ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ

ΣΧΟΛΗ : ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ : ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Παρακολούθηση και Διαχείριση Λειτουργίας Δικτύων Υπολογιστών»

«Monitoring and Management of Computer Networks»

ΣΠΟΥΔΑΣΤΕΣ: ΑΡΒΑΝΙΤΗ ΒΑΣΙΛΙΚΗ

ΣΤΑΣΙΝΟΥ ΚΑΛΛΙΡΟΗ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΜΑΝΔΑΛΟΣ ΛΟΥΚΑΣ

ΠΑΤΡΑ - 2013

ΠΡΟΛΟΓΟΣ - ΕΥΧΑΡΙΣΤΙΕΣ

Θα θέλαμε να ευχαριστήσουμε θερμά τον καθηγητή μας Λουκά Μάνδαλο για την απόφαση του να μας δώσει ένα ιδιαίτερα ενδιαφέρον θέμα, τη συνεχή του συμπαράσταση, την πολύτιμη βοήθεια, την υπομονή και τη σωστή καθοδήγηση του στη συγγραφή της πτυχιακής αυτής εργασίας. Επίσης, θα θέλαμε να ευχαριστήσουμε τις οικογένειες μας και τους φίλους μας για την ηθική και ψυχολογική υποστήριξη που μας παρείχαν όλο αυτό το διάστημα.

Πάτρα, Μάρτιος 2013

Αρβανίτη Βασιλική

Στασινού Καλλιρόη

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία ασχολείται με την παρακολούθηση και την διαχείριση δικτύων υπολογιστών. Για την επίτευξη αυτών των διεργασιών χρησιμοποιούνται τα ακόλουθα στοιχειά, όπως αναφέρονται στα τέσσερα κεφάλαια της εργασίας μας.

Το πρώτο κεφάλαιο αναφέρεται στο τι χρειάζεται ένα σύστημα διαχείρισης δικτύου, τι είναι διαχείριση δικτύου, τα είδη των δικτύων, ο σκοπός τους όπως επίσης επεξηγούνται οι έννοιες Manager, NE, Agents, Λογισμικό, MIB, NMP, που σχετίζονται με τα πρωτόκολλα και τις αρχιτεκτονικές διαχείρισης δικτύων υπολογιστών (Management of Computer Networks). Αναφέρονται ακόμα τα Μοντέλα διαχείρισης, οι Αρχιτεκτονικές διαχείρισης (Κεντρική, Ιεραρχική, Κατανεμημένη), οι Διαχειρίσεις Απόδοσης, Βλαβών, Κοστολόγησης, Ασφάλειας, και Διάρθρωσης.

Το δεύτερο κεφάλαιο αναλύει. το βασικό πρωτόκολλο διαχείρισης. δικτύων SNMP (Simple Network Management Protocol) , η λειτουργία του, οι εντολές που χρησιμοποιούνται καθώς επίσης και οι νεώτερες εκδόσεις SNMPv2 και SNMPv3 αναλυτικά.

Στο τρίτο κεφάλαιο παρουσιάζεται η λειτουργία του πρωτοκόλλου CMIP (Common Management Information Protocol) Επίσης γίνεται σύγκριση μεταξύ των SNMP και CMIP πρωτοκόλλων. Επίσης παρουσιάζεται το επιπρόσθετο στοιχείο του SNMP, το RMON , που χωρίζεται σε RMON1 και RMON2 που εκτελούν διαφορετικές εργασίες το καθένα.

Στο τέταρτο κεφάλαιο παραθέτονται εργαλεία παρακολούθησης-διαχείρισης (Monitoring) δικτύων υπολογιστών. Παρουσιάζονται τα δημοφιλέστερα εργαλεία για παρακολούθηση όπως : το Openview Network Node Manager (Hewlett Packard) ,το Whatsup Gold (Ipswitch) και toNet View (IBM). Τέλος ακολουθεί μια συγκριτική αξιολόγηση των παραπάνω εργαλείων.

Στο πέμπτο και τελευταίο κεφάλαιο παραθέτονται τα συμπεράσματα και τα αποτελέσματα της εργασίας μας.

ABSTRACT

This thesis deals with the management and monitoring of computer networks. For the achievement of these processes the following tools are used, as indicated in the four chapters of our thesis.

The first chapter deals with the needs of a network management system, what is network management, types of networks, their purpose and the meanings Manager, NE, Agents, Software, MIB, NMP which are related to protocols and architectures of computer network management are also explained. We will refer to management models, the management architecture (centralized, hierarchical, distributed), the Performance Management, Fault, Estimating, Safety, and Structure.

The second chapter analyzes the Simple Network Management Protocol, it's functions, the commands used as well as the newer versions SNMPv2 and SNMPv3 in detail.

In the third chapter the function of theCMIP (Common Management Information Protocol) is described and it is also compared to the SNMP. Also is illustrated the additional element of SNMP, the RMON which is divided into RMON1 RMON2 each performing different tasks.

In the fourth chapter, management-monitoring tools are described. Presented are the most popular tools for monitoring such as: Openview Network Node Manager (Hewlett Packard), the Whatsup Gold (Ipswitch) and Net View (IBM). Finally a comparative evaluation of these tools is made.

In the fifth and last chapter, there are the conclusions and the results of our work.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

Τα τελευταία χρόνια τα δίκτυα υπολογιστών και τα συστήματα κατανεμημένης επεξεργασίας έχουν γνωρίσει μεγάλη ανάπτυξη. Η τάση στην ανάπτυξη των συστημάτων αυτών είναι προς την κατεύθυνση μεγαλύτερων και περισσότερο πολύπλοκων δικτύων τα οποία θα υποστηρίζουν περισσότερες εφαρμογές και περισσότερους χρήστες. Συνεπώς, έχει αυξηθεί σημαντικά η πιθανότητα να συμβεί κάποιο λάθος και έτσι ολόκληρο το δίκτυο ή ένα μέρος του να τεθεί εκτός λειτουργίας ή να μειωθεί η αξιοπιστία και η απόδοση του. Ειδικά σε ένα μεγάλο τοπικό δίκτυο (που μπορεί να έχει έκταση ενός μεγάλου κτιριακού συγκροτήματος ή ενός Πανεπιστημίου), η συντήρηση και ο έλεγχος του μπορεί να είναι μια διαδικασία ασύμφορη, επίπονη και χρονοβόρα, που απαιτεί να ασχοληθούν αρκετοί άνθρωποι.

Για τους παραπάνω λόγους καθώς και η πολυπλοκότητα των δικτύων και η ύπαρξη συσκευών που ανήκουν σε διαφορετικούς κατασκευαστές, έχουν κάνει αναγκαία την ανάπτυξη εργαλείων που θα βοηθήσουν στην αυτόματη και αποτελεσματική διαχείριση των δικτύων. Έτσι έχουν αναπτυχθεί τα ανάλογα πρωτόκολλα και βάσεις διαχείρισης πληροφοριών καθώς και το αντίστοιχο λογισμικό το οποίο χρησιμοποιείται για να είναι εφικτή η διαχείριση του δικτύου.

1.1 ΤΙ ΕΙΝΑΙ ΔΙΚΤΥΟ ΥΠΟΛΟΓΙΣΤΩΝ.

Ένα δίκτυο Υπολογιστών είναι ένα σύστημα επικοινωνίας δεδομένων που συνδέει δύο η περισσότερους αυτόνομους και ανεξάρτητους υπολογιστές και περιφερειακές συσκευές. Δύο υπολογιστές θεωρούνται διασυνδεδεμένοι όταν μπορούν να ανταλλάσουν μεταξύ τους πληροφορίες.

1.1.1 ΣΚΟΠΟΣ ΤΩΝ ΔΙΚΤΥΩΝ.

Τα δίκτυα δημιουργήθηκαν για να εξυπηρετήσουν τις ανάγκες που προέκυψαν από την εξάπλωση της χρήσης των υπολογιστών. Βασικός σκοπός της ύπαρξης των δικτύων είναι ο διαμερισμός των πόρων του συστήματος και η ανταλλαγή πληροφοριών κάθε μορφής (προγράμματα, αρχεία, δεδομένα). Πόροι του συστήματος μπορούν να είναι είτε υλικό (hardware), π.χ. υπολογιστές, εκτυπωτές, plotters, σκληροί δίσκοι είτε λογισμικό (software), π.χ. δεδομένα, προγράμματα εφαρμογών, υπηρεσίες.

Τα προγράμματα, τα δεδομένα και οι συσκευές (σκληροί δίσκοι , εκτυπωτές, κλπ) είναι διαθέσιμα σε οποιονδήποτε είναι συνδεδεμένος στο δίκτυο, ανεξάρτητα από τη φυσική του θέση. Με τον τρόπο αυτό επιτυγχάνεται εξοικονόμηση χρημάτων, αύξηση της απόδοσης του συστήματος, κεντρικός έλεγχος και εύκολη επεκτασιμότητα.

Σε ένα δίκτυο μπορούμε να έχουμε ανταλλαγή δεδομένων, προγραμμάτων, χρήση κοινών βάσεων δεδομένων, αρχείων, αποστολή μηνυμάτων (electronic mail). Επιπλέον,

ανεξάρτητα της τεχνολογίας , ένα δίκτυο είναι ένα πανίσχυρο μέσο επικοινωνίας ανθρώπων που βρίσκονται σε διαφορετικά μέρη.

1.1.2ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΩΝ ΔΙΚΤΥΩΝ.

Η αρχιτεκτονική των δικτύων καθορίζει τον τρόπο με τον οποίο οι υπολογιστές και οι λοιπές συσκευές συνδέονται μεταξύ τους για να σχηματίσουν ένα σύστημα επικοινωνίας που θα επιτρέπει στους χρήστες να διαμοιράζονται πληροφορίες και συσκευές του δικτύου. Σε ένα δίκτυο δεδομένων περιλαμβάνονται:
1. Τερματικοί Κόμβοι. Ελέγχουν τους πόρους του δικτύου (λογισμικό και υλικό).
2. Υποδίκτυα. Φυσικά μέσα μετάδοσης, πρωτόκολλα επικοινωνίας, τοπολογία, τερματικοί κόμβοι, πόροι που μπορούν να διαφέρουν πολύ ανά υποδίκτυο.
3. Συσκευές Διασύνδεσης. Διασυνδέουν τα ετερογενή υποδίκτυα έτσι ώστε να εξασφαλίζεται η επικοινωνία τερματικών κόμβων που βρίσκονται σε διαφορετικά υποδίκτυα.

1.1.3 ΕΙΔΗ ΔΙΚΤΥΩΝ.

I. Με βάση την γεωγραφική ανάπτυξη διακρίνονται σε : Δίκτυα ευρείας περιοχής (Wide Area Networks,WAN), που καλύπτουν αποστάσεις μερικών χιλιομέτρων (συνήθως άνω των 5 km) στην ίδια πόλη, μέχρι χιλιάδων χιλιομέτρων σε διαφορετικές πόλεις – κράτη - ηπείρους . Αποτελούνται από υπολογιστές , τηλεπικοινωνιακές συσκευές και γραμμές.
Παραδείγματα τέτοιων δικτύων είναι τα δίκτυα των αεροπορικών εταιρειών, τα τραπεζικά δίκτυα , τα δημόσια δίκτυα δεδομένων κλπ . δίκτυα μικρών αποστάσεων ή τοπικά δίκτυα (Local Area Networks, LAN) που καλύπτουν μικρές αποστάσεις (μερικών εκατοντάδων μέτρων ή λίγων χιλιομέτρων) και περιορίζονται στα πλαίσια μιας επιχείρησης. Ο διαχωρισμός τους από τα δίκτυα ευρείας περιοχής οφείλεται στο ότι χρησιμοποιούν διαφορετικές τεχνικές λειτουργίας.

Πλεονεκτήματα των τοπικών δικτύων.

- Μικρό κόστος ανά χρήστη. Μια ακριβή περιφερειακή συσκευή (π.χ. ένας εκτυπωτής laser) ή προγράμματα εφαρμογών αποτελούν διαμοιραζόμενους πόρους και χρησιμοποιούνται από όλους τους χρήστες.
- Μεγάλη ταχύτητα μεταφοράς πληροφοριών.
- Επεκτασιμότητα.
- Βελτιστοποίηση της χρήσης των μηχανημάτων.
- Υψηλό επίπεδο παρεχομένων υπηρεσιών στους χρήστες του δικτύου.
- Συμβατότητα με συσκευές κατασκευασμένες με συγκεκριμένα πρότυπα.

Αστικά Δίκτυα (Metropolitan Area Networks, MAN), που καλύπτουν δίκτυα που δεν ξεπερνούν τα σύνορα μιας πόλης . Είναι ταχύτερα από τα τοπικά δίκτυα και μπορούν να μεταδίδουν εικόνα, φωνή και δεδομένα αποδοτικότερα.

II. Με βάση τον τηλεπικοινωνιακό φορέα εξυπηρέτησης διακρίνονται σε: Ιδιωτικά δίκτυα (Private Networks). Ανήκουν εξολοκλήρου σε ιδιωτικούς οργανισμούς και χρησιμοποιούν είτε αποκλειστικές γραμμές επικοινωνίας δημοσίων τηλεπικοινωνιακών φορέων (leased lines) χωρίς να τις μοιράζονται με άλλους χρήστες ή ιδιόκτητες γραμμές επικοινωνίας. Δημόσια δίκτυα (Public Networks) που εξυπηρετούν τις διασυνδέσεις μεταξύ απομακρυσμένων σημείων. Χρησιμοποιούνται όταν η απόσταση είναι μεγάλη και καθίσταται απαγορευτική , λόγω κόστους , η χρήση αποκλειστικών γραμμών ή όταν ο φόρτος μεταξύ των σημείων δεν είναι μεγάλος και επιτυγχάνεται έτσι μεγάλη ταχύτητα μεταφοράς.

III . Με βάση την τεχνική προώθησης της πληροφορίας διακρίνονται σε: Δίκτυα μεταγωγής και Δίκτυα Ακρόασης.

1.2 ΤΙ ΕΙΝΑΙ ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΟΥ.

Με τον όρο **«Διαχείριση Δικτύου»** εννοούμε η διαδικασία του αυτόματου (ή όσο το δυνατόν αυτοματοποιημένου) ελέγχου ενός οποιουδήποτε δικτύου υπολογιστών ώστε το κόστος συντήρησης του να είναι κατά το δυνατόν μικρότερο και η απόδοση του η καλύτερη δυνατή. Γενικά, οι βασικοί σκοποί της διαχείρισης του δικτύου είναι οι εξής:

- Η διατήρηση της ικανοποιητικής και αξιόπιστης λειτουργίας ακόμη και κάτω από συνθήκες υπερφόρτωσης ή βλάβης, καθώς επίσης και κάτω από αλλαγές της διαμόρφωσης του δικτύου (εισαγωγή νέων συσκευών ή υπηρεσιών).
- Η βελτίωση της απόδοσης του δικτύου, η οποία σχετίζεται με την ποιότητα και την ποσότητα των υπηρεσιών που παρέχονται στους χρήστες.

1.2.1ΤΙ ΧΡΕΙΑΖΕΤΑΙ ΕΝΑ ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΟΥ.

- Network Management Console:– Ο σταθμός εργασίας όπου παρακολουθεί ο διαχειριστής την κατάσταση του δικτύου.
- Network Management Protocol:– Το πρωτόκολλο με το οποίο θα επικοινωνεί με τις δικτυακές συσκευές.
- Network Management Agent:– Το software που εγκαθίσταται στην δικτυακή συσκευή για χρήση του πρωτοκόλλου διαχείρισης.
- Δικτυακές συσκευές ή και που να τρέχουν agents: – router, switches, hubs, servers, applications.

1.3 ΠΡΟΤΥΠΑ ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΣΥΣΤΗΜΑΤΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΩΝ.

Η αρχιτεκτονική που προτείνεται και χρησιμοποιείται σήμερα για την διαχείριση τηλεπικοινωνιακών δικτύων και δικτύων υπολογιστών αποτελείται από το Σύστημα Διαχείρισης των Δικτύων (Network Management System,NMS) ή το Σύστημα Λειτουργίας (Operation Systems , OS) και τα Στοιχεία εκείνα των δικτύων (Network Elements ,NE) τα οποία θέλουμε να διαχειριστούμε. Τέτοια NE΄s σε ένα δίκτυο είναι κυρίως μηχανήματα αποθήκευσης ή επεξεργασίας πληροφοριών , όπως hosts (workstation,terminal servers κ.α.),καθώς και μηχανήματα διασύνδεσης δικτύων, όπως routers, bridges, repeaters κ.α. στα οποία τρέχουν διαδικασίες διαχείρισης που ονομάζονται (agents) και είναι υπεύθυνες για την εκτέλεση των συναρτήσεων που καλούν τα συστήματα διαχείρισης. Για την μεταφορά της πληροφορίας μεταξύ των διαχειριστικών συστημάτων και των διαχειριζόμενων στοιχείων χρησιμοποιούνται κατάλληλα πρωτόκολλα μεταφοράς της πληροφορίας που αφορά την διαχείριση. Τα πρωτόκολλα αυτά καθορίζουν με σαφήνεια τον τρόπο επικοινωνίας, τη μορφή και την σημασία των μηνυμάτων που θα ανταλλαχθούν, όπως επίσης και τον τρόπο ορισμού και περιγραφής των στοιχείων που θέλουμε να διαχειριστούμε . Ένα από τα γνωστότερα πρωτόκολλα αυτά είναι το SNMP (Simple Network Management Protocol) , το οποίο συμπληρώνεται με τις προδιαγραφές για την δομή της πληροφορίας που αφορά τη διαχείριση (Structure of Management Information, SMI) και τη βάση πληροφορίας διαχείρισης (Management Information Base ,MIB) , προϊόντα του Internet Architecture Board (IAB) ,

της επιτροπής που εγκρίνει πρότυπα Request For Comments (RFCs) για την ομάδα πρωτοκόλλων TCP/IP –ορίζει ένα απλό και λειτουργικό τρόπο διαχείρισης δικτύων TCP/IP.

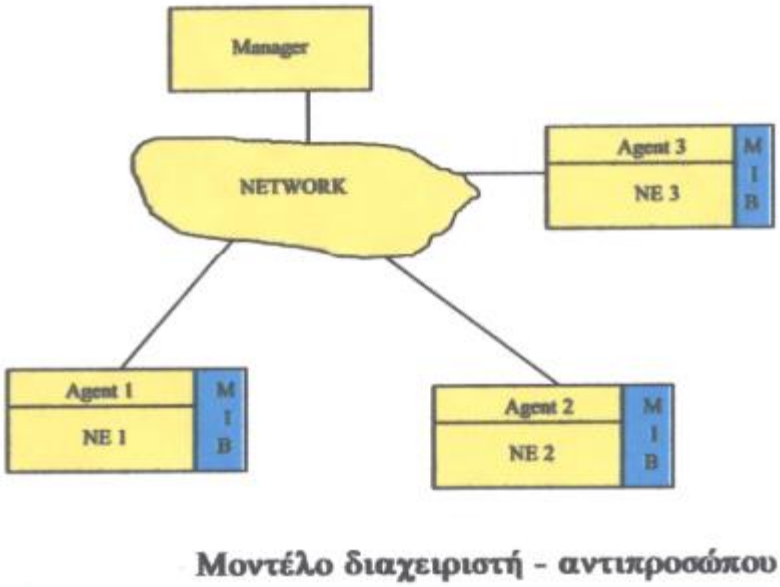
1.3.1 ΓΕΝΙΚΟ ΜΟΝΤΕΛΟ ΚΑΙ ΕΝΝΟΙΕΣ ΠΟΥ ΣΧΕΤΙΖΟΝΤΑΙ ΜΕ ΤΑ ΠΡΩΤΟΚΟΛΛΑ ΚΑΙ ΤΙΣ ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ.

Τα συστήματα διαχείρισης ενός δικτύου αντιγράφουν την γνωστή λογική του συστήματος **πελάτη–εξυπηρετητή**. Μόνο που στην περίπτωση ενός συστήματος διαχείρισης ο πελάτης ονομάζεται **διαχειριστής** και ο εξυπηρετητής ονομάζεται **αντιπρόσωπος.** Γενικότερα ένα σύστημα διαχείρισης αποτελείται από:

Το **διαχειριστή (manager)** που είναι ένα **πρόγραμμα (λογισμικό)** που εκτελείται σε κάποιο μηχάνημα του δικτύου και το οποίο χρησιμοποιεί ο υπεύθυνος συντήρησης του δικτύου (network administrator) για να στείλει εντολές διαχείρισης. Οι εντολές διαχείρισης μπορούν για παράδειγμα να αλλάζουν ρυθμίσεις σε μια δικτυακή συσκευή (χωρίς να χρειάζεται να μετακινηθούμε στο σημείο που βρίσκεται η συσκευή αυτή) ή ακόμα και να ελέγχει την κατάσταση λειτουργίας ενός τμήματος του δικτύου από μακριά.

Τα **διαχειριζόμενα στοιχεία δικτύου (Network Elements - NE)** τα οποία είναι δικτυακές συσκευές που συναντάμε σε ένα τοπικό δίκτυο όπως γέφυρες, δρομολογητές, modems, επαναλήπτες κλπ. Πολλές από αυτές τις συσκευές έχουν δυνατότητα απομακρυσμένης διαχείρισης. Για παράδειγμα ένας δρομολογητής μπορεί να μας επιτρέπει να αλλάζουμε τις ρυθμίσεις του (π.χ. πίνακας δρομολόγησης)
από κάποιο μηχάνημα του δικτύου χρησιμοποιώντας ιστοσελίδες.

Τους **αντιπροσώπους (Agents)** που είναι επίσης **προγράμματα (λογισμικό)** το οποίο βρίσκεται εγκατεστημένο σε κάθε **διαχειριζόμενο στοιχείο δικτύου** με σκοπό να καταστήσει δυνατή την επικοινωνία του με τον **διαχειριστή.** Η διαχείριση γίνεται με τον εξής τρόπο: Ο διαχειριστής (manager) στέλνει τις κατάλληλες εντολές διαχείρισης και ελέγχου μέσω του πρωτοκόλλου διαχείρισης δικτύου. Οι εντολές αυτές λαμβάνονται από τους agents στους οποίους απευθύνονται. Οι αντιπρόσωποι εκτελούν τις εντολές αυτές στα διαχειριζόμενα στοιχεία δικτύου (NE) που ελέγχουν.



Εικόνα 1.1 : Μοντέλο διαχειριστή - αντιπροσώπου

Την Διαχείριση με **Πληρεξούσιους Αντιπροσώπους (Proxy Agents)**. Ωστόσο εδώ πρέπει να σημειώσουμε ότι δεν μπορούμε να εκτελέσουμε προγράμματα agents σε όλες τις δικτυακές συσκευές. Εφ' όσον ο αντιπρόσωπος είναι ένα πρόγραμμα για να εκτελεστεί χρειάζεται η αντίστοιχη συσκευή που απευθύνεται να έχει δυνατότητες επεξεργασίας (επεξεργαστή, μνήμη...). Υπάρχουν δικτυακές συσκευές που έχουν τέτοιες δυνατότητες και άρα μπορούν να εκτελέσουν πρόγραμμα agent. Για παράδειγμα όπως έχουμε εξηγήσει, οι δρομολογητές είναι στην πραγματικότητα υπολογιστές, άρα έχουν δυνατότητα εκτέλεσης προγραμμάτων διαχείρισης. Υπάρχουν όμως συσκευές όπως τα hubs, οι γέφυρες και τα modems που δεν έχουν ικανότητα επεξεργασίας και άρα δεν μπορούν να εκτελέσουν πρόγραμμα agent. Για να διαχειριστούμε στοιχεία δικτύου στα οποία δεν μπορούμε να εκτελέσουμε agents, χρησιμοποιούμε τους λεγόμενους **πληρεξούσιους αντιπροσώπους (proxy agents).** Ένας πληρεξούσιος αντιπρόσωπος δέχεται τις εντολές από ένα διαχειριστή χρησιμοποιώντας το πρωτόκολλο διαχείρισης που είναι κατανοητό από αυτόν, αναλαμβάνει όμως να επικοινωνήσει με τη διαχειριζόμενη συσκευή και να εκτελέσει τις κατάλληλες εντολές διαχείρισης χρησιμοποιώντας το απλούστερο ενδεχομένως πρωτόκολλο που χρησιμοποιεί η συσκευή αυτή.

Την **βάση πληροφοριών διαχείρισης (Management Information Base - MIB)** η οποία είναι μια βάση δεδομένων που μοιράζονται μεταξύ τους οι διαχειριστές και αντιπρόσωποι και η οποία περιέχει πληροφορίες σχετικά με τα διαχειριζόμενα στοιχεία δικτύου (NE). Η βάση πληροφοριών διαχείρισης περιέχει επίσης πληροφορίες που καθορίζουν και την δομή του περιεχομένου της διαχειριζόμενης πληροφορίας (Πρόκειται για μια κανονική βάση δεδομένων: Περιέχει και πίνακες που περιγράφουν την δομή των πινάκων που περιέχουν τις πληροφορίες της βάσης). Σχεδιαστικά η MIB απεικονίζεται με μορφή δέντρου ενώ τα περιεχόμενα της παριστάνονται από τα φύλλα του δέντρου.

Τα **Πρωτόκολλα Διαχείρισης Δικτύου (Network Management Protocols - NMP)** με την βοήθεια των οποίων γίνεται η διαχείριση των NE καθώς και η επικοινωνία μεταξύ του **διαχειριστή** και των **agents.** Το πρωτόκολλο που χρησιμοποιείται ευρύτατα για τη διαχείριση σε TCP/IP δίκτυα είναι το **Simple Network Management Protocol** (**SNMP**) και το οποίο θα αναλύσουμε στο επόμενο κεφάλαιο. Για δίκτυα τα οποία βασίζονται στο μοντέλο OSI έχει αναπτυχθεί το πρωτόκολλο διαχείρισης πληροφορίας (**CMIP**). Πιο εξελιγμένες εκδόσεις του SNMP αποτελούν η **SNMPv2** και η **SNMPv3**.

.

Εικόνα 1.2 : Παράδειγμα διαχείρισης με συσκευή που μπορεί να εκτελέσει πρόγραμμα agent

Μοντέλο Agent/Manager

Agent: λογισμικό που είναι εγκατεστημένο στην προς διαχείριση συσκευή.

Manager: υπολογιστής ο οποίος έχει πλήρη γνώση του δικτύου και των εγκατεστημένων Agents.

Σε ένα μοντέλο διαχείρισης δικτύου Agent/Manager διακρίνουμε **τρία βασικά** στοιχεία:

- ***Δομή πληροφοριών διαχείρισης***.
- ***Βάση πληροφοριών διαχείρισης***.
- ***Πρωτόκολλο επικοινωνίας μεταξύ manager και agent***

1.4 ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΕΝΟΣ ΣΔΔ.

Λαμβάνοντας υπόψη τις λειτουργίες που ένα διαχειριστικό σύστημα απαιτείται να υποστηρίζει, τα παρακάτω γενικά χαρακτηριστικά - περιορισμοί ενισχύουν την λειτουργικότητα του συστήματος:

Το σύστημα πρέπει να παρέχει ένα γραφικό σύστημα παρουσίασης της τοπολογίας του δικτύου. Είναι προτιμότερο η παρουσίαση να γίνεται με ιεραρχικό τρόπο και να υπάρχουν λογικές συνδέσεις μεταξύ των διαφορετικών επιπέδων της ιεραρχίας. Για παράδειγμα, σε ένα επίπεδο παρουσιάζονται μόνο τα LANs και οι συνδέσεις μεταξύ τους, ενώ σε κατώτερο επίπεδο παρουσιάζονται τα τμήματα (segments) του κάθε LAN, στο επόμενο επίπεδο οι κόμβοι των segments κ.ο.κ. Πρέπει ακόμη το σύστημα να είναι σε θέση να αναγνωρίζει τις συνδέσεις μεταξύ των επιπέδων και το πως αυτές συσχετίζονται με την απόδοση και την λειτουργία ολόκληρου του δικτύου. Η ενοποιημένη εικόνα του διαχειριζόμενου δικτύου διατηρείται από το σύστημα, ενώ ο χρήστης μπορεί να επικεντρώνει την προσοχή του σε ορισμένα επίπεδα της ιεραρχίας. Είναι λειτουργικό, τέλος, να υπάρχει ομογενής αντιμετώπιση των στοιχείων του δικτύου σε επίπεδο διαπροσωπείας χρήστη, έστω και αν εσωτερικά υπάρχει ετερογένεια. Για παράδειγμα, σταθμοί εργασίας που διαχειρίζονται με διαφορετικά πρωτόκολλα πρέπει να παρουσιάζονται με τον ίδιο τρόπο στον χρήστη, και οι μέθοδοι άντλησης πληροφοριών για αυτούς να είναι όσο το δυνατών παρόμοιοι. Οι ανομοιογένειες πρέπει να κρύβονται από τον χρήστη, εκτός βέβαια αν ζητηθούν ή αποτελούν αιτία προβλημάτων.

Το σύστημα πρέπει να είναι ικανό να συλλέγει όλες τις πληροφορίες από τους διαχειριζόμενους κόμβους, με όσο είναι δυνατόν μεγαλύτερη διαφάνεια και ιδανικά μέσω ενός μόνο πρωτοκόλλου διαχείρισης. Βέβαια, σε ετερογενή περιβάλλοντα το σύστημα πρέπει να είναι σε θέση να χρησιμοποιεί διαφορετικά πρωτόκολλα διαχείρισης και/ή proxy agents.

Η επεκτασιμότητα (expandability) και η δυνατότητα προσαρμογής σε διαφορετικές ανάγκες διαχείρισης (customization) είναι δύο ακόμη σημαντικά χαρακτηριστικά - απαιτήσεις. Δεν υπάρχει σύστημα που να καλύπτει τις ανάγκες διαχείρισης κάθε δυνατού δικτύου. έτσι το σύστημα πρέπει να επιτρέπει την εύκολη προσθήκη νέων δυνατοτήτων και εργαλείων διαχείρισης ανάλογα με τις απαιτήσεις της κάθε εφαρμογής.

Μια ακόμη βασική λειτουργία ενός συστήματος διαχείρισης είναι η δυνατότητα ανίχνευσης και αναφοράς λαθών και προβλημάτων στο δίκτυο. Καθώς το διαχειριζόμενο δίκτυο επεκτείνεται, μια τέτοια υπηρεσία γίνεται όλο και περισσότερο πολύτιμο. Έστω και αν η διαχείριση λαθών δεν υποστηρίζεται, η ανίχνευση και η ειδοποίηση είναι απαραίτητα χαρακτηριστικά ενός διαχειριστικού συστήματος.

Το σύστημα πρέπει να παρέχει ένα αποδοτικό τρόπο φύλαξης του όγκου πληροφοριών που χρειάζεται για την διαχείριση, ιδιαίτερα όταν τα διαχειριζόμενα δίκτυα

είναι μεγάλα. Συχνά ένα σύστημα διαχείρισης βάσης δεδομένων (DBMS) είναι απαραίτητο καθώς εφαρμογές που configuration και accounting management είναι αδύνατον να λειτουργήσουν αποδοτικά χωρίς αυτό. Συνήθως χρησιμοποιείται το σχεσιακό μοντέλο (relational data model), ενώ γίνονται προσπάθειες να σχεδιαστούν και να υλοποιηθούν αντικειμενοστραφείς βάσεις δεδομένων (Object Oriented DBMS - OODBMS) ειδικά για χρήση σε συστήματα διαχείρισης δικτύων. Ανάλογα με την αρχιτεκτονική του ΣΔΔ και τις απαιτήσεις απόδοσης μπορεί να χρησιμοποιηθεί κεντροποιημένη (centralized) ή κατανεμημένη (distributed) βάση δεδομένων. Έχουν διατυπωθεί και άλλοι περιορισμοί που αφορούν την αλληλεπίδραση διαχειριζόμενου δικτύου και διαχειριστικού συστήματος :

Μια μινιμαλιστική φιλοσοφία στις επιδράσεις του ΣΔΔ στο διαχειριζόμενο δίκτυο που συνοψίζεται στο εξής : "Το αποτέλεσμα της εγκατάστασης ενός ΣΔΔ σε ένα δίκτυο πρέπει να είναι το ελάχιστο δυνατό, αντανακλώντας τον ελάχιστο κοινό παρανομαστή" . Η ανάγκη ελάχιστης επιρροής στους διαχειριζόμενους κόμβους ενισχύεται από τις μεγάλες διαφορές μεταξύ των κόμβων. Η διαδικασία άντλησης πληροφοριών και παρακολούθησης των κόμβων δεν πρέπει να προκαλεί σημαντικές καθυστερήσεις στην λειτουργία των κόμβων, καθώς κάτι τέτοιο οξύνει τις διαφορές απόδοσης. Τέλος, το φορτίο που εισάγει στο δίκτυο η λειτουργία του ΣΔΔ πρέπει να είναι όσο το δυνατόν μικρότερο, αλλιώς το κέρδος της δυνατότητας διαχείρισης, αντισταθμίζεται από την παρενέργεια της πεσμένης απόδοσης και των προβλημάτων που μπορεί να προκαλέσει η συμφόρηση του δικτύου.

Μια άλλη απαίτηση είναι η βιωσιμότητα του διαχειριστικού συστήματος σε κρίσιμες καταστάσεις. Όταν το διαχειριζόμενο δίκτυο "πέφτει" και γενικά σε καταστάσεις σημαντικών προβλημάτων και λαθών, το ΣΔΔ πρέπει να παραμείνει σε λειτουργία (σε όποιο βαθμό είναι αυτό δυνατό) . Όσο περισσότερο ανεκτικό στα λάθη του διαχειριζόμενου δικτύου είναι το ΣΔΔ, τόσο καλύτερα εκπληρώνει τον ρόλο του σε περιπτώσεις προβλημάτων.

1.5 ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΟΥ

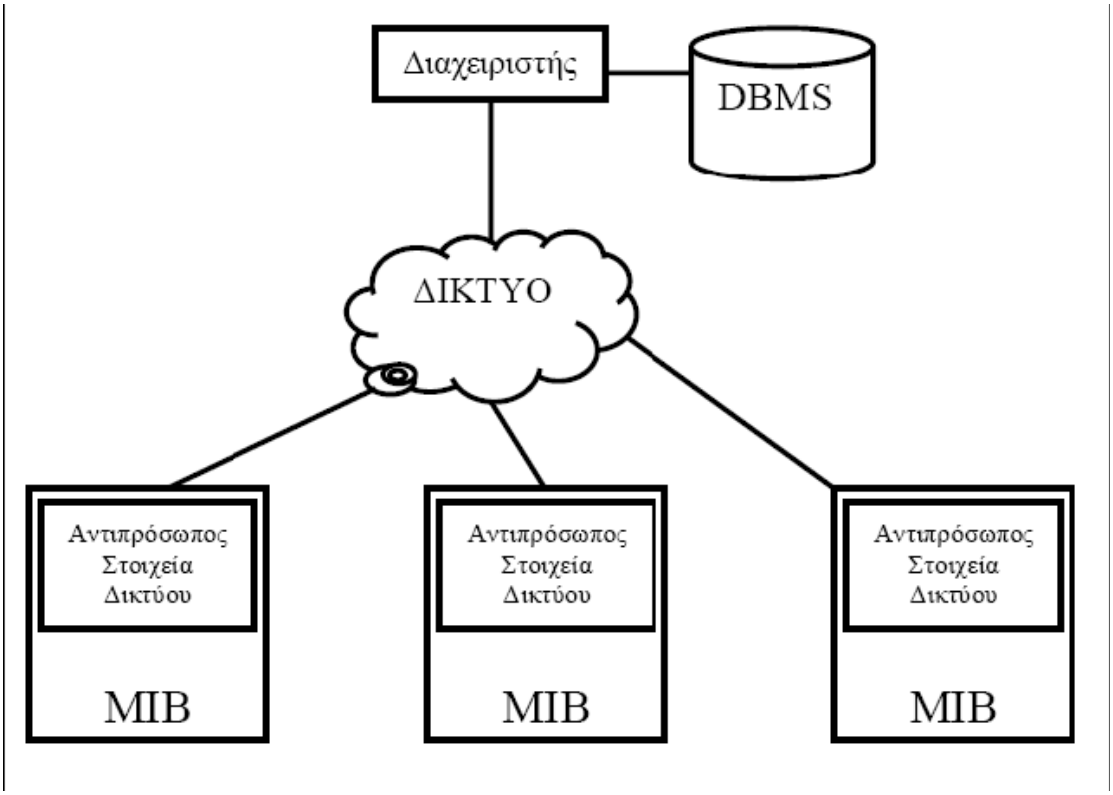
Για να μπορεί μια πλατφόρμα διαχείρισης δικτύου να εκτελεί τις λειτουργίες που περιγράφηκαν προηγουμένως, θα πρέπει να χρησιμοποιεί κάποια αρχιτεκτονική διαχείρισης. Οι αρχιτεκτονικές διαχείρισης του δικτύου που υπάρχουν είναι η **Κεντρική, η Ιεραρχική και η Κατανεμημένη.** Μια παραλλαγή τους που συνδυάζει τα δύο τελευταία είναι το **δικτυωμένο** ΣΔΔ. Οι διαφορές αυτών των αρχιτεκτονικών αναφέρονται κυρίως στον αριθμό διαχειριστών και στον βαθμό επικοινωνίας - ανεξαρτησίας τους. Κάθε μια προσφέρει κάποια πλεονεκτήματα και μειονεκτήματα έναντι των άλλων. Η επιλογή εξαρτάται από της απαιτήσεις διαχείρισης και τον χαρακτήρα του δικτύου που απαιτείται η διαχείριση. Γενική περιγραφή των τεσσάρων αρχιτεκτονικών, των πλεονεκτημάτων και μειονεκτημάτων τους δίνεται παρακάτω.

