Πανεπιστήμιο Θεσσαλίας

Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών,
Τηλεπικοινωνιών και Δικτύων

Εργαστήριο Τηλεπικοινωνιών και Δικτύων

Διπλωματική Εργασία

Θέμα: **«Ανάπτυξη ολοκληρωμένου συστήματος διαχείρισης και παρακολούθησης για** TCP/IP **δίκτυα δεδομένων**, **με χρήση του πρωτοκόλλου** SNMP»

Κολοκούρης Ιωάννης

A.M.: 1700054

Επιβλέπων: Καθηγητής Λέανδρος Τασιούλας

Βόλος, Ιούλιος 2005

Περιεχόμενα:

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή κ. Λέανδρο Τασιούλα που δέχτηκε τη συνεργασία μαζί μου στα πλαίσια της διπλωματικής μου εργασίας. Επίσης, οφείλω να τον ευχαριστήσω για τις πολύτιμες, εύστοχες συμβουλές σε σχέση με τη σταδιοδρομία μου και για τις πόρτες που μου άνοιξε, ακόμα κι αν μερικές δεν ήμουν έτοιμος να τις περάσω.

Επίσης, ευχαριστώ το Σπύρο Κοψιδά για τη βοήθειά του σε θέματα της Delphi και διαχείρισης δικτύου και το Δημήτρη Ζησιάδη για συμβουλές σε θέματα δικτύου και στο κείμενο της διπλωματικής.

Άλλο ένα ευχαριστώ στο Σπύρο, το Δημήτρη, το Φίλιππο και το Θανάση που με έκαναν να νιώσω ευπρόσδεκτος στο γραφείο τους και να περάσω ένα αποδοτικό αλλά και ευχάριστο εξάμηνο.

Ευχαριστώ την οικογένειά μου για την ηθική, συναισθηματική και οικονομική υποστήριξη όλα αυτά τα χρόνια.

Τέλος, ευχαριστώ την Αθηνά που με περίμενε 5 ολόκληρα χρόνια.

1. **Δίκτυα υπολογιστών**

Τα δίκτυα υπολογιστών αυξάνονται με εκρηκτικούς ρυθμούς. Πριν από είκοσι χρόνια πολλοί λίγοι ήταν αυτοί που είχαν πρόσβαση σε ένα δίκτυο. Στις μέρες μας, λόγω της ραγδαίας τεχνολογικής ανάπτυξης και των πολλαπλών επικοινωνιακών αναγκών που πρέπει να καλυφθούν, τα δίκτυα υπολογιστών έχουν γίνει απαραίτητο μέρος των υποδομών μας. Η διακυβέρνηση, το εμπόριο, τα χρηματοοικονομικά, η υγεία, η εκπαίδευση, και η διασκέδαση είναι μερικές μόνο από τις περιοχές της ανθρώπινης δραστηριότητας που επηρεάζονται από τις τρέχουσες τεχνολογικές προόδους. Η δικτύωση χρησιμοποιείται σε κάθε δραστηριότητα των επιχειρήσεων, όπως στη διαφήμιση, την παραγωγή, το σχεδιασμό, την κοστολόγηση και τη λογιστική. Γι' αυτό το λόγο οι περισσότερες εταιρίες έχουν πολλά δίκτυα. Δίκτυα υπολογιστών χρησιμοποιούνται από οργανισμούς σε περιβάλλον γραφείου για να μεταφέρουν πληροφορία, να μοιράζονται προγράμματα και δεδομένα, να μπορούν να συνδέονται με εκτυπωτές και πιθανώς με άλλα περιφερειακά. Πολλά σχολεία, σε όλες τις βαθμίδες, χρησιμοποιούν δίκτυα υπολογιστών για να παρέχουν στους διδασκόμενους και τους διδάσκοντες πρόσβαση σε πληροφορίες που υπάρχουν σε ηλεκτρονικές βιβλιοθήκες σε όλο τον πλανήτη. Επίσης, δίκτυα υπολογιστών χρησιμοποιούνται σε εργοστασιακό περιβάλλον ώστε να συνδέονται εργαλειομηχανές, ρομπότ και αισθητήρες και να υπάρχει κεντρικός έλεγχος και συντονισμός. Δίκτυα χρησιμοποιούν οι κρατικές, περιφερειακές και τοπικές δημόσιες υπηρεσίες, καθώς και οι στρατιωτικοί οργανισμοί. Με μια φράση τα δίκτυα υπολογιστών βρίσκονται πλέον παντού! Το μεγαλύτερο δίκτυο όλων είναι το γνωστό μας Internet (Διαδίκτυο).

1.1. Internet

Το Internet ξεκίνησε από ένα project του Αμερικανικού στρατού το 1969, το οποίο αποσκοπούσε στη δημιουργία ενός δικτύου μεταφοράς δεδομένων μεταξύ υπολογιστών. Το 1978, δημιουργήθηκε το πειραματικό δίκτυο ARPANET, που συνέδεε λίγους υπολογιστές και αποτέλεσε τον πρόγονο του σημερινού Internet. Το Internet, σήμερα, είναι ένα παγκόσμιο δίκτυο υπολογιστικών συσκευών που παρέχει την υποδομή για επικοινωνία, αποθήκευση και υπολογιστικές εργασίες. Οι συσκευές που το αποτελούν είναι ηλεκτρονικοί υπολογιστές (PCs), σταθμοί εργασίας

(workstations), εξυπηρετητές (servers) και οποιαδήποτε συσκευή μπορεί να έχει ένα network interface. Όλες αυτές ονομάζονται τερματικά συστήματα (end systems ή hosts). Οι συσκευές αυτές συνδέονται μεταξύ τους με ζεύξεις επικοινωνίας. Υπάρχουν πολλά είδη ζεύξεων επικοινωνίας που χαρακτηρίζονται από το φυσικό μέσο μετάδοσης, που μπορεί να είναι ομοαξονικό καλώδιο, συνεστραμμένο καλώδιο, οπτικές ίνες ή ραδιοφάσμα. Η ταχύτητα μεταφοράς (ρυθμός μεταφοράς) είναι διαφορετική για κάθε μέσο και για κάθε τεχνική μετάδοσης. Οι τερματικές συσκευές συνδέονται μεταξύ τους με switches (μεταγωγείς), δημιουργώντας μικρά δίκτυα. Τα δίκτυα αυτά συνδέονται μεταξύ τους με routers (δρομολογητές).

1.1.1. TCP/IP

Η επικοινωνία μεταξύ των συσκευών γίνεται μέσω πρωτοκόλλων. Ορισμός: «Ένα πρωτόκολλο ορίζει τη μορφή και τη σειρά των μηνυμάτων που ανταλλάσσονται ανάμεσα σε δυο ή περισσότερες επικοινωνούσες οντότητες, όπως και τις ενέργειες που γίνονται κατά τη διάρκεια μετάδοσης και/ή της λήψης ενός μηνύματος ή άλλου γεγονότος» [Δικτύωση Υπολογιστών – Kurose, Ross].

Το Transmission Control Protocol (TCP) και το Internet Protocol (IP) είναι τα κυριότερα πρωτόκολλα του Internet. Το TCP δημιουργεί μια λογική σύνδεση μεταξύ δυο τερματικών συσκευών (connection oriented) και μπορεί να εγγυηθεί αξιόπιστη μεταφορά δεδομένων από το ένα άκρο στο άλλο. Αυτά τα δεδομένα έχουν τη μορφή ανεξάρτητων πακέτων, τα οποία το TCP φροντίζει να φτάσουν χωρίς σφάλματα και με τη σωστή σειρά. Το IP πρωτόκολλο εκτελεί τρεις βασικές λειτουργίες. Πρώτη είναι η διευθυνσιοδότηση (addressing). Κάθε συσκευή στο διαδίκτυο χαρακτηρίζεται από μια μοναδική διεύθυνση. Αυτή αποτελείται από 32 bits (4 bytes) χωρισμένα σε τέσσερις οκτάδες. Μετατρέποντας κάθε οκτάδα από bits σε έναν δεκαδικό αριθμό, μια IP διεύθυνση μοιάζει με: «195.251.17.193». Δεύτερη βασική λειτουργία είναι η δρομολόγηση (routing). Με πληροφορία που αποκομίζεται από την IP διεύθυνση και από πίνακες δρομολόγησης που βρίσκονται σε κάθε συσκευή, το IP πρωτόκολλο αναλαμβάνει να βρει ένα μονοπάτι από μια τερματική συσκευή σε μια άλλη. Βοηθητικά πρωτόκολλα για αυτή τη λειτουργία είναι τα RIP, HELLO, IGRP, OSPF. Τρίτη βασική λειτουργία του IP είναι το fragmentation (κατακερματισμός). Το IP αναλαμβάνει να «σπάσει» την πληροφορία που πρέπει να σταλεί μέσω του δικτύου σε πακέτα, τα οποία είναι οι μονάδες μεταφοράς δεδομένων στο Internet. Τα πακέτα

αυτά αφού δημιουργηθούν, σταλούν και φτάσουν στην τερματική συσκευή προορισμού, επανα-συναρμολογούνται από το IP και παραδίδονται στην εφαρμογή για την οποία προορίζονται. Χαρακτηριστικά του IP είναι ότι δε δημιουργεί λογικές συνδέσεις (connectionless), δεν κάνει αξιόπιστη μεταφορά των δεδομένων και δεν εγγυάται ότι τα πακέτα θα φτάσουν στον προορισμό με τη σειρά όπου εστάλησαν.
TCP/IP ονομάζεται μια σουίτα πρωτοκόλλων με βασικά της πρωτόκολλα φυσικά το TCP και το IP. Άλλα πρωτόκολλα του Internet που ανήκουν στη σουίτα είναι τα:

- ICMP: Πρωτόκολλο ελέγχου που χρησιμοποιείται για αναφορά λαθών το IP. Στέλνει προαιρετικά, κάποια ενημερωτικά πακέτα σε περίπτωση εντοπισμού βλάβης. Η πιο γνωστή-συνηθισμένη εφαρμογή είναι το ping, ένα μήνυμα «hello» προς μια συσκευή και αναμονή για απάντηση, ώστε να ενημερωθούμε αν η συσκευή είναι σε λειτουργία.
- FTP: Πρωτόκολλο που χρησιμοποιείται για τη μεταφορά αρχείων.
- SMTP: Πρωτόκολλο που υλοποιεί την αποστολή και λήψη e-mails (ηλεκτρονικό ταχυδρομείο).
- TELNET: Πρωτόκολλο που επιτρέπει την απομακρυσμένη σύνδεση σε μια συσκευή του δικτύου.
- SNMP: Πρωτόκολλο που βοηθά στη διαχείριση του δικτύου (θα το αναλύσουμε παρακάτω).
- DNS: Πρωτόκολλο που εκτελεί την αντιστοίχηση της IP διεύθυνσης μιας συσκευής με το domain name της (όνομα υπολογιστή και υπηρεσίας).
- UDP: Πρωτόκολλο που υλοποιεί επικοινωνία μεταξύ δυο τερματικών συσκευών, χωρίς να δημιουργεί λογικό κανάλι. Δίνει τη δυνατότητα ανταλλαγής μηνυμάτων αλλά δεν εγγυάται την ασφαλή και αξιόπιστη μεταφορά αυτών. Οι εφαρμογές που το χρησιμοποιούν είναι υπεύθυνες να εξασφαλίσουν τη σωστή επικοινωνία.

1.1.1.1 TCP/IP vs. OSI

Στα τέλη της δεκαετίας του 1970, πριν την δημιουργία του Internet και της διαδικτύωσης, προκειμένου να προωθηθεί η συμβατότητα των αρχιτεκτονικών δικτύων των διαφόρων εταιριών, ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization – ISO) πρότεινε ένα μοντέλο αρχιτεκτονικής που ονομάζεται πρότυπο αναφοράς για τη διασύνδεση ανοιχτών συστημάτων (open

system interconnection reference model - OSI). Το μοντέλο αναφοράς OSI είναι μια διασταυρωμένη αρχιτεκτονική με επτά στρώματα ή επίπεδα (layers).

Επίπεδο	**Όνομα**	**Λειτουργία**
1	Φυσικό	Μετάδοση bits
2	Σύνδεση Δεδομένων	Μετάδοση πακέτων μέσα από μια δεδομένη ζεύξη
3	Δίκτυο	Μετάδοση πακέτων από άκρο σε άκρο
4	Διακίνηση	Παράδοση μηνυμάτων από άκρο σε άκρο
5	Σύνοδος	Εγκατάσταση και διαχείριση συνομιλίας από άκρο σε άκρο
6	Παρουσίαση	Διαμόρφωση, κρυπτογράφηση και συμπίεση δεδομένων
7	Εφαρμογές	Υπηρεσίες δικτύου (π.χ. ηλεκτρονικό ταχυδρομείο και μεταφορά αρχείων)

Κάθε επίπεδο παρέχει μια υπηρεσία που χρησιμοποιείται από το ακριβώς ανώτερο επίπεδο. Τα επίπεδα είναι αυτόνομα, δηλαδή αν γίνει κάποια αλλαγή σε ένα επίπεδο δεν επηρεάζονται τα υπόλοιπα. Κατά την επικοινωνία μεταξύ δυο κόμβων ενός δικτύου, υπάρχει λογική σύνδεση μεταξύ των αντίστοιχων επιπέδων του κάθε κόμβου, αλλά η πραγματική σύνδεση πραγματοποιείται μέσω της φυσικής διαδρομής.

Όπως προαναφέρθηκε, το μοντέλο επτά επιπέδων που περιγράψαμε επινοήθηκε πριν από την διαδικτύωση. Γι' αυτό το μοντέλο δεν περιέχει κάποιο επίπεδο για τα πρωτόκολλα διαδικτύου. Ακόμα, το μοντέλο OSI αφιερώνει ένα ολόκληρο επίπεδο στα πρωτόκολλα συνόδου, τα οποία έχουν γίνει λιγότερο σημαντικά. Έτσι, οι ερευνητές που ανέπτυξαν το TCP/IP επινόησαν ένα νέο μοντέλο διαστρωμάτωσης, το μοντέλο διαστρωμάτωσης TCP/IP (TCP/IP Layering Model) ή μοντέλο αναφοράς του Internet (Internet Reference model), το οποίο έχει πέντε επίπεδα.

Επίπεδο	**Όνομα**	**Λειτουργία**
1	Φυσικό	Μετάδοση bits
2	Διασύνδεση Δικτύου	Οργάνωση δεδομένων σε πακέτα και μεταφορά τους μέσα από μια δεδομένη ζεύξη

3	Διαδίκτυο	Μορφή πακέτων και μετάδοσής τους από άκρο σε άκρο
4	Μεταφορά	Αξιόπιστη παράδοση μηνυμάτων από άκρο σε άκρο
5	Εφαρμογή	Υπηρεσίες δικτύου

Αν και μερικά επίπεδα του μοντέλου αναφοράς TCP/IP αντιστοιχούν σε επίπεδα του μοντέλου αναφοράς OSI, το σχήμα διαστρωμάτωσης του ISO δεν έχει κανένα επίπεδο που να αντιστοιχεί σε επίπεδο διαδικτύου του TCP/IP.
Αντιστοιχίζοντας τα πρωτόκολλα του TCP/IP στα επίπεδα του OSI που ανήκουν, έχουμε ότι το IP και το ICMP ανήκουν στο επίπεδο Δικτύου (layer 3), το TCP και το UDP στο επίπεδο Διακίνησης (layer 4), το DNS στο επίπεδο Συνόδου (layer 5) και τα FTP, SMTP, TELNET και SNMP στο επίπεδο Εφαρμογής (layer 7).

1.1.2. Ports & Sockets

Οι εφαρμογές που τρέχουν στις συσκευές του δικτύου, όπως είπαμε έχουν την ανάγκη να επικοινωνήσουν με όμοιες ή διαφορετικές εφαρμογές σε άλλες συσκευές. Η IP διεύθυνση μπορεί να καθορίσει μοναδικά μια συσκευή-προορισμό αλλά δε μπορεί να καθορίσει και την εφαρμογή για την οποία προορίζεται κάποια πληροφορία. Σε κάθε συσκευή τρέχουν πολλές εφαρμογές, κάθε μια από τις οποίες συνδέεται (bind) σε μια port (θύρα) της συσκευής, από όπου μπορεί να λάβει ή να στείλει δεδομένα (πακέτα). Το port είναι ένα νούμερο από 16 bits (τιμές από 0 έως 65535). Μια εφαρμογή σε έναν υπολογιστή καθορίζεται από την IP διεύθυνση του υπολογιστή και τον αριθμό port της εφαρμογής. Έτσι κάθε πακέτο (UDP ή TCP) που στέλνεται στο Internet πρέπει να έχει μια IP διεύθυνση και ένα port προορισμού. Το ζεύγος αυτό ονομάζεται και socket και όπως είπαμε καθορίζει μοναδικά μια εφαρμογή. Εφαρμογές που είναι standard στο TCP/IP χρησιμοποιούν τον ίδιο αριθμό port πάντα. Για παράδειγμα http: port 80, telnet: port 23, ftp: port 21, smtp: port 25, snmp: port 161 & 162 κ.λ.π.

1.1.2. **Υπηρεσίες**

Το δίκτυο από μόνο του δεν έχει καμία πραγματική χρησιμότητα για τον άνθρωπο. Αυτό που δίνει αξία στο Internet (και όλα τα δίκτυα) είναι οι υπηρεσίες που εκτελούνται σε αυτό. Η πιο διαδεδομένη υπηρεσία του Internet είναι το Web (world wide web - WWW). Μας επιτρέπει την περιήγηση σε ιστοσελίδες που φιλοξενούνται σε web servers ανά τον κόσμο και περιέχουν ένα τεράστιο πλήθος από πολύ ή λιγότερο χρήσιμες πληροφορίες κάθε είδους. Επίσης, εξαιρετικά διαδεδομένο είναι το ηλεκτρονικό ταχυδρομείο. Η αποστολή και η λήψη δηλαδή μηνυμάτων μεταξύ χρηστών του Internet που διαθέτουν μια ηλεκτρονική ταχυδρομική διεύθυνση. Η αποθήκευση και η προώθηση των μηνυμάτων αυτών γίνεται από τους mail servers. Άλλη μια χρήσιμη υπηρεσία είναι τα στιγμιαία μηνύματα. Εφαρμογές τέτοιου τύπου είναι το ICQ και το Windows Messenger, τα οποία επίσης ακολουθούν την αρχιτεκτονική client-server. Με την αύξηση των ταχυτήτων των ζεύξεων, έχουν γίνει εφικτές νέες multimedia υπηρεσίες. Τέτοιες είναι το streaming video και audio (π.χ. τηλεόραση ή ραδιόφωνο μέσω Internet) και το VoIP, δηλαδή η τηλεφωνία μέσω Internet. Επίσης, οι υπηρεσίες κοινής χρήσης αρχείων μεταξύ ομότιμων κόμβων (peer to peer) έχουν διαδοθεί αρκετά, ειδικά μετά τη μεγάλη επιτυχία του Napster. Ακόμα, αρχιτεκτονικές ομότιμων κόμβων χρησιμοποιούνται και για το διαμοιρασμό επεξεργαστικής ισχύος. Αρκετά γνωστή είναι η εφαρμογή Seti@home. Μεγάλη απήχηση έχουν στην νεολαία τα κατανεμημένα (δικτυακά) παιχνίδια, που αποτελούν και αυτά μια υπηρεσία του δικτύου. Πολλές ακόμα εφαρμογές υπάρχουν και δημιουργούνται κάθε μέρα, δίνοντας ακόμα μεγαλύτερη αξία στο Internet.

