Δ Ι Α Χ Ε Ι Ρ Ι Σ Η Δ Ι Κ Τ Υ Ο Υ

Η αναγκαιότητα της Διαχείρισης Δικτύου

Ένα δίκτυο ηλεκτρονικών υπολογιστών (Η/Υ) είναι μια σύνθετη δομή που περιλαμβάνει τους Η/Υ και τις περιφερειακές συσκευές που συνδέονται σε αυτό, την καλωδίωση του κτιρίου και τις συσκευές που υποστηρίζουν τη λειτουργία των δικτυακών υπηρεσιών. Η σύνθετη αυτή δομή καθιστά σχεδόν υποχρεωτική την ύπαρξη ενός συστήματος παρακολούθησης και διαχείρισης του δικτύου για να μπορεί ένας διαχειριστής:

α) να εντοπίζει στο συντομότερο δυνατό χρόνο την εστία του προβλήματος,
β) να επιδιορθώνει το πρόβλημα και
γ) να αποκαθιστά τη λειτουργία και τις υπηρεσίες του δικτύου στα επίπεδα προδιαγραφών για τα οποία σχεδιάστηκε.

Για την αποτελεσματική διαχείριση ενός δικτύου δεδομένων είναι χρήσιμο, αν όχι απαραίτητο για τα μεγάλα σε μέγεθος δίκτυα, ο σχεδιασμός και η εγκατάσταση ενός ***Συστήματος Διαχείρισης Δικτύου (Network Management System, NMS).***

Ένα Σύστημα Διαχείρισης Δικτύου (NMS) είναι ένας συνδυασμός εργαλείων υλικού ή/ και λογισμικού, τα οποία επιτρέπουν στο διαχειριστή να επιβλέπει τα επιμέρους στοιχεία από τα οποία αποτελείται ένα δίκτυο και να το ελέγχει για σημεία με προβληματική λειτουργία σε σχέση με τα αποδεκτά επίπεδα λειτουργίας.

Για το σκοπό αυτό έχουν σχεδιαστεί πρότυπα Διαχείρισης Δικτύου για αποτελεσματικότερη κάλυψη όλων των παραμέτρων που απαιτούνται για την ομαλή λειτουργία ενός δικτύου.

Το μοντέλο **FCAPS**, αποτελεί το πλέον διαδεδομένο πλαίσιο για τη διαχείριση δικτύου.

Το όνομα FCAPS προκύπτει από τις έννοιες :

- **Fault** (σφάλμα),
- **Configuration** (παραμετροποίηση),
- **Accounting** (κόστος),
- **Performance** (επίδοση),
- **Security** (ασφάλεια).

Παραμετροποίηση (Configuration management, CM)

Η διαχείριση παραμετροποίησης ασχολείται με την παρακολούθηση των πληροφοριών των παραμέτρων του δικτύου και τις όποιες αλλαγές συμβαίνουν σε αυτό.

Σκοπός της είναι η διατήρηση της συνοχής του δικτύου και όλων των λειτουργικών προδιαγραφών του. Η περιοχή διαχείρισης αυτή είναι ιδιαίτερα σημαντική, γιατί αρκετά προβλήματα στη λειτουργία των δικτύων προκύπτουν από τις αλλαγές σε παραμέτρους αρχείων, ενημερώσεις λογισμικού ή αλλαγές στο υλικό του συστήματος.

Η διαχείριση παραμετροποίησης περιλαμβάνει τους στόχους:

- τη συλλογή και αποθήκευση παραμέτρων των συσκευών δικτύου, τοπικά ή από απόσταση
- την απλοποίηση της παραμετροποίησης των συσκευών
- την παρακολούθηση αλλαγών που συμβαίνουν στις παραμέτρους
- τη διαμόρφωση κυκλωμάτων μέσα από δίκτυα χωρίς μεταγωγή (non-switched networks)
- τον σχεδιασμό μελλοντικών επεκτάσεων

Διαχείριση Σφαλμάτων

Για τη διατήρηση της σωστής λειτουργίας ενός δικτύου πρέπει να υπάρχει μέριμνα για την καλή λειτουργία τόσο ολόκληρου του δικτύου όσο και των επιμέρους στοιχείων του. Υπάρχει διαφορά ανάμεσα στις έννοιες σφάλμα/βλάβη και λάθος σε ένα δίκτυο.

Το σφάλμα ή βλάβη είναι μια μη φυσιολογική κατάσταση που απαιτεί την προσοχή του διαχειριστή και την άμεση διόρθωσή του. Ένα σφάλμα συνεπάγεται μη σωστή λειτουργία ή μεγάλο αριθμό λαθών (πχ. Όταν μια γραμμή επικοινωνίας είναι κομμένη και δεν διέρχεται σήμα ή υπάρχει υπερβολικά μεγάλος αριθμός από λανθασμένα bit).

Το λάθος είναι ένα μεμονωμένο γεγονός, που συνήθως δεν συνεπάγεται διακοπή της επικοινωνίας. Στην περίπτωση ύπαρξης λαθών (πχ. λάθος bit στη γραμμή επικοινωνίας) υπάρχει δυνατότητα αντιστάθμισης των συνεπειών τους με τη χρήση μηχανισμών ελέγχου λαθών στα διάφορα πρωτόκολλα που χρησιμοποιούνται.

