ΕΚΔΟΣΕΙΣ "ΚΛΕΙΔΑΡΙΘΜΟΣ"

Βασίλης Θ. Τσαουσίδης

ΔΙΑΔΙΚΤΥΑΚΑ ΠΡΩΤΟΚΟΛΛΑ

Περιεχόμενα

Συγκριτική θεώρηση δικτυακών τεχνολογιών

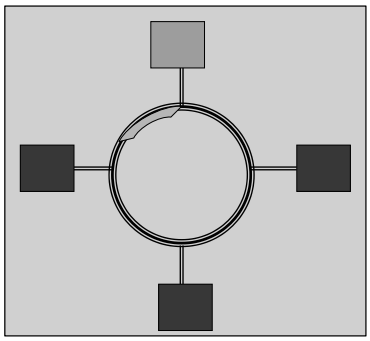
Ο στόχος μας από την συγκριτική θεώρηση δικτυακών τεχνολογιών που ακολουθεί είναι να αντιληφθούμε το μέγεθος της ετερογένειας ενός διαδικτύου και να κατανοήσουμε τις σχεδιαστικές αρχές της κάθε τεχνολογίας, καθώς επίσης και να αντιληφθούμε τι μπορεί να θεωρηθεί ως δεδομένη υπηρεσία και τι όχι σε ένα διαδίκτυο. Με βάση τις παρατηρήσεις μας, θα μπορούμε να αποφασίσουμε αργότερα για το πώς μπορούμε να σχεδιάσουμε διαδικτυακά πρωτόκολλα, ανάλογα με την τεχνολογία των κατώτερων στρωμάτων ή γενικότερα, πρωτόκολλα για όλα τα διαδίκτυα.

Θα συζητήσουμε συγκριτικά μερικά χαρακτηριστικά των τεχνολογιών Ethernet, Token Ring και Wireless.

Θεωρήστε ότι κάποιος καθηγητής διδάσκει σε μια τάξη φοιτητών. Ένας φοιτητής έχει μια απορία και αποφασίζει να την διατυπώσει αμέσως (χωρίς να ζητήσει άδεια). Ο καθηγητής δίνει την απάντηση και το μάθημα συνεχίζεται. Θεωρήστε επίσης τώρα ότι το μάθημα παρουσιάζει στη συνέχεια αρκετές δυσκολίες κατανόησης και επομένως πολλοί φοιτητές έχουν απορίες, τις οποίες αποφασίζουν να διατυπώσουν αμέσως, όπως ο φοιτητής προηγουμένως. Από τη στιγμή που μιλούν όλοι μαζί, ούτε ο καθηγητής, ούτε οι άλλοι φοιτητές μπορούν να διακρίνουν τις ερωτήσεις. Στο Ethernet

δίκτυο αυτή την κατάσταση την ονομάζουμε «σύγκρουση» (collision). Ενστικτωδώς, οι φοιτητές περιμένουν ένα τυχαίο χρονικό διάστημα και επαναλαμβάνουν την ερώτηση – αν και πάλι ρωτήσουν όλοι μαζί ίσως περιμένουν ακόμα περισσότερο την επόμενη φορά, προτού ξαναρωτήσουν. Όπως διαφαίνεται από την περιγραφή μας, όσο περισσότεροι είναι οι φοιτητές που διατυπώνουν ταυτόχρονα τις απορίες τους, τόσο δυσκολότερη η επικοινωνία με τον τρόπο της άμεσης και χωρίς – άδεια διατύπωσης.

