Πανεπιστήμιο Πελοποννήσου
Τμήμα Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών

Διαχείριση και Ασφάλεια Δικτύων

Εισαγωγή στη Διαχείριση Δικτύων

Ανάγκη διαχείρισης δικτύων

- Αναλογιστείτε το μέγεθος και την πολυπλοκότητα ενός οργανισμού παροχής επικοινωνιακών υπηρεσιών…
  - Εκατοντάδες+ δικτυακές συσκευές…
  - Εκατοντάδες++ ζεύξεις…
  - Δεκάδες πελάτες με συμφωνίες επιπέδου υπηρεσιών πραγματικού χρόνου (SLAs)…
  - Χιλιάδες πελάτες…
  - Απειλές ασφάλειας
- Ανάγκη αυτοματοποίησης των λειτουργιών παρακολούθησης και ελέγχου
- Ανάγκη για άμεση ανίχνευση συμβάντων και απόκριση

Λειτουργίες διαχείρισης

- Το μοντέλο "FCAPS" (κατά OSI…)
  - Διαχείριση σφαλμάτων (Fault management)
  - Διαχείριση διαμόρφωσης (Configuration management)
  - Λογιστική διαχείριση (Accounting management)
  - Διαχείριση απόδοσης (Performance management)
  - Διαχείριση ασφάλειας (Security management)

Διαχείριση σφαλμάτων

- Το σύνολο των διαδικασιών που επιτρέπουν:
  - την ανίχνευση των σφαλμάτων
  - τη διάγνωση
  - την απομόνωση
  - τη διόρθωση
- Λειτουργίες διαχείρισης σφαλμάτων:
  - Παρακολούθηση δικτυακών στοιχείων και ζεύξεων
  - Καθορισμός τιμών κατωφλίου (thresholds) και ορισμός ειδοποιήσεων και "συναγερμών"
  - Διατήρηση αρχείων καταγραφής
  - Αποκατάσταση ομαλής λειτουργίας
  - Πρόβλεψη και αποφυγή σφαλμάτων

Διαχείριση διαμόρφωσης

- Αναφέρεται στη διαδικασία απεικόνισης και ελέγχου της κατάστασης του δικτύου, σε φυσικό και λογικό επίπεδο:
  - Συλλογή πληροφοριών κατάστασης, είτε τακτικά είτε εκτάκτως εφόσον κριθεί απαραίτητο
  - Καθορισμός και τροποποίηση παραμέτρων λειτουργίας
  - Διαχείριση παραμέτρων λειτουργίας
- Ενδεικτικές λειτουργίες:
  - Εισαγωγή νέων συνδέσεων και λογικών δρόμων
  - Αναδρομολόγηση κίνησης
  - Αρχικοποίηση, επανεκκίνηση, αναδιαμόρφωση, τερματισμός δικτυακών στοιχείων και ζεύξεων

Λογιστική διαχείριση

- Περιλαμβάνει όλες τις διαδικασίες για:
  - Συλλογή και επεξεργασία στοιχείων χρήσης των διαθέσιμων πόρων
  - Χρέωση και τιμολόγηση
  - Διαχείριση διατήρησης στοιχείων όπως απαιτείται από την υφιστάμενη νομοθεσία
  - Διαχείριση παραμέτρων συλλογής και επεξεργασίας
  - Παρακολούθηση δεικτών ορθής χρήσης
- Στοχεύει:
  - Στο κέρδος…
  - Στο σχεδιασμό της εξέλιξης του δικτύου
  - Στη συμμόρφωση με κανονιστικές απαιτήσεις