1.5.1 ΚΕΝΤΡΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ (CENTRALIZED).

Πρόκειται για την πιο απλή και κλασική αρχιτεκτονική διαχείρισης. Η πλατφόρμα διαχείρισης βρίσκεται εγκατεστημένη σε ένα κεντρικό σταθμό εργασίας ο οποίος και αναλαμβάνει όλα τα καθήκοντα διαχείρισης του δικτύου .Η αρχιτεκτονική αυτή είναι συμβατή με το μοντέλο διαχειριστή–agents. Η πλατφόρμα διαχείρισης επιτελεί τις παρακάτω λειτουργίες:

- Αναλαμβάνει την επικοινωνία με όλα τα διαχειριζόμενα στοιχεία μέσω των agents και του πρωτοκόλλου διαχείρισης.

- Διαχειρίζεται την αποθήκευση των πληροφοριών διαχείρισης του δικτύου. Η αποθήκευση μπορεί να γίνεται κεντρικά σε ένα σημείο ή για λόγους ασφαλείας να είναι κατανεμημένη σε πολλά μηχανήματα, αλλά ο έλεγχος όπως και όλος ο σχεδιασμός της αρχιτεκτονικής είναι κεντρικός.
- Παρέχει μια ενιαία εικόνα του διαχειριζόμενου δικτύου στον υπεύθυνο διαχειριστή μέσω κατάλληλου περιβάλλοντος επικοινωνίας με το χρήστη.



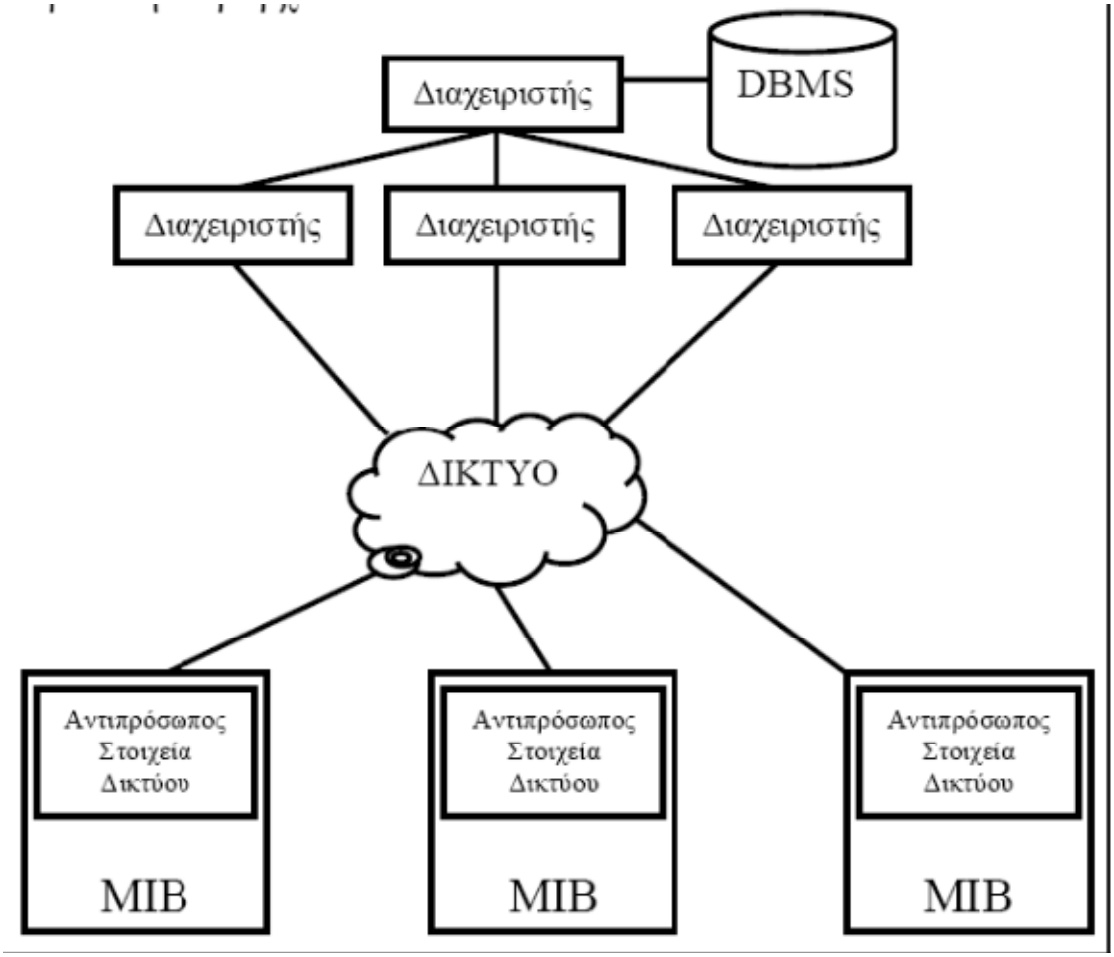
Εικόνα 1.3 : Κεντρική Αρχιτεκτονική Διαχείρισης Δικτύου

Γενικά, για την κεντροποιημένη αρχιτεκτονική ισχύει:
Είναι σύμφωνη με το γνωστό μοντέλο agent-manager. Περιέχει ένα κεντρικό διαχειριστή ο οποίος:

- Επικοινωνεί με όλα τα διαχειριζόμενα στοιχεία του δικτύου.
- Διαχειρίζεται την αποθήκευση των πληροφοριών του συστήματος
- Παρέχει μία ενοποιημένη εικόνα του διαχειριζόμενου δικτύου στο διαχειριστή μέσω
- κατάλληλου περιβάλλοντος επικοινωνίας με το χρήστη.

1.5.2 ΙΕΡΑΡΧΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ (HIERARCHICAL).

Στην αρχιτεκτονική αυτή χρησιμοποιούνται πολλές πλατφόρμες διαχείρισης .Η μία από αυτές λειτουργεί σαν κεντρικός σταθμός εξυπηρέτησης του δικτύου, ενώ οι άλλες σαν πελάτες και οι οποίες δεν έχουν χωριστό **σύστημα διαχείρισης βάσης δεδομένων (DBMS)**, αλλά χρησιμοποιούν το DBMS του κεντρικού σταθμού ενώ ο συντονισμός των λειτουργιών τους γίνεται από το διαχειριστή που βρίσκεται υψηλότερα στην ιεραρχία.



Εικόνα 1.4 : Ιεραρχική Αρχιτεκτονική Διαχείρισης Δικτύου

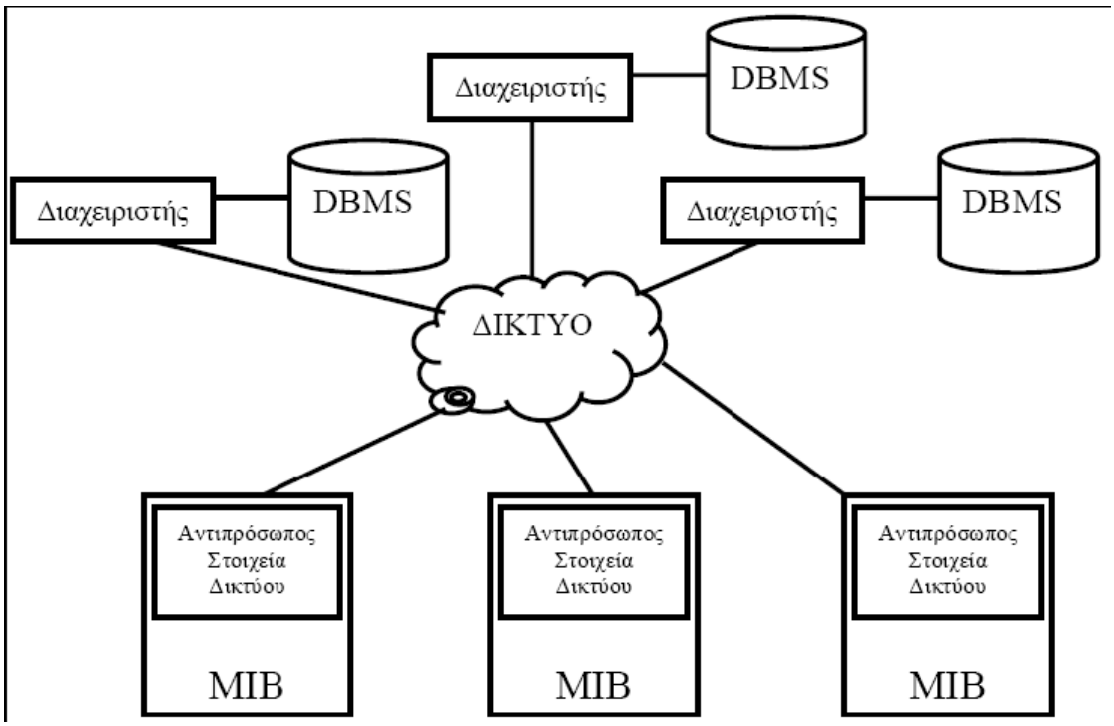
Ορισμένες από τις λειτουργίες στο ιεραρχικό σύστημα διαχείρισης εκτελούνται από τον κεντρικό διαχειριστή, ενώ άλλες ανατίθενται στους επιμέρους διαχειριστές. Γενικά ο κεντρικός διαχειριστής συγκεντρώνει μόνο τις σημαντικές πληροφορίες αφήνοντας τις επιμέρους λεπτομέρειες στους διαχειριστές που βρίσκονται στο χαμηλότερο επίπεδο. Η επικοινωνία μεταξύ του κεντρικού διαχειριστή και των επιμέρους διαχειριστών μπορεί να γίνεται μέσω του ίδιου του δικτύου που διαχειρίζονται είτε και μέσω ανεξάρτητου δικτύου διαχείρισης. Στην δεύτερη αυτή περίπτωση, έχουμε καλύτερη αξιοπιστία αφού ακόμα και σε περίπτωση σοβαρής βλάβης του κανονικού δικτύου, θα έχουμε επικοινωνία των διαχειριστών μεταξύ τους.

Γενικά η ιεραρχική αρχιτεκτονική :

- Προσφέρει καλύτερο έλεγχο και επίδοση στο διαχειριστή του δικτύου
- Προσφέρεται για ετερογενή δίκτυα
- Βρίσκει εφαρμογή και σε δίκτυα που υπάρχει ανάγκη διαίρεσης του διαχειριζόμενου περιβάλλοντος
- Παρέχει: Ολοκληρωμένο διαχειριστικό περιβάλλον, Ενοποιημένη αναπαράσταση ετερογενούς δικτύου, Κοινό περιβάλλον επικοινωνίας με το χρήστη

1.5.3 ΚΑΤΑΝΕΜΗΜΕΝΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ (DISTRIBUTED).

Αυτή η αρχιτεκτονική αποτελεί ουσιαστικά συνδυασμό της κεντρικής και της ιεραρχικής και χρησιμοποιεί πολλές ομότιμες πλατφόρμες διαχείρισης, κάθε μία από τις οποίες αποτελεί ένα κεντρικό σύστημα. Μια πλατφόρμα είναι επικεφαλής μιας σειράς από ομότιμα συστήματα διαχείρισης (όπως στην ιεραρχική αρχιτεκτονική διαχείρισης). Ωστόσο κάθε πλατφόρμα μπορεί να έχει το δικό της σύστημα διαχείρισης βάσης δεδομένων (DBMS) με στοιχεία που να αφορούν οποιοδήποτε σημείο του δικτύου. Επειδή η διαχείριση κατανέμεται σε τοπικούς διαχειριστές έχει γενικά μικρότερες απαιτήσεις σε υλικό και υπολογιστική ισχύ. Ο καθένας από τους τοπικούς διαχειριστές διαχειρίζεται μόνο τον τομέα της αρμοδιότητας του και δεν έχει το βάρος της παρακολούθησης ολόκληρου του δικτύου (αν χρειαστεί πληροφορίες για περιοχή του δικτύου που δεν του ανήκει μπορεί να τις ζητήσει από τον αντίστοιχο ομότιμο διαχειριστή).



Εικόνα 1.5 : Κατανεμημένη Αρχιτεκτονική Διαχείρισης Δικτύου

Γενικά , η κατανεμημένη αρχιτεκτονική

- Συνδυάζει την κεντροποιημένη με την ιεραρχική
- Έχει μία κεντρική πλατφόρμα διαχείρισης ή μια ιεραρχία από πλατφόρμες εξυπηρετητή πελάτη
- Χρησιμοποιεί ομότιμες πλατφόρμες διαχείρισης που καθεμιά τους χωριστά αποτελεί ένα κεντροποιημένο σύστημα.

Από τις τρείς αρχιτεκτονικές που προαναφέρθηκαν η πιο συχνά χρησιμοποιούμενη παρατηρείται να είναι η **κατανεμημένη διαχείριση δικτύου.**

Ένα κεντρικό σύστημα διαχείρισης δικτύου είναι το παραδοσιακό σύστημα διαχείρισης το οποίο προτιμάται ιδιαίτερα από κατασκευαστές συστημάτων mainframe. Ένα τέτοιο σύστημα υπονοεί κεντρικό έλεγχο, όπου οι σημαντικοί πόροι βρίσκονται στο κεντρικό

σύστημα και οι υπηρεσίες παρέχονται στους απομεμακρυσμένους χρήστες. Το σύστημα αυτό δίνει τη δυνατότητα στο διαχειριστή να έχει πλήρη έλεγχο, να εξισορροπεί τους πόρους σε σχέση με τις ανάγκες και να βελτιστοποιεί τη χρήση των πόρων.

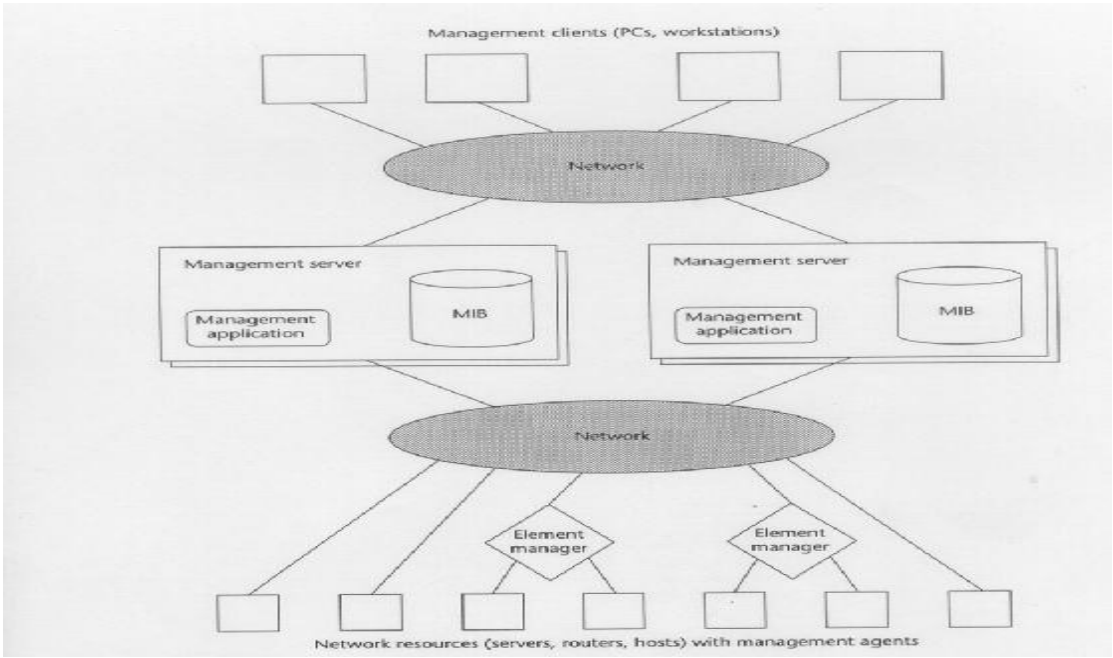
Για τα κλασικά συστήματα διαχείρισης δικτύου ένας κεντρικός υπολογιστής έχει το ρόλο του σταθμού διαχείρισης του δικτύου, όμως μπορούν πιθανόν να υπάρχουν ένας ή δύο ακόμη εφεδρικοί σταθμοί (back-up). Τα υπόλοιπα από τα στοιχεία του δικτύου όπως έχουμε δει περιέχουν το λογισμικό του πράκτορα και μία βάση πληροφοριών διαχείρισης για να παρακολουθούνται και να ελέγχονται από το σταθμό διαχείρισης. Όταν το δίκτυο είναι μεγάλο σε μέγεθος και έχει μεγάλη κίνηση φορτίου τότε το κεντρικό σύστημα διαχείρισης δεν μπορεί να λειτουργήσει ικανοποιητικά. Στη περίπτωση αυτή μία κατανεμημένη κατανομή μπορεί να λειτουργήσει καλύτερα.

Η κατανεμημένη διαχείριση τοποθετεί τη διαχείριση σε ιεραρχικά επίπεδα ανάλογα με το είδος των συσκευών, το είδος του δικτύου, τη γεωγραφία του κλπ. Για τον περιορισμό της αναρχίας:

- Τα κέντρα κατανεμημένης διαχείρισης έχουν περιορισμένη πρόσβαση στον έλεγχο και την παρακολούθηση του δικτύου, συνήθως περιορίζονται στους πόρους που διαθέτουν
- Ένας κεντρικός σταθμός διαχείρισης και ένας εφεδρικός έχει καθολικά δικαιώματα πρόσβασης και τη δυνατότητα διαχείρισης όλων των πόρων του δικτύου. Μπορεί επίσης να συναλλάσσεται με άλλα κέντρα διαχείρισης λιγότερο ενεργά και να παρακολουθεί και να ελέγχει τη λειτουργία τους.

Ενώ η κατανεμημένη διαχείριση δίνει τη δυνατότητα κεντρικού ελέγχου παρέχει επίσης τα ακόλουθα πλεονεκτήματα:

- Ελαχιστοποιείται η επιβάρυνση από την κυκλοφορία διαχείρισης του δικτύου. Η κυκλοφορία γίνεται τοπικά.
- Η κατανεμημένη διαχείριση προσφέρει μεγαλύτερη ευελιξία σε περίπτωση επέκτασης του δικτύου.
- Η χρήση πολλαπλών σταθμών ελαχιστοποιεί την περίπτωση βλάβης σε όλο το δίκτυο.



Εικόνα 1.6 : Η βασική δομή που χρησιμοποιείται από τα περισσότερα κατανεμημένα συστήματα διαχείρισης της αγοράς.

Πιο κοντά στο χρήστη βρίσκονται σταθμοί διαχείρισης. Αυτοί δίνουν στο χρήστη το δικαίωμα πρόσβασης σε υπηρεσίες διαχείρισης και παρέχουν πληροφορίες χρησιμοποιώντας ένα γραφικό περιβάλλον. Ανάλογα με τα δικαιώματα πρόσβασης ένας σταθμός διαχείρισης μπορεί να έχει πρόσβαση σε έναν ή περισσότερους εξυπηρετητές διαχείρισης. Ο εξυπηρετητής διαχείρισης είναι η καρδιά του συστήματος. Κάθε εξυπηρετητής υποστηρίζει μια ομάδα από εφαρμογές διαχείρισης και μια Βάση Πληροφοριών Διαχείρισης (MIB). Επίσης έχουν αποθηκευμένα κοινά μοντέλα διαχείρισης δεδομένων και παρέχουν πληροφορίες σε εφαρμογές και σε πόρους του δικτύου. Οι πόροι αυτοί του δικτύου που υποστηρίζουν το ίδιο πρωτόκολλο διαχείρισης δικτύου με τους εξυπηρετητές περιέχουν λογισμικό πράκτορα και διαχειρίζονται από έναν ή περισσότερους εξυπηρετητές διαχείρισης. Το πλεονέκτημα του κατανεμημένου συστήματος είναι φανερό – η προσθήκη νέων πόρων στο δίκτυο γίνεται με τρομερή ευκολία.

1.6 ΜΟΝΤΕΛΟ ΛΕΙΤΟΥΡΓΙΑΣ.

Το Μοντέλο Λειτουργίας διαιρεί όλο το πλέγμα της διαχείρισης σε πέντε λειτουργικές περιοχές **à FCAPS**. Οι απαιτήσεις που ορίζονται κατά **ISO** είναι:

- Διαχείριση βλαβών (Fault Management)
- Διαχείριση διάρθρωσης (Configuration Management)
- Διαχείριση κοστολόγησης (Accounting Management)
- Διαχείριση απόδοσης (Performance Management)
- Διαχείριση ασφάλειας (Security Management)

1.7 ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΟΥ- NETWORK MANAGEMENT.

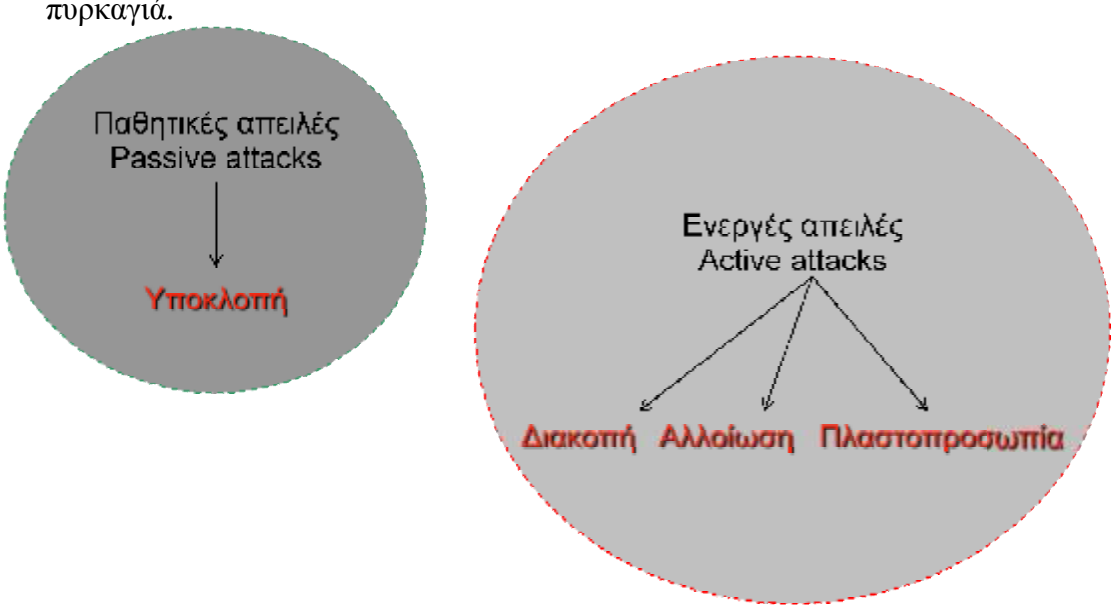
Ο οργανισμός International Organization for Standardization – ISO, έχει προτείνει ένα μοντέλο διαχείρισης δικτύου (network management model) για την κατανόηση των βασικών λειτουργιών των συστημάτων διαχείρισης δικτύου (network management systems). Το μοντέλο αυτό περιλαμβάνει πέντε κύριες δραστηριότητες:

I. Διαχείριση βλαβών (fault management). Τα μέσα διαχείρισης βλαβών έχουν σκοπό να ανιχνεύσουν και να διορθώσουν τυχόν σφάλματα με στόχο την επαναφορά του δικτύου στη σωστή λειτουργία. Συγκεκριμένα, με τη χρήση ορισμένων μεθόδων ανιχνεύεται το λάθος και προτείνονται τρόποι αντιμετώπισης. Επίσης ξεχωρίζονται τα αίτια του λάθους (root cause) από τις επιπλοκές αυτού (side effect) που είναι πιθανόν να παρουσιάσουν και τέλος προσφέρουν προειδοποιήσεις (alarms) σε περιπτώσεις συμβάντων που θεωρούνται μη φυσιολογικά ή ακόμα και σε μεταβολή χαρακτηριστικών έξω από συγκεκριμένα όρια.

II. Διαχείριση διάρθρωσης (configuration management). Η λειτουργία αυτή περιλαμβάνει την επισκόπηση και τη διαχείριση των πόρων του συστήματος, την παρακολούθηση εγκατάστασης και τοποθέτησης νέων χρηστών και την πρόληψη υπερφόρτωσης δικτύου χρησιμοποιώντας τεχνικές εναλλακτικής δρομολόγησης ή απορρίπτοντας μέρος της δημιουργημένης κυκλοφορίας. Πρόκειται για μια σημαντική λειτουργία αφού δεν θα είχε νόημα η διαχείριση δικτύου αν δεν μπορούσαμε να διαχειριστούμε τις συσκευές αυτού. Καθώς τα δίκτυα επεκτείνονται σε διαστάσεις, χρειαζόμαστε τρόπους να συλλέγουμε πληροφορίες για διάφορες συσκευές και να καθορίζουμε τις παραμέτρους τους χωρίς να χρειάζεται να βρισκόμαστε κοντά τους.

III. Διαχείριση ασφάλειας (security management). Με τη διάδοση των κατανεμημένων συστημάτων (distributed systems) οι πληροφορίες είναι κατανεμημένες σε διάφορα

σημεία και αυξάνεται η ανάγκη για ασφάλεια. Θα πρέπει να εξασφαλίζονται η εμπιστευτικότητα (confidentiality), η μη μεταβολή δεδομένων (data integrity), και η πιστοποίηση ταυτότητας (authentication). Το σύστημα επίσης θα πρέπει να εξασφαλίζει την ασφάλεια τόσο σε λειτουργικό επίπεδο (έλεγχος πρόσβασης μέσα στο δίκτυο) όσο και σε φυσικό, εννοώντας κινδύνους από καταστροφές όπως πυρκαγιά.



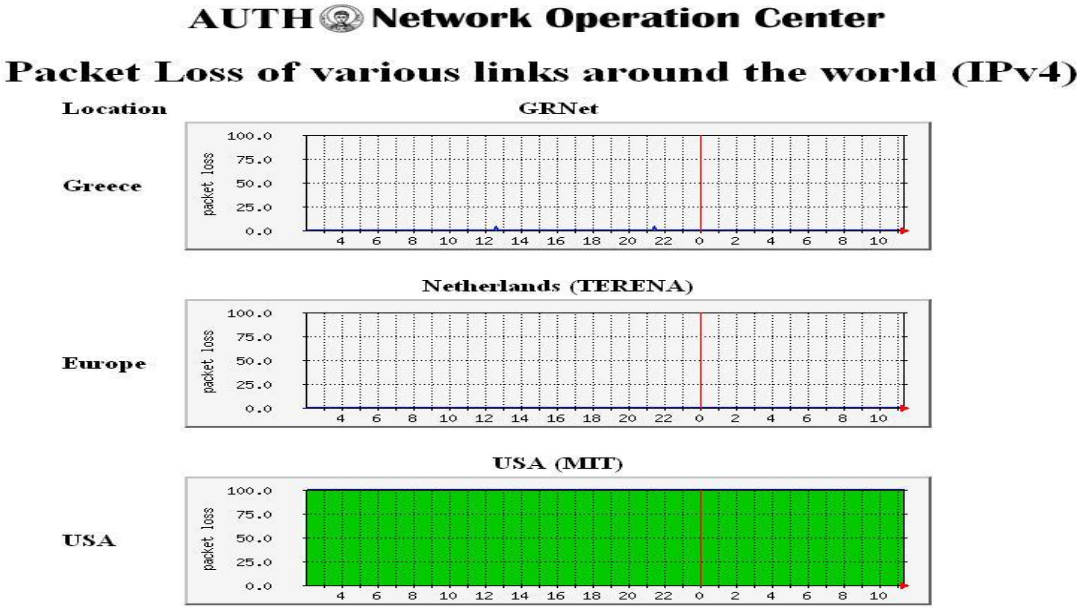
Εικόνα 1.7: Ενεργές και παθητικές απειλές

- Οι παθητικές απειλές αφορούν στην παρακολούθηση των μεταδόσεων με στόχο την υποκλοπή πληροφοριών. Διακρίνονται: στην αποκάλυψη του περιεχομένου διαχειριστικών μηνυμάτων: αντιμετωπίζεται με υπηρεσίες διασφάλισης της εμπιστευτικότητας των μηνυμάτων στην ανάλυση της κυκλοφορίας του δικτύου, μηχανισμός ασφάλειας = κρυπτογράφηση (εμπιστευτικότητα) ωστόσο, ακόμη και αν ο εισβολέας δεν αποκτήσει πρόσβαση στο περιεχόμενο μπορεί να εξάγει πολύτιμες πληροφορίες όπως η θέση και η ταυτότητα των συστημάτων αποστολής και λήψης, η συχνότητα και το μήκος των αποστελλόμενων μηνυμάτων. Είναι δύσκολο να ανακαλυφθούν καθώς δεν περιλαμβάνουν τροποποίηση δεδομένων **à** έμφαση στην πρόληψη και όχι στον εντοπισμό
- Οι ενεργές απειλές περιλαμβάνουν τροποποίηση της ροής δεδομένων ή δημιουργία λανθασμένης ροής δεδομένων. Διακρίνονται: στην άρνηση υπηρεσίας μηνυμάτων: η χρήση ή διαχείριση των υπηρεσιών επικοινωνίας εμποδίζεται ή ανακόπτεται η λειτουργία του δικτύου είτε λόγω απενεργοποίησης είτε λόγω υπερφόρτωσής του με μηνύματα και κίνηση που οδηγούν σε αισθητή μείωση της απόδοσής του, τροποποίηση της ροής δεδομένων: τμήματα μηνυμάτων τροποποιούνται ή μηνύματα καθυστερούν ή επαναμεταδίδονται ώστε να προκαλέσουν μη αναμενόμενο αποτέλεσμα **à** αντιμετωπίζεται με την υπηρεσία διασφάλισης της ακεραιότητας των μηνυμάτων, υπηρεσίες χρονοσήμανσης πλάνης: μια οντότητα προσποιείται ότι είναι κάποια άλλη σύλληψη και γίνεται αναμετάδοση μιας σειράς αποδείξεων γνησιότητας ή επικύρωσης
- Στόχος είναι ο εντοπισμός τους και η επαναφορά του συστήματος σε κανονική λειτουργία **à** δύσκολη η πρόληψη

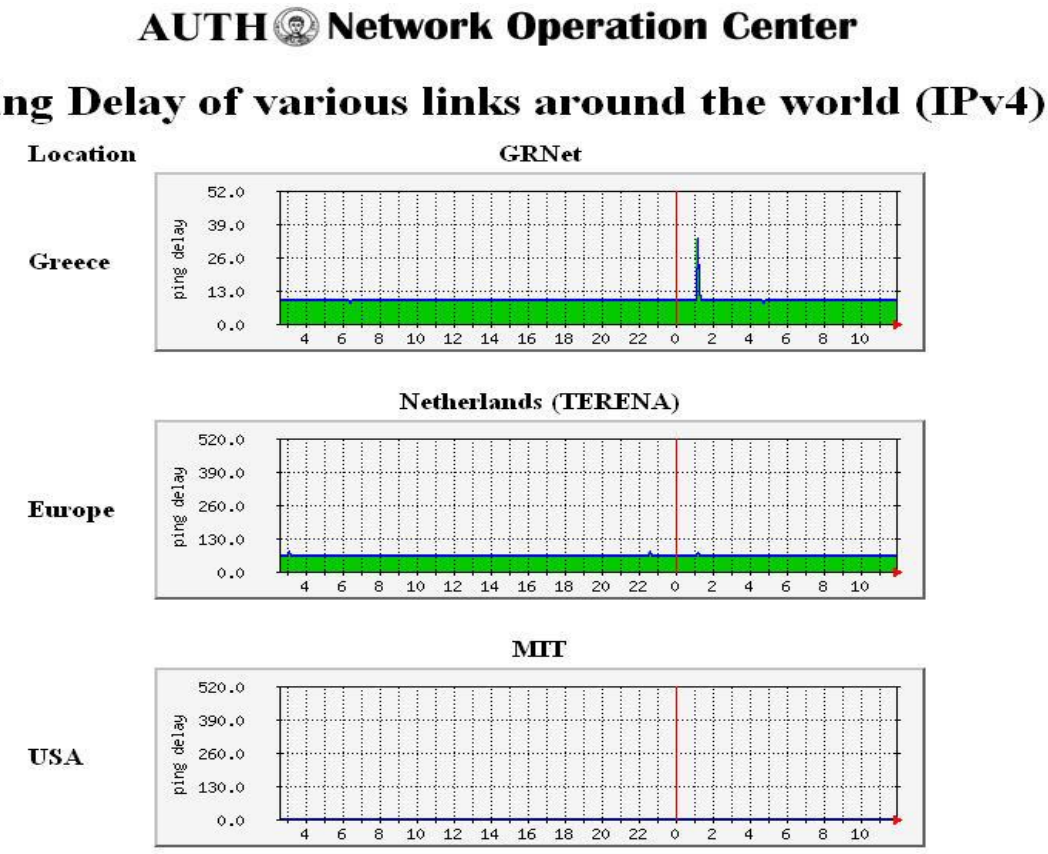
Εκτός των απειλών που προαναφέρθηκαν, ως απειλές κατά του συστήματος διαχείρισης μπορούν να θεωρηθούν οι ακόλουθες:

- ενεργοποίηση εφαρμογής απομίμησης της εφαρμογής διαχείρισης **à** αντιμετωπίζεται με την αποτελεσματική αυθεντικοποίηση οντοτήτων και με την πιστοποίηση της προέλευσης δεδομένων
- τροποποίηση υπαρχόντων ή δημιουργία νέων διαχειριστικών δεδομένων που αποθηκεύονται στη βάση δεδομένων διαχείρισης **à** αντιμετωπίζεται με υπηρεσίες ελέγχου προσπέλασης και ακεραιότητας δεδομένων
- Αποποίηση αιτήσεων διαχείρισης στον προορισμό **à** αντιμετωπίζεται με ενεργοποίηση υπηρεσιών μη αποποίησης παράδοσης μηνύματος

IV. Διαχείριση απόδοσης (performance management).



Εικόνα 1.8 : Παρακολούθηση απόδοσης δικτύων ανά τον κόσμο



Εικόνα 1.9 : Χρόνος απόκρισης κόμβων ανά τον κόσμο

Η λειτουργία αυτή περιλαμβάνει την παρακολούθηση της επίδοσης του δικτύου, δηλαδή το μέγεθος της συμφόρησης στα διάφορα στοιχεία αυτού και τη συλλογή στατιστικών στοιχείων για τα διάφορα κομμάτια του με σκοπό να χρησιμοποιηθούν στη διαχείριση διαμόρφωσης.