Εδώ θα πρέπει να αναφέρουμε κάποιες ακόμα δυνατότητες που μας προσφέρουν τα δίκτυα υπολογιστών και είναι πολύ δημοφιλείς τον τελευταίο καιρό. Υπηρεσίες όπως η τηλε-εκπαίδευση (e-learning), η τηλε-εργασία, η ηλεκτρονική διακυβέρνηση (e-government) και το ηλεκτρονικό εμπόριο (e-commerce) χρησιμοποιούνται όλο και περισσότερο. Όλες αυτές αποτελούν υπηρεσίες που στηρίζονται στο Internet και απευθύνονται σε φοιτητές, εργαζόμενους, καταναλωτές, πολίτες και γενικότερα πολυπληθείς κοινωνικές ομάδες. Η εύκολη πρόσβαση στην πληροφορία που έχει ανάγκη ο κάθε χρήστης, χαρακτηρίζει αυτές τις υπηρεσίες και τους προσδίδει ιδιαίτερη χρησιμότητα.

1.2. Intranets

Εκτός από το Internet υπάρχουν και ιδιωτικά δίκτυα που καλούνται ενδοδίκτυα (intranets). Αυτά είναι εταιρικά ή κυβερνητικά δίκτυα, που είναι αποκομμένα από το Internet ή έχουν περιορισμένη επικοινωνία με αυτό μέσω συστημάτων ασφαλείας που φιλτράρουν την κίνηση των πληροφοριών. Τα Intranets χρησιμοποιούν τους ίδιους τύπους συσκευών (PCs, routers, servers), ζεύξεων και πρωτοκόλλων με το Internet, οπότε είναι απόλυτα συμβατά με αυτό. Η αξία των δικτύων αυτών είναι μεγάλη διότι αυξάνουν την παραγωγικότητα και επιταχύνουν τις διαδικασίες. Παραδείγματα Intranets είναι το δίκτυο των ATM μιας τράπεζας, το δίκτυο υπολογιστών μιας πολυεθνικής εταιρίας και το δίκτυο των υπολογιστών ενός υπουργείου. Τέλος, ενδεικτικό παράδειγμα χρήσιμης εφαρμογής που στηρίζεται στο intranet των υπολογιστών της εφορίας είναι το TAXIS, που παρέχει πρόσβαση στα οικονομικά δεδομένα του κάθε πολίτη από κάθε υποκατάστημα της Δ.Ο.Υ. στην Ελλάδα.

2. **Διαχείριση Δικτύου**

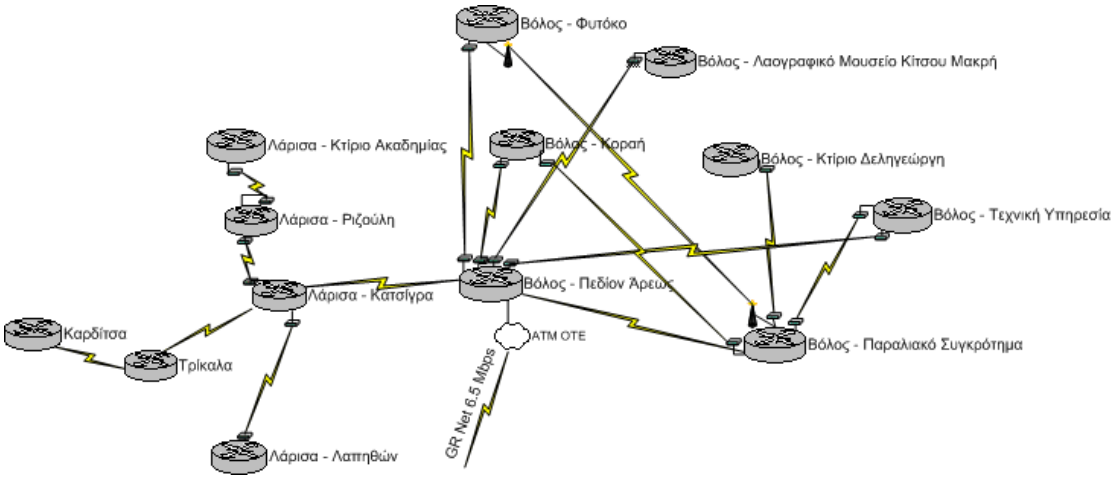
Όλα τα παραπάνω συνηγορούν στο πόσο χρήσιμα και επικερδή μπορεί να είναι τα δίκτυα υπολογιστών για τους ανθρώπους, λόγω κυρίως των υπηρεσιών που στηρίζονται σε αυτά. Όμως, πόσο εύκολο ή δύσκολο είναι να διατηρηθεί ένα δίκτυο σε κατάσταση λειτουργίας, χωρίς προβλήματα και χωρίς διακοπές; Ποιος είναι υπεύθυνος για αυτό; Υπεύθυνος ομαλής λειτουργίας του δικτύου είναι ο Διαχειριστής του δικτύου (Network Manager) και η δουλειά του στις περισσότερες των περιπτώσεων είναι αρκετά δύσκολη. Ένας ορισμός της διαχείρισης δικτύου είναι: «Η διαχείριση δικτύων περιλαμβάνει την ανάπτυξη, ολοκλήρωση και συντονισμό του υλικού, λογισμικού και ανθρώπινου στοιχείου για παρακολούθηση, δοκιμή, καταμέτρηση, ανάλυση, αποτίμηση και έλεγχο των πόρων δικτύου και των στοιχείων, ώστε να ικανοποιούν τη λειτουργική απόδοση πραγματικού χρόνου και τις απαιτήσεις Ποιότητας Υπηρεσίας με ένα λογικό κόστος» [Saydam 1996]. Σύμφωνα με το Διεθνή Οργανισμό Τυποποίησης (ISO), ορίζονται πέντε περιοχές διαχείρισης δικτύου:

- *Διαχείριση απόδοσης*. Στόχος της διαχείρισης απόδοσης είναι να μετρά και να αναλύει την απόδοση των διαφόρων συστατικών του δικτύου (ζεύξεις, δρομολογητές, υπηρεσίες). Η μειωμένη απόδοση συγκεκριμένων μονάδων του δικτύου πρέπει να εντοπίζεται και να αντιμετωπίζεται κατάλληλα.

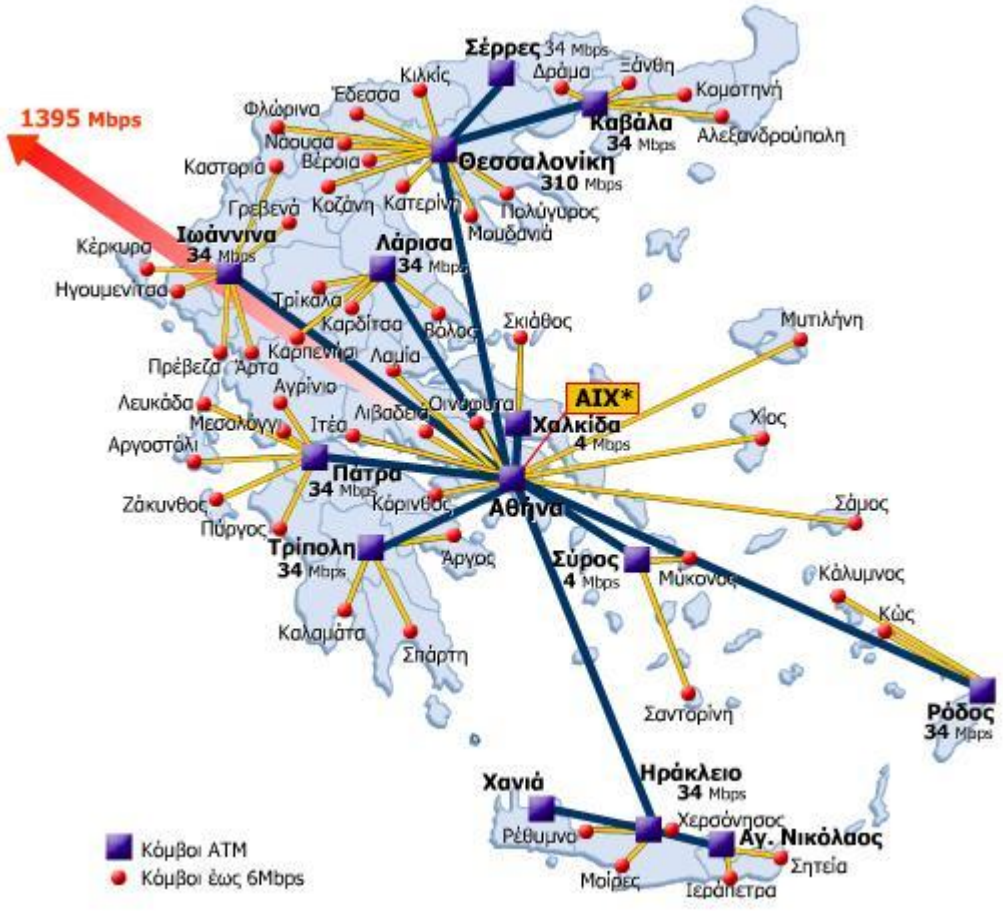
- *Διαχείριση σφαλμάτων*. Στόχος της είναι η ανίχνευση και η διόρθωση των σφαλμάτων μέσα στο δίκτυο. Τα σφάλματα μπορεί να είναι εμφανή (διακοπή μιας σύνδεσης) ή λιγότερο εμφανή (ανεξήγητη καθυστέρηση στο δίκτυο). Όμως, ο διαχειριστής πρέπει να εντοπίζει γρήγορα την αιτία τους και να τα διορθώνει. Στην καλύτερη περίπτωση θα πρέπει να τα προβλέπει και να τα αποτρέπει.
- *Διαχείριση παραμετροποίησης*. Στόχος είναι ο εντοπισμός και η παρακολούθηση των διαχειριζόμενων συσκευών του δικτύου και η παραμετροποίηση (configuration) των συσκευών αυτών και του λογισμικού τους.
- *Λογιστική διαχείριση*. Στόχος είναι η καταγραφή και ο έλεγχος της χρήσης των πόρων του δικτύου από τους χρήστες και η χρέωση με βάση αυτή. Η περιοχή αυτή είναι ιδιαίτερα σημαντική όταν οι υπηρεσίες και οι πόροι του δικτύου χρεώνονται.
- *Διαχείριση ασφάλειας*. Στόχος της διαχείρισης ασφάλειας είναι ο έλεγχος πρόσβασης στους πόρους του δικτύου από τους χρήστες, ανάλογα με την πολιτική πρόσβασης. Οι υπηρεσίες πρέπει να είναι διαθέσιμες μόνο στους χρήστες που έχουν το δικαίωμα πρόσβασης και σύμφωνα με το Service Level Agreement (SLA). Δηλαδή, δε φτάνει οι υπηρεσίες να είναι διαθέσιμες, αλλά πρέπει και η ποιότητά τους (Quality of service - QoS) να είναι στο προσυμφωνημένο επίπεδο.

2.1. **Πολυπλοκότητα δικτύων**

Αυτές είναι οι βασικές αρμοδιότητες του Διαχειριστή του δικτύου. Σε όλα αυτά προστίθεται η πολυπλοκότητα του δικτύου, που μπορεί να αποτελείται από μεγάλο αριθμό συσκευών και χρηστών. Επίσης, το δίκτυο μπορεί να εκτείνεται σε πολλά σημεία μιας πόλης ή και σε ολόκληρη τη χώρα. Για να μπορέσουμε να αποκτήσουμε μια εικόνα δικτύου, στις παρακάτω εικόνες φαίνονται το δίκτυο του Πανεπιστημίου Θεσσαλίας (που εκτείνεται σε Βόλο, Λάρισα, Τρίκαλα και Καρδίτσα),



και το δίκτυο της εταιρίας FORTHNet Α.Ε. (που είναι εξαπλωμένο σε ολόκληρη την Ελλάδα), με τις φυσικές ζεύξεις μεταξύ των κόμβων.



Στις εικόνες αυτές φαίνεται μόνο το backbone, δηλαδή η ραχοκοκαλιά του δικτύου που αποτελείται από τους δρομολογητές. Σε κάθε έναν από αυτούς τους κόμβους, είναι συνδεδεμένες δεκάδες ή και εκατοντάδες τερματικές συσκευές. Μπορούμε έτσι

να φανταστούμε την πολυπλοκότητα του δικτύου και τη δυσκολία παρακολούθησης και διαχείρισής του.

2.2. **Λογισμικό Διαχείρισης Δικτύου**

Βλέπουμε ότι η δουλειά του διαχειριστή δεν είναι εύκολη, όμως υπάρχουν πακέτα λογισμικού που τον βοηθούν στην επίβλεψη και τη διαχείριση του δικτύου. Αυτά λέγονται Συστήματα Διαχείρισης Δικτύου (Network Management Systems - NMS) και εγκαθίστανται σε έναν υπολογιστή που μπορεί να επικοινωνήσει με τα υπόλοιπα μηχανήματα του δικτύου. Μέσω αυτού, ο διαχειριστής έχει εποπτεία της κίνησης που υπάρχει στο δίκτυο, των ποιών συσκευών υπάρχουν στο δίκτυο και της κατάστασης των συσκευών αυτών. Επίσης, υπάρχει δυνατότητα αλλαγής των ρυθμίσεων των συσκευών από απόσταση. Έτσι, μέσα από ευκολονόητα γραφήματα και επεξεργασμένα δεδομένα, μπορεί ο διαχειριστής ανά πάσα στιγμή να έχει μια καλή εικόνα του δικτύου και επίσης να ενημερώνεται ταχύτατα για πιθανές βλάβες ή άλλα συμβάντα. Μάλιστα, κάποιος αρκετά προσεκτικός και προνοητικός μπορεί να προβλέψει μια βλάβη λόγω ανωμαλίας στην κίνηση του δικτύου ή στη συμπεριφορά των συσκευών και να δράσει κατάλληλα αποτρέποντας τις συνέπειες.

Τα λογισμικά πακέτα αυτά παρέχονται συνήθως από τους κατασκευαστές του δικτυακού εξοπλισμού. Για παράδειγμα, η Cisco και η 3com που κατασκευάζουν routers, switches, access points και άλλες συσκευές διασύνδεσης υπολογιστών, έχουν δημιουργήσει και τα δικά τους NMS πακέτα, τα οποία προωθούν στους πελάτες τους. Ομοίως, η Hewlett Packard εμπορεύεται το πολύ γνωστό OpenView. Μερικές φορές, τα πακέτα αυτά υποστηρίζουν τη διαχείριση μόνο των συσκευών της εταιρίας (π.χ. CiscoWorks 2000), πράγμα που περιορίζει πολύ στην επιλογή του δικτυακού εξοπλισμού και εγκλωβίζει τους πελάτες. Ευτυχώς, τις περισσότερες φορές υποστηρίζονται λίγο ή πολύ όλες οι συσκευές, ανεξαρτήτως εταιρίας κατασκευής (π.χ. πακέτο OpenView). Αυτό επιτυγχάνεται μέσω ευρέως διαδεδομένων πρωτοκόλλων, που αποτελούν standards στη διαχείριση του δικτύου, τα οποία οι κατασκευαστές φροντίζουν να υποστηρίζονται από τις συσκευές τους. Βέβαια, υπάρχουν και ανεξάρτητες εταιρίες λογισμικού που παρέχουν αξιόλογα πακέτα NMS. Τέτοιες είναι για παράδειγμα η CastleRock με το SNMPc, η Novell με το ZENworks και η MG-SOFT. Τέλος, τελευταία έχουν δημιουργηθεί κάποια project groups με

σκοπό την υλοποίηση και συντήρηση open source NMS πακέτων, που διατίθενται δωρεάν με άδεια τύπου GPL. Αυτά δεν έχουν ακόμα τις δυνατότητες των εμπορικών πακέτων αλλά το γεγονός ότι είναι δωρεάν και υπάρχει πρόσβαση στον κώδικά τους για βελτιώσεις και τροποποιήσεις, τα κάνει ανταγωνιστικά. Τέτοια πακέτα είναι το OpenNMS υλοποιημένο σε Java, το NINO σε html, JavaScript και Perl και άλλα λιγότερο γνωστά. Ακόμα, υπάρχει το Net-SNMP, μια βιβλιοθήκη από command line scripts που βοηθούν στη διαχείριση του δικτύου και μπορούν να καλεστούν από άλλα προγράμματα σαν εξωτερικές συναρτήσεις.

2.3. **Πρωτόκολλα Διαχείρισης Δικτύου**

Τα πρωτόκολλα που αναφέραμε ότι χρησιμοποιούνται στη διαχείριση του δικτύου ποικίλουν. Για παράδειγμα, το Internet Control Message Protocol (ICMP) βοηθά στην ομαλή λειτουργία ενός δικτύου με πακέτα πληροφοριών σχετικά με την κατάσταση αυτού. Ένα πολύ γνωστό μας feature του ICMP είναι το ping. Η αποστολή, δηλαδή, ενός UDP πακέτου σε έναν host του δικτύου, ο οποίος αν το λάβει, πρέπει να απαντήσει με ack πακέτο. Έτσι, μπορούμε να δούμε ποιες συσκευές του δικτύου είναι σε λειτουργία και αν υπάρχει επικοινωνία με αυτές. Ένα άλλο πρωτόκολλο είναι το Telnet. Μέσω αυτού, μπορούμε να συνδεθούμε απομακρυσμένα με μια συσκευή, αν βέβαια το υποστηρίζει. Έπειτα, μπορούμε να τροποποιήσουμε ρυθμίσεις της συσκευής σα να είχαμε πρόσβαση τοπικά ή να δούμε τις πληροφορίες που είναι κατασκευασμένη η συσκευή να μας παρέχει μέσω του Telnet. Λόγω του ότι κάθε συσκευή του δικτύου έχει πάντα μια μοναδική IP διεύθυνση, πολλά NMS πακέτα χρησιμοποιούν τον DNS server, αν υπάρχει, για να αντιστοιχίσουν την IP διεύθυνση με το όνομα της συσκευής και για να μάθουν πληροφορίες για το δίκτυο και τη μορφή του. Ένα ακόμα πρωτόκολλο διαχείρισης δικτύου είναι το Common Management Information Protocol (CMIP), που όμως δεν είναι καθόλου διαδεδομένο. Τέλος, το πιο διαδεδομένο από όλα τα πρωτόκολλα για τη διαχείριση του δικτύου είναι το Simple Network Management Protocol (SNMP), το οποίο θα αναλύσουμε περισσότερο αφού αποτέλεσε βασικό κομμάτι της διπλωματικής εργασίας.

3. Simple Network Management Protocol (SNMP)

Το SNMP προτάθηκε το 1988, για να βοηθήσει τους διαχειριστές των δικτύων να διαχειριστούν τις IP συσκευές από απόσταση. Μέσω εύκολων λειτουργιών δίνεται η δυνατότητα στο διαχειριστή να δει και να αλλάξει την κατάσταση των συσκευών που υποστηρίζουν το SNMP. Για παράδειγμα, μπορεί κανείς να κλείσει ένα interface ενός router ή να δει τη θερμοκρασία της CPU ενός server, όλα αυτά από απόσταση και με απλές εντολές του SNMP. Επίσης, με το SNMP μπορούμε να δημιουργήσουμε έναν χάρτη με όλες τις SNMP συσκευές του δικτύου και να παρακολουθούμε την κατάστασή τους. Τέλος, μπορούμε να κανονίσουμε ώστε οι συσκευές από μόνες τους να μας ειδοποιούν όταν ένα ανεπιθύμητο γεγονός συμβεί. Για παράδειγμα, να ρυθμίσουμε έναν server να μας ειδοποιήσει αν το ποσοστό του σκληρού του δίσκου που έχει καταληφθεί υπερβεί ένα κατώφλι (π.χ. 90%), ώστε να ενεργήσουμε κατάλληλα πριν ο σκληρός γεμίσει εντελώς και δημιουργηθούν προβλήματα.

Το SNMP είναι πρωτόκολλο επιπέδου εφαρμογής και αποτελεί μέρος της σουίτας πρωτοκόλλων TCP/IP. Η πρώτη έκδοσή του ήταν το SNMPv1. Αργότερα (1995) ήρθε η βελτιωμένη έκδοση SNMPv2 που κυριαρχεί αυτή τη στιγμή, αν και από το 2002 έχει ήδη γίνει standard η έκδοση SNMPv3 που λύνει πολλά προβλήματα ασφαλείας.

