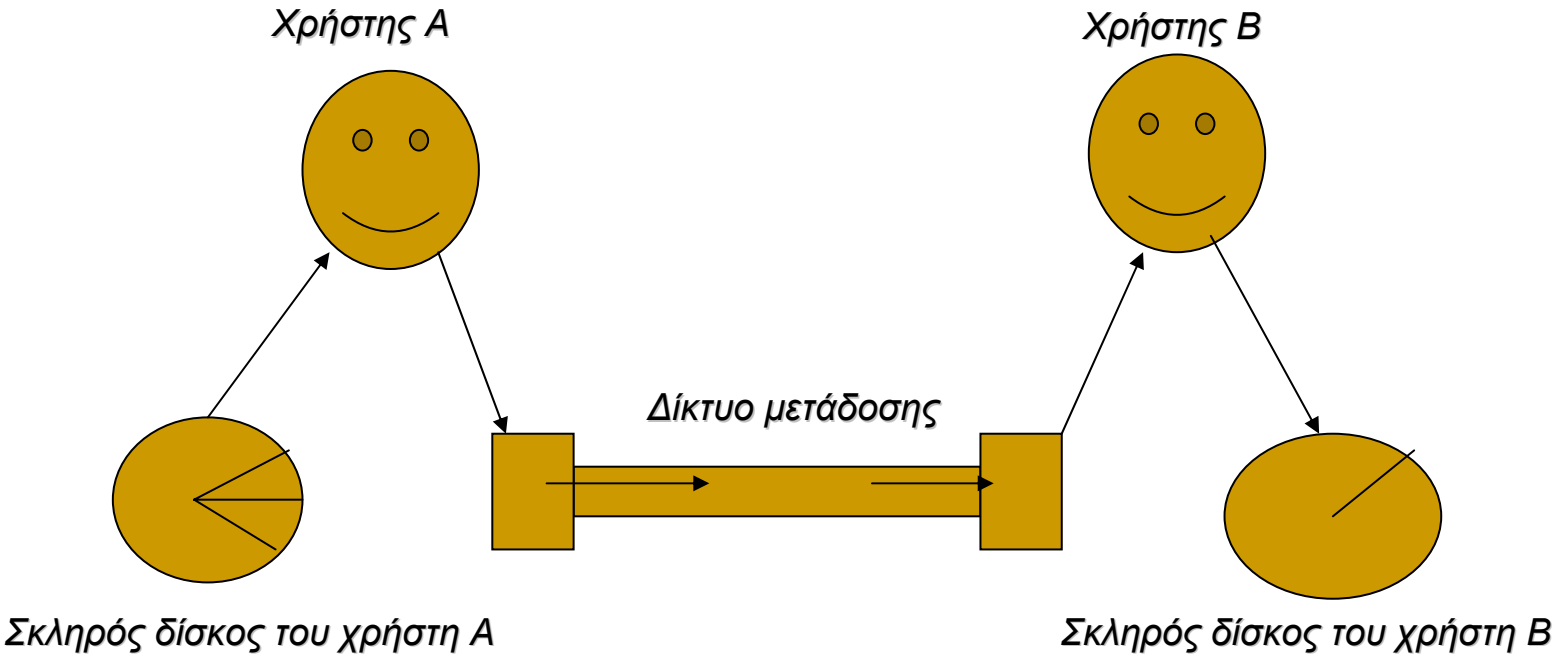
Γενικές αρχές του Δικτύου – Η Αρχή «από άκρο σε άκρο» (End-to-End Argument)

Εισαγωγή

- Βασική αρχή του σχεδιαστή οποιουδήποτε συστήματος είναι ο σαφής προσδιορισμός του πώς κάθε συνάρτηση (λειτουργία) που υπεισέρχεται στο σύστημα αλληλεπιδρά με τις υπόλοιπες.
- Θέματα που ανακύπτουν στα τηλεπικοινωνιακά συστήματα: πού θα υλοποιούνται οι συναρτήσεις?
  - Στο υποσύστημα που αποτελεί τον κορμό του δικτύου?
  - Στον πελάτη/χρήστη του δικτύου?
  - Από κοινού και στα δύο παραπάνω?
  - Η κάθε πλευρά (δίκτυο-χρήστης) θα έχει τις δικές της συναρτήσεις?

