Κεφάλαιο 7

Διαχείριση Δικτύου

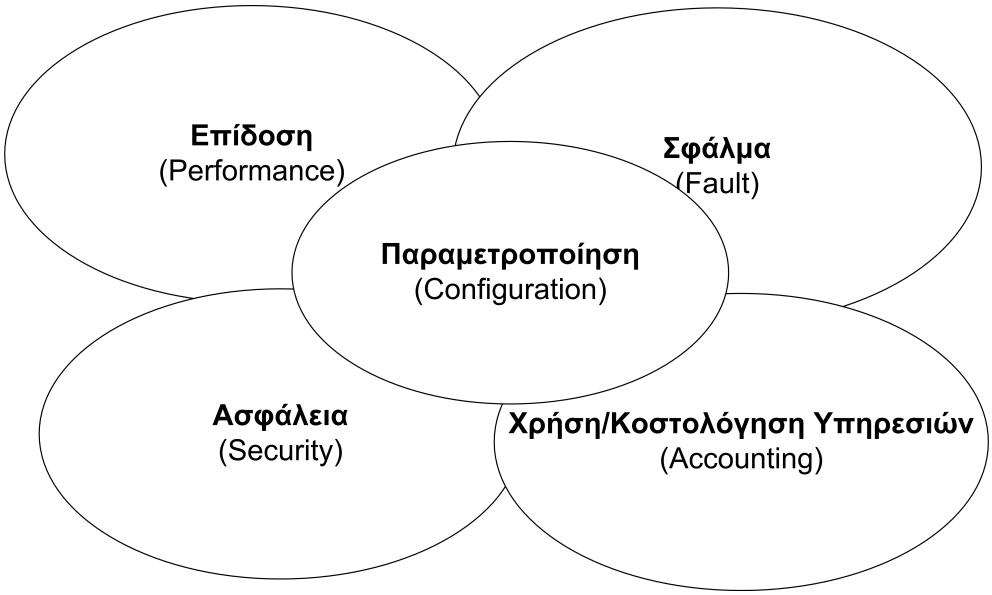
7.2 Περιοχές / Τομείς Διαχείρισης Δικτύου στο Μοντέλο OSI

Σε δίκτυα μεσαίου και μεγάλου μεγέθους είναι σχεδόν πάντοτε απαραίτητος ο σχεδιασμός και η εγκατάσταση ενός *Συστήματος Διαχείρισης Δικτύου, NMS (Network Management System)*. Ένα τέτοιο σύστημα αποτελείται από υλικό και λογισμικό που επιτρέπει στο διαχειριστή να επιβλέπει (και σε αρκετές περιπτώσεις να ρυθμίζει) τα στοιχεία που αποτελούν το δίκτυο και να ελέγχει για σημεία με προβληματική λειτουργία. Η διαχείριση γίνεται από κεντρικό σημείο, τυπικά από ένα υπολογιστή που έχει οριστεί ως υπολογιστής διαχείρισης (Manager Server).

Η Διαχείριση Δικτύου στο μοντέλο OSI χωρίζεται σε πέντε περιοχές, όπως φαίνεται στο σχήμα 7.1. Οι περιοχές αυτές είναι:

- Παραμετροποίηση (Configuration Management)
- Διαχείριση Σφαλμάτων (Fault Management)
- Διαχείριση Επιδόσεων (Performance Management)
- Διαχείριση Κόστους (Accounting Management)
- Διαχείριση Ασφάλειας (Security Management)

Το μοντέλο αυτό ονομάζεται και *FCAPS* από τα αρχικά των λέξεων *Fault Configuration Accounting Performance Security*. Παρακάτω θα εξηγήσουμε τις διαδικασίες αυτές.



Σχήμα 7.1: *Περιοχές Διαχείρισης του OSI*

7.2.1 Παραμετροποίηση

Η *Διαχείριση Παραμετροποίησης (Configuration Management, CM)* ασχολείται με την παρακολούθηση των παραμέτρων του δικτύου και των αλλαγών που συμβαίνουν σε αυτό.

Τα προβλήματα που παρουσιάζονται σε ένα δίκτυο είναι συχνά αποτέλεσμα των αλλαγών που κάνει ο διαχειριστής στις ρυθμίσεις του. Αυτή η περιοχή διαχείρισης είναι πολύ σημαντική γιατί παρακολουθεί και καταγράφει όλες αυτές τις αλλαγές.

Πότε γίνονται αλλαγές στις ρυθμίσεις;

Αλλαγές στις ρυθμίσεις μπορεί να γίνουν όταν:

- Ο διαχειριστής του δικτύου προσθέτει ή αφαιρεί υπολογιστές ή δικτυακό υλικό
- Ο διαχειριστής προσθέτει ή αφαιρεί εφαρμογές (λογισμικό)
- Ο διαχειριστής αλλάζει τις ρυθμίσεις μιας συσκευής την ώρα που αυτή είναι σε χρήση
- Γίνονται αυτόματες ενημερώσεις στο λογισμικό ή εγκατάσταση νέων εκδόσεων κλπ

- Γίνεται αναβάθμιση στα ενσωματωμένα προγράμματα (firmware) δικτυακών συσκευών (δρομολογητών, switch κλπ.)

Μια σωστή διαχείριση παραμετροποίησης περιλαμβάνει την καταγραφή όλων των παραπάνω (και ακόμα περισσότερων) αλλαγών. Η καταγραφή μπορεί φυσικά να γίνεται χειροκίνητα χωρίς χρήση λογισμικού, αλλά σε οποιοδήποτε μεγάλο δίκτυο αυτό γενικά είναι χρονοβόρο και οδηγεί σε σφάλματα. Συνήθως χρησιμοποιείται κατάλληλο λογισμικό διαχείρισης παραμέτρων όπως το CiscoWorks 2000 ή το Infosim.

Η διαχείριση παραμέτρων περιλαμβάνει τους παρακάτω στόχους:

- Τη συλλογή και αποθήκευση παραμέτρων των συσκευών του δικτύου, είτε τοπικά είτε από απόσταση (δεν είναι πάντα δυνατή η απομακρυσμένη διαχείριση μιας συσκευής: οι πιο απλές / φτηνές δικτυακές συσκευές δεν διαθέτουν περιβάλλον απομακρυσμένης διαχείρισης)
- Την απλοποίηση της παραμετροποίησης των συσκευών
- Την παρακολούθηση αλλαγών που συμβαίνουν στις παραμέτρους
- Τη διαμόρφωση νοητών κυκλωμάτων μέσα από δίκτυα χωρίς μεταγωγή (non-switched networks). Πρόκειται για το λεγόμενο *provisioning*: ο διαχειριστής βρίσκει διαδρομές και καθορίζει τα νοητά κυκλώματα που θα χρησιμοποιηθούν στην δικτυακή επικοινωνία
- Το σχεδιασμό και την πρόβλεψη μελλοντικών επεκτάσεων

Η διαχείριση παραμέτρων υλικού και λογισμικού αποτελείται από πέντε ξεχωριστές δράσεις:

Σημείωση: Τα παρακάτω σημεία είναι μετάφραση στο βιβλίο σας από το αντίστοιχο άρθρο της Wikipedia. Προσπαθήσαμε εδώ να κάνουμε καλύτερη μετάφραση γιατί δυστυχώς στο σχολικό βιβλίο δεν βγαίνει νόημα…

- **Σχεδιασμός και Διαχείριση Παραμέτρων:** Πρόκειται για ένα επίσημο έγγραφο που περιγράφει τους τομείς και τις παραμέτρους με τις οποίες ασχολείται η διαχείριση και περιλαμβάνει μεταξύ άλλων:
  - Το προσωπικό
  - Τις διαδικασίες εκπαίδευσης
  - Τα εργαλεία και τις διαδικασίες που πρέπει να ακολουθούνται

  - Τις μεθόδους ελέγχου κ.α.

- **Ταυτοποίηση Παραμετροποίησης:** Ορίζει τις βασικές προδιαγραφές και παραμέτρους του δικτύου (baseline) με βάση τις οποίες γίνεται κατόπιν η παρακολούθηση των αλλαγών σε αυτό

- **Έλεγχος Παραμετροποίησης:** Περιλαμβάνει την αξιολόγηση όλων των προτάσεων για αλλαγές ή βελτιώσεις πάνω στο δίκτυο. Κατά τον έλεγχο κάποιες αλλαγές μπορεί να εγκρίνονται και άλλες να απορρίπτονται

- **Κοστολόγηση Κατάστασης Παραμετροποίησης:** (Σημείωση: κανονικά δεν είναι κοστολόγηση, αλλά καταγραφή) Περιλαμβάνει την καταγραφή και αναφορά όλων των παραμέτρων του δικτύου (υλικού, λογισμικού, firmware κλπ) και των αποκλίσεων τους σε σχέση με τις αρχικές προδιαγραφές

- **Επαλήθευση και Αξιολόγηση Παραμετροποίησης:** Πρόκειται για μια ανεξάρτητη έκθεση αξιολόγησης του υλικού και του λογισμικού του δικτύου προκειμένου να διαπιστωθεί αν τηρεί συγκεκριμένες προδιαγραφές που απαιτούνται από κανονισμούς (π.χ. για στρατιωτική χρήση κλπ.)