V. Διαχείριση Κοστολόγησης (accounting management).

Η κίνηση μετράται σε MBytes

DOMAIN	TOTALS	NATIONAL	INTERNATIONAL
ad	1.177.906,69 - 3,50% 2.721.323,17 - 4,35%	343.264,42 - 29,14% 1.082.393,70 - 39,77%	834.642,27 - 70,86% 1.638.927,30 - 60,23%
adispo.gr	0,00 - 0,00% 0,00 - 0,00%	0,00 - 0,00% 0,00 - 0,00%	0,00 - 100,00% 0,00 - 0,00%
agro	804.325,03 - 2,39% 1.125.098,14 - 1,80%	203.281,63 - 25,27% 436.829,83 - 38,83%	601.043,40 - 74,73% 688.267,84 - 61,17%
ahepahosp.gr	730.381,91 - 2,17% 52.014,76 - 0,08%	140.829,47 - 19,28% 23.065,96 - 44,35%	589.552,43 - 80,72% 28.948,80 - 55,65%
arch	602.889,92 - 1,79% 351.065,47 - 0,56%	243.508,74 - 40,39% 113.511,73 - 32,33%	359.381,17 - 59,61% 237.552,08 - 67,67%
arts	27.405,49 - 0,08% 1.024,26 - 0,00%	441,96 - 1,61% 18,12 - 1,77%	26.963,53 - 98,39% 1.006,14 - 98,23%
astro	75.089,40 - 0,22% 125.508,16 - 0,20%	7.579,73 - 10,09% 36.894,69 - 29,40%	67.509,66 - 89,91% 88.613,43 - 70,60%
bio	545.467,02 - 1,62% 1.116.707,66 - 1,79%	116.977,62 - 21,45% 68.174,46 - 6,10%	428.489,40 - 78,55% 1.048.531,68 - 93,89%
ccf	963.024,09 - 2,86% 2.442.323,11 - 3,91%	583.683,52 - 60,61% 1.876.890,43 - 76,85%	379.340,57 - 39,39% 564.091,80 - 23,10%

POP	SMTP	SNMP	SSH	TELNET	VARIOUS
150,26 - 0,01% 104,45 - 0,00%	520,35 - 0,04% 1.135,87 - 0,04%	0,01 - 0,00% 0,09 - 0,00%	6,34 - 0,00% 9,72 - 0,00%	0,33 - 0,00% 0,05 - 0,00%	485,53 - 0,04% 464,68 - 0,02%
0,00 - 0,00% 0,00 - 0,00%	0,00 - 0,00% 0,00 - 0,00%	0,00 - 0,00% 0,00 - 0,00%	0,00 - 0,00% 0,00 - 0,00%	0,00 - 0,00% 0,00 - 0,00%	0,00 - 100,00% 0,00 - 0,00%
851,47 - 0,11% 27,43 - 0,00%	7,22 - 0,00% 215,30 - 0,02%	0,05 - 0,00% 4,67 - 0,00%	1,10 - 0,00% 0,03 - 0,00%	0,32 - 0,00% 0,02 - 0,00%	258,90 - 0,03% 149,65 - 0,01%
559,12 - 0,08% 20,73 - 0,04%	0,59 - 0,00% 10,37 - 0,02%	0,00 - 0,00% 0,00 - 0,00%	1,10 - 0,00% 0,89 - 0,00%	0,01 - 0,00% 0,00 - 0,00%	4,25 - 0,00% 2,59 - 0,00%
327,75 - 0,05%	848,46 - 0,14%	0,00 - 0,00%	0,75 - 0,00%	0,18 - 0,00%	108,81 - 0,02%

Εικόνα 1.10 : Ποσοστό κίνησης δεδομένων

Το τελευταίο αυτό χαρακτηριστικό επιβάλλει την παρακολούθηση της χρήσης των πόρων του συστήματος, κοστολογώντας τους χρήστες για αυτήν. Συγκεκριμένα σκοπό έχει τη συλλογή, αποθήκευση, επεξεργασία και τον έλεγχο των πληροφοριών διαχείρισης των πόρων και της χρέωσης. Επίσης τα στοιχεία μπορούν να βοηθήσουν στον έλεγχο για την ασφάλεια του δικτύου, μια και κρατούνται στοιχεία για τις ενέργειες ενός χρήστη (log files).

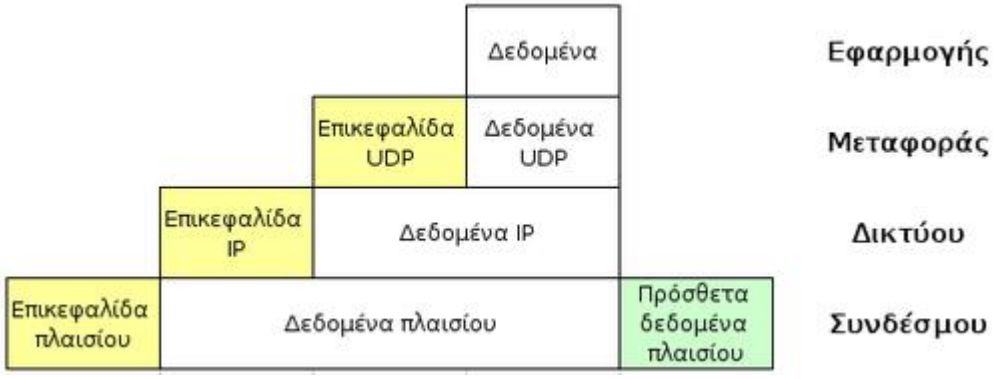
1.8 TCI/IP ΚΑΙ OSI ΠΡΟΣΕΓΓΙΣΕΙΣ

Το **"TCP/IP"** ***(***Transmission Control Program/Internet Protocol=Πρωτόκολλο Ελέγχου Μετάδοσης και πρωτόκολλο του Internet***)*** είναι μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων. Η ονομασία TCP/IP προέρχεται από τις συντομογραφίες των δυο κυριότερων πρωτοκόλλων που περιέχει το TCPή Transmission Control Protocol ***(****Πρωτόκολλο Ελέγχου Μετάδοσης****)*** και το IP ή Internet Protocol ***(****Πρωτόκολλο Διαδικτύου****)***.

Αυτή η συλλογή πρωτοκόλλων, όπως και πολλές άλλες άλλωστε, είναι οργανωμένη σε στρώματα ή επίπεδα (layers). Το καθένα τους απαντά σε συγκεκριμένα προβλήματα μεταφοράς δεδομένων και παρέχει μια καθορισμένη υπηρεσία στα υψηλότερα στρώματα. Τα ανώτερα επίπεδα είναι πιο κοντά στη λογική του χρήστη και εξετάζουν πιο αφηρημένα δεδομένα, στηριζόμενα σε πρωτόκολλα χαμηλότερων στρωμάτων για να μεταφράσουν δεδομένα σε μορφές που μπορούν να διαβιβαστούν με φυσικά μέσα.

Το μοντέλο OSI, το οποίο παραμένει έως σήμερα μόνο θεωρητικό, προτείνει την κατάταξη των πρωτοκόλλων δικτύων σε έναν οργανωμένο σωρό 7 στρωμάτων. Συγκρίσεις ανάμεσα στο μοντέλο OSI και το TCP/IP δείχνουν τη σημασία των πρωτοκόλλων που περιέχονται στη σουίτα IP, από την άλλη πλευρά όμως μπορεί να προκληθεί σύγχυση, καθώς το TCP/IP αποτελείται από μόνο 4 στρώματα.

1.8.1 ΕΠΙΠΕΔΑ ΤΗΣ ΣΟΥΙΤΑΣ TCP/IP.



Εικόνα 1.11 : Παράδειγμα ενθυλάκωσης δεδομένων σ΄ ένα διάγραμμα UDP μέσα σε πακέτο IP

Τα πρωτόκολλα Διαδικτύου κάνουν χρήση της ενθυλάκωσης (encapsulation) για να παρέχουν γενικά πρωτόκολλα και υπηρεσίες. Ένα πρωτόκολλο υψηλού στρώματος χρησιμοποιεί τα πρωτόκολλα των κατώτερων για να λειτουργήσει.

Το παρακάτω σχεδιάγραμμα τοποθετεί τα διάφορα πρωτόκολλα του TCP/IP με βάση τα κριτήρια του μοντέλο OSI :

7. **Εφαρμογής**	π.χ. HTTP, SMTP, SNMP, FTP, Telnet, NFS
6. **Παρουσίασης (Presentation)**	Application π.χ. XDR, ASN.1, SMB, AFP
5. **Συνεδρίας (Session)**	π.χ. ISO 8327 / CCITT X.225, RPC, NetBIOS, ASP
4. **Μεταφοράς (Transport)**	π.χ. TCP, UDP, RTP, SPX, ATP
3. **Δικτύου (Network)**	π.χ. IP (IPv4 ή IPv6), ICMP, IGMP, ARP, OSPF, RIP, IPX, DDP
2. **Συνδέσμου (Link)**	π.χ. Ethernet, Token Ring, PPP, HDLC, Frame relay, ATM
1. **Φυσικό (Physical)**	π.χ. Ραδιοφωνικό σήμα, Λέιζερ, Οπτική Ίνα

Τα τρία ανώτερα στρώματα του μοντέλου OSI (Εφαρμογής, Παρουσίασης και Συνεδρίας) αποτελούν ένα ενιαίο στρώμα στο TCP/IP, το επίπεδο Εφαρμογής. Τα χαρακτηριστικά του στρώματος Συνεδρίας αναλαμβάνονται από τις ίδιες εφαρμογές ή απλώς αγνοούνται. Ένα απλουστευμένο σχεδιάγραμμα της στοίβας του μοντέλου TCP/IP ακολουθεί :

4. **Εφαρμογής**	π.χ. HTTP, FTP, DNS *(Πρωτόκολλα δρομολόγησης, όπως το RIP, που βασίζονται στο πρωτόκολλο UDP μπορούν επίσης να καταχωρηθούν στο στρώμα Δικτύου)*

3. **Μεταφοράς**	π.χ. TCP, UDP, RTP *(Πρωτόκολλα δρομολόγησης, όπως το OSPF, που λειτουργούν πάνω από το IP, μπορούν επίσης να καταχωρηθούν στο στρώμα Δικτύου)*
2. **Δικτύου**	Για το TCP/IP, χρησιμοποιείται μόνο το IP *(Τα πρωτόκολλα ICMP και IGMP, παρόλο που βασίζονται πάνω στο IP για την λειτουργία τους, καταχωρούνται στο στρώμα Δικτύου. Το ARP αποτελεί μια από τις ολιγάριθμες εξαιρέσεις, εφόσον είναι ανεξάρτητο του IP)*
1. **Συνεδρίας**	π.χ. Ethernet, Token Ring, κλπ.

Αυτά τα 4 επίπεδα, συναποτελούν το **Μοντέλο Διαστρωμάτωσης του Internet** ή αλλιώς, **Μοντέλο αναφοράς του Internet**.

1.8.2 ΑΝΑΛΥΣΗ ΤΩΝ ΕΠΙΠΕΔΩΝ.

Εφαρμογής

Το στρώμα εφαρμογής χρησιμοποιείται από την πλειοψηφία των δικτυωμένων προγραμμάτων. Το πρόγραμμα παραδίδει τα δεδομένα σε μια μορφή που ορίζει το ίδιο. Εφόσον το TCP/IP δεν παρέχει στρώματα μεταξύ των στρωμάτων εφαρμογής και μεταφοράς, όλες οι λειτουργίες παρουσίασης και συνεδρίας πρέπει να υλοποιηθούν σ' αυτό το επίπεδο. Αυτή η διαδικασία διευκολύνεται με τη χρήση βιβλιοθηκών.

Μεταφοράς

Το στρώμα μεταφοράς είναι υπεύθυνο για την μεταφορά μηνυμάτων, ανεξαρτήτως του υποκείμενου δικτύου, με έλεγχο σφαλμάτων (error control), κατάτμηση (fragmentation) και ρύθμιση ροής (flow control). Η μετάδοση μηνυμάτων μεταξύ δυο οντοτήτων μπορεί να κατηγοριοποιηθεί ως εξής: Η λειτουργία του στρώματος αυτού μπορεί να συγκριθεί με αυτή οποιουδήποτε μηχανισμού/μέσου μεταφοράς, π.χ. ένα όχημα που πρέπει να εξασφαλίζει την πλήρη και ασφαλή διακίνηση του φορτίου του. Το στρώμα μεταφοράς παρέχει αυτή την υπηρεσία σύνδεσης εφαρμογών μεταξύ τους, κάνοντας χρήση θυρών (ports). Καθώς το IP προσφέρει μόνο παράδοση *όσο το δυνατόν καλύτερα* (best effort delivery), το στρώμα μεταφοράς είναι το πρώτο επίπεδο όπου λαμβάνεται υπόψη το θέμα της αξιοπιστίας.

Παραδείγματος χάρη, σε μια προσπάθεια αξιόπιστης μετακίνησης δεδομένων, το TCP που είναι ένα connection-oriented πρωτόκολλο, έχει τα εξής χαρακτηριστικά:

- τα δεδομένα έρχονται στην ίδια σειρά με την οποία στάλθηκαν
- ελάχιστος έλεγχος σφαλμάτων
- ανεπιθύμητα αντίγραφα απορρίπτονται
- χαμένα/απορριφθέντα πακέτα ξαναστέλνονται
- έλεγχος κυκλοφοριακής συμφόρησης (congestion control)

Τα πρωτόκολλα δυναμικής δρομολόγησης (dynamic routing), που κανονικά θα έπρεπε να βρίσκονται σε αυτό το στρώμα του TCP/IP (αφού λειτουργούν πάνω από το IP) αντιμετωπίζονται συχνά ως τμήματα του επίπεδου δικτύου (π.χ. το OSPF).

Το νέο SCTP είναι επίσης ένας "αξιόπιστος", connection-oriented μηχανισμός μεταφοράς. Είναι stream - oriented, όχι byte - oriented όπως το TCP, και προσφέρει την δυνατότητα multiplexing πολλών ρευμάτων (stream) σε μια μόνο σύνδεση. Προτείνει υποστήριξη multi-homing, την δυνατότητα δηλαδή για μια οντότητα να μπορέσει, στα πλαίσια μιας συγκεκριμένης σύνδεσης, να κάνει χρήση πολλαπλών (εφόσον υπάρχουν) διευθύνσεων IP, που αντιπροσωπεύουν πολλαπλές interfaces (διασυνδετικές διατάξεις), έτσι ώστε αν κάποια παρουσιάσει βλάβη, να μη χαθεί η σύνδεση.

Το UDP είναι ένα connectionless πρωτόκολλο διαγραμμάτων δεδομένων (datagrams). Όπως και το IP, είναι ένα best effrot ή "αναξιόπιστο" πρωτόκολλο: ο έλεγχος σφαλμάτων είναι αδύναμος (απλό checksum). Χρησιμοποιείται κυρίως σε εφαρμογές streaming μέσων (ήχος, βίντεο, κλπ.) όπου η έγκαιρη άφιξη των δεδομένων είναι πιο σημαντική από την ακεραιότητα τους. Ο χρόνος που κερδίζεται σε σχέση με τα connection - oriented πρωτόκολλα, που πρέπει να καθιερώσουν μια αξιόπιστη σύνδεση, το καθιστά ιδανικό για απλές ερώτημα/απάντηση εφαρμογές (π.χ. DNS).

Το TCP και το UDP εκμεταλλεύονται από εφαρμογές που διακρίνονται (στο επίπεδο του δικτύου) από την θύρα TCP ή UDP τους. Ορισμένοι αριθμοί θυρών είναι κλειστοί και αναφέρονται σε πολύ συγκεκριμένες εφαρμογές.

Το RTP είναι ένα πρωτόκολλο διαγραμμάτων δεδομένων σχεδιασμένο για στοιχεία πραγματικού χρόνου (real-time) όπως τα ***streaming audio*** και ***video***. Αν και παρουσιάζεται στο στρώμα μεταφοράς (αντί για το επίπεδο συνεδρίας), βασίζεται στο UDP για τη λειτουργία του.

Δικτύου

Ο σκοπός του στρώματος δικτύου είχε αρχικά καθοριστεί ως η μεταφορά πακέτων μέσω ενός ενιαίου δικτύου. Με την εμφάνιση πιο σύνθετων μορφών δικτύων, προστέθηκαν επιπλέον χαρακτηριστικά στο στρώμα αυτό, έτσι ώστε ο ρόλος του να είναι πια η διακίνηση δεδομένων από το δίκτυο πηγή στο δίκτυο προορισμού. Αυτό προϋποθέτει συνήθως τη δρομολόγηση πακέτων διαμέσου ενός δικτύου δικτύων (internetwork) ή διαδικτύου (με μικρά γράμματα).

Στην σουίτα πρωτοκόλλων Διαδικτύου, το IP μεταφέρει τα πακέτα δεδομένων από την πηγή, στον προορισμό. Το IP μπορεί να εξυπηρετήσει διάφορα πρωτόκολλα ανωτέρων επιπέδων (upper layer protocols) ˙ το καθένα τους προσδιορίζεται με έναν αποκλειστικό αριθμό πρωτοκόλλου: π.χ. το ICMP και το IGMP έχουν τους αριθμούς 1 και 2 αντίστοιχα.

Μερικά πρωτόκολλα που στηρίζονται στο IP, π.χ. το ICMP (χρησιμοποιείται για την διάδοση διαγνωστικών πληροφοριών σχετικά με την μεταφορά πακέτων μέσω IP) παρουσιάζονται πάνω από το IP αλλά παρέχουν υπηρεσίες επιπέδου διαδικτύου, απεικονίζοντας έτσι την ασυμβατότητα μεταξύ του Διαδικτύου, των πρωτοκόλλων Διαδικτύου και του μοντέλου OSI. Όλα τα πρωτόκολλα δρομολόγησης (π.χ. BGP, OSPF, RIP, κλπ.) ανήκουν επίσης στο στρώμα δικτύου, αν και θα μπορούσαν να τοποθετηθούν σε ανώτερα επίπεδα.

Συνδέσμου

Το στρώμα αυτό, ρόλος του οποίου είναι η διακίνηση πακέτων του επιπέδου δικτύου μεταξύ δυο οντοτήτων, δεν είναι στην ακρίβεια μέρος της σουίτας πρωτοκόλλων Διαδικτύου, διότι το IP λειτουργεί με διάφορα στρώματα συνδέσμου. Η διαδικασία διαβίβασης (αντ. λήψης) πακέτων σε (αντ. από) ένα συγκεκριμένο επίπεδο συνδέσμου μπορεί να ελέγχεται είτε από τον οδηγό του interface, είτε το firmware ή σύνολο εξειδικευμένων κυκλωμάτων (chipsets), είτε τέλος από ένα συνδυασμό τον προ-αναφερθέντων. Αυτά θα εκτελέσουν τις λειτουργίες σύνδεσης δεδομένων (data link), όπως π.χ. την πρόσθεση

επικεφαλίδας (packet header) πριν την αποστολή, την ίδια τη διαβίβαση του πλαισίου (frame) με τη χρήση ενός φυσικού μέσου.

Για συνδέσεις μέσω μόντεμ (σε γραμμή τηλεφώνου), τα πακέτα IP μεταφέρονται συνήθως χρησιμοποιώντας το PPP. Σε ευρυζωνικές συνδέσεις (π.χ. ADSL) συναντάμε το PPPoE. Σε τοπικά δίκτυα, τα πρωτόκολλα Ethernet ή IEEE 802.11 (για ενσύρματα ή ασύρματα δίκτυα αντίστοιχα) είναι πιο κοινά. Για δίκτυα ευρείας περιοχής (WAN) χρησιμοποιούνται συχνά το PPP πάνω σε γραμμές T-carrier ή E-carrier, το Frame relay, το ATM ή το Packet over SONET/SDH (POS).

Το στρώμα συνδέσμου είναι επίσης το επίπεδο όπου τα πακέτα μπορούν να αναχαιτιστούν για να σταλθούν σ' ένα ιδεατό ιδιωτικό δίκτυο (Virtual Private Network, VPN). Σ' αυτήν την περίπτωση, τα δεδομένα του επιπέδου αυτού αντιμετωπίζονται ως δεδομένα εφαρμογής, και "ξανακατεβαίνουν" τη στοίβα πρωτοκόλλων Διαδικτύου για να σταλθούν. Στη λαμβάνουσα πλευρά, τα δεδομένα ανεβαίνουν δυο φορές τη στοίβα (μια για το VPN και μια δεύτερη για τη δρομολόγηση).

Το φυσικό επίπεδο, που αποτελείται από τα φυσικά στοιχεία του δικτύου (π.χ. hubs, repeaters, καλώδια δικτύου, οπτικές ίνες, ομοαξονικά καλώδια, κάρτες δικτύων) και τις προδιαγραφές χαμηλού επιπέδου των σημάτων (τάση, συχνότητα, κλπ.), θεωρείται συχνά ως μέρος του στρώματος συνδέσμου.

Μια ματιά σε κάθε ένα από τα στρώματα του OSI, καθώς και το ρόλο τους..

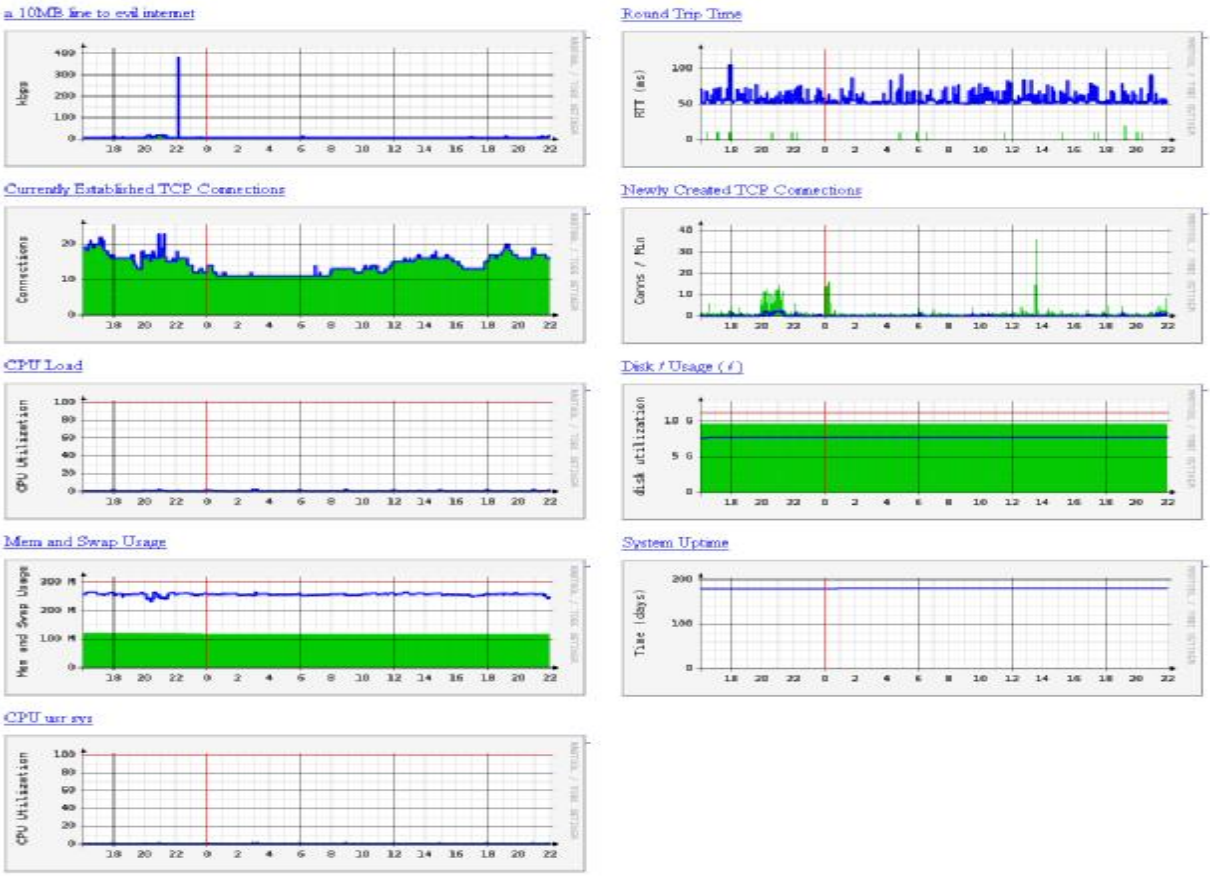
ΕΦΑΡΜΟΓΗ ΕΠΙΠΕΔΟ 7	Παρέχει στο χρήστη εφαρμογές για την πρόσβαση στο δίκτυο. Αυτό το στρώμα αντιπροσωπεύει υπηρεσίες, οι οποίες υποστηρίζουν άμεσα τις εφαρμογές χρήστη, όπως το λογισμικό για μεταφορές αρχείων, πρόσβαση σε βάσεις δεδομένων, και E-mail.
ΠΑΡΟΥΣΙΑΣΗ ΕΠΙΠΕΔΟ 6	Το στρώμα παρουσίασης, συνήθως είναι μέρος ενός λειτουργικού συστήματος, που μετατρέπει εισερχόμενα και εξερχόμενα δεδομένα από μία παρουσιάσιμη μορφή στην άλλη. Επίσης οι υπηρεσίες περιλαμβάνουν κρυπτογράφηση κειμένου και συμπίεση των δεδομένων.
ΣΥΝΕΔΡΙΑ ΕΠΙΠΕΔΟ 5	Ανοίγει τις διαχειρίσεις και κλείνει τις συνομιλίες μεταξύ των δύο υπολογιστών. Εκτελεί την αναγνώριση ονόματος και τις λειτουργίες, όπως η ασφάλεια, που απαιτείται για να επιτρέψει τις δύο εφαρμογές να επικοινωνούν μέσω του δικτύου, προβλέπει επίσης την αντιμετώπιση των λαθών.
ΜΕΤΑΦΟΡΑ ΕΠΙΠΕΔΟ 4	Αυτό το στρώμα παρέχει την διαφανή μεταφορά δεδομένων μεταξύ συστημάτων και είναι υπεύθυνο για την ανάκτηση και τη ροή ελέγχου σφαλμάτων end-to-end. Εξασφαλίζει πλήρη δεδομένα μεταφοράς. Ακολουθίες πακέτων δεδομένων, και ζητήματα αναμετάδοσης των πακέτων που λείπουν. Επίσης, συλλέγει ξανά μηνύματα-πακέτα για περισσότερο αποδοτική μετάδοση μέσω του δικτύου.
ΔΙΚΤΥΟ ΕΠΙΠΕΔΟ 3	Το στρώμα 3 ιδρύει, διατηρεί και τερματίζει τις συνδέσεις δικτύου. Δρομολογεί πακέτα δεδομένων σε όλα τα τμήματα του δικτύου. Μεταφράζει τις λογικές διευθύνσεις και τα ονόματα σε φυσικές διευθύνσεις.

ΣΥΝΔΕΣΗ ΔΕΔΟΜΕΝΩΝ **ΕΠΙΠΕΔΟ 2**	Μεταδίδει πακέτα δεδομένων από υπολογιστή σε υπολογιστή στο ίδιο τμήμα δικτύου. Εξασφαλίζει την αξιοπιστία της φυσικής συνάφειας που καθορίστηκε στο επίπεδο 1. Προτυποποιεί πώς τα πλαίσια δεδομένων θα αναγνωρίζουν και θα παρέχουν τον απαραίτητο ελεγχο και χειρισμό στη διαχείριση σφαλμάτων. Στο επίπεδο σύνδεσης δεδομένων είναι χωρισμένο σε δύο υποεπίπεδα: Το Media Access Control (MAC) στρώμα και το στρώμα Logical Link Control (LLC). Το υποεπίπεδο MAC ελέγχει πώς ένας υπολογιστής στο δίκτυο αποκτά πρόσβαση στα στοιχεία και την άδεια να τα μεταδώσει. Το στρώμα LLC ελέγχει το πλαίσιο συγχρονισμού , τον έλεγχο ροής και τον έλεγχο σφαλμάτων.
ΦΥΣΙΚΟ **ΕΠΙΠΕΔΟ 1**	Το φυσικό στρώμα ορίζει όλες τις ηλεκτρικές και φυσικές προδιαγραφές για τις συσκευές. Αυτό περιλαμβάνει τη διάταξη των τάσεων των καρφιτσών , καθώς και τις προδιαγραφές των καλωδίων. Κόμβοι, επαναλήπτες και προσαρμογείς δικτύου είναι συσκευές που βρίσκονται στο φυσικό επίπεδο. Ορίζει τις καλωδιώσεις και συνδέσεις. Μεταδίδει τα δεδομένα πάνω από το φυσικό μέσο.

1.9 ΤΟ MRTG (Multi Router Traffic Grapher)

Το πρόγραμμα MRTG είναι ελεύθερο λογισμικό γραμμένο στη γλώσσα Perl από τους Tobias Oetiker και Dave Rand για την παρακολούθηση της δικτυακής κίνησης δρομολογητών. Βέβαια στη συνέχεια αναπτύχθηκε σε εργαλείο που μπορεί να δημιουργήσει στατιστικά και γραφικές παραστάσεις από πολλούς τύπους κόμβων ενός δικτύου.

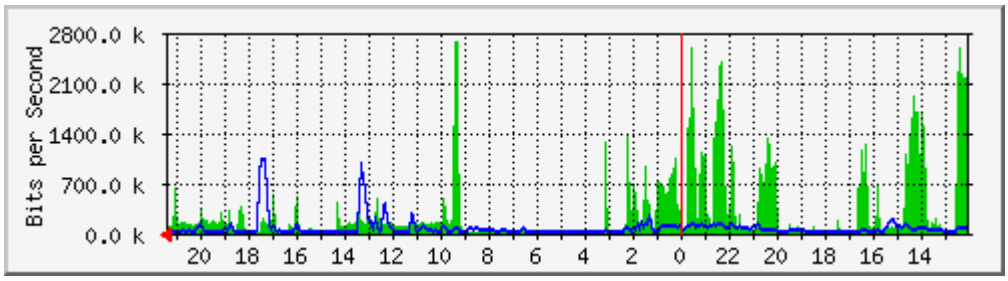
Διατίθεται δωρεάν κάτω από την άδεια GPL v2 του GNU και μπορεί να εκτελεστεί σε πολλά λειτουργικά συστήματα όπως τα Windows, Linux και Mac OS. Το MRTG χρησιμοποιεί το πρωτόκολλο SNMP (Simple Network Management Protocol) για αποστολή αιτήσεων σε συσκευές που υποστηρίζουν το πρωτόκολλο SNMP. Η συσκευή συλλέγει τα ζητούμενα δεδομένα και τα αποστέλλει πίσω στο MRTG εμφωλευμένα σε μορφή πρωτοκόλλου SNMP. Στη συνέχεια το πρόγραμμα καταγράφει τις πληροφορίες που έλαβε, σε εγγραφές για τη συσκευή σε μια βάση δεδομένων.



Εικόνα 1.12 : Καταγραφή των πληροφοριών που έλαβε, σε εγγραφές για τη συσκευή σε μια βάση δεδομένων.

Τέλος το MRTG δημιουργεί ένα έγγραφο ιστοσελίδας από τις εγγραφές, και προβάλλει μια λίστα γραφημάτων με λεπτομέρειες δικτυακής κίνησης για την επιλεγμένη συσκευή. Παρακάτω φαίνονται ορισμένα χαρακτηριστικά του MRTG:

- Μέτρηση για κάθε κόμβο δυο τιμών δικτυακής κίνησης, εισερχόμενης και εξερχόμενης.
- Λήψη των δεδομένων από ένα πράκτορα SNMP ή από τη γραμμή εντολών.
- Συνήθως η συλλογή των πληροφοριών γίνεται κάθε πέντε λεπτά αλλά μπορεί να οριστεί σε μικρότερα χρονικά διαστήματα.
- Προβολή τεσσάρων γραφημάτων για κάθε κόμβο σε μορφή εικόνων GIF ή PNG. Τα γραφήματα δείχνουν την κίνηση ανά ημέρα, εβδομάδα, μήνα και έτος με την εισερχόμενη σε χρώμα πράσινο και την εξερχόμενη σε μπλε. Αυτόματη κλιμάκωση των τιμών των αξόνων του κάθε γραφήματος για εμφάνιση της μεγαλύτερης λεπτομέρειας.
- Εμφάνιση της μέγιστης, μέσης και τρέχουσας εισερχόμενης και εξερχόμενης κίνησης.
- Είναι δυνατή και η αποστολή προειδοποιητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου αν οι παρακολουθούμενοι κόμβοι παρουσιάζουν κίνηση πάνω από κάποιο όριο.



Εικόνα 1.13 : παρακολούθηση κίνησης σε οικιακό δίκτυο.

ΚΕΦΑΛΑΙΟ 2

2.1 ΣΥΣΤΗΜΑΤΑ ΔΙΑΧΕΙΡΗΣΗΣ ΔΙΚΤΥΩΝ

Η μεγάλη και ραγδαία αύξηση του αριθμού των πληροφοριακών συστημάτων τα οποία είναι συνδεμένα στο διαδίκτυο, καθώς και η αύξηση των υποδικτύων τους, δημιούργησε την ανάγκη της ανάπτυξης εφαρμογών και πρωτοκόλλων διαχείρισης των συστημάτων αυτών καθώς και των πόρων χρήσης των δικτύων.

Η βασική ιδέα ενός συστήματος διαχείρισης δικτύου είναι ότι γενικά υπάρχουν δύο ειδών συστήματα-οντότητες σε κάθε σχηματισμό/διαμόρφωση δικτύου.
Οι διαχειριστές και οι πράκτορες. Κάθε κόμβος στο δίκτυο, όπως Η/Υ, servers, bridges, routers κ.α. περιλαμβάνει και έναν πράκτορα. Ο πράκτορας αυτός είναι υπεύθυνος για τα εξής:

- Συλλογή και αποθήκευση πληροφοριών για το τοπικό περιβάλλον
- Την παροχή των πληροφοριών αυτών τους διαχειριστές, είτε έπειτα από μια αίτηση από τον διαχειριστή, είτε όταν συμβεί ένα γεγονός.
- Την εκτέλεση εντολών από τον διαχειριστή που έχουν να κάνουν με την αλλαγή των παραμέτρων

Επίσης ένα σύστημα διαχείρισης δικτύων περιλαμβάνει διαμορφώσεις. Μία διαμόρφωση περιλαμβάνει και έναν ή περισσότερους διαχειριστές ή σταθμούς διαχείρισης. Ένας σταθμός διαχείρισης προσφέρει ένα user interface έτσι ώστε ένας άνθρωπος να μπορεί να ελέγξει και να παρατηρήσει εύκολα τις λειτουργίες του δικτύου.

Το user interface επιτρέπει στο διαχειριστή να εκτελέσει εντολές και του προσφέρει και δυνατότητες παραγωγής reports ώστε με αυτά να αξιολογεί το δίκτυο κάθε στιγμή. Ένα σύστημα διαχείρισης δικτύου είναι ένα σύνολο από εφαρμογές οι οποίες ικανοποιούν τις ανάγκες εκείνες που απαιτούνται από τη διαχείριση ενός δικτύου. Οι εφαρμογές αυτές περιέχουν τις ελάχιστες εκείνες δυνατότητες που να επιτρέπουν την παρακολούθηση της απόδοσης, τον έλεγχο της διαμόρφωσης και άλλες μετρήσεις στο δίκτυο. Οι εφαρμογές διαχείρισης δικτύου λειτουργούν πάνω σε ένα κοινό πρωτόκολλο διαχείρισης. Το πρωτόκολλο διαχείρισης προσφέρει όλες εκείνες τις βασικές λειτουργίες για την ανάκτηση των πληροφοριών διαχείρισης από τους πράκτορες και για την μεταφορά και ενεργοποίηση εντολών σε αυτού.

Τέλος, ο κάθε πράκτορας συντηρεί μία βάση δεδομένων η οποία περιέχει πληροφορίες που έχουν να κάνουν με τη διαμόρφωση του δικτύου και την κίνηση αυτού. Ο σταθμός διαχείρισης συντηρεί μία καθολική βάση δεδομένων με πληροφορίες από όλους τους πράκτορες για όλο το δίκτυο.

2.2 ΤΟ SNMP

Ένα τέτοιο πρωτόκολλο είναι το SNMP. Το πρωτόκολλο SNMP (Simple Network Management Protocol) είναι επέκταση ενός παλαιότερου πρωτοκόλλου διαχείρισης δικτύων το SGMP (Simple Gateway Monitoring Protocol) το οποίο παρουσιάστηκε το 1987. Το SGMP είχε σχεδιασθεί απλά για τον έλεγχο των πυλών σε ένα δίκτυο. Το 1988

παρουσιάστηκε το SNMP σαν ένα πρωτόκολλο διαχείρισης πρωτόκολλο διαχείρισης δικτύων. Η απλότητα του καθώς και η δυνατότητα του να χρησιμοποιηθεί τόσο σε μικρά όσο και σε μεγαλύτερα δίκτυα και ειδικά στο Internet το έκανε πολύ δημοφιλής.

Το SNMP αποτελεί το πιο διαδεδομένο πρωτόκολλο για τη διαχείριση δικτύων βασισμένων στο TCP/IP. Το SNMP, γενικά, αποτελεί ένα πρωτόκολλο για την ανταλλαγή πληροφοριών διαχείρισης, αλλά κάνει και πολλά περισσότερα από αυτή την βασική και κύριά του λειτουργία. Πιο συγκεκριμένα, το SNMP, επιπλέον καθορίζει και ένα format για την αναπαράσταση των πληροφοριών διαχείρισης καθώς και ένα πλαίσιο για την οργάνωση κατανεμημένων συστημάτων σε συστήματα διαχειριστές και διαχειριζόμενους πράκτορες. Επίσης ένας αριθμός από συγκεκριμένες δομές βάσεων δεδομένων, που ονομάζονται βάσεις πληροφοριών διαχείρισης, έχουν καθοριστεί ως τμήμα του SNMP. Αυτές οι MIBs ορίζουν τις διαχειριζόμενες συσκευές για τα πιο κοινά αντικείμενα που παίρνουν μέρος στην διαχείριση δικτύου, όπως οι δρομολογητές, οι γέφυρες και τα LANs.