Διαχείριση απόδοσης

- Η διαχείριση απόδοσης αφορά:
  - Την παρακολούθηση της δραστηριότητας του δικτύου
  - Τον έλεγχο του δικτύου για την πραγματοποίηση ενεργειών που θα οδηγήσουν σε βελτίωση της απόδοσης
- Ενδεικτικές λειτουργίες:
  - Παρακολούθηση χαρακτηριστικών παραμέτρων επίδοσης όπως ρυθμός μετάδοσης, ρυθμός απώλειας πακέτων, καθυστερήσεις, …
  - Παρακολούθηση τιμών αναφορικά με την τήρηση των SLAs
  - Δημιουργία ενημερώσεων
  - Διαχείριση αρχείων καταγραφής
  - Τροποποίηση παραμέτρων λειτουργίας με σκοπό τη βελτίωση της απόδοσης

Διαχείριση ασφάλειας

- Τελικός στόχος: η προστασία του δικτύου και των χρηστών του από εισβολές και κακόβουλες ενέργειες
- Ενδεικτικές λειτουργίες:
  - Ανάπτυξη και διαχείριση πολιτικής ασφάλειας
  - Αποτροπή, ανίχνευση και αντιμετώπιση επιθέσεων
  - Διαχείριση περιοχών δικτύου
  - Διαχείριση δικαιωμάτων πρόσβασης
  - Διαχείριση στοιχείων κρυπτογραφίας
  - Διαχείριση αρχείων καταγραφής

Μερικές εικόνες…

Συστήματα διαχείρισης δικτύου

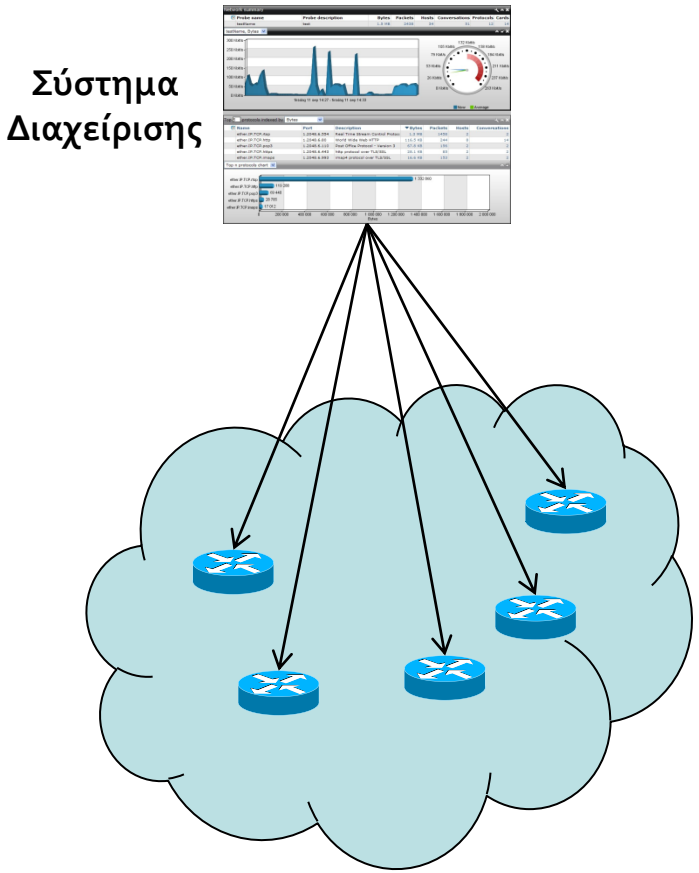
- Βασικά χαρακτηριστικά:
  - Γραφική διεπαφή χρήστη, π.χ.:
    - Γραφικό σύστημα παρουσίασης της τοπολογίας του δικτύου
    - Γραφήματα δεικτών
  - Συλλογή όλων των πληροφοριών από τα διαχειριζόμενα στοιχεία με όσο δυνατόν μεγαλύτερη διαφάνεια
  - Εύκολη προσθήκη νέων δυνατοτήτων και εργαλείων διαχείρισης ανάλογα με τις απαιτήσεις του κάθε δικτύου
  - Δυνατότητα ανίχνευσης, ειδοποίησης και αναφοράς προβληματικών καταστάσεων στο δίκτυο
  - Αποδοτικός τρόπος φύλαξης του όγκου πληροφοριών που χρειάζεται για τη διαχείριση
  - Σταθερότητα και αξιοπιστία: πρέπει να παραμένει ενεργό ακόμα και όταν σημαντικές καταστάσεις προβλημάτων συμβαίνουν στο δίκτυο