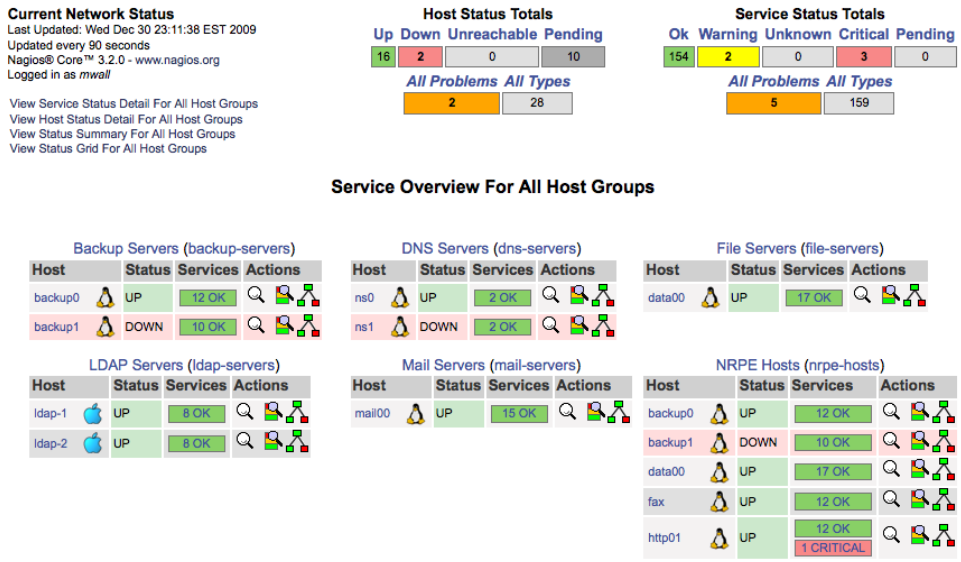
7.2.2 Διαχείριση Σφαλμάτων

Για να λειτουργεί σωστά το δίκτυο, θα πρέπει να φροντίζουμε να λειτουργούν σωστά τα επιμέρους στοιχεία του. Σε ένα δίκτυο μπορεί να συμβαίνουν τόσο βλάβες / σφάλματα όσο και λάθη.

Σημείωση: Το βιβλίο εδώ αναφέρει το “σφάλμα” ως συνώνυμο της “βλάβης”. Στην πραγματικότητα “σφάλμα” και “λάθος” είναι συνώνυμες λέξεις στα ελληνικά. Στην ξένη βιβλιογραφία η βλάβη αναφέρεται ως **fault** ενώ το λάθος ως **error** και είναι πράγματι διαφορετικές έννοιες όπως θα δείτε στους παρακάτω ορισμούς.

Βλάβη ή σφάλμα είναι μια μη φυσιολογική κατάσταση που απαιτεί την προσοχή του διαχειριστή και την άμεση διόρθωση του. Μια βλάβη συνεπάγεται μη σωστή λειτουργία ή μεγάλο αριθμό λαθών και προβλημάτων. Για παράδειγμα ένα καλώδιο δικτύου το οποίο δεν κάνει καλή επαφή μπορεί να προκαλεί διακοπές στο δίκτυο ή μεγάλο αριθμό από λανθασμένα bit.

Λάθος είναι ένα μεμονωμένο γεγονός το οποίο συνήθως δεν συνεπάγεται διακοπή της επικοινωνίας. Σε πολλές περιπτώσεις το δίκτυο μπορεί να διορθώνει αυτόματα λάθη που οφείλονται σε τυχαία γεγονότα (π.χ. παρεμβολή σε ένα καλώδιο δικτύου



Σχήμα 7.2: *Σύστημα Διαχείρισης Δικτύου (NMS)*

μπορεί να προκαλέσει τη λανθασμένη λήψη κάποιων bit) χρησιμοποιώντας μηχανισμούς ελέγχου που περιέχονται στα ίδια τα πρωτόκολλα (θυμηθείτε π.χ. ότι το TCP έχει άθροισμα ελέγχου και τη δυνατότητα να μεταδώσει ξανά τα χαλασμένα τμήματα).

Ο εντοπισμός ενός σφάλματος (βλάβης) μπορεί να γίνει έμμεσα, με την *παρατήρηση ενδείξεων* από την κίνηση και τη συμπεριφορά του δικτύου σε πραγματικό χρόνο (παρατηρούμε ότι μια σελίδα που κανονικά ανοίγει πολύ γρήγορα καθυστερεί υπερβολικά, ή ότι ένας κοινόχρηστος φάκελος στο δίκτυο δεν ανταποκρίνεται) είτε σε *μορφή συναγερμού (alarm)* εφόσον έχουμε εγκαταστήσει ένα Σύστημα Διαχείρισης Δικτύου (σχήμα 7.2).

Σε περίπτωση σφάλματος, υπάρχουν συγκεκριμένα βήματα που πρέπει να ακολουθήσουμε για την αντιμετώπιση του και γενικά ονομάζονται *Κύκλος Επεξεργασίας Διαχείρισης Σφαλμάτων, Fault Management Process Cycle*. Τα συνήθη βήματα είναι τα παρακάτω:

- **Να προσδιοριστεί το σφάλμα**, να βρεθεί δηλαδή τι είδους σφάλμα είναι και από που μπορεί να προέρχεται
- **Να εντοπιστεί το σφάλμα**, ώστε να ανακαλυφθεί σε πιο σημείο του δικτύου βρίσκεται
- **Να απομονωθεί το υπόλοιπο του δικτύου**, ώστε να λειτουργεί χωρίς να εμποδίζεται από το σφάλμα

- **Να αναδιαμορφωθεί το δίκτυο** ώστε να μπορεί να λειτουργεί όσο το δυνατόν καλύτερα για όσο υπάρχει ακόμα το σφάλμα
- **Να γίνει έλεγχος και ανάλυση των ενδείξεων** ώστε να κατανοηθεί καλύτερα η αιτία και να δοθεί μια καλύτερη εξήγηση της πηγής του σφάλματος
- **Να επισκευαστεί ή να αντικατασταθεί** το υλικό ή το λογισμικό που προκάλεσε τη βλάβη ώστε το δίκτυο να επανέλθει στην προηγούμενη του λειτουργική κατάσταση
- **Να παρακολουθηθεί το δίκτυο** από το διαχειριστή για ένα προκαθορισμένο χρονικό διάστημα ώστε να επιβεβαιωθεί η σωστή λειτουργία του και να είμαστε σίγουροι ότι το σφάλμα επιλύθηκε επιτυχώς

Η επίδραση που έχει ένα σφάλμα στο δίκτυο μπορεί να μετριαστεί αν έχουμε φροντίσει να υπάρχουν για παράδειγμα πολλαπλές (εναλλακτικές) διαδρομές που να ενώνουν δυο σημεία επικοινωνίας (αλλαγή διαδρομής). Όσο αφορά το δικτυακό υλικό, μπορούμε να διαθέτουμε πολλαπλές δικτυακές συσκευές για την ίδια εργασία ώστε να αναλαμβάνει κάποια άλλη το φορτίο του δικτύου σε περίπτωση βλάβης.

Για παράδειγμα, σε πολλούς εξυπηρετητές δικτύου χρησιμοποιούμε συστήματα mirror (καθρέπτη) στους σκληρούς δίσκους: τα δεδομένα μας αποθηκεύονται ταυτόχρονα σε περισσότερους από ένα δίσκους και το σύστημα μπορεί να συνεχίσει να λειτουργεί κανονικά ακόμα και μετά από απώλεια ενός ή περισσότερων δίσκων. Στην περίπτωση αυτή βέβαια ειδοποιείται ο διαχειριστής για να αντικαταστήσει το χαλασμένο δίσκο το συντομότερο δυνατόν.

7.2.3 Διαχείριση Επιδόσεων

Η *Διαχείριση Επιδόσεων* (Performance Management ή Capacity Management) διασφαλίζει ότι η απόδοση του δικτύου βρίσκεται σε αποδεκτά επίπεδα, αυτά δηλαδή για τα οποία σχεδιάστηκε.

Για το σκοπό αυτό, η διαχείριση επιδόσεων αξιολογεί κάποια μετρήσιμα χαρακτηριστικά απόδοσης όπως το χρόνο απόκρισης του δικτύου, την απώλεια πακέτων, τη χρήση των γραμμών επικοινωνίας, το βαθμό λαθών που συμβαίνουν κλπ. Οι πληροφορίες αυτές συλλέγονται σε ένα σύστημα διαχείρισης δικτύου (χρησιμοποιώντας πρωτόκολλα όπως το SNMP) με τους παρακάτω τρόπους:

- **Με συνεχή παρακολούθηση** και εκτίμηση της τρέχουσας κατάστασης από το διαχειριστή

- **Με ορισμό συναγερμών** στο σύστημα διαχείρισης δικτύου, το οποίο και θα μας ειδοποιήσει όταν τα επίπεδα απόδοσης μεταβληθούν σε σχέση με τα προκαθορισμένα και αποδεκτά

Με σωστά σχεδιασμένη στρατηγική συλλογής και ανάλυσης δεδομένων απόδοσης, ο διαχειριστής μπορεί:

- Να πιστοποιήσει την αποτελεσματικότητα και αξιοπιστία του δικτύου
- Να προβλέψει τα προβλήματα πριν εμφανιστούν
- Να επανασχεδιάσει το δίκτυο για ακόμα καλύτερες επιδόσεις
- Να προετοιμάσει το δίκτυο για μελλοντικές βελτιώσεις / επεκτάσεις

Για να εκτιμήσει καλύτερα την κατάσταση, ο διαχειριστής επιλέγει κάποιες παραμέτρους (πόρους) του δικτύου τους οποίους παρακολουθεί στενά.

7.2.4 Διαχείριση Κόστους

Η *Διαχείριση Κόστους* (Accounting Management ή Billing Management) ασχολείται με την παρακολούθηση πληροφοριών κόστους που σχετίζονται με τη χρήση των πόρων ενός δικτύου.