Το SNMP πρωτόκολλο λειτουργεί στο $7^{ο}$ επίπεδο του OSI μοντέλου δηλαδή στο επίπεδο εφαρμογών. Το SNMP διευκολύνει τη μεταφορά πληροφοριών διαχείρισης μεταξύ συσκευών δικτύου. Αποτελεί στοιχείο του TCP/IP πρωτοκόλλου και δίνει τη δυνατότητα στους διαχειριστές δικτύων να ελέγχουν την απόδοση του δικτύου, να εντοπίζουν, να λύνουν προβλήματα δικτύου και γενικότερα να το διαχειρίζονται πιο εύκολα μέσα από τις πληροφορίες που μπορούν να αντλήσουν μέσα από την χρήση του SNMP.

Ένα δίκτυο το οποίο χρησιμοποιεί το SNMP αποτελείται από τρία βασικά στοιχεία :

- τις συσκευές προς διαχείριση,
- τους πράκτορες (agents),
- το σύστημα διαχείρισης δικτύου (Network – Management System).

Οι συσκευές προς διαχείριση είναι συσκευές οι οποίες συνδέονται στο δίκτυο και περιέχουν SNMP πράκτορες. Οι συσκευές αυτές συλλέγουν και αποθηκεύουν πληροφορίες κατάλληλες για την διαχείριση του δικτύου και παρέχουν τις πληροφορίες αυτές στο σύστημα διαχείρισης δικτύου χρησιμοποιώντας το πρωτόκολλο SNMP. Π.χ. ο δρομολογητής είναι μια τέτοια συσκευή διότι αποτελεί στοιχείο ενός δικτύου και για τη διαχείρισή του χρησιμοποιείται το πρωτόκολλο SNMP.

Πιο συγκεκριμένα ένας πράκτορας είναι ένα λογισμικό διαχείρισης δικτύου το οποίο όπως είπαμε «ανήκει» σε μια συσκευή προς διαχείριση. Ο πράκτορας ουσιαστικά γνωρίζει τοπικά μια πληροφορία της συσκευής κατάλληλη προς διαχείριση και μεταφράζει την πληροφορία αυτή σε μορφή συμβατή για την χρήση της από το πρωτόκολλο SNMP.

Σαν σύστημα διαχείρισης δικτύου ονομάζουμε ένα σύνολο από εφαρμογές, οι οποίες παρακολουθούν και ελέγχουν τις συσκευές προς διαχείριση και η παρουσία τους σε κάθε δίκτυο είναι ζωτικής σημασίας.

Ο ρόλος του συστήματος διαχείρισης είναι κεντρικός και διαθέτει τις παρακάτω δυνατότητες:

- Καθορίζει τις δικές του διαχειριστικές εφαρμογές πάνω από μία κοινή αρχιτεκτονική διαχείρισης δικτύων (διαχειριστική πλατφόρμα).
- Έχει δυνατότητα ταυτόχρονης εκτέλεσης διαφόρων διαχειριστικών εφαρμογών.
- Έχει ευκολότερη ανάπτυξη και συντήρηση του λογισμικού του συστήματος.
- Προσφέρει στον χρήστη μία αρχιτεκτονική διαχείρισης που μπορεί να επεκταθεί και να προσαρμοστεί στις δικές του ειδικές ανάγκες.

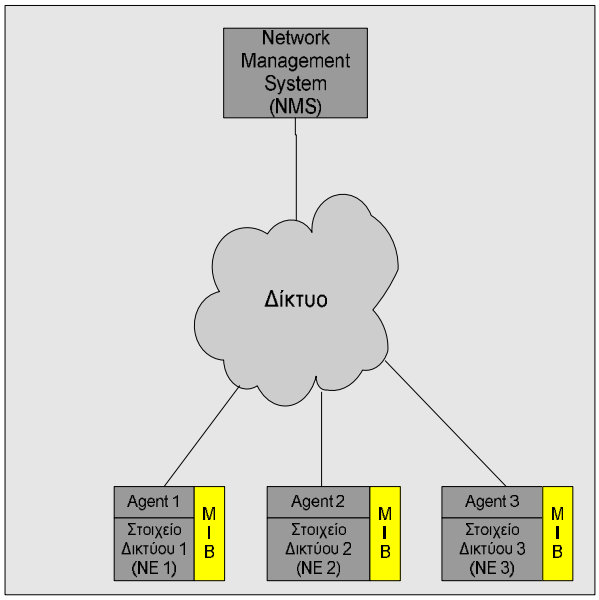
Επίσης το σύστημα διαχείρισης αποτελείται και από τα εξής στοιχεία :

- Πρωτόκολλα επικοινωνίας, κυρίως για την παροχή επικοινωνιακών υπηρεσιών.
- Πρωτόκολλο διαχείρισης δικτύου υλοποιημένο στο επίπεδο εφαρμογής.

- Εφαρμογές διαχείρισης δικτύων οι οποίες χρησιμοποιούν τις υπηρεσίες του πρωτοκόλλου διαχείρισης δικτύων.

Με βάση τα παραπάνω το παρακάτω σχήμα περιγράφει την λογική του SNMP:

Το SNMP βασίζεται στο μοντέλο διαχείρισης δικτύων που φαίνεται στο παρακάτω σχήμα :



Εικόνα 2.1 : Περιγραφή της λογικής του SNMP:

Κάθε πληροφορία αποθηκεύεται σε μια κατάλληλη δομή δεδομένων που να αναγνωρίζεται από το πρωτόκολλο SNMP. Το σύνολο των δομών δεδομένων που χρησιμοποιούνται στο πρωτόκολλο για κάθε διαχειριζόμενο αντικείμενο ονομάζεται Βάση πληροφορίας διαχείρισης (Management Information Base – MIB).

Η Βάση Δεδομένων Διαχείρισης Πληροφοριών MIB αποτελεί την καρδιά του πρωτοκόλλου SNMP. Είναι απαραίτητη για την αναπαράσταση των χαρακτηριστικών κάθε διαχειριζόμενου πράκτορα. Επίσης περιλαμβάνει ορισμούς για τις διαχειριζόμενες συσκευές, τους πράκτορες οι οποίοι είναι διαθέσιμοι καθώς και τις αιτήσεις για τις πληροφορίες τις οποίες έχουν δεχθεί. Όλες αυτές οι πληροφορίες οι οποίες και χρειάζονται για τη διαχείριση μιας συγκεκριμένης συσκευής είναι αποθηκευμένες σε ένα αρχείο το οποίο είναι γνωστό ως MIB file.

Το αρχείο MIB είναι έτσι οργανωμένο ώστε να υπακούσει σε ένα γενικότερο πλαίσιο, το οποίο ονομάζεται Δομή των Πληροφοριών Διαχείρισης (Structure of Management Information – SMI).

Γενικά μπορούμε να πούμε ότι μία MIB είναι το σύνολο βαθμωτών μεταβλητών και δισδιάστατων πινάκων ενώ ταυτόχρονα ορίζεται ότι το πρωτόκολλο δίνει την δυνατότητα στο διαχειριστή να καθορίζει την τιμή των μεταβλητών της MIB και σε ένα πράκτορα να εκδίδει αυτόνομα ειδοποιήσεις που λέγονται παγίδες (traps).

Το πρωτόκολλο SNMP περιλαμβάνει τις ακόλουθες εντολές:

- GET: Με αυτή την εντολή αυτή ο κεντρικός σταθμός μπορεί να ανακτήσει μια τιμή ενός αντικειμένου, από έναν πράκτορα. Έτσι ανακτάται η τιμή των διάφορων μεταβλητών, οι οποίες περιγράφουν την κατάσταση μιας συγκεκριμένης συσκευής.

- SET: Ο κεντρικός σταθμός με αυτή την εντολή θέτει τιμή σε μια μεταβλητή της MIB και έτσι καθορίζει μια χαρακτηριστική τιμή μιας διαχειριζόμενης συσκευής.
- TRAP: Αυτή η εντολή χρησιμοποιείται μόνο από ένα πράκτορα και ενημερώνει το σταθμό διαχείρισης για την πραγματοποίηση ενός γεγονότος.

Πιο αναλυτικά ο NMS όπως βλέπουμε και στο σχήμα είναι ένας κόμβος του δικτύου που έχει εγκατεστημένο το περιβάλλον του SNMP και επιτρέπει μονόδρομη ή αμφίδρομη επικοινωνία με τους πράκτορες. Μέσω των πρακτόρων οι διαχειριζόμενες συσκευές ανταλλάσουν πληροφορίες μαζί του. Γενικά διαχειριζόμενη μπορεί να είναι οποιαδήποτε συσκευή που ανήκει στο δίκτυο. Ο πράκτορας κωδικοποιεί ή αποκωδικοποιεί τα μηνύματα που στέλνονται ή λαμβάνονται από μία άλλη SNMP οντότητα (NMP ή άλλο πράκτορα).

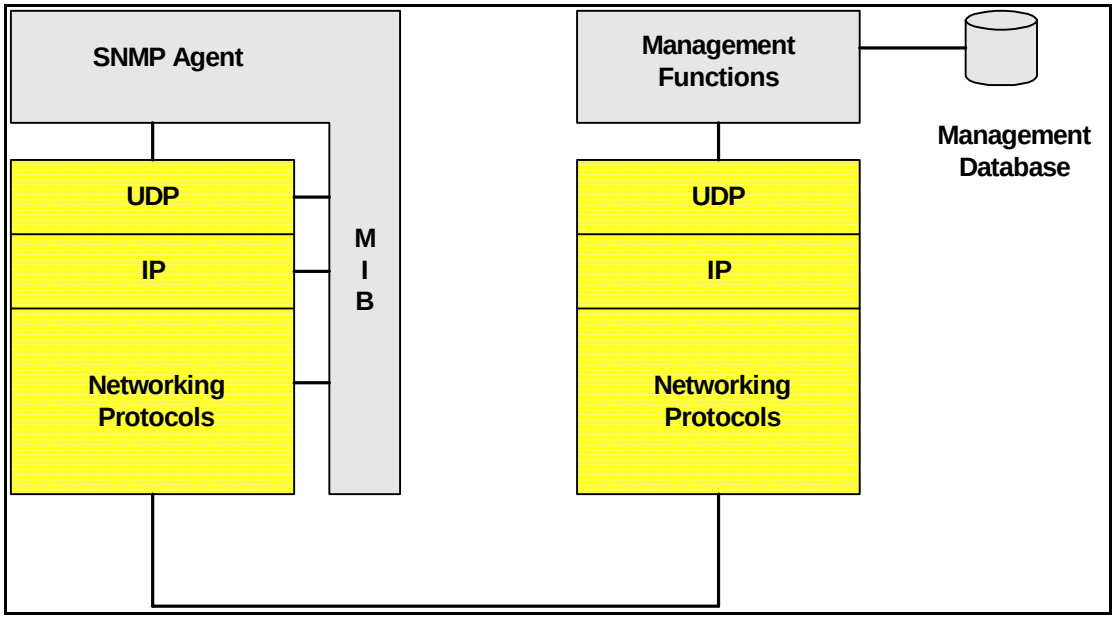
Το πρωτόκολλο SNMP λειτουργεί στο πρωτόκολλο δικτύων TCP/IP. Το πρωτόκολλο TCP/IP χρησιμοποιείται σε τοπικά δίκτυα καθώς και σε δίκτυα ευρείας περιοχής και στο Διαδίκτυο. Ο όρος TCP/ IP είναι ακρωνύμιο των λέξεων Πρωτόκολλο Ελέγχου Μετάδοσης (Transmission Control Protocol- TCP)/ Πρωτόκολλο Διαδικτύου (Internet Protocol- IP). Στην πραγματικότητα έχουμε μία ομάδα πρωτοκόλλων.

Το TCP/IP είναι στο 4ο (TCP) και 3ο (IP) επίπεδο του 7επίπεδου μοντέλου OSI. Στο επίπεδο διασύνδεσης δεδομένων (data lint layer) έχουμε πρωτόκολλα όπως το IP σειριακής γραμμής (Serial Line IP-SLIP) ή το Πρωτόκολλο σημείου-προς –σημείο (point-to-point- PPP) ή τα πρωτόκολλα IEEE 802.X. Στο επίπεδο δικτύου (network layer) βρίσκεται το πρωτόκολλο IP. Στο επίπεδο μεταφοράς το TCP και το UDP (Πρωτόκολλο Πακέτων Χρηστή- User Datagram Protocol). Στο επίπεδο εφαρμογών βρίσκεται το πρωτόκολλο μεταφοράς αρχείων (File Transfer Protocol), το Απλό Πρωτόκολλο Μεταφοράς Ταχυδρομείου (Simple Mail Transfer Protocol –SMTP), και το Απλό Πρωτόκολλο Διαχείρισης Δικτύου (Simple Network Management Protocol- SNMP).

Το SNMP μεταφέρει τις πληροφορίες του με μηνύματα UDP. Ο λόγος που επιλέχθηκαν τα UDP μηνύματα είναι ο παρακάτω: Τα μηνύματα TCP μπορούν να λειτουργήσουν με μεγάλες ποσότητες δεδομένων, γιατί οι πληροφορίες μεταφέρονται πολύ εύκολα. Σε περιπτώσεις όμως κατάρρευσης του δικτύου ή γενικά βλάβης παρατηρήθηκε ότι τα UDP θα κάνουν τη δουλειά τους σε αντίθεση με τα TCP. Για την ακρίβεια τα TCP αρχίζουν να χάνουν την αξιοπιστία τους και να δεν δουλεύουν πλήρως σε περιπτώσεις με 5% απώλειες συνολικών πακέτων και περίπου σε περιπτώσεις 33% γίνονται πλήρως άχρηστα. Αντίθετα τα UDP λειτουργούν σωστά (αν και μπορεί να αργήσουν μερικές φορές στη μεταφορά πακέτων). Για το λόγο αυτό χρησιμοποιείται περισσότερο τα UDP, ενώ μπορεί να χρησιμοποιηθούν και τα δύο πρωτόκολλα μαζί σε συνεργασία σε ένα δίκτυο TCP/IP. Αυτό σημαίνει ότι σε περιπτώσεις μεγάλης ποσότητας δεδομένων χρησιμοποιείται το UDP, ενώ αν υπάρξει κάποιο πρόβλημα στην πορεία αυτό διορθώνεται από το TCP.

Ο σημαντικότερος όμως λόγος που SNMP χρησιμοποιεί το πρωτόκολλο UDP είναι ότι ο NMS δεν χρειάζεται να περιμένει απάντηση σε μία αίτησή του προς τον πράκτορα, αλλά μπορεί να συνεχίσει να στέλνει κι άλλες αιτήσεις. Επιπλέον, η εγκατάσταση σύνδεσης και η διαδικασία επιβεβαιώσεων του TCP θα επιβάρυνε ιδιαίτερα το διαχειριζόμενο δίκτυο, ενώ η απώλεια ενός πακέτου δεν είναι τόσο σημαντική ώστε να δικαιολογεί το επιπλέον φορτίο. Φυσικά αυτό δεν σημαίνει ότι το SNMP δεν μπορεί να χρησιμοποιήσει το TCP ή και άλλα πρωτόκολλα μεταφοράς. Παράδειγμα μπορεί να υλοποιηθεί και κατευθείαν πάνω στο 802.3, με περιορισμένη χρησιμότητα βέβαια εντός του τοπικού δικτύου.

Η απλότητα του SNMP είναι και ο λόγος για τον οποίο το συγκεκριμένο πρωτόκολλο έχει επικρατήσει. Το SNMP χρειάζεται μικρή υπολογιστική ισχύ και δικτυακούς πόρους ενώ ταυτόχρονα καταφέρνει και συγκεντρώνει τις πληροφορίες που χρειάζεται με ένα μικρό αριθμό εντολών για όλες τις συσκευές του δικτύου.



Εικόνα 2.2 : Στο παραπάνω σχήμα φαίνεται η βασική λειτουργία του SNMP :

Με βάση όλα τα παραπάνω μπορούμε να συμπεράνουμε ότι η αρχιτεκτονική πάνω στην οποία βασίζεται το πρωτόκολλο ανήκει στην φιλοσοφία του μοντέλου διαχειριστή – πράκτορα. Κάθε πράκτορας λοιπόν διαθέτει την δική του MIB με ένα αριθμό μεταβλητών π.χ. μετρητές , τύπους interfaces κτλ .

Το πρωτόκολλο SNMP δίνει την δυνατότητα στο διαχειριστή να μπορεί να παρακολουθεί και να αλλάζει τις τιμές αυτές ανάλογα με την λειτουργία και την επίδοση του δικτύου. Έτσι το SNMP ακολουθεί ένα μοντέλο που δίνει την δυνατότητα στον NMS να παρακολουθεί κάθε παράμετρο του δικτύου και ανάλογα με το πώς αυτή συσχετίζεται με τις τιμές και στους υπόλοιπους πράκτορες να τις αλλάζει. Επίσης το SNMP αποστέλλει και αυτόκλητα μηνύματα (TRAPs) στους πράκτορες. Τα μηνύματα αυτά είναι πολύ σημαντικά γιατί μπορούν έγκαιρα να ενημερώσουν τον διαχειριστή για έκτακτα γεγονότα τα οποία συμβαίνουν στο δίκτυο και έτσι να αναγνωρίζει τι ακριβώς συμβαίνει σε μια χρονική στιγμή στο δίκτυο.

Η πληροφορία η οποία χρησιμοποιείται κατά την λειτουργία του πρωτοκόλλου SNMP παριστάνεται με ένα υποσύνολο του συντακτικού ASN.1 και κωδικοποιείται κατά την μεταφορά της σύμφωνα με σύμφωνα με τους λεγόμενους Basic Encoding Ruler (BER-Βασικοί κανόνες κωδικοποίησης). Τα μηνύματα τα οποία κωδικοποιούνται με την χρήση των BERs μπορούν να καταταγούν στις παρακάτω υπηρεσίες :

- Get – Request: Με το μήνυμα αυτό ζητείται η τιμή ενός συγκεκριμένου διαχειριζόμενου αντικειμένου από τη MIB του agent.
- Get – Next – Request: Με αυτό το μήνυμα ζητείται η τιμή του αμέσως επόμενου αντικειμένου στην δομή της MIB.
- Set – Request: Με το μήνυμα αυτό το NMS μπορεί να ζητήσει από τον agent να μεταβάλει την τιμή ενός συγκεκριμένου στιγμιότυπου ενός αντικειμένου.

Ο πράκτορας απαντάει στις αιτήσεις του NMS με μηνύματα Get – Response, επιστρέφοντας κάποιο αντικείμενο της MIB που του είχε ζητηθεί. Οι κατηγορίες των Traps που μπορεί να στείλει ένας agent στον αντίστοιχο διαχειριστή του δικτύου είναι:

Trap	**Λειτουργία**
coldStart, warmStart	αρχικοποίηση πράκτορα
linkDown, linkup	Μεταβολές στο interface του πράκτορα
authenticationFailure	Αποτυχία εξουσιοδότησης
egpNeighborLoss	Απώλεια του gateway ενός γείτονα EGP
enterpriseSpecific	Ορισμός TRAPs από τον κατασκευαστή

Η μεγάλη ανάπτυξη του SNMP, στο τέλος της δεκαετίας του ‘80 και στις αρχές της δεκαετίας του ’90, έφερε στην επιφάνεια και τα μειονεκτήματά του. Τα τελευταία περιλαμβάνουν την έλλειψη ορισμένων λειτουργιών, όπως είναι η αδυναμία να καθοριστεί η μεταφορά «ακατέργαστων» δεδομένων (bulk data) και μειονεκτήματα που έχουν να κάνουν με την ασφάλεια, όπως η έλλειψη μηχανισμών αυθεντικότητας και μυστικότητας (authentication and privacy mechanisms).

Πολλά από τα προβλήματα που είχαν να κάνουν με την έλλειψη ορισμένων λειτουργιών αντιμετωπίστηκαν με την εμφάνιση και την έκδοση του SNMPv2, που το πρώτο RFC που το καθορίζει εμφανίστηκε το 1993. Επίσης έκδοση του 1993 του SNMPv2 περιείχε και μία λειτουργία όσον αφορά την ασφάλεια, αλλά αυτή δεν έγινε ευρέως αποδεκτή επειδή δεν υπήρχαν σαφείς ορισμοί στις σχετικές προδιαγραφές. Η επόμενη έκδοση, η SNMPv2c δεν περιείχε καμιά υπηρεσία ασφαλείας. Για να διορθωθεί αυτή η έλλειψη της υπηρεσίας ασφαλείας στο SNMP, ένας αριθμός από ανεξάρτητες μεταξύ τους ομάδες, άρχισε να δουλεύει πάνω στην συμπλήρωση του SNMPv2 με δυνατότητες που έχουν να κάνουν με την ασφάλεια. Από την εργασία αυτή αναδείχθηκαν δύο ανταγωνιστικές προσεγγίσεις: το SNMPv2u και το SNMPv2*.

Τελικά οι δύο αυτές προσεγγίσεις αποτέλεσαν τη βάση για μια νέα ομάδα, που εργαζόταν υπό την αιγίδα του IETF (Internet Engineering Task Force), για την έκδοση ενός νέου πρωτοκόλλου του SNMPv3, που θα περιείχε όλες αυτές τις απαιτούμενες λειτουργίες ασφαλείας, που στην περίπτωση του SNMPv3 είναι οι: πιστοποίηση (authentication), η μυστικότητα (privacy) και ο έλεγχος πρόσβασης (access control).

Τον Ιανουάριο του 1998 η ομάδα αυτή έβγαλε στη δημοσιότητα ένα σύνολο από RFCs (βλέπε και πίνακα). Τα κείμενα αυτά ορίζουν ένα πλαίσιο ενσωμάτωσης χαρακτηριστικών ασφαλείας σε μία ενιαία οντότητα η οποία μπορεί να περιλαμβάνει είτε το SNMPv1 είτε το SNMPv2. Είναι απαραίτητο να γίνει κατανοητό ότι το SNMPv3 δεν είναι ένα αυτόνομο (stand - alone) πρωτόκολλο που έρχεται να αντικαταστήσει το SNMPv1 και το SNMPv2. Το SNMPv3 καθορίζει ορισμένες λειτουργίες ασφάλειας οι οποίες θα χρησιμοποιηθούν σε συνδυασμό με το, προτεινόμενο, SNMPv2 αλλά και με το SNMPv1. Κάτι τέτοιο ορίζεται από το RFC 2271, που περιγράφει μια αρχιτεκτονική - πλαίσιο μέσα στο οποίο θα είναι δυνατή η συνύπαρξη όλων των υπαρχόντων και μελλοντικών εκδόσεων του SNMP.

Αριθμός	**Τίτλος Ημ/νία**
RFC 2271	An Architecture for Describing SNMP Management Frameworks January 1998
RFC 2272	Message Processing and Dispatching for SNMP January 1998
RFC 2273	SNMPv3 Applications January 1998
RFC 2274	User-Based Security Model for SNMPv3 January 1998
RFC 2275	View-Based Access Control Model (VACM) for SNMPv3 January 1998

Από τα παραπάνω RFCs βλέπουμε ότι μόνο τα τρία από το πέντε RFCs έχουν να κάνουν με την ασφάλεια. Ωστόσο και τα άλλα δύο είναι σημαντικά μιας και ορίζουν όπως είπαμε ένα γενικότερο πλαίσιο μέσα στο οποίο λειτουργεί το SNMPv3. Η παρακάτω εικόνα περιγράφει τη σχέση των διαφόρων εκδόσεων του SNMP σε σχέση με το format.

Η επεξεργασία σχετικά με την ασφάλεια γίνεται σε επίπεδο μηνύματος. Για παράδειγμα, το SNMPv3 ορίζει ένα Μοντέλο Ασφάλειας Χρήστη (στο εξής USM – User Security Model) το οποίο και χρησιμοποιεί τα κατάλληλα πεδία στο message header.

2.3 ΤΟ ΠΡΩΤΟΚΟΛΛΟ SNMPv2

Το πρωτόκολλο SNMPv2 αποτελεί τη δεύτερη έκδοση του SNMP και είναι πιο σαφώς πιο εξελιγμένο από το αρχικό SNMP. Ουσιαστικά συμπληρώνει αρκετά κενά του SNMP και κάνει δυνατή τη διαχείριση πιο πολύπλοκων δικτύων, καθώς προσφέρει καλύτερη υποστήριξη κατανεμημένων στρατηγικών διαχείρισης. Επίσης παρέχει εντολές ασφάλειας που ήταν και το αδύνατο σημείο του SNMP.

Οι σημαντικότερες από τις βελτιώσεις που εισάγει το SNMPv2 είναι :

- ***Βελτιώσεις στην δομή της πληροφορίες διαχείρισης (Structure of Management Information – SMI).*** Ουσιαστικά η SNMPv2 SMI επεκτείνει την αρχική SNMP SMI έτσι ώστε να περιληφθούν αρκετοί νέοι τύποι και να ενισχυθεί η τεκμηρίωση των αρχικών αντικειμένων που περιείχε το SNMP. Σημαντική αλλαγή είναι δυνατότητα για εισαγωγή και διαγραφή στοιχείων σε πίνακες . Οι πίνακες οι οποίοι έχουν αυτή την ιδιότητα ονομάζονται επανεγγράψιμοι και προσφέρουν μεγαλύτερη ευελιξία και επεκτασιμότητα στο χειρισμό των στοιχείων της MIB.
- ***Εισαγωγή νέων λειτουργιών πρωτοκόλλου (Protocol Operations).*** Μία νέα λειτουργία που εισάγει το SNMPv2 είναι η δυνατότητα να αντλούνται μαζικά πληροφορίες από την MIB του αντικειμένου και έτσι να αποφεύγονται οι συνεχείς αιτήσεις στις συσκευές. Επίσης μία άλλη λειτουργία προστέθηκε είναι η δυνατότητα κατανεμημένης αρχιτεκτονικής διαχείρισης.
- ***Νέες MIB.*** Το SNMPv2 ορίζει δύο νέες MIB. Η SNMPv2 MIB είναι ανάλογη της SNMP group της MIB-II και περιέχει πληροφορίες του πρωτοκόλλου καθώς και πληροφορίες για την οργάνωση και την διάρθρωση ενός πράκτορα. Η Manager-To-

Manager MIB σχεδιάστηκε ειδικά για να υποστηρίξει κατανεμημένη αρχιτεκτονική διαχείρισης. Σε MTM MIB εκτός από τα στοιχεία των διαχειριστών και πρακτόρων υπάρχουν στοιχεία με το διπλό ρόλο δηλαδή στοιχεία πράκτορα - διαχειριστή. Τα στοιχεία αυτά συγκεντρώνουν πληροφορίες από τους πράκτορες που διαχειρίζονται και έτσι τις αποθηκεύουν με μια πιο "συνολική" μορφή στην Manager-To-Manager MIB.

- ***Ασφάλεια .*** Το SNMPv2 βασίστηκε στο secure SNMP όσο αφορά την ασφάλεια. Τα βασικότερα στοιχεία που εισάγει το SNMP στον τομέα της ασφαλείας είναι τα ακόλουθα :
  - **Συνοχή – Ορθότητα δεδομένων (Data Integrity)**. Εξασφαλίζει την μεταφορά των δεδομένων χωρίς αλλαγές, πολλά αντίγραφα, χαμένα κομμάτια , επαναλήψεις ή και αναδιατάξεις
  - **Αναγνώριση Πηγής δεδομένων (Data origin authentication)**: Επιτρέπει την αναγνώριση και επιβεβαίωση της ταυτότητας της πηγής των μηνυμάτων.
  - **Εχεμύθεια δεδομένων (Data confidentially):** Εξασφαλίζει ότι στα δεδομένα δεν έχουν πρόσβαση μη εξουσιοδοτημένοι χρήστες, οντότητες η διαδικασίες.

Για να υποστηρίξει όλες αυτές τις βελτιώσεις το SNMPv2 εισάγει μεγαλύτερο αριθμό εντολών (PDU) σε σχέση με το SNMP. Αυτά είναι:

- **Response PDU:** Με το μήνυμα αυτό απαντάει ο agent στις διάφορες αιτήσεις που δέχεται από τον manager.
- **GetRequest PDU:** Το μήνυμα αυτό είναι σχεδόν ίδιο με το αντίστοιχο του SNMP. Η μόνη διαφορά είναι ότι αν κάποια από τις ζητούμενες μεταβλητές δεν μπορεί να ανακτηθεί επιστρέφονται οι υπόλοιπες. Στο SNMP δεν επιστρεφόταν τίποτα.
- **GetNextRequest PDU:** Ισχύουν τα ίδια με το GetRequest μήνυμα.
- **GetBulkRequest PDU:** Με το μήνυμα αυτό ο διαχειριστής μπορεί να ζητήσει να του αποσταλεί ένα υποσύνολο αντικειμένων της MIB σε ένα μόνο Response. Με τον τρόπο αυτό μειώνεται η επιβάρυνση του δικτύου αν για 10 αιτήσεις έπρεπε να σταλούν δέκα ξεχωριστά πακέτα.
- **SetRequest PDU:** Σχεδόν η ίδια λειτουργία με το αντίστοιχο μήνυμα του SNMP. Η διαφορά έγκειται στον αυστηρότερο έλεγχο των τιμών που αποστέλλονται πριν ατές εγγραφούν στη MIB.
- **InformationRequest PDU:** Το μήνυμα αυτό ανταλλάσσεται μεταξύ διαχειριστικών οντοτήτων προσφέροντας έναν τρόπο μεταφοράς πληροφορίας μεταξύ τους.
- **SNMPv2 Trap:** Η ίδια λειτουργία με το αντίστοιχο μήνυμα του SNMP.

2.4 ΤΟ SNMPv3

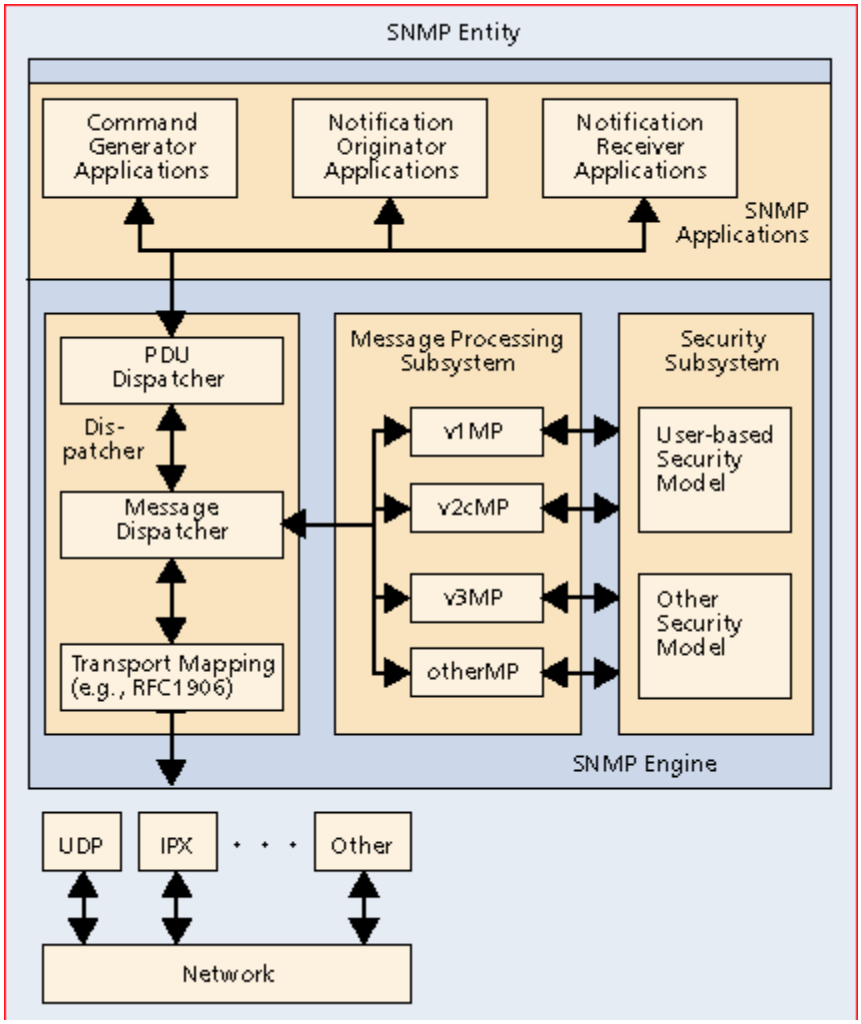
Το SNMPv3 αποτελεί την τρίτη έκδοση του πρωτοκόλλου SNMP. Η αρχιτεκτονική του SNMPv3 αποτελείται από μία συλλογή κατανεμημένων οντοτήτων SNMP, οι οποίες αλληλεπιδρούν μεταξύ τους. Κάθε οντότητα υλοποιεί και ένα μέρος της SNMP ικανότητας και μπορεί να δρα είτε σαν πράκτορας, είτε σαν ένας διαχειριστής είτε σαν συνδυασμός και των δύο. Μία τέτοια οντότητα αποτελείται από μία συλλογή από διεργασίες οι οποίες είναι ένα σύνολο από ιδιότητες και παραμέτρους.

Το πρότυπο RFC 2271 καθορίζει μία απαραίτητη σχεδιαστική απαίτηση για το SNMPv3: Πρέπει να σχεδιαστεί μια αρχιτεκτονική η οποία θα μπορεί να

- Επιτρέπει την υλοποίηση της σε ευρεία γκάμα δικτυακών περιβαλλόντων, ορισμένων από των οποίων να χρειάζονται μία ελάχιστη και φθηνή λειτουργικότητα και άλλων που θα μπορούν να υποστηρίξουν επιπλέον λειτουργικότητα, ώστε να μπορέσουν να διαχειριστούν μεγάλο μέγεθος δικτύου
- Να μπορεί να κάνει εφικτή την υιοθέτηση πιο προηγμένων από τα υπάρχοντα standard, ασχέτως αν αυτά είναι ευρέως αποδεκτά
- Να μπορεί να κάνει χρήση εναλλακτικών μεθόδων ασφαλείας

Κάθε SNMP οντότητα περιλαμβάνει έναν απλό μηχανισμό SNMP, ή αλλιώς μια SNMP μηχανή. Κάθε μηχανή υλοποιεί λειτουργίες όπως το να στέλνει και να λαμβάνει μηνύματα, να πιστοποιεί την αυθεντικότητα και να κρυπτογραφεί και να αποκρυπτογραφεί μηνύματα και τελικά να ελέγχει την πρόσβαση στα διαχειριζόμενα αντικείμενα. Μία SNMP μηχανή καθορίζεται ως ένα σύνολο από διαφορετικές λειτουργίες. Η αρχιτεκτονική αυτή προσφέρει σημαντικά πλεονεκτήματα. Ο ρόλος πλέον μιας SNMP οντότητας καθορίζεται από το ποιες ακριβώς από τις παραπάνω λειτουργίες υλοποιούνται στην οντότητα αυτή.

Επίσης η αρχιτεκτονική αυτή επιτρέπει τον καθορισμό διαφορετικών εκδόσεων για κάθε διεργασία, που με τι σειρά της έχει ως αποτέλεσμα το να μπορεί κάποιος να χρησιμοποιεί εναλλακτικές του πρωτοκόλλου τεχνικές, για ορισμένες λειτουργίες. Επίσης το SNMPv3 χρησιμοποιεί τον λεγόμενο Traditional SNMP manager.



Εικόνα 2.3 : Ένας traditional SNMP manager

Ο traditional SNMP manager αλληλεπιδρά με έναν SNMP πράκτορα στέλνοντας σε αυτόν εντολές και λαμβάνοντας trap μηνύματα. Επίσης ο SNMP manager μπορεί να αλληλεπιδράσει και με άλλους SNMP managers με την αποστολή Inform Requests PDUs (Protocol Data Units) και λαμβάνοντας Inform Requests PDUs, τα οποία αποτελούν και το acknowledge στα Inform Request PDUs.

Στην ορολογία που χρησιμοποιεί το SNMPv3, ένας traditional SNMP manager περιλαμβάνει τρεις κατηγορίες εφαρμογών.

- **Command Generator Applications**: Η Command Generator Applications παρακολουθεί και χειρίζεται τα διαχειριζόμενα δεδομένα στους απομακρυσμένους agents. Οι εφαρμογές αυτές κάνουν χρήση και των SNMPv1 ή/και του SNMPv2 PDU, συμπεριλαμβανομένου των Get, GetNext, GetBulk και Set.
- **Notification Originator Application**. Η Notification Originator Application, ξεκινά ασύγχρονες μεταδόσεις, στην περίπτωση του traditional SNMP manager.
- **Notification Receiver Application**. Η Notification Originator Application αποτελεί και την τρίτη κατηγορία εφαρμογών η οποία επεξεργάζεται εισερχόμενα ασύγχρονα μηνύματα, τα οποία περιλαμβάνουν τα InformRequest, SNMPv2-Trap και SNMPv1-Trap PDUs. Έτσι στην περίπτωση ενός εισερχόμενου InformRequest PDU, η Notification Receiver Application θα απαντήσει με ένα Response PDU.