3.1. Manager

Το SNMP αποτελείται από δυο είδη οντοτήτων, το Manager και τον Agent. Ο Manager είναι ένα λογισμικό που τρέχει σε κάποιον υπολογιστή (Network Management Station) και έχει την αρμοδιότητα της διαχείρισης του δικτύου. Έχει δυνατότητα εκτέλεσης τριών βασικών λειτουργιών:

α. Να στέλνει «get» μηνύματα στους agents που υπάρχουν στα μηχανήματα του δικτύου, ρωτώντας την κατάστασή τους και να λαμβάνει έπειτα την απάντηση.

β. Να στέλνει «set» μηνύματα σε έναν agent, αλλάζοντας την κατάσταση ή μια ρύθμιση μια συσκευής

γ. Να λαμβάνει τα «trap» μηνύματα που στέλνονται από τους agents όταν κάτι ασυνήθιστο συμβεί και να αντιδρά σε αυτά ανάλογα με το πώς έχει ρυθμιστεί να αντιδράσει.

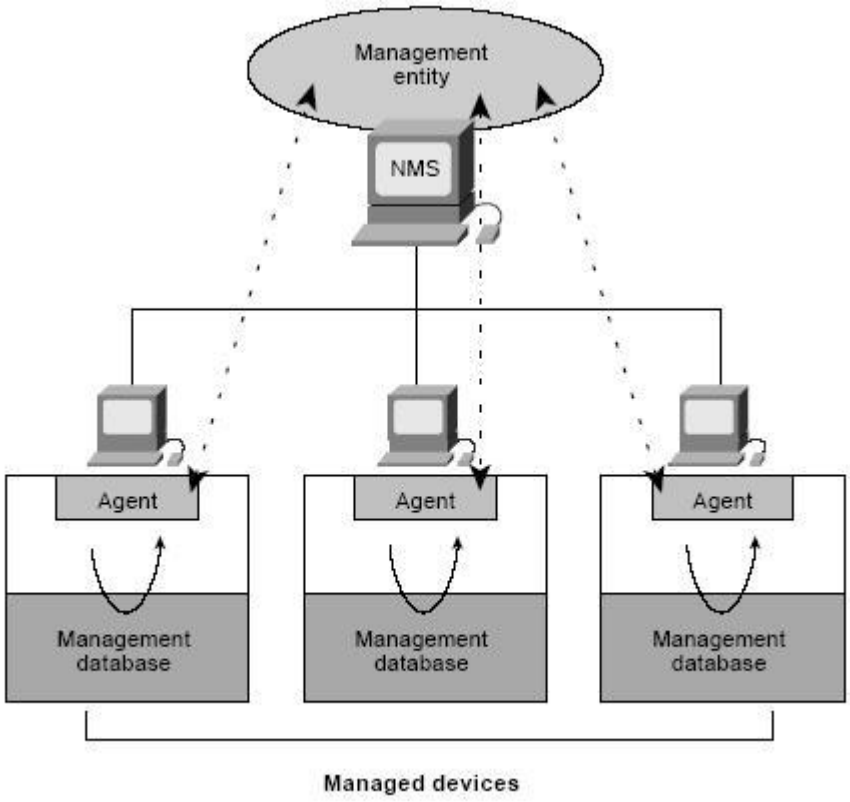
3.2. Agent

Ο Agent είναι και αυτός λογισμικό που τρέχει στις συσκευές του δικτύου που υποστηρίζουν το SNMP και συνήθως παρέχεται από τον κατασκευαστή της συσκευής. Παρέχει στον manager πληροφορίες χρήσιμες για τη διαχείριση της συσκευής, τις οποίες έχει συλλέξει κατά τη διάρκεια λειτουργίας αυτής. Για παράδειγμα, ο agent ενός router μπορεί να ενημερώσει για το αν τα interfaces του είναι up ή down. Και ο agent είναι υπεύθυνος για τρεις βασικές λειτουργίες:

α. Να απαντά στα «get» μηνύματα του manager στέλνοντας την πληροφορία που του ζητήθηκε σε ένα μήνυμα τύπου «response».

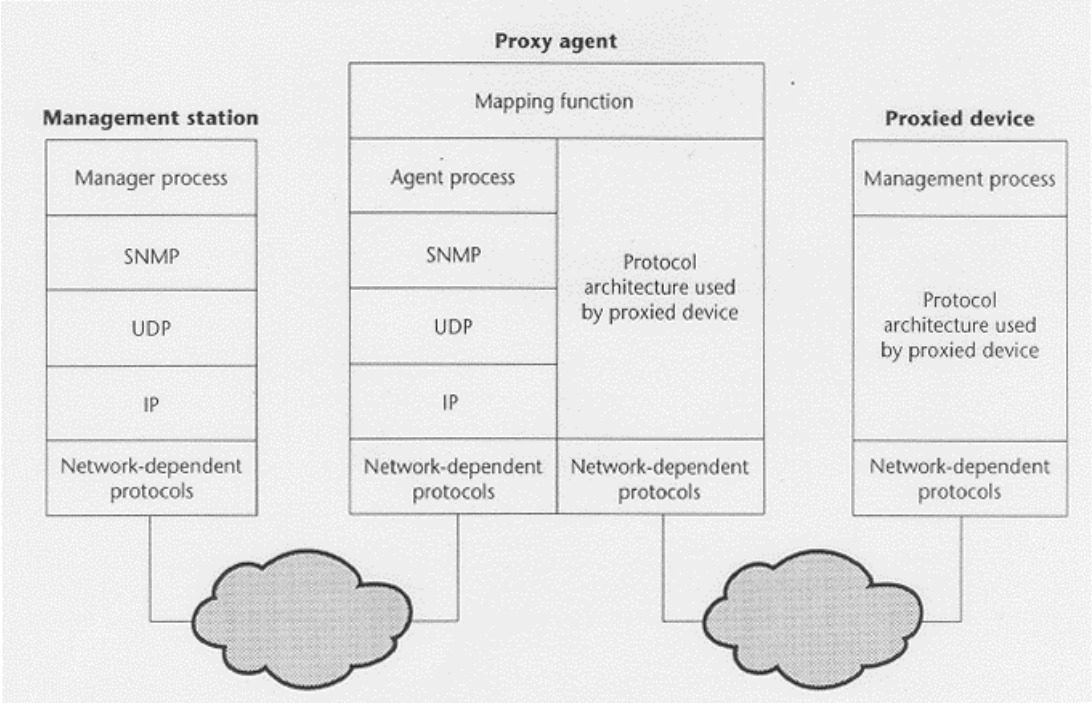
β. Να τροποποιεί την κατάλληλη ρύθμιση της συσκευής ανάλογα με το «set» μήνυμα που λαμβάνει από το manager.

γ. Να στέλνει «trap» μηνύματα όταν συμβούν ασυνήθιστα γεγονότα. Το ποια γεγονότα είναι ασυνήθιστα ορίζεται από πριν στον agent.



3.2.1. **Ενδιάμεσοι** agents

Ακόμα, υπάρχουν και οι λεγόμενοι «ενδιάμεσοι agents», που είναι hardware συσκευές που υποστηρίζουν το SNMP και ο ρόλος τους είναι να συνδέονται σε άλλες συσκευές που δεν υποστηρίζουν το SNMP αλλά κάποιο δικό τους πρωτόκολλο και να ενημερώνονται για την κατάστασή τους μιλώντας το πρωτόκολλο αυτό. Δηλαδή παίζουν το ρόλο της ενδιάμεσης διεπαφής μεταξύ manager και συσκευής δικτύου που δεν υποστηρίζει SNMP.



3.3. Management Information Base

Ένα άλλο σημαντικό στοιχείο του SNMP είναι η Management Information Base (MIB), μια βάση δεδομένων που βρίσκεται σε κάθε SNMP συσκευή και κρατά πληροφορίες σχετικά με την κατάσταση αυτής. Είναι οργανωμένη σε ένα δέντρο από αντικείμενα (managed object), των οποίων τις τιμές μπορεί ο manager να κάνει «get» (δηλαδή να τις διαβάσει) ή «set» (δηλαδή να τις τροποποιήσει). Τα αντικείμενα αυτά χαρακτηρίζονται από ένα μοναδικό ID (object ID - OID). Διαφορετικά είδη συσκευών υποστηρίζουν διαφορετικά αντικείμενα στις MIBs τους, αλλά και οι συσκευές του ίδιου τύπου πολλές φορές έχουν διαφορές στις MIBs τους. Κάποια αντικείμενα τέλος, υπάρχουν by default σε όλες τις συσκευές. Η δομή αυτών των αντικειμένων είναι πολύ αυστηρά ορισμένη και ονομάζεται Structure of Management Information (SMI).

Σύμφωνα με τον ορισμό αυτής της δομής, υπάρχουν έξι στοιχεία που καθορίζουν ένα αντικείμενο:

α. Το όνομα ή OID του αντικειμένου, που έχει δυο μορφές. Την αριθμητική που είναι κάτι σαν το «1.3.6.1.2.1.1.5» και την πιο ευκολονόητη στον άνθρωπο, που για παράδειγμα για την παραπάνω αριθμητική τιμή είναι «sysName».

β. Το syntax, που ορίζεται με βάση ένα μέρος του Abstract syntax Notation One (ASN.1), το οποίο είναι machine-independent. Το syntax μας ενημερώνει τι τύπος είναι αυτό το αντικείμενο (integer, integer32, unsigned32, octet string, object identifier, IPaddress, counter32, counter64, gauge32, timeticks ή opaque).

γ. Το Encoding που ορίζει πως η τιμή του managed object μετατρέπεται σε string, χρησιμοποιώντας τους Basic Encoding Rules (BER).

δ. Το access, που ορίζει τον τύπο της πρόσβασης που μπορεί να έχει κανείς στο αντικείμενο αυτό. Μπορεί να έχει πρόσβαση μόνο read, μόνο write, και τα δυο ή καθόλου πρόσβαση.

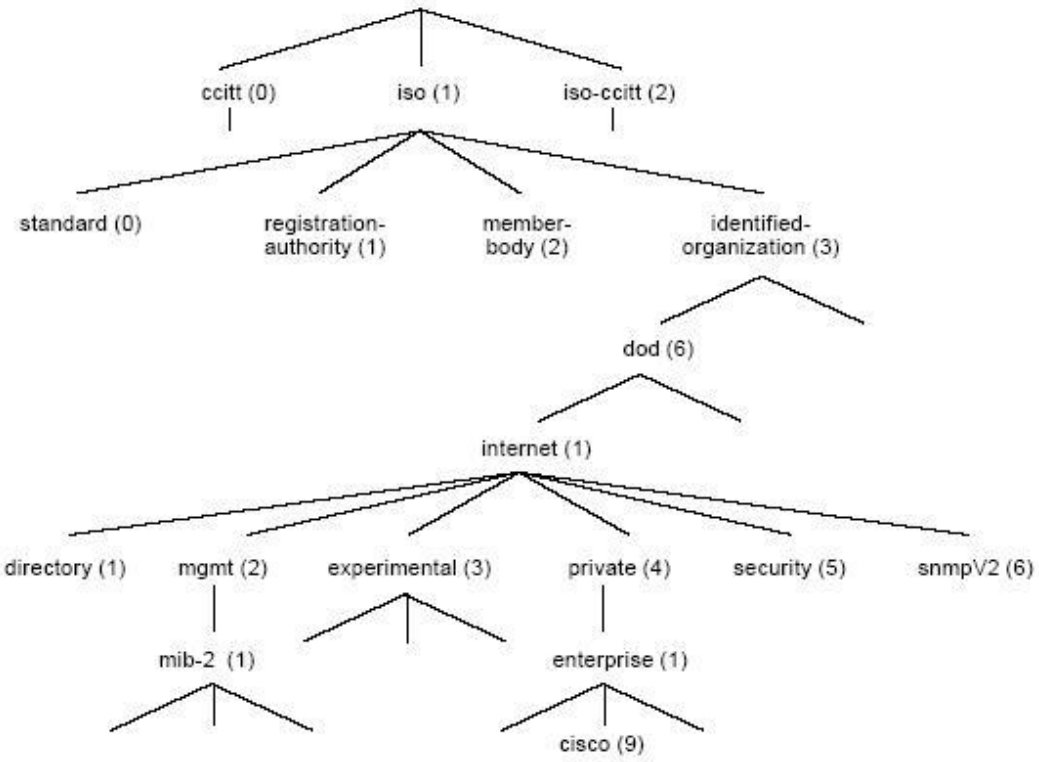
ε. Το «status» που μας ενημερώνει αν το αντικείμενο είναι πρόσφατο και έγκυρο (current), αν είναι απαρχαιωμένο (obsolete) ή αποδοκιμασμένο (deprecated).

στ. Τέλος, υπάρχει μια περιγραφή του τι πληροφορία ακριβώς μας δίνει το αντικείμενο αυτό.

Μέσα σε ένα αρχείο MIB, ο ορισμός ενός αντικειμένου (π.χ. το sysUpTime) μοιάζει κάπως έτσι:

```
sysUpTime OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The time (in hundredths of a second) since the
            network management portion of the system was last
            re-initialized."
    ::= { system 3 }
```

Η μορφή του δέντρου της MIB έχει την παρακάτω μορφή. Υπάρχει η δυνατότητα κάθε εταιρία να έχει ένα δικό της κλαδί στο δέντρο όπου θα ορίζει τα MIB αντικείμενα που υποστηρίζουν οι δικές της συσκευές. Έτσι, στο κλαδί «1.3.6.1.4.1» ή «iso.org.dod.internet.private.enterprise» μπορεί να προστεθεί όποια εταιρία επιθυμεί και να αποκτήσει τι δικό της enterprise id.



Δε θα αναλύσουμε παραπάνω τη δομή της MIB, αλλά θα δώσουμε δυο παραδείγματα αντικειμένων. Το αντικείμενο με όνομα «sysDescr» έχει OID «1.3.6.1.2.1.1.1». Κάθε αριθμός αντιπροσωπεύει έναν κόμβο στο δέντρο της MIB ενώ έχει και ένα όνομα ευκολονόητο από τον άνθρωπο (συγκεκριμένα «iso.org.dod.internet.mgmt.mib-2.system.sysDescr»). Το syntax του είναι «Octet string» που σημαίνει ότι η τιμή του αντικειμένου αυτού αποτελεί κείμενο και όχι π.χ. αριθμό. Το αντικείμενο αυτό μας δίνει την περιγραφή της συσκευής όπως αυτή έχει οριστεί από τον κατασκευαστή. Ένα δεύτερο αντικείμενο είναι το «udpInDatagrams» με OID «1.3.6.1.2.1.7.1», ή αλλιώς «iso.org.dod.internet.mgmt.mib-2.udp.udpInDatagrams». Το syntax του είναι «counter32» που σημαίνει ότι η τιμή του αντικειμένου αυτού είναι ένας πάντα θετικός integer 32 bit. Η πληροφορία που μας δίνει είναι το πόσα udp πακέτα έχουν φτάσει στη συσκευή και έχουν παραδοθεί στο παραπάνω επίπεδο (layer) χωρίς πρόβλημα.

3.4. **Εντολές** SNMP

Οι βασικές εντολές που υποστηρίζει το SNMP είναι οι παρακάτω:

- «Get»: Ένας manager μπορεί να στείλει ένα μήνυμα «get» σε έναν agent και να του ζητήσει να τον ενημερώσει για την τρέχουσα τιμή ενός MIB αντικειμένου.
- «GetNext»: Με την εντολή αυτή ένας manager ζητά από έναν agent την τιμή του επόμενου MIB αντικειμένου από αυτό που ζήτησε πριν. Κάνοντας συνεχώς GetNext παίρνουμε όλα τα αντικείμενα του δέντρου, από εκεί που ξεκινάμε και κάτω, σα να κάναμε Depth First Search (DFS).
- «GetBulk»: Με την εντολή αυτή ο manager ζητά από έναν agent τις τιμές πολλών διαδοχικών MIB αντικειμένων. Η εντολή αυτή δεν υποστηρίζεται στο SNMPv1.
- «Set»: Με την εντολή αυτή ο manager στέλνει στον agent μια νέα τιμή για ένα MIB αντικείμενο.
- «response»: Ο agent μέσω αυτής της εντολής απαντά στα «get», «getNext», «GetBulk» και «set» μηνύματα του manager.
- «trap»: Ο agent στέλνει ένα μήνυμα στο manager δηλώνοντας ότι μια δυσλειτουργία έχει προκληθεί.
- «Inform»: Ο manager στέλνει σε έναν άλλο manager, αν υπάρχει, ένα ενημερωτικό μήνυμα. Δεν υποστηρίζεται στο SNMPv1.

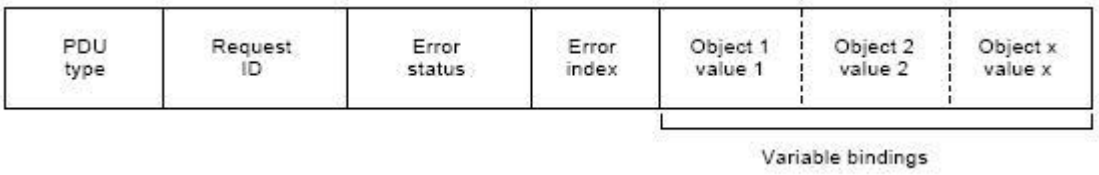
3.5. **Επικοινωνία**

Το SNMP χρησιμοποιεί UDP πακέτα για την επικοινωνία μεταξύ agent και manager. Το UDP δεν είναι αξιόπιστο αφού δε δημιουργεί κανάλι επικοινωνίας αλλά κάνει μια και μόνο προσπάθεια μετάδοσης των δεδομένων χωρίς να εγγυάται επιτυχία. Έτσι και η επικοινωνία agent και manager δεν είναι αξιόπιστη. Τεχνικές επανεκπομπής μετά το πέρας ενός χρόνου (timeout) μπορούν να χρησιμοποιηθούν. Επίσης, θα μπορούσε να χρησιμοποιηθεί TCP για τη σύνδεση, το οποίο δημιουργεί κανάλι επικοινωνίας και η επιτυχία της μετάδοσης μπορεί να εγγυηθεί. Αυτό όμως θα δημιουργούσε επιπλέον φόρτο στο δίκτυο. Το SNMP έχει φτιαχτεί για να λειτουργεί τη στιγμή που το δίκτυο αντιμετωπίζει προβλήματα, που σημαίνει ότι προτιμάται τα πακέτα της επικοινωνίας να είναι μικρά και ευέλικτα ώστε να μην αυξάνουν το πρόβλημα. Το port 161 χρησιμοποιείται για αποστολή και λήψη «get» και «set» μηνυμάτων, ενώ το port 162 για τα «trap» μηνύματα.

3.6. **Μορφή των** SNMP **πακέτων**

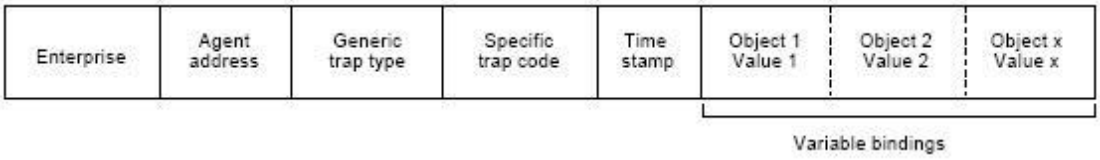
Τα πακέτα του SNMP αποτελούνται από δυο μέρη, το header και το protocol data unit (PDU).

Στο header υπάρχει πληροφορία για το version του SNMP (v1, v2c, v3) που χρησιμοποιείται και το community string που θα χρειαστεί για την αυθεντικοποίηση.
Το PDU για τα μηνύματα τύπου «get», «getNext», «response» και «set» χωρίζεται στα παρακάτω μέρη:



- Το «PDU type» είναι ο τύπος του πακέτου («get», «getNext», «set», «response»).
- Το «Request ID» είναι ένας αριθμός που συνδέει τις αιτήσεις («get», «getNext») με τις αντίστοιχες απαντήσεις («response»).
- Το «Error status» είναι ένας αριθμός που προσδιορίζει κάποιο πιθανό λάθος που έχει συμβεί. Συμπληρώνεται μόνο στο «response» μήνυμα ενώ για άλλο τύπο μηνύματος παίρνει την τιμή 0.
- Ομοίως και το «Error index», που σχετίζει το λάθος του Error status με ένα συγκεκριμένο αντικείμενο της MIB.
- Τέλος, τα «variable bindings» είναι ζεύγη MIB αντικειμένων και των τιμών που αυτά έχουν. Τα πεδία αυτά δε χρησιμοποιούνται στους τύπους «get» και «getNext».