Το παράδειγμά μας αναδεικνύει με εντυπωσιακή ακρίβεια τη λειτουργία/συμπεριφορά του δικτύου Ethernet. Ένας χρήστης Ethernet επιχειρεί να στείλει αμέσως τα δεδομένα του χωρίς να περιμένει άδεια και χωρίς να χρονοτριβεί. Η τακτική αυτή είναι σίγουρα αποτελεσματική όταν δεν υπάρχουν πολλοί χρήστες και δεν προκαλούνται *συγκρούσεις*. Διαφορετικά, μπορεί να αποδειχθεί αναποτελεσματική για όλους τους χρήστες. Αντιθέτως, η τακτική του δακτυλίου με κουπόνι (token ring) στοχεύει κυρίως στην ομαλή λειτουργία του δικτύου σε περιπτώσεις όπου υπάρχουν πολλοί χρήστες. Στο παράδειγμά μας τώρα, θεωρούμε ότι ο φοιτητής σηκώνει το χέρι του για να ζητήσει άδεια (να πάρει το κουπόνι) προτού διατυπώσει την απορία του. Αυτό ίσως παίρνει περισσότερο χρόνο μέχρι ο καθηγητής να δώσει το λόγο στο φοιτητή (ο καθηγητής μπορεί να γράφει στον πίνακα και να μην βλέπει τον φοιτητή, ή να περιμένει να ολοκληρώσει τη φράση του προτού δώσει άδεια). Στην περίπτωση όμως όπου πολλοί φοιτητές ταυτόχρονα θέλουν να διατυπώσουν απορίες, η τακτική της 'άδειας' δηλαδή του κουπονιού, αποδίδει πολύ καλύτερα. Θα πάρουν όλοι άδεια με τη σειρά και οι συγκρούσεις θα αποφευχθούν πλήρως.



Σχήμα 3-1. Δακτύλιος με κουπόνι

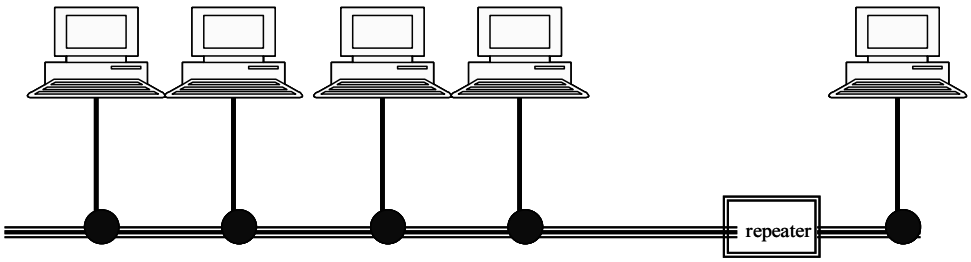
Επειδή η διαχείριση του κουπονιού γίνεται από κάποιον διαχειριστή, στο δακτύλιο με κουπόνι (σχ. 3-1) καθίσταται δυνατή και η ευέλικτη διαχείριση του δικτύου με βάση τις ανάγκες των εφαρμογών. Για παράδειγμα, ο διαχειριστής μπορεί να καθορίσει

τον χρόνο χρήσης του κουπονιού από έναν υπολογιστή (token holding time) καθώς και να θέσει περιορισμό στον συνολικό χρόνο περιφοράς του κουπονιού (token rotation time). Το τελευταίο είναι πολύ χρήσιμο για εφαρμογές (όπως κάποιες πολυμεσικές) που έχουν/πρέπει να στείλουν δεδομένα σε τακτά χρονικά διαστήματα προκειμένου να επιτύχουν καλύτερη ποιότητα υπηρεσιών (Quality of Service).

Ας δούμε τις λειουργίες των δύο τεχνολογιών λίγο πιο αναλυτικά.

3.1. Χαρακτηριστικά του Ethernet

Θεωρήστε το δίκτυο Ethernet του σχήματος 3-2.



Σχήμα 3-2. Δίκτυο Ethernet

Όλοι οι συνδεδεμένοι υπολογιστές μοιράζονται την πρόσβαση στο δίκτυο, το οποίο, όπως φαίνεται στο σχήμα 3-2, ενισχύεται από έναν επαναλήπτη. Το Ethernet ανήκει στην κατηγορία των δικτύων *πολλαπλής προσπέλασης με ανίχνευση φέροντος σήματος και ανίχνευση σύγκρουσης* (Carrier Sense Multiple Access with Collision Detection ή επιγραμματικά, CSMA/CD). Όταν υπάρχουν δεδομένα προς αποστολή, στέλνουμε τα δεδομένα μας, αφού πρώτα προσαρτήσουμε την ακόλουθη επικεφαλίδα

Ethernet Frame					
64	48	48	16		32
Preample	**Dest.Address**	**Src Address**	**Type**	**Body**	**CRC**

Αξίζει να παρατηρήσουμε τρία πράγματα.