Όλες αυτές οι εφαρμογές κάνουν χρήση των υπηρεσιών που προσφέρονται από την SNMP engine για αυτή την οντότητα. Η SNMP engine εκτελεί δύο γενικές λειτουργίες:

- Δέχεται εξερχόμενα PDUs από άλλες SNMP εφαρμογές, εκτελεί την απαραίτητη επεξεργασία, όπως την εισαγωγή κωδικών πιστοποίησης και κρυπτογράφησης, και μετά ενσωματώνει τα PDUs σε μηνύματα προς μετάδοση
- Δέχεται εισερχόμενα SNMP μηνύματα από το επίπεδο μεταφοράς, εκτελεί όλη την απαραίτητη επεξεργασία, όπως την πιστοποίηση και την αποκρυπτογράφηση, και μετά εξάγει τα PDUs από το μήνυμα και τα περνά στην κατάλληλη εφαρμογή

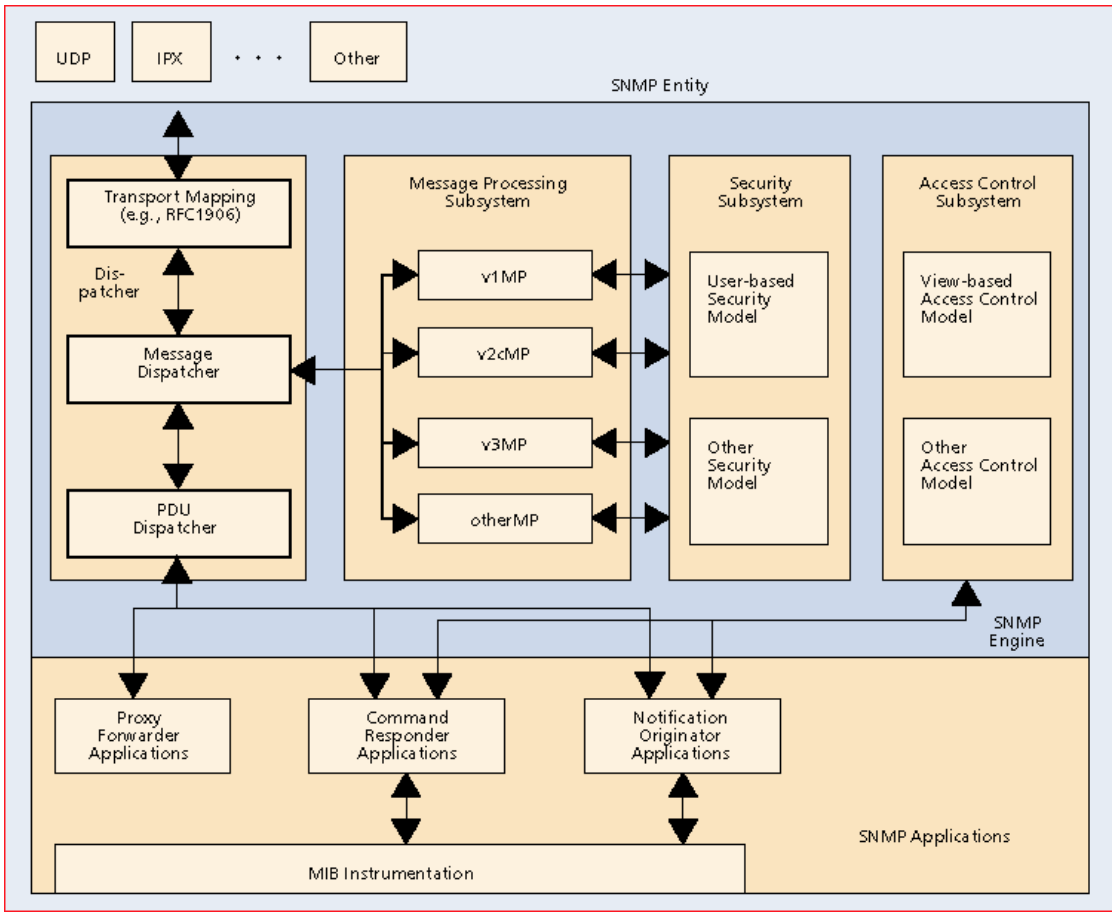
Σε έναν traditional manager, η SNMP engine περιέχει έναν Dispatcher, ένα υποσύστημα επεξεργασίας μηνυμάτων (Message Processing Subsystem) και ένα υποσύστημα ασφαλείας (Security Subsystem).

Ο Dispatcher είναι ένας απλός traffic manager. Ο Dispatcher, για τα εξερχόμενα PDUs δέχεται από τις εφαρμογές και εκτελεί τις παρακάτω λειτουργίες. Επίσης ο Dispatcher για κάθε PDU καθορίζει τι είδους επεξεργασία απαιτείται (π.χ SNMPv1 ή SNMPv2 ή SNMPv3) και περνά το PDU στο κατάλληλο επεξεργαστή μηνυμάτων.

Στην συνέχεια το υποσύστημα επεξεργασία μηνυμάτων επιστρέφει ένα μήνυμα που περιέχει ένα PDU και κάποιους κατάλληλους headers που περιγράφουν την εφαρμογή για την οποία προορίζεται αυτό το μήνυμα. Ο Dispatcher διαβάζει τους headers αυτούς και προωθεί το μήνυμα στην εφαρμογή αυτή. Για τα εισερχόμενα μηνύματα ο Dispatcher δέχεται μηνύματα από το επίπεδο μεταφοράς και εκτελεί τις ακόλουθες λειτουργίες. Για κάθε μήνυμα ο Dispatcher δρομολογεί το μήνυμα αυτό στον κατάλληλο επεξεργαστή μηνυμάτων. Ακολούθως ο επεξεργαστής αυτός του επιστρέφει ένα PDU που περιέχεται σε ένα μήνυμα το οποίο και ο Dispatcher το περνά στην κατάλληλη εφαρμογή.

Το υποσύστημα επεξεργασίας μηνυμάτων δέχεται εξερχόμενα PDUs από τον Dispatcher και τα προετοιμάζει για μετάδοση ενσωματώνοντας σε αυτά τους κατάλληλους headers και τους επιστρέφει στον Dispatcher. Το υποσύστημα επεξεργασίας μηνυμάτων επίσης δέχεται εισερχόμενα μηνύματα από τον Dispatcher, επεξεργάζεται τον κάθε header του μηνύματος και έπειτα επιστρέφει το ενσωματωμένο PDU στον Dispatcher. Μία υλοποίηση του υποσυστήματος επεξεργασίας μηνυμάτων μπορεί να υποστηρίζει πολλαπλά format μηνυμάτων ανάλογα με το πρωτόκολλο (SNMPv1, SNMPv2 ή SNMPv3).

Το υποσύστημα ασφαλείας εκτελεί λειτουργίες πιστοποίησης και κρυπτογράφησης. Κάθε εξερχόμενο μήνυμα περνιέται στο υποσύστημα ασφαλείας από το υποσύστημα επεξεργασίας μηνυμάτων. Ανάλογα με το ποια υπηρεσία απαιτείται το υποσύστημα ασφαλείας μπορεί να κρυπτογραφήσει το ενσωματωμένο PDU -και πιθανόν ορισμένα πεδία στον header του μηνύματος- και να παράγει έναν κωδικό πιστοποίησης τον οποίο και θα εισάγει στον header του μηνύματος. Παρομοίως κάθε εισερχόμενο μήνυμα περνιέται στο υποσύστημα ασφαλείας από το υποσύστημα επεξεργασίας μηνυμάτων. Εάν απαιτείται το υποσύστημα ασφαλείας ελέγχει τον κωδικό πιστοποίησης και αποκρυπτογραφεί το PDU. Στη συνέχεια επιστρέφει το επεξεργασμένο μήνυμα στο υποσύστημα επεξεργασίας μηνυμάτων. Ένα τέτοιο υποσύστημα ασφαλείας μπορεί να υποστηρίζει πολλά μοντέλα ασφαλείας, αλλά αυτό που έχει γίνει μέχρι τώρα είναι το User-Based Security Model (USM) για το SNMPv3. Επίσης το SNMPv3 χρησιμοποιεί έναν Traditional SNMP agent



Εικόνα 2.4 : Ένας traditional SNMP agent

Ο traditional SNMP agent μπορεί να περιλαμβάνει τρεις τύπους εφαρμογές.

- **Command Response Applications.** Οι Command Response Applications, οι οποίες προσφέρουν πρόσβαση στα δεδομένα της διαχείρισης. Οι εφαρμογές αυτές απαντούν σε εισερχόμενες αιτήσεις με την ανάκτηση ή/και την ανάθεση (set) διαχειριζόμενων συσκευών και στη συνέχεια παράγουν ένα Response PDU.
- **Notification Originator Applications.** Οι Notification Originator Applications που ξεκινούν και εδώ ασύγχρονες μεταδόσεις, στην περίπτωση του traditional agent για την εφαρμογή αυτή χρησιμοποιούνται οι SNMPv1-Trap ή οι SNMPv2-Trap PDU.

- **Proxy Forwarder Applications.** Οι Proxy Forwarder Applications που προωθούν μηνύματα μεταξύ των SNMP οντοτήτων.

Μια SNMP engine για έναν traditional agent έχει ό,τι έχει και μία SNMP engine για έναν traditional manager συν το υποσύστημα ελέγχου πρόσβασης (Access Control Subsystem). Αυτό το υποσύστημα προσφέρει υπηρεσίες πιστοποίησης στον έλεγχο της πρόσβασης στις MIBs για διάβασμα και αναθέσεις διαχειριζόμενων αντικειμένων. Οι υπηρεσίες αυτές πραγματοποιούνται στη βάση των περιεχομένων των PDUs. Μία υλοποίηση του υποσυστήματος ασφάλειας μπορεί να υποστηρίξει αρκετά διαφορετικά μοντέλα ελέγχου πρόσβασης. Μέχρι τώρα αυτό που έχει οριστεί είναι το View-Based Access Control Model (VACM) για το SNMPv3.

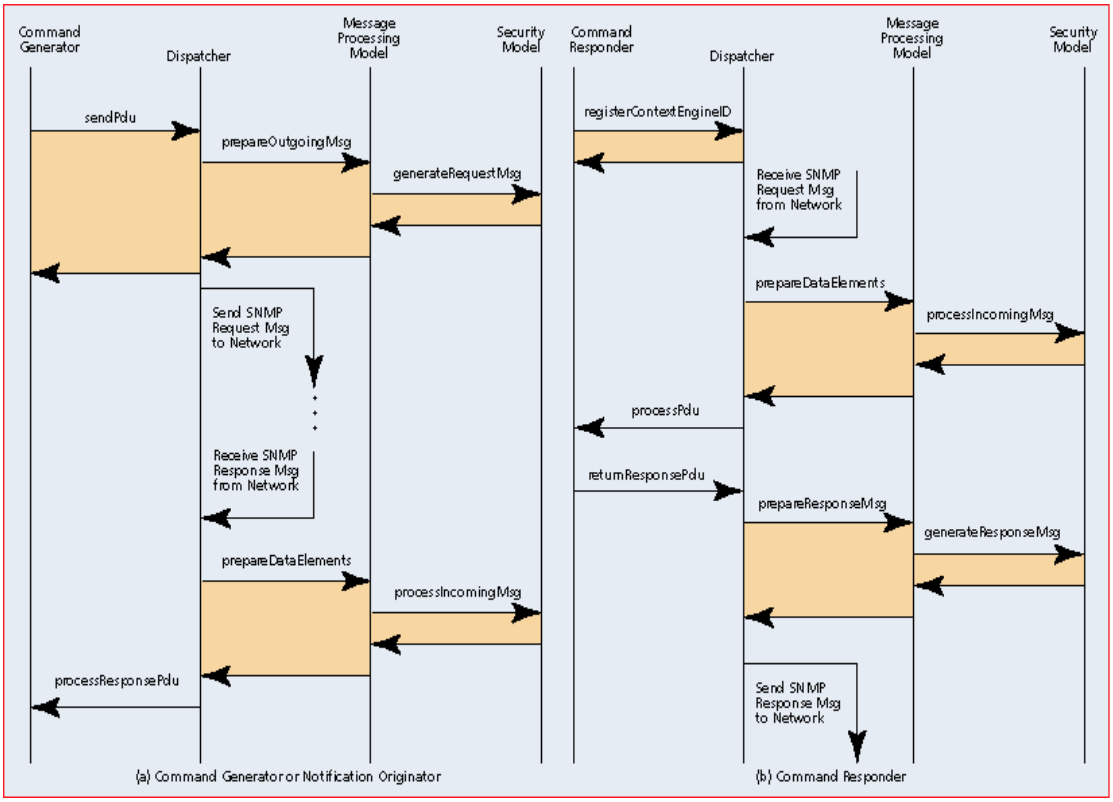
2.4.1 SNMPV3 ΟΡΟΛΟΓΙΑ

Τα σχετικά RFCs ορίζουν και μια σειρά από ορισμένες ορολογίες σχετικά με το SNMPv3. Παρακάτω φαίνεται η ορολογία αυτή:

snmpEngineID	Unique and unambiguous identifier of an SNMP engine, as well as the SNMP entity that corresponds to that engine.
contextEngineID	Uniquely identifies an SNMP entity that may realize an instance of a context with a particular contextName.
contextName	Identifies a particular context within an SNMP engine. It is passed as a parameter to the Dispatcher and Access Control Subsystem.
scopedPDU	A block of data consisting of a contextEngineID, a contextName, and an SNMP PDU. It is passed as a parameter to/from the Security Subsystem.
snmpMessageProcessingModel	Unique identifier of a message processing model of the Message Processing Subsystem. Possible values include SNMPv1, SNMPv2c, and SNMPv3.
snmpSecurityModel	Unique identifier of a security model of the Security Subsystem. Possible values include SNMPv1, SNMPv2c, and USM.
principal	The entity on whose behalf services are provided or processing takes place. A principal can be an individual acting in a particular role; a set of individuals, with each acting in a particular role; an application or set of applications; and combinations thereof.
securityName	A human-readable string representing a principal. It is passed as a parameter in all of the SNMP primitives (Dispatcher, Message Processing, Security, Access Control)

2.4.2 ΕΦΑΡΜΟΓΕΣ SNMPV3 – (SNMP APPLICATIONS)

Οι υπηρεσίες μεταξύ των διαφόρων modules μιας SNMP οντότητας ορίζονται στα RFCs με τη μορφή των στοιχειωδών κλήσεων (στο εξής με την αγγλική ονομασία primitives) και παραμέτρων (parameters). Μπορούμε να φανταστούμε αυτές τις primitives και τις παραμέτρους σαν έναν τυποποιημένο τρόπο αναπαράστασης των υπηρεσιών SNMP. Πιο συγκεκριμένα μία primitive καθορίζει την λειτουργία που πρόκειται να πραγματοποιηθεί και οι παράμετροι χρησιμοποιούνται για τη μεταφορά δεδομένων και πληροφοριών ελέγχου. Παρακάτω φαίνεται μια εικόνα η οποία βασίζεται στο RFC 2271, η οποία δείχνει πως όλα αυτές οι primitives εκτελούνται στην πραγματικότητα:



Εικόνα 2.5 : RFC 2271, δείχνει πως όλα αυτές οι primitives εκτελούνται στην πραγματικότητα:

Το (a) μέρος της εικόνας δείχνει τη σειρά των γεγονότων στα οποία ένας Command Generator ή ένας Notification Generator ζητά να μεταδοθεί ένα PDU και στη συνέχεια τι γίνεται όταν έρχεται η απάντηση σε αυτό το PDU, όλα αυτά φυσικά συμβαίνουν σε έναν manager. Το (b) μέρος της εικόνας δείχνει τι συμβαίνει σε έναν agent, πως δηλαδή ένα εισερχόμενο μήνυμα καταλήγει στο να γίνει dispatch ένα PDU σε μια εφαρμογή και στη συνέχεια πως η εφαρμογή αυτή απαντά στο PDU που δέχθηκε, με ένα εξερχόμενο μήνυμα. Αναλυτικά σε κάθε μια εφαρμογή συμβαίνουν τα εξής:

Command Generator Applications: Μία Command Generator Application χρησιμοποιεί το sendPDU και processResponsePDU Dispatcher primitives. Το sendPDU δίνει στον Dispatcher τις απαραίτητες πληροφορίες για τον προορισμό του PDU, για τις παραμέτρους ασφαλείας και το ίδιο τελικά το PDU. Ο Dispatcher στη συνέχεια ξεκινά το

Message Processing Model, το οποίο με τη σειρά του καλεί το Security Model, για να ετοιμάσουν το μήνυμα. Ο Dispatcher περνά το μήνυμα στο επίπεδο μετάδοσης (Transport Layer) για να μεταδοθεί. Εάν η μετάδοση είναι επιτυχής ο Dispatcher αναθέτει έναν sendPDUHandler identifier για αυτό το PDU και επιστρέφει αυτήν την τιμή στον Command Generator.

Αυτός αποθηκεύει την τιμή αυτή ώστε να μπορεί να ξεχωρίσει τη μελλοντική απάντηση για αυτό το PDU. Ο Dispatcher παραδίδει κάθε εισερχόμενη απάντηση σε PDU στη σωστή Command Generator Application χρησιμοποιώντας την processResponsePDU primitive.

Command Response Applications: Μία Command Response Application χρησιμοποιεί τέσσερις primitives του Dispatcher (registerContextEngineID, unregisterContextEngineID, processPdu, returnResponsePdu) και μία primitive του Access Control Subsystem (isAccessAllowed). Η registerContextEngineID δίνει τη δυνατότητα σε μια command responder application να καταχωρήσει (register) τον εαυτό της ως μια συγκεκριμένη SNMP engine, που μπορεί να κάνει ορισμένες συγκεκριμένες δουλειές με συγκεκριμένα PDU. Μόλις μια command response application έχει κάνει register, όλα τα εισερχόμενα μηνύματα που περιέχουν τον registered συνδυασμό contextEngineID και pduType προωθούνται σε αυτή. Μόλις παραλάβει το πακέτο από τον Dispatcher ένας command responder εκτελεί τα παρακάτω βήματα:

- Εξετάζει το περιεχόμενο του PDU. Αυτό θα πρέπει να ταιριάζει με αυτά που έχει κάνει register.
- Καθορίζει εάν επιτρέπεται η πρόσβαση ώστε να γίνει η απαραίτητη εργασία για αυτό το PDU. Για το σκοπό αυτό καλείται η isAccessAllowed primitive. Η παράμετρος securityModel δείχνει πια μέθοδος-μοντέλο στο Access Control Subsystem χρησιμοποιείται.
- Εάν επιτρέπεται η πρόσβαση ο command responder εκτελεί την κατάλληλη εργασία και ετοιμάζει ένα response PDU. Εάν η πρόσβαση αποτύχει ο command responder ετοιμάζει ένα κατάλληλο για την περίπτωση αυτή response PDU.
- Ο command responder καλεί τον Dispatcher με ένα returnResponsePdu primitive για να στείλει το response PDU.

Notification Generator Applications: Μία Notification Generator Application ακολουθεί την ίδια λογική με μια Command Generator Application.

Notification Receiver Applications: Παρομοίως μια Notification Receiver Application λειτουργεί όμοια με μια Command Respond Application.

Proxy Forwarder Applications: Μία Proxy Forwarder Application χρησιμοποιεί primitives του Dispatcher για να προωθήσει μηνύματα SNMP.

Ένας proxy forwarder προωθεί τεσσάρων ειδών μηνύματα:

- Μηνύματα που περιέχουν PDU από έναν command generator και τα προωθεί είτε στην τελική SNMP engine είτε σε μια πιο κοντινή προς αυτή.
- Μηνύματα από notification generator applications και τα μεταχειρίζεται όπως παραπάνω.
- Μηνύματα που περιέχουν Response PDU και τα μεταχειρίζεται παρομοίως.
- Μηνύματα που περιέχουν έναν report indicator.

2.4.3 USER-BASED SECURITY MODEL

Το SNMPv3 έχει πρόβλεψη για ασφάλεια κατά τις διαχειριστικές λειτουργίες που πραγματοποιεί. Το RCF 2274 που περιλαμβάνεται στο SNMP ορίζει το «μοντέλο ασφάλειας χρήστη» USM. Το USM δίνει τη δυνατότητα για πιστοποίηση και απόρρητη επικοινωνία με τα στοιχεία του δικτύου. Ποιό συγκεκριμένα το User Security Model παρέχει ασφάλεια ως προς τις ακόλουθες απειλές :

- **Τροποποίηση πληροφορίας**: Μια οντότητα μπορεί να μεταβάλλει στο ενδιάμεσο του δικτύου τις εντολές που αποστέλλονται από μια οντότητα με δικαιώματα διαχείρισης, κατά τέτοιον τρόπο ώστε να μπορεί ακόμα και να μεταβάλλει τις τιμές κάποιων αντικειμένων του SNMP.
- **Απόκρυψη και αλλαγή ταυτότητας**: Κάποιες διαχειριστικές λειτουργίες εκτελούνται λανθασμένα γιατί κάποια οντότητα αποκρύπτει την πραγματική της ταυτότητα και εμφανίζεται ώς μια η οποία έχει διαχειριστικά δικαιώματα
- .**Μεταβολή ακολουθίας μηνυμάτων**: Επειδή το SNMP λειτουργεί πάνω απο UDP το οποίο είναι datagram, connectionless πρωτόκολλο, γίνεται να κρατηθούν ορισμένα μηνύματα και να αναδιαταχθούν, ή να επαναληφθούν (replay attack) ώστε να προκαλέσουν ανεπιθύμητες λειτουργίες.
- **Αποκάλυψη λειτουργιών**: Ενας κακόβουλος χρήστης μπορεί παρατηρώντας τις συναλλαγές που κάνει το πρωτόκολλο του SNMP με κάποια στοιχεία του δικτύου που διαχειρίζεται να μάθει τις τιμές των αντικειμένων που μεταβάλλονται. Για παράδειγμα παρατηρώντας τη συναλλαγή κατά την οποία μεταβάλλεται το password μια διαχειριζόμενης οντότητας μπορεί ένας κακόβουλος χρήστης να μάθει το νέο password.

Το USM πάντως, δεν έχει σχεδιαστεί για να αποτρέπει απειλές όπως:

- **Denial of Service(DOS)**: Δημιουργώντας υψηλό φόρτο στο δίκτυο, μπορεί κάποιος κακόβουλος χρήστης να αποτρέψει μια επιθυμητή συναλλαγή μεταξύ του διαχειριστή και μιας οντότητας του δικτύου.
- **Traffic Analysis**: Ενας επιτιθέμενος μπορεί να παρακολουθήσει κάποιες επαναλαμβανόμενες patterns της κίνησης μεταξύ managers και agents.

Το ότι δεν υπάρχει πρόβλεψη για αποτροπή επιθέσεων DOS είναι αποτέλεσμα του ότι στην πλειονότητα των περιπτώσεων, η κίνηση που προκαλείται από την επίθεση δεν μπορεί να διακριθεί απο την κανονική και νόμιμη.

2.4.4 ΚΡΥΠΤΟΓΡΑΦΙΚΕΣ ΛΕΙΤΟΥΡΓΙΕΣ

Δυο κρυπτογραφικές λειτουργίες ορίζονται στο μοντέλο ασφάλειας χρήστη: **πιστοποίηση** και **κρυπτογράφηση**. Για την υποστήριξη αυτών, το SNMP απαιτεί δυο κλειδιά: το μυστικό κλειδί (privKey) και ένα κλειδί πιστοποίησης (authKey). Διαφορετικές τιμές αυτών των κλειδιών κρατώνται για τις εξής ομάδες χρηστών :

- Τοπικούς χρήστες
- Απομακρυσμένους χρήστες

Αυτές οι τιμές είναι χαρακτηριστικά των χρηστών που αποθηκεύονται ξεχωριστά για κάθε ένα, και δεν είναι προσβάσιμες μέσω SNMP. Το USM χρησιμοποιεί δυο εναλλακτικά πρωτόκολλα για πιστοποίηση χρηστών: Το HMAC-MD5-96 και το HMAC-SHA-96. Τα πρωτόκολλα αυτά χρησιμοποιούν μια ασφαλή one-way hash function και ένα κλειδί για να

παράγουν ένα κώδικα πιστοποίησης μηνύματος (MAC). Για την κρυπτογράφηση χρησιμοποιείται ο DES σε CBC mode με μυστικό κλειδί το privKey που αναφέραμε παραπάνω.

2.4.5 AUTHORITY ΚΑΙ ΜΗ AUTHORITY SNMP ΚΛΗΣΕΙΣ

Σε κάθε μεταφορά μηνύματος μια από τις δυο οντότητες που επικοινωνούν ορίζεται αν είναι η authoritative οντότητα ή όχι ανάλογα με τους ακόλουθους κανόνες:

- Όταν ένα SNMP μήνυμα περιμένει απάντηση (πχ. Get, GetNext, GetBulk, Set, Inform PDU), τότε ο αποδέκτης του μηνύματος είναι authoritative.
- Αντίθετα όταν το μήνυμα δεν απαιτεί απάντηση (πχ. Traps) τότε ο αποστολέας είναι authoritative.

Αυτή η διάκριση γίνεται για τους εξής δυο λόγους:

- Η ώρα αποστολής ενός μηνύματος καθορίζεται σε σχέση με ένα ρολόι που διατηρεί η συσκευή που εκτελεί την authoritative κλήση. Έτσι όταν στέλνει ένα μήνυμα, η μη-authoritative συσκευή ρυθμίζει το εσωτερικό της ρολόι σύμφωνα με το timestamp που περιέχεται στο μήνυμα αυτό.
- Ο δεύτερος λόγος έχει σχέση με τα κλειδιά. Τα κλειδιά αποθηκεύονται στην authoritative συσκευή, ώστε αυτή να είναι υπεύθυνη για αυτά χωρίς να υπάρχει το ρίσκο να κρατιούνται και σε άλλες συσκευές σε ένα κατανεμημένο δίκτυο.

Με αυτόν τον τρόπο, συσκευές που χρησιμοποιούνται ως Command Generators ελέγχουν τα timestamps από τα snmp μηνύματα ώστε να μην είναι δυνατή η αναπαραγωγή τους με τα ακόλουθα ανεπιθύμητα αποτελέσματα.

ΚΕΦΑΛΑΙΟ 3

Το πρωτόκολλο CMIP , σύγκριση των πρωτοκόλλων SNMP και CMIP και η λειτουργία RMON του πρωτοκόλλου SNMP

3.1 ΤΟ ΠΡΩΤΟΚΟΛΛΟ CMIP

Στα τέλη της δεκαετίας του 1980 ξεκίνησε ένα έργο, που χρηματοδοτείται από τις κυβερνήσεις, και οι μεγάλες εταιρείες. Το Πρωτόκολλο Διαχείρισης Πληροφοριών (CMIP) γεννήθηκε. Το CMIP (Common Management Information Protocol) έχει ως βάση το πρωτόκολλο OSI και εκτελεί την εξής λειτουργία: ανταλλάσει πληροφορίες μεταξύ των εφαρμογών διαχείρισης δικτύων (network management applications) και πρακτόρων διαχείρισης (management agents). Ο σχεδιασμός του σχετίζεται με το SNMP (Simple Network Management Protocol). Το CMIP δημιουργήθηκε για να βελτιώσει την λειτουργεί που μέχρι πριν εξυπηρετούσε το SNMP δηλαδή τις ικανότητες των συστημάτων διαχείρισης δικτύων και να επανορθώσει τις ασάφειες του.

3.2 ΤΕΧΝΙΚΕΣ ΛΕΙΤΟΥΡΓΙΕΣ

Το CMIP είναι ένα πρωτόκολλο που καθορίζει πώς οι πληροφορίες διαχείρισης δικτύων ανταλλάσσονται μεταξύ των εφαρμογών διαχείρισης των δικτύων (network management applications) και των πρακτόρων διαχείρισης (management agents). Χρησιμοποιεί έναν μηχανισμό ISO και έχει δημιουργηθεί διασφαλίζοντας τον πλήρη έλεγχο και λειτουργία της πρόσβασης, εξουσιοδότησης και δημιουργίας αρχείων ασφαλείας. Η ανταλλαγή πληροφοριών γίνεται μέσω αντικειμένων . Αυτά ονομάζονται συσκευές διαχείρισης , οι οποίες μπορούν να ελέγχουν, να αλλαχθούν και να παρακολουθούν, αλλά και να χρησιμοποιηθούν για να πραγματοποιούν ενέργειες.

Το CMIP ανταλλάσσει τις πληροφορίες του δικτύου μέσω μηνυμάτων, τα οποία ονομάζονται PDUs. Το μήνυμα μπορεί να θεωρηθεί ως ένα αντικείμενο που περιέχει μεταβλητές που έχουν ονόματα και τιμές. Το CMIP περιέχει έντεκα τύπους PDU.

Στο CMIP, οι μεταβλητές αντιμετωπίζονται ως πολύπλοκες δομές δεδομένων με πολλές ιδιότητες . Αυτές περιλαμβάνουν :

- ιδιότητες μεταβλητής οι οποίες αντιπροσωπεύουν τα χαρακτηριστικά της μεταβλητής (τον τύπο δεδομένων της, αν είναι εγγράψιμη)
- συμπεριφορά της μεταβλητής : ποιες ενέργειες αυτής της μεταβλητής μπορούν να ενεργοποιηθούν.
- ειδοποιήσεις : η μεταβλητή παράγει μια αναφορά γεγονότος κάθε φορά που ένα συγκεκριμένο γεγονός προκύπτει (π.χ. το κλείσιμο ενός τερματικού θα προκαλούσε ένα γεγονός ειδοποίησης)

Οι εφαρμογές διαχείρισης δικτύων μπορούν να ξεκινήσουν ανταλλαγές πληροφοριών με πράκτορες διαχείρισης χρησιμοποιώντας τις ακόλουθες ενέργειες:

- ACTION (Απαιτεί μία ενέργεια να προκύψει όπως ορίζεται από το αντικείμενο διαχείρισης).
- CANCEL_GET (Ακυρώνει μία GET απαίτηση).
- CREATE (Δημιουργεί ένα στιγμιότυπο του αντικείμενου διαχείρισης).
- DELETE (Διαγράφει ένα στιγμιότυπο του αντικείμενου διαχείρισης).
- GET (Απαιτεί την τιμή από ένα στιγμιότυπο του αντικείμενου διαχείρισης).
- SET (Θέτει την τιμή σε ένα στιγμιότυπο του αντικείμενου διαχείρισης).

Ένας πράκτορας διαχείρισης μπορεί να αρχικοποιήσει μια ανταλλαγή πληροφοριών με την εφαρμογή διαχείρισης δικτύου χρησιμοποιώντας μία EVENT_REPORT ενέργεια. Αυτή η ενέργεια χρησιμοποιείτε για να στέλνει ειδοποιήσεις (notifications) στην εφαρμογή διαχείρισης, βασισμένων σε αρχικοποιημένες συνθήκες που έχει θέσει η εφαρμογή διαχείρισης δικτύων χρησιμοποιώντας την ACTION (ενέργεια).

Το CMIP δεν καθορίζει το πώς θα λειτουργεί το πρόγραμμα διαχείρισης δικτύων, αλλά τον μηχανισμό ανταλλαγής πληροφοριών των αντικειμένων διαχείρισης και το πώς οι πληροφορίες αυτές θα χρησιμοποιηθούν ή θα μεταφραστούν.

3.2.1 ΕΦΑΡΜΟΓΗ

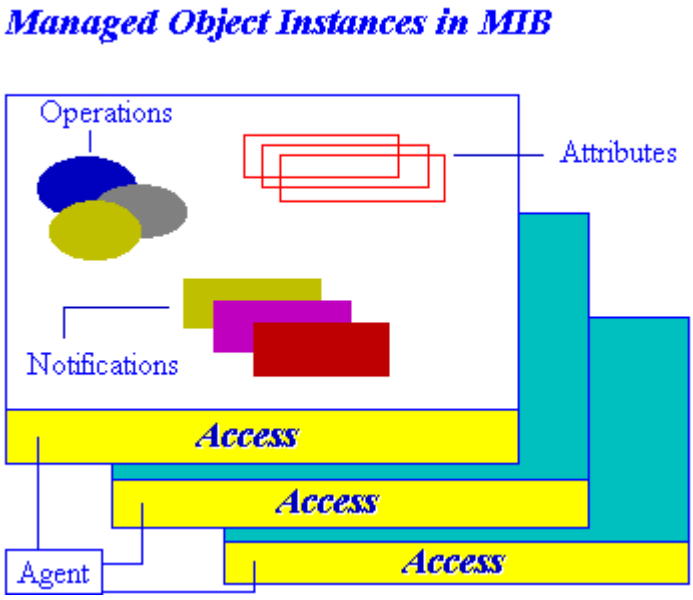
Αρχική προϋπόθεση σε ένα σύστημα διαχείρισης δικτύου είναι να είναι ικανό από πλευράς υλικού και λογισμικού αντίστοιχα, να παρακολουθεί και να ρυθμίζει τις πληροφορίες και στοιχεία του δικτύου. Σε ένα σύστημα διαχείρισης δικτύου, κάθε στοιχείο χρησιμοποιεί ένα μέρος λογισμικού για να μεταφέρει τις πληροφορίες της κατάστασης, μεταφοράς και των ρυθμίσεων του στο λογισμικό διαχείρισης. Επειδή τα στοιχεία ενός δικτύου και οι ιδιότητες των διαχειριζόμενων συσκευών έχουν ιεραρχική δομή, αυτή είναι η πιο κοινή φόρμα που χρησιμοποιείται για να οργανώσει τέτοιες πληροφορίες.

Το μοντέλο διαχείρισης OSI-CMIP χρησιμοποιεί ένα MIB (Management Information Base) για να αποθηκεύει τις δομημένες πληροφορίες που αναπαριστούν τα στοιχεία του δικτύου και τις ιδιότητές τους. Η δομή αποκαλείται **SMI** (structure of management information-δομή διαχειριζόμενων πληροφοριών).

3.2.2.ΔΟΜΗ ΔΙΑΧΕΙΡΗΖΟΜΕΝΩΝ ΠΛΗΡΟΦΟΡΙΩΝ (SMI)

Το OSI-CMIP δημιουργεί ένα αντικειμενοστραφές σύστημα διαχείρισης με διαχειριζόμενα αντικείμενα τις λογικές αναπαραστάσεις ενός υπαρκτού αντικειμένου υλικού ή λογισμικού ή δομής δεδομένων. Τα διαχειριζόμενα αντικείμενα παρέχουν πρότυπα για την ενσωμάτωση πληροφοριών και λειτουργιών. Το αντικειμενοστραφές μοντέλο συμπεριλάβει επίσης την λειτουργία της ειδοποίησης για τα διάφορα συμβάντα. Τα συμβάντα μπορούν να προκύψουν οποιαδήποτε στιγμή, ανεξάρτητα με τους υπολογισμούς του διαχειριστή. Το μοντέλο με διαχειριζόμενο αντικείμενο περιλαμβάνει επίσης υποστήριξη για κληρονομικότητα. Τα στιγμιότυπα του διαχειριζόμενου αντικείμενου έχουν διάφορα χαρακτηριστικά που τα ορίζουν όπως ιδιότητες, πληροφορίες , λειτουργίες κτλ.

Μια ιεραρχία κληρονομικότητας επιτρέπει στην προέκταση των υπαρχόντων κλάσεων διαχειριζόμενων αντικειμένων να γίνει υποκλάση και επιτρέπει την εξειδίκευση. Τα καινούργια διαχειριζόμενα αντικείμενα που μόλις δημιουργήθηκαν εισάγονται σε μια δενδρική δομή. Ένα διαχειριζόμενο αντικείμενο μπορεί να αναπαριστά ένα πολύπλοκο στοιχείο μέσω της ενθυλάκωσης.



Εικόνα 3.1 : Αναπαράσταση διαχειριζόμενου αντικειμένου μέσω της ενθυλάκωσης

Οι πληροφορίες υλοποίησης και άλλες σχετικές πληροφορίες είναι κρυμμένες από το σύστημα διαχείρισης. Το σύστημα ενδιαφέρεται αποκλειστικά για τις **ιδιότητες**, **λειτουργίες**, **συμπεριφορές** και ειδοποιήσεις που αρχικοποιούνται στο MIB.

- Οι ιδιότητες σχετίζονται με αυτό.
- Οι λειτουργίες διαχείρισης μπορούν να εφαρμοστούν σ' αυτό.
- Τις αναφορές για τα γεγονότα μπορεί να τις δημιουργεί.
- Οι καθορισμένες συμπεριφορές επιδεικνύονται από αυτό σε απάντηση στις λειτουργίες διαχείρισης.