Βέβαια δεν παρέχουν όλα τα δίκτυα υπηρεσίες επί πληρωμή. Για παράδειγμα η τυπική χρήση ενός εταιρικού δικτύου δεν προκαλεί αύξηση του κόστους εκτός αν χρησιμοποιούνται υλικά που αναλώνονται (π.χ. εκτύπωση σε ένα δικτυακό εκτυπωτή) ή συνδέσεις δικτύου με ογκοχρέωση (π.χ. μισθωμένες γραμμές, δορυφορικές συνδέσεις). Στην περίπτωση αυτή προφανώς παρακολουθούνται μόνο οι συγκεκριμένες υπηρεσίες. Σε δίκτυα που δεν έχουν στόχο το κέρδος η έννοια αυτή αντικαθίσταται από την έννοια της Διοίκησης (Administration).

Ανάλογα με την περίπτωση, ο σκοπός της διαχείρισης κόστους είναι:

Για επιχειρήσεις με στόχο το κέρδος:

- **Ο υπολογισμός του σωστού ποσού χρέωσης** που προκύπτει από τις επί πληρωμή υπηρεσίες στους αντίστοιχους χρήστες (ή ομάδες χρηστών, ή οργανισμούς)

Για επιχειρήσεις χωρίς στόχο το κέρδος:

- **Δημιουργία κοστολόγησης (ή σωστότερα: καταγραφής) της χρήσης των πόρων** του δικτύου ανά χρήστη ή ανά τμήμα για να προσδιοριστούν καλύτερα λειτουργίες όπως η λήψη αντιγράφων ασφαλείας ή ο συγχρονισμός των δεδομένων

Η διαχείριση κόστους επίσης καλείται να αναγνωρίσει και να εντοπίσει χρήστες ή ομάδες χρηστών του δικτύου που:

- **Παραβιάζουν τα δικαιώματα πρόσβασης** και επιβαρύνουν το δίκτυο με άσκοπες λειτουργίες
- **Κάνουν μη αποτελεσματική χρήση του δικτύου**

Ο διαχειριστής είναι υπεύθυνος να αποφασίσει και να ορίσει τις παραμέτρους που θα παρακολουθούνται και θα καταγράφονται, τα χρονικά διαστήματα της καταγραφής καθώς και τον τρόπο υπολογισμού (αλγόριθμο) του κόστους. Αν δεν απαιτείται χρέωση, η συλλογή των δεδομένων θα χρησιμοποιηθεί για βελτιστοποίηση της απόδοσης.

7.2.5 Διαχείριση Ασφάλειας

Η *Διαχείριση Ασφαλείας* σε ένα δίκτυο αναφέρεται στη διαχείριση πληροφοριών που σχετίζονται με την ομαλή λειτουργία του δικτύου, την παρακολούθηση και έλεγχο πρόσβασης σε τμήματα του ή όλο το δίκτυο και στην ασφάλεια των δεδομένων που διακινούνται και αποθηκεύονται σε αυτό.

Για να ολοκληρωθεί το έργο της διαχείρισης ασφάλειας, πρέπει σε τακτά διαστήματα να συλλέγονται και να αναλύονται οι πληροφορίες που σχετίζονται με τους παραπάνω τομείς. Για το σκοπό αυτό χρησιμοποιούνται εργαλεία λογισμικού όπως:

- Πλατφόρμες συλλογής και ελέγχου δικτυακών δεδομένων (NMS Platforms)
- Εργαλεία κρυπτογράφησης (cryptography tools)
- Εργαλεία αυθεντικοποίησης (authentication tools) για τον έλεγχο πρόσβασης
- Συστήματα ελέγχου εισβολέων (intrusion detection systems)
- Τείχος προστασίας (firewall)
- Εφαρμογή πολιτικών ασφαλείας (security policies)
- Ημερολόγιο (αρχεία) καταγραφής (security logs) κ.α.

Καθένα από τα παραπάνω εργαλεία έχει διαφορετική εφαρμογή και στοχεύει να καλύψει επιμέρους ανάγκες ασφαλείας ενός δικτύου. Ένας διαχειριστής θα χρησιμοποιήσει περισσότερα από ένα εργαλεία για να εξασφαλίσει την ασφάλεια του δικτύου. Για το λόγο αυτό η διαχείριση ασφαλείας είναι μια αρκετά πολύπλοκη διαδικασία.

Για να είναι αποτελεσματική η διαχείριση ασφαλείας, θα πρέπει να προβλεφθούν οι πιθανές απειλές και τα σημεία κινδύνου ώστε να επιλεγούν τα σημεία που χρειάζονται μεγαλύτερη προσοχή και προστασία. Αφού γίνει αυτή η αναγνώριση, εγκαθίσταται και ρυθμίζεται το κατάλληλο λογισμικό. Μέσα από αυτό ο διαχειριστής παρακολουθεί και εντοπίζει πηγές κινδύνου και επιθέσεις στο δίκτυο στο συντομότερο χρονικό διάστημα.

7.3 Πρότυπα Διαχείρισης

Τα *βασικά συστατικά ή οντότητες* από τις οποίες αποτελείται ένα τυπικό Σύστημα Διαχείρισης Δικτύου είναι:

- **Ο Διαχειριστής Δικτύου** (Manager Server)
- **Ο Αντιπρόσωπος** (Agent)
- **Η Βάση Πληροφοριών Διαχείρισης** (Management Information Base, MIB)

Σημείωση: Επειδή από τα παραπάνω, ίσως δεν είναι προφανές, θα πρέπει να ξεκαθαρίσουμε:

Ο Διαχειριστής και ο Αντιπρόσωπος είναι προγράμματα που εκτελούνται σε μηχανήματα του δικτύου.

Συγκεκριμένα, ο διαχειριστής (πρόγραμμα) χρησιμοποιείται από τον διαχειριστή (άνθρωπο) προκειμένου να λάβει πληροφορίες για την κατάσταση του δικτύου. Ο διαχειριστής (πρόγραμμα) εκτελείται σε ένα υπολογιστή που είναι επιφορτισμένος με τη διαχείριση του δικτύου και συχνά ονομάζεται Manager Server.

Ο διαχειριστής (πρόγραμμα) συλλέγει δεδομένα επικοινωνώντας με τους αντιπροσώπους, που είναι αντίστοιχα προγράμματα που εκτελούνται σε κάθε τμήμα / συσκευή του δικτύου που διαθέτει δυνατότητα διαχείρισης. Προφανώς δεν είναι όλες οι συσκευές ή τα τμήματα του δικτύου κατάλληλα για την εκτέλεση προγραμμάτων αντιπροσώπου και άρα δεν είναι πάντα διαχειρίσιμα με κεντρικό τρόπο. Δεν μπορούμε να έχουμε αντιπρόσωπο να εκτελείται σε ένα…καλώδιο δικτύου. Επίσης φτηνές δικτυακές συσκευές δεν διαθέτουν συνήθως δυνατότητα διαχείρισης. Για παρά-

δειγμα ένας φτηνός μεταγωγέας δικτύου (switch) όπως αυτός που έχετε πιθανόν στο σχολικό εργαστήριο δεν είναι διαχειριζόμενος. Για να διαθέτει μια συσκευή τέτοια δυνατότητα χρειάζεται να έχει επεξεργαστή, μνήμη και το κατάλληλο πρόγραμμα από τον κατασκευαστή της (firmware). Το πρόγραμμα αυτό δρα ως αντιπρόσωπος (agent) και επιτρέπει την ανταλλαγή πληροφοριών με το διαχειριστή (πρόγραμμα) μέσω πρωτοκόλλων διαχείρισης (π.χ. SNMP). Όταν φτιάχνουμε ένα δίκτυο μεσαίου ή μεγάλου μεγέθους προσπαθούμε να χρησιμοποιούμε δικτυακές συσκευές με δυνατότητα διαχείρισης όπου είναι δυνατόν. Μερικές φορές ωστόσο το κόστος μπορεί να είναι απαγορευτικό.

Τα πιο γνωστά *Πρότυπα Διαχείρισης Δικτύου (Network Management, NM)* είναι:

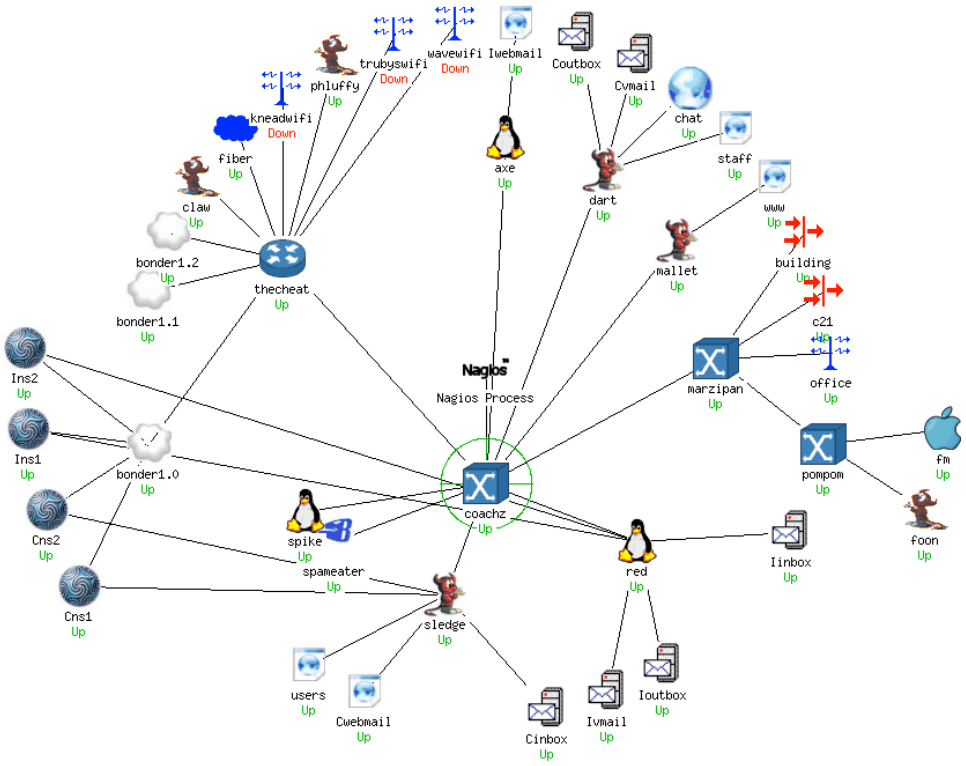
- Το **SNMP, Simple Network Management Protocol** του Διαδικτύου
- Το **CMIP, Common Management Information Protocol** του OSI

7.3.1 Βασικά Συστατικά Συστήματος Διαχείρισης (MS – MIB – AGENT)

Ο *Διαχειριστής Δικτύου (Manager Server)* είναι ένας ή περισσότεροι υπολογιστές που διαχειρίζεται τα στοιχεία του δικτύου που έχουν επιλεγεί για αυτό το σκοπό. Ο Manager Server εκτελεί κατάλληλο λογισμικό διαχειριστή το οποίο συχνά εμφανίζει στο διαχειριστή (άνθρωπο) το δίκτυο σε μορφή χάρτη (σχήμα 7.3) επιτρέποντας του να δει με μια ματιά την κατάσταση όλων των διαχειριζόμενων συσκευών.

