρωτόκολλο TCP.

Υπηρεσίες χωρίς σύνδεση

Όπως αναφέραμε νωρίτερα, το UDP παρέχει μία υπηρεσία χωρίς σύνδεση. Αυτό σημαίνει ότι κάθε διάγραμμα δεδομένων χρήστη που στέλνεται από το UDP είναι ένα ανεξάρτητο διάγραμμα δεδομένων. Δεν υπάρχει σχέση μεταξύ των διαφορετικών διαγραμμάτων δεδομένων χρήστη, ακόμα κι αν προέρχονται από την ίδια διαδικασία πηγής και πηγαίνουν στο ίδιο πρόγραμμα προορισμού. Τα διαγράμματα δεδομένων χρήστη δεν είναι αριθμημένα. Επίσης, δεν έχει δημιουργηθεί καμία σύνδεση και κανένας τερματισμός σύνδεσης όπως στην περίπτωση του TCP. Αυτό σημαίνει ότι κάθε διάγραμμα δεδομένων χρήστη μπορεί να ταξιδέψει σε διαφορετική διαδρομή.
Ένα από τα παρακλάδια της κατάστασης χωρίς σύνδεση είναι ότι η διαδικασία που χρησιμοποιεί το UDP δεν μπορεί να στείλει μία ροή δεδομένων στο UDP και να περιμένει από αυτό να την χωρίσει σε διαφορετικά, σχετιζόμενα διαγράμματα δεδομένων χρήστη. Αντίθετα, κάθε

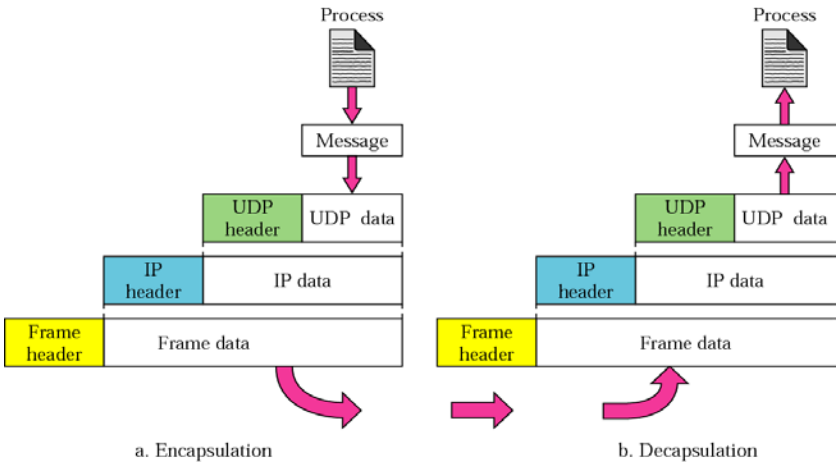
αίτηση πρέπει να είναι αρκετά μικρή ώστε να χωράει σε ένα διάγραμμα δεδομένων χρήστη. Μόνο οι διαδικασίες που στέλνουν σύντομα μηνύματα θα πρέπει να χρησιμοποιούν το UDP.

Έλεγχος ροής και λαθών

Το UDP είναι ένα πολύ απλό, αναξιόπιστο πρωτόκολλο αναφοράς. Δεν υπάρχει έλεγχος ροής και επομένως κανένας μηχανισμός παραθύρων. Ο παραλήπτης μπορεί να υπερχειλίσει με εισερχόμενα μηνύματα.
Δεν υπάρχει μηχανισμός ελέγχου λαθών στο UDP εκτός από το άθροισμα ελέγχου. Αυτό σημαίνει ότι αυτός ο αποστολέας δεν γνωρίζει αν ένα μήνυμα έχει χαθεί ή αντιγραφεί. Όταν ο παραλήπτης ανιχνεύει ένα λάθος μέσα από το άθροισμα ελέγχου, το διάγραμμα δεδομένων χρήστη απορρίπτεται σιωπηρά. Η έλλειψη ελέγχου ροής και ελέγχου λαθών σημαίνει ότι η διαδικασία που χρησιμοποιεί το UDP θα πρέπει να υποκαθιστά αυτούς τους μηχανισμούς.

Ενσωμάτωση και αφαίρεση

Για να στείλει ένα μήνυμα από μία διαδικασία σε άλλη, το πρωτόκολλο UDP ενσωματώνει και μετά αφαιρεί τα μηνύματα (**δείτε την Εικόνα παρακάτω**).



Ενσωμάτωση και αφαίρεση

Ενσωμάτωση

Όταν μία διαδικασία πρέπει να στείλει ένα μήνυμα μέσω UDP, το περνάει στο UDP μαζί με ένα ζεύγος διευθύνσεων υποδοχών και μαζί με το μήκος των δεδομένων. Το UDP λαμβάνει τα δεδομένα και προσθέτει την κεφαλίδα UDP. Το UDP περνάει στη συνέχεια το διάγραμμα δεδομένων χρήστη στο IP μαζί με τις διευθύνσεις υποδοχών. Το IP προσθέτει την δική του κεφαλίδα, χρησιμοποιώντας την τιμή 17 στο πεδίο πρωτοκόλλου, κάτι που δείχνει ότι

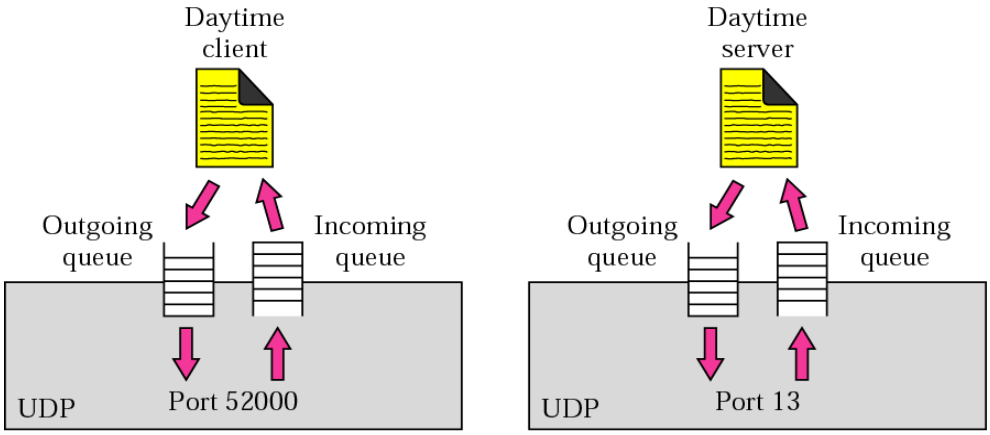
τα δεδομένα προέρχονται από το πρωτόκολλο UDP. Το διάγραμμα δεδομένων IP περνάει στο επίπεδο σύνδεσης δεδομένων. Το επίπεδο σύνδεσης δεδομένων λαμβάνει το διάγραμμα δεδομένων IP, προσθέτει τη δική του κεφαλίδα (και πιθανώς μία ουρά) και το περνάει στο φυσικό επίπεδο. Το φυσικό επίπεδο κωδικοποιεί τα bits σε ηλεκτρικά ή οπτικά σήματα και τα στέλνει στην απομακρυσμένη συσκευή.

Αφαίρεση

Όταν το μήνυμα φτάνει στον κεντρικό υπολογιστή προορισμού, το φυσικό επίπεδο αποκωδικοποιεί τα σήματα σε bits και το περνάει στο επίπεδο σύνδεσης δεδομένων. Το επίπεδο σύνδεσης δεδομένων χρησιμοποιεί την κεφαλίδα (και την ουρά) για να ελέγξει τα δεδομένα. Αν δεν υπάρχει λάθος, η κεφαλίδα και η ουρά απομακρύνονται και το διάγραμμα δεδομένων περνάει στο IP. Το λογισμικό IP κάνει το δικό του έλεγχο. Αν δεν υπάρχει λάθος, η κεφαλίδα απομακρύνεται και το διάγραμμα δεδομένων χρήστη περνάει στο UDP με τις διευθύνσεις IP του αποστολέα και του παραλήπτη. Το UDP χρησιμοποιεί το άθροισμα ελέγχου για να ελέγξει όλο το διάγραμμα δεδομένων χρήστη. Αν δεν υπάρχει λάθος, η κεφαλίδα απομακρύνεται και τα δεδομένα εφαρμογής μαζί με τη διεύθυνση υποδοχής του αποστολέα περνάνε στη διαδικασία. Η διεύθυνση υποδοχής του αποστολέα περνάει στη διαδικασία σε περίπτωση που θα χρειαστεί να απαντήσει στο ληφθέν μήνυμα.

Τοποθέτηση σε ουρά

Μιλήσαμε για τις θύρες χωρίς όμως να αναφερθούμε στην υλοποίησή τους. Στο UDP, οι ουρές σχετίζονται με τις θύρες (**δείτε την Εικόνα παρακάτω**).
Στον client, όταν μία διαδικασία ξεκινά, αιτείται έναν αριθμό θυρών από το λειτουργικό σύστημα. Μερικές υλοποιήσεις δημιουργούν μία εισερχόμενη και μία εξερχόμενη ουρά που σχετίζεται με κάθε διαδικασία. Άλλες υλοποιήσεις δημιουργούν μόνο μία εισερχόμενη ουρά που σχετίζεται με κάθε διαδικασία.



Ουρές στο UDP

Σημειώνουμε ότι ακόμα κι αν μία διαδικασία θέλει να επικοινωνήσει με πολλές, παίρνει μόνο έναν αριθμό θύρας και σταδιακά μία εξερχόμενη και μία εισερχόμενη ουρά. Οι ουρές που ανοίγονται από τον client, στις περισσότερες περιπτώσεις, αναγνωρίζονται από εφήμερους αριθμούς θυρών. Οι ουρές λειτουργούν όσο εκτελείται η διαδικασία. Όταν η διαδικασία τερματίζεται, οι ουρές τερματίζονται.

Η διαδικασία client μπορεί να στέλνει μηνύματα στην εξερχόμενη ουρά χρησιμοποιώντας τον αριθμό θύρας της πηγής που ορίζεται στην αίτηση. Το UDP αφαιρεί τα μηνύματα ένα προς ένα και, αφού προσθέσει την κεφαλίδα UDP, τα παραδίδει στο IP. Μία εξερχόμενη ουρά μπορεί να υπερχειλίσει. Αν συμβεί αυτό, το λειτουργικό σύστημα μπορεί να ζητήσει από τη διαδικασία client να περιμένει πριν στείλει άλλα μηνύματα.

Όταν ένα μήνυμα φτάνει για ένα client, το UDP ελέγχει αν έχει δημιουργηθεί μία εισερχόμενη ουρά για τον αριθμό ουράς που προορίζεται στο πεδίο αριθμού ουράς προορισμού του διαγράμματος δεδομένων χρήστη. Αν υπάρχει μία τέτοια ουρά, το UDP στέλνει το ληφθέν διάγραμμα δεδομένων χρήστη στο τέλος της ουράς. Αν δεν υπάρχει τέτοια ουρά, το UDP απορρίπτει το διάγραμμα δεδομένων χρήστη και ζητά από το πρωτόκολλο ICMP να στείλει ένα μήνυμα απρόσιτης θύρας στο server. Όλα τα εισερχόμενα μηνύματα για το συγκεκριμένο πρόγραμμα client, είτε προέρχονται από τον ίδιο είτε από άλλο server, στέλνονται στην ίδια ουρά. Μία εισερχόμενη ουρά μπορεί να υπερχειλίσει. Αν συμβεί αυτό, το UDP απομακρύνει το διάγραμμα δεδομένων χρήστη και ζητά να σταλεί ένα μήνυμα απρόσιτης θύρας στο server.

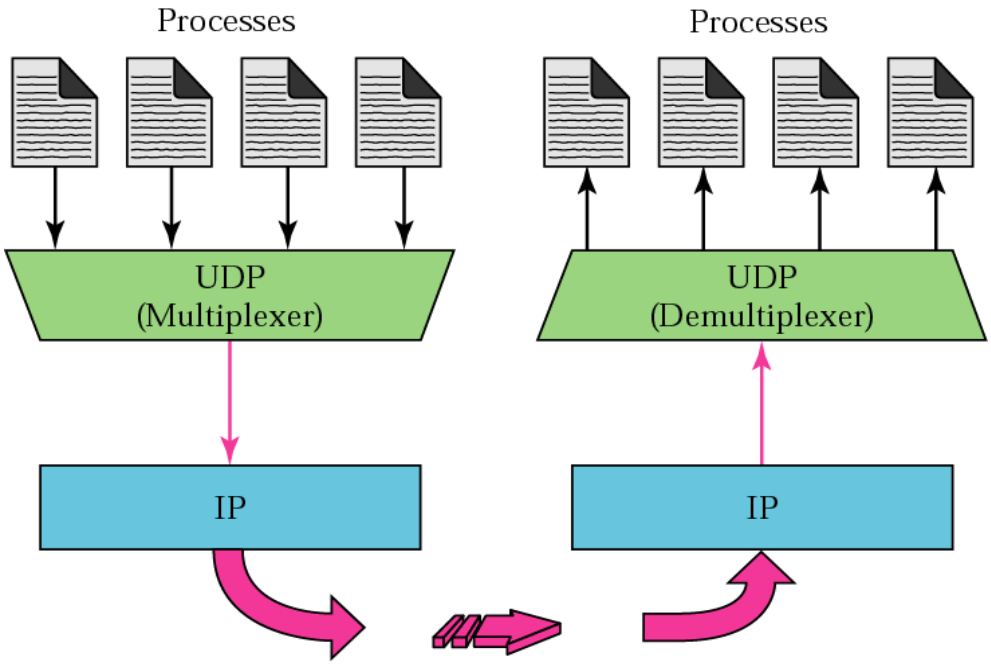
Στον server, ο μηχανισμός δημιουργίας ουρών είναι διαφορετικός. Στην απλούστερη μορφή του, ένας server ζητά εισερχόμενες και εξερχόμενες ουρές χρησιμοποιώντας τη γνωστή θύρα του όταν ξεκινά να εκτελείται. Οι ουρές παραμένουν ανοιχτές όσο εκτελείται ο server.

Όταν φτάσει ένα μήνυμα για το server, το UDP ελέγχει αν έχει δημιουργηθεί μία εισερχόμενη ουρά για τον αριθμό θύρας που ορίζεται στο πεδίο αριθμού ουράς προορισμού του διαγράμματος δεδομένων χρήστη. Αν υπάρχει μία τέτοια ουρά, το UDP στέλνει το ληφθέν διάγραμμα δεδομένων χρήστη στο τέλος της ουράς. Αν δεν υπάρχει τέτοια ουρά, το UDP απορρίπτει το

διάγραμμα δεδομένων χρήστη και ζητά από το πρωτόκολλο ICMP να στείλει ένα μήνυμα απρόσιτης θύρας στο client. Όλα τα εισερχόμενα μηνύματα για κάποιο συγκεκριμένο server, είτε προέρχονται από τον ίδιο είτε από άλλο server, στέλνονται στην ίδια ουρά. Μία εισερχόμενη ουρά μπορεί να υπερχειλίσει. Αν συμβεί αυτό, το UDP απομακρύνει το διάγραμμα δεδομένων χρήστη και ζητά να σταλεί ένα μήνυμα απρόσιτης θύρας στο client.
Όταν ένας server θέλει να απαντήσει σε ένα client, στέλνει μηνύματα στην εξερχόμενη ουρά χρησιμοποιώντας τον αριθμό θύρας της πηγής που ορίζεται στην αίτηση. Το UDP απομακρύνει τα μηνύματα ένα προς ένα και, αφού προσθέσει την κεφαλίδα UDP, τα παραδίδει στο IP. Μία εξερχόμενη ουρά μπορεί να υπερχειλίσει. Αν συμβεί αυτό, το λειτουργικό σύστημα ζητά από το server να περιμένει πριν στείλει άλλα μηνύματα.

Πολύπλεξη και αποπολύπλεξη

Σε έναν κεντρικό υπολογιστή που εκτελεί τα πρωτόκολλα TCP/IP, υπάρχει μόνο ένα UDP και πιθανώς πολλές διαδικασίες που θέλουν να χρησιμοποιήσουν τις υπηρεσίες του. Για να αντιμετωπίσει αυτήν την κατάσταση, το UDP πολυπλέκει και αποπολυπλέκει (**δείτε την Εικόνα παρακάτω**).



Πολύπλεξη και αποπολύπλεξη

Πολύπλεξη

Στον αποστολέα, μπορεί να υπάρχουν πολλές διαδικασίες που πρέπει να στείλουν διαγράμματα δεδομένων χρήστη. Υπάρχει όμως μόνο ένα UDP. Πρόκειται για μία σχέση πολλών με ένα και απαιτείται πολύπλεξη. Το UDP δέχεται μηνύματα από διαφορετικές διαδικασίες, οι οποίες διαφοροποιούνται από τον αριθμό θύρας που τους έχει εκχωρηθεί. Μετά την προσθήκη της κεφαλίδας, το UDP περνάει το διάγραμμα δεδομένων χρήστη στο IP.