Το PDU για τα μηνύματα τύπου «trap» αποτελείται από τα μέρη:



- Το «Enterprise» προσδιορίζει τον τύπο και τον κατασκευαστή της συσκευής που έστειλε το trap μήνυμα.

- Το «Agent address» αποτελεί την IP διεύθυνση της συσκευής που έστειλε το μήνυμα.
- Το «Generic trap type» είναι ένας αριθμός από 0 έως 6 που προσδιορίζει τον τύπο της δυσλειτουργίας που προκάλεσε το trap μήνυμα. Οι τύποι αυτοί είναι προκαθορισμένοι για όλες τις συσκευές και είναι 0: coldStart, 1: warmStart, 2: linkDown, 3: linkUp, 4: authenticationFailure, 5: egpNeighborLoss, 6: άλλος τύπος μη προκαθορισμένος.
- Το «Specific trap code» συμπληρώνεται αν το Generic trap code έχει τιμή 6, και καθορίζει το είδος του trap από ένα σύνολο traps ορισμένων από τον κατασκευαστή της συσκευής στο αντίστοιχο enterprise MIB.
- Το «time stamp» είναι ο χρόνος που έχει περάσει από την εκκίνηση λειτουργίας της συσκευής και τη γέννηση του trap μηνύματος.
- Τα «variable bindings», όπως και πριν, είναι ζεύγη MIB αντικειμένων και των τιμών που αυτά έχουν.

3.7. **Διαφορές μεταξύ εκδόσεων**

Οι διαφορές μεταξύ SNMPv1 και SNMPv2 είναι μικρές. Τα βασικότερα επιπλέον χαρακτηριστικά του SNMPv2 είναι:

- Η εντολή «getBulk» με την οποία ο manager μπορεί να ζητήσει μεγάλο αριθμό από συνεχόμενα MIB αντικείμενα από τον agent. Είναι το ίδιο με πολλά συνεχόμενα «getNext».
- Τα μηνύματα τύπου «Inform» που μπορούν να σταλούν από manager σε manager, αν υπάρχουν παραπάνω από ένας στο δίκτυο.
- Κάποιοι επιπλέον τύποι MIB αντικειμένων, όπως ο 64 bit integer, τα bit strings και επιπλέον τύποι IP διευθύνσεων.

Οι διαφορές του SNMPv3 σε σχέση με το SNMPv2, όπως θα δούμε και παρακάτω, βρίσκονται μόνο στον τομέα της ασφάλειας.

3.8. **Ασφάλεια**

Το βασικό πρόβλημα του SNMPv1 και SNMPv2 είναι αυτό της ασφάλειας. Αν και υπάρχει ένα password που ονομάζεται «community string» και χρησιμοποιείται για

την διαπίστευση (authentication) manager και agent, αυτό μπορεί να υποκλαπεί εύκολα με ένα network sniffer (π.χ. το Ethereal), διότι τα μηνύματα που στέλνονται μεταξύ manager και agent δεν κρυπτογραφούνται. Έτσι, οποιοσδήποτε έχει πρόσβαση στο δίκτυο, μπορεί να βρει το community string και έπειτα να έχει και αυτός τη δυνατότητα να κάνει get και set στα αντικείμενα των agents και κατ' επέκταση στις ρυθμίσεις των συσκευών. Υπάρχουν δυο ειδών community strings, το «public» με το οποίο μπορεί κανείς να κάνει μόνο get και το «private» με το οποίο γίνεται get και set. Οι agents των συσκευών συνήθως έχουν by default ορισμένα τα community strings στις τιμές «public» και «private» αντίστοιχα και πρέπει να αλλαχθούν αμέσως μόλις η συσκευή ενσωματωθεί στο δίκτυό μας. Εδώ θα πρέπει να αναφέρουμε ότι συνήθως οι agents στέλνουν ένα trap μήνυμα όταν κάποιος με λάθος community string προσπαθεί να επικοινωνήσει μαζί τους. Ενημερώνουν δηλαδή, ότι υπάρχει πρόβλημα στην διαπίστευση κάποιου χρήστη, πράγμα που ίσως να σημαίνει ότι ο χρήστης αυτός προσπαθεί να μαντέψει το community string.

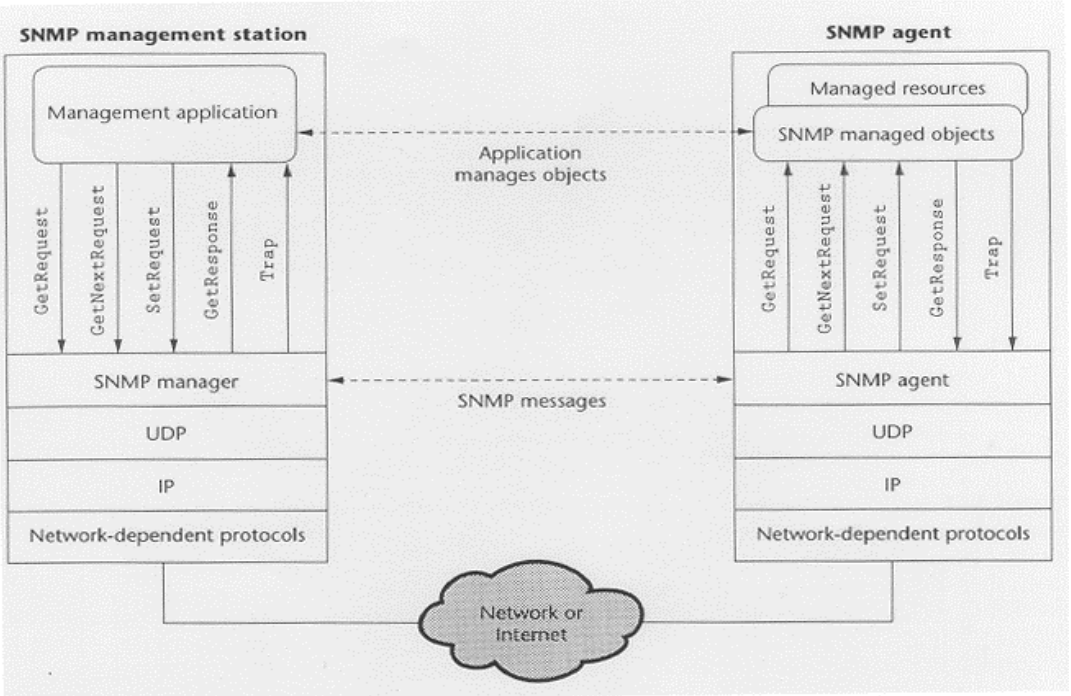
Η λύση του προβλήματος έρχεται στο SNMPv3, το οποίο παρέχει δυνατότητες διαπίστευσης (με χρήση συνάρτησης κατακερματισμού) και κρυπτογραφίας (με τον DES αλγόριθμο). Παρόλα αυτά, το SNMPv3 δεν υποστηρίζεται ακόμα από πολλούς κατασκευαστές διότι αν και παρέχει μεγαλύτερη ασφάλεια, αυξάνει το κόστος των συσκευών και την καθυστέρηση στο δίκτυο. Επίσης, αν όλες οι συσκευές του δικτύου δεν υποστηρίζουν το SNMPv3 τότε δεν υπάρχει νόημα εφαρμογής του διότι όπως γνωρίζουμε η ασφάλεια του δικτύου είναι όπως ο πιο αδύναμος κρίκος μιας αλυσίδας. Η πιο αδύναμη συσκευή σε θέμα ασφάλειας ορίζει και το συνολικό επίπεδο ασφάλειας του δικτύου. Από την άλλη, η αλλαγή ταυτόχρονα όλων των συσκευών που δεν υποστηρίζουν το SNMPv3 δεν είναι εφικτή. Αυτό που γίνεται είναι αρχικά το SNMPv3 να υποστηρίζεται από παλιότερες συσκευές με updates σε επίπεδο software και οι νέες συσκευές να το υποστηρίζουν σε επίπεδο hardware. Μερικοί κατασκευαστές, για να αντιμετωπίσουν το πρόβλημα της ασφάλειας, ρυθμίζουν τις συσκευές να μην υποστηρίζουν τη «set» λειτουργία μετατρέποντας το SNMP σε πρωτόκολλο απλά παρακολούθησης του δικτύου και όχι διαχείρισης.

Μια άλλη λύση στο πρόβλημα μπορεί να δοθεί από ένα firewall. Εφόσον ο manager με τους agents επικοινωνούν σε συγκεκριμένα ports, μπορούν εύκολα να φτιαχτούν κανόνες στο firewall που θα αποτρέπουν πακέτα εκτός του δικτύου με προορισμό τα ports 161 και 162 του udp να εισέρχονται στο δίκτυο. Αυτό βέβαια δε θα λύσει το

πρόβλημα των απειλών εσωτερικά του δικτύου. Μερικές φορές δημιουργείται μέσα στο δίκτυο ένα κρυπτογραφημένο, απομονωμένο δίκτυο (Virtual Private Network) το οποίο παρέχει ασφαλή επικοινωνία μεταξύ agent και manager και χρησιμοποιείται μόνο από το διαχειριστή του δικτύου. Αυτό όμως είναι ακριβό και δύσκολο στη διαχείριση. Τέλος, καλή ιδέα είναι η συχνή αλλαγή των community strings, η οποία μπορεί να γίνει και αυτόματα με ένα script.

3.9. **Ανακεφαλαίωση**

Ανακεφαλαιώνοντας, το SNMP είναι ένα πρωτόκολλο που βοηθά στη διαχείριση του δικτύου. Υπάρχουν δυο είδη οντοτήτων, ο agent που βρίσκεται στις συσκευές του δικτύου που υποστηρίζουν το SNMP και ο manager που βρίσκεται σε έναν κεντρικό υπολογιστή τον οποίο λειτουργεί ο διαχειριστής του δικτύου. Ο agent διατηρεί μια βάση δεδομένων (MIB) με προκαθορισμένα αντικείμενα τα οποία έχουν κάποιες τιμές που προσδιορίζουν τη λειτουργία της συσκευής. Ο manager μπορεί να κάνει get ή set την τιμή ενός τέτοιου αντικειμένου και να δει ή να τροποποιήσει αντίστοιχα την κατάσταση της συσκευής. Αν κάτι ασυνήθιστο συμβεί, ο agent στέλνει ένα trap μήνυμα στον manager ειδοποιώντας τον για τη δυσλειτουργία. Το ποιο γεγονός είναι ασυνήθιστο ορίζεται εκ των προτέρων στον agent. Η αυθεντικοποίηση των μηνυμάτων αυτών γίνεται μέσω του community string, το οποίο προκαλεί και τα προβλήματα ασφαλείας. Αυτά λύνονται με τη χρήση του SNMPv3.



4. **Λογισμικό Πακέτο** UTH-NMS

Τα NMS λογισμικά που κυκλοφορούν από τις κατασκευάστριες εταιρίες των δικτυακών συσκευών ή από εταιρίες λογισμικού, κοστίζουν πολύ και δεν είναι πάντα ευέλικτα. Σε περιπτώσεις μικρών δικτύων η αγορά τους είναι ασύμφορη. Από την άλλη, τα open source NMS πακέτα δεν είναι τόσο αξιόπιστα και δεν υποστηρίζουν πάντα όλες τις λειτουργίες που ένας διαχειριστής δικτύου χρειάζεται. Βέβαια, σε περιπτώσεις στις οποίες δίνεται ο κώδικας, μπορεί κανείς να αναπτύξει τα επιπρόσθετα εργαλεία που θα χρειαστεί και έπειτα να τα ενσωματώσει στο πακέτο. Αυτό είναι πολύ δύσκολο και χρονοβόρο διότι πρέπει πρώτα να διαβάσει και να κατανοήσει χιλιάδες γραμμές κώδικα γραμμένο από άλλους προγραμματιστές.

Τα παραπάνω μας οδήγησαν στη δημιουργία ενός NMS λογισμικού πακέτου από το μηδέν. Το λογισμικό αυτό δημιουργήθηκε κυρίως για να καλύψει τις ανάγκες διαχείρισης του ασύρματου δικτύου του Εργαστηρίου Τηλεπικοινωνιών και Δικτύων του Τ.Μ.Η.Υ.Τ.Δ. Θα μπορεί να βελτιωθεί από άλλους φοιτητές του τμήματος στα πλαίσια διπλωματικών ή άλλων εργασιών, ώστε να γίνει ένα ανταγωνιστικό open source NMS πακέτο.

4.1. Delphi

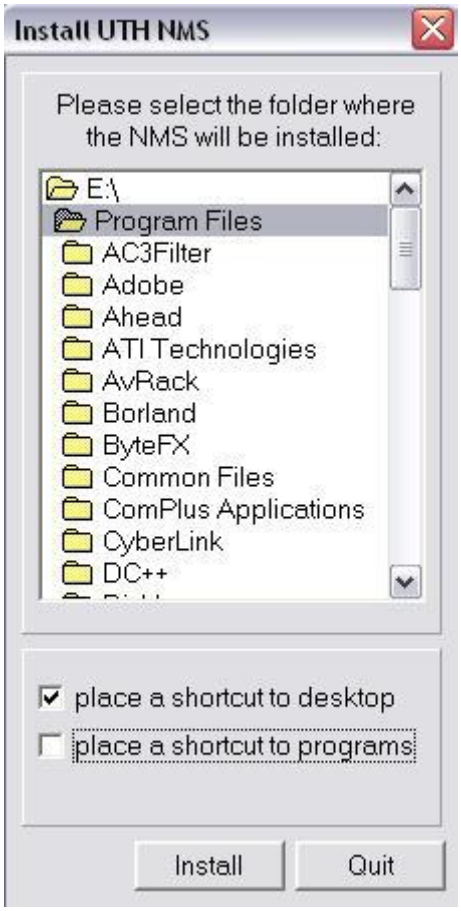
Το λογισμικό μας είναι γραμμένο σε Delphi 7 της Borland. Η Delphi είναι ένα προγραμματιστικό περιβάλλον όπου βασίζεται στη γλώσσα προγραμματισμού Pascal. Εμφανίστηκε το 1995 και μέχρι το 2005 έχει φτάσει την έκδοση 9 (Delphi 2005). Οι εφαρμογές που αναπτύσσονται σε Delphi προορίζονται κυρίως για περιβάλλοντα Windows. Όμως, με τη χρήση του Kylix, που εμφανίστηκε το 2001, οι εφαρμογές μπορούν να γίνουν compile και να εκτελεστούν σε Linux. Το output αρχείο είναι ένα μοναδικό executable αρχείο. Κομμάτια κώδικα Delphi μπορούν να γίνουν «αντικείμενα» και ενσωματωθούν σε νέες εφαρμογές με τη μορφή VCL/CLX components.

Η επιλογή της Delphi έγινε λόγω των πολλών πλεονεκτημάτων της:

1. Είναι πολύ γρήγορη.
2. Βοηθά πολύ στη δημιουργία Graphical User Interface (GUI).
3. Είναι σταθερή.
4. Είναι ιδανική για δικτυακές εφαρμογές.
5. Παρέχει εύκολη διασύνδεση με οποιαδήποτε βάση δεδομένων.
6. Τρέχει σε Windows αλλά και Unix με χρήση του Kylix.
7. Χρησιμοποιείται πολύ, με αποτέλεσμα να υπάρχουν πολλά έτοιμα κομμάτια επαναχρησιμοποιήσιμου κώδικα.
8. Υπάρχουν πολλά forums και newsgroups αφιερωμένα σε αυτή.

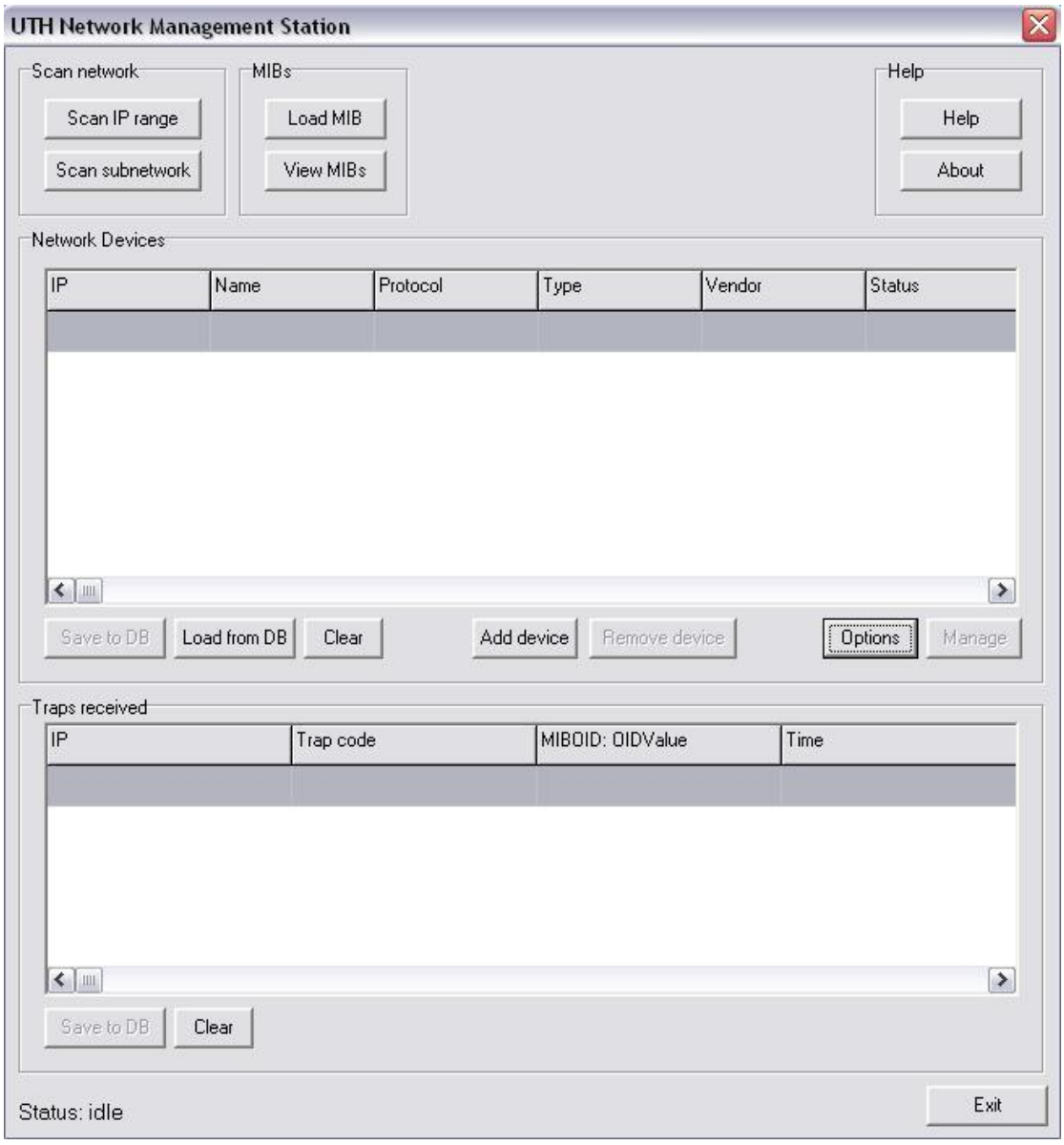
4.2. **Εγκατάσταση**

Η εγκατάσταση του λογισμικού μας γίνεται με το «setup.exe» αρχείο. Μαζί με αυτό πρέπει να υπάρχει ο φάκελος «UTH-NMS» όπου υπάρχουν όλα τα αναγκαία αρχεία της εγκατάστασης. Το «setup.exe» αρχείο απλά αντιγράφει τα αρχεία αυτά στο φάκελο της εγκατάστασης που θα επιλέξει ο χρήστης. Επίσης, αν ζητηθεί δημιουργούνται shortcuts στο desktop και στο start-programs.