Το λογισμικό πραγματοποιεί τις παρακάτω λειτουργίες:

- Αποστέλλει αιτήματα στους αντιπροσώπους που είναι εγκατεστημένοι στο δίκτυο
- Λαμβάνει απαντήσεις από τους αντιπροσώπους
- Ορίζει μεταβλητές παρακολούθησης στους αντιπροσώπους. Ουσιαστικά καθορίζει ποια είναι τα μεγέθη που θα μετρώνται. Για παράδειγμα, ο διαχειριστής μπορεί να ορίσει να μετρώνται τα πλαίσια ανα δευτερόλεπτο που διακινούνται σε μια θύρα Ethernet ενός switch. Για το σκοπό αυτό θα στείλει αντίστοιχη οδηγία στον αντιπρόσωπο που εκτελείται στο switch αυτό
- Παρακολουθεί τους συναγερμούς. Ειδοποιεί τον διαχειριστή (άνθρωπο) όταν οι παράμετροι λειτουργίας του δικτύου είναι εκτός των αποδεκτών ορίων



Σχήμα 7.3: *Δικτυακός Χάρτης*

(μπορεί να στείλει ειδοποιήσεις μέσω email, sms κλπ)

- Προσφέρει κατάλληλο περιβάλλον χρήστη (π.χ. δικτυακό χάρτη) για την καλύτερη παρακολούθηση των πληροφοριών του δικτύου από τον άνθρωπο

Ο *Αντιπρόσωπος Δικτύου* είναι το λογισμικό που εκτελείται σε κάθε δικτυακή συσκευή που είναι υπό διαχείριση.

Όπως αναφέραμε και πριν, δεν είναι όλες οι συσκευές δικτύου κατάλληλες για την εκτέλεση λογισμικού αντιπροσώπου. Οι φτηνές συσκευές συνήθως δεν έχουν δυνατότητες διαχείρισης και προσπαθούμε να τις αποφεύγουμε σε δίκτυα μεσαίου / μεγάλου μεγέθους.

Βασικές λειτουργίες του αντιπροσώπου είναι:

- Η συλλογή πληροφοριών από τα διαχειριζόμενα αντικείμενα του δικτύου
- Η διαμόρφωση παραμέτρων των διαχειριζόμενων αντικειμένων. Σε αρκετές

διαχειριζόμενες συσκευές είναι δυνατή η αλλαγή ρυθμίσεων με την αποστολή κατάλληλων εντολών από το Manager Server

- Η απάντηση στα αιτήματα των προγραμμάτων διαχείρισης δικτύου
- Η δημιουργία και αποστολή συναγερμών στους διαχειριστές

Η *Βάση Πληροφοριών Διαχείρισης ή MIB, Management Information Base* είναι ένα σχήμα αποθήκευσης πληροφοριών σε μορφή βάσης δεδομένων που χρησιμοποιείται για τη διαχείριση των αντικειμένων / οντοτήτων ενός δικτύου. Αντικείμενο θεωρείται εδώ κάθε συσκευή που είναι συνδεδεμένη στο δίκτυο (υπολογιστές, εκτυπωτές, δικτυακές συσκευές, δρομολογητές κλπ).

Η δομή της παραπάνω βάσης είναι ιεραρχική και μοιάζει με αντεστραμμένο δέντρο. Κάθε φύλλο είναι ένα διαχειριζόμενο αντικείμενο και αντιστοιχεί σε ένα πόρο του συστήματος. Η εισαγωγή πληροφοριών γίνεται μέσω μιας ακολουθίας αριθμών που προσδιορίζει με μοναδικό τρόπο ένα αντικείμενο (Ταυτοποίηση Αντικειμένου ή Object Identifier).

Οι MIBs συνήθως χρησιμοποιούν δομές πινάκων με πολλές μεταβλητές (πεδία). Οι πίνακες μπορεί να έχουν από μηδέν εγγραφές και άνω και ένα σύστημα διαχείρισης έχει πρόσβαση σε αυτούς για να εκτελέσει τυπικές λειτουργίες βάσεων δεδομένων: εισαγωγή δεδομένων, ανάκτηση (αναζήτηση), ανάκτηση επόμενης / προηγούμενης εγγραφής, ενημέρωση, διαγραφή κλπ.

Κεφάλαιο 8

Ασφάλεια Δικτύων

8.1 Βασικές Έννοιες Ασφάλειας Δεδομένων

Για να κατανοήσουμε την έννοια της ασφάλειας, θα πρέπει:

- Να σκεφτούμε τι σημαίνει για τον καθένα μας. Η ασφάλεια αντιμετωπίζεται διαφορετικά από ιδιώτες και από εταιρίες
- Να βρούμε ποιοι είναι αυτοί που προσπαθούν να την παραβιάσουν
- Να ανακαλύψουμε τις προθέσεις των εισβολέων και το πιθανό όφελος τους από μια επιτυχή παραβίαση

Όταν σκεφτόμαστε την ασφάλεια σε προσωπικό επίπεδο και σε σχέση με την τεχνολογία, το Διαδίκτυο και τους υπολογιστές, συνήθως σκεφτόμαστε υποκλοπή δεδομένων όπως τον αριθμό της πιστωτικής μας κάρτας ή τους κωδικούς του e-banking με σκοπό προφανώς το οικονομικό όφελος. Άνθρωποι που έχουν δημόσιο προφίλ (ηθοποιοί, τραγουδιστές, πολιτικοί κλπ) ή που ασχολούνται με τα κοινά μπορεί να έχουν στις συσκευές τους ευαίσθητα δεδομένα που πρέπει να παραμείνουν μυστικά. Τυχόν διαρροή τέτοιων πληροφοριών μπορεί να είναι επιζήμια για το ίδιο το άτομο ή τον οργανισμό στον οποίο εργάζεται. Ο μέσος άνθρωπος πάντως σε γενικές γραμμές είναι αδιάφορος για την ασφάλεια πέρα από τις πληροφορίες που μεταφέρει και αποθηκεύει σε υπολογιστικά συστήματα και που έχουν να κάνουν με ηλεκτρονικές συναλλαγές (η υποκλοπή των οποίων μπορεί να προκαλέσει απώλεια χρημάτων).

Μπορούμε να θεωρήσουμε ότι ασφάλεια γενικότερα είναι η προσπάθεια προστασίας από εξωτερικές επιβουλές (κακόβουλες ενέργειες) στις πληροφορίες και τα

συστήματα κατά τη λειτουργία τους ή κατά την επικοινωνία τους με άλλα συστήματα.

Κάθε πράγμα που θέλουμε να προστατεύσουμε αποτελεί για μας ένα *αγαθό* η απώλεια του οποίου μπορεί να μας προκαλέσει οικονομική ή άλλη ζημιά.

Αγαθό ή πόρος ενός υπολογιστικού / πληροφοριακούς συστήματος είναι κάθε αντικείμενο που ανήκει ή στηρίζει το σύστημα και το οποίο αξίζει να προστατευθεί.

Σε μια εταιρία, τα παραπάνω αγαθά μπορεί να ανήκουν τόσο στο υλικό όσο και στο λογισμικό του συστήματος και προφανώς περιέχουν επίσης τα δεδομένα (τα οποία πολλές φορές είναι αναντικατάστατα σε σχέση με όλα τα άλλα τμήματα):

Αγαθά είναι:

- Κτήρια, υπολογιστές, δικτυακός εξοπλισμός και υποδομή
- Έπιπλα, γραφεία κλπ.
- Αρχεία (ηλεκτρονικά και έντυπα), πληροφορίες σε συστήματα βάσεων δεδομένων κλπ.
- Λογισμικό εφαρμογών, λειτουργικά συστήματα κλπ.

Για να είναι αποτελεσματική η προστασία μας στις επιθέσεις, θα πρέπει αρχικά να κατανοούμε ποιοι αποτελούν την απειλή, ποια δικά μας δεδομένα τους είναι χρήσιμα και πως μπορούν να τα χρησιμοποιήσουν εναντίον μας. Για παράδειγμα ένα πολύ σημαντικό όπλο στην ασφάλεια δεδομένων αποτελεί η διαδικασία της κρυπτογράφησης. Η πρώτη ισχυρή κρυπτογράφηση έγινε από τους Γερμανούς κατά το δεύτερο παγκόσμιο πόλεμο: έπρεπε να μεταδίδουν μηνύματα προς τα υποβρύχια τους μέσω ασυρμάτου χωρίς να μπορεί να γίνει υποκλοπή από τους συμμάχους. Για το σκοπό αυτό έφτιαξαν τη μηχανή Enigma. Ωστόσο στην Αγγλία, οι σύμμαχοι ανακάλυψαν αδυναμίες τόσο στη μηχανή όσο και στη διαδικασία μετάδοσης μηνυμάτων και κατάφερναν να αποκωδικοποιούν τα μηνύματα σε καθημερινή βάση.