1. Η επικεφαλίδα καθορίζει διευθύνσεις 48 bits, κάτι που προσδίδει ένα ιδιαίτερο χαρακτηριστικό στις διευθύνσεις των υπολογιστών που είναι συνδεδεμένοι σε Ethernet. Για παράδειγμα, οι διευθύνσεις αυτές δεν είναι αναγνώσιμες από άλλα δίκτυα.
2. Η επικεφαλίδα του Ethernet δεν περιέχει κανένα πεδίο που να ευνοεί την ποιότητα παροχής υπηρεσιών, τις προτεραιότητες χρηστών ή τις απαιτήσεις των εφαρμογών που απαιτούν συγχρονισμένη (σταθερού ρυθμού) μετάδοση δεδομένων.
3. Ακόμα και αν δεν έχουμε τίποτα να στείλουμε, πρέπει να 'γεμίσουμε' το πεδίο `body` της επικεφαλίδας με τέτοια ποσότητα δεδομένων, ώστε να εγγυηθούμε τη δυνατότητα ανίχνευσης των πιθανών συγκρούσεων. Η ποσότητα αυτή για ένα δίκτυο με Bandwidth 10Mbps και καθυστέρηση διάδοσης 25.6μs (RTT=51.2μs) είναι 512 bits.

Με άλλα λόγια, πρέπει να στείλουμε τουλάχιστον 512 bits προκειμένου να σιγουρευτούμε ότι, εφόσον υπήρχε σύγκρουση[1] στο μεσοδιάστημα μέχρι να φτάσει το σήμα από το ένα άκρο του δικτύου στο άλλο, ο αποστολέας δεν έχει ολοκληρώσει την αποστολή δεδομένων του. Με αυτόν τον τρόπο ο αποστολέας ανιχνεύει τις συγκρούσεις και αντιλαμβάνεται ότι τα δεδομένα που έστειλε δεν έχουν φθάσει στον προορισμό τους με επιτυχία. Μας ενδιαφέρει περισσότερο να τονίσουμε εδώ ότι ο αποστολέας έχει τη δυνατότητα να *ανιχνεύει* τις συγκρούσεις. Εφόσον ανιχνευθούν συγκρούσεις, η στρατηγική του Ethernet είναι η αναμονή μέχρι κάποιο χρονικό σημείο (χρονοθυρίδα), τυχαία εκλεγόμενο από μια κλίμακα αρχικού μεγέθους 51.1μs, κατά το οποίο θα επιχειρηθεί και πάλι η αποστολή δεδομένων. Το διάστημα αυτό μεγαλώνει εκθετικά εφόσον οι συγκρούσεις συνεχίζονται, μειώνοντας την πιθανότητα συγκρούσεων αφού επεκτείνεται η κλίμακα των χρονοθυρίδων.

Για την ακρίβεια, ο αλγόριθμος λειτουργεί ως εξής

[1] δύο υπολογιστές αποφάσισαν να στείλουν δεδομένα ταυτόχρονα, αφού διέγνωσαν ότι το κανάλι δεν είναι κατειλημμένο

Αν το κανάλι είναι ελεύθερο:
- Στείλε δεδομένα άμεσα με τους περιορισμούς
  - Μέγιστο μήκος δεδομένων 1500 bytes
  - Ελάχιστο μήκος δεδομένων 64 bytes

Αν το κανάλι είναι κατειλημμένο:
- Περίμενε μέχρι να ελευθερωθεί το κανάλι και κατόπιν στείλε άμεσα (*1-persistent* (*ειδική κατηγορία p-persistent*)

Εφόσον υπάρξει σύγκρουση:

- Ξαναπροσπάθησε μετά από κάποια καθυστέρηση
  - 1η φορά: ομοιόμορφα κατανεμημένη μεταξύ 0 και 51.2μs
  - 2η φορά: ομοιόμορφα κατανεμημένη μεταξύ 0 και 102.4μs
  - 3η φορά: ομοιόμορφα κατανεμημένη μεταξύ 0 και 204.8μs
  - παραιτήσου μετά από καποιο αριθμό προσπαθειών (συνήθως 16)

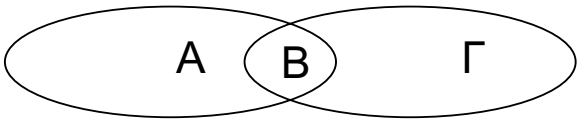
Παρατηρούμε ότι η λογική μας εδώ είναι να χρησιμοποιήσουμε άμεσα το κανάλι. Μόνο εφόσον υπάρχει σύγκρουση πρέπει να εφαρμόσουμε τον αλγόριθμο αποφυγής συγκρούσεων. Αξίζει τώρα να δούμε σε αντιπαράθεση τη λογική σχεδιασμού του ανάλογου αλγορίθμου στα ασύρματα δίκτυα.

3.2 Σύγκριση με ασύρματα δίκτυα

Στα ασύρματα δίκτυα υπάρχει ένα δεδομένο επιπλέον που δεν μπορούμε να αγνοήσουμε: η ύπαρξη *κρυφών* σταθμών. Κατά τα άλλα, τα τοπικά ασύρματα δίκτυα έχουν την ίδια φιλοσοφία 'πολλαπλής προσπέλασης με ανίχνευση φέροντος σήματος', όπως και το Ethernet. Ένας σταθμός λέγεται *κρυφός* (hidden node, σχ. 3-3) εφόσον βρίσκεται εκτός εμβέλειας του αποστολέα, όμως εντός της εμβέλειας του παραλήπτη. Αυτό σημαίνει ότι ο κρυφός σταθμός δεν μπορεί να ανιχνεύσει πότε στέλνει δεδομένα ο απομακρυσμένος αποστολέας, ώστε να αποφύγει τη σύγκρουση.

Η ύπαρξη κρυφών σταθμών συνεπάγεται ουσιαστικά την αδυναμία ανίχνευσης των συγκρούσεων και επιβάλλει εξαρχής μία άλλη στρατηγική: την *αποφυγή* των συγκρούσεων. Η αποφυγή επιτυγχάνεται με πολύ παρόμοιο – με το Ethernet – τρόπο: τώρα η κλίμακα χρονοθυρίδων επεκτείνεται με βάση μια παράμετρο που ονομάζεται *ανταγωνιστικό παράθυρο* (contention window). Σημειώνουμε ότι η αποφυγή συγκρούσεων στα ασύρματα δίκτυα είναι πρωταρχικός στόχος, σε αντίθεση με το Ethernet όπου είναι δευτερεύων στόχος. Το Ethernet μπορεί να ανιχνεύσει τις συγκρούσεις, ενώ τα ασύρματα δίκτυα εφαρμόζουν ειδικά πρωτόκολλα για να τις αποφύγουν. Τα πρωτόκολλα αυτά προβλέπουν την ανταλλαγή μηνυμάτων RTS/CTS (Request-to-send

Clear-to-send) προκειμένου να αποφύγουν τις συγκρούσεις με τους κρυφούς σταθμούς.



Σχήμα 3-3. Κρυφός κόμβος. Ο Γ είναι εκτός εμβέλειας του Α.