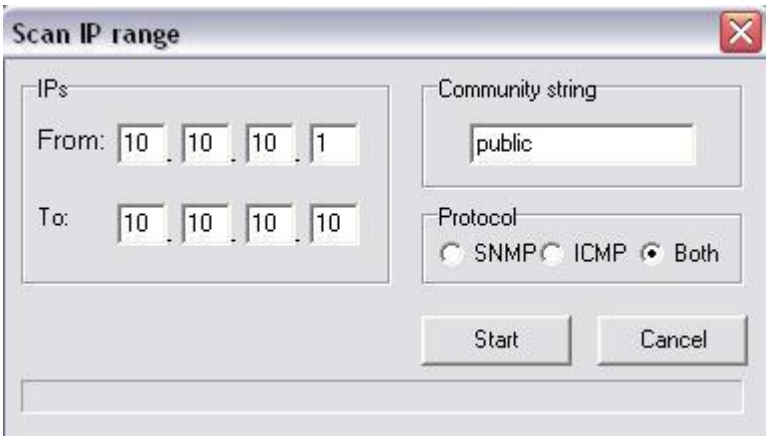
4.3. **Περιγραφή λειτουργίας**

Το λογισμικό μας εγκαθίσταται σε έναν υπολογιστή συνδεδεμένο στο δίκτυο, μέσω του οποίου ο διαχειριστής θα έχει την εποπτεία του δικτύου. Με την εκκίνηση της εφαρμογής βλέπουμε το κύριο παράθυρο, από το οποίο μας δίνεται η δυνατότητα για επιλέξουμε τι θέλουμε να κάνουμε.



4.3.1. Scan IP range

Υπάρχει η δυνατότητα ο χρήστης να κάνει scan σε ένα εύρος IP διευθύνσεων, ψάχνοντας για δικτυακές συσκευές. Τα δεδομένα εισόδου που χρειάζονται είναι η αρχική IP, η τελική IP, το community string στο οποίο απαντάνε οι SNMP συσκευές και το πρωτόκολλο (ICMP, SNMP ή και τα δυο) με το οποίο θα γίνει η αναζήτηση.



Το πρόγραμμα έπειτα, σε κάθε ενδιάμεση IP διεύθυνση, στέλνει ένα ICMP ping πακέτο και ένα SNMP get πακέτο (σε MIB αντικείμενο που υποστηρίζεται by default σε κάθε συσκευή). Αν υπάρξει απάντηση σε οποιοδήποτε από τα δυο, τότε προστίθεται η IP (δηλαδή η συσκευή) σε μια λίστα η οποία φαίνεται στο κύριο παράθυρο της εφαρμογής. Αν μάλιστα υποστηρίζεται το SNMP από τη συσκευή, τότε μπορούμε ακόμα να μάθουμε το όνομά της (από το αντικείμενο sysName της MIB), τον κατασκευαστή της (από το MIB αντικείμενο sysObjectID) και πιθανά τον τύπο της (από λέξεις κλειδιά στην περιγραφή της συσκευής που παίρνουμε από το αντικείμενο sysDescr). Λόγω του ότι το scanning γίνεται από ξεχωριστό thread, υπάρχει η δυνατότητα οποιαδήποτε στιγμή να διακόψουμε τη διαδικασία και να επιστρέψουμε στο κύριο παράθυρο της εφαρμογής. Ο χρόνος που διαρκεί το scanning εξαρτάται από τρεις παραμέτρους. Πρώτον τον αριθμό των IP διευθύνσεων που βρίσκονται στο block ψαξίματος, δεύτερον το χρόνο που κάνει να φτάσει η απάντηση (Round Trip Time - RTT) και τρίτον το χρόνο που έχουμε ορίσει να περιμένει η εφαρμογή μέχρι να θεωρήσει ότι δεν πρόκειται να λάβει απάντηση (timeout). Αν ο τελευταίος αυτός χρόνος είναι πολύ μεγάλος τότε το ψάξιμο καθυστερεί πολύ κάθε φορά που δε λαμβάνουμε απάντηση από μια IP διεύθυνση (είτε επειδή δεν αντιστοιχεί σε κάποια συσκευή, είτε επειδή η συσκευή δεν απαντάει). Αν όμως είναι πολύ μικρός τότε μπορεί, εξαιτίας μιας καθυστέρησης του δικτύου, να μη βρούμε κάποια συσκευή που ενώ απάντησε, το πακέτο δεν έφτασε έγκαιρα στο NMS. Ο μέγιστος χρόνος που μπορεί να διαρκέσει το scanning είναι όταν καμία IP διεύθυνση (δηλαδή συσκευή) δεν απαντήσει, οπότε θα χρειαστεί χρόνος {αριθμός IP διευθύνσεων}*{max(χρόνος timeout SNMP, χρόνος timeout ICMP)}. Ο ελάχιστος χρόνος που μπορεί να διαρκέσει το scanning είναι όταν όλες οι IP διευθύνσεις απαντήσουν και αυτός είναι {αριθμός IP διευθύνσεων}*{RTT}. Στα παραπάνω δεν έχουμε υπολογίσει το χρόνο τοπικής επεξεργασίας των δεδομένων που, με τους

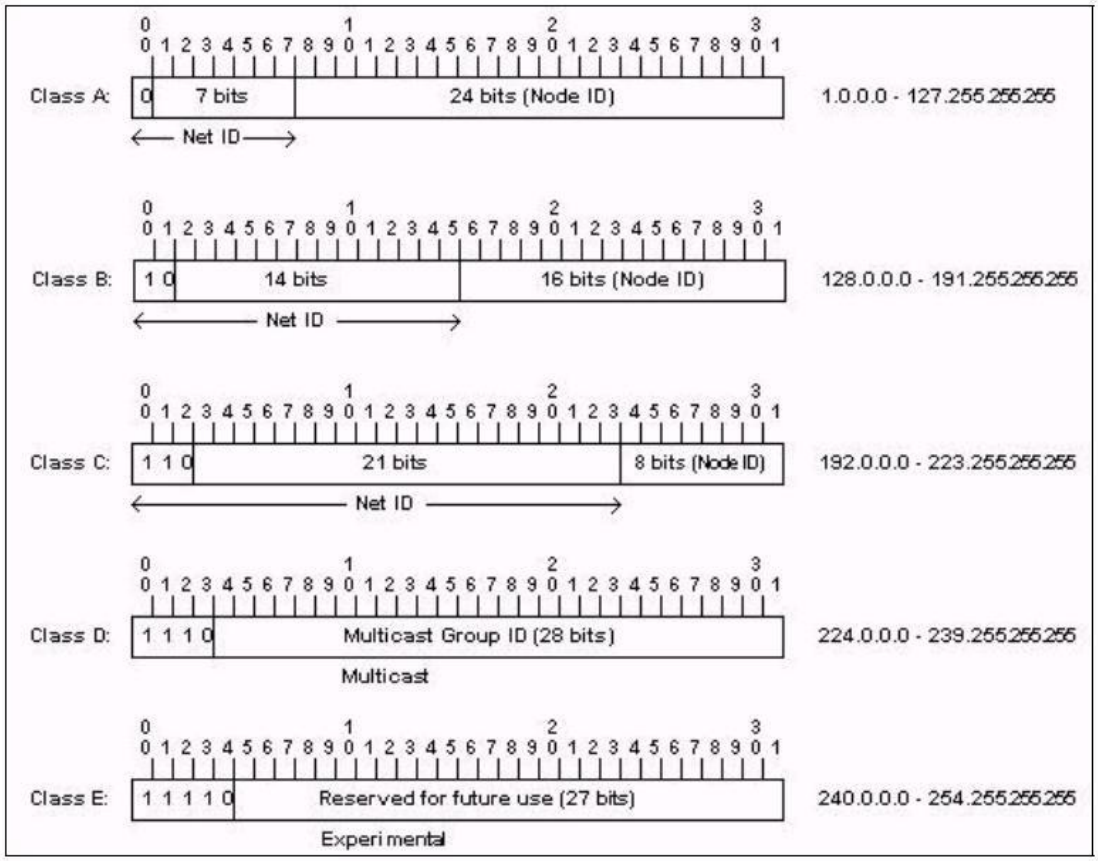
σημερινούς επεξεργαστές, είναι αμελητέος μπροστά στους χρόνους μεταφοράς των πακέτων στο δίκτυο. Τέλος, να αναφέρουμε ότι στο κάτω μέρος του παραθύρου υπάρχει ένα progress bar που μας δείχνει την πρόοδο του ψαξίματος.

4.3.2. Scan sub-network

Μια άλλη δυνατότητα που έχει ο χρήστης είναι να κάνει scan ένα υποδίκτυο. Ένα υποδίκτυο ορίζεται από μια IP διεύθυνση και το network mask. Το network mask αποτελείται, όπως και η IP διεύθυνση, από τέσσερα bytes (32 bits) και μας βοηθάει να βρούμε ποιο κομμάτι της IP διεύθυνσης αποτελεί το δίκτυο και ποιο το συγκεκριμένο μηχάνημα του δικτύου. Τα 32 bits του network mask αποτελούνται από μια σειρά από «1», ακολουθούμενα από μια σειρά από «0» (π.χ. 11111111.11111111.00000000.00000000 ή στο δεκαδικό 255.255.0.0). Οι θέσεις με «1» φανερώνουν ότι οι αντίστοιχες θέσεις στην IP διεύθυνση αποτελούν το δίκτυο. Για παράδειγμα όταν έχουμε IP διεύθυνση 195.251.17.193 και network mask 255.255.255.0 τότε:

195.251.17.193 = 11000011.11111011.00010001.11000001
255.255.255.0 = 11111111.11111111.11111111.00000000
|----------δίκτυο----------|-μηχάνημα-|

Άρα το κομμάτι της IP διεύθυνσης που δηλώνει το δίκτυο είναι το 195.251.17, ενώ το 193 δηλώνει το συγκεκριμένο μηχάνημα μέσα στο δίκτυο.
Υπάρχουν πέντε βασικές κλάσεις δικτύων (class A, B, C, D, E) και η διαφορά μεταξύ τους είναι το μέγεθός τους.



Τα class A δίκτυα έχουν network mask 11111111.00000000.00000000.00000000 ή 255.0.0.0. Τα 8 πρώτα bits (1 byte) δηλώνουν το δίκτυο και τα υπόλοιπα 24 bits το μηχάνημα μέσα στο δίκτυο. Τα δίκτυα αυτά μπορούν να έχουν μέχρι 16777214 μηχανήματα!

Τα class B δίκτυα έχουν network mask 11111111.11111111.00000000.00000000 ή 255.255.0.0. Τα 16 πρώτα bits (2 bytes) δηλώνουν το δίκτυο και τα υπόλοιπα 16 το μηχάνημα μέσα στο δίκτυο. Μπορούν να υπάρχουν μέχρι 65534 διαφορετικά μηχανήματα μέσα στο δίκτυο.

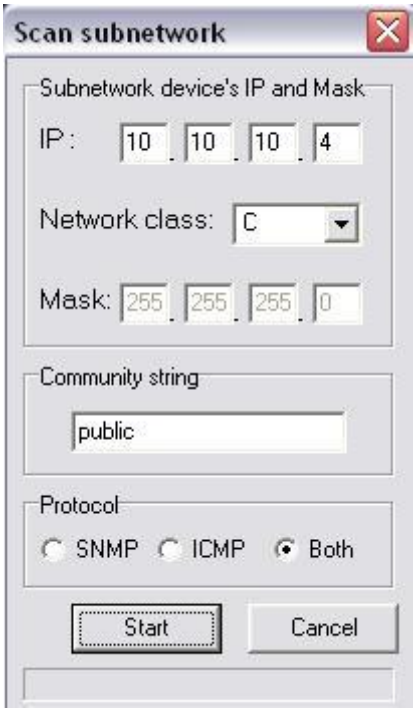
Τα class C δίκτυα έχουν network mask 11111111.11111111.11111111.00000000 ή 255.255.255.0. Τα 24 πρώτα bits (3 bytes) δηλώνουν το δίκτυο και τα υπόλοιπα 8 το μηχάνημα μέσα στο δίκτυο. Μπορούν να υπάρχουν μέχρι 254 διαφορετικά μηχανήματα μέσα στο δίκτυο.

Τα class D δίκτυα περιέχουν multicast IP διευθύνσεις και τέλος, τα class E δίκτυα είναι δεσμευμένα για πειραματικούς σκοπούς.

Επειδή οι IP διευθύνσεις κάποια στιγμή άρχισαν να λιγοστεύουν και ακόμα και η μικρότερη κλάση δικτύου (class C) ορίζει μεγάλα δίκτυα (254 μηχανήματα), μπορούμε να ορίσουμε υποδίκτυα των τριών κλάσεων A, B και C. Για παράδειγμα, μπορούμε να έχουμε το υποδίκτυο 255.255.255.224

(11111111.11111111.11111111.11100000) του class C δικτύου. Αυτό σημαίνει ότι τα 27 πρώτα bits της IP διεύθυνσης ορίζουν το δίκτυο και τα υπόλοιπα 5 το μηχάνημα. Σε αυτή την περίπτωση μπορούν να υπάρχουν 30 μηχανήματα στο υποδίκτυο (5 δυαδικά ψηφία ελευθερίας μας δίνουν 2^5=32 διαφορετικές IP διευθύνσεις, από τις οποίες η πρώτη αναφέρεται στο δίκτυο και η τελευταία είναι η broadcast διεύθυνση).

Στο πρόγραμμά μας, το scanning ενός δικτύου γίνεται δίνοντας μια IP διεύθυνση που να ανήκει στο δίκτυο, την κλάση του δικτύου ή το network mask σε περίπτωση μικρότερου υποδικτύου, το πρωτόκολλο που θα χρησιμοποιηθεί και το community string των SNMP συσκευών του δικτύου.



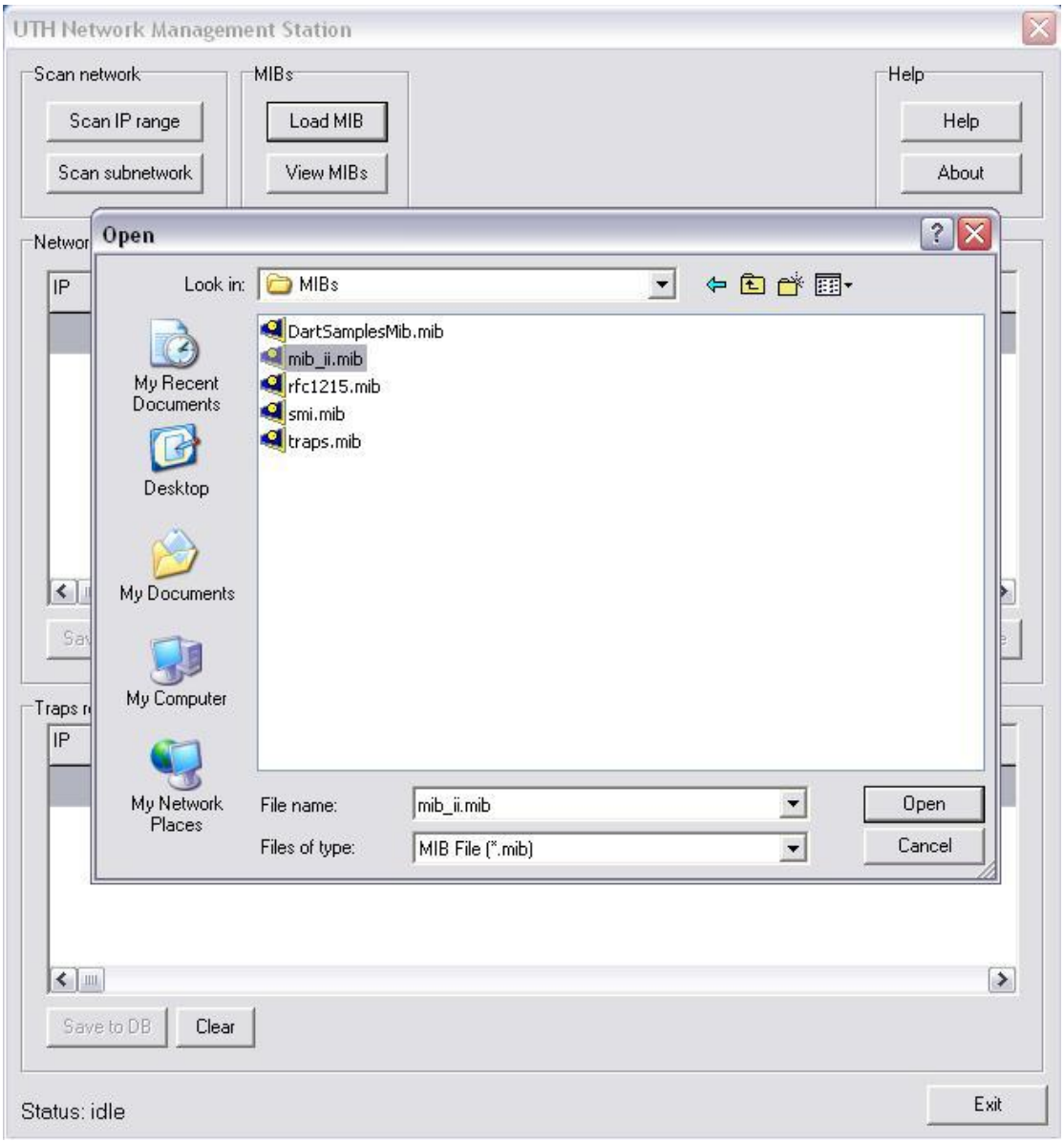
Το πρόγραμμα, χρησιμοποιώντας την IP διεύθυνση και τη network mask, υπολογίζει την αρχική και τελική IP διεύθυνση του υποδικτύου και έπειτα η διαδικασία του ψαξίματος είναι ακριβώς ίδια με το range IP scan.

4.3.3. **Δυναμικό φόρτωμα** MIB **αρχείων**

Όπως έχουμε αναφέρει, κάθε εταιρία μπορεί να δημιουργήσει τα δικά της MIB αντικείμενα που θα υποστηρίζουν οι συσκευές της. Τα αντικείμενα αυτά ορίζονται σύμφωνα με τη δομή SMI σε αρχεία «*.mib». Σε ένα τέτοιο αρχείο μπορεί να ορίζονται πολλά αντικείμενα. Για να πάρουμε την πληροφορία από αυτά τα αρχεία

πρέπει να κάνουμε parsing (διάβασμα δομημένου αρχείου). Επειδή αυτή είναι μια εργασία εξαιρετικά χρονοβόρα στον προγραμματισμό της, στο πρόγραμμά μας έχουμε χρησιμοποιήσει μια βιβλιοθήκη (dll αρχείο) του πακέτου PowerTCP SNMP Tool. Δηλώσαμε δηλαδή τα απαραίτητα dll αρχεία στην Borland Delphi 7 και μας δόθηκε η δυνατότητα να χρησιμοποιήσουμε κάποια αντικείμενα που μας παρέχουν συναρτήσεις με τις οποίες μπορούμε να φορτώνουμε «*.mib» αρχεία και να χρησιμοποιήσουμε την πληροφορία τους. Πιο συγκεκριμένα μπορούμε να για κάθε MIB αντικείμενο να δούμε το όνομά του, το object ID του, την περιγραφή του, τον τύπο του (string, integer, counter) και τον τύπο της πρόσβασης που μπορούμε να έχουμε σε αυτό (read, write, no access).