Οι ιδιότητες είναι χαρακτηριστικά του διαχειριζόμενου αντικειμένου. Μπορούν να έχουν μία ή περισσότερες τιμές. Κάθε διαχειριζόμενο αντικείμενο έχει εξωτερικές ορατές ιδιότητες οι οποίες σχετίζονται με λειτουργίες σε ένα αντικείμενο. Οι ιδιότητες ανήκουν σε διάφορους τύπους ιδιοτήτων οι οποίοι ορίζονται ως μέρος των πληροφοριών διαχείρισης. Η τιμή μιας ιδιότητας έχει νόημα μόνο στα πλαίσια του τύπου ιδιότητας στον οποίο ανήκει.

Οι λειτουργίες μπορούν να προκύψουν σε στιγμιότυπα των διαχειριζόμενων αντικειμένων. Μπορούν να εφαρμόσουν σε ολόκληρα διαχειριζόμενα αντικείμενα.

- Δημιουργία ενός καινούργιου διαχειριζόμενου αντικειμένου
- Διαγραφή ενός διαχειριζόμενου αντικειμένου
- Εκτέλεση μιας δράσης πάνω σε ένα διαχειριζόμενο αντικείμενο.

Συμπεριφορά: κάθε κλάση διαχειριζόμενου αντικείμενου έχει μια συγκεκριμένη συμπεριφορά που περιγράφει την απόκριση ενός στιγμιότυπου αυτού του διαχειριζόμενου αντικειμένου σε λειτουργίες διαχείρισης.

3.3 ΣΥΓΚΡΙΣΗ ΤΟΥ ΠΡΩΤΟΚΟΛΛΟΥ CMIP ΜΕ ΤΟ SNMP

Μέχρι στιγμής το μεγαλύτερο πλεονέκτημα του SNMP από το CMIP είναι ότι ο σχεδιασμός του είναι απλός, γι 'αυτό είναι τόσο εύκολο στη χρήση σε ένα μικρό δίκτυο, όπως επίσης και σε ένα μεγάλο, με ευκολία εγκατάστασης. Ένας ακόμα βασικός παράγοντας είναι η έλλειψη 'ανησυχίας' για τους πόρους του συστήματος είναι εξίσου πολύ σημαντικό. Επίσης, ο απλός σχεδιασμός , το καθιστά απλό και για τον χρήστη που διαχειρίζεται μεταβλητές του συστήματος του πρόγραμμα που θα ήθελαν να παρακολουθούν.

Ένα άλλο σημαντικό πλεονέκτημα σε SNMP είναι ότι είναι σε ευρεία χρήση σήμερα σε όλο τον κόσμο. Λόγω της ανάπτυξης (διάρκεια ενός χρόνου όταν δεν υπάρχει άλλο πρωτόκολλο αυτού του τύπου) έγινε πολύ δημοφιλές, και το υποστήριξαν οι μεγαλύτεροι πωλητές εξοπλισμού δικτύωσης, όπως hubs, γέφυρες και δρομολογητές, καθώς και majoring λειτουργίας συστήματα.

Ακόμη και έχει τεθεί σε χρήση στο εσωτερικό σε τρία μηχανήματα Coca-Cola στο Πανεπιστήμιο του Στάφορντ, στο Πάλο Άλτο της Καλιφόρνια. Λόγω του μικρότερου μεγέθους του SNMP, έχει ακόμη τεθεί σε εφαρμογή και σε συσκευές όπως φρυγανιέρες και συσκευές αναπαραγωγής ήχου. Στην επίδειξη Interop 1990, ο John Romkey, έδειξε ότι μέσω SNMP πρόγραμμα που εκτελείται σε έναν υπολογιστή, μπορεί να ελέγχετε ένα πρότυπο τοστιέρα μέσω ενός δικτύου.

Το SNMP δεν σημαίνει ότι είναι ένα τέλειο πρωτόκολλο διαχείρισης του δικτύου. Όμως, λόγω του ότι είναι απλά σχεδιασμένο ,τα λάθη που προκύπτουν μπορούν να διορθωθούν. Η πρώτη ανησυχία που δημιουργήθηκε από τις περισσότερες εταιρείες είναι ότι υπάρχουν κάποια μεγάλα προβλήματα με την ασφάλεια. Κάθε 'αξιοπρεπής' χάκερ μπορεί να έχει εύκολη πρόσβαση σε πληροφορίες SNMP, δίνοντάς οποιαδήποτε πληροφορία σχετικά με το δίκτυο, καθώς επίσης και τη δυνατότητα να κλείσει τα συστήματα στο δίκτυο. Η τελευταία έκδοση του SNMP, που ονομάζεται SNMP v2, έχει προσθέσει κάποια μέτρα ασφαλείας που είχαν μείνει έξω από SNMP, για την καταπολέμηση των τριών μεγαλύτερων προβλημάτων που μαστίζουν το SNMP:

- Διαφύλαξη των Δεδομένων (για να αποτρέψει τους εισβολείς από το να αποκτήσουν πρόσβαση στις πληροφορίες που μεταφέρονται κατά μήκος του δικτύου),
- ο έλεγχος ταυτότητας (για να αποτρέψει τους εισβολείς από το να στέλνουν ψευδή στοιχεία σε όλο το δίκτυο), και
- ελέγχου πρόσβασης (η οποία περιορίζει την πρόσβαση συγκεκριμένων μεταβλητών σε ορισμένους χρήστες, αφαιρώντας έτσι τη δυνατότητα του χρήστη συντρίβεται κατά λάθος το δίκτυο).

Το μεγαλύτερο πρόβλημα δηλαδή με το SNMP (αρκετά ειρωνικά) είναι το ίδιο πράγμα που έκανε μεγάλη την επιτυχία του, η απλότητα του σχεδιασμού του. Αυτό οφείλεται κυρίως στην ταχεία δημιουργία του SNMP, διότι ποτέ δεν είχε σχεδιαστεί για να είναι το πρωτόκολλο διαχείρισης δικτύου της δεκαετίας του 1990. Όπως και το προηγούμενο ελάττωμα, έτσι κι αυτό έχει διορθωθεί αρκετά με τη νέα έκδοση, SNMPv2. Αυτή η νέα έκδοση επιτρέπει περισσότερες προδιαγραφές-λεπτομέρειες των μεταβλητών, συμπεριλαμβανομένης της χρήσης της δομής των δεδομένων πίνακα για ευκολότερη ανάκτηση των δεδομένων. Επίσης, προστίθενται δύο νέα PDU που χρησιμοποιούνται για να ελέγχουν τα αντικείμενα πινάκων. Στην πραγματικότητα, έχουν τόσα πολλά νέα χαρακτηριστικά , έχουν δηλαδή προστεθεί τυπικές προδιαγραφές του SNMP και έχουν επεκταθεί από 36 σελίδες (με v1) σε 416 σελίδες με SNMPv2. Μερικοί άνθρωποι μπορεί να

πουν ότι SNMPv2 έχει χάσει την απλότητα, αλλά η αλήθεια είναι ότι οι αλλαγές ήταν αναγκαίες, και δεν θα μπορούσαν να έχουν αποφευχθεί.

Μόλις εμφανίστηκε ο πρωτόκολλο CMIP πολλοί πίστευαν ότι λόγω του ότι επειδή οι δαπάνες για την ανάπτυξη ήταν μεγάλες καθώς και η μελέτη που είχαν κάνει, ότι το νέο πρωτόκολλο θα γίνει γρήγορα ευρεία η χρήση του , και θα ανατρέψει το SNMP από το θρόνο του. Δυστυχώς, τα προβλήματα με την εφαρμογή του έχουν καθυστερήσει τη χρήση του, και είναι τώρα διαθέσιμο μόνο σε περιορισμένη μορφή από τους προγραμματιστές.

Το CMIP σχεδιάστηκε για να είναι καλύτερο από το SNMP με κάθε τρόπο, από την διόρθωση όλων των ελαττωμάτων μέχρι και την επέκταση , καθιστώντας το ένα μεγαλύτερο και πιο λεπτομερή διαχειριστή του δικτύου. Η σχεδίαση του είναι παρόμοια με το SNMP, όπου τα PDU χρησιμοποιούνται ως μεταβλητές για την παρακολούθηση του δικτύου. Το CMIP περιέχει όμως 11 τύποι του PDU (σε σύγκριση με 5 του SNMP). Σε CMIP, οι μεταβλητές θεωρηθεί ως πολύ πολύπλοκες και εξελιγμένες δομές δεδομένων με τρία χαρακτηριστικά. Αυτά περιλαμβάνουν:

- Μεταβλητή χαρακτηριστικά: που αντιπροσωπεύουν τα χαρακτηριστικά των μεταβλητών (στοιχεία του τύπου, εάν είναι εγγράψιμο)
- Μεταβλητή συμπεριφορές: ποιες ενέργειες αυτής της μεταβλητής μπορεί να προκληθεί.
- Ειδοποιήσεις: η μεταβλητή δημιουργεί μια έκθεση κάθε φορά που υπάρχει ένα συγκεκριμένο συμβάν (π.χ. ένα τερματικό κλείσει θα μπορούσε να προκαλέσει μια μεταβλητή κοινοποίησης συμβάντος)

Ως μέτρο σύγκρισης, το SNMP απασχολεί μόνο τις μεταβλητές ιδιότητες ενός και τριών παραπάνω. Το μεγαλύτερο χαρακτηριστικό του πρωτοκόλλου CMIP είναι ότι οι μεταβλητές της όχι μόνο μεταδίδουν πληροφορίες προς και από τον τερματικό σταθμό (όπως σε SNMP), αλλά μπορούν επίσης να χρησιμοποιηθούν για την εκτέλεση εργασιών (που θα ήταν αδύνατο υπό SNMP). Για παράδειγμα, αν ένα τερματικό σε ένα δίκτυο δεν μπορεί να φτάσει τον διακομιστή αρχείων (fileserver) μετά από ένα προκαθορισμένο αριθμό προσπαθειών , τότε μπορεί να κοινοποιηθεί από το CMIP κατάλληλη ειδοποίηση. Με το SNMP, ωστόσο, ο χρήστης θα πρέπει να πει ότι ειδικά για την παρακολούθηση των ανεπιτυχών προσπαθειών πρέπει να επικοινωνήσει με το διακομιστή, και στη συνέχεια τι πρέπει να κάνει όταν η μεταβλητή φτάσει ένα όριο (που έχει ορίσει ο ίδιος). Το CMIP οδηγεί επομένως σε ένα πιο αποτελεσματικό σύστημα διαχείρισης, και απαιτεί λιγότερη εργασία από τον χρήστη, δεν χρειάζεται να ενημερώνει συνεχώς για την κατάσταση του δικτύου. Περιέχει επίσης μέτρα ασφαλείας στα οποία δεν προβλέπονται στο SNMP.

Μετά την ανάγνωση τις παραπάνω παραγράφου, μας δημιουργούνται τα εξής ερωτήματα: αν το CMIP είναι τόσο υπέροχο, γιατί δεν χρησιμοποιείται τόσο πολύ; Η απάντηση είναι ότι έχει μόνο ένα σημαντικό μειονέκτημα που το καθιστά μη προτιμώμενο. Το CMIP απαιτεί περίπου δέκα φορές περισσότερους πόρους συστήματος που απαιτούνται για την λειτουργία του SNMP. Με άλλα λόγια, πολύ λίγα συστήματα στον κόσμο, θα είναι σε θέση να χειριστούν μια πλήρη εφαρμογή για το CMIP χωρίς να υποβάλλονται σε μαζικές τροποποιήσεις του δικτύου. Αυτό το μειονέκτημα δεν έχει φθηνή λύση. Για το λόγο αυτό, πολλοί πιστεύουν πως το CMIP είναι καταδικασμένο να αποτύχει. Το άλλο ελάττωμα στο CMIP είναι ότι είναι πολύ δύσκολο σαν πρόγραμμα. Η πολύπλοκη φύση του απαιτεί τόσες πολλές διαφορετικές μεταβλητές που μόνο λίγοι έμπειροι προγραμματιστές είναι σε θέση να το χρησιμοποιήσουν στο μέγιστο των δυνατοτήτων του.

Λαμβάνοντας υπόψη τις παραπάνω πληροφορίες, μπορεί κανείς να δει ότι και τα δύο συστήματα διαχείρισης έχουν τα πλεονεκτήματα και τα μειονεκτήματά τους. Ωστόσο, ο καθοριστικός παράγοντας για να αποφασίσει κάποιος μεταξύ των δύο, βρίσκεται στην εφαρμογή τους. Είναι σχεδόν αδύνατο να βρεθεί ένα σύστημα με τους απαραίτητους πόρους

για την υποστήριξη του μοντέλου του CMIP, ακόμα κι αν είναι ανώτερη του SNMP (V1 και V2), τόσο στο σχεδιασμό όσο και στη λειτουργία. Πολλοί άνθρωποι πιστεύουν ότι η αυξανόμενη δύναμη των σύγχρονων συστημάτων σύντομα θα ταιριάζει καλά με το μοντέλο του CMIP, και θα μπορούσε να οδηγήσει στην εκτεταμένη χρήση του, αλλά από τη στιγμή που έρθει αυτή η στιγμή, το SNMP θα μπορούσε κάλλιστα να έχει το ίδιο προσαρμοστεί για να γίνει ό, τι προσφέρει το CMIP και περισσότερο. Όπως έχουμε δει με άλλα προϊόντα, όταν μια τεχνολογία επιτυγχάνει να παρακινήσει μια κρίσιμη μάζα, είναι πολύ δύσκολο να πείσει τους χρήστες να αρχίσει να χρησιμοποιεί μια νέα τεχνολογία. Το SNMP είναι ευρέως διαθέσιμο και είναι το πιο δημοφιλές πρωτόκολλο διαχείρισης δικτύων. Παρ' όλα αυτά δεν παρέχει όλη την λειτουργικότητα του CMIP. Στις σημερινές ανάγκες, το TCP/IP και το πρωτόκολλο διαχείρισης δικτύου του SNMP είναι σε ευρεία χρήση. Έχουν σχεδόν πλήρη έλεγχο της αγοράς πρωτοκόλλων διαδικτυακής επικοινωνίας (πολλοί θα καταδίκαζαν το OSI και άρα το CMIP ως αποτυχία). Το OSI όμως έχει ένα πλεονέκτημα : χρηματοδοτήθηκε από κυβερνήσεις και μεγάλους οργανισμούς. Άρα, αν το OSI γίνει ποτέ εύχρηστο στα υπάρχοντα δίκτυα, θα αποκτήσει αμέσως μια μεγάλη αγορά. Επίσης είναι πολύ πιο δυνατό από το SNMP.

Τέλος ίσως το SNMP να χρησιμοποιηθεί σε μια κατάσταση όπου είναι αναγκαία η μέτρια ασφάλεια είναι και SNMP v2 να χρησιμοποιηθεί όπου η ασφάλεια αποτελεί υψηλή προτεραιότητα.

3.3.1 ΧΡΗΣΗ ΤΩΝ ΔΥΟ ΠΡΩΤΟΚΟΛΛΩΝ

- Οι περισσότερες συσκευές τηλεπικοινωνιών υποστηρίζουν το πρωτόκολλο CMIP, και γι' αυτό χρησιμοποιείτε . Η Παγκόσμια Ένωση Τηλεπικοινωνιών (ITU) συστήνει το CMIP ως πρωτόκολλο για την διαχείριση των συσκευών στο Telecommunication Management Network (TNT) standard.
- Είναι σχεδιασμένο να λειτουργεί με βάση το πρωτόκολλο ISO. Παρ' όλα αυτά η πιο διαδεδομένη τεχνολογία που χρησιμοποιείται σήμερα στα περισσότερα LAN δίκτυα είναι το TCP/IP και οι πιο πολλές LAN συσκευές υποστηρίζουν SNMP.
- Επίσης απαιτεί ένα μεγάλο αριθμό πόρων του συστήματος, το οποίο έχει ως αποτέλεσμα την υπερφόρτωση του συστήματος.
- Επιπροσθέτως, το CMIP είναι πιο πολύπλοκο και πιο δύσκολο στον προγραμματισμό γι' αυτό χρειάζεται εξειδικευμένο προσωπικό για να διαχειριστεί ένα σύστημα διαχείρισης δικτύων βασισμένο στο CMIP.

3.3.2 ΚΟΣΤΟΣ ΚΑΙ ΠΕΡΙΟΡΙΣΜΟΙ ΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ

Το CMIP απαιτεί εκτός από ικανό προσωπικό και ικανά συστήματα που να μπορούν να υποστηρίξουν τις απατήσεις του. Επίσης είναι αρκετά δυσεύρετο το λογισμικό του CMIP λόγω περιορισμένης διαθεσιμότητας. Αυτό έχει ως αποτέλεσμα το υψηλό κόστος αγοράς του λογισμικού όπως επίσης και την αύξηση του κόστους αγοράς ικανών συστημάτων για να χρησιμοποιήσουν το CMIP.

3.3.3.Η ΠΙΟ ΔΗΜΟΦΙΛΗΣ ΕΝΑΛΛΑΚΤΙΚΗ ΛΥΣΗ

Το SNMP είναι ευρέως διαθέσιμο και είναι το πιο δημοφιλές πρωτόκολλο διαχείρισης δικτύων. Παρ' όλα αυτά δεν παρέχει όλη την λειτουργικότητα του CMIP.

Στις σημερινές ανάγκες, το TCP/IP και το πρωτόκολλο διαχείρισης δικτύου του SNMP είναι σε ευρεία χρήση. Έχουν σχεδόν πλήρη έλεγχο της αγοράς πρωτοκόλλων

διαδικτυακής επικοινωνίας (πολλοί θα καταδίκαζαν το OSI και άρα το CMIP ως αποτυχία). Το OSI όμως έχει ένα πλεονέκτημα : χρηματοδοτήθηκε από κυβερνήσεις και μεγάλους οργανισμούς. Άρα, αν το OSI γίνει ποτέ εύχρηστο στα υπάρχοντα δίκτυα, θα αποκτήσει αμέσως μια μεγάλη αγορά. Επίσης είναι πολύ πιο δυνατό από το SNMP. Δυστυχώς, αυτό θέτει το πρόβλημα των πόρων του συστήματος και επίσης κάνει το πρωτόκολλο δύσκολο στην κατανόηση.

3.4 RMON: ΑΠΟΜΑΚΡΥΣΜΕΝΟΣ ΕΛΕΓΧΟΣ (REMOTE MONITORING)

MIBs (RMON1 and RMON2)

Η Απομακρυσμένη Παρακολούθησης Δικτύου (Remote Network Monitoring, RMON) MIB αναπτύχθηκε από το IETF (Internet Engineering Task Force) για την υποστήριξη παρακολούθησης και ανάλυσης πρωτοκόλλου του LAN δικτύων. Η αρχική έκδοση (αναφέρεται ως RMON1) επικεντρώθηκε στα Επιπέδου 1 και Επιπέδου 2 του πρωτοκόλλου OSI και επεξεργάζεται πληροφορίες σε Ethernet και Token Ring δίκτυα. Έχει επεκταθεί σε RMON2 που προσθέτει και την υποστήριξη για την παρακολούθηση του Δικτύου στο Επίπεδο 7 του OSI δηλαδή του Επιπέδου Εφαρμογής. Πρόκειται για ένα βιομηχανικό πρότυπο προδιαγραφών το οποίο παρέχει σχεδόν την ίδια λειτουργικότητα με αυτή που προσφέρεται από συσκευές που έχουν σχεδιαστεί αποκλειστικά για την ανάλυση δικτύων. Τα RMON είναι χτισμένα για πολλά κορυφαία τεχνολογικά προϊόντα, switches και routers.

Αναλυτικότερα , είναι μια βασική λειτουργία που με τη χρήση του SNMP επιτρέπει την παρακολούθηση των διαφόρων δικτύων και συστημάτων για την ανταλλαγή δεδομένων λειτουργίας . Το RMON παρέχει στους διαχειριστές του δικτύου, με μεγαλύτερη ελευθερία, στην επιλογή του δικτύου παρακολούθησης με μεθόδους που ανταποκρίνονται στις ιδιαίτερες ανάγκες τους.

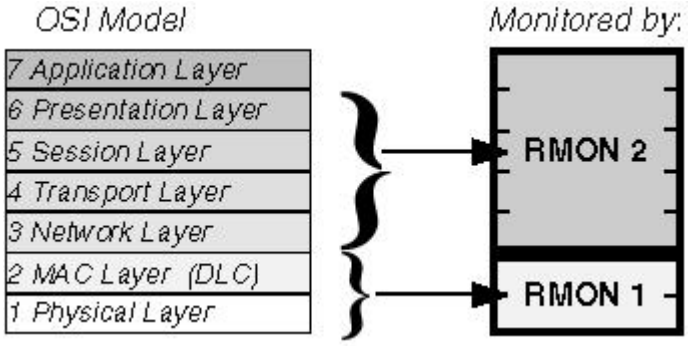
Το RMON αναπτύχθηκε αρχικά για την αντιμετώπιση του προβλήματος της διαχείρισης των LAN σε απομακρυσμένες περιοχές από μια κεντρική τοποθεσία. Η λειτουργία RMON, η οποία αποτελεί προέκταση του SNMP MIB, είναι μια βασική προδιαγραφή παρακολούθησης. Μέσα σε ένα RMON δεδομένο παρακολούθησης του δικτύου ορίζεται ένα σύνολο στατιστικών στοιχείων και λειτουργιών που ανταλλάσσονται μεταξύ των συστημάτων παρακολούθησης. Αυτά τα δεδομένα χρησιμοποιούνται για την παρακολούθηση της χρήσης του δικτύου, για το σχεδιασμό του δικτύου και την απόδοση (tuning). Επίσης βοηθά στην διάγνωση βλαβών του δικτύου.

Υπάρχουν 2 εκδόσεις του RMON. Η RMON1 (RMONv1) και RMON2 (RMONv2). RMON1 ορίζεται για τη βασική παρακολούθηση του δικτύου και μπορεί πλέον να βρεθεί σε όλους τους σύγχρονους υπολογιστές ενός δικτύου. Η RMON2 (RMONv2) είναι μια επέκταση της RMON που εστιάζει σε υψηλότερα στρώματα της κίνησης πάνω από το Επίπεδο 1 (MAC) του TCP/IP πρωτοκόλλου. Η RMON2 δίνει έμφαση στην “κίνηση” του δικτύου και στην κυκλοφορία των δεδομένων στο επίπεδο εφαρμογής (Επίπεδο 4 στο TCP/IP). Επίσης επιτρέπει στις εφαρμογές διαχείρισης δικτύου την παρακολούθηση των πακέτων δεδομένων για όλα τα στρώματα του δικτύου. Αυτό είναι η διαφορά από το RMON το οποίο επιτρέπει μόνο την παρακολούθηση του δικτύου στο Επίπεδο 1 του TCP/IP (MAC).

Οι υλοποιήσεις του RMON πραγματοποιούνται γενικά ως διμερής λύση πελατών/εξυπηρετητών: Ο "πελάτης" είναι η εφαρμογή που τρέχει στο σταθμό διαχείρισης του δικτύου και παρουσιάζει τις πληροφορίες του RMON στον διαχειριστή. Οι "εξυπηρετητές" είναι οι συσκευές ελέγχου που διανέμονται σε όλα τα μακρινά δίκτυα από

τον κεντρικό σταθμό και συλλέγουν τις πληροφορίες για το RMON και αναλύουν τα πακέτα δικτύων. Η συσκευή ελέγχου ονομάζεται "probe" και τρέχει ένα πρόγραμμα λογισμικού, αποκαλούμενο γενικά RMON "πράκτορας." Οι πελάτες, ή οι σταθμούς διαχείρισης, επικοινωνούν με τη χρήση SNMP(Simple Network Management Protocol).

Υπάρχει ένας αριθμός παραλλαγών στο RMON MIB. Για παράδειγμα, το Token Ring. Το RMON MIB παρέχει αντικείμενα ειδικά για τη διαχείριση δίκτυα Token Ring. Η SMON MIB είναι μια επέκταση του RMON που παρέχει ανάλυση RMON για δίκτυα με “switch”.



Εικόνα 3.2 : Τα RMON1 και RMON2 εστιάζουν σε διαφορετικά επίπεδα του μοντέλου OSI:

RMON 1 MIB Group	**Λειτουργία**	**Στοιχεία**
Στατιστικά	Περιέχει στατιστικά στοιχεία. Δημιουργούνται από τον ανιχνευτή για τον διαχειριστή.	Πακέτα που απορρίφθηκαν, πακέτα που στάλθηκαν, σύνολο bytes (σε οκτάδες), σφάλματα, συχνότητες και συγκρούσεις.
Ειδοποιήσεις	Σε τακτά χρονικά διαστήματα παίρνει στατιστικά δείγματα και τα συγκρίνει με προηγούμενα.	Συμπεριλαμβάνει και πίνακα ειδοποιήσεων.
Φιλοξενιτής (Host)	Περιέχει στατιστικά στοιχεία που σχετίζονται με το host.	Host διεύθυνση, πακέτα, and τον αριθμό τον bytes που λαμβάνει και πληροφορίες για τα πακέτα με σφάλμα.
Φίλτρα (Filters)	Τα πακέτα συνοδεύονται από ένα φίλτρο.	Περιέχει ένα φίλτρο τύπου μάσκα ή όχι μάσκα.
Πακέτα	Επιτρέπει την συλλογή πακέτων.	Το μέγεθος του buffer για τα πακέτα που συλλέγονται, ειδοποιήσεις και τον αριθμό των πακέτων.
Γεγονότα (Events)	Ελέγχει την κοινοποίηση των γεγονότων από αυτή τη συσκευή.	Περιέχει τον τύπος του συμβάντος, την περιγραφή του τελευταίου συμβάντος με την ώρα που στάλθηκε.

Δακτύλιος (Token Ring)	Υποστηρίζει Token Ring	Δεν χρησιμοποιείται συχνά .

RMON 2 MIB Group	**Στοιχεία**
‘’Κατάλογος’’ Πρωτοκόλλου (Protocol Directory)	Ο ‘κατάλογος’ του πρωτοκόλλου είναι μια απλή λειτουργία για την εφαρμογή RMON2 . Ελέγχει ποια πρωτόκολλα ένα υλοποιούν την λειτουργία RMON2. Αυτό είναι ιδιαίτερα σημαντικό όταν η εφαρμογή και η λειτουργία είναι από διαφορετικούς προμηθευτές.
Κατανομή πρωτοκόλλου (Protocol Distribution)	Γίνεται χαρτογράφηση των δεδομένων που συλλέγονται από ένα ‘καθετήρα’ για το σωστό όνομα του πρωτοκόλλου που μπορεί στη συνέχεια να εμφανιστεί στον διαχειριστή του δικτύου.
Διεύθυνση χαρτογράφησης (Address mapping)	Διεύθυνση μετάφρασης μεταξύ του MAC επιπέδου και του επιπέδου διευθύνσεις δικτύου οι οποίες είναι πολύ πιο εύκολο να διαβαστούν και να θυμόνται. Η διεύθυνση μετάφρασης δεν βοηθά μόνο το διαχειριστή του δικτύου, που υποστηρίζει το SNMP πλατφόρμα διαχείρισης αλλά θα οδηγήσει σε βελτίωση των χαρτών τοπολογίας του δικτύου.
Επίπεδο δικτύου του ‘Φιλοξενιτή’ (Network Layer host)	Συλλέγει στατιστικά από το επίπεδο δικτύου (IP layer).
Επίπεδο Δικτύου ‘Μήτρες’ (Network layer matrix)	Ανακτημένα από το επίπεδο δικτύου (IP layer) στατιστικά στοιχεία, για τις συνομιλίες μεταξύ των σετ από δύο διευθύνσεις.
Επίπεδο Εφαρμογής ‘Φιλοξενιτή’ (Application layer host)	Συλλογή στατιστικό στοιχείων από το επίπεδο εφαρμογής του ‘φιλοξενιτή’
Ιστορικό του χρήστη (User history)	Αυτή η λειτουργία δίνει τη δυνατότητα στο διαχειριστή του δικτύου, να ρυθμίσει και να μελετήσει το ιστορικό του κάθε μετρητή του συστήματος, όπως ένα συγκεκριμένο ιστορικό στοιχείο σε ένα συγκεκριμένο διακομιστή αρχείων.
‘Καθετήρας’ διαμόρφωσης (Probe configuration)	Το RMON2 έχει ένα σημαντικό χαρακτηριστικό, είναι δυνατή η εφαρμογή RMON σε έναν προμηθευτή για να ρυθμίσει απομακρυσμένο ‘καθετήρα’ (probe) RMON άλλου προμηθευτή.

ΚΕΦΑΛΑΙΟ 4

4.1 ΕΡΓΑΛΕΙΑ ΔΙΑΧΕΙΡΗΣΗΣ ΔΙΚΤΥΩΝ

Έχει αναφερθεί προηγουμένως ότι στο Σύστημα Διαχείρισης Δικτύου (Network Management System -NMS) υπάρχουν εγκατεστημένα εργαλεία (προγράμματα) διαχείρισης δικτύου. Σήμερα κυκλοφορούν αρκετά τέτοια εργαλεία διαχείρισης δικτύου είτε για επαγγελματική χρήση (μεγάλα δίκτυα εταιριών, Πανεπιστημίων), είτε για ερασιτεχνική (μικρά δίκτυα). Μερικά από αυτά είναι τα εξής:

- Από την εταιρεία Ipswitch, το Whatsup Gold
- Από την εταιρεία Hewlett-Packard, το πολύ γνωστό Openview Network Node Manager, το οποίο αποτελείται από άλλα, πιο εξειδικευμένα υποπρογράμματα (ανάλογα τις ανάγκες διαχείρισης)
- Από την εταιρεία IBM, το Tivoli Netview

Τα παραπάνω εργαλεία πρέπει να παρέχουν πολλές δυνατότητες ελέγχου και διαχείρισης του δικτύου στον διαχειριστή, αλλά πάντα μέσα από ένα εύκολο και χρηστικό περιβάλλον εργασίας. Δηλαδή, μας ενδιαφέρει να μπορεί ο διαχειριστής να καταλάβει την κατάσταση ενός δικτύου μόνο μία ματιά στο χάρτη του δικτύου, και από εκεί και πέρα –αν χρειάζεται- να προβεί στις κατάλληλες ρυθμίσεις των συσκευών που ανήκουν στο δίκτυο που ελέγχει και επιτηρεί.

4.2 WHATSUP GOLD (WUG)

Είναι ένα σύστημα διαχείρισης δικτύου και λογισμικού παρακολούθησης που αναπτύχθηκε από την Ipswitch, Inc που ιδρύθηκε το 1991. Η Ipswitch, Inc είναι μια ιδιωτική εταιρεία που έχει την έδρα της στο Λέξινγκτον της Μασαχουσέτης. Το WhatsUp Gold προσφέρει σε ένα ολοκληρωμένο δίκτυο, το σύστημα, την εφαρμογή , την παρακολούθηση καταγραφής και διαχείρισης τόσο σε υλικό όσο και εικονικά περιβάλλοντα υποδομών.

4.2.1 ΕΠΙΣΚΟΠΗΣΗ ΤΟΥ WHATSUP GOLD.

Υπάρχουν πέντε βασικές πτυχές του λογισμικού:

- **Ανακάλυψη** - Αυτόματη ανακάλυψη όλων των πόρων (δίκτυο συσκευές, τα συστήματα και τις διασυνδέσεις τους) και χαρτογράφηση της συνδεσιμότητας με Layer 2/3 τεχνολογίες δικτύων, συμπεριλαμβανομένων ARP, SNMP, ICMP, SSH, LLDP, WMI, Telnet, κλπ.
- **Χαρτογράφηση** - Πλήρης χαρτογράφηση του δικτύου και αυτόματη δημιουργία ενός πλήρους Layer 2/3 τοπολογία χάρτη του δικτύου με ορατότητα σε τόσο σωματική όσο και IP συνδεσιμότητα, συμπεριλαμβανομένων των VMware και VLAN-συγκεκριμένες πληροφορίες.
- **Παρακολούθηση** - Η παρακολούθηση της υγείας, της διαθεσιμότητας και της κατάστασης του δικτύου, τα συστήματα και τις υποδομές εφαρμογών που χρησιμοποιεί ένα συνδυασμό και των δύο ενεργητικών και παθητικών τεχνολογιών παρακολούθησης. Έγκαιρη προειδοποίηση ειδοποιήσεις παγίδων μέσω SNMP και με μηνύματα από Syslog συσκευές υποδομής.

- **Προειδοποίηση** - Μια ενιαία εικόνα του ταμπλό με ειδοποιήσεις από ολόκληρη την υποδομή (θέματα επιδόσεων, συμφόρησης της κυκλοφορίας, τα σφάλματα διαμόρφωσης, κλπ.). Πολυεπίπεδες κλιμακώσεις.
- **Αναφορά** - Standard και προσαρμόσιμες αναφορές που παρέχουν πλήρη ορατότητα στην υγεία και την απόδοση της υποδομής.

4.2.2 AWARDS

- Network Management Product of the Year, 2012 – Network Computing Awards
- PC Magazine:Editors' Choice Award, 2012 – WhatsUp Gold v16
- Global Excellence Award, 2012 – Info Security Products Guide
- Best Software Product of the Year, 2011 (WhatsUp Gold Premium) – IT Pro Awards
- Network Management Product of the Year, 2010 – Network Computing Awards

Προϊόν/Τεχνολογία: What's Up Gold v14.1

Hardware, Software ή Υπηρεσία: Λογισμικό

Ξεκίνησε : Οκτώβριος2009 (Αναβάθμιση)

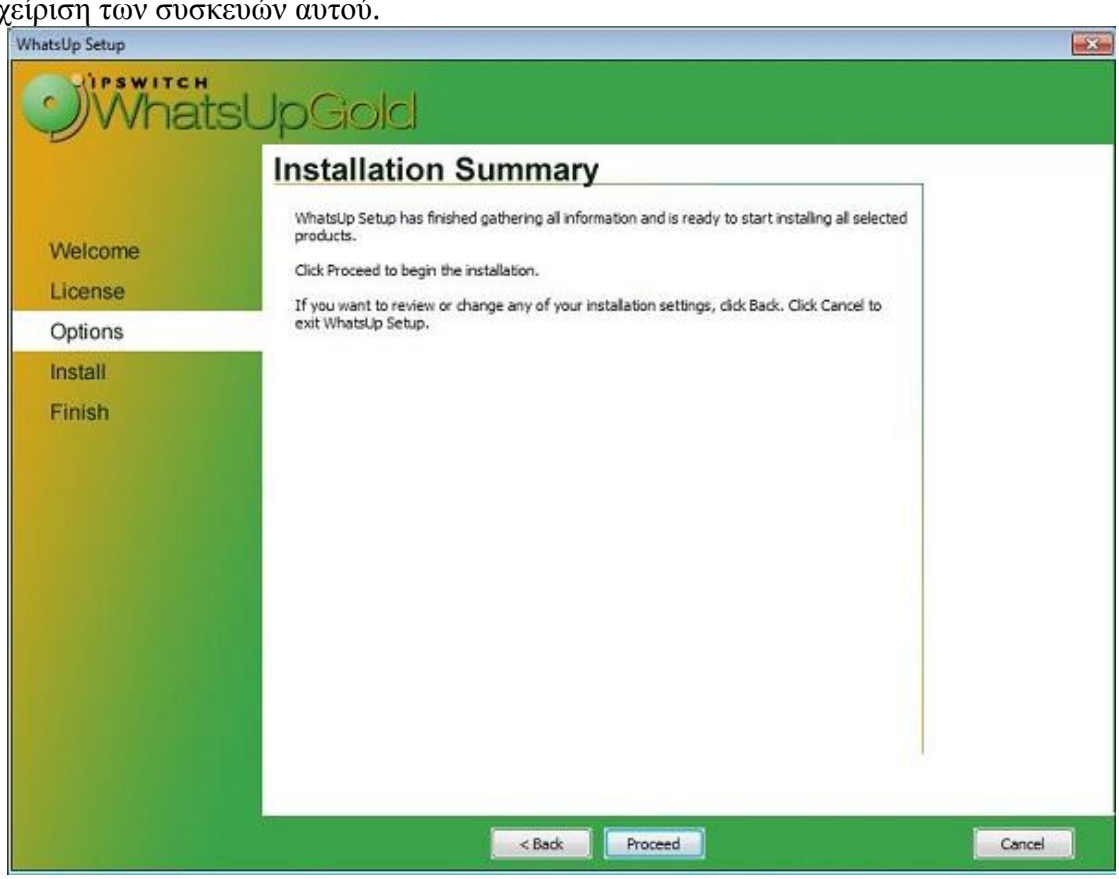
4.2.3 ΤΙ ΚΑΝΕΙ ΤΟ WHATSUP GOLD.