Συστήματα διαχείρισης δικτύου

- Κυριότερες τοπολογίες:
  - Κεντρικοποιημένη αρχιτεκτονική
  - Ιεραρχικά κατανεμημένη αρχιτεκτονική
  - Κατανεμημένη αρχιτεκτονική
- Βασικά δομικά στοιχεία:
  - Σταθμός Διαχείρισης (Network Management Station)
  - Διαχειριζόμενα στοιχεία – «αντικείμενα»
  - Πράκτορας (Agent)
  - Βάση Πληροφοριών Διαχείρισης (Management Information Base)
  - Βάση Δεδομένων Διαχείρισης (Management Database)
  - Πρωτόκολλο Διαχείρισης Δικτύου (Network Management Protocol)
    - TCP/IP: Simple Network Management Protocol (SNMP)
    - OSI: Common Management Information Protocol (CMIP)

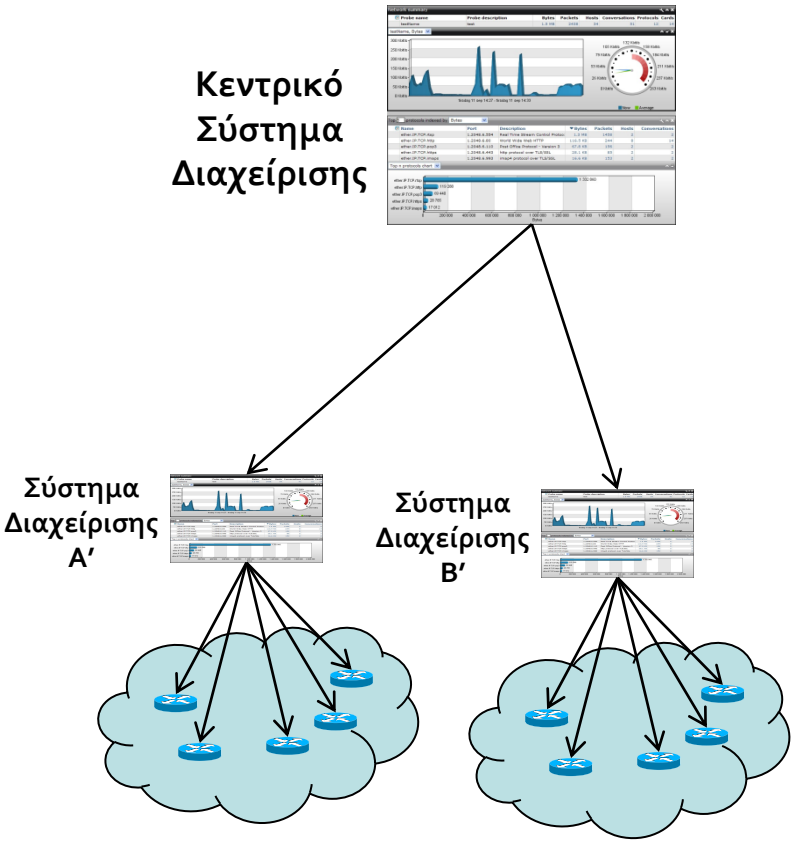
Κεντρικοποιημένη αρχιτεκτονική

- Κεντρικός διαχειριστής:
  - Επικοινωνεί με όλα τα υπό διαχείριση στοιχεία
  - Πραγματοποιεί το σύνολο της διαχείρισης
- Πλεονεκτήματα:
  - Απλότητα
  - Συνολική διαχείριση
- Μειονεκτήματα:
  - Απαιτήσεις επεξεργαστικής ισχύος
  - Αδυναμία κλιμάκωσης
  - Μοναδικό σημείο αποτυχίας