Παράδειγμα: Μεταφορά αρχείων (File Transfer)



«Απειλές» για τη σωστή μεταφορά αρχείων

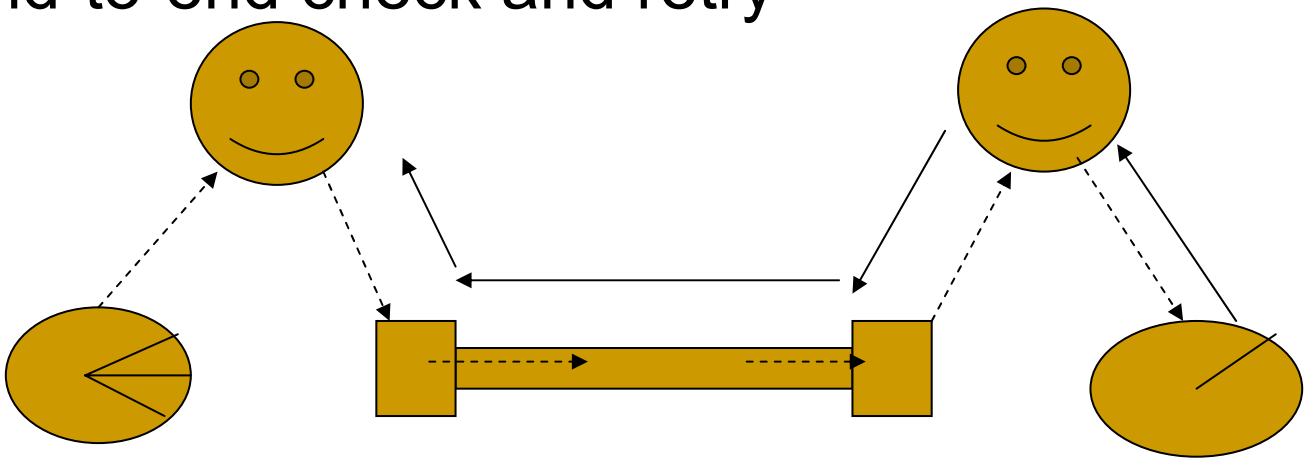
1. «Χτυπημένος» δίσκος του χρήστη Α, στα sectors που βρίσκεται το αρχείο
2. Σφάλματα software, είτε στο σύστημα αρχείων, είτε στο πρωτόκολλο μεταφοράς, είτε στο τηλεπικοινωνιακό δίκτυο (για παράδειγμα σφάλματα στο buffering ή στην αντιγραφή του αρχείου)
3. Σφάλματα hardware
4. Το τηλεπικοινωνιακό δίκτυο μπορεί να χάσει πακέτα, ή να διπλοπαραδώσει κάποια κ.ο.κ.
5. Κάποιος από τους Α,Β να «καταρρεύσει» στα μισά της διαδικασίας
6. …

Πώς αντιμετωπίζουμε τους κινδύνους?

- Προσεχτική σχεδίαση του συστήματος (πρωτόκολλα time-out/retry, κωδικοποίηση για ανίχνευση σφαλμάτων, πολλαπλές αποστολές των πακέτων κ.ο.κ.)
- Ωστόσο:
  - Δεν υπάρχουν τέλεια προγράμματα (εξασφάλιση μηδενικών σφαλμάτων software είναι ουσιαστικά αδύνατη).
  - Αν τα σφάλματα έχουν μικρή πιθανότητα εμφάνισης (ρεαλιστική θεώρηση), τότε η παραπάνω λύση κοστίζει

Εναλλακτική προσέγγιση (από άκρο σε άκρο)

- End-to-end check and retry



  - Ο Α υπολογίζει το checksum των δεδομένων του πριν τα αποστείλει. Ο Β υπολογίζει το checksum αυτών που λαμβάνει. Αν ο κώδικας βάσει του οποίου υπολογίζεται το checksum είναι κατάλληλα επιλεγμένος, ταύτιση των παραπάνω δύο checksums συνεπάγεται ορθή μεταφορά του αρχείου.
  - Αν τα checksums δεν συμφωνούν (κάτι που λογικά θα γίνεται σπάνια), γίνεται επαναμετάδοση.

Ένα «αξιόπιστο» δίκτυο δεδομένων πώς βοηθάει?

- Μειώνει την πιθανότητα απώλειας ή διπλοπαράδοσης πακέτων (απειλή 4), αλλά οι υπόλοιπες απειλές παραμένουν. Συνεπώς, ο checksum έλεγχος στα άκρα είναι αναπόφευκτος. Συνεπώς:
- Οι πρόσθετες τεχνικές για μείωση λαθών μέσα στο τηλεπικοινωνιακό δίκτυο αποφέρουν κόστος στη συνολική μετάδοση, παρά όφελος.