Μπορούμε επίσης να προχωρήσουμε σε μερικές ακόμα παρατηρήσεις. Το δίκτυο Ethernet ουσιαστικά καλύπτει έναν χώρο που τον ονομάζουμε *χώρο συγκρούσεων* (collision domain). Μπορεί κανείς να ελέγχει το κανάλι και να αποφασίσει να στείλει δεδομένα μόνον εφόσον το κανάλι δεν χρησιμοποιείται από άλλους χρήστες. Σε περίπτωση που το κανάλι είναι κατειλημμένο, ο υποψήφιος χρήστης πρέπει να περιμένει μέχρις ότου το κανάλι περάσει σε κατάσταση απραξίας (idle state). Βέβαια, ο αποστολέας πρέπει να εξετάσει την πιθανότητα συγκρούσεων *και* αφού τελειώσει με την αποστολή των δεδομένων του (όχι μόνο πρίν), αφού υπάρχει ενδεχόμενο, την ώρα που το κανάλι 'φαινόταν' idle, κάποιος απομακρυσμένος χρήστης να έστελνε τα δικά του δεδομένα.

3.3 Δακτύλιος με κουπόνι

Σε αντιπαράθεση, ο δακτύλιος με κουπόνι αποτελεί επίσης ένα χώρο συγκρούσεων αφού, κατά κανόνα, κανείς δεν μπορεί να στείλει δεδομένα όταν κάποιος άλλος έχει το κουπόνι. Ο όρος «χώρος συγκρούσεων» δε χρησιμοποιείται σε αυτή την περίπτωση γιατί από το σχεδιασμό του ο δακτύλιος με κουπόνι δεν επιτρέπει τις συγκρούσεις. Αξίζει όμως να παρατηρήσουμε και να σχολιάσουμε ενδεικτικά μια επικεφαλίδα ενός δακτυλίου με κουπόνι, προκειμένου να βγάλουμε χρήσιμα συμπεράσματα για τη λειτουργικότητά του. Σημειώνουμε ότι ο δακτύλιος με κουπόνι χρησιμοποιείται από τα δίκτυα IBM 4Mbps, IEEE 802.5/token ring και 100Mbps FDDI (Fiber Distribution Data Interface).

8	8	48	48		32	8	24
Start of frame	**Ctrl**	**Dest. Address**	**Src Address**	**Body**	**CRC**	**End of Frame**	**Status**

- `SD(1)-AC(1)-FC(1)-DA(2/6)-SA(2/6)-Data-FCS(4)-ED(1)-FS(1)`

- SD/ED: Starting/Ending Delimiter
- AC: Access Control
  - P-P-P-T-M-R-R-R (T: token, M: monitor)
- FC: Frame Control
- FCS: Frame check sequence
- FS: Frame Status
  - A-C-r-r-A-C-r-r

Token Format: SD - AC - FC

Σχήμα 3-4. Τα πεδία Control και Status

Βλέπουμε λοιπόν στο σχήμα 3-4 ότι ο σχεδιαστής του δακτυλίου με κουπόνι έχει προβλέψει τα πεδία control και status. Το πρώτο επιτρέπει τη χρήση προτεραιοτήτων και κρατήσεων (reservation) του κουπονιού καθώς και τον διαχειριστικό έλεγχο από μια (εκλεγμένη) μονάδα. Το δεύτερο επιτρέπει ένα είδος αναφοράς σε σχέση με το αποτέλεσμα της προώθησης δεδομένων. Για παράδειγμα, όταν το A έχει τιμή 1 σημαίνει ότι ο παραλήπτης έχει ενημερωθεί για το μήνυμα του αποστολέα. Όταν το C έχει την τιμή 1 σημαίνει ότι ο παραλήπτης έχει επιπλέον αντιγράψει και επεξεργαστεί το μήνυμα.

Έχει ενδιαφέρον να εξετάσουμε και τον αλγόριθμο που καθορίζει την κυκλοφορία του κουπονιού στο δίκτυο και την δυνατότητα των συνδεδεμένων υπολογιστών να δεσμεύει το κουπόνι.

Ορίζουμε καταρχήν τις παρακάτω μονάδες:

Χρόνος χρήσης του κουπονιού THT (Token Holding Time) είναι ο χρόνος που επιτρέπεται σε κάποιον υπολογιστή να δεσμεύσει το κουπόνι. Προφανώς ο χρόνος 'μεταφράζεται' σε ποσότητα δεδομένων που μπορεί να στείλει ένας υπολογιστής.