Από τα παραπάνω είναι προφανές ότι οι κυβερνήσεις είναι αυτές που διαθέτουν τον καλύτερο εξοπλισμό τόσο για να προστατεύσουν τα δεδομένα τους όσο και για να προβούν σε παραβιάσεις ασφαλείας εναντίον άλλων κρατών.

Μια εταιρεία ή οργανισμός με πολλούς εργαζόμενους και πελάτες συνήθως απευθύνεται σε συμβούλους ασφαλείας. Σε πολλές περιπτώσεις επιλέγεται μια λύση μεγάλου κόστους που προσπαθεί να δημιουργήσει τη μεγαλύτερη δυνατή ασφάλεια. Η πραγματικότητα όμως είναι ότι *δεν μπορεί ποτέ να υπάρξει απόλυτη ασφάλεια*, εκτός αν δεν έχουμε ευαίσθητα δεδομένα και δεν υπάρχουν μυστικά που πρέπει να μεταδοθούν. Σε ένα υπολογιστικό σύστημα η ασφάλεια είναι πάντα τόσο καλή όσο

είναι ο πιο αδύναμος κρίκος του, και αυτός αποδεικνύεται συχνά ότι είναι ο άνθρωπος.

Επίσης η μεγαλύτερη ασφάλεια κάνει συνήθως ένα σύστημα πιο δύσχρηστο: οι χρήστες καλούνται συνέχεια να εισάγουν κωδικούς και οι κινήσεις τους ελέγχονται τόσο συχνά που το σύστημα μπορεί να είναι δυσκίνητο. Αν και αρχικός σκοπός είναι η αύξηση της ασφάλειας, ένα δύσχρηστο σύστημα στην πραγματικότητα μειώνει την ασφάλεια: σύντομα οι χρήστες θα ψάξουν να βρουν τρόπους για να παρακάμψουν ή να συντομεύσουν τις διαδικασίες αντικαθιστώντας τις με άλλες, ανασφαλείς.

Τελικά η ασφάλεια βασίζεται πάντα σε μια ανάλυση αντιστάθμισης του κόστους και των ωφελημάτων που μπορούν να επιτευχθούν. Είναι ένας συμβιβασμός που στη μια μεριά έχει το κόστος της απώλειας ή διαρροής των δεδομένων και στην άλλη το κόστος προφύλαξης τους από διαφορετικές απειλές. Σε αντίθεση με τους ειδικούς ασφαλείας που προτείνουν λύσεις με το μέγιστο κόστος, η πραγματική ασφάλεια συνήθως αναγνωρίζει τις συνηθισμένες απειλές και προσπαθεί να λάβει τα απαραίτητα μέτρα για αυτές, ενώ μπορεί να αγνοεί απειλές που είναι σπάνιες ή απίθανες.

Για παράδειγμα, μια συνηθισμένη επίθεση σε μια τράπεζα μπορεί να έχεις ως αποτέλεσμα την υποκλοπή στοιχείων πελατών όπως τραπεζικοί λογαριασμοί και πιστωτικές κάρτες. Το σύστημα ασφαλείας της τράπεζας θα πρέπει να είναι προετοιμασμένο για τέτοιες επιθέσεις. Μέχρι τι επίπεδο όμως; Τι απώλεια έχει η τράπεζα από τη διαρροή μιας πιστωτικής κάρτας; Εκτός από την προφανή άμεση οικονομική ζημιά, υπάρχει και η έμμεση: οι πελάτες δεν έχουν πλέον εμπιστοσύνη στη τράπεζα. Απώλεια πελατών σημαίνει επίσης μελλοντική οικονομική απώλεια.

Γενικά είναι πιο εύκολο να υπολογίσουμε μια άμεση ζημιά (π.χ. από την καταστροφή ενός υλικού) από την έμμεση (απώλεια εμπιστοσύνης). Ένα άλλο κόστος μπορεί να είναι οι νομικές συνέπειες που προκύπτουν ως αποτέλεσμα της παραβίασης ασφάλειας. Τέλος, αν μια εταιρεία βασίζεται στην αδιάλειπτη παροχή υπηρεσιών μέσω Διαδικτύου και δεχθεί επίθεση άρνησης υπηρεσίας (DOS attack) η απώλεια χρημάτων (πέρα από τις νομικές συνέπειες) μπορεί να είναι ανυπολόγιστη. Σκεφτείτε για παράδειγμα μια εταιρεία όπως το Amazon: αν το site του Amazon σταματήσει ξαφνικά να είναι προσβάσιμο, θα χάνονται αρκετά εκατομμύρια πωλήσεων κάθε λεπτό.

8.2 Εμπιστευτικότητα – Ακεραιότητα – Διαθεσιμότητα – Αυθεντικότητα – Εγκυρότητα

Τα βασικά προβλήματα που πρέπει να επιλύσει κάποιος κατά την ανάλυση και το σχεδιασμό του επιπέδου ασφαλείας που θέλει να πετύχει είναι τέσσερα:

- **Εμπιστευτικότητα (confidentaliaty):** Αποτροπή της πρόσβασης σε ιδιωτικές πληροφορίες από άτομα που δεν έχουν εξουσιοδότηση.

  Για παράδειγμα, όταν κάνουμε μια ηλεκτρονική παραγγελία μέσω Διαδικτύου θέλουμε να εξασφαλίσουμε ότι ο αριθμός της πιστωτικής μας κάρτας δεν θα είναι ορατός παρά μόνο από το σύστημα που θα τελέσει τη συναλλαγή.

- **Αυθεντικοποίηση (authentication) ή πιστοποίηση ταυτότητας:** Η εξασφάλιση ότι η πληροφορία προέρχεται πραγματικότητα από αυτόν που νομίζουμε (ή που ισχυρίζεται) ότι τη μετέδωσε.

  Για παράδειγμα, να μπορούμε να διασφαλίσουμε ότι το άτομο που έστειλε τον αριθμό της πιστωτικής κάρτας είναι πράγματι ο κάτοχος της. Ή όταν κάποιος εισέρχεται σε ένα υπολογιστικό σύστημα ότι πράγματι είναι το πρόσωπο στο οποίο ανήκει ο αντίστοιχος λογαριασμός χρήστη.

- **Ακεραιότητα (integrity):** είναι η διασφάλιση ότι οι πληροφορίες δεν έχουν αλλοιωθεί και όλες οι αλλαγές που έχουν γίνει σε αυτές προέρχονται από εξουσιοδοτημένα άτομα.

  Για παράδειγμα, αν κάποιος τρίτος μπορούσε να υποκλέψει τη συναλλαγή πληρωμής μιας ηλεκτρονικής αγοράς, θα μπορούσε να κατευθύνει το χρηματικό ποσό στο δικό του λογαριασμό. Μια τέτοια αλλοίωση σημαίνει απώλεια ακεραιότητας των δεδομένων.

  Όταν αναφερόμαστε σε πληροφορίες, *εξουσιοδοτημένα άτομα* είναι προφανώς ο αρχικός δημιουργός της πληροφορίας και τα άτομα στα οποία αυτός έχει δώσει τα αντίστοιχα δικαιώματα πρόσβασης (μερικούς ή πλήρης).

- **Μη Άρνηση Ταυτότητας (non-repudiation):** Η μη-αποποίηση των ευθυνών εκ των υστέρων χρηστών που συμμετείχαν σε μια ηλεκτρονική επικοινωνία.

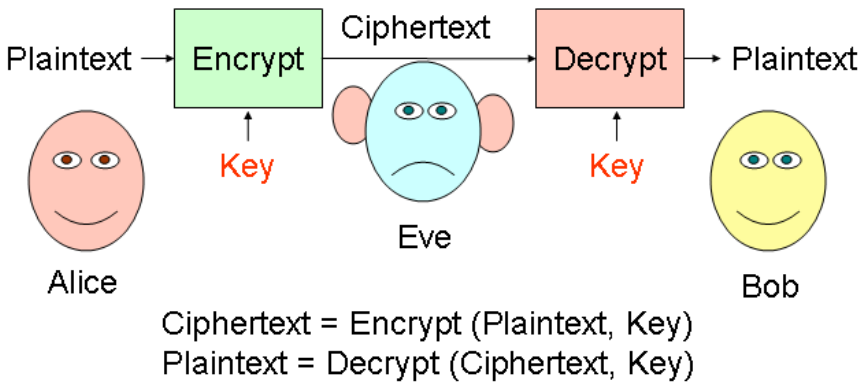
  Ουσιαστικά αυτό σημαίνει ότι μπορούμε να επιρρίψουμε με σιγουριά ευθύνες σε χρήστες για κινήσεις ή παραλήψεις που έκαναν κατά τη διάρκεια μιας επικοινωνίας αφού μπορούμε να είμαστε σίγουροι για τους συμμετέχοντες και το ρόλο του καθενός. Είναι σημαντικό οι συμμετέχοντες σε μια επικοινωνία που χειρίζεται εμπιστευτικές πληροφορίες, να μη μπορούν να αρνηθούν την εμπλοκή τους.

Ο συνδυασμός της Αυθεντικότητας (πιστοποίηση ταυτότητας) και της Ακεραιότητας (μη αλλοίωσης) των δεδομένων είναι γνωστός ως *Εγκυρότητα (validity)* των πληροφοριών.