Το WhatsUp Gold παρέχει ένα ισχυρό αποδοτικό δίκτυο και μια εφαρμογή στη λύση διαχείρισης για ενσύρματα και ασύρματα δίκτυα όλων των μεγεθών. Εγκαθιστώντας το λογισμικό ανακαλύπτονται τα στοιχεία και οι χάρτες συνδέονται με το δίκτυο περιουσιακών στοιχείων μέσα σε λίγα λεπτά. Αξιοποιώντας το SNMP v1-3 το whatsup Gold επιτρέπει την έξυπνη παρακολούθηση, σε συνδυασμό με ισχυρές δυνατότητες συναγερμού και κοινοποίησης για να κρατήσει την υποδομή δικτύου και τα διευθυντικά στελέχη ενημερώνονται σε πραγματικό χρόνο όταν προκύπτουν θέματα. Δεν έχει σημασία πόσο περίπλοκη είναι η υποδομή του δικτύου, διαισθητική ο χώρος εργασίας και οι πίνακες, εγγυάται γρήγορη πλοήγηση σε ειδοποιήσεις και τα θέματα αποδίδονται σε πραγματικό χρόνο. Έτσι η πρόσβαση σε περισσότερες από 200 εκθέσεις τεκμηριώνουν όλες τις εύρος ζώνης συσκευές και σχετικές με την εφαρμογή δραστηριότητες.

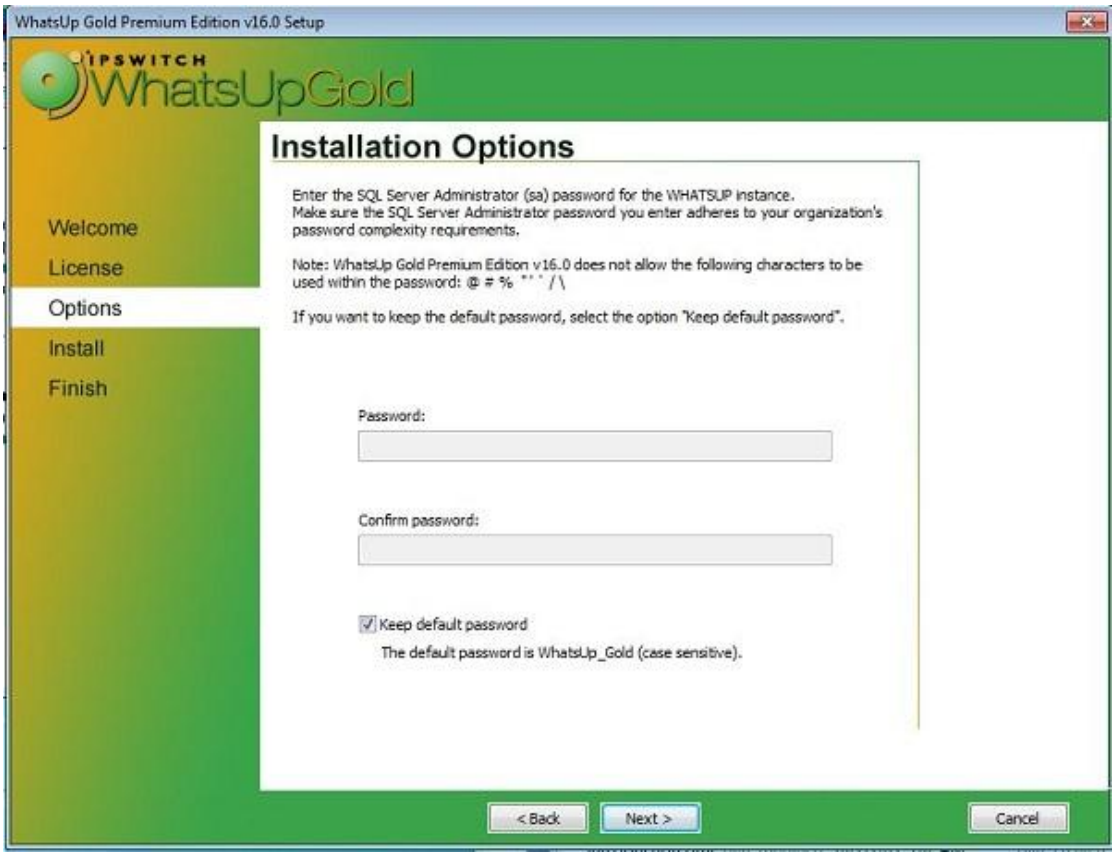
Καινοτόμα προϊόντα, όπως τα Gold whatsup φέρνουν βελτιώσεις σε έξυπνη παρακολούθηση, στην ευκολία χρήσης και ενοποίησης εργαλείων.

Αυτό που το καθιστά Καινοτόμο: Το WhatsUp Gold παρέχει ένα ισχυρό αποδοτικό δίκτυο και λύση στην εφαρμογή διαχείρισης για ενσύρματα και ασύρματα δίκτυα όλων των μεγεθών. Επίσης προσφέρει σε κλάσματα του δευτερολέπτου σε πραγματικό χρόνο γραφικές παραστάσεις που απεικονίζουν έναν πλούτο κρίσιμων πληροφοριών σχετικά με την κατάσταση του δικτύου. Επιπροσθέτως εισήγαγε πρόσφατα ένα βελτιστοποιημένο περιβάλλον εργασίας που προσφέρει πρόσβαση στην κατάσταση του δικτύου και την υποβολή εκθέσεων μέσω Web-enabled PDAs και Smartphones. Με καινοτόμα χαρακτηριστικά όπως one-click login, απευθείας Link κοινοποιήσεις και την υποβολή εκθέσεων NetFlow, whatsup Gold φέρνει μια εντελώς νέα διάσταση της φορητότητας για τη διαχείριση του δικτύου, επιτρέποντας στους χρήστες να διαχειρίζονται το δίκτυό τους οπουδήποτε, οποτεδήποτε. Ακόμα προσφέρει ένα επίπεδο ενοποίησης εργαλείων που ταιριάζει στη σημερινή βιομηχανία, με τη δημιουργία λύσεων για τους διαχειριστές δικτύου που περιλαμβάνει: το δίκτυο παρακολούθησης της εφαρμογής παρακολούθησης, ασύρματο δίκτυο παρακολούθησης, τη διαχείριση της αλλαγής, Layer 2 ανάλυσης κίνησης και σύντομα, την παρακολούθηση και τη διαχείριση εικονικής πραγματικότητας (virtualization) , όλα σε μία εύκολη στη χρήση εφαρμογή. Τέλος, δίνει στους πελάτες πρόσβαση σε ένα ευρύ φάσμα των plug-ins, συμπεριλαμβανομένων των Monitor ροής, VoIP Monitor, WhatsConnected, WhatsConfigured και Εκδότης ροής - όλα μέσα από το πιο ευέλικτο πρόγραμμα αδειοδότησης της βιομηχανίας.

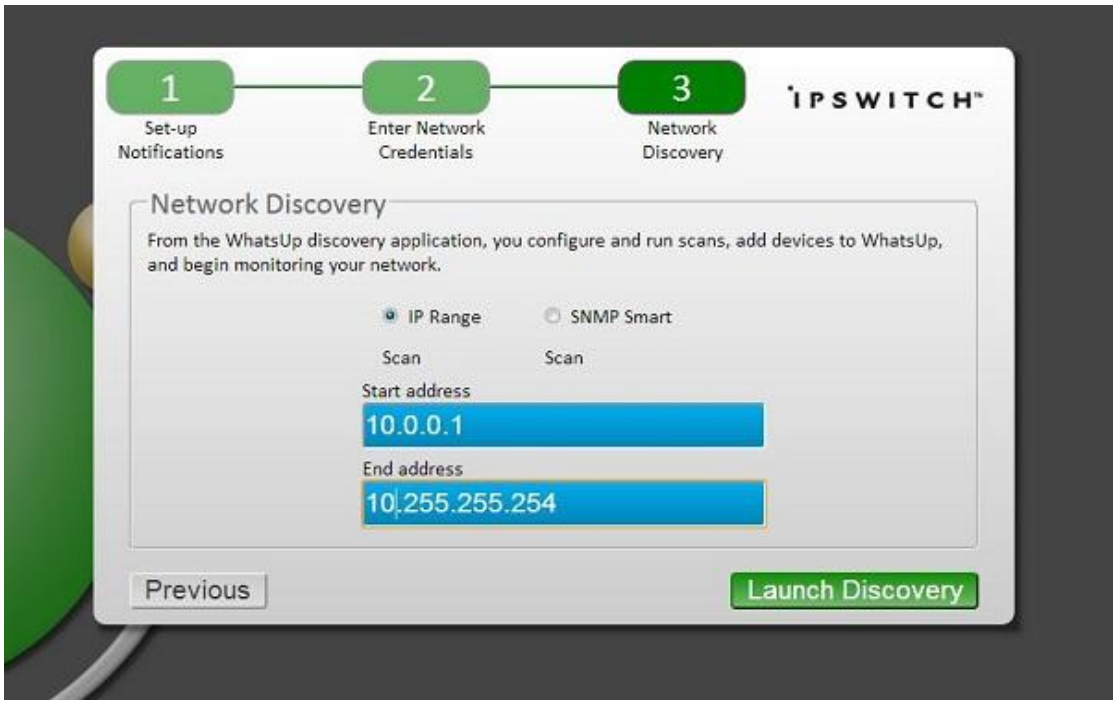
Παρακάτω, υπάρχουν κάποιες εικόνες (screenshots) από τη λειτουργία του προγράμματος **Ipswitch Whatsup Gold** για γίνει κατανοητή η απεικόνιση ενός δικτύου και η διαχείριση των συσκευών αυτού.



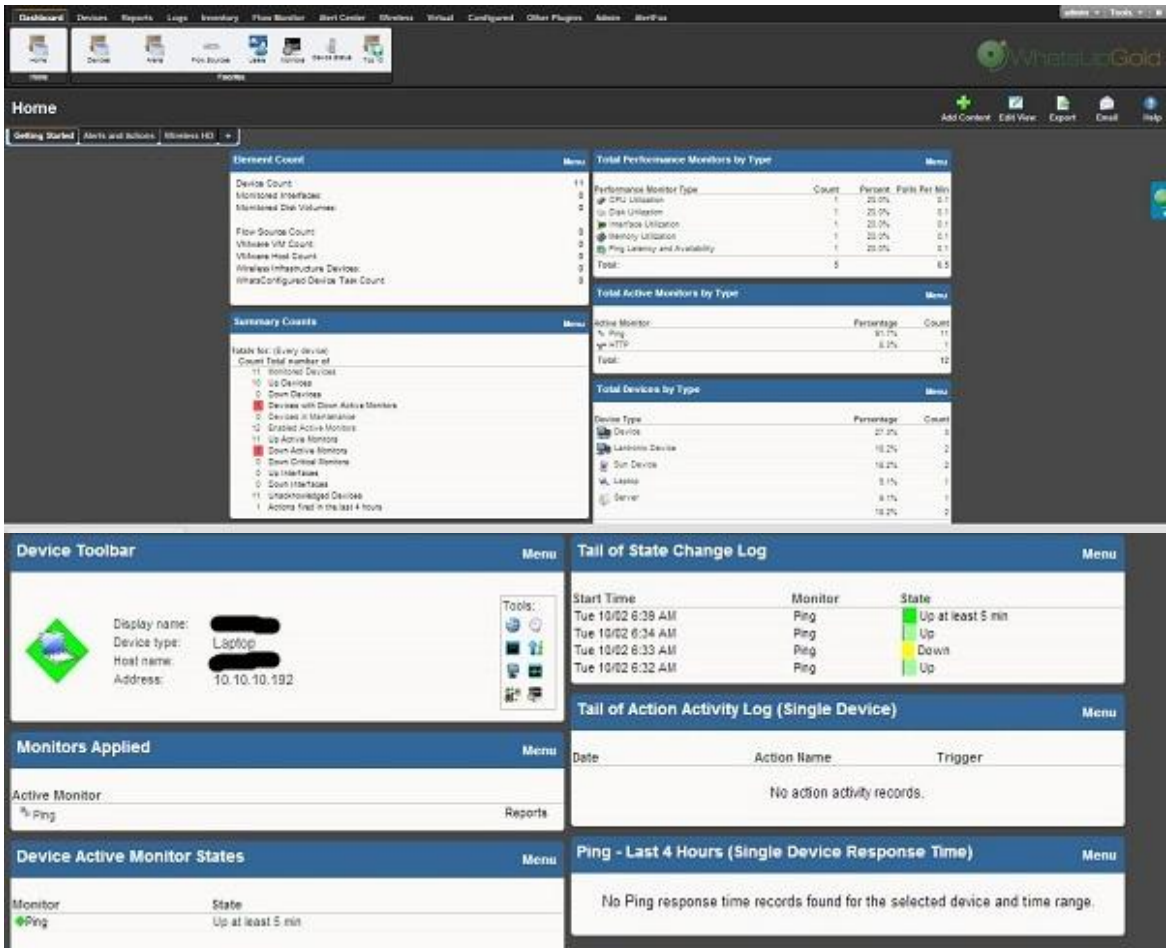
Εικόνα 4.1: Εγκατάσταση του λογισμικού



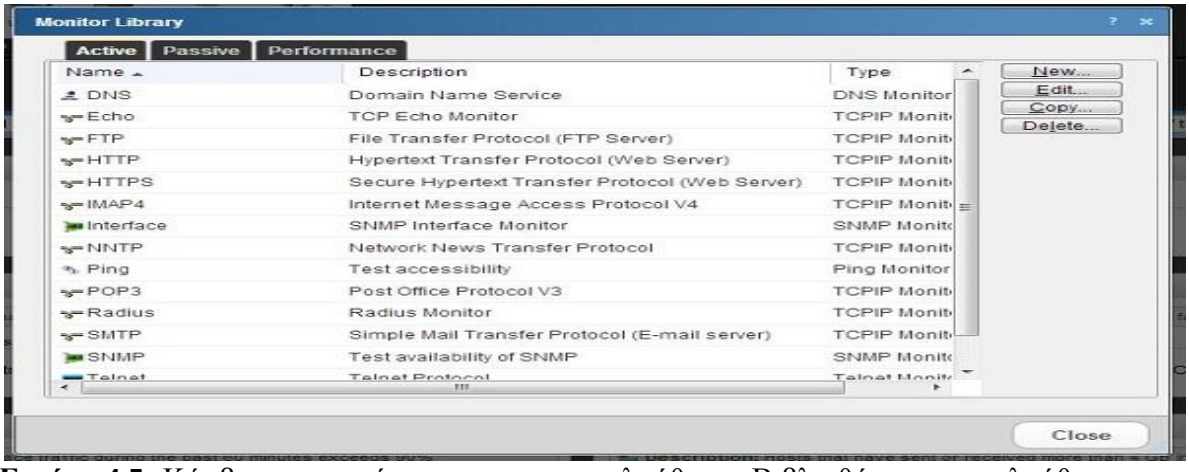
Εικόνα 4.2: Προστασία στοιχείων με κωδικό.



Εικόνα 4.3: Ρύθμιση επιλογών δικτύου.

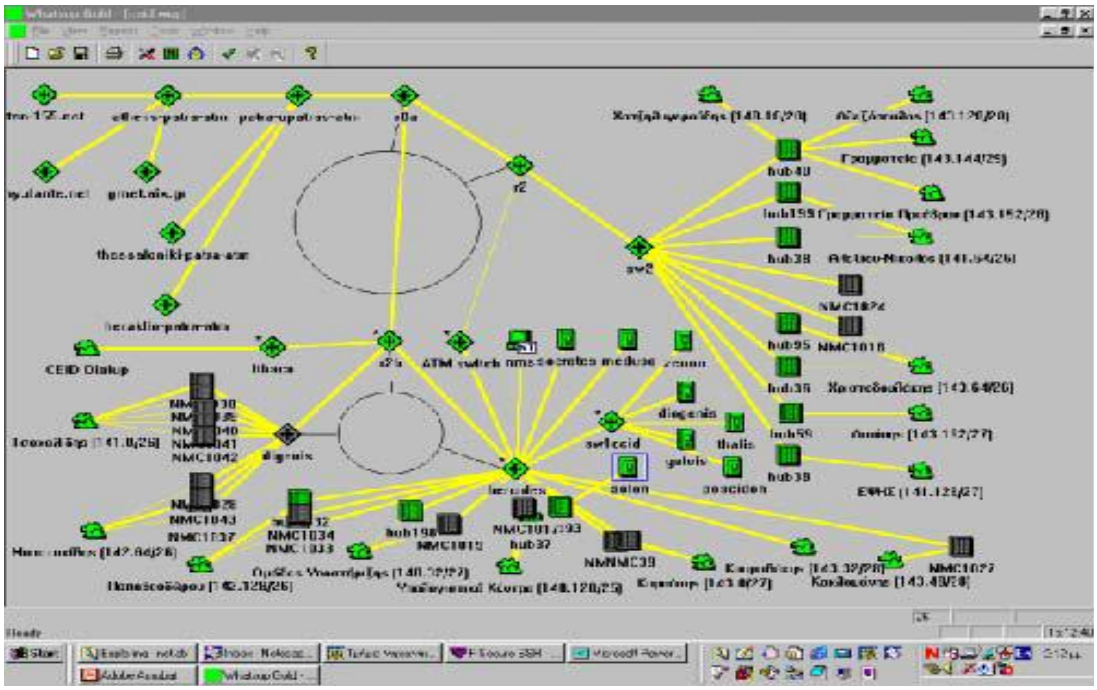


Εικόνα 4.4:Αρχική σελίδα επιλογών για το πρόγραμμα παρακολούθησης. Επίσης μας παρέχει οθόνες εφαρμογών που παρακολουθούμε τις διεργασίες που γίνονται, οθόνη παρακολούθησης των ενεργών μελών και παρακολούθηση επιπρόσθετων συνδεδεμένων συσκευών.

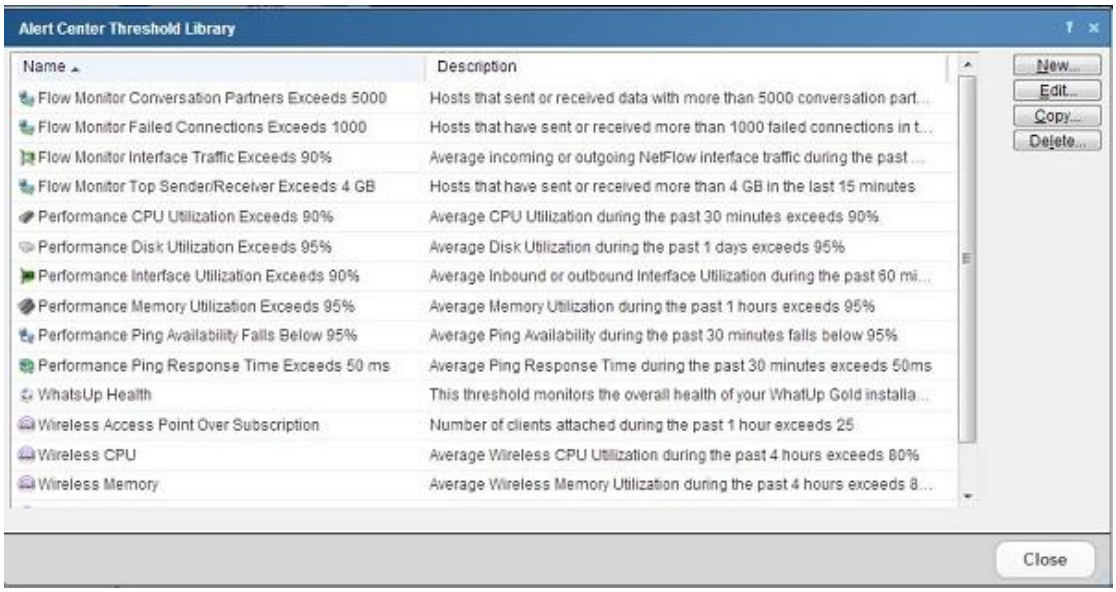


Εικόνα 4.5: Κόμβοι που παρέχονται για παρακολούθηση. Βιβλιοθήκη παρακολούθησης που μας δίνει την δυνατότητα να δούμε το όνομα των κόμβων την περιγραφή τους και τον τύπο τους.

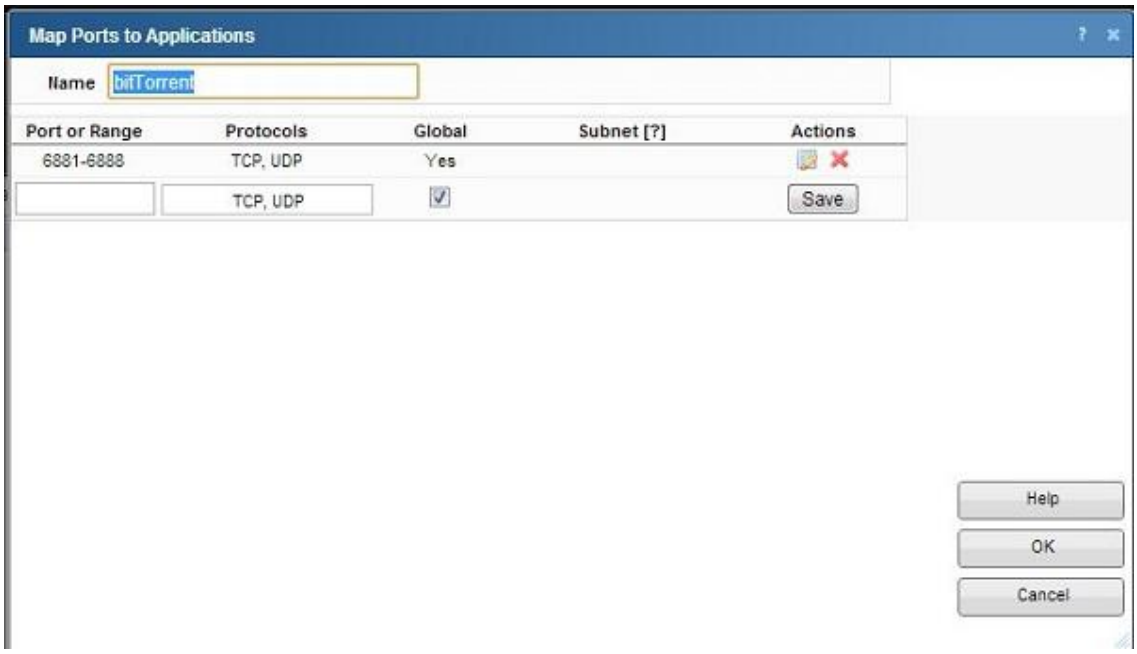
Εικόνα 4.6: Εισαγωγή συσκευών με τις διευθύνσεις τους τον ρόλο τους και την κατάσταση τους.



Εικόνα 4.7 Σχηματική απεικόνιση του δικτύου. Από εδώ μπορούμε να παρατηρήσουμε την διαγραμματική απεικόνιση του δικτύου μας, ποιες συσκευές είναι άμεσα συνδεδεμένες μεταξύ τους, ποιά είναι κεντρικά σημεία μεγάλης σημαντικότητας και επιπροσθέτως σε ποιο σημείο του δικτύου μας έχουμε πρόβλημα και ποιους σταθμούς επηρεάζει.



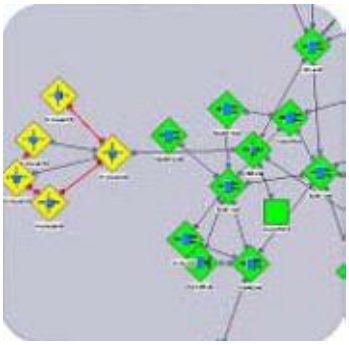
Εικόνα 4.8: Παράθυρο βιβλιοθήκης αναφοράς βλαβών. Στο παράθυρο αυτό μπορούμε να δούμε τα σημεία του δικτύου μας που έχουν πρόβλημα και αναφορά του προβλήματος αυτού.



Εικόνα 4.9: Παράθυρο αναφοράς προβλήματος και βοήθειας.

4.3 ΠΛΑΤΦΟΡΜΑ OPENVIEW

HP OpenView Network Node Manager



4.3.1 ΓΕΝΙΚΕΣ ΛΕΙΤΟΥΡΓΙΕΣ.

- διαχείριση δικτύων όλων των μεγεθών
- αυτόματη ανακάλυψη δικτύων
- ανάλυση προβλήματος αιτίας ρίζας
- απευθυνόμενες όψεις δικτύων

Πρόκειται για μία πανίσχυρη πλατφόρμα διαχείρισης δικτύου μέσω του πρωτοκόλλου IP βασισμένη στα δεδομένα του πρωτοκόλλου SNMP.

Τα προγράμματα OpenView Network Node Manager και Network Node Manager Extended Topology παρέχουν σε οποιαδήποτε διοικητική ομάδα τη δυνατότητα να εξετάσουν και να αντιμετωπίσουν τις βασικές προκλήσεις επιχειρήσεων και δικτύων.

Τα δύο αυτά προγράμματα περιλαμβάνουν ευφυή διαγνωστικά για τα δίκτυα. Αυτή η νέα προσέγγιση στην ανάλυση ρίζας-αιτίας (root-cause) περιλαμβάνει ένα σύνολο εύχρηστων εργαλείων για να βοηθήσει στον προσδιορισμό και την επίλυση καταστάσεων προτού αυτές γίνουν προβλήματα.

Τα ευφυή διαγνωστικά δικτύων μπορούν να φέρουν σε πέρας προηγμένες δυνατότητες κάλυψης για τη μείωση γεγονότων δικτύων, την ανάλυση ρίζας-αιτίας και μια νέα διοικητική έννοια της ανάλυσης καταστάσεων, η οποία καθορίζει ενεργά την ομαλή λειτουργία των πρωτοκόλλων δικτύων και των δικτύων σύνθετων δομών.

Περιλαμβάνει επίσης συσχετισμούς “out of the box” για την ενισχυμένη ανάλυση ρίζας-αιτίας και το νέο συνθέτη συσχετισμού για να προσαρμόσει εύκολα το OpenView στις ανάγκες του καθενός.

Το OpenView NNM μπορεί να λειτουργήσει σε λειτουργικά συστήματα Windows NT/2000, Solaris 7.0, 8.0 καθώς και σε UX 11.0 και UX 11i της Hewlett-Packard.

4.3.2 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΑΙ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΟΥ ORNVIEW NNM -

προηγμένη ανάλυσης ρίζας-αιτίας

- Ευφυή διαγνωστικά για τα δίκτυα (ταυτότητα δικτύων) για προηγμένη ανάλυση ρίζας-αιτίας, μείωση γεγονότων, δυνατότητα ανίχνευσης λαθών επιπέδου 2 και 3.
- Δυνατότητα διασύνδεσης web μορφής με δυναμική εμφάνιση της κατάστασης των διαφόρων συσκευών.

- Ιδανικό για διαχειριστές δικτύων. Με τη βοήθεια του, αποτρέπουν προβλήματα προτού αυτά εμφανιστούν.
- Οι διαχειριστές είναι σε θέση να χειριστούν το δίκτυο πιο έξυπνα, γεγονός που ωφελεί γενικά την καλύτερη λειτουργία του δικτύου και μειώνει το κόστος.
- Όταν μια σημαντική συσκευή αποτυγχάνει, η μηχανή συσχετισμού γεγονότος εξερευνά τη διαδρομή που προκάλεσε το συγκεκριμένο γεγονός για να επισημάνει την αρχική αιτία της αποτυχίας.

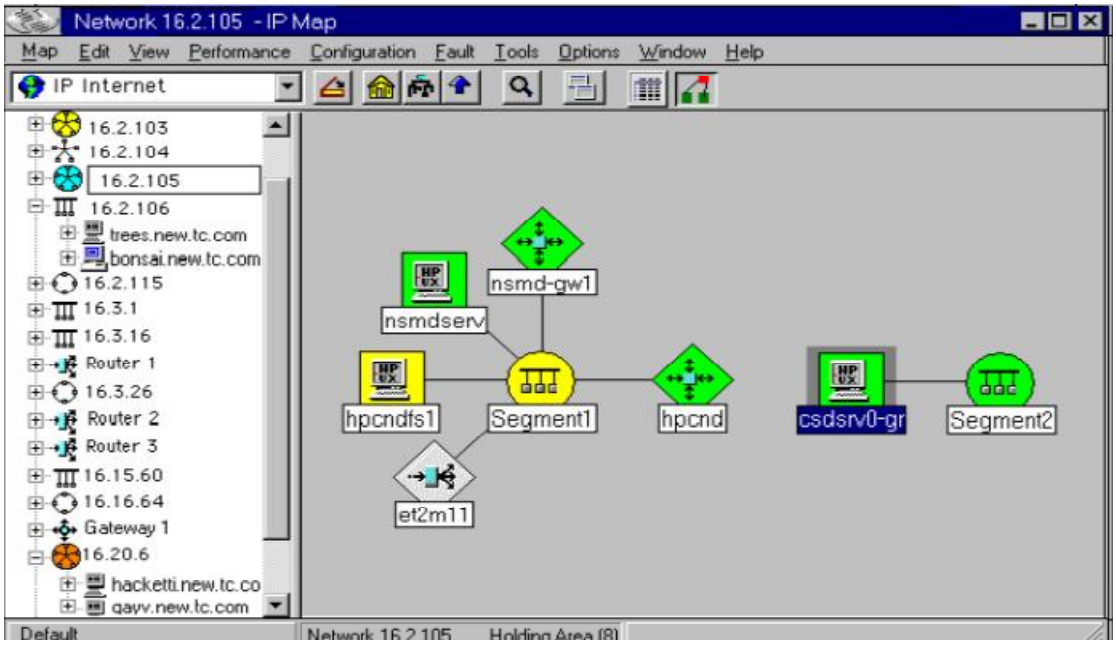
Ανακάλυψη, χάρτες και όψεις

- Η ακριβής ανακάλυψη του στρώματος 3 και του ετερογενούς στρώματος 2 επηρέασε σημαντικά τα δίκτυα Ethernet και το ATM, τα LANs και τα WANs.
- Οπτική χαρτογράφηση των συσκευών στρώματος 2 και 3, συνδετικότητα και σχέσεις.
- Παρέχει γραφική μορφή όψης δικτύου.
- Ανακαλύπτει τις συσκευές δικτύου και παρέχει έναν χάρτη για να επεξηγήσει τη δομή του δικτύου και τη κατάσταση των συσκευών και των διαφόρων τμημάτων του δικτύου τμημάτων μνήμης.
- Δυναμικές όψεις για:
  - συσκευές και τύπους συσκευών
  - πρωτόκολλα που υπάρχουν πάνω από το συντομότερο ανοικτό μονοπάτι δικτύων (Open Shortest Path First), Hot Standby Router Protocol (HSRP) και IPv6
  - VLANs (εικονικά τοπικά δίκτυα)
  - σύνθετες σχέσεις μεταξύ συσκευών σαν τα πλέγματα και τους συγκεντρωτικούς κόμβους και άλλους σχηματισμούς υψηλής διαθεσιμότητας, συμπεριλαμβανομένου του HSRP της Cisco
  - συνδυασμοί όπως VLANs που τρέχουν πέρα από το στρώμα 2 όσον αφορά την τοπολογία

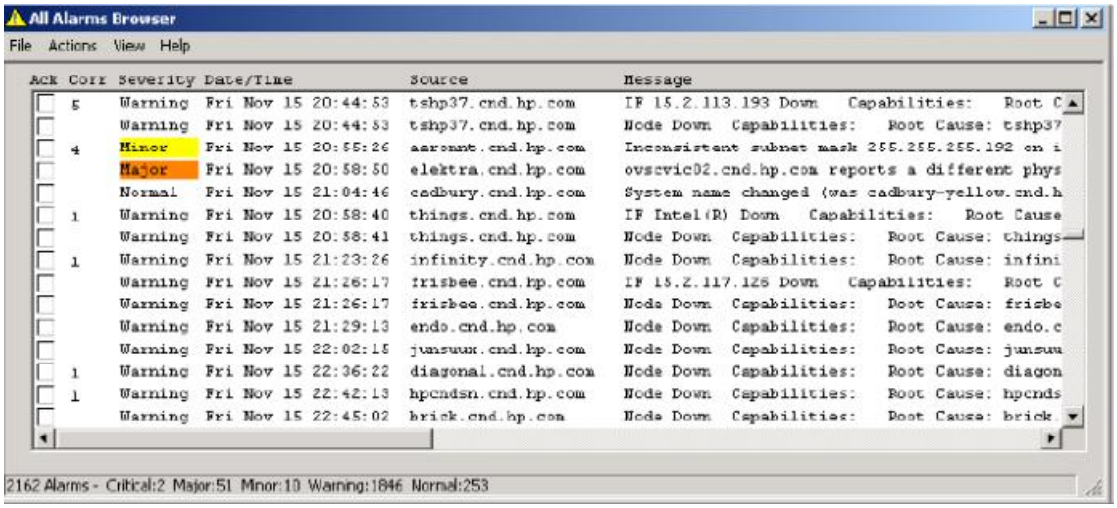
Συλλογή στοιχείων, αποθήκευση και υποβολή εκθέσεων

- Ευφυής συλλογή στοιχείων
- “Out of the box” αναφορές για το δυναμικό προγραμματισμό ανάπτυξης
- Τεχνολογία συσχετισμού γεγονότος
- Δυναμική διαχείριση δικτύου με την υποβολή αναφορών αποθήκευση δεδομένων
- Δυνατότητες κάλυψης λαθών με προγραμματιζόμενα backup
- Εξελιξιμότητα: οι σταθμοί συλλογής που λειτουργούν σε Windows NT και UNIX μπορούν να διανεμηθούν σε όλο το περιβάλλον έτσι ώστε τα δεδομένα να μπορούν να συλλεχθούν τοπικά και να διαβιβαστούν σε έναν ή περισσότερους σταθμούς διαχείρισης

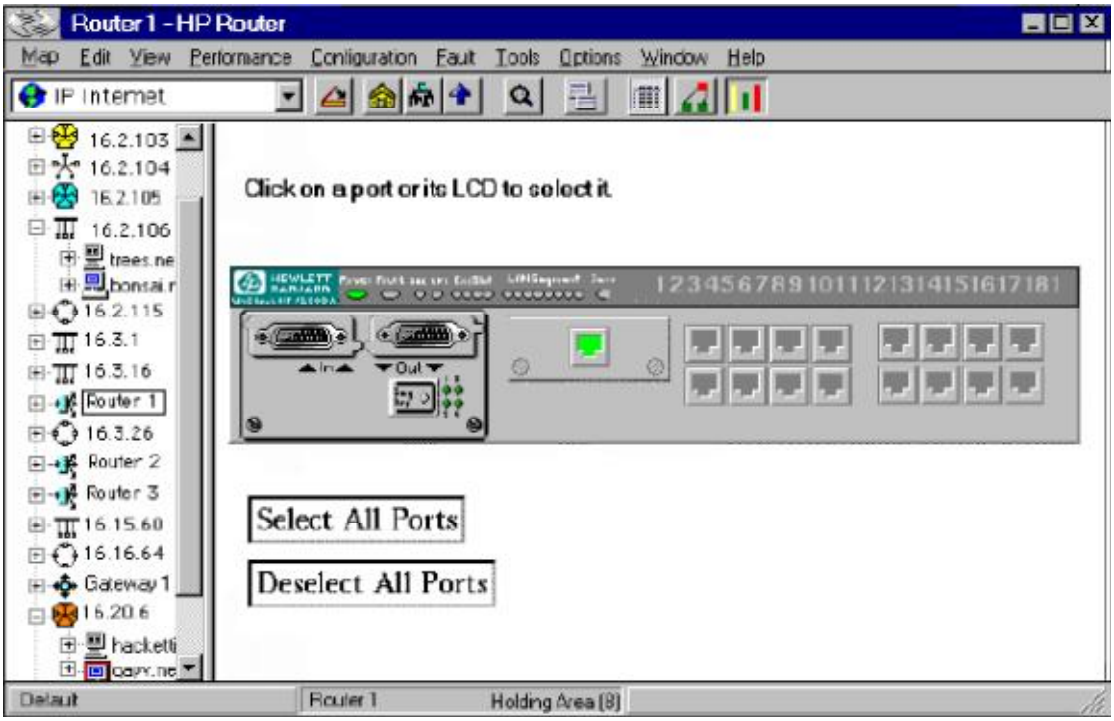
Μια ευρεία σειρά υποστηριζόμενων συσκευών και πρωτοκόλλων συμπεριλαμβανομένων των IPv6, OSPF, HSRP



Εικόνα 4.10 Σχηματική απεικόνιση του δικτύου
(HP Openview Network Node Manager)



Εικόνα 4.11 Παράδειγμα μηνυμάτων αναφοράς βλαβών και λαθών
(HP Openview Network Node Manager)



Εικόνα 4.12: Διαχείριση μιας συσκευής router
(HP Openview Network Node Manager)

4.3 ΠΛΑΤΦΟΡΜΑ TIVOLI NET VIEW FOR z/OS.

Maintain the highest degree of availability of your System z™ networks.