Αποπολύπλεξη

Στον παραλήπτη, υπάρχει μόνο ένα UDP. Μπορούμε όμως να έχουμε πολλές διαδικασίες που μπορούν να δέχονται διαγράμματα δεδομένων χρήστη. Πρόκειται για μία σχέση ενός προς πολλούς και απαιτείται αποπολύπλεξη. Το UDP λαμβάνει διαγράμματα δεδομένων χρήστη από το IP. Μετά από τον έλεγχο λαθών και την αφαίρεση της κεφαλίδας, το UDP παραδίδει κάθε μήνυμα στην κατάλληλη διαδικασία βάσει του αριθμού θύρας.

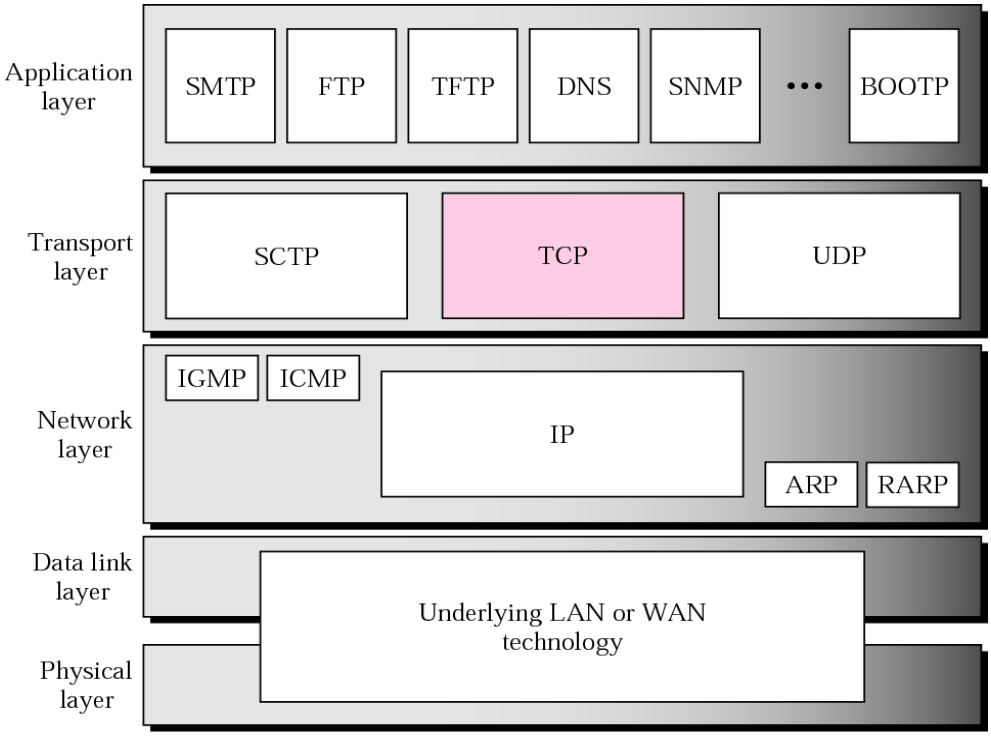
5.4 ΧΡΗΣΗ ΤΟΥ UDP

Παρακάτω βρίσκουμε μερικές χρήσεις του πρωτοκόλλου:

- Το UDP είναι κατάλληλο για μία διαδικασία που αιτείται απλή επικοινωνία αίτησης-απάντησης με μικρή ανησυχία για τον έλεγχο ροής και λαθών. Δεν χρησιμοποιείται συνήθως για μία διαδικασία όπως το FTP που πρέπει να στέλνει μαζικά δεδομένα.
- Το UDP είναι κατάλληλο για μία διαδικασία με μηχανισμούς εσωτερικής ροής και ελέγχου λαθών. Για παράδειγμα, το TFTP συμπεριλαμβάνει έλεγχο ροής και λαθών. Μπορεί εύκολα να χρησιμοποιήσει το UDP.
- Το UDP είναι ένα κατάλληλο πρωτόκολλο μεταφοράς για multicasting. Η δυνατότητα multicasting ενσωματώνεται στο λογισμικό UDP αλλά όχι στο λογισμικό TCP.
- Το UDP χρησιμοποιείται για διαχειριστικές διαδικασίες όπως το SNMP.
- Το UDP χρησιμοποιείται για μερικά πρωτόκολλα ενημέρωσης διαδρομής, όπως το RIP.

6 Transmission Control Protocol (TCP)

Παραδοσιακά, τα πρωτόκολλα TCP/IP ορίζουν δύο πρωτόκολλα για το επίπεδο μεταφοράς: τα UDP και TCP. Μελετήσαμε το UDP και τώρα θα ασχοληθούμε με το TCP.
Η Εικόνα παρακάτω παρουσιάζει τη σχέση του TCP με τα άλλα πρωτόκολλα του TCP/IP. Το TCP βρίσκεται μεταξύ του επιπέδου εφαρμογής και του επιπέδου δικτύου και εξυπηρετεί ως ενδιάμεσος μεταξύ των προγραμμάτων εφαρμογής και των λειτουργιών του δικτύου.



Πρωτόκολλα TCP/IP

Το TCP, όπως και το UDP, είναι πρωτόκολλο διαδικασίας προς διαδικασία (πρόγραμμα προς πρόγραμμα). Το TCP, επομένως, όπως και το UDP, χρησιμοποιεί αριθμούς θυρών. Αντίθετα από το UDP, το TCP είναι ένα πρωτόκολλο που βασίζεται στη σύνδεση και δημιουργεί μία εικονική σύνδεση μεταξύ δύο TCP για να στείλει δεδομένα. Επιπλέον, το TCP χρησιμοποιεί μηχανισμούς ελέγχου ροής και λαθών στο επίπεδο μεταφοράς.
Εν συντομία, το TCP ονομάζεται αξιόπιστο, με σύνδεση πρωτόκολλο μεταφοράς. Προσθέτει χαρακτηριστικά σύνδεσης και αξιοπιστίας στις υπηρεσίες του IP.

6.1 ΥΠΗΡΕΣΙΕΣ TCP

Πριν εντρυφήσουμε στο TCP, ας εξηγήσουμε τις υπηρεσίες που προσφέρονται από το TCP στις διαδικασίες στο επίπεδο εφαρμογής.

Επικοινωνία από διαδικασία σε διαδικασία

Όπως το UDP, το TCP παρέχει επικοινωνία από διαδικασία σε διαδικασία χρησιμοποιώντας αριθμούς θυρών. **Ο Πίνακας παρακάτω** καταγράφει μερικούς γνωστούς αριθμούς θυρών που χρησιμοποιούνται από το TCP.

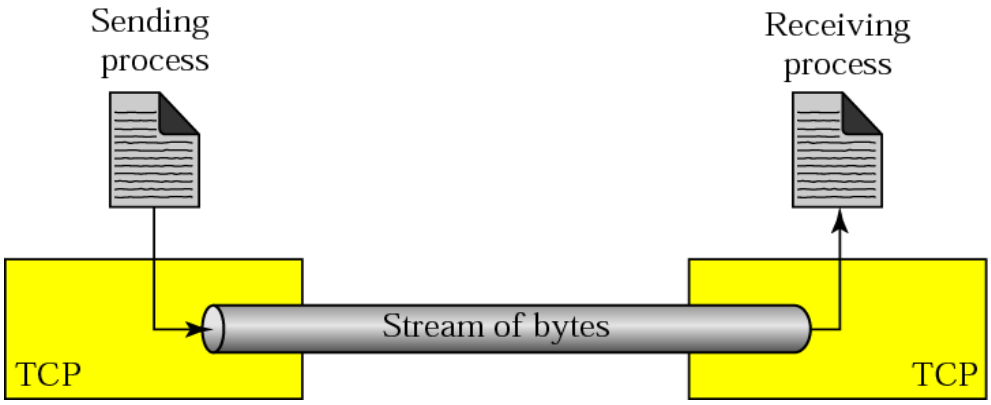
Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

Γνωστές θύρες που χρησιμοποιούνται από το TCP

Υπηρεσία παράδοσης ροής

Το TCP, αντίθετα από το UDP, είναι ένα πρωτόκολλο που βασίζεται στη ροή. Στο UDP, μία διαδικασία (ένα πρόγραμμα εφαρμογής) στέλνει μηνύματα με προκαθορισμένα όρια, στο UDP για παράδοση. Το UDP προσθέτει τη δική του κεφαλίδα σε κάθε τέτοιο μήνυμα και τα παραδίδει στο IP για μετάδοση. Κάθε μήνυμα από τη διαδικασία ονομάζεται διάγραμμα δεδομένων χρήστη και γίνεται σταδιακά ένα διάγραμμα δεδομένων IP.

Ούτε το IP ούτε το UDP αναγνωρίζουν οποιαδήποτε σχέση μεταξύ διαγραμμάτων δεδομένων. Το TCP, από την άλλη, επιτρέπει στη διαδικασία που στέλνει, να παραδίδει δεδομένα ως ροή bytes και επιτρέπει στη διαδικασία που λαμβάνει, να αποκτά δεδομένα ως μία ροή bytes. Το TCP δημιουργεί ένα περιβάλλον στο οποίο οι δύο διαδικασίες φαίνεται ότι συνδέονται από έναν φανταστικό <<σωλήνα>> που μεταφέρει τα δεδομένα τους στο Internet. Αυτό το φανταστικό περιβάλλον απεικονίζεται στην **Εικόνα παρακάτω**. Η διαδικασία που στέλνει, παράγει (γράφει) τη ροή των bytes και η διαδικασία που στέλνει καταναλώνει (διαβάζει) αυτή τη ροή.



Παράδοση ροής

Πλήρης αμφίδρομη επικοινωνία

Το TCP προσφέρει υπηρεσία πλήρους αμφίδρομης επικοινωνίας, όπου τα δεδομένα μπορούν να ρέουν προς τις δύο κατευθύνσεις ταυτόχρονα. Κάθε TCP έχει μία μνήμη αποστολής και μία μνήμη λήψης και τα τμήματα μετακινούνται προς τις δύο κατευθύνσεις.

Υπηρεσία με σύνδεση

Το TCP, αντίθετα από το UDP, είναι ένα πρωτόκολλο που βασίζεται στη σύνδεση. Όταν μία διαδικασία στο Α θέλει να στείλει και να λάβει δεδομένα από μία άλλη διαδικασία στο Β, συμβαίνουν τα εξής:

1. Τα δύο TCP ιδρύουν μία σύνδεση μεταξύ τους.
2. Τα δεδομένα ανταλλάσσονται και προς τις δύο κατευθύνσεις.
3. Η σύνδεση τερματίζεται.

Σημειώνουμε ότι αυτή είναι εικονική σύνδεση και όχι φυσική. Το τμήμα TCP ενσωματώνεται σε ένα διάγραμμα δεδομένων IP και μπορεί να σταλεί εκτός σειράς, ή να χαθεί ή να αλλοιωθεί ή να σταλεί δύο φορές. Κάθε πακέτο μπορεί να χρησιμοποιήσει διαφορετική διαδρομή για να φτάσει στον

προορισμό. Δεν υπάρχει φυσική σύνδεση. Το TCP δημιουργεί ένα περιβάλλον με ροή bytes στο οποίο δέχεται την ευθύνη της παράδοσης των bytes με την σειρά, στην άλλη συσκευή. Η κατάσταση είναι παρόμοια με τη δημιουργία μίας γέφυρας που ενώνει πολλά νησιά και περνάει όλα τα bytes από το ένα νησί στο άλλο με μία μόνα σύνδεση.

Αξιόπιστη υπηρεσία

Το TCP είναι ένα αξιόπιστο πρωτόκολλο μεταφοράς. Χρησιμοποιεί ένα μηχανισμό επιβεβαίωσης για να ελέγχει την ασφαλή άφιξη των δεδομένων. Θα συζητήσουμε για αυτό το χαρακτηριστικό στην ενότητα για τον έλεγχο λαθών.

6.2 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ TCP

Για να παρέχει τις υπηρεσίες που αναφέρθηκαν στην προηγούμενη ενότητα, το TCP διαθέτει αρκετά χαρακτηριστικά που συνοψίζονται εν συντομία σε αυτήν την ενότητα και μελετώνται αργότερα λεπτομερώς.

Σύστημα αρίθμησης

Αν και το λογισμικό TCP παρακολουθεί τα τμήματα που μεταδίδονται ή λαμβάνονται, δεν υπάρχει πεδίο για την τιμή του αριθμού ενός τμήματος στην κεφαλίδα του τμήματος. Αντίθετα, υπάρχουν δύο πεδία που ονομάζονται αριθμός σειράς και αριθμός επιβεβαίωσης. Αυτά τα δύο πεδία αναφέρουν τον αριθμό του byte και όχι τον αριθμό του τμήματος.

Αριθμός byte

Το TCP αριθμεί όλα τα bytes δεδομένων που μεταδίδονται σε μία σύνδεση. Η αρίθμηση είναι ανεξάρτητη σε κάθε κατεύθυνση. Όταν το TCP λαμβάνει bytes δεδομένων από μία διαδικασία τα αποθηκεύει στη μνήμη αποστολής και τα αριθμεί. Η αρίθμηση δεν ξεκινά απαραίτητα από το 0 αλλά αντίθετα, το TCP παράγει έναν τυχαίο αριθμό μεταξύ 0 και 2^32-1 για τον αριθμό του πρώτου byte. Για παράδειγμα, αν ο τυχαίος αριθμός τυχαίνει να είναι 1057 και τα συνολικά δεδομένα που θα σταλούν είναι 6.000 bytes, τα bytes αριθμούνται από το 1057 έως το 7.056. Θα δούμε ότι η αρίθμηση των bytes χρησιμοποιείται για έλεγχο ροής και λαθών.

Αριθμός σειράς

Αφού αριθμηθούν τα bytes, το TCP εκχωρεί έναν αριθμό σειράς σε κάθε τμήμα που στέλνεται. Ο αριθμός σειράς για κάθε τμήμα είναι ο αριθμός του πρώτου byte που μεταφέρεται σε αυτό το τμήμα.
Όταν ένα τμήμα μεταφέρει ένα συνδυασμό δεδομένων και πληροφορίες ελέγχου (μεταφορά ως εξωτερικό φορτίο), χρησιμοποιεί έναν αριθμό σειράς. Αν ένα τμήμα δεν μεταφέρει δεδομένα χρήστη, δεν ορίζει λογικά έναν αριθμό σειράς. Το πεδίο είναι εκεί αλλά η τιμή δεν είναι έγκυρη. Μερικά όμως τμήματα, όταν μεταφέρουν μόνο πληροφορίες ελέγχου χρειάζονται έναν αριθμό σειράς για να έχουν έτσι μία επιβεβαίωση από τον παραλήπτη. Αυτά τα τμήματα χρησιμοποιούνται για έναρξη, τερματισμό ή αναστολή σύνδεσης. Κάθε ένα από αυτά τα τμήματα καταναλώνει έναν αριθμό σειράς καθώς μεταφέρει ένα byte, δεν υπάρχουν όμως δεδομένα. Αν ο τυχαίος αριθμός σειράς είναι χ, το πρώτο byte δεδομένων έχει αριθμό χ+1. Το byte χ θεωρείται πλαστό byte που χρησιμοποιείται για να ανοίξει μία σύνδεση ένα τμήμα ελέγχου.

Αριθμός επιβεβαίωσης

Η επικοινωνία στο TCP είναι πλήρως αμφίδρομη: όταν δηλαδή ιδρύεται μία σύνδεση, και τα δύο μέρη μπορούν να στέλνουν και να λαμβάνουν δεδομένα ταυτόχρονα. Κάθε μέρος αριθμεί τα bytes, συνήθως με διαφορετικό αριθμό έναρξης. Ο αριθμός σειράς σε κάθε κατεύθυνση παρουσιάζει τον αριθμό του πρώτου byte που μεταφέρεται από το τμήμα. Κάθε μέρος επίσης χρησιμοποιεί έναν αριθμό επιβεβαίωσης για να επιβεβαιώσει ότι τα bytes ελήφθησαν. Ο αριθμός επιβεβαίωσης όμως ορίζει τον αριθμό του επόμενου byte που το μέρος περιμένει να λάβει. Επιπλέον, ο αριθμός επιβεβαίωσης είναι αθροιστικός, πράγμα που σημαίνει ότι το μέρος παίρνει τον αριθμό του τελευταίου byte που έχει λάβει, σώο και αβλαβές, προσθέτει 1 σε αυτό και ανακοινώνει αυτό το άθροισμα ως αριθμό επιβεβαίωσης. Ο όρος αθροιστικός εδώ σημαίνει
ότι αν το μέρος χρησιμοποιεί το 5.643 ως αριθμό επιβεβαίωσης, έχει δεχθεί όλα τα bytes από την αρχή έως το 5.642. Σημειώνουμε ότι αυτό δεν σημαίνει ότι το μέρος έχει λάβει 5.642 bytes επειδή ο αριθμός του πρώτου byte δεν ξεκινά απαραίτητα από το μηδέν.