Σε περιπτώσεις που είναι απαραίτητη η αδιάλειπτη παροχής πρόσβασης σε πληροφορίες από εξουσιοδοτημένους χρήστες, ορίζεται και η έννοια της *διαθεσιμότητας* των πληροφοριών. Για παράδειγμα αν μια εταιρεία που διαθέτει λογαριασμούς ηλεκτρονικού ταχυδρομείου δεν μπορεί να εξυπηρετήσει τους εξουσιοδοτημένους χρήστες της λόγω επίθεσης στο δίκτυο της, αυτό αποτελεί απώλεια διαθεσιμότητας.

Ασφάλεια των πληροφοριών είναι η επίτευξη του σχεδιαζόμενου επιπέδου διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των πληροφοριών.

Για την εξασφάλιση της εμπιστευτικότητας των πληροφοριών, η πιο συχνά χρησιμοποιούμενη τεχνική είναι η κρυπτογράφηση: Σκοπός της κρυπτογράφησης είναι η μετατροπή ενός αρχικού μηνύματος με τρόπο τέτοιο ώστε να μη μπορεί να διαβαστεί από οποιονδήποτε εκτός από τον τελικό παραλήπτη. Προφανώς ο παραλήπτης θα χρησιμοποιήσει την αντίστροφη τεχνική (αποκρυπτογράφηση) για να αποκαλύψει την αρχική πληροφορία. Όσο αφορά την ασφάλεια σε μια μετάδοση δεδομένων, θεωρούμε ότι πάντα υπάρχει κάποιος που προσπαθεί να υποκλέψει τις πληροφορίες που μεταδίδουμε και ότι έχει πιθανότητες να το πετύχει.

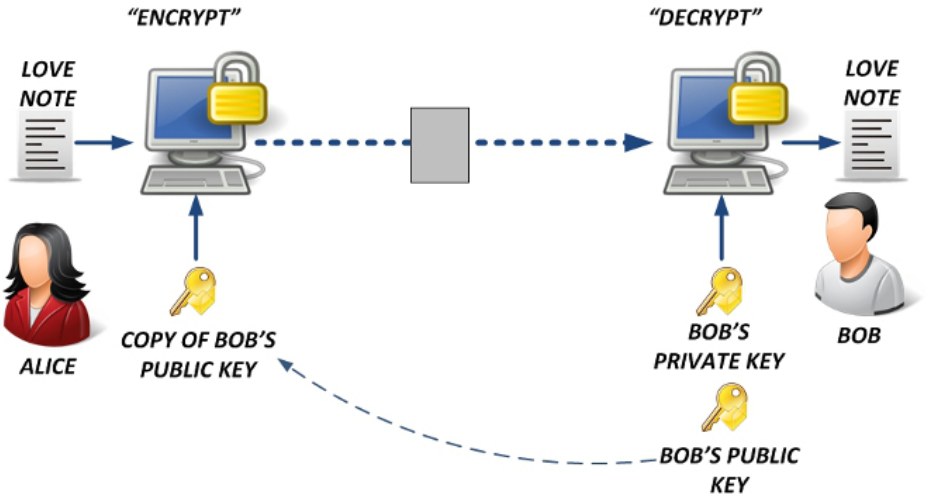


Σχήμα 8.1: *Κρυπτογραφημένη Επικοινωνία*

- **Κρυπτογράφηση** είναι η εφαρμογή μιας τεχνικής, συνήθως ένος μαθηματικού αλγόριθμου, μετατροπής της πληροφορίας από μορφή απλού κειμένου σε μορφή μη-αναγνωρίσιμη ώστε να μην είναι προσβάσιμη κατά τη μεταφορά

της από μη εξουσιοδοτημένα άτομα

- **Αποκρυπτογράφηση:** είναι μια τεχνική αντίστροφη της κρυπτογράφησης που εφαρμόζεται μόνο από εξουσιοδοτημένα άτομα σε κρυπτογραφημένη πληροφορία ώστε να επανέλθει στην αρχική μορφή απλού κειμένου
- **Κρυπτογράφημα (ή κρυπτόγραμμα, ciphertext)** είναι η μη-αναγνωρίσιμη μορφή που προκύπτει όταν υποστεί κρυπτογράφηση το αρχικό απλό κείμενο
- **Κλειδί (key)** είναι ένας κωδικός από ψηφιακά δεδομένα (μια σειρά από bytes ή ένα αρχείο π.χ.) το οποίο χρησιμοποιείται από τον αλγόριθμο κρυπτογράφησης / αποκρυπτογράφησης για την αντίστοιχη διαδικασία



Σχήμα 8.2: *Κρυπτογράφηση Δημόσιου Κλειδιού*

Υπάρχουν δυο βασικά είδη κρυπτογράφησης: στην *συμμετρική* κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Στην περίπτωση αυτή το κλειδί ονομάζεται και *μυστικό κλειδί (secret key)* καθώς όποιος το έχει μπορεί προφανώς να αποκρυπτογραφήσει το μήνυμα. Είναι σημαντικό σε αυτή την περίπτωση το κλειδί να μη διαρρεύσει και πρέπει επίσης να βρεθεί ασφαλής τρόπος για να δοθεί σε όλα τα ενδιαφερόμενα μέρη.

Αντίθετα στην *κρυπτογράφηση με δημόσιο κλειδί* (σχήμα 8.2) ή μη-συμμετρική κρυπτογράφηση, κάθε χρήστης διαθέτει δύο κλειδιά: ένα *δημόσιο κλειδί (public key)* και ένα *ιδιωτικό κλειδί (private key)*. Η ιδέα εδώ είναι ότι όλοι ανταλλάσσουν τα δημόσια κλειδιά τους ενώ κρατάνε τα ιδιωτικά ως μυστικά. Στη κρυπτογράφηση δημόσιου κλειδιού, ότι κλειδώνει με το δημόσιο κλειδί ξεκλειδώνει μόνο με το αντίστοιχο ιδιωτικό (τα κλειδιά δημιουργούνται ως ζεύγη). Έτσι αν ο χρήστης Α θέλει

να στείλει ένα ιδιωτικό μήνυμα στον Β, χρησιμοποιεί το δημόσιο κλειδί του Β για να το κρυπτογραφήσει. Το μήνυμα έπειτα μπορεί να αποκρυπτογραφηθεί μόνο από τον Β χρησιμοποιώντας το ιδιωτικό κλειδί του.

Παράρτημα Α΄

Μεθοδολογία Ασκήσεων Υποδικτύωσης

Α΄.1 Μεθοδολογία Ασκήσεων Υποδικτύωσης

Για να επιλύσουμε ασκήσεις υποδικτύωσης θα πρέπει:

- Να γνωρίζουμε μετατροπή από δυαδικό στο δεκαδικό και το ανάποδο (το βιβλίο και το βοήθημα περιγράφουν κάποιους εύκολους τρόπους).
- Να γνωρίζουμε τις δυνάμεις του δύο (όχι απαραίτητα απ'έξω βέβαια, αρκεί να γράψουμε το αντίστοιχο πινακάκι πριν ξεκινήσουμε).

Τα παραπάνω είναι απαραίτητα, καθώς για να δουλέψουμε με τις μάσκες στην υποδικτύωση θα πρέπει να έχουμε τις αντίστοιχες οκτάδες στο δυαδικό. Τα δεδομένα / ζητούμενα της άσκησης μπορεί να δίνονται / ζητούνται σε οποιοδήποτε από τα δύο συστήματα. Καλό θα είναι να εξασκηθείτε στις μετατροπές. Επίσης συνηθίστε να ελέγχετε το αποτέλεσμα μιας μετατροπής κάνοντας την αντίστροφα.

Χρήσιμο tip: Ένας αριθμός στο δυαδικό με το τελευταίο ψηφίο 0 είναι ζυγός, ενώ με 1 είναι μονός. Είναι η πιο γρήγορη αρχική επαλήθευση που μπορείτε να κάνετε.

Μάσκα Δικτύου και Διευθύνσεις Δικτύου / Εκπομπής

Η μάσκα δικτύου σε μια άσκηση μπορεί να δίνεται σε οποιαδήποτε από τις παρακάτω μορφές:

```
Δεκαδική: 255.255.240.0
Δυαδικό: 11111111 11111111 11110000 00000000
CIDR (πρόθεμα): /20
```

Όταν θέλουμε να εργαστούμε με τη μάσκα για να βρούμε διευθύνσεις δικτύου, εκπομπής ή να κάνουμε υποδικτύωση, πάντα θα πρέπει να τη φέρουμε στη δυαδική της μορφή.

Παράδειγμα 1

Δίνεται η διεύθυνση IP 192.168.3.124 με μάσκα 255.255.255.0. Να υπολογιστεί η Διεύθυνση Δικτύου και η Διεύθυνση Εκπομπής.

Απάντηση

Θα πρέπει να γράψουμε τη μάσκα και τη διεύθυνση IP στις αντίστοιχες δυαδικές μορφές κάνοντας τη μετατροπή. Για τη μάσκα είναι εύκολο να θυμάστε φυσικά ότι το 255 (που συναντάται πολύ συχνά) είναι απλά οκτώ άσοι: 11111111. Φτιάχνουμε το παρακάτω πινακάκι:

IP (Δεκαδικό):	192.	168.	3.	124
IP (Δυαδικό):	1100 0000	1010 1000	0000 0011	0111 1100
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	0000 0000
Διεύθυνση Δικτύου:	1100 0000	1010 1000	0000 0011	0000 0000
Διεύθ. Δικτύου (Δεκαδικό):	192.	168.	3.	0

Βοηθάει αν γράφουμε τους δυαδικούς χωρισμένους σε τετράδες ψηφίων ώστε να μη μπερδευόμαστε στο μέτρημα. Δεν είναι ωστόσο απαραίτητο.