Το NetView παρέχει αυτοματοποίηση, και στο δίκτυο και στα συστήματα διαχείρισης για την αντιμετώπιση των απαίτηση του σήμερα για την ευελιξία της επιχείρησής σας στο System z

Παρέχει βασικές δυνατότητες και προηγμένες λειτουργίες που σχετίζονται με τη δικτύωση τον αυτοματισμό, την ενισχυμένη εταιρική ολοκλήρωση,(πελατών-ανά-τιμή χρόνου), την ευκολία στη χρήση, καθώς και λειτουργίες διαχείρισης που λειτουργούν σε συνεργασία με άλλα προϊόντα που υποστηρίζει ετερογενή δίκτυα, που περιλαμβάνουν τόσο σε TCP/IP και υποστηρίζει την αλλαγή του συστήματος και τις απαιτήσεις δικτύου που υπάρχουν στο σύστημα z. NetView. Παρέχει τη δυνατότητα μέσα από μια ενιαία κονσόλα γι να διαχειριστείτε ολόκληρο το δίκτυο

NetView Tivoli για z/OS V6.1: Η τελευταία έκδοση του NetView εστιάζεται στο ενισχυμένο πρόβλημα προσδιορισμού και διαχείρισης ώστε να αυξήσει τις λειτουργίες απόδοσης και αποτελεσματικότητας. Ακόμα παρέχει υψηλή διαθεσιμότητα και αυτοματισμού για τη βελτίωση της συνολικής διαθεσιμότητας του συστήματος. Έχει νέες λειτουργίες Canzlog που παρέχουν ταχύτερη επίλυση προβλημάτων με περιήγηση στο αρχείο καταγραφής του δικτύου του συστήματος και την ενίσχυση της αυτοματοποίησης με το νέο ενοποιημένο μήνυμα καταγραφής ικανοτήτων. Επιπροσθέτως παρέχει βελτιωμένη διάγνωση και διαχείριση προβλημάτων με το νέο πακέτο παρακολούθησης και ανάλυσης.

4.3.1 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΟΦΕΛΗ.

Ενοποιημένο αρχείο καταγραφής (Canzlog) δίνει την δυνατότητα αναζήτησης περιλαμβάνοντας ενισχυμένη πρόσβαση σε χαρακτηριστικές ιδιότητες μηνυμάτων καθώς και σε μεμονωμένα μηνύματα. Ισχυρό φιλτράρισμα εφαρμόζεται εύκολα ώστε να ανακτήσετε τα αρχεία καταγραφής που βασίζονται σε μια μεγάλη ποικιλία από παράγοντες, όπως το χρονικό εύρος, JobName, JobID, αναγνωριστικό μηνύματος, τομέα, ταυτότητες άδεια και ομάδες, διακριτικό αυτοματισμού, ρυθμιζόμενα χαρακτηριστικά χρήστη , ή συνδυασμούς αυτών των αξιών.

Ίχνος πακέτου: Η NetView IP ίχνος πακέτου συνάρτηση επιτρέπει την ανάλυση περιόδου λειτουργίας ανίχνευσης πακέτου, μεμονωμένες συνδέσεις μπορεί να πέσουν και μπορούν να αποθηκευτούν τα δεδομένα ανίχνευσης του πακέτου για μεταγενέστερη ανάκτηση ή περαιτέρω ανάλυση.

PKTTRACE εντολών μπορεί να χρησιμοποιηθεί μέσω της εντολής γραμμή, χρονόμετρο, ή αυτόματης έναρξης και διακοπής ίχνους και τα κριτήρια επιλογής ανίχνευσης.

Υποδίκου IP και z/OS: Updated MultiSystem Manager ενοποιείται με OMNibus Tivoli της IBM και Tivoli NetWork Manager. Ο παράγοντας MultiSystem Manager για OMNibus Tivoli της IBM και IBM Tivoli Network Manager στην NetView συγκεντρώνει τις απόψεις και τις σχέσεις και φορτώνει στο NetView για την z/OS. Έτσι έχουμε προσωρινή αποθήκευση δεδομένων για τη διαχείριση αντικειμένου πόρων (RODM). Οι πόροι αυτοί μπορούν στη συνέχεια να προβληθούν και να διαχειριστούν από την Κονσόλα διαχείρισης του NetView (NMC).

Υποστήριξη για zEnterprise: νέα διεπαφή και τους τύπους καναλιού OSA ειδικά για την πλατφόρμα zEnterprise. Αυτά τα νέα στοιχεία είναι διαθέσιμα για εμφάνιση μέσω της κονσόλας διαχείρισης NetView, Tivoli Enterprise κονσόλα ® σε χώρους εργασίας.

Υποστήριξη για συνεχή διαθεσιμότητα και εύρεση ενεργών λύσεων:. Το πρόγραμμα NetView παρέχει τη δυνατότητα παρακολούθησης της κατάστασης του φόρτου εργασίας και άλλα διαχειριζόμενα στοιχεία που έχουν οριστεί υπό προϋποθέσεις.Αναλύουν τα δεδομένα σε ένα πακέτο ανίχνευσης για τον προσδιορισμό πιθανών δικτυακών προβλημάτων του συστήματος.

Η εντολή PKTTRACE απλοποιεί την ιχνογράφηση ξεκινώντας αυτόματα τα στοιχεία που απαιτούνται ίχνος. Όμως είναι καλύτερα να χρησιμοποιούνται z/OS δεδομένα προσωρινής αποθήκευσης RODM.

Παροχές που παρέχουν βελτιωμένη ορατότητα των δραστηριοτήτων του συστήματος, καθώς και ταχύτερη επίλυση του προβλήματος. Μειώνει σημαντικά το χρόνο που απαιτείται για την αναγνώριση του προβλήματος και την διάγνωση. Αυτή η ενσωμάτωση επιτρέπει την καλύτερη προβολή, δημιουργία και εμφάνιση του δικτύου σχέσεων. Χρησιμοποιώντας το DLA παρέχει παρακολούθηση και ορατότητα στο σύστημά σας για βελτιωμένη κατανομή και αξιοποίηση z/OS. Περνώντας το zEnterprise παρέχει νέες δυνατότητες υβριδικών όπως μείωση χρόνου ανάκτησης σε περιπτώσεις καταστροφών.

Το Tivoli NetView ® για z/OS ® παρέχει τις βασικές δυνατότητες και προηγμένες λειτουργίες για να σας βοηθήσει να συντηρήσετε τον υψηλότερο βαθμό διαθεσιμότητας των δικτύων zTM του συστήματος. Προσφέρει ένα ευρύ σύνολο από εργαλεία για τη διαχείριση και τη σύνθετη διατήρηση, πολλαπλών προμηθευτών·, multiplatform δικτύων και συστημάτων από ένα σημείο ελέγχου. Επίσης, παρέχει λειτουργίες διαχείρισης που λειτουργούν σε συνεργασία με άλλα προϊόντα.

Γενικά οι λειτουργίες και δυνατότητες του NetView για z/OS V6.1: IBM ® Tivoli ® συνοψίζονται ως εξής:

- ανάλυση και αυτοματοποίηση συστήματος z/OS, NetView και εργασία καταγραφής μηνυμάτων μέσω ενός ενοποιημένου αρχείου καταγραφής (Canzlog) για πραγματικό χρόνο και αρχειοθετημένα μηνύματα.
- Ενσωματωμένη ανάλυση των δεδομένων ανίχνευσης πακέτων που μειώνει το χρόνο διάγνωσης.
- Υποστήριξη για υλικό zEnterprise.
- Υποστήριξη για δυναμική εικονική IP διεύθυνση άμεσης αναμονής διανομής.
- Ολοκληρωμένο περιβάλλον με IBM Tivoli Network Manager.
- Βελτιωμένη NetView βιβλιοθήκη προσαρμογέα (DLA) για sysplex, ω/OS συστημάτων και δεδομένων IP.
- Υποστήριξη για λύση στην συνεχή διαθεσιμότητα.
- Χρηστικότητα και συνέπεια ενημέρωσης για την Κονσόλα διαχείρισης του NetView.
- Ενημέρωση παραμέτρων στυλ. Χρήση NetView για να διαχειριστείτε τα συστήματα mainframe σας, στα δίκτυα IP και το κλειδί των υπηρεσιών αυτών των συστημάτων και δικτύων υποστήριξης. Επίσης παρέχει νέες δυνατότητες που ταιριάζει με την εξέλιξη στο περιβάλλον, και ενισχύει τους δεσμούς με την Tivoli υπηρεσία διαχείρισης χαρτοφυλακίου, επιτρέποντάς σας να αποκτήσετε μεγαλύτερη ορατότητα, έλεγχο και αυτοματοποίηση πάνω από το περιβάλλον σας.

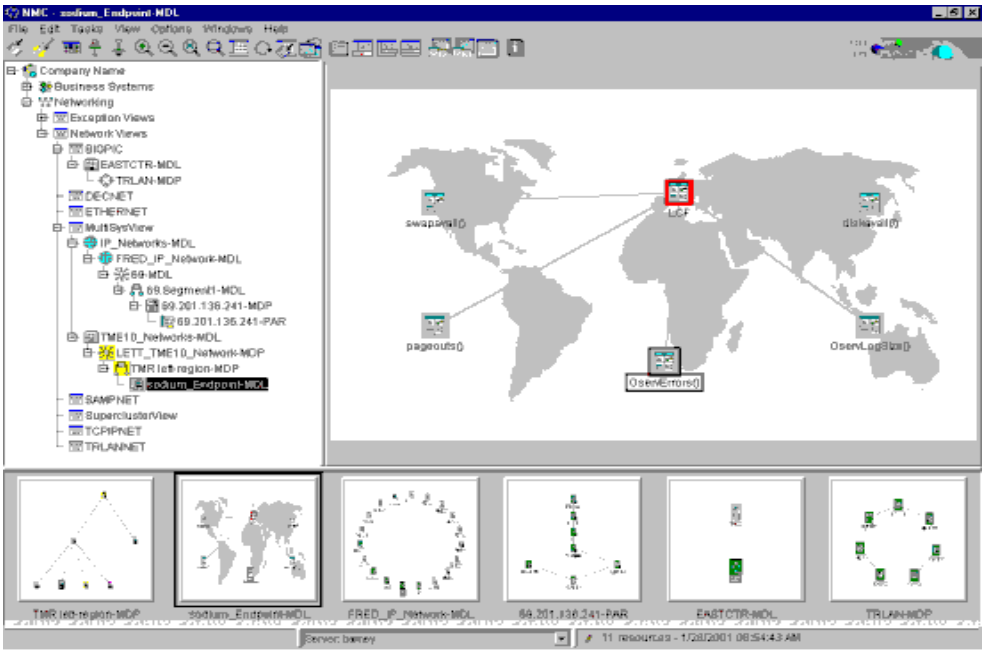
Η αυτοματοποίηση υποστήριξης έχει επεκταθεί για να απλοποιήσετε τις παραμέτρους αυτοματισμού, τη βελτίωση της διαθεσιμότητας του συστήματος και μείωση των λειτουργικών δαπανών, παρέχοντας μια ενιαία, συνεκτική μέθοδο μέσω της οποίας μπορούν να αυτοματοποιηθούν όλα τα μηνύματα του δικτύου.

Το λογισμικό Tivoli NetView παρέχει διαχείριση για το περιβάλλον mainframe (συμπεριλαμβανομένου του λειτουργικού συστήματος και επικοινωνιών διακομιστών) με βελτιώσεις για την καλύτερη διαχείριση του δικτύου σας , συμπεριλαμβανομένων της

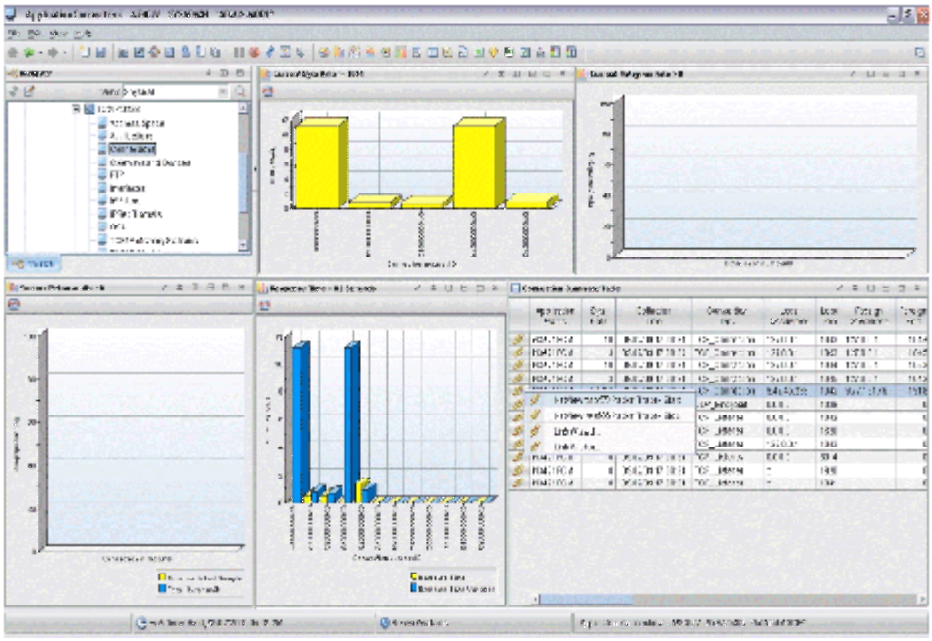
αποτελεσματικότερης διάγνωσης προβλημάτων και βελτιωμένη διαχείριση δικτύου end-to-end μέσω αυστηρότερης ολοκλήρωσης με το OMNIbus Tivoli της IBM και του διαχειριστή του δικτύου.

Η διαχείριση εταιρικού NetView διαδραματίζει καίριο ρόλο στις ενέργειες συνεχής διαθεσιμότητας. Αυτή η λύση αυξάνει σημαντικά το σύστημα και το φόρτο εργασίας ενώ επίσης μειώνει το χρόνο ανάκτησης σε περιπτώσεις καταστροφών.

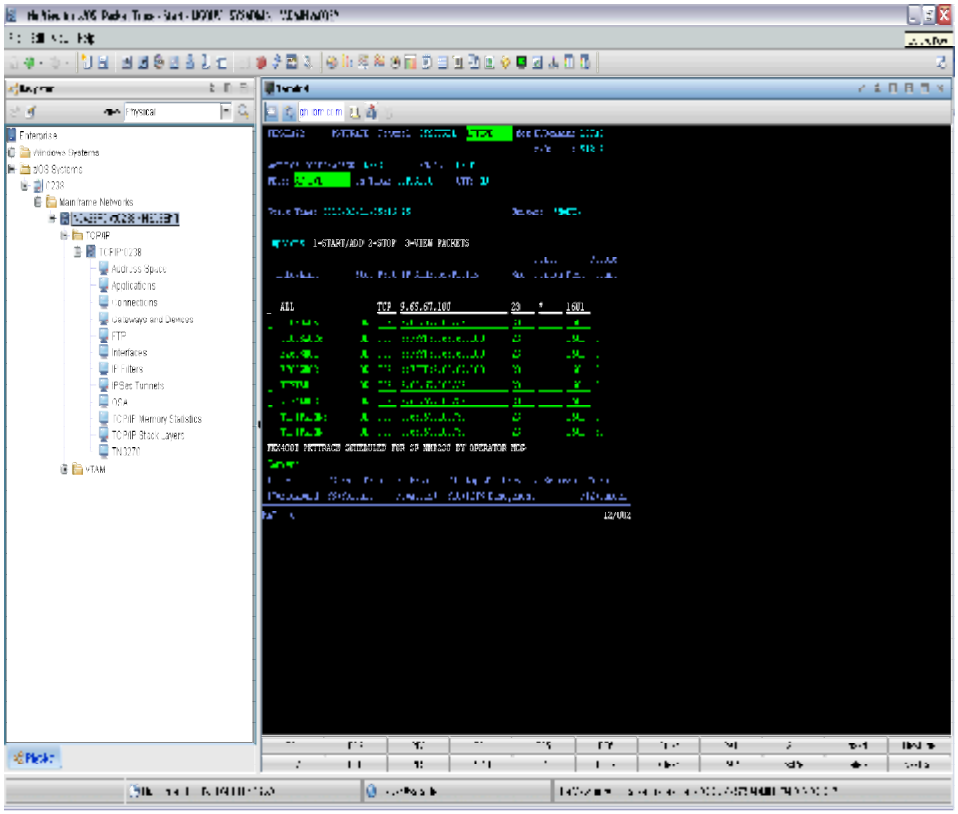
NetView για z/OS έχει σχεδιαστεί για: • βελτίωση του δικτύου αποτελεσματικότητας και αύξηση του συστήματος διαθεσιμότητας • μείωση ή την εξάλειψη της ανάγκης για επέμβαση χειριστή για αντιμετώπιση προβλημάτων • με τα μηνύματα συστήματος διαχειρίζεστε μεγαλύτερα δίκτυα, περισσότερους πόρους και περισσότερα συστήματα με λιγότερους πόρους και προσωπικό (ο έλεγχος μπορεί να ενοποιείται σε ενιαία κονσόλα αν είναι επιθυμητό).



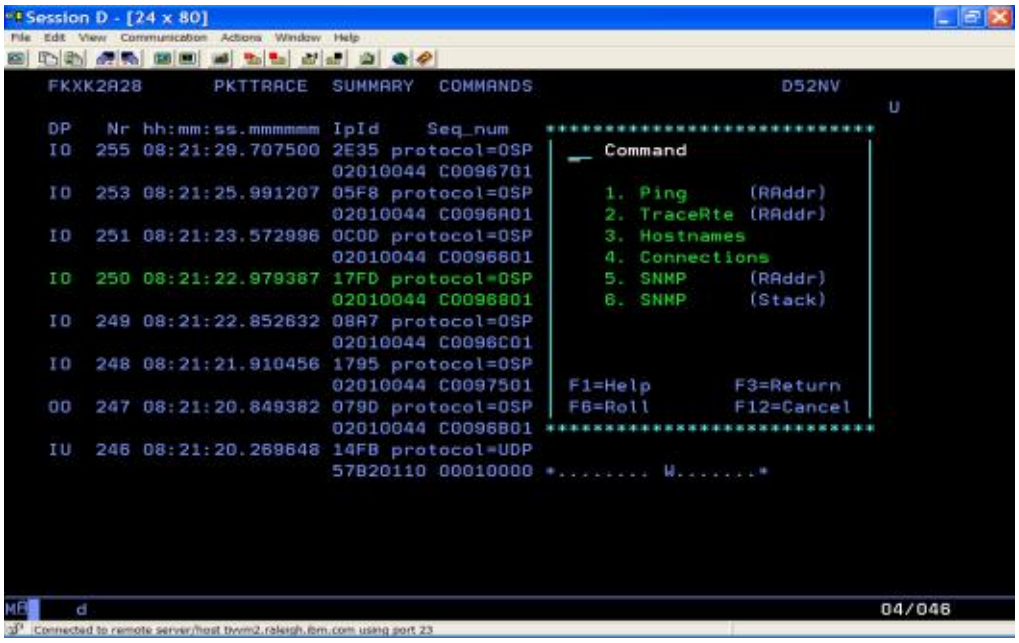
Εικόνα 4.13 Τοπολογίες δικτύων που περιλαμβάνει το λογισμικό. Κατηγοριοποίηση δικτύου και εικονική προσομοίωση.



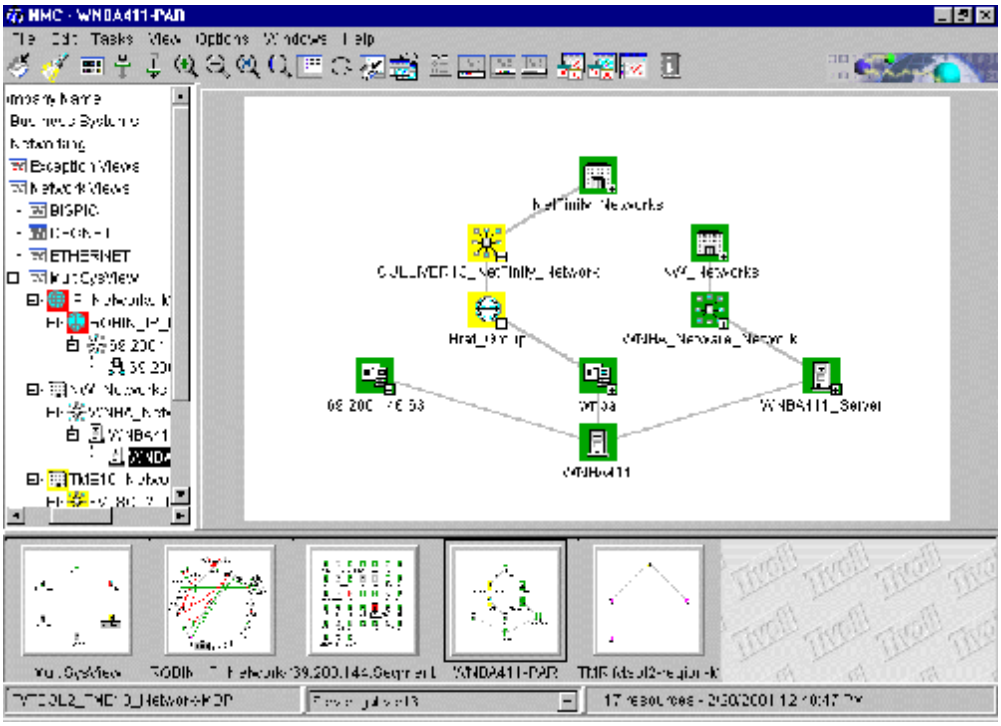
Εικόνα 4.14: Πίνακας ελέγχου αποτελεσμάτων από την παρακολούθηση του δικτύου. Στατιστικά στοιχεία κίνησης του δικτύου για την ποσοτική λειτουργία του.



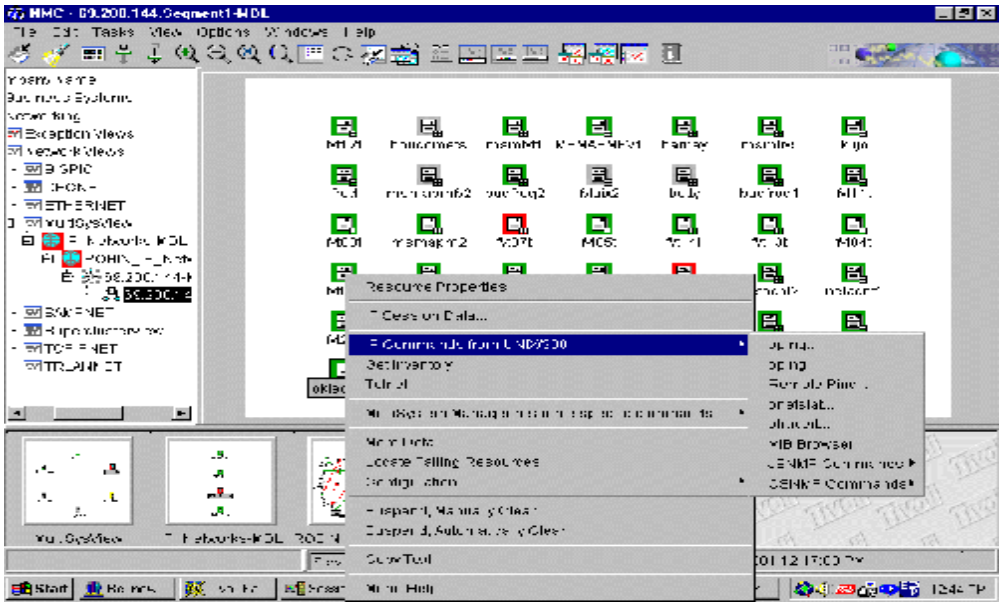
Εικόνα 4.15: Έλεγχος κόμβων δικτύου με εμφάνιση των διευθύνσεων τους.



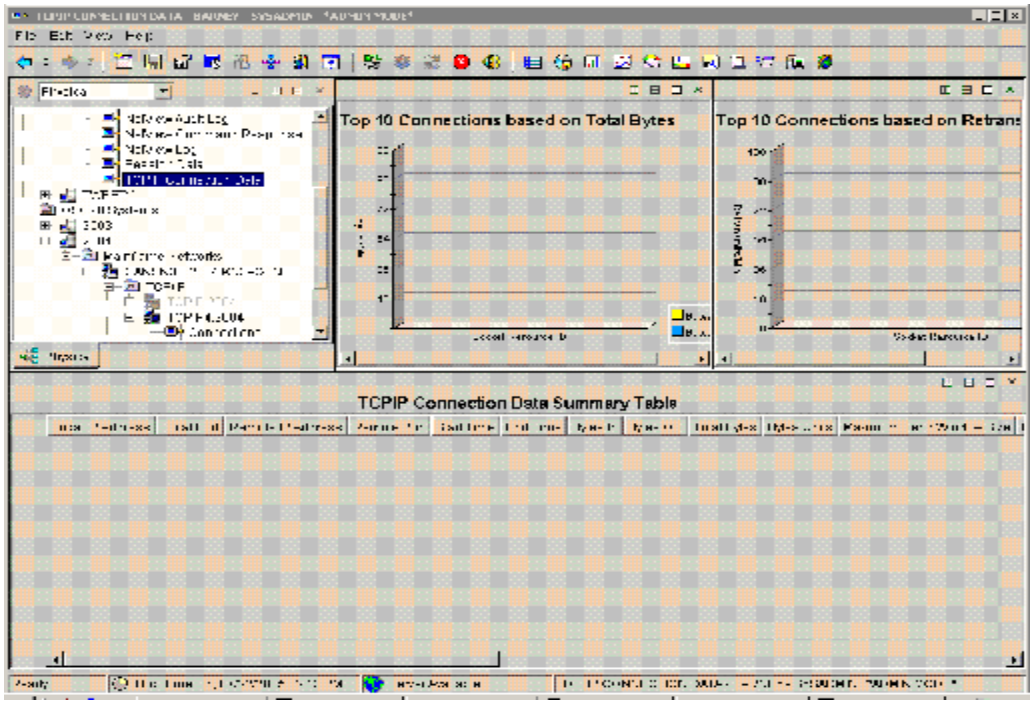
Εικόνα 4.16: Αναφορά του PKTTRACE. Χρόνος στιγμιοτύπων.



Εικόνα 4.17: Αρχική σελίδα επιλογών. Τρόπος σύνδεσης των κόμβων και απεικόνιση του ανάλογα με τις ανάγκες μας, με περισσότερα η λιγότερα στοιχεία.



Εικόνα 4.18:Επιλογές για την ευκολότερη εύρεση των στοιχείων που επιθυμούμε. Αλλαγή επίλογών των κόμβων ή επέκταση τους για περισσότερες χρήσεις.



Εικόνα 4.19:Αποτελέσματα κατάστασης δικτύου

4.4 ΣΥΓΚΡΙΣΗ OPEN VIEW NNM – TIVOLI NETVIEW.

Και τα δύο παραπάνω προϊόντα παρέχουν network inventory, διαχείριση εξαιρέσεων, και δυνατότητα σύνταξης αναφορών, καθώς και διαχείριση απόδοσης και πρόβλεψη πιθανών προβλημάτων.

Παρ' όλα αυτά έχουν και κάποια αρνητικά σημεία όπως: έλλειψη βάσεων δεδομένων, διαχείριση εφαρμογών, μεταφορά φωνής μέσω πρωτοκόλλου IP (voice over IP). Επίσης δεν υποστηρίζουν εργαλεία ανίχνευσης εγκατάστασης κλήσης (call-setup) και όσον αφορά την ασύρματη κάλυψη, αυτή περιορίζεται στο πρωτόκολλο SNMP MIB II.

Για τη σύγκριση πρέπει να λάβουμε υπόψη παράγοντες όπως: υπερφόρτωση συστήματος ώστε να έχουμε ομαλή λειτουργία του προγράμματος, κόστος αγοράς και συντήρησης, καθώς και κατά πόσο αυτό επιλύει τα ζητούμενα προβλήματα. Για παράδειγμα αν θέλουμε απλά να ελέγχουμε την κατάσταση και διαθεσιμότητα 300 – 400 κόμβων ενός δικτύου τα παραπάνω προγράμματα είναι υπερβολικά. Πιο κατάλληλο θα ήταν ένα πρόγραμμα σαν το WhatsUp Gold της Ipswitch που αναλύσαμε παραπάνω.

Αν πάλι μας ενδιαφέρει ο έλεγχος ενός μεγαλύτερου δικτύου (10000 κόμβοι) τότε το OpenView υπερέχει του NetView όσον αφορά την τιμή. Και τα δύο προγράμματα έχουν πολύ καλή δυνατότητα αναφορών μέσω web αλλά, το NetView δεν παρουσιάζει αρκετά ισχυρή διαχείριση εξαιρέσεων σε σχέση με το OpenView.

Παρακάτω δίνουμε έναν συγκριτικό πίνακα τιμών και αξιολόγησης των δύο προγραμμάτων σύμφωνα με το περιοδικό Network Computing:

	Weight	Tivoli Systems NetView 6.0.1	HP OpenView Network Node Manager 6.1
EXCEPTION HANDLING	25%	3	3.5
PERFORM. REPORTING	25%	3.5	4
ADMINISTRATIVE EASE	20%	4	4
INVENTORY	20%	3	3
PRICE AND MAINTENANCE	10%	3	5
TOTAL SCORE		3.33	3.78
		C+	B

	HP OpenView Network Node Manager 6.1	Tivoli Systems NetView 6.0.1
Price for 1,000 nodes	$13,176	$6,200
Price for 10,000 nodes	$20,394	$62,000
Annual maint. fee (as percentage of purchase price)	20% with first year included in price	15% with first year included in price

Εικόνα 4.20: Συγκριτικός πίνακας λογισμικών HP OPENVIEW NETWORK NODE MANAGER και TIVOLI SYSTEM S NETVIEW 6.0.1

\

ΚΕΦΑΛΑΙΟ 5

5.1 ΣΥΜΠΕΡΑΣΜΑΤΑ

Στο τελευταίο κεφάλαιο της εργασίας αυτής παραθέτονται τα αποτελέσματα και τα συμπεράσματα που εισπράχθηκαν μέσα από την έρευνα.

Στο πρώτο κεφάλαιο αναφέρθήκαμε στο τι χρειάζεται ένα σύστημα διαχείρισης δικτύου, τι είναι διαχείριση δικτύου, τα είδη των δικτύων, ο σκοπός τους όπως επίσης επεξηγούνται έννοιες που σχετίζονται με τα πρωτόκολλα και τις αρχιτεκτονικές διαχείρισης δικτύων υπολογιστών (Management of Computer Networks). Αναφέρθηκαν ακόμα τα Μοντέλα διαχείρισης, οι Αρχιτεκτονικές διαχείρισης, οι Διαχειρίσεις Απόδοσης, Βλαβών, Κοστολόγησης, Ασφάλειας, και Διάρθρωσης. Κατανοήσαμε πώς όλα αυτά τα στοιχεία συνδέονται επικοινωνούν και πολλες φορές αλληλοεξαρτώνται μεταξύ τους. Η αρχιτεκτονική διαχείρισης που συνδιάζει καλύτερα όλα τα απαραίτητα στοιχεία για την σωστή λειτουργία του δικτύου είναι η κατανεμημένη αρχιτεκτονική και αυτό γιατί συνδυάζει την κεντροποιημένη με την ιεραρχική**,** έχει μία κεντρική πλατφόρμα διαχείρισης ή μια ιεραρχία από πλατφόρμες εξυπηρετητή πελάτη και χρησιμοποιεί ομότιμες πλατφόρμες διαχείρισης που καθεμιά τους χωριστά αποτελεί ένα κεντροποιημένο σύστημα.

Στο δεύτερο κεφάλαιο από την εκτενή ανάλυση του πρωτοκόλλου SNMP (simple network management protocol) συμπεραίνουμε ότι είναι το πιο ευχρηστο και σύνηθες πρωτόκολλο για απομακρυσμένες παρακολουθίσεις δικτύων. Μπορεί να χρησιμοποιήθει από το πιο απλό δικτυο, μέχρι το πιο σύνθετο. Με τις εκδόσεις SNMPv2 και SNMPv3 έχουν βελτιωθεί και οι πιο μικρές λεπτομέριες που μπορεί να το υποβαθμίζαν δεύτερο στην κατηγορία του , με καλύτερο πρωτόκολλο το CMIP .

Στο τρίτο κεφάλαιο, το CMIP αντιθέτως είναι σχεδιασμένο αποκλειστικά για συστήματα με πολλούς πόρους, διότι τους απαιτεί για να λειτουργήσει και είναι το πιο βασικό μειωνέκτημα του. Μια βασική λειτουργία που επεξηγήθηκε είναι η RMON απομακρυσμένης παρακολούθησης δικτύου. Τοποθετείτε στο επίπεδο 1 και επίπεδο 2 του πρωτοκόλλου TCP/IP. Αναπτύχθηκε αρχικά για την αντιμετώπιση του προβλήματος της διαχείρισης των LAN σε απομακρυσμένες περιοχές από μια κεντρική τοποθεσία.Είναι μια αρκετά βασική λειτουργία παρακολούθησης και αποτελεί προέκταση του SNMP MIB.

Στο τέταρτο κεφάλαιο παρουσιάζονται τα δημοφιλέστερα εργαλεία για παρακολούθηση όπως : το Openview Network Node Manager (Hewlett Packard) ,το Whatsup Gold (Ipswitch) και το Net View (IBM). Από την έρευνα για τα εργαλεία αυτά καταλήξαμε στα εξής αποτελέσματα: το Openview Network Node Manager (Hewlett Packard) είναι πιο οικονομικό για 10.000 κόμβους παρά για 1.000 έναντι του προγράμματος Tivoli Net View (IBM). Επίσης τα χαρακτηριστικά του Openview Network Node Manager παίρνουν καλύτερη βαθμολογία έναντι του Tivoli Net View (IBM). Το Whatsup Gold (Ipswitch) Τιμή: 795-1090 $ (ανάλογα με το αν παρέχεται τεχνική υποστήριξη και upgrade) αποτελεί ένα γρήγορο και ασφαλή τρόπο να ελέγξουμε την κατάσταση ενός δικτύου. Η διαμόρφωση περιβάλλοντος του δικτύου είναι εύκολο να προσαρμοστεί στα μέτρα του καθενός αλλά και στις ανάγκες της κάθε επιχείρησης ανάλογα με το μέγεθος αυτής. Έχει ένα πολύ καλό γραφικό ενδιάμεσο περιβάλλον (interface) και η πρόσβαση σε αυτό μπορεί να γίνει και απο απομακρυσμένο περιβάλλον μέσω κάποιου άλλου υπολογιστή ή browser. Δουλεύει σε πλατφόρμες Windows 95/98/ NT/2000/XP.

ΠΗΓΕΣ-ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Τα RFC 2271,2272,2273,2274,2275 μέσω της σελίδας

http://www.ibr.cs.tu-bs.de/projects/snmpv3

[2] Home Page of the SNMPv3 Working Group

http://ietf.org/html.charters/snmpv3-charter.html

[3] The Simple Times Magazine: http://www.simple-times.org

[4] The Internet Protocol Journal Volume 1, Number 3, December 1998 http://www.cisco.com/ipj

[5] IEEE Communications Surveys Fourth Quarter 1998 Vol.1 No.1

http://www.comsoc.org/pubs/surveys

[6] Marshall, Rose. The Simple Book. New Jersey: Prentice Hall, 1994.

[7]Comer, Douglas E. Internetworking with TCP/IP

http://www.hp.com/bizsupport/wja/live/manual/8.1/installs/wja-openview-nnm.pdf

[8] Το πρόγραμμα Open View

http://www.notepage.net/hpopenview/hpopenview.htm

[9] Το πρόγραμμα HP-Network Management Proocol

http://www8.hp.com/us/en/software-solutions/software.html?compURI=1170657#.UOUyAvJeBHM

[9] Το πρόγραμμα IBM Tivoli Netview

http://www-01.ibm.com/software/tivoli/products/netview-performance/

http://www-01.ibm.com/software/tivoli/products/netview-zos/

[10] Το Simple Network Management Protocol (SNMP)

http://el.wikipedia.org/wiki/Simple_Network_Management_Protocol

[11] ΠΡΟ.ΜΕ.Σ.Ι.Π Διαχείριση και Ασφάλεια Δικτύων

[12] Εργασία: Διαχείρηση δικτύων – Πρωτόκολλο SNMP – Εργαλεία λογισμικού διαχείρησης δικτύων των Καλπαξίδου Ελένη και Σωτηριάδη Ιωάννη

[13] Εργασία: Μελέτες Περιπτώσεων Διαχείρισης Καταγραφής Κίνησης Πανεπιστημιακών Δικτύων της Αγγελικής Α. Κωνσταντόγλου

[14]Βασικές λειτουργίες του πρωτοκόλλου CMIP http://en.wikipedia.org/wiki/Common_Management_Information_Protocol

[15]Βιβλίο : Διαδίκτυα με TCP/IP – Αρχές πρωτόκολλα και αρχιτεκτονικές του Douglas E. Comer

[16] Η λειτουργία RMON
http://en.wikipedia.org/wiki/RMON