Έλεγχος ροής

Το TCP, αντίθετα από το UDP, παρέχει έλεγχο ροής. Ο παραλήπτης των δεδομένων ελέγχει πόσα δεδομένα στέλνονται από τον αποστολέα. Αυτό γίνεται για να αποτραπεί η υπερφόρτωση του παραλήπτη με δεδομένα. Το σύστημα αρίθμησης επιτρέπει στο TCP να χρησιμοποιεί έλεγχο ροής που βασίζεται σε bytes.

Έλεγχος λαθών

Για να παρέχει αξιόπιστη υπηρεσία, το TCP υλοποιεί ένα μηχανισμό ελέγχου λαθών. Αν και ο έλεγχος λαθών θεωρεί ένα τμήμα ως τη μονάδα δεδομένων για την ανίχνευση λαθών (απολεσθέντα ή αλλοιωμένα τμήματα), ο έλεγχος λαθών βασίζεται σε bytes.

Έλεγχος συμφόρησης

Το TCP, αντίθετα από το UDP, λαμβάνει υπόψη τη συμφόρηση στο δίκτυο. Η ποσότητα δεδομένων που στέλνεται από έναν αποστολέα δεν ελέγχεται μόνο από τον παραλήπτη (έλεγχος ροής), αλλά καθορίζεται και από το επίπεδο συμφόρησης στο δίκτυο.

6.3 ΜΙΑ TCP ΣΥΝΔΕΣΗ

Το TCP βασίζεται σε σύνδεση. Ένα πρωτόκολλο μεταφοράς που βασίζεται σε σύνδεση δημιουργεί μία εικονική διαδρομή μεταξύ πηγής και προορισμού. Όλα τα τμήματα που ανήκουν σε ένα μήνυμα στέλνονται μετά σε αυτήν την εικονική διαδρομή. Χρησιμοποιώντας μία εικονική διαδρομή για όλο το μήνυμα, διευκολύνουμε τη διαδικασία επιβεβαίωσης όπως και την αναμετάδοση καταστραμμένων ή χαμένων πλαισίων. Το σημαντικό είναι ότι μία TCP σύνδεση είναι εικονική και όχι φυσική. Το TCP λειτουργεί σε υψηλότερο επίπεδο. Το TCP χρησιμοποιεί τις υπηρεσίες του IP για να διανείμει μεμονωμένα τμήματα στον παραλήπτη αλλά ελέγχει το ίδιο τη σύνδεση. Ένα τμήμα που χάθηκε ή αλλοιώθηκε αναμεταδίδεται. Αντίθετα από το TCP, το IP δεν γνωρίζει αυτήν την αναμετάδοση. Αν ένα τμήμα φτάσει εκτός σειράς, το TCP το κρατά μέχρι να φτάσουν τα τμήματα που λείπουν –το IP δεν γνωρίζει αυτήν την αποκατάσταση της σειράς.
Στο TCP, η μετάδοση που βασίζεται σε σύνδεση απαιτεί τρεις φάσεις: έναρξη σύνδεσης, μεταφορά δεδομένων και τερματισμό σύνδεσης.

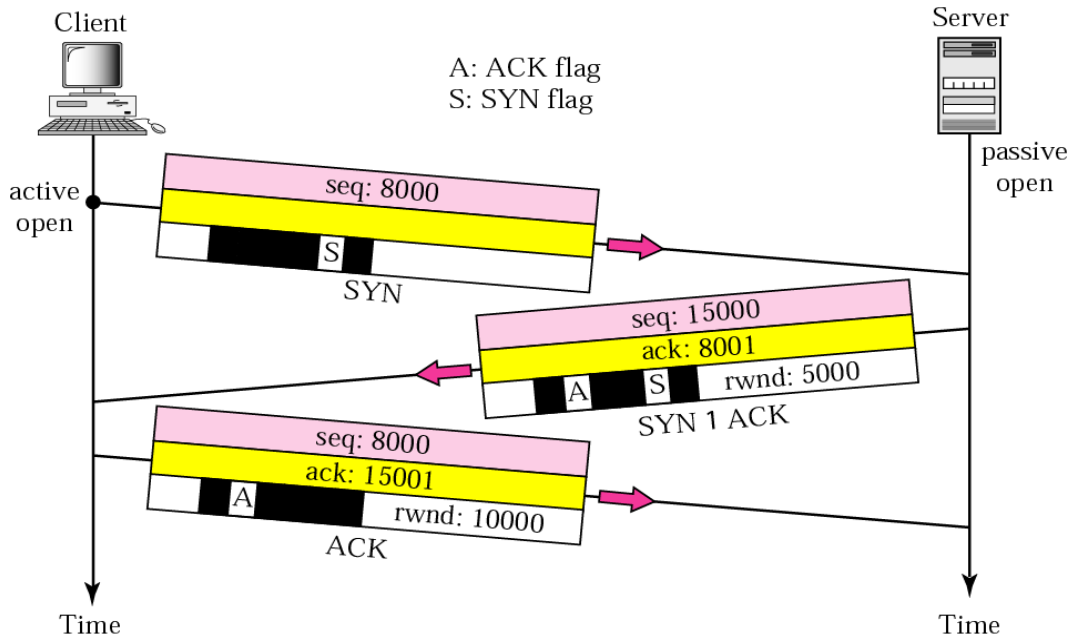
Έναρξη σύνδεσης

Το TCP μεταδίδει δεδομένα σε κατάσταση πλήρους αμφίδρομης επικοινωνίας. Όταν συνδέονται δύο TCP σε δύο συσκευές, μπορούν να στέλνουν τμήματα η μία στην άλλη ταυτόχρονα. Αυτό δείχνει ότι κάθε τμήμα πρέπει να αρχικοποιήσει την επικοινωνία και να πάρει έγκριση από το άλλο μέρος πριν αρχίσουν να μεταδίδονται δεδομένα.

Χαιρετισμός τριών τρόπων

Η έναρξη της σύνδεσης στο TCP ονομάζεται χαιρετισμός τριών τρόπων, Στο παράδειγμά μας, ένα πρόγραμμα εφαρμογής, ο client, θέλει να κάνει μία σύνδεση με άλλο πρόγραμμα εφαρμογής, τον server, χρησιμοποιώντας το TCP ως πρωτόκολλο επιπέδου μεταφοράς.
Η διαδικασία ξεκινά με τον server. Το πρόγραμμα server λέει στο TCP ότι είναι έτοιμο να δεχθεί μία σύνδεση. Αυτό ονομάζεται αίτηση για ένα παθητικό άνοιγμα. Αν και ο server TCP είναι έτοιμος να δεχθεί οποιαδήποτε σύνδεση από οποιαδήποτε μηχανή στον κόσμο, δεν μπορεί να κάνει ο ίδιος τη σύνδεση.
Το πρόγραμμα client εκδίδει μία αίτηση για ένα ενεργητικό άνοιγμα. Ένας client που θέλει να συνδεθεί με έναν ανοιχτό server λέει στο TCP ότι μπορεί να συνδεθεί στον συγκεκριμένο server. Το TCP μπορεί να ξεκινήσει τώρα τη διαδικασία χαιρετισμού τριών τρόπων όπως φαίνεται **στην Εικόνα παρακάτω**. Για να δείξουμε τη διαδικασία χρησιμοποιούμε δύο γραμμές χρόνου: μία σε κάθε σημείο. Κάθε τμήμα έχει τιμές για όλα τα πεδία κεφαλίδας του και ίσως και για μερικά από τα πεδία επιλογών. Δείχνουμε όμως μόνο τα λίγα απαραίτητα πεδία για να καταλάβουμε κάθε φράση. Δείχνουμε τον αριθμό σειράς, τον αριθμό επιβεβαίωσης, τις σημαίες ελέγχου (μόνο εκείνες που έχουν οριστεί) και το μέγεθος του παραθύρου αν δεν είναι κενό. Τα τρία βήματα σε αυτήν τη φάση είναι τα εξής:

1. Ο client στέλνει το πρώτο τμήμα, ένα τμήμα SYN, στο οποίο έχει οριστεί μόνο η σημαία SYN. Αυτό το τμήμα υπάρχει για το συγχρονισμό των αριθμών σειράς. Ο client στο δικό μας παράδειγμα επιλέγει έναν τυχαίο αριθμό ως τον πρώτο αριθμό σειράς και τον στέλνει στο server. Αυτός ο αριθμός σειράς ονομάζεται αρχικός αριθμός σειράς (ISN). Σημειώνουμε ότι αυτό το τμήμα δεν περιέχει αριθμό επιβεβαίωσης. Ούτε ορίζει το μέγεθος του παραθύρου: ο ορισμός του μεγέθους του παραθύρου έχει νόημα μόνο όταν ένα τμήμα συμπεριλαμβάνει μία επιβεβαίωση. Σημειώνουμε ότι το τμήμα SYN είναι τμήμα ελέγχου και δεν περιέχει δεδομένα. Διαθέτει ωστόσο έναν αριθμό σειράς. Όταν ξεκινά η μεταφορά δεδομένων, ο αριθμός σειράς αυξάνεται κατά 1. Μπορούμε να πούμε ότι το τμήμα SYN δεν φέρει πραγματικά δεδομένα αλλά μπορούμε να θεωρήσουμε ότι περιέχει ένα φανταστικό byte.



Έναρξη σύνδεσης χρησιμοποιώντας χαιρετισμό τριών τρόπων

2. Ο server στέλνει το δεύτερο τμήμα, ένα τμήμα SYN+ACK όπου έχουν οριστεί δύο bits σημαίας: τα SYN και ACK. Αυτό το τμήμα έχει διπλό σκοπό. Είναι αρχικά ένα τμήμα SYN για επικοινωνία προς την άλλη κατεύθυνση. Ο server χρησιμοποιεί αυτό το τμήμα για να αρχικοποιήσει έναν αριθμό σειράς που θα αριθμεί τα bytes που στέλνονται από το server στον client. Ο server επίσης επιβεβαιώνει τη λήψη του τμήματος SYN από τον client ορίζοντας τη σημαία ACK και προβάλλοντας τον επόμενο αριθμό σειράς που περιμένει να λάβει από τον client. Επειδή περιέχει μία επιβεβαίωση, πρέπει επίσης να ορίσει το μέγεθος παραθύρου του παραλήπτη, το rwnd (θα χρησιμοποιηθεί από τον client) όπως θα δούμε στην ενότητα για τον έλεγχο ροής.

3. Ο client στέλνει το τρίτο τμήμα, το οποίο είναι ένα τμήμα ACK. Επιβεβαιώνει τη λήψη του δεύτερου τμήματος με τη σημαία ACK και του πεδίου του αριθμού επιβεβαίωσης. Σημειώνουμε ότι ο αριθμός σειράς σε αυτό το τμήμα είναι ίδιος με αυτόν του τμήματος SYN (το τμήμα ACK δεν έχει αριθμό σειράς). Ο client πρέπει επίσης να ορίσει το μέγεθος παραθύρου του server. Μερικές υλοποιήσεις επιτρέπουν σε αυτό το τρίτο τμήμα στη φάση της σύνδεσης να μεταφέρει το πρώτο μπλοκ δεδομένων από τον client. Σε αυτήν την περίπτωση, το τρίτο τμήμα πρέπει να έχει ένα νέο αριθμό σειράς που δείχνει τον αριθμό του byte του πρώτου byte των δεδομένων. Γενικά, το τρίτο τμήμα δεν φέρει συνήθως δεδομένα και δεν διαθέτει αριθμό σειράς.

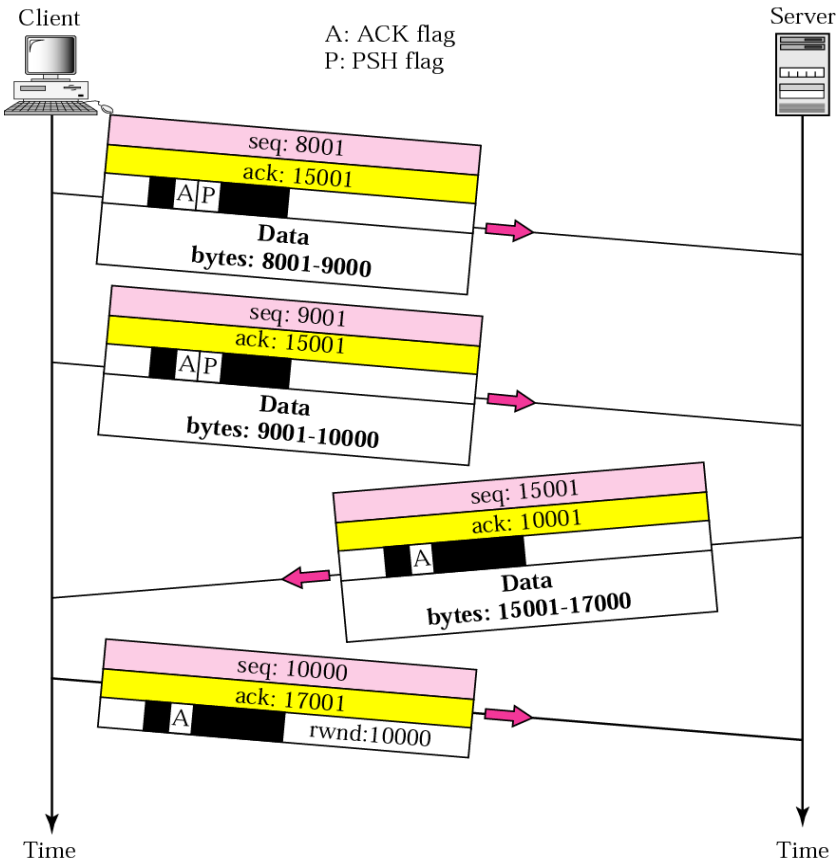
Επίθεση πλημμύρας SYN

Η διαδικασία έναρξης σύνδεσης στο TCP είναι ευάλωτη σε ένα σοβαρό πρόβλημα ασφάλειας που ονομάζεται επίθεση πλημμύρας SYN. Αυτό συμβαίνει όταν ένας κακοπροαίρετος χρήστης στέλνει ένα μεγάλο αριθμό τμημάτων SYN σε ένα server, προσποιούμενος ότι κάθε τμήμα προέρχεται από διαφορετικό client, παραποιώντας τις διευθύνσεις IP της πηγής στα διαγράμματα δεδομένων. Ο server,υποθέτοντας ότι οι clients εκδίδουν ένα ενεργητικό άνοιγμα, κατανέμει τις κατάλληλους πόρους, δημιουργεί πίνακες TCB και ορίζει χρονόμετρα. Ο TCP server στέλνει μετά τα τμήματα SYN+ACK στους πλαστούς clients, τα οποία χάνονται. Σε αυτό το διάστημα όμως, πολλοί πόροι καταλαμβάνονται χωρίς να χρησιμοποιούνται. Αν σε αυτό το διάστημα ο αριθμός των τμημάτων SYN είναι μεγάλος, ο server σταδιακά εξαντλεί τους πόρους του και μπορεί να καταρρεύσει. Αυτή η επίθεση πλημμύρας SYN ανήκει σε μία ομάδα επιθέσεων κατά της ασφάλειας που ονομάζεται επίθεση άρνησης παροχής υπηρεσίας, στην οποία ένας επιτιθέμενος μονοπωλεί ένα σύστημα με τόσες πολλές αιτήσεις παροχής υπηρεσίας που το σύστημα καταρρέει και αρνείται να παράσχει υπηρεσίες σε όλες τις αιτήσεις.
Μερικές υλοποιήσεις του TCP ακολουθούν στρατηγικές εξάρθρωσης των αποτελεσμάτων μίας επίθεσης SYN. Μερικές έχουν θέσει ένα όριο αιτήσεων σύνδεσης μέσα σε συγκεκριμένο χρόνο. Άλλες αποκλείουν τα διαγράμματα δεδομένων που προέρχονται από ανεπιθύμητες διευθύνσεις πηγών. Μία πρόσφατη στρατηγική είναι η αναβολή της κατανομής των πόρων μέχρι να οργανωθεί όλη η σύνδεση χρησιμοποιώντας αυτό που ονομάζεται cookie. Το SCTP, το νέο πρωτόκολλο επιπέδου μεταφοράς, χρησιμοποιεί αυτήν την στρατηγική.