Όταν συμβεί κάποιο σφάλμα υπάρχουν συγκεκριμένα βήματα για την επίλυση του, τα οποία ονομάζονται **Κύκλος Επεξεργασίας Διαχείρισης Σφαλμάτων (Fault Management Process Cycle).** Σύμφωνα με αυτόν και αφού συμβεί το σφάλμα, τα συνήθη βήματα που πρέπει να ακολουθούν είναι τα παρακάτω:

● Να προσδιοριστεί το σφάλμα, δηλαδή τι είδους σφάλμα είναι και από πού μπορεί να προέρχεται.

● Να εντοπιστεί το σφάλμα, ώστε να ανακαλυφθεί από ποιο σημείο του δικτύου βρίσκεται.

● Να απομονωθεί το υπόλοιπο του δικτύου, ώστε να μπορεί αυτό να λειτουργεί χωρίς παρεμπόδιση από το σφάλμα.

● Να αναδιαμορφωθεί το δίκτυο, ώστε να ελαχιστοποιηθεί η επίδραση της βλάβης σε κάποιο ή κάποια από στοιχεία του.

● Να γίνει έλεγχος και ανάλυση των ενδείξεων, ώστε να κατανοηθεί καλύτερα η αιτία και να δοθεί μια πληρέστερη εξήγηση της πηγής του σφάλματος.

● Να επισκευαστεί ή να αντικατασταθεί το στοιχείο της βλάβης, ώστε να επανέλθει το δίκτυο στην αρχική του κατάσταση.

● Να παρακολουθηθεί το δίκτυο από τον Διαχειριστή για ένα προκαθορισμένο χρονικό διάστημα, ώστε να βεβαιωθεί ότι το σφάλμα επιλύθηκε με επιτυχία.

Διαχείριση Επιδόσεων (Performance Management ή Capacity Management)

Η Διαχείριση Επιδόσεων επικεντρώνεται στη διασφάλιση ότι η απόδοση του δικτύου παραμένει στα αποδεκτά επίπεδα, αυτά για τα οποία σχεδιάστηκε να λειτουργεί.

Μελετά

- το χρόνο απόκρισης του δικτύου,
- την απώλεια πακέτων,
- τη χρήση των γραμμών επικοινωνίας,
- τα ποσοστά χρήσης,
- το βαθμό λαθών που συμβαίνουν κ.ά.

Αυτές οι πληροφορίες συνήθως συλλέγονται με την εφαρμογή ενός συστήματος διαχείρισης δικτύου, όπως είναι το πρωτόκολλο **SNMP**, με τους εξής τρόπους:

● με συνεχή παρακολούθηση και εκτίμηση από το διαχειριστή της τρέχουσας κατάστασης

● με ορισμό συναγερμών, όταν τα επίπεδα απόδοσης ανέβουν ή κατέβουν από τα προκαθορισμένα και αποδεκτά επίπεδα

Διαχείριση Κόστους (Accounting Management ή Billing Management)

Η διαχείριση κόστους ασχολείται με την παρακολούθηση των πληροφοριών που σχετίζονται με τη χρήση των πόρων ενός δικτύου και του κόστους που συνεπάγεται από αυτή τη χρήση.

Μάλιστα σε πολλές επιχειρήσεις και οργανισμούς υπάρχει χρέωση για τις προσφερόμενες υπηρεσίες του δικτύου. Ωστόσο, στα δίκτυα που δεν έχουν στόχο το κέρδος, η έννοια του κόστους (Accounting) μερικές φορές αντικαθίσταται από την έννοια της διοίκησης (Administration).

Διαχείριση Ασφάλειας (Security Management)

Η διαχείριση ασφάλειας ενός δικτύου ασχολείται με τη διαχείριση πληροφοριών που σχετίζονται με:

- την ομαλή λειτουργία του δικτύου.
- την παρακολούθηση και τον έλεγχο της πρόσβασης σε τμήματα του ή και σε όλο το δίκτυο,
- την ασφάλεια των δεδομένων που διακινούνται και αποθηκεύονται σε αυτό.

Για το σκοπό αυτό απαιτείται η χρήση εργαλείων λογισμικού, όπως:

- Πλατφόρμες συλλογής και ελέγχου δικτυακών δεδομένων (NMS Platforms)
- Εργαλεία κρυπτογράφησης (cryptography tools)
- Εργαλεία αυθεντικοποίησης (authentication) για έλεγχο πρόσβασης
- Συστήματα ελέγχου εισβολέων (intrusion detection systems)
- Διαμόρφωση και ενεργοποίηση δικτυακού τείχους προστασίας (network firewall)
- Εφαρμογή μεθόδων-πολιτικών ασφαλείας (security policies)
- Ημερολόγια καταγραφής (logs) κ.ά.

Για να είναι αποτελεσματική η διαχείριση ασφαλείας ενός δικτύου πρέπει να προβλεφθούν όλες οι πιθανές αιτίες ή τα σημεία κινδύνου, ώστε να επιλεγούν τα σημεία όπου χρειάζονται μεγαλύτερη προσοχή από τους διαχειριστές.