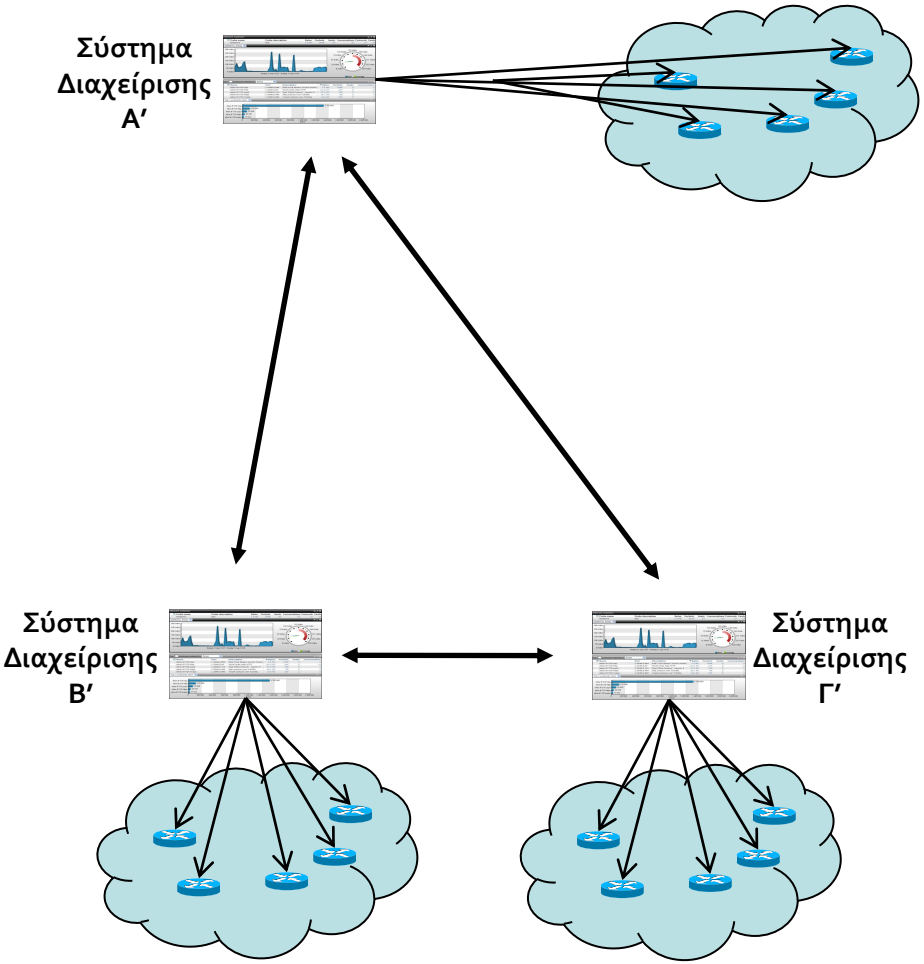
Ιεραρχικά κατανεμημένη αρχιτεκτονική

- Οι σταθμοί διαχείρισης οργανώνονται με ιεραρχικό τρόπο
- Οι διαχειριστές του χαμηλότερου επιπέδου ελέγχουν συγκεκριμένα τμήματα του δικτύου
- Οι πληροφορίες διαχείρισης διαχέονται προς τα πάνω έχοντας ήδη υποστεί επεξεργασία
- Ανεβαίνοντας επίπεδο, οι διαχειριστές έχουν εικόνα όλου του υποδέντρου που ορίζουν
- Ο διαχειριστής – ρίζα του δέντρου διαχείρισης έχει πλήρη εικόνα του δικτύου