Μεταφορά δεδομένων

Αφού ιδρυθεί η σύνδεση, μπορεί να λάβει χώρα η προς δύο κατευθύνσεις μεταφορά δεδομένων. Ο client και ο server μπορούν να στείλουν δεδομένα και επιβεβαιώσεις και προς τις δύο κατευθύνσεις. Θα μελετήσουμε τους κανόνες επιβεβαίωσης αργότερα στο κεφάλαιο αλλά προς το παρόν αρκεί να γνωρίζουμε ότι τα δεδομένα που ταξιδεύουν προς την ίδια κατεύθυνση ως επιβεβαίωση μεταφέρονται στο ίδιο τμήμα. Η επιβεβαίωση μεταφέρεται μαζί με τα δεδομένα. **Η Εικόνα παρακάτω** παρουσιάζει ένα παράδειγμα. Σε αυτό το παράδειγμα, αφού ιδρυθεί η σύνδεση (δεν φαίνεται στην εικόνα) ο client στέλνει 2000 bytes δεδομένων σε δύο τμήματα. Ο server στέλνει μετά 2000 bytes σε ένα τμήμα. Ο client στέλνει ένα ακόμα τμήμα. Τα πρώτα τρία τμήματα φέρουν δεδομένα και επιβεβαίωση, αλλά το τελευταίο φέρει μόνο μία επιβεβαίωση επειδή δεν υπάρχουν άλλα δεδομένα προς αποστολή. Σημειώνουμε τις τιμές των αριθμών ακολουθίας και επιβεβαίωσης. Τα τμήματα δεδομένων που αποστέλλονται από τον client έχουν τιμή στη σημαία PSH (push) ώστε ο server TCP να γνωρίζει ότι πρέπει να παραδώσει

δεδομένα στο server της διαδικασίας μόλις τα λάβει. Το τμήμα από το server, από την άλλη, δεν ορίζει τη σημαία push. Οι περισσότερες TCP υλοποιήσεις παρέχουν την επιλογή ορισμού ή όχι αυτής της σημαίας.



Μεταφορά δεδομένων

Τερματισμός σύνδεσης

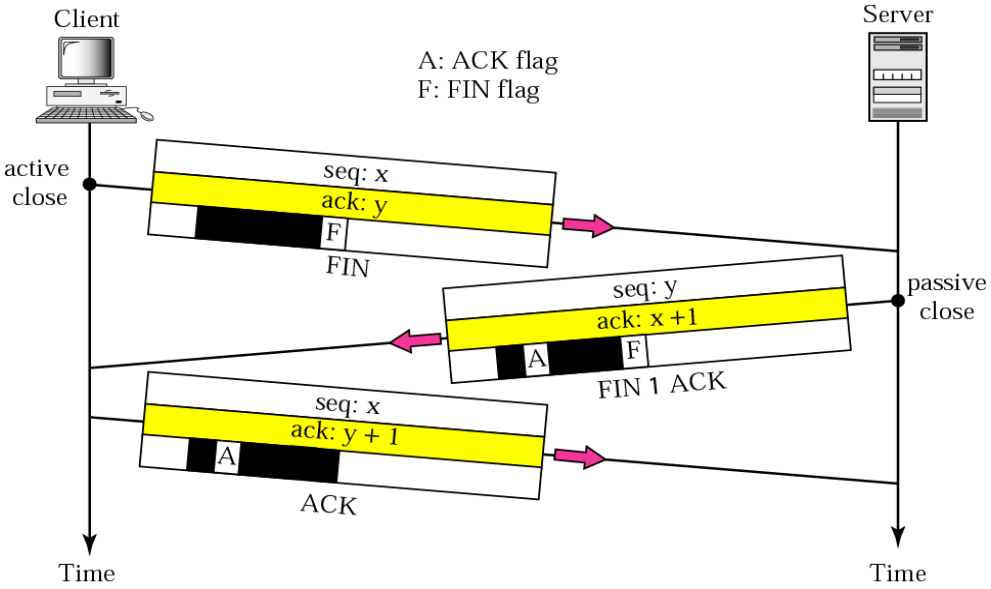
Οποιοδήποτε από τα δύο μέρη που εμπλέκεται στην ανταλλαγή δεδομένων (client ή server) μπορεί να κλείσει τη σύνδεση, αν και συνήθως ατό γίνεται από τον client. Οι περισσότερες υλοποιήσεις σήμερα επιτρέπουν δύο επιλογές για τον τερματισμό της σύνδεσης: χαιρετισμός τριών τρόπων και χαιρετισμός τεσσάρων τρόπων με μία ημίκλειστη επιλογή.

Χαιρετισμός τριών τρόπων

Οι περισσότερες υλοποιήσεις σήμερα επιτρέπουν το χαιρετισμό τριών τρόπων για τον τερματισμό μίας σύνδεσης, όπως φαίνεται στην **Εικόνα παρακάτω**.

1. Σε μία κανονική κατάσταση, ο client TCP, αφού λάβει μία εντολή κλεισίματος από τον client, στέλνει το πρώτο τμήμα, ένα τμήμα FIN

στο οποίο έχει οριστεί η σημαία FIN. Σημειώνουμε ότι ένα τμήμα FIN μπορεί να συμπεριλαμβάνει το τελευταίο μπλοκ δεδομένων που αποστέλλεται από τον client ή μπορεί να είναι ένα τμήμα ελέγχου όπως φαίνεται στην εικόνα. Αν είναι μόνο ένα τμήμα ελέγχου, έχει μόνο έναν αριθμό σειράς.



Τερματισμός σύνδεσης χρησιμοποιώντας χαιρετισμό τριών τρόπων

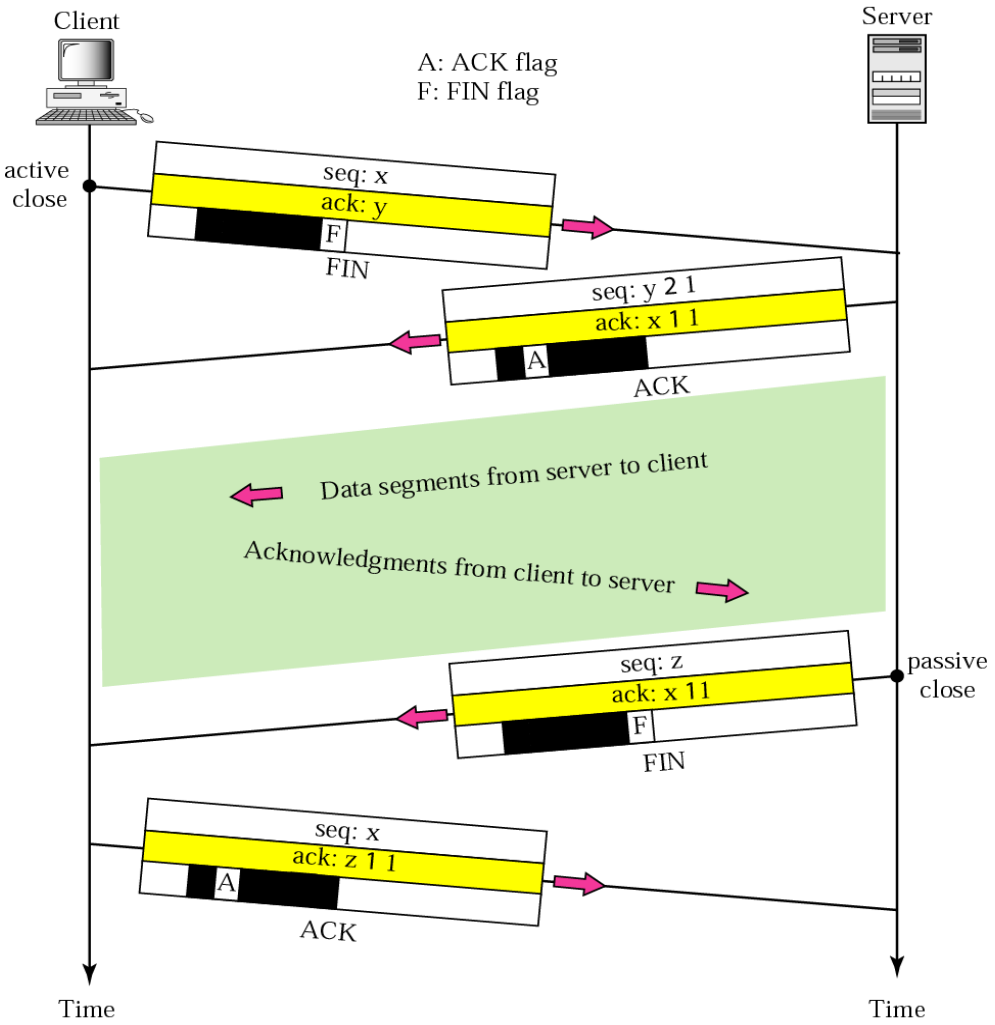
2. Ο server TCP αφού λάβει το τμήμα FIN, ενημερώνει τη διαδικασία του για την κατάσταση και στέλνει το δεύτερο τμήμα, ένα τμήμα FIN+ACK, για να επιβεβαιώσει τη λήψη του τμήματος FIN από τον client και ταυτόχρονα για να ανακοινώσει το κλείσιμο της σύνδεσης στην άλλη κατεύθυνση. Αυτό το τμήμα μπορεί επίσης να περιέχει το τελευταίο μπλοκ δεδομένων από το server. Αν δεν φέρει δεδομένα, έχει μόνο έναν αριθμό ακολουθίας.
3. Ο client TCP στέλνει το τελευταίο τμήμα, ένα τμήμα ACK, για να επιβεβαιώσει τη λήψη του τμήματος FIN από τον TCP server. Αυτό το τμήμα περιέχει τον αριθμό επιβεβαίωσης, ο οποίος είναι ένα συν τον αριθμό σειράς που έλαβε από το τμήμα FIN από το server. Αυτό το τμήμα δεν μπορεί να φέρει δεδομένα και δεν έχει αριθμό σειράς.

Ημίκλειστη κατάσταση

Στο TCP, το ένα άκρο μπορεί να σταματήσει να στέλνει δεδομένα ενώ εξακολουθεί να λαμβάνει. Αυτό ονομάζεται ημίκλειστη κατάσταση. Αν και τα δύο άκρα μπορούν να εκδώσουν ημίκλειστη κατάσταση, συνήθως αυτό γίνεται από τον client. Μπορεί να συμβεί όταν ο server χρειάζεται όλα τα δεδομένα πριν ξεκινήσει την επεξεργασία. Ένα καλό παράδειγμα είναι η ταξινόμηση. Όταν ο client στέλνει δεδομένα στο server προς ταξινόμηση, ο server πρέπει να λάβει όλα τα δεδομένα πριν ξεκινήσει την ταξινόμηση. Αυτό

σημαίνει ότι ο client, αφού στείλει όλα τα δεδομένα, μπορεί να κλείσει τη σύνδεση στην εξερχόμενη κατεύθυνση. Η εισερχόμενη όμως πρέπει να παραμείνει ανοιχτή για να λάβει τα ταξινομημένα δεδομένα. Ο server, αφού λάβει τα δεδομένα χρειάζεται χρόνο για την ταξινόμηση και η εξερχόμενη κατεύθυνσή του παραμένει ανοιχτή.

Η Εικόνα παρακάτω παρουσιάζει ένα παράδειγμα ημίκλειστης κατάστασης. Ο client κλείνει κατά το ήμισυ τη σύνδεση στέλνοντας ένα τμήμα FIN. Ο server δέχεται το μήνυμα ημίκλειστης κατάστασης στέλνοντας το τμήμα ACK. Η μεταφορά δεδομένων από τον client στο server σταματά. Ο server όμως, μπορεί να συνεχίσει να στέλνει δεδομένα. Όταν ο server έχει στείλει όλα τα επεξεργασμένα δεδομένα, στέλνει ένα τμήμα FIN, το οποίο επιβεβαιώνεται από ένα ACK από τον client.



Ημίκλειστη κατάσταση

Μετά το κατά το ήμισυ κλείσιμο της σύνδεσης, τα δεδομένα μπορούν να ταξιδέψουν από το server στον client και οι επιβεβαιώσεις μπορούν να ταξιδέψουν από τον client στον server. Ο client δεν μπορεί να στείλει άλλα δεδομένα στο server. Το δεύτερο τμήμα (ACK) δεν έχει αριθμό σειράς. Αν και ο client έχει δεχθεί τον αριθμό σειράς y-1 και περιμένει τον y, ο αριθμός σειράς του server εξακολουθεί να είναι y-1. Όταν η σύνδεση τελικά κλείσει, ο αριθμός σειράς του τελευταίου τμήματος ACK εξακολουθεί να είναι το x, επειδή δεν χρησιμοποιούνται αριθμοί σειράς κατά τη μεταφορά δεδομένων σε αυτήν την κατεύθυνση.

Επαναφορά σύνδεσης

Το TCP στο ένα άκρο μπορεί να αρνηθεί μία αίτηση σύνδεσης, να αναστείλει μία σύνδεση, ή να τερματίσει μία ανενεργή σύνδεση. Όλα αυτά γίνονται από τη σημαία RST (reset).

Άρνηση σύνδεσης

Υποθέτουμε ότι το TCP στη μία πλευρά έχει αιτηθεί μία σύνδεση με μία θύρα που δεν υπάρχει. Το TCP από την άλλη πλευρά μπορεί να στείλει ένα τμήμα με ορισμένο το RST bit για να ακυρώσει τη σύνδεση.

Αναστολή σύνδεσης

Ένα TCP ίσως θελήσει να αναστείλει μία σύνδεση εξαιτίας μίας μη κανονικής κατάστασης. Μπορεί να στείλει ένα τμήμα RST για να κλείσει τη σύνδεση.

Τερματισμός ανενεργής σύνδεσης

Το TCP στη μία πλευρά ίσως ανακαλύψει ότι το TCP της άλλης πλευράς είναι ανενεργό για αρκετό χρονικό διάστημα. Μπορεί να στείλει ένα τμήμα RST για να καταστρέψει τη σύνδεση. Η διαδικασία είναι ίδια με την αναστολή μίας σύνδεσης.

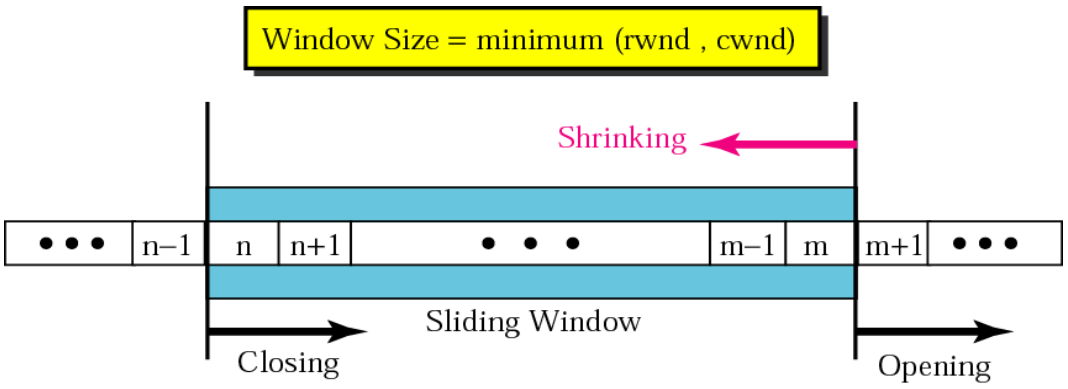
6.4 ΕΛΕΓΧΟΣ ΡΟΗΣ

Ο έλεγχος ροής ρυθμίζει την ποσότητα δεδομένων που μπορεί να στείλει μία πηγή πριν λάβει μία επιβεβαίωση από τον προορισμό. Υπάρχει μία ακραία περίπτωση όπου ένα πρωτόκολλο επιπέδου μεταφοράς θα μπορούσε να στείλει ένα byte δεδομένων και να περιμένει για την επιβεβαίωση πριν στείλει το επόμενο byte και αυτή η διαδικασία θα είναι εξαιρετικά αργή. Αν τα δεδομένα διανύουν μεγάλη απόσταση, η πηγή είναι ανενεργή μέχρι να έρθει η επιβεβαίωση.

Υπάρχει η άλλη ακραία περίπτωση όπου ένα πρωτόκολλο επιπέδου μεταφοράς μπορεί να στείλει όλα τα δεδομένα χωρίς να ανησυχεί για επιβεβαιώσεις. Αυτό επιταχύνει τη διαδικασία, αλλά υπερφορτώνει τον παραλήπτη. Εκτός από αυτό, αν χαθεί, επαναληφθεί, ληφθεί εκτός σειράς ή αλλοιωθεί μέρος των δεδομένων, η πηγή δεν θα γνωρίζει τίποτα μέχρι να γίνει έλεγχος για όλα από τον προορισμό.
Το TCP προσφέρει μία λύση που βρίσκεται ανάμεσα από αυτές τις δύο ακραίες περιπτώσεις. Ορίζει ένα παράθυρο που περιορίζεται από τη μνήμη με τα δεδομένα που παραδίδονται από το πρόγραμμα εφαρμογής και είναι έτοιμα προς αποστολή. Το TCP στέλνει μία ποσότητα δεδομένων που ορίζεται από το πρωτόκολλο κυλιόμενου παραθύρου.