Πατώντας το κουμπί για να φορτώσουμε μια καινούρια MIB, ζητείται ο προσδιορισμός του path του αρχείου και έχουμε τη δυνατότητα να κάνουμε browse στους φακέλους του τοπικού μηχανήματος ώστε να βρούμε το MIB αρχείο. Η διαδρομή αυτή αποθηκεύεται σε ένα αρχείο με όνομα MIBs.txt, στο φάκελο «config», μέσα στο φάκελο της εγκατάστασης. Έτσι, αν κλείσουμε και ξανά-ανοίξουμε το πρόγραμμα, όλα τα MIB αρχεία που είχαμε φορτώσει θα ξανά-φορτωθούν.



Με την εγκατάσταση του λογισμικού μας παρέχονται και πέντε βασικές MIBs, που βρίσκονται στο φάκελο «MIBs», στο φάκελο εγκατάστασης:

- «SNMPv2-SMI.mib»
- «SNMPv2-TC.mib»
- «SNMPv2-CONF.mib»
- «HOST-RESOURCES-MIB.mib»
- «SNMPv2-MIB.mib»

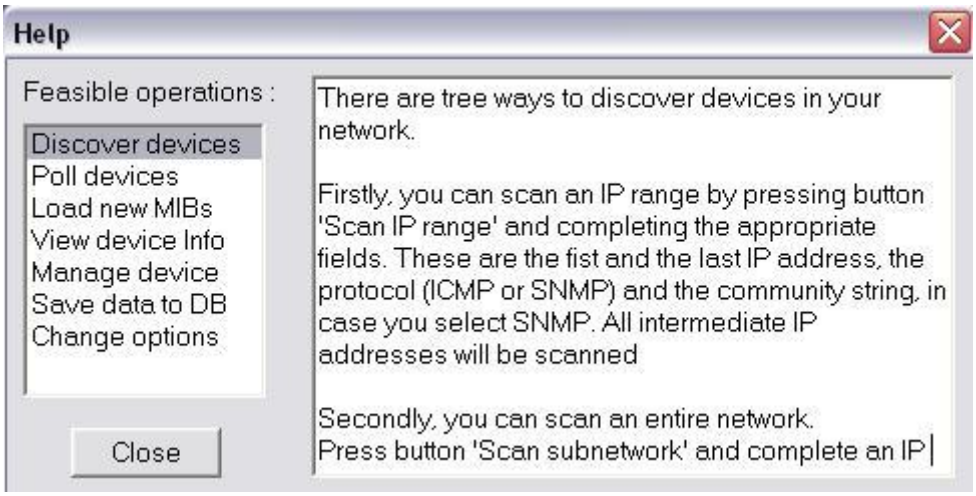
Αυτές φορτώνονται αυτόματα από το πρόγραμμα αφού χρειάζονται για την ομαλή διαχείριση των SNMP συσκευών.

4.3.4. **Εμφάνιση φορτωμένων** MIB **αρχείων**

Πατώντας το κουμπί «View MIBs» απλά βλέπουμε ποιες MIBs έχουμε ήδη φορτώσει στο πρόγραμμά μας.

4.3.5. **Βοήθεια**

Στο Help δίνονται πληροφορίες για τις δυνατότητες του λογισμικού. Πατώντας το κουμπί «Help» ένα νέο παράθυρο εμφανίζεται, στο οποίο υπάρχει μια λίστα από δυνατές λειτουργίες. Επιλέγοντας μια βλέπουμε δίπλα μια μικρή περιγραφή-βοήθεια.



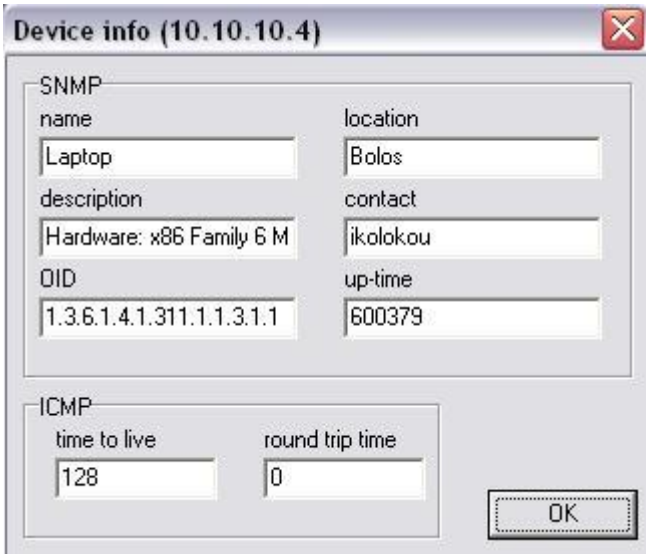
4.3.6. About

Στο «About» δίνονται πληροφορίες για την κατασκευή του λογισμικού.

4.3.7. **Λίστα συσκευών**

Στο κεντρικό παράθυρο του προγράμματός μας εμφανίζεται η λίστα των συσκευών που έχουν εντοπιστεί. Αρχικά δεν υπάρχει καμία συσκευή στη λίστα αλλά μόλις ο χρήστης κάνει Scan IP range ή Scan subnetwork τότε, σταδιακά οι συσκευές που εντοπίζονται προστίθενται στη λίστα. Οι πληροφορίες που βλέπουμε άμεσα για κάθε συσκευή είναι η IP διεύθυνσή της, η κατάσταση που βρίσκεται (up ή down) και το πρωτόκολλο που χρησιμοποιήθηκε για να βρεθεί (ICMP, SNMP ή και τα δυο). Αν το

πρωτόκολλο είναι το SNMP τότε βλέπουμε και επιπλέον πληροφορίες όπως το όνομα, τον κατασκευαστή και τον τύπο της συσκευής. Για ακόμα περισσότερες πληροφορίες μπορούμε να κάνουμε double click σε μια συσκευή και ένα παράθυρο σαν το παρακάτω θα εμφανιστεί.



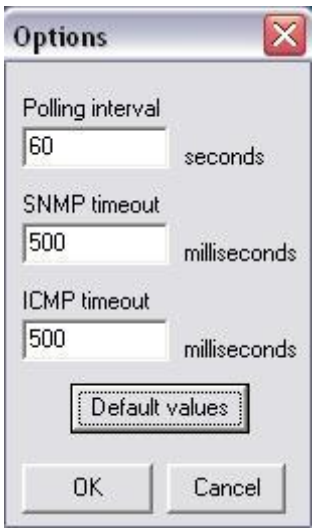
Οι πληροφορίες που δίνονται για τη συσκευή αν υποστηρίζεται το SNMP είναι το όνομά της, η τοποθεσία της, η περιγραφή της, ο υπεύθυνος-διαχειριστής της, το ID της και ο χρόνος σε timeticks που αυτή είναι ενεργή. Αν υποστηρίζεται το ICMP, τότε βλέπουμε το time to live (TTL) και το round trip time (RTT) του ping πακέτου.

4.3.8. Polling

Σε κάθε συσκευή που βρίσκεται στη λίστα, κάθε ένα συγκεκριμένο χρονικό διάστημα (polling interval), γίνεται polling. Δηλαδή, το NMS στέλνει ένα μήνυμα (ICMP ping και SNMP πακέτα) για να δει αν η συσκευή είναι ακόμα σε λειτουργία ή αν η κατάστασή της έχει αλλάξει. Μπορεί σε κάποια συσκευή ξαφνικά να γίνει αλλαγή στο όνομα ή την περιγραφή της, ή η συσκευή να πάψει να επικοινωνεί με το NMS. Οποιαδήποτε τέτοια αλλαγή θα γίνει αμέσως φανερή. Η default τιμή του polling interval είναι τα 60 δευτερόλεπτα, αλλά αυτό ο χρήστης μπορεί να το αλλάξει. Η αλλαγή γίνεται από το πλήκτρο «Options».

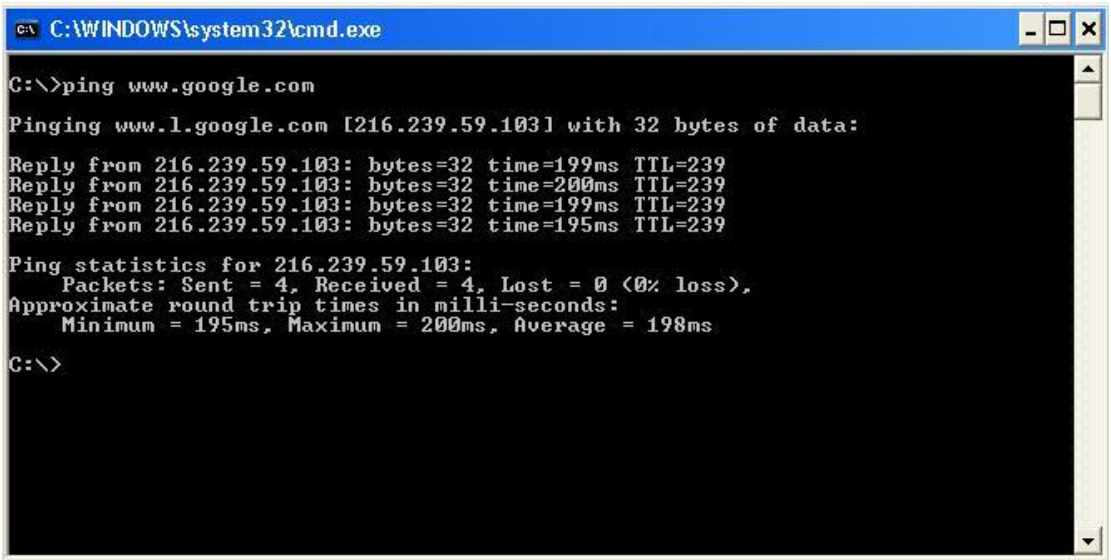
4.3.9. **Ρυθμίσεις**

Επιλέγοντας το πλήκτρο «Options» στο κεντρικό παράθυρο, εμφανίζεται ένα νέο παράθυρο με κάποιες τιμές που μπορούμε να ρυθμίσουμε.



- Το «polling interval» που είδαμε και πριν, είναι ο χρόνος που αναμένει το NMS μεταξύ δυο διαδοχικών polling. Μετριέται σε δευτερόλεπτα και έχει default τιμή 60 seconds.
- Το «SNMP timeout», που επίσης αναφέραμε πριν, είναι ο χρόνος που το NMS αναμένει για απάντηση αφού στείλει ένα SNMP get.
- Τέλος, το «ICMP timeout» είναι ο χρόνος που το NMS αναμένει για απάντηση αφού στείλει ένα ICMP ping.

Οι δυο τελευταίοι χρόνοι μετρούνται σε milliseconds και η default τιμή τους είναι 500 millisecond. Για να καταλάβουμε αν αυτές οι τιμές είναι λογικές, κάνουμε ένα ping σε έναν host εκτός του δικτύου μας και παρατηρούμε το RTT (Round Trip Time).

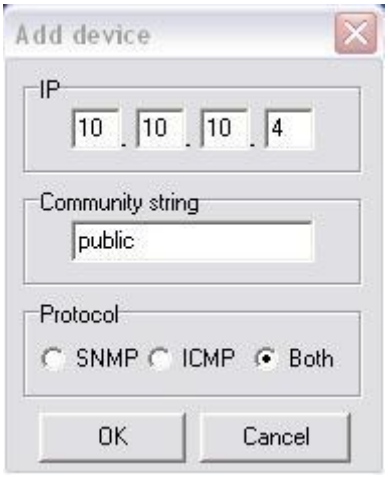


Βλέπουμε ότι ο μέσος όρος του RTT είναι 198ms αρκετά μικρότερος από τη δικιά μας default τιμή. Ακόμα, το NMS συνήθως θα επικοινωνεί με συσκευές εντός του τοπικού δικτύου, όπου οι χρόνοι απόκρισης είναι ακόμα μικρότεροι.

Οι τιμές που θέτουμε στο Options αποθηκεύονται στο αρχείο «options.txt» μέσα στο φάκελο «config», ώστε την επόμενη φορά που θα εκτελέσουμε το πρόγραμμα να φορτωθούν από εκεί.

4.3.10. **Προσθήκη μιας συσκευής**

Αν ο χρήστης θελήσει να προσθέσει μια συσκευή στη λίστα, της οποίας γνωρίζει την IP διεύθυνση, αυτό γίνεται πατώντας το κουμπί «Add device». Ζητούνται η IP διεύθυνση, το πρωτόκολλο αναζήτησης που θα χρησιμοποιηθεί και το community string αν το πρωτόκολλο είναι το SNMP.



4.3.11. **Διαγραφή συσκευής**

Αν ο χρήστης θελήσει να διαγράψει μια συσκευή από τη λίστα, αρκεί να επιλέξει τη συσκευή κάνοντας απλό click πάνω της και έπειτα να πατήσει το πλήκτρο «Remove device». Για διαγραφή όλων των συσκευών υπάρχει το πλήκτρο «clear».

4.3.12. **Αποθήκευση λίστας συσκευών**

Υπάρχει δυνατότητα ο διαχειριστής-χρήστης αφού έχει χαρτογραφήσει το δίκτυό του κι έχει δημιουργηθεί η επιθυμητή λίστα των συσκευών, να αποθηκεύσει τη λίστα αυτή σε βάση δεδομένων ώστε να μπορεί αργότερα να την ανακτήσει. Πατώντας το κουμπί «Save to DB», ο χρήστης μπορεί να επιλέξει την τοποθεσία που θα αποθηκευτεί και το όνομα που θα έχει το αρχείο της βάση δεδομένων. Η βάση δεδομένων που χρησιμοποιείται είναι η Microsoft Access, η οποία δεν είναι ανάγκη να είναι εγκατεστημένη στον τοπικό υπολογιστή. Απλά το αρχείο της αποθήκευσης είναι τύπου «*.mdb» και μπορεί να ανοιχτεί με την MS Access. Η βάση δεδομένων που δημιουργείται αποτελείται από έναν πίνακα με όνομα «Devices», του οποίου τα πεδία είναι τα:

- «IPstring», τύπου string, που αποθηκεύει την IP διεύθυνση της συσκευής. Το πεδίο αυτό αποτελεί και πρωτεύον κλειδί, αφού η IP διεύθυνση κάθε συσκευής είναι μοναδική.
- «communityStr», τύπου string, που αποθηκεύει το community string των συσκευών που υποστηρίζουν το SNMP.
- «SNMPprotocol», τύπου Boolean, που μας δείχνει αν η συσκευή υποστηρίζει SNMP ή όχι.
- «ICMPprotocol», τύπου Boolean, που μας δείχνει αν η συσκευή υποστηρίζει ICMP ή όχι.
- «typeString», τύπου string, που αποθηκεύει τον τύπο της συσκευής (hub, access point, router), αν αυτός έχει βρεθεί και αν η συσκευή υποστηρίζει το SNMP.
- «nameString», τύπου string, που αποθηκεύει το όνομα της συσκευής, αν αυτή υποστηρίζει το SNMP.
- «vendorString», τύπου string, που αποθηκεύει το όνομα του κατασκευαστή, επίσης αν η συσκευή υποστηρίζει το SNMP και έχει βρεθεί ο κατασκευαστής της.

4.3.13. **Φόρτωμα λίστας συσκευών**

Αφού ο διαχειριστής αποθηκεύσει σε βάση δεδομένων τις συσκευές που έχει ανακαλύψει, μπορεί οποιαδήποτε στιγμή να τις ανακτήσει από τη βάση δεδομένων. Πατώντας το κουμπί «Load from DB» μπορεί ο χρήστης να βρει το αρχείο «*.mdb» της βάσης δεδομένων που θέλει να φορτώσει. Οι συσκευές φορτώνονται στη λίστα

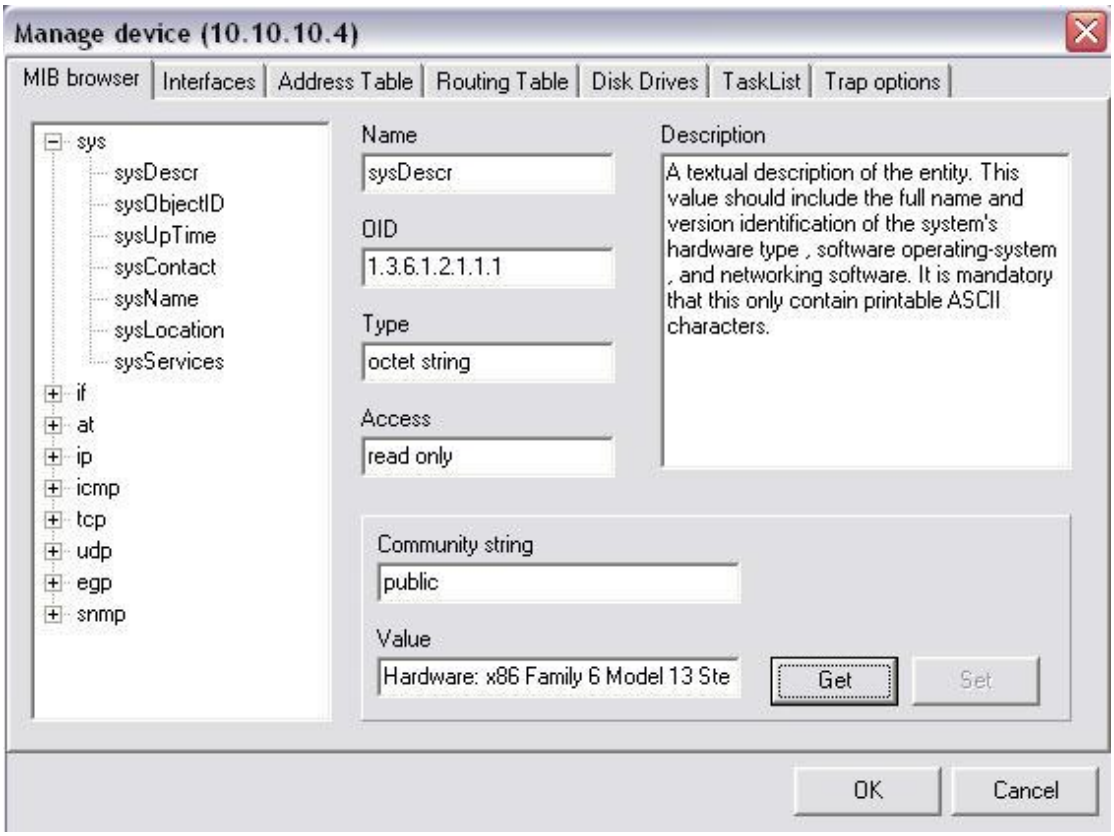
του κεντρικού παραθύρου του προγράμματος αλλά με status down. Έπειτα, γίνεται αυτόματα polling όλων των συσκευών ώστε να βρεθεί το πραγματικό status τους και οι τυχών αλλαγές που έχουν γίνει.

4.3.14. **Διαχείριση** SNMP **συσκευής**

Τις συσκευές που υποστηρίζουν το SNMP, μπορούμε να τις διαχειριστούμε μέσα από το NMS. Αυτό γίνεται μέσω των MIB αντικειμένων, των οποίων τις τιμές μπορούμε να δούμε και να τροποποιήσουμε. Επιλέγοντας από τη λίστα μια συσκευή που να υποστηρίζει το SNMP, ενεργοποιείται το κουμπί «Manage» που μας οδηγεί σε νέο παράθυρο με περισσότερες επιλογές διαχείρισης της συσκευής. Στο παράθυρο αυτό υπάρχουν tab sheets τα οποία μας παρέχουν πληροφορίες για τη συσκευή και μας επιτρέπουν να κάνουμε επιθυμητές ρυθμίσεις σε MIB αντικείμενα αυτής. Ακόμα, μπορούμε να ρυθμίσουμε την αντίδραση του NMS σε εισερχόμενα traps από τη συσκευή.