Χρόνος περιφοράς του κουπονιού TRT (Token Rotation Time) είναι ο χρόνος που χρειάζεται το κουπόνι να ολοκληρώσει την περιφορά του στον δακτύλιο. Προφανώς, ο χρόνος αυτός εξαρτάται από τον αριθμό των υπολογιστών που έχουν δεδομένα για αποστολή (active nodes) και υπολογίζεται ως

TRT <= ActiveNodes x THT + Ring Latency

Χρονικό περιθώριο περιφοράς του κουπονιού TTRT (Target Token Rotation Time) είναι ο στόχος που θέτει το δίκτυο αναφορικά με το χρόνο περιφοράς του κουπονιού. Ο χρόνος αυτός καθορίζεται μέσα από μια ανταγωνιστική διαδικασία προτάσεων των συνδεδεμένων υπολογιστών. Αυτό δικαιολογείται μεθοδολογικά, αν αναλογιστούμε ότι ο χρόνος περιφοράς του κουπονιού προσδιορίζει το χρόνο που θα χρειαστεί για να μπορέσει να ξαναπάρει το κουπόνι ένας υπολογιστής. Ο χρόνος αυτός προσδιορίζει και την ποιότητα παροχής υπηρεσιών όταν οι υπολογιστές 'τρέχουν' εφαρμογές που απαιτούν συνεχή και σταθερού ρυθμού μετάδοση δεδομένων. Με βάση λοιπόν το σκεπτικό μας, είναι λογικό από αυτή την ανταγωνιστική διαδικασία να κερδίζει ο υπολογιστής που απαιτεί το μικρότερο χρόνο περιφοράς (αφού έτσι ουσιαστικά εξυπηρετούνται και οι υπολογιστές που απαιτούν μεγαλύτερο χρόνο περιφοράς).

Αρχικά λοιπόν, κάθε σταθμός μετράει το `TRT` (measured TRT) μεταξύ δύο διαδοχικών αφίξεων του κουπονιού. Αν το

measured TRT> TTRT => late token

δηλαδή το κουπόνι έχει αφιχθεί με καθυστέρηση η αποστολή δεδομένων δεν είναι δυνατή. Διαφορετικά, ο σταθμός δικαιούται να κρατήσει το κουπόνι.

Υπάρχει και μία διάκριση στο είδος της επικοινωνίας (σύγχρονη/ασύγχρονη). Εφόσον η επικοινωνία απαιτεί συγχρονισμό (με την έννοια της σταθερής ροής δεδομένων), ο συνδεδεμένος κόμβος (υπολογιστής) δικαιούται να υπερβεί το όριο του TTRT κατά ένα TTRT. Επομένως, ο μέγιστος[2] χρόνος περιφοράς του κουπονιού είναι 2TTRT.

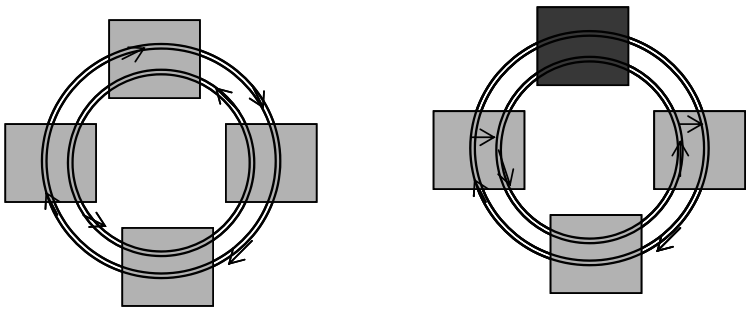
Τέλος, υπάρχει η ανάγκη διαχειριστκού ελέγχου του κουπονιού από κάποιον διαχειριστή, ο οποίος εκλέγεται από τους σταθμούς του δικτύου. Η αρμοδιότητά του είναι να ασχολείται (ι) με τα 'ορφανά' δεδομένα, αυτά δηλαδή που έχουν αποσταλεί όμως παραμένουν στο δίκτυο διότι ο αποστολέας (ο οποίος έχει και την αρμοδιότητα να τα αποσύρει από το δίκτυο) έχει τεθεί για κάποιο λόγο εκτός λειτουργίας ή (ιι) με τις περιπτώσεις κουπονιών που έχουν υποστεί μεταβολή και κυκλοφορούν στον δακτύλιο χωρίς να αναγνωρίζονται από τους σταθμούς του δικτύου.