Πρωτόκολλο κυλιόμενου παραθύρου

Για να επιτύχει τον έλεγχο ροής, το TCP χρησιμοποιεί ένα πρωτόκολλο κυλιόμενου παραθύρου. Με αυτήν τη μέθοδο, ένας κεντρικός υπολογιστής χρησιμοποιεί ένα παράθυρο για εξερχόμενη επικοινωνία (απεσταλμένα δεδομένα). Το παράθυρο καταλαμβάνει ένα τμήμα της μνήμης που περιέχει bytes που λαμβάνονται από τη διαδικασία. Τα bytes μέσα στο παράθυρο είναι αυτά που μπορεί να βρίσκονται υπό μεταφορά και μπορούν να σταλούν χωρίς να υπάρχει ανησυχία για την επιβεβαίωση. Το φανταστικό παράθυρο έχει δύο τοίχους: έναν αριστερά και ένα δεξιά. Το παράθυρο ονομάζεται κυλιόμενο παράθυρο επειδή οι τοίχοι δεξιά και αριστερά μπορούν να κυλήσουν όπως βλέπουμε **στην Εικόνα παρακάτω**. Οι αριθμοί εκφράζουν τα bytes μέσα και έξω από το παράθυρο.



Κυλιόμενο παράθυρο

Το παράθυρο είναι ανοιχτό, κλειστό, ή συρρικνωμένο. Αυτές οι τρεις δραστηριότητες, όπως θα δούμε, τελούν υπό τον έλεγχο του παραλήπτη (και εξαρτώνται από τη συμφόρηση στο δίκτυο) και όχι του αποστολέα. Ο αποστολέας πρέπει να υπακούσει στις εντολές του παραλήπτη σε αυτό το σημείο.

Το άνοιγμα ενός παραθύρου σημαίνει μετακίνηση του δεξιού τοίχου προς τα δεξιά. Αυτό επιτρέπει την τοποθέτηση περισσοτέρων νέων bytes στη μνήμη, τα οποία μπορούν να σταλούν. Το κλείσιμο του παραθύρου σημαίνει ότι μερικά bytes έχουν επιβεβαιωθεί και ο αποστολέας δεν χρειάζεται να ανησυχεί πλέον για αυτά. Η συρρίκνωση του παραθύρου σημαίνει μετακίνηση του δεξιού τοίχου προς τα αριστερά. Αυτό αποθαρρύνεται και δεν επιτρέπεται σε μερικές υλοποιήσεις επειδή σημαίνει ότι μερικά bytes δεν έχουν πλέον τη δυνατότητα να σταλούν. Αυτό αποτελεί πρόβλημα αν ο αποστολέας έχει ήδη στείλει αυτά τα bytes. Σημειώνουμε ότι ο αριστερός τοίχος δεν μπορεί να μετακινηθεί προς τα αριστερά επειδή αυτό θα ανακαλούσε μερικές από τις ήδη απεσταλμένες επιβεβαιώσεις.
Το μέγεθος του παραθύρου στη μία άκρη, ορίζεται από τη μικρότερη των εξής τιμών: παράθυρο παραλήπτη (rwnd) ή παράθυρο συμφόρησης (cwnd). Το παράθυρο παραλήπτη είναι η τιμή που διαφημίζεται από το άλλο άκρο σε ένα τμήμα που περιέχει επιβεβαίωση. Είναι ο αριθμός των bytes που μπορεί να δεχθεί το άλλο άκρο πριν η μνήμη του υπερχειλίσει και τα δεδομένα απορριφθούν. Το παράθυρο συμφόρησης είναι η τιμή που καθορίζεται από το δίκτυο για να αποφευχθεί η συμφόρηση. Θα μιλήσουμε για τη συμφόρηση αργότερα σε αυτό το κεφάλαιο.

Κλείσιμο παραθύρου

Η συρρίκνωση του παραθύρου δεν προτείνεται. Υπάρχει όμως μία εξαίρεση: ο παραλήπτης μπορεί προσωρινά να κλείσει το παράθυρο στέλνοντας ένα rwnd με τιμή 0. Αυτό μπορεί να συμβεί αν για κάποιο λόγο ο παραλήπτης δεν θέλει να λάβει άλλα δεδομένα από τον αποστολέα για λίγο. Σε αυτήν την περίπτωση, ο αποστολέας δεν συρρικνώνει το παράθυρο, αλλά σταματά να στέλνει δεδομένα μέχρι να φτάσει μία νέα διαφήμιση. Ακόμα κι όταν το παράθυρο κλείσει από μία εντολή του παραλήπτη, ο αποστολέας μπορεί να στέλνει πάντα τμήματα με ένα byte δεδομένων. Αυτό ονομάζεται επισταμένη εξέταση και χρησιμοποιείται για να αποτραπεί ένα αδιέξοδο.

6.5 ΕΛΕΓΧΟΣ ΛΑΘΩΝ

Το TCP είναι ένα αξιόπιστο πρωτόκολλο επιπέδου μεταφοράς. Αυτό σημαίνει ότι ένα πρόγραμμα εφαρμογής που παραδίδει μία ροή δεδομένων στο TCP βασίζεται στο TCP για την παράδοση όλης της ροής στο πρόγραμμα εφαρμογής στο άλλο άκρο, με σειρά, χωρίς λάθη και χωρίς μέρη απολεσθέντα ή διπλά.
Το TCP παρέχει αξιοπιστία, χρησιμοποιώντας έλεγχο λαθών. Ο έλεγχος λαθών συμπεριλαμβάνει μηχανισμούς ανίχνευσης αλλοιωμένων τμημάτων, χαμένων τμημάτων, τμημάτων εκτός σειράς και διπλών τμημάτων. Ο έλεγχος λαθών επίσης συμπεριλαμβάνει ένα μηχανισμό για διόρθωση λαθών αφού

ανιχνευθούν. Η ανίχνευση και η διόρθωση λαθών στο TCP επιτυγχάνεται μέσω της χρήσης τριών απλών εργαλείων: άθροισμα ελέγχου, επιβεβαίωση και λήξη χρόνου.

Άθροισμα ελέγχου

Κάθε τμήμα συμπεριλαμβάνει ένα πεδίο αθροίσματος ελέγχου το οποίο χρησιμοποιείται για να κάνει έλεγχο σε ένα αλλοιωμένο τμήμα. Αν το τμήμα είναι αλλοιωμένο, απορρίπτεται από το TCP προορισμού και θεωρείται απολεσθέν. Το TCP χρησιμοποιεί ένα άθροισμα ελέγχου με 16 bits που είναι υποχρεωτικό σε κάθε τμήμα.

Επιβεβαίωση

Το TCP χρησιμοποιεί μηνύματα ACK για να επιβεβαιώσει τη λήψη τμημάτων δεδομένων. Τα τμήματα ελέγχου που δεν μεταφέρουν δεδομένα αλλά διαθέτουν αριθμό σειράς επίσης επιβεβαιώνονται. Τα τμήματα ACK δεν επιβεβαιώνονται ποτέ.

Παραγωγή επιβεβαιώσεων

Πότε παράγει ο παραλήπτης επιβεβαιώσεις; Κατά την εξέλιξη του TCP, αρκετοί κανόνες έχουν οριστεί και χρησιμοποιηθεί από αρκετές υλοποιήσεις. Παραθέτουμε εδώ τους πιο συνηθισμένους κανόνες. Η σειρά ενός κανόνα δεν ορίζει απαραίτητα τη σημασία του.

1. Όταν ένα άκρο στέλνει ένα τμήμα δεδομένων στο άλλο άκρο, πρέπει να συμπεριλαμβάνει μία επιβεβαίωση που δίνει τον επόμενο αριθμό σειράς που αναμένεται να δεχθεί. Αυτός ο κανόνας μειώνει τον αριθμό των τμημάτων που απαιτούνται και επομένως, μειώνει την κίνηση.
2. Όταν ο παραλήπτης δεν έχει να στείλει δεδομένα και δέχεται ένα τμήμα σε σειρά (με τον αναμενόμενο αριθμό σειράς) και το προηγούμενο τμήμα έχει ήδη επιβεβαιωθεί, ο παραλήπτης καθυστερεί να στείλει ένα τμήμα ACK μέχρι να φτάσει ένα άλλο τμήμα ή μέχρι να περάσει μία χρονική περίοδος (συνήθως 500 ms). Με άλλα λόγια, ο παραλήπτης πρέπει να καθυστερήσει την αποστολή ενός τμήματος ACK αν υπάρχει μόνο ένα εξέχον τμήμα σε σειρά. Αυτός ο κανόνας επίσης αποτρέπει τη δημιουργία επιπλέον κίνησης από τα τμήματα ACK.
3. Όταν ένα τμήμα φτάνει με αριθμό σειράς που αναμένεται από τον παραλήπτη και το προηγούμενο τμήμα (σε σειρά) δεν έχει επιβεβαιωθεί, ο παραλήπτης αμέσως στέλνει ένα τμήμα ACK. Με άλλα λόγια, δεν πρέπει να υπάρχουν περισσότερα από δύο σε σειρά μη ανεπιβεβαίωτα τμήματα μία συγκεκριμένη στιγμή. Αποτρέπεται έτσι η

περιττή αναμετάδοση τμημάτων που μπορεί να δημιουργήσουν συμφόρηση στο δίκτυο.

4. Όταν ένα τμήμα φτάνει με εκτός σειράς αριθμό που είναι μεγαλύτερος από τον αναμενόμενο, ο παραλήπτης αμέσως στέλνει ένα τμήμα ACK που ανακοινώνει τον αριθμό σειράς του τμήματος που αναμένεται ακολούθως. Αυτό οδηγεί σε γρήγορη αναμετάδοση τμημάτων που λείπουν.
5. Όταν φτάνει ένα τμήμα που λείπει, ο παραλήπτης στέλνει ένα τμήμα ACK για να ανακοινώσει τον επόμενο αριθμό σειράς που αναμένεται. Ενημερώνεται έτσι ο παραλήπτης ότι τα τμήματα που αναφέρονται ως απολεσθέντα έχουν ληφθεί.
6. Αν φτάσει ένα διπλό τμήμα, ο παραλήπτης αμέσως στέλνει μία επιβεβαίωση. Λύνονται έτσι μερικά προβλήματα όταν ένα τμήμα ACK έχει χαθεί.

Τύπος επιβεβαίωσης

Στο παρελθόν, το TCP χρησιμοποιούσε μόνο ένα έναν τύπο επιβεβαίωσης: αθροιστική επιβεβαίωση. Σήμερα, μερικές TCP υλοποιήσεις χρησιμοποιούν και επιλεκτικές επιβεβαιώσεις.

Αθροιστική επιβεβαίωση (ACK). Το TCP σχεδιάστηκε αρχικά για να επιβεβαιώνει τη λήψη τμημάτων αθροιστικά. Ο παραλήπτης διαφημίζει το επόμενο byte που περιμένει να λάβει, αγνοώντας όλα τα τμήματα που λαμβάνονται εκτός σειράς. Αυτό μερικές φορές αναφέρεται σε μία θετική αθροιστική επιβεβαίωση ή ACK. Η λέξη <<θετική>> δείχνει ότι τα απορριφθέντα, απολεσθέντα ή διπλά τμήματα δεν αναφέρονται. Το πεδίο ACK των 32 bits που συμπληρώνει την κεφαλίδα TCP χρησιμοποιείται για αθροιστικές επιβεβαιώσεις και η τιμή του ισχύει μόνο όταν η σημαία ACK έχει την τιμή 1.

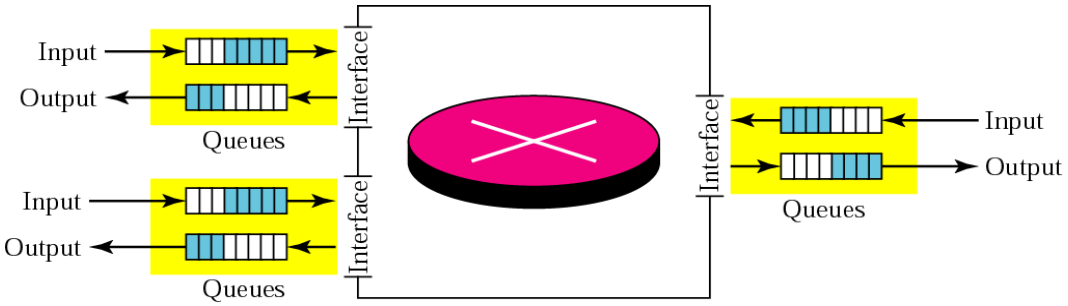
Επιλεκτική επιβεβαίωση (SACK). Όλο και περισσότερες υλοποιήσεις προσθέτουν ακόμα έναν τύπο επιβεβαίωσης που ονομάζεται **επιλεκτική επιβεβαίωση** ή **SACK.** Ένα SACK δεν αντικαθιστά το ACK, αλλά αναφέρει επιπλέον πληροφορίες στον αποστολέα. Ένα SACK αναφέρει το μπλοκ δεδομένων που βρίσκεται εκτός σειράς και τα μπλοκ τμημάτων που επαναλαμβάνονται. Επειδή όμως δεν υπάρχει πρόβλεψη στην κεφαλίδα TCP για την προσθήκη αυτού του τύπου πληροφοριών, το SACK υλοποιείται ως μία επιλογή στο τέλος της κεφαλίδας TCP.

6.6 ΕΛΕΓΧΟΣ ΣΥΜΦΟΡΗΣΗΣ

Ένα σημαντικό θέμα σε ένα δίκτυο είναι η συμφόρηση. Η συμφόρηση σε ένα δίκτυο μπορεί να συμβεί αν το φορτίο στο δίκτυο – ο αριθμός των πακέτων που στέλνονται στο δίκτυο – είναι μεγαλύτερο από την χωρητικότητα του δικτύου – τον αριθμό των πακέτων που μπορεί να χειριστεί ένα δίκτυο. Ο έλεγχος συμφόρησης αναφέρεται στους μηχανισμούς και τις τεχνικές που ελέγχουν τη συμφόρηση και συγκρατούν το φορτίο κάτω από τη χωρητικότητα.

Θα μπορούσαμε να αναρωτηθούμε γιατί υπάρχει συμφόρηση σε ένα δίκτυο. Η συμφόρηση συμβαίνει σε οποιοδήποτε σύστημα παρουσιάζεται αναμονή. Για παράδειγμα, συμβαίνει συμφόρηση σε έναν αυτοκινητόδρομο εξαιτίας κάποιας ανωμαλίας στη ροή, όπως ένα ατύχημα την ώρα αιχμής, το οποίο δημιουργεί μπλοκάρισμα.

Η συμφόρηση σε ένα δίκτυο συμβαίνει επειδή οι δρομολογητές και οι διακλαδωτές έχουν ουρές – μνήμες όπου τοποθετούνται τα πακέτα πριν και μετά την επεξεργασία. Ένας δρομολογητής, για παράδειγμα, έχει μία ουρά εισόδου και μία ουρά εξόδου για κάθε διεπαφή. Όταν ένα πακέτο φτάνει στην εισερχόμενη διεπαφή, περνάει από τρία βήματα πριν φύγει, όπως βλέπουμε στην **Εικόνα παρακάτω.**



Ουρές δρομολογητή

1. Το πακέτο τοποθετείται στο τέλος της ουράς εισόδου ενώ περιμένει τον έλεγχο.
2. Η ρουτίνα επεξεργασίας του δρομολογητή αφαιρεί το πακέτο από την ουρά εισόδου μόλις φτάσει μπροστά την ουρά και χρησιμοποιεί τον πίνακα δρομολόγησής του και τη διεύθυνση προορισμού για να βρει τη διαδρομή.
3. Το πακέτο τοποθετείται στην κατάλληλη ουρά εξόδου και περιμένει τη σειρά του για να σταλεί.

Πρέπει να γνωρίζουμε δύο ζητήματα. Πρώτον, αν ο ρυθμός άφιξης των πακέτων είναι υψηλότερος από το ρυθμό επεξεργασίας τους, οι ουρές εισόδου μεγαλώνουν σε μέγεθος και αναμονή. Δεύτερον, αν ρυθμός άφιξης

των πακέτων είναι μικρότερος από το ρυθμό επεξεργασίας τους, οι ουρές εξόδου μεγαλώνουν.

Μηχανισμοί ελέγχου συμφόρησης

Ο έλεγχος συμφόρησης αναφέρεται σε τεχνικές και μηχανισμούς που μπορούν να αποτρέψουν τη συμφόρηση, πριν συμβεί, ή να την απομακρύνουν, μετά την εμφάνισή της. Γενικά μπορούμε να μοιράσουμε τους μηχανισμούς ελέγχου συμφόρησης σε δύο μεγάλες κατηγορίες: έλεγχος συμφόρησης ανοιχτού βρόγχου (πρόληψη) και έλεγχος συμφόρησης κλειστού βρόγχου (απομάκρυνση).