Η διεύθυνση δικτύου προκύπτει από το λογικό “ΚΑΙ” της μάσκας και της διεύθυνσης IP.

Χρήσιμο tip: Όπου η μάσκα είναι 255 (ή 11111111), προκύπτει ακριβώς ο ίδιος αριθμός που αναγράφεται στην αντίστοιχη οκτάδα της διεύθυνσης IP. Όπου η μάσκα είναι μηδέν (ή 00000000) προκύπτει μηδέν στην αντίστοιχη οκτάδα. **Προσέξτε στις μάσκες δικτύου που έχουν άλλους αριθμούς: θα πρέπει να το κάνετε ανά ψηφίο.**

Για να υπολογίσουμε τη διεύθυνση εκπομπής, θα πρέπει να πάρουμε τη **διεύθυνση δικτύου που βρήκαμε πριν** και να βάλουμε 1 (ένα) σε όλα τα bit που ανήκουν στο τμήμα του υπολογιστή. Οπότε είναι σκόπιμο να γράψετε σε ένα πίνακα τη διεύθυνση δικτύου και τη μάσκα ξανά:

Διεύθυνση Δικτύου:	1100 0000	1010 1000	0000 0011	0000 0000
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	0000 0000
Διεύθυνση Εκπομπής:	1100 0000	1010 1000	0000 0011	1111 1111
Διεύθ. Εκπομπής (Δεκαδικό):	192.	168.	3.	255

Κάνουμε “1” όλα τα bit στη διεύθυνση δικτύου στα οποία τα αντίστοιχα ψηφία της μάσκας είναι μηδέν. Έπειτα μετατρέπουμε ξανά στο δεκαδικό και παίρνουμε τη διεύθυνση εκπομπής 192.168.3.255. Προσοχή, για να βρούμε τη διεύθυνση εκπομπής πρέπει να ξεκινήσουμε από τη **διεύθυνση δικτύου** και όχι την IP!

Όπως καταλαβαίνετε, η εύρεση της διεύθυνσης εκπομπής είναι πολύ εύκολη αν έχουμε μάσκα με τιμές μόνο 255 και 0. Αν ωστόσο η μάσκα που έχουμε αντιστοιχεί σε υποδικτύωση (ή υπερδικτύωση) θα πρέπει να κάνετε το παραπάνω προσεκτικά. Δείτε το παρακάτω παράδειγμα.

Παράδειγμα 2

Δίνεται η διεύθυνση IP 192.168.5.73/27. Να βρείτε τη διεύθυνση δικτύου και τη διεύθυνση εκπομπής.

Απάντηση

Στο συγκεκριμένο παράδειγμα μας δίνεται η μάσκα σε μορφή CIDR. Οπότε ξέρουμε ότι απλά θα γράψουμε 27 άσους. Μια τέτοια μάσκα δεν αντιστοιχεί σε μια τυποποιημένη κλάση (A,B,C). Έχουμε δώσει τρία παραπάνω bit στο τμήμα δικτύου και έτσι το τμήμα υπολογιστή διαθέτει μόνο 5 bit. Πρόκειται δηλ. για υποδικτύωση. Κάνουμε ξανά τον αντίστοιχο πίνακα:

IP (Δεκαδικό):	192.	168.	5.	73
IP (Δυαδικό):	1100 0000	1010 1000	0000 0101	0100 1001
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	1110 0000
Διεύθυνση Δικτύου:	1100 0000	1010 1000	0000 0101	0100 0000
Διεύθ. Δικτύου (Δεκαδικό):	192.	168.	5.	64

Δώστε προσοχή στην τελευταία οκτάδα!

Αντίστοιχα, (και με την ίδια προσοχή!) θα πρέπει να υπολογίσουμε τη διεύθυνση εκπομπής. Ξεκινάμε από τη **διεύθυνση δικτύου** που βρήκαμε πριν και με τη μάσκα που έχουμε:

Διεύθυνση Δικτύου:	1100 0000	1010 1000	0000 0101	0100 0000
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	1110 0000
Διεύθυνση Εκπομπής:	1100 0000	1010 1000	0000 0101	0101 1111
Διεύθ. Εκπομπής (Δεκαδικό):	192.	168.	5.	95

Η διεύθυνση εκπομπής προκύπτει όταν κάνουμε “1” τα ψηφία στη διεύθυνση δικτύου στα οποία τα αντίστοιχα ψηφία της μάσκας είναι “0”. Δηλ. κάνουμε “1” τα ψηφία που ανήκουν στο τμήμα υπολογιστή. Και βλέπετε ότι σε αυτή τη περίπτωση η απάντηση δεν είναι προφανής (όπως όταν έχουμε μόνο 255 και 0 στη μάσκα).

Για να επαληθεύετε τα αποτελέσματα σας μπορείτε πάντα να επισκεφθείτε μια από τις πολλές σελίδες στο διαδίκτυο που υπολογίζουν τις αντίστοιχες διευθύνσεις. Π.χ. για διευθύνσεις δικτύου και εκπομπής, δείτε:

http://www.remotemonitoringsystems.ca/broadcast.php

Ασκήσεις προς επίλυση

1. Να βρείτε τη διεύθυνση δικτύου και εκπομπής σε ένα δίκτυο όπου μια διεύθυνση IP είναι 10.14.28.55 και η μάσκα είναι 255.240.0.0. (Τα αποτελέσματα να εκφραστούν και στο δεκαδικό σύστημα).

2. Να βρείτε τη διεύθυνση δικτύου και εκπομπής σε ένα δίκτυο με IP 192.168.3.94 /26. (Τα αποτελέσματα να εκφραστούν και στο δεκαδικό σύστημα).

3. Να βρείτε τη διεύθυνση δικτύου και εκπομπής σε ένα δίκτυο με IP 192.168.230.20 και μάσκα 255.255.248.0. (Τα αποτελέσματα να εκφραστούν και στο δεκαδικό σύστημα).

Υποδικτύωση

Στην υποδικτύωση, δίνουμε κάποια ψηφία από το τμήμα υπολογιστή στο τμήμα δικτύου. Έτσι για παράδειγμα, ενώ στην κλάση C έχουμε 24 bit στο τμήμα δικτύου και 8 στο τμήμα υπολογιστή, με την υποδικτύωση μπορούμε να μειώσουμε το τμήμα υπολογιστή και να αυξήσουμε το τμήμα δικτύου. Για παράδειγμα, αν δώσουμε 27 bit στο τμήμα δικτύου (με τη βοήθεια πάντα της μάσκας) θα μας μείνουν μόνο 5 bit στο τμήμα υπολογιστή.

Χωρίζουμε ένα δίκτυο κλάσης C συνήθως για διαχειριστικούς λόγους: Δεν θέλουμε ένα δίκτυο με 254 μηχανήματα αλλά μερικά δίκτυα με λιγότερα (ένα για το λογιστήριο, ένα για την αποθήκη, ένα για τη μισθοδοσία κλπ). Χωρίζουμε ένα δίκτυο κλάσης B σε μικρότερα γιατί σχεδόν καμιά εταιρεία δεν θα χρησιμοποιήσει σε μια εγκατάσταση 65534 υπολογιστές: χωρίζοντας το σε μερικά κομμάτια π.χ. των 8000 υπολογιστών, μπορούμε να τα διαθέσουμε σε πολλές εταιρείες και να αποφύγουμε τη σπατάλη διευθύνσεων.

Χρήσιμο tip: Όταν δίνουμε bits από το τμήμα υπολογιστή στο τμήμα δικτύου, έχουμε υποδικτύωση. Όταν δίνουμε bits από το τμήμα δικτύου στο τμήμα υπολογιστή έχουμε υπερδικτύωση.

Παραδείγματα Υποδικτύωσης

Παράδειγμα 1

Δίνεται η διεύθυνση δικτύου 192.168.12.0/24.

1. Να χωριστεί το δίκτυο σε 5 τουλάχιστον υποδίκτυα, να δοθούν οι διευθύνσεις δικτύου και εκπομπής για κάθε υποδίκτυο
2. Πόσους υπολογιστές έχει το κάθε υποδίκτυο;

Απάντηση

Είναι εμφανές ότι έχουμε ένα δίκτυο κλάσης C με μάσκα 255.255.255.0. Αν το χωρίσουμε σε 5 υποδίκτυα, το κάνουμε μάλλον για διαχειριστικούς λόγους.

Θα πρέπει να πάρουμε κάποια bit από το τμήμα υπολογιστή και να τα δώσουμε στο τμήμα δικτύου. Αλλά πόσα;

Αντί για ένα δίκτυο, θέλουμε πλέον 5. Με 2 bit επιπλέον μπορούμε να φτιάξουμε 2^2=4 δίκτυα ενώ με 3 bit, 2^3=8. Προφανώς τα δύο bit είναι λίγα, ενώ τα τρία περισσεύουν. Ωστόσο δεν έχουμε ενδιάμεση επιλογή και θα χρησιμοποιήσουμε τρία bit. Άλλωστε για αυτό το λόγο και η άσκηση λέει **τουλάχιστον** 5 υποδίκτυα, και όχι ακριβώς 5! Αν μας δώσουν πλήθος υποδικτύων που είναι δύναμη του 2, θα μπορέσουμε να το κάνουμε ακριβώς.

Στο σημείο αυτό είναι χρήσιμο να έχουμε το παρακάτω πινακάκι δυνάμεων του 2. Αν δεν είστε εξοικειωμένοι με τις δυνάμεις του 2 τουλάχιστον μέχρι το 2^8 καλό θα είναι να το γράψετε πριν ξεκινήσετε την άσκηση για να το έχετε ως αναφορά:

Ψηφία n	**Πλήθος 2^n**
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	256

Και από τον πίνακα είναι εμφανές ότι για 5 υποδίκτυα χρειαζόμαστε 3 bit. Αυτά τα τρία bit θα πάρουν τιμή “1” στη μάσκα του δικτύου που θα φτιάξουμε!