Ένα πλεονέκτημα του δακτυλίου με κουπόνι είναι η αξιοπιστία του αφού επιτρέπει και τον διπλό δακτύλιο (dual ring configuration, σχ. 3-5), ο οποίος παρέχει τη δυνατότητα λειτουργίας του δακτυλίου ακόμη και αν κάποιος σταθμός τεθεί εκτός λειτουργίας. Όπως φαίνεται στο παρακάτω σχήμα, ο δακτύλιος αναμορφώνεται μέσω ενός ελά-

[2] όταν έχουμε σύχγρονη επικοινωνία και η οποία μάλιστα πρέπει να έπεται της ασύγχρονης

σματος που δημιουργεί κύκλωμα με τους υπόλοιπους σταθμούς, αλλάζοντας τη ροή του κουπονιού.

Συμπερασματικά μπορούμε να πούμε ότι ο δακτύλιος με κουπόνι λύνει το πρόβλημα των συγκρούσεων, παρέχει μεγαλύτερη αξιοπιστία και επιτρέπει καλύτερη ποιότητα παροχής υπηρεσιών από το Ethernet, με κόστος την χαμηλότερη απόδοση σε περιόδους περιορισμένης χρήσης του δικτύου και υψηλότερο κόστος διαχείρισης, εγκατάστασης και συντήρησης.



Σχήμα 3-5. Διπλός δακτύλιος.

Ανεξάρτητα από τις διαφορές τους, το Ethernet και το Token Ring είναι αξιόπιστα (reliable) δίκτυα μετάδοσης δεδομένων με πολύ χαμηλή πιθανότητα λάθους κατά τη μεταφορά πακέτων. Αντιθέτως, τα ασύρματα δίκτυα έχουν χαμηλή αξιοπιστία. Για παράδειγμα, όταν χάνεται ένα πακέτο πάνω από ένα ασύρματο δίκτυο δεν μπορεί να θεωρήσει κανείς την συμφόρηση ως την πιο πιθανή αιτία του προβλήματος, αλλά ενδεχομένως και κάποιους εξωγενείς παράγοντες που επηρεάζουν το κανάλι επικοινωνίας. Επιπλέον, σε ένα ασύρματο δίκτυο δεν μπορεί κανείς να ανιχνεύσει τις συγκρούσεις (δεν έχει εγγυήσεις ότι όλοι οι δικτυωμένοι χρήστες λαμβάνουν σήμα από όλους) και επομένως η στρατηγική αποφυγής των συγκρούσεων είναι διαφορετική, λιγότερο αποτελεσματική και πιο χρονοβόρα.

Ας αναλογιστούμε τώρα πώς επηρεάζουν αυτά τα διαφορετικά χαρακτηριστικά δικτύων τον σχεδιασμό πρωτοκόλλων ενός διαδικτύου. Το διαδίκτυό μας θα έχει ετερογένεια στην ταχύτητα των επιμέρους καναλιών. Ο αποστολέας και ο παραλήπτης δεν θα γνωρίζουν εξαρχής ποια είναι η χωρητικότητα του δικτύου. Λόγω της πιθανότητας ύπαρξης αναξιόπιστων δικτύων (όπως το ασύρματο δίκτυο), η αποτυχημένη αποστολή ενός πακέτου δεν θα μπορεί να σηματοδοτήσει την παρουσία συμφόρησης στο διαδίκτυο. Η ποιότητα παροχής υπηρεσιών δεν μπορεί να είναι εγγυημένη στους χρήστες. Η αξιοπιστία στη μεταφορά πακέτων επίσης δεν μπορεί να είναι δεδομένη.