End-to-End Argument

- Μία συνάρτηση (λειτουργία) υλοποιείται σωστά μόνο με πλήρη γνώση της εφαρμογής που εκτελείται στα τελικά σημεία του τηλεπικοινωνιακού δικτύου.
- Είναι μία γενική αρχή που χρησιμοποιείται σαν «οδηγός» στο σχεδιασμό πρωτοκόλλων διαφόρων εφαρμογών.
- **Το Internet διαμορφώθηκε τις τελευταίες δεκαετίες με βάση την παραπάνω αρχή.**

Θέματα απόδοσης

- Δεν αποκλείονται τεχνικές στο χαμηλό επίπεδο του δικτύου: με κατάλληλη σχεδίαση, μπορούν να βελτιώσουν τη συνολική απόδοση
- **Η κεντρική ιδέα είναι ότι <u>δεν χρειάζεται</u> το τηλεπικοινωνιακό σύστημα να παρέχει τέλεια αξιοπιστία.**
- Για το μηχανικό τηλεπικοινωνιών, η προσθήκη τεχνικών ελέγχου μετάδοσης πρέπει να γίνεται προσεχτικά ώστε πραγματικά να αποτελεί όφελος και όχι επιβάρυνση του συστήματος.

Παράδειγμα 2: Εγγύηση παράδοσης

- Το ACK μήνυμα στο ARPANET (*RFNM – Request For Next Message*) αποδείχτηκε στην πράξη ότι δεν βοήθησε τις ARPANET εφαρμογές. Γιατί?
- Γνώση ότι εγγυημένα το μήνυμα έφτασε στον παραλήπτη δεν είναι τόσο σημαντική από μόνη της – αυτό που η εφαρμογή πραγματικά χρειάζεται να ξέρει είναι αν ο παραλήπτης έδρασε στο μήνυμα όπως ακριβώς επιβάλλει το εκάστοτε πρωτόκολλο.
- Τα επιθυμητά ACKs είναι αυτά από άκρο σε άκρο, που με απλά λόγια θα είναι της μορφής “I did it” – “I didn’t”

Παράδειγμα 3: αποφυγή διπλότυπων πακέτων μηνυμάτων

- Ένα πακέτο μπορεί να σταλεί δύο φορές (λόγω π.χ. κάποιου time-out/retry μηχανισμού όταν συμβαίνει σφάλμα).
- Ακόμα κι αν το δίκτυο ανιχνεύει διπλότυπα πακέτα και δεν τα στέλνει, η εφαρμογή η ίδια μπορεί να δημιουργήσει τέτοια (λόγω κάποιου δικού της σφάλματος), τα οποία πακέτα για το δίκτυο φαίνονται να είναι νέα!!
- Ένα απλό παράδειγμα: μία σύνδεση (π.χ. telnet) δείχνει να έχει κολλήσει και ο χρήστης επιχειρεί ξανά. Η ίδια η εφαρμογή πρέπει να αναγνωρίσει τη δεύτερη αίτηση ως ίδια με την πρώτη και να την αγνοήσει

Παράδειγμα 4: Μετάδοση δεδομένων με μυστικότητα

- Αν το δίκτυο έχει μηχανισμούς μυστικότητας:
  - Αν το σύστημα μετάδοσης πραγματοποιεί κρυπτογράφηση/αποκρυπτογράφηση, τότε αναγκαστικά η διαχείριση των κλειδιών πρέπει να γίνεται εσωτερικά σε αυτό – και κάτι τέτοιο ίσως αποτελεί αδύνατο σημείο για την εξασφάλιση της ασφάλειας.
  - Τα μεταδιδόμενα δεδομένα μπορεί να τα «πειράξει» ένας εισβολέας (hacker)
  - Η πιστοποίηση ταυτότητας πρέπει αναπόφευκτα να ελέγχεται από την εφαρμογή (με απλά λόγια από τους τελικούς χρήστες).

Συμπέρασμα

- Η ίδια η εφαρμογή πραγματοποιεί κρυπτογράφηση από άκρο-σε-άκρο:
  - Έλεγχος πιστοποίησης ταυτότητας
  - Διαχειρίζεται η ίδια το κλειδί
- Δεν υπάρχει ανάγκη το ίδιο το δίκτυο να παρέχει μηχανισμούς κρυπτογράφησης
- Εικονικά δίκτυα πάνω στο Internet: χρησιμοποιούν ακριβώς αυτήν την τεχνική (κρυπτογράφηση από άκρο σε άκρο)