Για να ξεκινήσουμε πρέπει να γράψουμε τη διεύθυνση δικτύου στο δυαδικό:

Διεύθυνση Δικτύου:	192.	168.	12.	0
Δ. Δικτύου (Δυαδικό):	1100 0000	1010 1000	0000 1100	0000 0000
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	1110 0000
Μάσκα (Δεκαδικό):	255.	255.	255	224

Δώσαμε τρία επιπλέον ψηφία από το τμήμα υπολογιστή στο τμήμα δικτύου, έτσι η νέα μάσκα είναι 255.255.255.224.

Μπορούμε τώρα να γράψουμε τα οκτώ υποδίκτυα που προκύπτουν (θυμηθείτε ότι περισσεύουν…)

Α/Α	**1η οκτάδα**	**2η οκτάδα**	**3η οκτάδα**	**4η οκτάδα**		**Διευθύνσεις**
0	1100 0000	1010 1000	0000 1100	000	00000	192.168.12.0
					11111	192.168.12.31
1	1100 0000	1010 1000	0000 1100	001	00000	192.168.12.32
					11111	192.168.12.63
2	1100 0000	1010 1000	0000 1100	010	00000	192.168.12.64
					11111	192.168.12.95
3	1100 0000	1010 1000	0000 1100	011	00000	192.168.12.96
					11111	192.168.12.127
4	1100 0000	1010 1000	0000 1100	100	00000	192.168.12.128
					11111	192.168.12.159
5	1100 0000	1010 1000	0000 1100	101	00000	192.168.12.160
					11111	192.168.12.191
6	1100 0000	1010 1000	0000 1100	110	00000	192.168.12.192
					11111	192.168.12.223
7	1100 0000	1010 1000	0000 1100	111	00000	192.168.12.224
					11111	192.168.12.255

Πως τα γράψαμε; Θυμηθείτε στις τρεις πρώτες οκτάδες δεν υπάρχει καμιά αλλαγή: ανήκουν εξ'ολοκλήρου στο δίκτυο. Στη τέταρτη οκτάδα ωστόσο, τα τρία πρώτα bit δείχνουν το δίκτυο και τα άλλα πέντε τον υπολογιστή. Οπότε για κάθε ένα από τους 8 συνδυασμούς των τριών πρώτων ψηφίων τα άλλα πέντε μπορούν να πάρουν όλες τις τιμές από 00000 μέχρι 11111.

Σε όλα αυτά τα υποδίκτυα, η πρώτη διεύθυνση που βρίσκουμε είναι η διεύθυνση δικτύου και η τελευταία η διεύθυνση εκπομπής! Μπορείτε αν θέλετε να το επαληθεύσετε με τη βοήθεια της μάσκας υποδικτύου.

Έτσι μπορούμε να δώσουμε τον παρακάτω πίνακα απαντήσεων:

A/A	Διεύθυνση Δικτύου	Διεύθυνση Εκπομπής	IP Από – Εώς	Πλήθος Υπολογιστών
0	192.168.12.0	192.168.12.31	192.168.12.1 192.168.12.30	30
1	192.168.12.32	192.168.12.63	192.168.12.33 192.168.12.62	30
2	192.168.12.64	192.168.12.95	192.168.12.65 192.168.12.94	30
3	192.168.12.96	192.168.12.127	192.168.12.97 192.168.12.126	30
4	192.168.12.128	192.168.12.159	192.168.12.129 192.168.12.158	30
5	192.168.12.160	192.168.12.191	192.168.12.161 192.168.12.190	30
6	192.168.12.192	192.168.12.223	192.168.12.193 192.168.12.222	30
7	192.168.12.224	192.168.12.255	192.168.12.225 192.168.12.254	30

Παράδειγμα 2

Ενώ στο πρώτο παράδειγμα μας ζήτησαν συγκεκριμένο αριθμό δικτύων, σε άλλη περίπτωση μπορεί να μας ζητήσουν να φτιάξουμε υποδίκτυα με συγκεκριμένο αριθμό μηχανημάτων. Για παράδειγμα:

Δίνεται η διεύθυνση δικτύου 192.168.14.0 με μάσκα 255.255.255.0 (δηλ /24). Να χωριστεί σε υποδίκτυα ώστε το καθένα από αυτά να έχει τουλάχιστον 14 μηχανήματα.

Απάντηση

Σκεφτόμαστε με τον ίδιο τρόπο όπως προηγουμένως, μόνο που τώρα υπολογίζουμε πόσα bit χρειαζόμαστε για τα μηχανήματα. Τα υπόλοιπα bit θα τα διαθέσουμε στο τμήμα δικτύου.

Για 14 μηχανήματα, χρειαζόμαστε 4 ψηφία, γιατί 2^4=16. Τα 3 ψηφία δεν αρκούν (2^3=8). Παρατηρήστε ότι με 4 ψηφία θα έχουμε **ακριβώς 14 μηχανήματα, γιατί χάνουμε δύο διευθύνσεις ανά υποδίκτυο (δικτύου και εκπομπής).**

Εδώ λοιπόν θα κρατήσουμε τα 4 τελευταία ψηφία της 4ης οκτάδας για το τμήμα υπολογιστή και θα δώσουμε τα άλλα 4 στο τμήμα υπολογιστή.

Θα έχουμε λοιπόν συνολικά 16 υποδίκτυα, με 14 μηχανήματα στο καθένα. Θα υπολογίσουμε αρχικά τη μάσκα δικτύου:

Διεύθυνση Δικτύου:	192.	168.	14.	0
Δ. Δικτύου (Δυαδικό):	1100 0000	1010 1000	0000 1110	0000 0000
Μάσκα (Δυαδικό):	1111 1111	1111 1111	1111 1111	1111 0000
Μάσκα (Δεκαδικό):	255.	255.	255	240

Α/Α	**1η οκτάδα**	**2η οκτάδα**	**3η οκτάδα**	**4η οκτάδα**		**Διευθύνσεις**
0	1100 0000	1010 1000	0000 1110	0000	0000	192.168.14.0
					1111	192.168.14.15
1	1100 0000	1010 1000	0000 1110	0001	0000	192.168.14.16
					1111	192.168.14.31
2	1100 0000	1010 1000	0000 1110	0010	0000	192.168.14.32
					1111	192.168.14.47
3	1100 0000	1010 1000	0000 1110	0011	0000	192.168.14.48
					1111	192.168.14.63
4	1100 0000	1010 1000	0000 1110	0100	0000	192.168.14.64
					1111	192.168.14.79
5	1100 0000	1010 1000	0000 1110	0101	0000	192.168.14.80
					1111	192.168.14.95
6	1100 0000	1010 1000	0000 1110	0110	0000	192.168.14.96
					1111	192.168.12.111
7	1100 0000	1010 1000	0000 1110	0111	0000	192.168.14.112
					1111	192.168.14.127

Και ακόμα 8 υποδίκτυα που δεν δείχνουμε για οικονομία χώρου (και χαρτιού)!

Όπως καταλαβαίνετε, σε καθένα από αυτά τα υποδίκτυα η πρώτη διεύθυνση είναι η **διεύθυνση δικτύου και η τελευταία η διεύθυνση εκπομπής.** Το κάθε υποδίκτυο συνδέει ακριβώς 14 υπολογιστές. Συνολικά έχουμε 16 X 14 = 224 υπολογιστές αντί για 254.

Μπορείτε να δείτε πάντα σε ένα αντίστοιχο web calculator αν έχετε κάνει τους σωστούς υπολογισμούς:

http://jodies.de/ipcalc

Προσπαθήστε τώρα να λύσετε τη δραστηριότητα 3η του βιβλίου (σελ. 81) χωρίς τη βοήθεια του site :D

Παράρτημα Β΄

Ορόσημα (Milestones)

Β΄.1 Ορόσημα στη Συγγραφή του Βοηθήματος

Ημερομηνία	Περιγραφή
12/09/2016	Δημιουργία του GitHuB Repository
02/10/2016	Δημιουργία του αρχικού σκελετού αρχείων LaTeX.
02/10/2016	Συγγραφή της πρώτης ενότητας (1.2.2)
09/10/2016	Ολοκλήρωση Κεφαλαίου 1
09/10/2016	Δημιουργία της Παρουσίασης διδασκαλίας
29/10/2016	Ολοκλήρωση Κεφαλαίου 2
29/01/2017	Ολοκλήρωση Κεφαλαίου 3
07/02/2017	Ολοκλήρωση Κεφαλαίου 4
08/02/2017	Προσθήκη Παραρτήματος: Μεθοδολογία Ασκήσεων Κεφ. 3
09/02/2017	Ολοκλήρωση όλων των εναπομείναντων εικόνων / σχημάτων
16/02/2017	Προσθήκη φωτογραφίας / αφιέρωσης
18/02/2017	Ολοκλήρωση Κεφαλαίου 8
19/02/2017	Προσθήκη Επίσημου Εξωφύλλου Έκδοσης (Σκίτσο)
19/02/2017	Ολοκλήρωση Κεφαλαίου 7
21/02/2017	Ολοκλήρωση Κεφαλαίου 5
23/02/2017	Προσθήκη του παρόντος Παραρτήματος
24/02/2017	Ολοκλήρωση κειμένου. Αναθεώρηση alpha1
27/02/2017	Αναθεώρηση beta1
01/03/2017	Επίσημη Κυκλοφορία 1.00
04/10/2017	Επίσημη Κυκλοφορία 2.00