Έλεγχος συμφόρησης ανοιχτού βρόγχου

Στον έλεγχο συμφόρησης ανοιχτού βρόγχου, οι μέθοδοι εφαρμόζονται για να αποτραπεί η συμφόρηση πριν συμβεί. Σε αυτούς τους μηχανισμούς, ο έλεγχος συμφόρησης αντιμετωπίζεται από την πηγή ή τον προορισμό. Βλέπουμε παρακάτω μία σύντομη λίστα μεθόδων που μπορούν να αποτρέψουν τη συμφόρηση.

Μέθοδος αναμετάδοσης. Μία καλή μέθοδος αναμετάδοσης μπορεί να αποτρέψει τη συμφόρηση. Η μέθοδος αναμετάδοσης και τα χρονόμετρα αναμετάδοσης πρέπει να σχεδιάζονται ώστε να είναι αποδοτικά και ταυτόχρονα να αποτρέπουν τη συμφόρηση.

Μέθοδος επιβεβαίωσης. Η μέθοδος επιβεβαίωσης που επιβάλλεται από τον παραλήπτη μπορεί επίσης να επηρεάσει τη συμφόρηση. Αν ο παραλήπτης δεν επιβεβαιώνει κάθε πακέτο που δέχεται, μπορεί να καθυστερήσει τον αποστολέα και να βοηθήσει στην αποτροπή συμφόρησης.

Μέθοδος απόρριψης. Μία καλή μέθοδος απόρριψης που επιβάλλεται από τους δρομολογητές μπορεί να αποτρέψει τη συμφόρηση και ταυτόχρονα να μην δημιουργήσει προβλήματα στην ακεραιότητα της μετάδοσης. Για παράδειγμα, στη μετάδοση ήχου, αν η μέθοδος είναι η απόρριψη των λιγότερο ευαίσθητων πακέτων όταν η συμφόρηση είναι πιθανή, η ποιότητα του ήχου διατηρείται και η συμφόρηση αποτρέπεται.

Έλεγχος συμφόρησης κλειστού βρόγχου

Οι μηχανισμοί ελέγχου συμφόρησης κλειστού βρόγχου προσπαθούν να διορθώσουν τη συμφόρηση αφού εμφανιστεί. Έχουν χρησιμοποιηθεί πολλοί μηχανισμοί από διάφορα πρωτόκολλα. Θα περιγράψουμε μερικούς.

Πίεση προς τα πίσω. Όταν ένας δρομολογητής συμφορείται, μπορεί να ζητήσει από τον προηγούμενο ανοδικό δρομολογητή να μειώσει το ρυθμό των εξερχόμενων πακέτων. Η ενέργεια μπορεί να επαναληφθεί σε όλη τη διαδρομή ως το δρομολογητή αμέσως πριν την πηγή. Αυτός ο μηχανισμός ονομάζεται πίεση προς τα πίσω.

Σημείο πνιγμού. Ένα σημείο πνιγμού είναι ένα πακέτο που αποστέλλεται από ένα δρομολογητή στην πηγή για να την ενημερώσει για τη συμφόρηση. Αυτό το είδος ελέγχου είναι παρόμοιο με το πακέτο καταστολής πηγής του ICMP.

Υπονοούμενη σήμανση. Η πηγή μπορεί να ανιχνεύσει μία υπονοούμενη προειδοποίηση της συμφόρησης και να μειώσει το ρυθμό αποστολής. Για παράδειγμα, η καθαρή καθυστέρηση στη λήψη μίας επιβεβαίωσης μπορεί να είναι ένα σήμα ότι το δίκτυο έχει συμφορηθεί.

Ρητή σήμανση. Οι δρομολογητές που συναντούν συμφόρηση μπορούν να στείλουν ένα ρητό σήμα, όπως για παράδειγμα τον ορισμό τιμής για ένα bit σε ένα πακέτο, κάτι που θα ενημερώνει τον αποστολέα ή τον παραλήπτη για τη συμφόρηση.

Έλεγχος συμφόρησης στο TCP

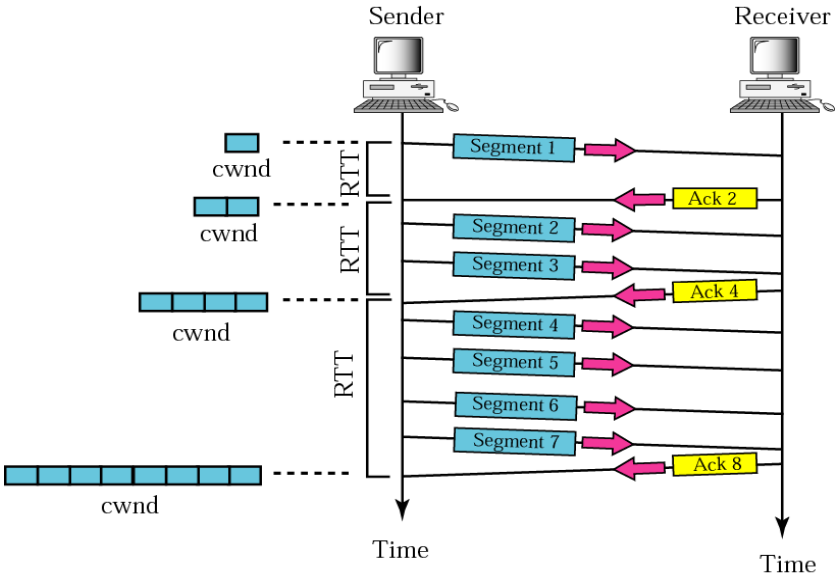
Παράθυρο συμφόρησης

Προηγουμένως, μιλήσαμε για τον έλεγχο ροής και προσπαθήσαμε να βρούμε λύσεις για την περίπτωση που ο παραλήπτης είναι υπερφορτωμένος με δεδομένα. Είπαμε ότι το μέγεθος παραθύρου του αποστολέα καθορίζεται από το διαθέσιμο χώρο μνήμης του παραλήπτη (rwnd). Με άλλα λόγια, υποθέτουμε ότι μόνο ο παραλήπτης μπορεί να υπαγορεύσει στον αποστολέα το μέγεθος του παραθύρου του. Αγνοήσαμε εντελώς μία άλλη οντότητα, το δίκτυο. Αν το δίκτυο δεν μπορεί να παραδώσει τα δεδομένα όσο γρήγορα δημιουργούνται από τον αποστολέα, πρέπει να πει στον αποστολέα να επιβραδύνει. Με άλλα λόγια, εκτός από τον παραλήπτη, το δίκτυο είναι μία δεύτερη οντότητα που καθορίζει το μέγεθος του παραθύρου του αποστολέα.
Σήμερα, το μέγεθος του παραθύρου του αποστολέα καθορίζεται όχι μόνο από τον παραλήπτη αλλά και από τη συμφόρηση στο δίκτυο.
Ο αποστολέας έχει δύο πληροφορίες: το μέγεθος παραθύρου του παραλήπτη, όπως αυτό διαφημίζεται και το μέγεθος παραθύρου της συμφόρησης. Το μέγεθος του παραθύρου είναι το ελάχιστο αυτών των δύο.
Δείχνουμε εν συντομία πώς προσδιορίζεται το μέγεθος του παραθύρου συμφόρησης (cwnd).

Μέθοδος συμφόρησης

Η γενική στρατηγική του TCP για το χειρισμό της συμφόρησης βασίζεται σε τρεις φάσεις: αργή εκκίνηση, αποφυγή συμφόρησης και ανίχνευση συμφόρησης. Στη φάση της αργής εκκίνησης, ο αποστολέας ξεκινά με πολύ αργό ρυθμό μετάδοσης αλλά αυξάνει το ρυθμό γρήγορα για να φτάσει ένα όριο. Όταν φτάσει το όριο, ο ρυθμός μετάδοσης των δεδομένων μειώνεται για να αποφευχθεί η συμφόρηση. Τέλος, αν ανιχνευθεί συμφόρηση, ο αποστολέας επιστρέφει στην αργή εκκίνηση ή την αποφυγή συμφόρησης ανάλογα με τον τρόπο που θα ανιχνευθεί η συμφόρηση.

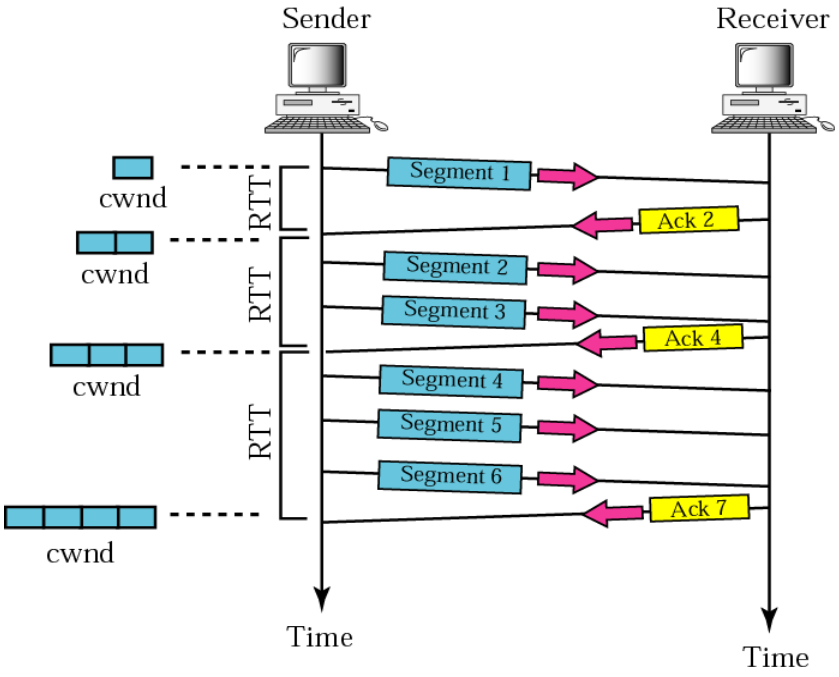
Αργή εκκίνηση: Εκθετική αύξηση. Ένας από τους αλγορίθμους που χρησιμοποιείται για τον έλεγχο της συμφόρησης στο TCP ονομάζεται αργή εκκίνηση. Αυτός ο αλγόριθμος βασίζεται στην ιδέα ότι το μέγεθος του παραθύρου συμφόρησης (cwnd) ξεκινά με ένα μέγιστο μήκος τμήματος (MSS). Το MSS καθορίζεται κατά την έναρξη της σύνδεσης με μία επιλογή που έχει το ίδιο όνομα. Το μέγεθος του παραθύρου αυξάνεται κατά ένα MSS κάθε φορά που επιβεβαιώνεται ένα τμήμα. Όπως δείχνει το όνομα, ο αλγόριθμος ξεκινά αργά αλλά αυξάνεται εκθετικά. Για να καταλάβετε την ιδέα, δείτε την **Εικόνα παρακάτω**. Σημειώνουμε ότι έχουμε εφαρμόσει τρεις απλοποιήσεις για να γίνουμε πιο κατανοητοί και να περιορίσουμε το μέγεθος της εικόνας. Έχουμε χρησιμοποιήσει αριθμούς τμημάτων αντί για αριθμούς byte (σαν κάθε τμήμα να περιέχει μόνο ένα byte). Υποθέτουμε ότι το rwnd είναι πολύ μεγαλύτερο από το cwnd, ώστε το μέγεθος παραθύρου του αποστολέα να ισούται πάντα με το cwnd. Δείχνουμε μόνο τις επιβεβαιώσεις μετά τη λήψη των τμημάτων μεγέθους παραθύρου, κάτι που σημαίνει ότι αγνοούμε τους κανόνες για την παραγωγή επιβεβαιώσεων. Ο αποστολέας ξεκινά με cwnd = 1 MSS. Αυτό σημαίνει ότι ο αποστολέας μπορεί να στείλει μόνο ένα τμήμα. Αφού λάβει την επιβεβαίωση για το τμήμα 1, το μέγεθος του παραθύρου συμφόρησης αυξάνεται κατά 1, που σημαίνει ότι το cwnd είναι τώρα 2. Τώρα μπορούν να σταλούν ακόμα δύο τμήματα. Όταν τα δύο τμήματα επιβεβαιωθούν, το μέγεθος του παραθύρου αυξάνεται κατά ένα MSS για κάθε επιβεβαιωμένο τμήμα, που σημαίνει ότι το cwnd είναι 4. Τώρα μπορούν να σταλούν ακόμα τέσσερα τμήματα. Όταν και τα τέσσερα τμήματα επιβεβαιωθούν, το μέγεθος του παραθύρου αυξάνεται κατά 4, το οποίο σημαίνει ότι το cwnd είναι 8. Σημειώνουμε ότι δεν έχει σημασία αν τα τμήματα επιβεβαιώνονται κατά ένα, δύο ή περισσότερα. Το αποτέλεσμα είναι το ίδιο.



Αργή εκκίνηση, εκθετική αύξηση

Η αργή κίνηση δεν μπορεί να συνεχίζεται επ' αόριστον. Πρέπει να υπάρχει ένα όριο στο οποίο θα σταματά αυτή η φάση. Ο αποστολέας παρακολουθεί μία μεταβλητή που ονομάζεται ssthresh (όριο αργής εκκίνησης). Όταν το μέγεθος του παραθύρου σε bytes φτάσει αυτό το όριο, η αργή εκκίνηση σταματά και ξεκινά η επόμενη φάση. Στις περισσότερες υλοποιήσεις η τιμή του ssthresh είναι 65.535 bytes.

Αποφυγή συμφόρησης: Γραμμική αύξηση. Αν ξεκινήσουμε με τον αλγόριθμο αργής εκκίνησης, το μέγεθος του παραθύρου συμφόρησης αυξάνεται εκθετικά. Για να αποφύγουμε τη συμφόρηση πριν συμβεί, πρέπει να επιβραδύνουμε αυτήν την εκθετική αύξηση. Το TCP ορίζει έναν άλλο αλγόριθμο που ονομάζεται αποφυγή συμφόρησης, ο οποίος αυξάνεται προσθετικά και όχι εκθετικά. Όταν το μέγεθος του παραθύρου συμφόρησης φτάσει το όριο της αργής εκκίνησης, σταματά η φάση αργής εκκίνησης και ξεκινά η φάση της προσθετικής αύξησης. Σε αυτόν τον αλγόριθμο, κάθε φορά που επιβεβαιώνεται όλο το παράθυρο των τμημάτων, το μέγεθος του παραθύρου συμφόρησης αυξάνεται κατά ένα. Για να παρουσιάσουμε αυτόν τον αλγόριθμο, τον εφαρμόζουμε στο ίδιο σενάριο με την αργή εκκίνηση αν και όπως θα δούμε, η αποφυγή συμφόρησης συνήθως ξεκινά όταν το μέγεθος του παραθύρου είναι πολύ μεγαλύτερο από 1. **Η Εικόνα παρακάτω** παρουσιάζει αυτήν την τακτική.



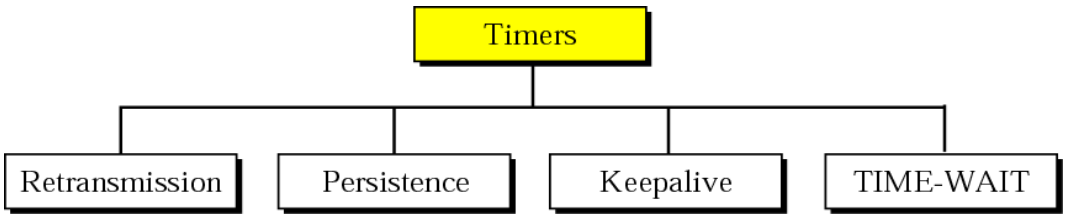
Αποφυγή συμφόρησης, γραμμική αύξηση

Ανίχνευση συμφόρησης: Μοναδιαία μείωση. Αν παρουσιαστεί συμφόρηση, το μέγεθος παραθύρου της συμφόρησης πρέπει να μειωθεί. Ο μόνος τρόπος που ο αποστολέας μπορεί να καταλάβει ότι έχει παρουσιαστεί συμφόρηση είναι η ανάγκη αναμετάδοσης ενός τμήματος. Η αναμετάδοση όμως μπορεί να συμβεί σε δύο περιπτώσεις: όταν λήξει ένα χρονόμετρο RTO ή όταν ληφθούν τρία ACK. Και στις δύο περιπτώσεις, το μέγεθος του ορίου μειώνεται στο μισό (μοναδιαία μείωση). Οι περισσότερες TCP υλοποιήσεις έχουν δύο αντιδράσεις:

1. Αν επέλθει λήξη χρόνου, υπάρχει μία ισχυρή πιθανότητα συμφόρησης και κάποιο τμήμα έχει προφανώς απορριφθεί στο δίκτυο και δεν υπάρχουν νέα για τα τμήματα που εστάλησαν μετά. Σε αυτήν την περίπτωση το TCP αντιδρά δυναμικά:
   α. Περνάει στην τιμή του ορίου το μισό του τρέχοντος μεγέθους παραθύρου.
   β. Περνάει στο cwnd το μέγεθος ενός τμήματος.
   γ. Ξεκινά ξανά τη φάση αργής εκκίνησης.
2. Αν ληφθούν τρία ACK, υπάρχει μία πιο μειωμένη πιθανότητα συμφόρησης και ένα τμήμα μπορεί να έχει απορριφθεί αλλά μερικά τμήματα μετά από αυτό μπορεί να έχουν φτάσει ασφαλώς καθώς έχουν ληφθεί τρία ACK. Αυτό ονομάζεται γρήγορη μετάδοση και γρήγορη ανάρρωση. Σε αυτήν την περίπτωση το TCP έχει μία πιο αδύναμη αντίδραση, όπως βλέπουμε παρακάτω:
   α. Περνάει στην τιμή του ορίου το μισό του τρέχοντος μεγέθους παραθύρου.
   β. Περνάει στο cwnd την τιμή του ορίου (μερικές υλοποιήσεις προσθέτουν τα μεγέθη τριών τμημάτων στο όριο).
   γ. Ξεκινά η φάση αποφυγής συμφόρησης.