4.3.14.1. MIB browser

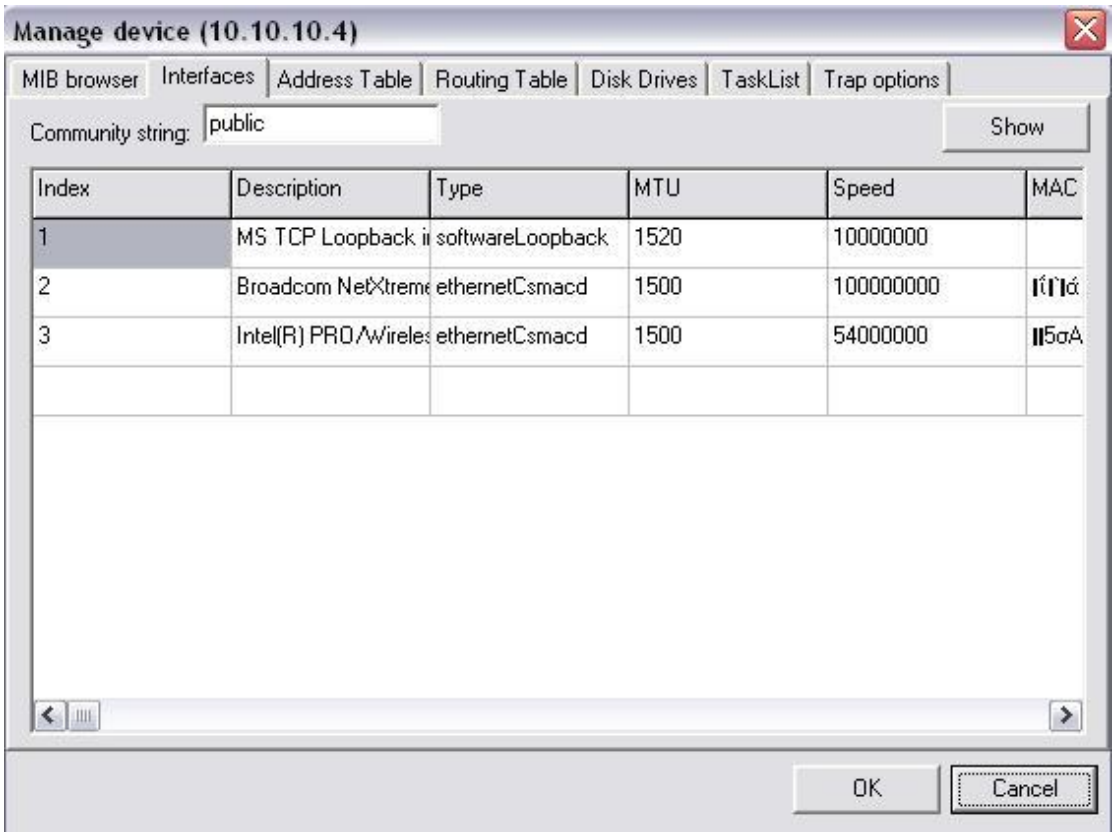
Στο tab sheet «MIB browser» έχουμε της δυνατότητα να δούμε το δέντρο με τα MIB αντικείμενα που έχουμε φορτώσει στο NMS. Επιλέγοντας οποιοδήποτε αντικείμενο θέλουμε από το δέντρο, εμφανίζεται η πλήρης περιγραφή του.



Επιλέγοντας το κατάλληλο community string και πατώντας το κουμπί «Get», εμφανίζεται η τιμή που έχει το αντικείμενο αυτό στη συσκευή που έχουμε επιλέξει, αν βέβαια η συσκευή αυτή υποστηρίζει το συγκεκριμένο MIB αντικείμενο. Μάλιστα, αν το αντικείμενο έχει write access τότε το κουμπί «Set» ενεργοποιείται και μπορούμε να δώσουμε μια νέα τιμή στο πεδίο «value» και να την αναθέσουμε στο αντικείμενο της συσκευής. Στην τελευταία περίπτωση θα χρειαστεί να αλλάξουμε και το community string σε «private» ή στην τιμή που μας δίνει write access στη συγκεκριμένη συσκευή. Το αν η τροποποίηση του αντικειμένου ήταν επιτυχημένη ή αποτυχημένη, ανακοινώνεται σε pop up μήνυμα.

4.3.14.2. Interfaces

Στο tab sheet αυτό, μπορούμε να δούμε τα network interfaces που έχει η συσκευή που έχει επιλεγεί. Η πληροφορία αυτή μας δίνεται μέσω του SNMP οπότε χρειάζεται να προσδιοριστεί το community string που δίνει read access στη συγκεκριμένη συσκευή. By default χρησιμοποιείται η τιμή «public» αλλά αν δεν είναι σωστή τότε πρέπει ο χρήστης να εισάγει τη σωστή τιμή και να πατήσει το κουμπί «Show».



Στον πίνακα που εμφανίζεται υπάρχουν πολλές στήλες, κάθε μια από τις οποίες μας δίνει μια πληροφορία που παίρνουμε από ένα αντικείμενο της MIB. Ακολουθεί μια περιγραφή των στηλών:

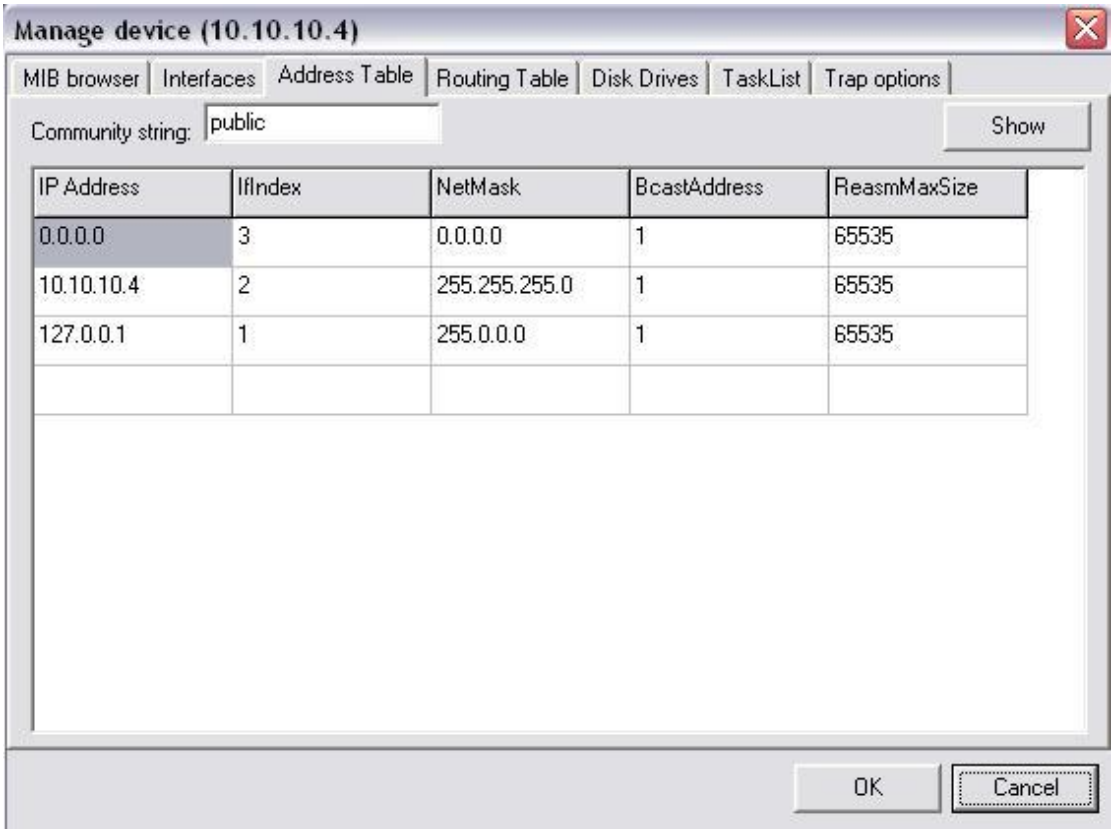
- «Index» είναι ο αύξων αριθμός του interface.
- «Description» είναι μια περιγραφή του interface.
- «Type» είναι ο τύπος του interface (π.χ. Ethernet, ATM, ISDN κ.ά.). Η τιμή αυτού του πεδίου είναι ένας integer από 1 έως 140, όπου κάθε αριθμός αντιστοιχεί σε ένα δεδομένο τύπο interface.
- «MTU» είναι το μέγεθος του μεγαλύτερου UDP πακέτου που μπορεί να σταλεί από αυτό το interface, μετρημένο σε octets (1 octet = 8 bits).
- «Speed» είναι η μέγιστη ταχύτητα που υποστηρίζει αυτό το interface (Baud rate).
- «MAC address» είναι η physical address της κάρτας του interface.
- «Admin status» είναι η επιθυμητή από το διαχειριστή κατάσταση του interface. Παίρνει τιμές από 1 έως 5, οι οποίες αντιστοιχούν σε 1: up, 2: down, 3: testing, 4: unknown και 5: dormant.
- «Oper status» είναι η τρέχουσα κατάσταση λειτουργίας του interface και παίρνει τιμές όμοιες με τις παραπάνω (up, down, testing).

- «Last change» δείχνει την τιμή που είχε το αντικείμενο «sysUpTime» όταν έγινε η τελευταία αλλαγή στην κατάσταση του interface. Αν δεν υπήρξε αλλαγή στο interface από όταν η συσκευή μπήκε σε λειτουργία τότε η τιμή του «Last change» είναι μηδέν. Το «sysUpTime» δείχνει το χρόνο σε εκατοστά του δευτερολέπτου από την εκκίνηση λειτουργίας της συσκευής.
- «InOctets» είναι ο συνολικός αριθμός από octets που έχουν ληφθεί από το interface.
- «InUcastPkts» είναι ο αριθμός από unicast πακέτα του υποδικτύου που έχουν παραδοθεί σε υψηλότερου επιπέδου (layer) πρωτόκολλο.
- «InNUcastPkts» είναι ο αριθμός από μη unicast πακέτα του υποδικτύου (π.χ. broadcast ή multicast) που έχουν παραδοθεί σε υψηλότερου επιπέδου (layer) πρωτόκολλο.
- «InDiscards» είναι ο αριθμός των εισερχόμενων πακέτων που «πετάχτηκαν» (discarded) ενώ δεν είχαν κάποιο σφάλμα (π.χ. λόγω έλλειψης buffer).
- «InErrors» είναι ο αριθμός των εισερχόμενων πακέτων που δεν παραδόθηκαν σε πρωτόκολλο υψηλότερου επιπέδου λόγω σφάλματός τους (error).
- «InUnknownProtos» είναι ο αριθμός των εισερχόμενων πακέτων που έπρεπε να «πεταχτούνε» διότι αναφέρονταν σε άγνωστο πρωτόκολλο (μη υποστηριζόμενο).
- «OutOctets» είναι ο αριθμός από octets που στάλθηκαν από το interface προς το δίκτυο.
- «OutUcastPkts» είναι ο αριθμός των πακέτων που πρωτόκολλα υψηλότερου επιπέδου ζήτησαν να μεταδοθούν προς unicast IP διευθύνσεις, μαζί με αυτά που τελικά δεν κατάφεραν να μεταδοθούν λόγω λαθών.
- «OutNUcastPkts» είναι ο αριθμός των πακέτων που πρωτόκολλα υψηλότερου επιπέδου ζήτησαν να μεταδοθούν προς μη unicast IP διευθύνσεις (π.χ. broadcast ή multicast), μαζί με αυτά που τελικά δεν κατάφεραν να μεταδοθούν λόγω λαθών.
- «OutDiscards» είναι ο αριθμός των πακέτων προς μετάδοση που «πετάχτηκαν» (discarded) ενώ δεν είχαν κάποιο σφάλμα (π.χ. λόγω έλλειψης buffer).
- «OutErrors» είναι ο αριθμός των πακέτων προς μετάδοση που δε μπόρεσαν να μεταδοθούν λόγω λαθών.
- «OutQLen» το μέγεθος σε πακέτα της ουράς των πακέτων προς μετάδοση.

- «Specific» είναι ένα αντικείμενο που η περιγραφή του εξαρτάται από τον τύπο του interface. Δηλαδή, ανάλογα με τον τύπο του interface, το αντικείμενο μπορεί να παριστάνει και κάτι διαφορετικό. Η default τιμή, που του δίνεται όταν δε χρησιμοποιείται, είναι «0.0».

4.3.14.3. Address Table

Στο tab sheet αυτό φαίνεται ο πίνακας διευθύνσεων της επιλεγμένης συσκευής. Τα δεδομένα που παρουσιάζονται και πάλι λαμβάνονται από τη συσκευή μέσω SNMP, οπότε πρέπει να δοθεί το κατάλληλο community string. By default χρησιμοποιείται το «public».



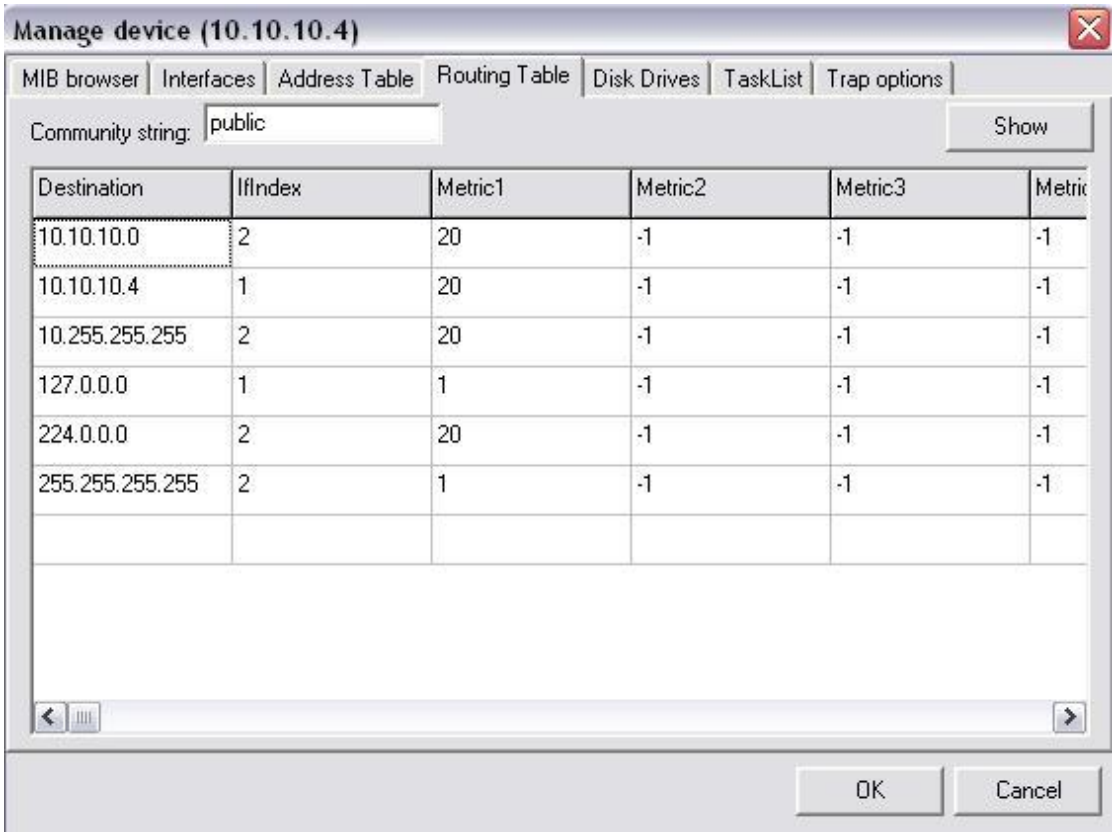
Κάθε γραμμή του πίνακα αντιστοιχεί και σε ένα interface της συσκευής. Ακολουθεί περιγραφή των στηλών του πίνακα που βλέπουμε παραπάνω:

- «IP Address» είναι η IP διεύθυνση του interface της συσκευής.
- «IfIndex» είναι ο αύξων αριθμός του παραπάνω interface, όπως εμφανίστηκε και στο tab sheet «Interfaces».
- «NetMask» είναι η network mask του interface.

- «BcastAddress» είναι το λιγότερο σημαντικό ψηφίο της broadcast IP διευθύνσεως του δικτύου στο οποίο συνδέεται το interface αυτό. Αν η τιμή είναι 1 τότε η broadcast IP διεύθυνση είναι το standard, δηλαδή αρχικά το κομμάτι της IP διεύθυνσης που ορίζει το δίκτυο (που βρίσκεται με το network mask) και μετά όλα τα bits 1.
- «ReasmMaxSize» είναι το μεγαλύτερο UDP πακέτο που προέρχεται από κατακερματισμένο IP πακέτο και μπορεί να ληφθεί και να επανασυνδεθεί (re-assembled) στο interface αυτό.

4.3.14.4. Routing Table

Στο tab sheet αυτό φαίνεται το Routing Table της επιλεγμένη συσκευής. Περισσότερο ενδιαφέρον παρουσιάζεται όταν η συσκευή είναι ένας router. Όπως και πριν, οι πληροφορίες που παρουσιάζονται αποκτώνται μέσω SNMP.



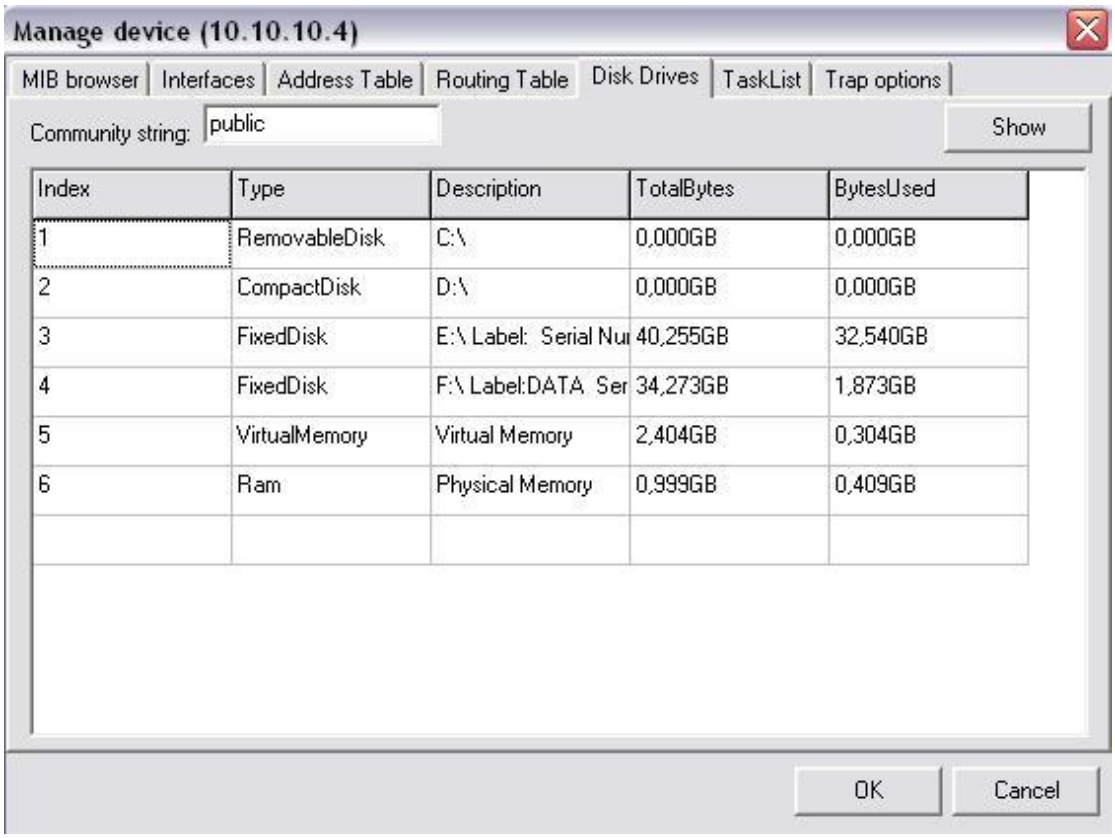
Κάθε γραμμή του πίνακα αντιστοιχεί σε μια διαδρομή (route). Ακολουθεί η περιγραφή των στηλών του πίνακα:

- «Destination» είναι η IP διεύθυνση του προορισμού. Η τιμή «0.0.0.0» μπορεί να εμφανιστεί και σημαίνει την default διαδρομή (route).