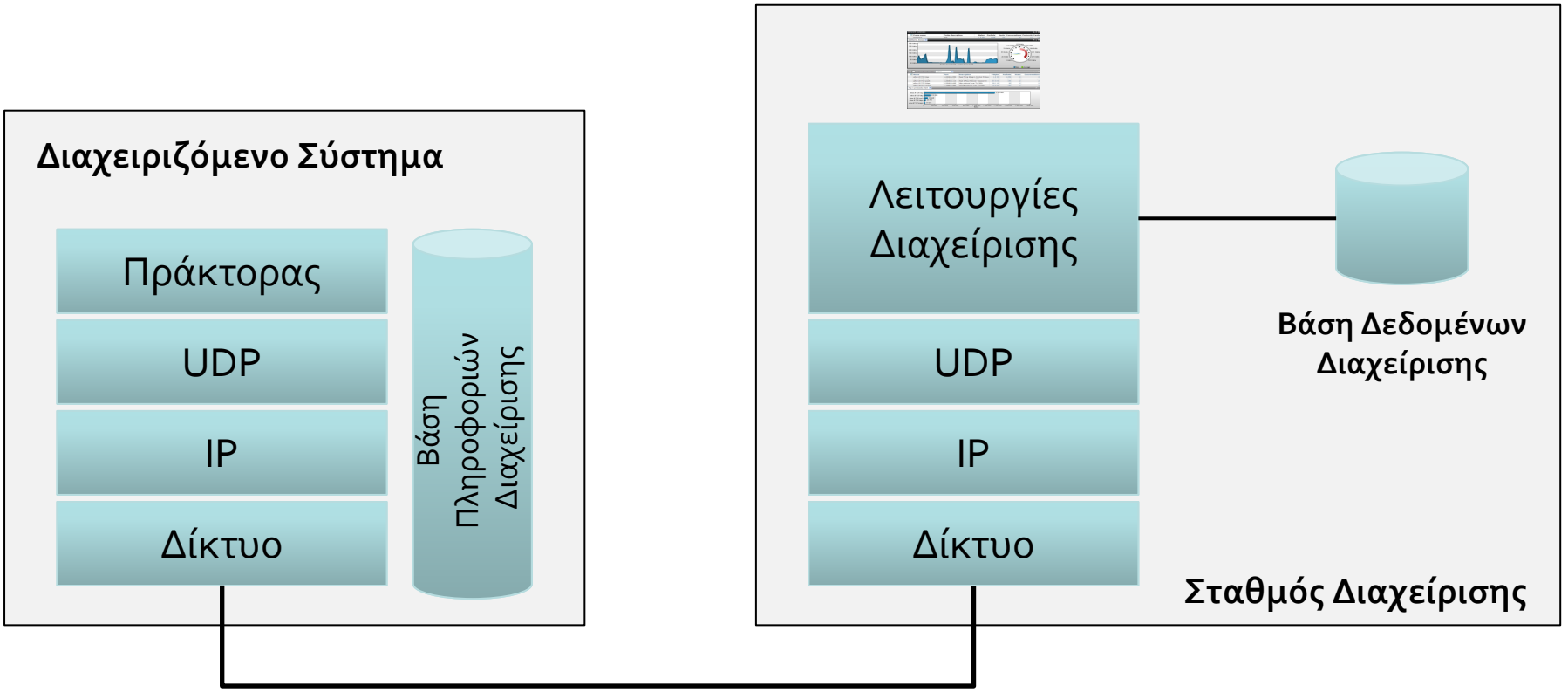


Κατανεμημένη αρχιτεκτονική

- Η διαχείριση κατανέμεται σε «τοπικούς» διαχειριστές
- Οι διαχειριστές αποτελούν «ομότιμες» οντότητες



Διαχειριστής και διαχειριζόμενος



Μοντέλο λειτουργίας

- Ακολουθείται το μοντέλο πελάτη – εξυπηρετητή (client – server)
  ή αλλιώς…
  διαχειριστή – πράκτορα (manager – agent)

- Δύο τρόποι συλλογής πληροφοριών:
  - Ερώτηση & απάντηση
  - Αναφορά γεγονότων