6.7 ΧΡΟΝΟΜΕΤΡΑ TCP

Για να εκτελέσουν ομαλά τις λειτουργίες τους, οι περισσότερες υλοποιήσεις του TCP χρησιμοποιούν τουλάχιστον τέσσερα χρονόμετρα, όπως φαίνεται στην **Εικόνα παρακάτω.**



Χρονόμετρα TCP

Χρονόμετρο αναμετάδοσης

Για να αναμεταδώσει ένα απολεσθέν τμήμα, το TCP χρησιμοποιεί ένα χρονόμετρο αναμετάδοσης που διαχειρίζεται το χρόνο λήξης της αναμετάδοσης (RTO), το χρόνο αναμονής για την επιβεβαίωση ενός τμήματος. Όταν το TCP στέλνει ένα τμήμα, δημιουργεί ένα χρονόμετρο αναμετάδοσης για αυτό το συγκεκριμένο τμήμα. Τότε μπορεί να συμβούν δύο πράγματα:

1. Αν ληφθεί επιβεβαίωση για το συγκεκριμένο τμήμα πριν ξεκινήσει το χρονόμετρο, το χρονόμετρο καταστρέφεται.
2. Αν το χρονόμετρο ξεκινήσει πριν έρθει η επιβεβαίωση, το τμήμα αναμεταδίδεται και το χρονόμετρο μηδενίζεται.

Χρονόμετρο επιμονής

Για να χειριστεί μία διαφήμιση ενός παραθύρου μηδενικού μεγέθους, το TCP χρειάζεται ακόμα ένα χρονόμετρο. Αν το παραλαμβάνον TCP ανακοινώνει μέγεθος παραθύρου μηδέν, το αποστέλλον TCP σταματά να μεταδίδει τμήματα μέχρι το παραλαμβάνον TCP στείλει ένα τμήμα ACK που ανακοινώνει μη μηδενικό μέγεθος παραθύρου. Αυτό το τμήμα ACK μπορεί να χαθεί. Θυμηθείτε ότι τα τμήματα ACK δεν επιβεβαιώνονται στο TCP. Αν χαθεί αυτή η επιβεβαίωση, το παραλαμβάνον TCP πιστεύει ότι έκανε τη δουλειά του και περιμένει από το αποστέλλον TCP να στείλει περισσότερα τμήματα. Δεν υπάρχει χρονόμετρο αναμετάδοσης για ένα τμήμα που περιέχει μόνο μία επιβεβαίωση. Το αποστέλλον TCP δεν έχει λάβει επιβεβαίωση και περιμένει από το άλλο TCP να στείλει μία επιβεβαίωση που θα διαφημίζει το μέγεθος του παραθύρου.

Και τα δύο TCP μπορούν να συνεχίσουν να περιμένουν το ένα το άλλο για πάντα (αδιέξοδο). Για να διορθωθεί αυτό το αδιέξοδο, το TCP χρησιμοποιεί ένα χρονόμετρο επιμονής για κάθε σύνδεση. Όταν το αποστέλλον TCP λάβει μία επιβεβαίωση με μέγεθος παραθύρου μηδέν, ξεκινά ένα χρονόμετρο επιμονής. Όταν το χρονόμετρο επιμονής ξεκινήσει, το αποστέλλον TCP στέλνει ένα ειδικό τμήμα που ονομάζεται επισταμένη έρευνα. Αυτό το τμήμα περιέχει μόνο 1 byte δεδομένων. Έχει αριθμό σειράς αλλά αυτός ποτέ δεν επιβεβαιώνεται και μάλιστα αγνοείται στον υπολογισμό του αριθμού σειράς για τα υπόλοιπα δεδομένα. Η επισταμένη έρευνα ειδοποιεί το παραλαμβάνον TCP ότι η επιβεβαίωση χάθηκε και πρέπει να σταλεί ξανά.
Η τιμή του χρονομέτρου επιμονής παίρνει την τιμή του χρόνου αναμετάδοσης. Αν όμως δεν ληφθεί απάντηση από τον παραλήπτη, αποστέλλεται ακόμα ένα τμήμα επισταμένης έρευνας και η τιμή του χρονομέτρου επιμονής διπλασιάζεται και μηδενίζεται. Ο αποστολέας συνεχίζει να στέλνει τμήματα επισταμένης έρευνας και να διπλασιάζει και να μηδενίζει την τιμή του χρονομέτρου επιμονής μέχρι η τιμή να φτάσει στο όριο (συνήθως τα 60 δευτερόλεπτα). Μετά ο αποστολέας στέλνει ένα τμήμα επισταμένης έρευνας κάθε 60 δευτερόλεπτα μέχρι να ανοίξει πάλι το παράθυρο.

Χρονόμετρο διατήρησης στη ζωή

Το χρονόμετρο διατήρησης στη ζωή χρησιμοποιείται σε μερικές υλοποιήσεις για να αποτρέπεται μία σύνδεση μεταξύ δύο TCP που είναι πολύ καιρό ανενεργή. Υποθέτουμε ότι ένας client ανοίγει μία TCP σύνδεση σε ένα server, μεταφέρει μερικά δεδομένα και γίνεται silent. Ίσως ο client έχει καταρρεύσει. Σε αυτή την περίπτωση, η σύνδεση παραμένει ανοιχτή για πάντα.
Για να διορθωθεί αυτή η κατάσταση, οι περισσότερες υλοποιήσεις εξοπλίζουν ένα server με ένα χρονόμετρο διατήρησης στη ζωή. Κάθε στιγμή που ο server ακούει έναν client, μηδενίζει το χρονόμετρο. Ο χρόνος λήξης έρχεται συνήθως μετά από δύο ώρες. Αν ο server δεν ακούσει τον client μετά από δύο ώρες, στέλνει ένα τμήμα επισταμένης έρευνας. Αν δεν υπάρχει απάντηση μετά από 10 τέτοια τμήματα, τα οποία απέχουν μεταξύ τους 75 δευτερόλεπτα, υποθέτει ότι ο client έχει καταρρεύσει και τερματίζει τη σύνδεση.

Χρονόμετρο αναμονής

Το χρονόμετρο TIME-WAIT (2MSL) χρησιμοποιείται κατά τον τερματισμό σύνδεσης.

7 ΕΠΟΜΕΝΗ ΓΕΝΙΑ: IPv6

Το πρωτόκολλο επιπέδου δικτύου της οικογένειας πρωτοκόλλων TCP/IP βρίσκεται στην έκδοση IPv4 (Internetworking Protocol, έκδοση 4). Το IPv4 παρέχει επικοινωνία κεντρικού υπολογιστή με κεντρικό υπολογιστή μεταξύ συστημάτων στο Internet. Αν και το IPv4 είναι καλά σχεδιασμένο, η επικοινωνία δεδομένων έχει εξελιχθεί από την έναρξη του IPv4 τη δεκαετία του 1970. Το IPv4 έχει τις εξής ατέλειες, που το καθιστούν ακατάλληλο για το Internet που μεγαλώνει συνέχεια:

- Παρά τις βραχυπρόθεσμες λύσεις, όπως η διαίρεση δικτύου, η διευθυνσιοδότηση χωρίς κλάσεις και το NAT, η μείωση των διευθύνσεων εξακολουθεί να είναι σοβαρό πρόβλημα για το Internet.
- Το Internet πρέπει να εξυπηρετεί τη μετάδοση ήχου και εικόνας σε πραγματικό χρόνο. Αυτός ο τύπος μετάδοσης απαιτεί στρατηγικές ελάχιστης καθυστέρησης δέσμευσης των πόρων, κάτι που δεν προσφέρει το IPv4.
- Το Internet πρέπει να εξυπηρετεί κρυπτογραφία και αυθεντικοποίηση δεδομένων για κάποιες εφαρμογές. Δεν παρέχονται υπηρεσίες κρυπτογραφίας ή αυθεντικοποίησης στο IPv4.

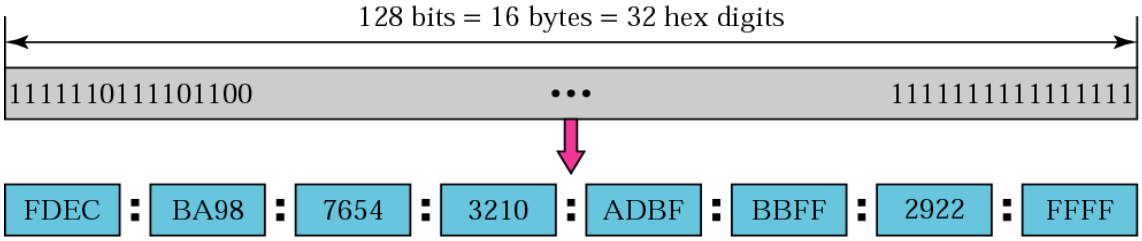
Για να καλύψει αυτές τις ατέλειες, προτάθηκε το IPv6 (Internetworking Protocol, έκδοση 6), επίσης γνωστό ως IPng (Internetworking Protocol, επόμενη γενιά) που αποτελεί τώρα ένα πρότυπο. Στο IPv6, το Internet Protocol τροποποιήθηκε ριζικά για να εξυπηρετήσει την προβλεπόμενη αύξηση του Internet. Η μορφή και το μήκος των διευθύνσεων IP άλλαξαν μαζί με τη μορφή του πακέτου. Άλλαξαν επίσης και σχετικά πρωτόκολλα, όπως το ICMP. Άλλα πρωτόκολλα στο επίπεδο δικτύου, όπως τα ARP, RARP, και IGMP, διαγράφηκαν ή συμπεριλήφθηκαν στο πρωτόκολλο ICMPv6. Πρωτόκολλα δρομολόγησης, όπως τα RIP και OSPF, επίσης τροποποιήθηκαν ελαφρώς για να εξυπηρετήσουν αυτές τις αλλαγές. Οι ειδικοί στην επικοινωνία προβλέπουν ότι το IPv6 και τα σχετικά πρωτόκολλα σύντομα θα αντικαταστήσουν την τρέχουσα έκδοση του IP. Η υιοθέτηση του IPv6 ήταν αργή. Ο λόγος είναι ότι η αρχική αιτία για την ανάπτυξή του, η μείωση των διευθύνσεων IPv4, καθυστέρησε εξαιτίας τριών βραχυπρόθεσμων διορθώσεων: διευθυνσιοδότηση χωρίς κλάσεις, χρήση του DHCP για δυναμική κατανομή διεύθυνσης και NAT. Η αυξανόμενη χρήση όμως του Internet και νέες υπηρεσίες, όπως το κινητό IP, η τηλεφωνία IP και η κινητή τηλεφωνία με δυνατότητες IP, πιθανώς θα επιβάλουν την ολοκληρωτική αντικατάσταση του IPv4 με το IPv6.

Το IP επόμενης γενιάς, ή IPv6, έχει μερικά πλεονεκτήματα σε σχέση με το IPv4 που μπορούν να συνοψιστούν ως εξής:

- **Μεγαλύτερος χώρος διευθύνσεων.** Μία διεύθυνση IPv6 έχει μήκος 128 bits. Σε σύγκριση με τη διεύθυνση IPv4 που έχει μήκος 32 bits, επέρχεται μία τεράστια αύξηση στο χώρο διευθύνσεων.
- **Καλύτερη μορφή κεφαλίδας.** Το IPv6 χρησιμοποιεί μία νέα μορφή κεφαλίδας στην οποία οι επιλογές χωρίζονται από τη βασική κεφαλίδα και εισάγονται, όταν χρειάζεται, μεταξύ της βασικής κεφαλίδας και των δεδομένων των ανώτερων επιπέδων. Απλοποιείται και επιτυγχάνεται έτσι η διαδικασία δρομολόγησης επειδή οι περισσότερες επιλογές δεν χρειάζεται να ελέγχονται από δρομολογητές.
- **Νέες επιλογές.** Το IPv6 έχει νέες επιλογές που επιτρέπουν επιπλέον λειτουργίες.
- **Πρόβλεψη για επέκταση.** Το IPv6 σχεδιάστηκε έτσι, ώστε να επιτρέπει την επέκταση του πρωτοκόλλου αν αυτό είναι απαραίτητο για νέες τεχνολογίες ή εφαρμογές.
- **Υποστήριξη για κατανομή πόρων.** Στο IPv6, το πεδίο τύπου υπηρεσίας έχει αφαιρεθεί αλλά έχει προστεθεί ένας μηχανισμός (ονομάζεται ετικέτα ροής) που δίνει δυνατότητα στην πηγή να αιτείται ειδικό χειρισμό του πακέτου. Αυτός ο μηχανισμός μπορεί να χρησιμοποιηθεί για να υποστηρίξει την κίνηση, όπως ήχου και βίντεο, σε πραγματικό χρόνο.
- **Υποστήριξη για περισσότερη ασφάλεια.** Οι επιλογές κρυπτογραφίας και αυθεντικοποίησης στο IPv6 παρέχουν εμπιστευτικότητα και ακεραιότητα για το πακέτο.

Διευθύνσεις IPv6

Μία διεύθυνση IPv6 αποτελείται από 16 bytes (οκτάδες) και έχει μήκος 128 bits (**δείτε την Εικόνα παρακάτω**).



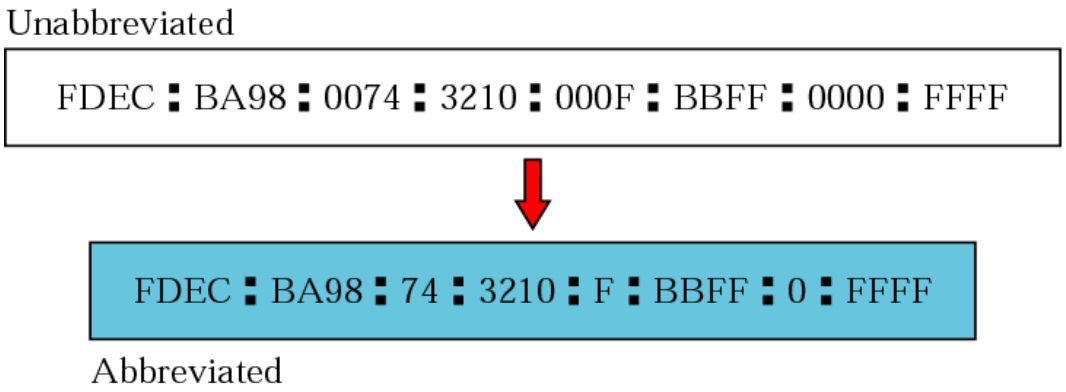
Διεύθυνση IPv6

Δεκαεξαδική γραφή

Για να γίνουν οι διευθύνσεις πιο ευανάγνωστες, το IPv6 ορίζει τη γραφή δεκαεξαδικού αριθμού. Με αυτήν τη μέθοδο γραφής, 128 bits χωρίζονται σε

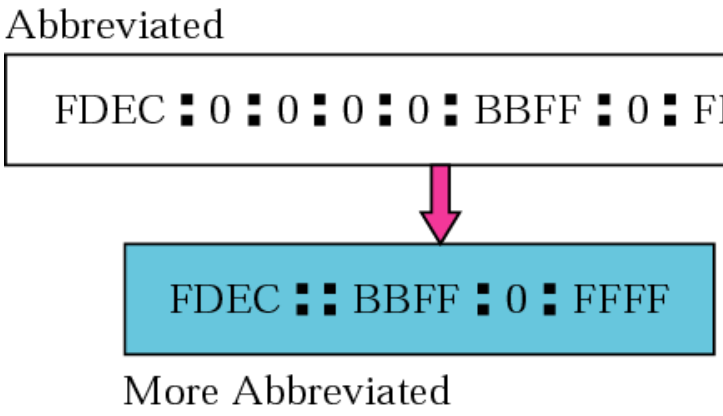
οκτώ ενότητες που κάθε μία έχει μήκος 2 bytes. Δύο bytes στη δεκαεξαδική γραφή χρειάζονται τέσσερα δεκαεξαδικά ψηφία. Επομένως, η διεύθυνση αποτελείται από 32 δεκαεξαδικά ψηφία, και κάθε 4, υπάρχει ένα σύμβολο ερωτηματικού.