ΔΙΑΔΙΚΤΥΑΚΑ ΠΡΩΤΟΚΟΛΛΑ

Τα διαδικτυακά πρωτόκολλα αποτελούν τη βάση της τεχνολογίας του Διαδικτύου.

Με βάση ποιές αρχές σχεδιάστηκαν; Πώς αλληλεπιδρούν στην απόδοση τους η δικτυακή υποδομή, οι δικτυακές εφαρμογές και η πληθώρα των χρηστών; Πώς αντιμετωπίζουν την ετερογένεια των τοπικών δικτύων, τη συμφόρηση και τις απαιτήσεις ποιότητας στην παροχή υπηρεσιών; Πώς συνεργάζονται μεταξύ τους, ώστε να αποφεύγουν τις επικαλύψεις λειτουργικότητας;

Το βιβλίο απαντά στα ερωτήματα αυτά χρησιμοποιώντας μια μεθοδολογία εναποιημένης παρουσίασης των συναφών εννοιών, ακολουθώντας την πιο πρόσφατη τάση διδασκαλίας των δικτύων/διαδικτύων, σε αντίθεση με την παραδοσιακή θεώρηση των "λειτουργικών στρωμάτων". Μια σειρά εργαστηριακών ασκήσεων και πειραμάτων στο τελευταίο κεφάλαιο δίνει τη δυνατότητα στον αναγνώστη να διαπιστώσει στην πράξη τις λειτουργίες και τις διαφορές των διαδικτυακών πρωτοκόλλων.

Ίσως αναρωτηθεί κανείς πόσο διαχρονική είναι η θεματολογία αυτού του βιβλίου. Η έμφαση δίνεται κυρίως στους μηχανισμούς και στις σχεδιαστικές αρχές του Διαδικτύου και κάθε διαδικτύου. Σκεφτείτε ότι το Διαδίκτυο έχει μια ιδιοτυπία σε σχέση με άλλα δίκτυα: είναι ένα σύνολο αυτόνομων δικτύων χωρίς κεντρική διαχείριση. Αυτό σημαίνει ότι αναπτύσσεται χωρίς ομοιομορφία και ότι φιλοξενεί, παράλληλα, πρωτόκολλα δοκιμασμένα και πιθανώς ξεπερασμένα μαζί με πρωτόκολλα μοντέρνα και πιθανώς πειραματικά. Αυτή η "συμβίωση" δεν είναι επιλογή σχεδιασμένη αλλά πηγάζει από τη λειτουργική δομή του και την αυτονομία του.

Ο συγγραφέας

Ο **Βασίλης Τσαουσίδης** ειδικεύεται στα δίκτυα υπολογιστών. Πήρε το διδακτορικό δίπλωμα από το τμήμα Επιστήμης Υπολογιστών του πανεπιστημίου Humboldt του Βερολίνου και δίδαξε στα πανεπιστήμια Rutgers του Νιου Τζέρσευ, SUNY Stony Brook της Νέας Υόρκης, Northeastern της Βοστώνης και στο Δημοκρίτειο Πανεπιστήμιο Θράκης. Ο Βασίλης Τσαουσίδης ειναι στην ομάδα εκδοτών των διεθνών περιοδικών IEEE Transactions on Mobile Computing, Computer Networks και International Journal of Wireless Communications and Mobile Computing και διετέλεσε πρόεδρος πολλών διεθνών συνεδρίων. Εχει δημοσιεύσει 60 ερευνητικές εργασίες και έχει επιβλέψει διδακτορικές και μεταπτυχιακές διατριβές σε πανεπιστήμια της Αμερικής.

Επισκεφθείτε μας στο Internet:
http://www.klidarithmos.gr

ISBN 960-209-746-9

ΚΛΕΙΔΑΡΙΘΜΟΣ
Σολωμού 57, 10432, ΑΘΗΝΑ, Τηλ. 210-5237635