Σύντμηση. Αν και η διεύθυνση IP, ακόμα και στη μορφή δεκαεξαδικού αριθμού, είναι πολύ μεγάλη, πολλά ψηφία είναι μηδενικά. Σε αυτήν την περίπτωση, μπορούμε να συντμήσουμε τη διεύθυνση. Τα μηδενικά στην αρχή ενός τμήματος (τέσσερα ψηφία μεταξύ δύο ερωτηματικών) μπορούν να παραληφθούν. Μόνο τα μηδενικά της αρχής μπορούν να αφαιρεθούν και όχι τα μηδενικά που βρίσκονται στο τέλος του αριθμού. Για παράδειγμα, βλέπουμε την **Εικόνα παρακάτω.**



Συντμημένη διεύθυνση

Χρησιμοποιώντας αυτήν τη μορφή σύντμησης, το 0074 μπορεί να γραφτεί ως 74, το 000F ως F και το 0000 ως 0. Σημειώνουμε ότι το 3210 δεν μπορεί να συντμηθεί. Επιπλέον συντμήσεις είναι εφικτές αν υπάρχουν συνεχόμενα τμήματα που αποτελούνται μόνο από μηδενικά. Μπορούμε να αφαιρέσουμε τα μηδενικά μαζικά και να τα αντικαταστήσουμε με ένα σύμβολο άνω και κάτω τελείας. **Η Εικόνα παρακάτω** παρουσιάζει αυτήν την έννοια.



Συντμημένη διεύθυνση με συνεχόμενα μηδενικά

Σημειώνουμε ότι αυτός ο τύπος σύντμησης επιτρέπεται μόνο μία φορά ανά διεύθυνση. Αν υπάρχουν δύο σειρές τμημάτων με μηδενικά, μόνο μία από αυτές μπορεί να συντμηθεί. Η επαναφορά της συντμημένης διεύθυνσης είναι πολύ απλή: υπογραμμίζουμε τα μη συντμημένα τμήματα και εισάγουμε μηδενικά για να πάρουμε την αρχική, εκτεταμένη διεύθυνση.

Γραφή CIDR. Το IPv6 επιτρέπει διευθυνσιοδότηση χωρίς κλάσεις και γραφή CIDR. Για παράδειγμα, **η Εικόνα παρακάτω** δείχνει πώς μπορούμε να ορίσουμε ένα πρόθεμα των 60 bits χρησιμοποιώντας CIDR.

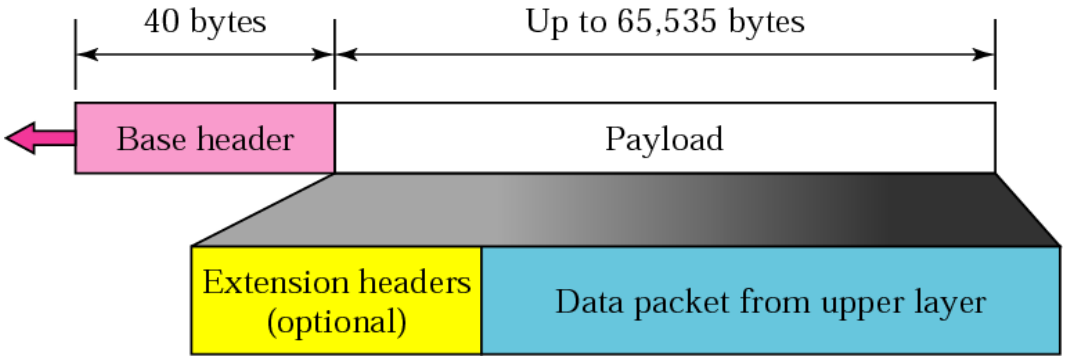
Διεύθυνση CIDR

Κατηγορίες διευθύνσεων

Το IPv6 ορίζει τρεις τύπους διευθύνσεων: unicast, anycast και multicast.
Μία unicast διεύθυνση ορίζει έναν υπολογιστή. Το πακέτο που αποστέλλεται σε μία unicast διεύθυνση πρέπει να παραδοθεί σε εκείνο το συγκεκριμένο υπολογιστή.
Μία anycast διεύθυνση ορίζει μία ομάδα υπολογιστών με διευθύνσεις που έχουν το ίδιο πρόθεμα. Για παράδειγμα, όλοι οι υπολογιστές που συνδέονται στο ίδιο φυσικό δίκτυο μοιράζονται την ίδια διεύθυνση προθέματος. Ένα πακέτο που αποστέλλεται σε κάποια anycast διεύθυνση πρέπει να παραδοθεί μόνο σε ένα από τα μέλη της ομάδας – το πιο κοντινό ή το πιο εύκολα προσπελάσιμο.
Μία διεύθυνση multicast ορίζει μία ομάδα υπολογιστών. Ένα πακέτο που αποστέλλεται σε μία multicast διεύθυνση πρέπει να παραδοθεί σε κάθε μέλος της ομάδας.

Μορφή πακέτου

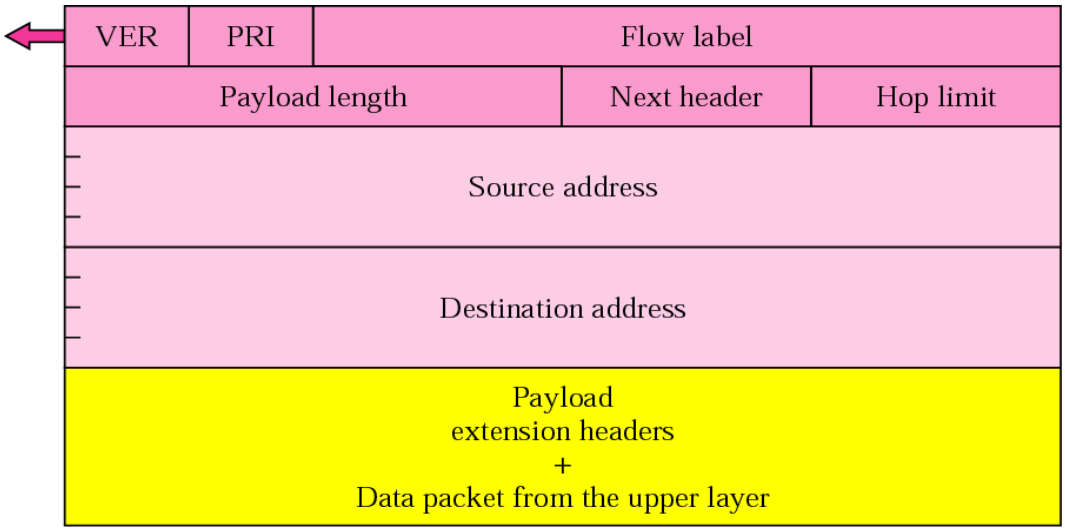
Το πακέτο IPv6 παρουσιάζεται στην **Εικόνα παρακάτω**. Κάθε πακέτο αποτελείται από μία υποχρεωτική βασική κεφαλίδα που ακολουθείται από το ωφέλιμο φορτίο. Το ωφέλιμο φορτίο αποτελείται από δύο μέρη: προαιρετικές κεφαλίδες επέκτασης και δεδομένα από ανώτερο επίπεδο. Η βασική κεφαλίδα καταλαμβάνει 40 bytes, ενώ οι κεφαλίδες επέκτασης και τα δεδομένα από το ανώτερο επίπεδο περιέχουν έως και 65.535 bytes πληροφοριών.



Διάγραμμα δεδομένων IPv6

Βασική κεφαλίδα

Η Εικόνα παρακάτω παρουσιάζει τη βασική επικεφαλίδα με τα οχτώ πεδία της.



Μορφή ενός διαγράμματος δεδομένων IPv6

Αυτά τα πεδία είναι τα εξής:

- **Έκδοση.** Αυτό το πεδίο των 4 bits ορίζει τον αριθμό έκδοσης του IP. Για το IPv6, η τιμή είναι 6.
- **Προτεραιότητα.** Αυτό το πεδίο προτεραιότητας των 4 bits ορίζει την προτεραιότητα του πακέτου έχοντας υπόψη τη συμφόρηση.
- **Ετικέτα ροής.** Η ετικέτα ροής είναι ένα πεδίο με 3 bytes (24 bits) που σχεδιάστηκε για να παρέχει ειδικό χειρισμό σε μία συγκεκριμένη ροή δεδομένων.

- **Ωφέλιμο φορτίο μήκους.** Το πεδίο ωφέλιμου φορτίου μήκους 2 bytes ορίζει το μήκος του διαγράμματος δεδομένων IP εκτός από τη βασική κεφαλίδα.
- **Επόμενη κεφαλίδα.** Η επόμενη κεφαλίδα είναι ένα πεδίο με 8 bits που ορίζει την κεφαλίδα που ακολουθεί τη βασική κεφαλίδα στο διάγραμμα δεδομένων. Η επόμενη κεφαλίδα είναι μία από τις προαιρετικές κεφαλίδες επέκτασης που χρησιμοποιούνται από το IP ή η κεφαλίδα ενός ενσωματωμένου πακέτου όπως το UDP ή το TCP. Κάθε κεφαλίδα επέκτασης επίσης περιέχει αυτό το πεδίο. **Ο Πίνακας παρακάτω** παρουσιάζει τις τιμές των επόμενων κεφαλίδων. Σημειώνουμε ότι το πεδίο αυτό στην έκδοση 4 ονομάζεται πρωτόκολλο.

Code	*Next Header*
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (No next header)
60	Destination option

Κωδικοί επόμενης κεφαλίδας

- **Όριο σταθμού.** Αυτό το πεδίο των 8 bits για το όριο σταθμού εξυπηρετεί τον ίδιο σκοπό με το πεδίο TTL στο IPv4.
- **Διεύθυνση πηγής.** Το πεδίο διεύθυνσης πηγής έχει μήκος 16 bytes (128 bits) και είναι μία Internet διεύθυνση που αναγνωρίζει την αρχική πηγή του διαγράμματος δεδομένων.
- **Διεύθυνση προορισμού.** Το πεδίο διεύθυνσης προορισμού έχει μήκος 16 bytes (128 bits) και είναι μία Internet διεύθυνση που συνήθως

αναγνωρίζει τον τελικό προορισμό του διαγράμματος δεδομένων. Αν όμως χρησιμοποιείται δρομολόγηση πηγής, αυτό το πεδίο περιέχει τη διεύθυνση του επόμενου δρομολογητή.

Προτεραιότητα

Το πεδίο προτεραιότητας του πακέτου IPv6 ορίζει την προτεραιότητα κάθε πακέτου έχοντας υπόψη και άλλα πακέτα από την ίδια πηγή. Για παράδειγμα, αν ένα από τα δύο συνεχόμενα διαγράμματα δεδομένων πρέπει να απορριφθεί λόγω της συμφόρησης, το διάγραμμα δεδομένων με τη χαμηλότερη προτεραιότητα πακέτου θα είναι αυτό που θα απορριφθεί. Το IPv6 χωρίζει την κίνηση σε δύο μεγάλες κατηγορίες: ελεγχόμενης συμφόρησης και μη ελεγχόμενης συμφόρησης.
Κίνηση ελεγχόμενης συμφόρησης. Αν μία πηγή προσαρμοστεί σε καθυστέρηση κίνησης όταν υπάρχει συμφόρηση, η κίνηση ονομάζεται κίνηση ελεγχόμενης συμφόρησης. Για παράδειγμα, το TCP, το οποίο χρησιμοποιεί το πρωτόκολλο κυλιόμενου παραθύρου, μπορεί εύκολα να απαντήσει στην κίνηση. Στην κίνηση ελεγχόμενης συμφόρησης, καταλαβαίνουμε ότι τα πακέτα μπορεί να φτάνουν καθυστερημένα ή να χάνονται ή να λαμβάνονται εκτός σειράς. Τα δεδομένα ελεγχόμενης συμφόρησης παίρνουν προτεραιότητες από 0 ως 7, όπως φαίνεται στον **Πίνακα παρακάτω**. Η προτεραιότητα 0 είναι η χαμηλότερη και η προτεραιότητα 7 είναι η υψηλότερη.

Priority	*Meaning*
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

Προτεραιότητες για την κίνηση ελεγχόμενης συμφόρησης

Οι περιγραφές της προτεραιότητας είναι οι εξής:

- **Καμία συγκεκριμένη κίνηση.** Η προτεραιότητα 0 εκχωρείται σε ένα πακέτο όταν η διαδικασία δεν ορίζει προτεραιότητα.

- **Δεδομένα παρασκηνίου.** Αυτή η ομάδα (προτεραιότητα 1) ορίζει δεδομένα που συνήθως παραδίδονται στο παρασκήνιο. Η παράδοση των ειδήσεων είναι ένα καλό παράδειγμα.
- **Μη ελεγχόμενη κίνηση δεδομένων.** Αν ο χρήστης δεν περιμένει να ληφθούν δεδομένα, το πακέτο παίρνει προτεραιότητα 2. Η ηλεκτρονική αλληλογραφία ανήκει σε αυτήν την ομάδα. Ο παραλήπτης αλληλογραφίας δεν γνωρίζει πότε φτάνει ένα μήνυμα. Επιπλέον, ένα μήνυμα αποθηκεύεται συνήθως πριν προωθηθεί. Μία μικρή καθυστέρηση έχει πολύ λίγες επιπτώσεις.
- **Ελεγχόμενη κίνηση μαζικών δεδομένων.** Ένα πρωτόκολλο που μεταφέρει δεδομένα ενώ ο χρήστης περιμένει να τα λάβει (πιθανώς με καθυστέρηση) παίρνει προτεραιότητα 4. Τα FTP και HTTP ανήκουν σε αυτήν την ομάδα.
- **Διαλογική κίνηση.** Πρωτόκολλα όπως το TELNET που απαιτούν αλληλεπίδραση με το χρήστη ανήκουν στη δεύτερη υψηλότερη ομάδα προτεραιότητας (6).
- **Κίνηση ελέγχου.** Η κίνηση ελέγχου έχει την υψηλότερη προτεραιότητα (7). Πρωτόκολλα δρομολόγησης όπως τα OSPF και RIP και πρωτόκολλα διαχείρισης όπως το SNMP ανήκουν σε αυτήν την ομάδα.

Κίνηση όχι ελεγχόμενης συμφόρησης. Αναφέρεται στον τύπο κίνησης όπου αναμένεται η ελάχιστη καθυστέρηση. Η απόρριψη πακέτων δεν είναι επιθυμητή. Η αναμετάδοση στις περισσότερες περιπτώσεις είναι αδύνατη. Με άλλα λόγια, η πηγή δεν προσαρμόζεται στη συμφόρηση. Ο ήχος και το βίντεο πραγματικού χρόνου είναι παραδείγματα αυτού του είδους κίνησης.
Οι αριθμοί προτεραιότητας από 8 ως 15 εκχωρούνται στην κίνηση όχι ελεγχόμενης συμφόρησης. Αν και δεν υπάρχουν ακόμα συγκεκριμένες λειτουργίες που παίρνουν αυτές τις προτεραιότητες, αυτές εκχωρούνται ανάλογα με το πόσο επηρεάζεται η ποιότητα των ληφθέντων πακέτων αν κάποια από τα σταλμένα πακέτα απορριφθούν. Τα δεδομένα που περιέχουν τη μικρότερη δυνατή περιττή επανάληψη (όπως ήχος και βίντεο χαμηλής πιστότητας) μπορεί να πάρουν υψηλότερη προτεραιότητα (15). Τα δεδομένα που περιέχουν μεγαλύτερη περιττή επανάληψη (όπως ήχος και βίντεο χαμηλής πιστότητας) παίρνουν μία χαμηλότερη προτεραιότητα (8). Δείτε τον **Πίνακα παρακάτω.**

Priority	*Meaning*
8	Data with most redundancy
. . .	. . .
15	Data with least redundancy

Προτεραιότητες για την κίνηση όχι ελεγχόμενης συμφόρησης

8 ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Behrouz A. Forouzan, Πρωτόκολλο TCP/IP, Τρίτη Έκδοση, Μ. Γκιούρδας, 2006.

2. Tanenbaum Andrew S, Δίκτυα Υπολογιστών, Τέταρτη Αμερικανική Έκδοση, Εκδόσεις Κλειδάριθμος, 2003.

3. Joe Casad, Μάθετε το TCP/IP σε 24 ώρες, Τρίτη Έκδοση, Μ. Γκιούρδας.

4. Comer Daglas E, Διαδίκτυα με TCP/IP, Κλειδάριθμος.

5. William Stallings, Data and Computer Communications, Seventh Edition, Prentice Hall, 2004.

6. William Stallings, High-speed Networks TCP/IP and ATM design principles, First Edition, Prentice Hall, 1998.