- «IfIndex» είναι ο αύξον αριθμός του interface της συσκευής, μέσω του οποίου θα βρούμε το next hop (επόμενο κόμβο) της διαδρομής αυτής.
- «Metric1» είναι ένα αντικείμενο του οποίου η έννοια εξαρτάται από το πρωτόκολλο της δρομολόγησης. Η τιμή «-1» σημαίνει ότι το metric αυτό δε χρησιμοποιείται. Ομοίως και για τα «Metric2», «Metric3», «Metric4» και «Metric5».
- «NextHop» είναι η IP διεύθυνση του επόμενου κόμβου (next hop) της διαδρομής.
- «Type» είναι ο τύπος της διαδρομής. Είναι αριθμός που παίρνει τιμές από 1 έως 4. Οι τιμές αυτές αντιστοιχούν στα: 1: other, 2: invalid, 3: direct και 4: indirect.
- «Proto» είναι ο μηχανισμός δρομολόγησης μέσω του οποίου γνωστοποιήθηκε αυτή η διαδρομή. Παίρνει τιμές από 1 έως 14 που αντιστοιχούν στα: 1: other, 2: local, 3: netmgmt, 4: icmp, 5: egp, 6: ggp, 7: hello, 8: rip, 9: is-is, 10: es-is, 11: cicolgrp, 12: bbnSpflgp, 13: ospf και 14: bgp.
- «Age» είναι τα δευτερόλεπτα που έχουν περάσει από τη στιγμή που η διαδρομή αυτή έγινε updated.
- «Mask» είναι το network mask της IP διεύθυνσης του προορισμού.
- «Info» είναι ένα αντικείμενο που η περιγραφή του εξαρτάται από το πρωτόκολλο που είναι υπεύθυνο για αυτή τη διαδρομή. Δηλαδή, ανάλογα με το πρωτόκολλο, το αντικείμενο μπορεί να αντιστοιχεί και σε κάτι διαφορετικό. Η default τιμή, που του δίνεται όταν δε χρησιμοποιείται, είναι «0.0».

4.3.14.5. Disk Drives

Σε αυτό το tab sheet, παίρνουμε πληροφορίες για τους δίσκους της συσκευής και την κατάστασή τους. Αυτή η πληροφορία είναι σημαντική ειδικά αν η συσκευή είναι ένας server.

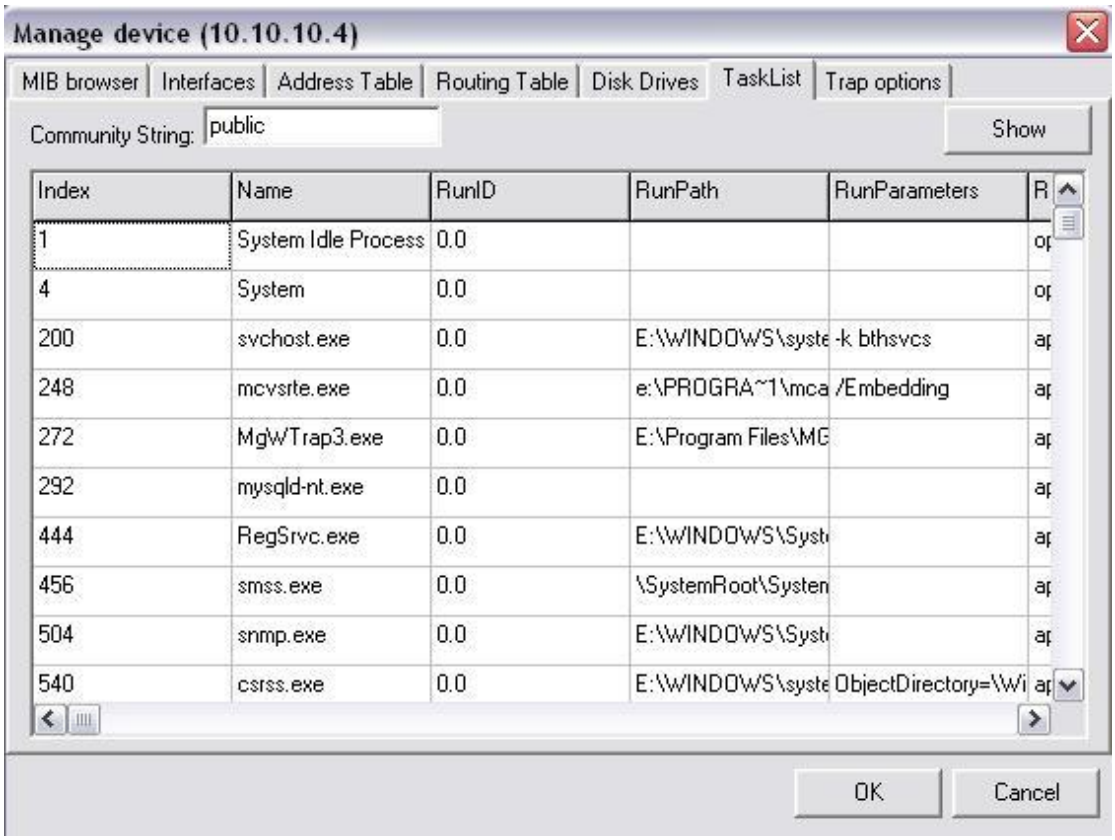


Κάθε γραμμή του πίνακα αντιστοιχεί σε μια μνήμη (RAM ή ROM). Η περιγραφή κάθε στήλης ακολουθεί:

- «Index» είναι ένας αύξων αριθμός που αντιστοιχεί σε μια μνήμη.
- «Type» είναι ο τύπος της μνήμης. Οι πιθανοί τύποι είναι «Ram», «VirtualMemory», «FixedDisk», «RemovableDisk», «FloppyDisk», «CompactDisk», «RamDisk» και «other».
- «Description» είναι μια περιγραφή της μνήμης. Συνήθως το όνομά της.
- «TotalBytes» είναι η συνολική χωρητικότητα της μνήμης.
- «BytesUsed» είναι το μέγεθος της μνήμης που χρησιμοποιείται.

4.3.14.6. Task List

Αυτό το tab sheet εμφανίζει τα προγράμματα (tasks) που τρέχουν στην επιλεγμένη συσκευή.

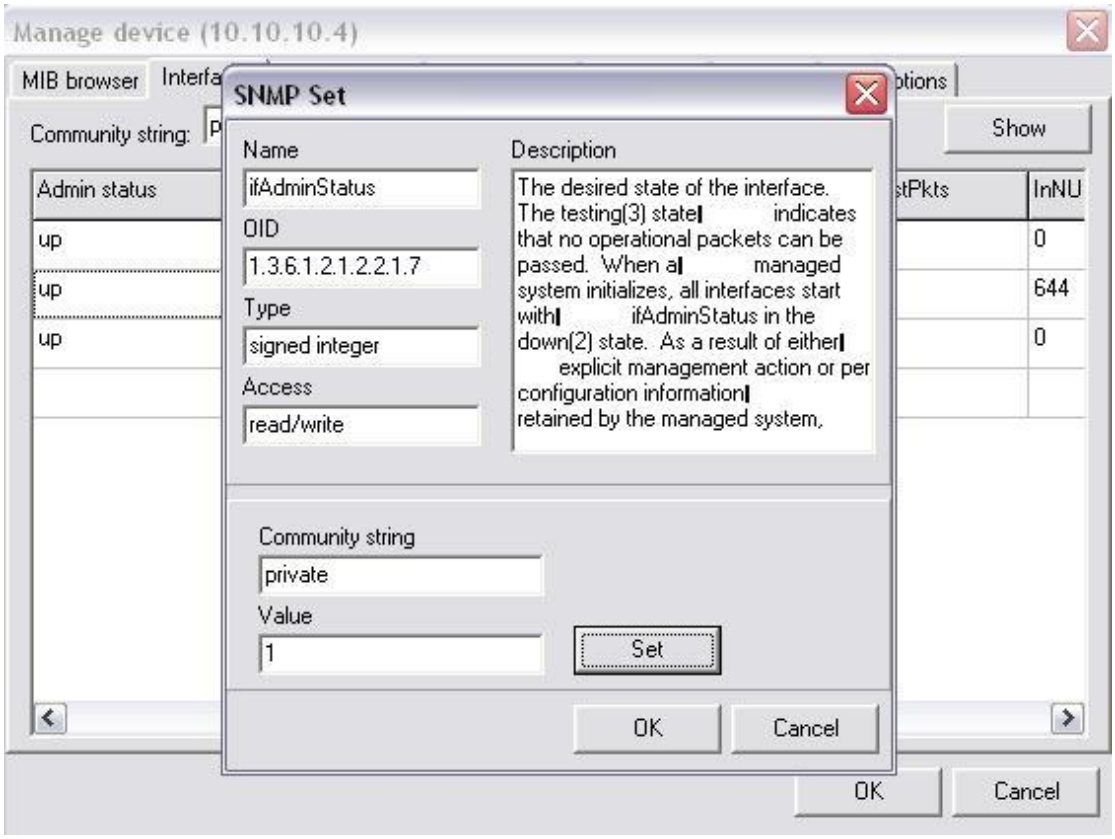


Κάθε γραμμή είναι και ένα διαφορετικό task. Η περιγραφή των στηλών ακολουθεί:

- «Index» είναι ένας μοναδικός αριθμός που αντιστοιχεί στο κάθε πρόγραμμα.
- «Name» είναι το όνομα του προγράμματος.
- «RunID» είναι το ID του λογισμικού πακέτου του προγράμματος.
- «RunPath» είναι το path από το οποίο φορτώθηκε το πρόγραμμα.
- «RunParameters» είναι οι παράμετροι που χρησιμοποιήθηκαν όταν φορτώθηκε το πρόγραμμα.
- «RunType» είναι ο τύπος του προγράμματος. Οι δυνατές τιμές είναι «operatingSystem», «deviceDriver», «application» και «unknown».
- «RunStatus» είναι η τρέχουσα κατάσταση του προγράμματος. Οι δυνατές τιμές είναι «running», «runnable», «notRunnable» και «invalid». Μάλιστα, αν θέσουμε την τιμή ενός προγράμματος σε «invalid» τότε το πρόγραμμα αυτό θα σταματήσει να τρέχει και θα εκπέσει από τη μνήμη.

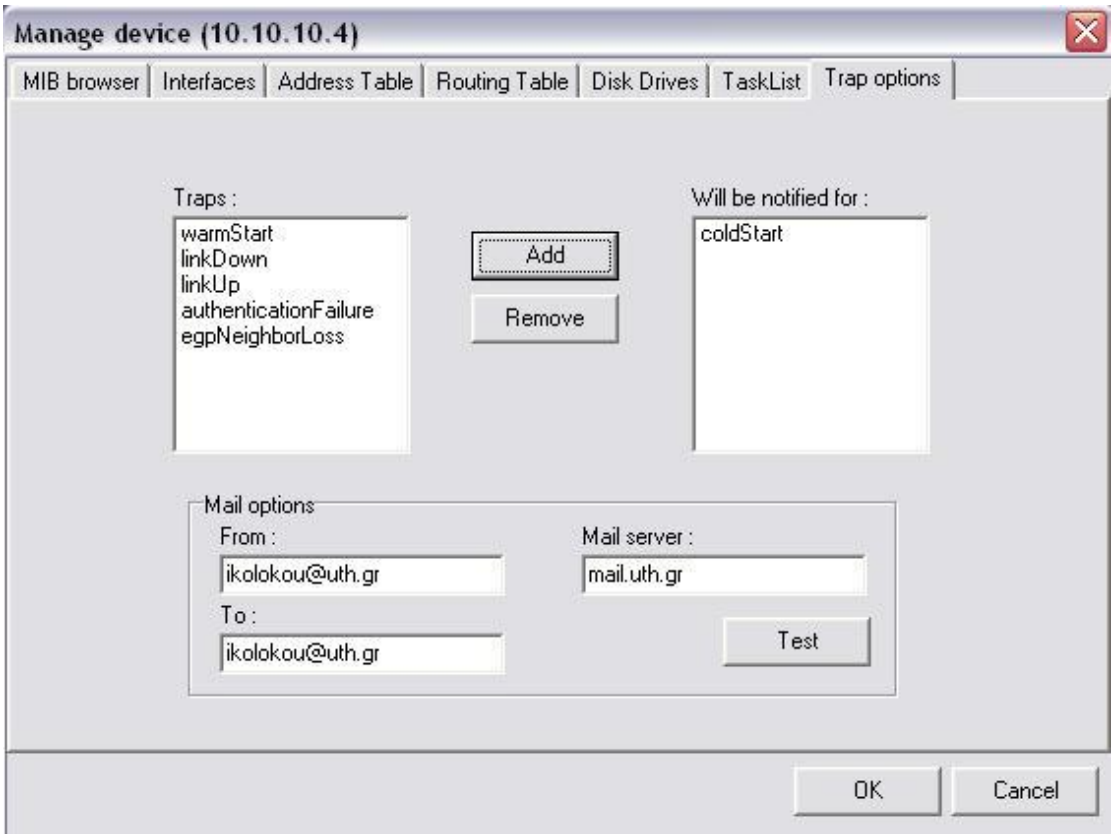
Σε οποιονδήποτε από τους πίνακες (δηλαδή τα tab sheets) που είδαμε μέχρι τώρα, αν κάνουμε double click σε κάποιο κελί βλέπουμε ένα παράθυρο που μας δίνει τη δυνατότητα να κάνουμε set το αντικείμενο αυτό, αν βέβαια το αντικείμενο που το κελί αντιπροσωπεύει μας δίνει δικαίωμα write. Στο παράθυρο αυτό εμφανίζονται όλες

οι πληροφορίες που αφορούν το αντικείμενο, καθώς και η πιο πρόσφατη τιμή του. Αν, όπως είπαμε, υπάρχει write access τότε μπορούμε να πληκτρολογήσουμε την επιθυμητή τιμή του αντικειμένου και να πατήσουμε το πλήκτρο «Set». Διαφορετικά το κουμπί «Set» θα είναι απενεργοποιημένο.



4.3.14.7. **Ρυθμίσεις ενημέρωσης κατά τη λήψη** Trap

Στο τελευταίο αυτό tab sheet, ο διαχειριστής μπορεί να ορίσει αν θα ειδοποιηθεί σε περίπτωση λήψης trap μηνύματος από τη συσκευή που έχει επιλεγεί. Υπάρχει μια λίστα με όλα τα generic traps, δηλαδή τα γενικά ορισμένα traps για όλες τις συσκευές, από την οποία μπορεί να διαλέξει αυτά για τα οποία θέλει να ειδοποιηθεί (πατώντας «Add»). Επίσης, επειδή η ειδοποίηση γίνεται μέσω e-mail, ζητούνται ο mail server που θα χρησιμοποιηθεί και οι διευθύνσεις του αποστολέα και του παραλήπτη. Πατώντας το πλήκτρο «Test» στέλνεται ένα δοκιμαστικό e-mail για να σιγουρευτεί ο χρήστης ότι έχει συμπληρώσει τα στοιχεία σωστά.



Η πληροφορία του πότε πρέπει να ειδοποιήσει και ποιόν το NMS, αποθηκεύεται σε μια βάση δεδομένων. Το αρχείο της βάσης αυτής ονομάζεται «trapNotification.mdb» και βρίσκεται μέσα στο φάκελο «DataBases», του φακέλου εγκατάστασης. Η βάση δεδομένων αυτή, αποτελείται από έναν πίνακα με όνομα «TrapNot». Τα πεδία του πίνακα αυτού είναι τα:

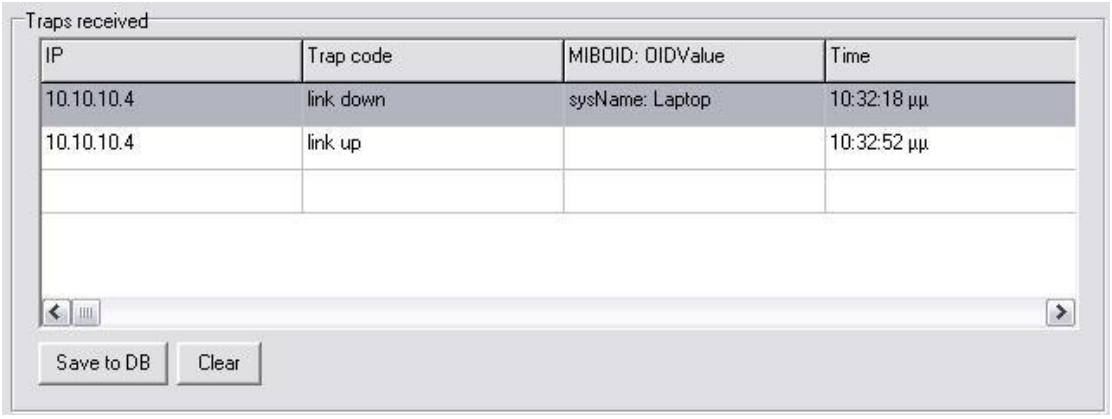
- «IPstring» που αποθηκεύει την IP διεύθυνση της συσκευής από την οποία αν έρθει το trap θα πρέπει να σταλεί το e-mail.
- «name» που κρατά το όνομα του trap.
- «OID» που είναι το object ID του trap αντικειμένου.
- «fromMail» που αποθηκεύει την ηλεκτρονική διεύθυνση του αποστολέα.
- «toMail» που αποθηκεύει την ηλεκτρονική διεύθυνση του παραλήπτη.
- «mailServer» που ορίζεται ο mail server που θα χρησιμοποιηθεί για την αποστολή του e-mail.

Η αποθήκευση των παραπάνω δεδομένων γίνεται για δυο λόγους. Ο κύριος είναι για να ξέρει το NMS πώς να δράσει όταν λάβει ένα trap από μια συσκευή. Δηλαδή να ψάξει τη βάση δεδομένων και αν υπάρχει η κατάλληλη εγγραφή να στείλει e-mail στον κατάλληλο παραλήπτη. Ο δεύτερος λόγος είναι όταν ξανά-επιλέξει ο χρήστης το

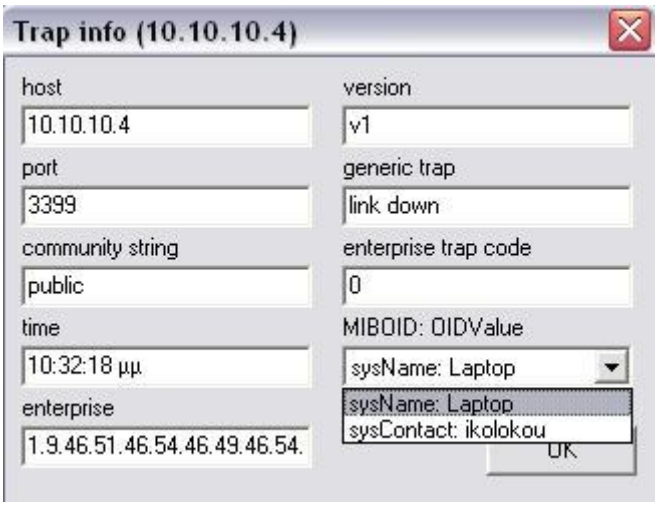
tab sheet αυτό να μπορεί να δει τα traps για τα οποία έχει επιλέξει να ειδοποιείται, όταν προέρχονται από την επιλεγμένη συσκευή.

4.3.15. **Εισερχόμενα** Traps

Κατά την εκκίνηση του NMS μας λογισμικού, ένα ανεξάρτητο thread ξεκινά, το οποίο είναι υπεύθυνο για τη λήψη των trap μηνυμάτων από τους agents. Το thread αυτό ακούει συνεχώς στο udp port 162, όπου φτάνουν τα trap μηνύματα. Μόλις λάβει ένα μήνυμα τότε το επεξεργάζεται και το εμφανίζει στη λίστα των trap μηνυμάτων στο κυρίως παράθυρο του προγράμματος.



Οι πληροφορίες που παίρνουμε με την πρώτη ματιά είναι η IP διεύθυνση της συσκευής που έστειλε το trap, το όνομά του, η ώρα που έφτασε και το πρώτο από τα ζεύγη MIB αντικείμενο-τιμή που πιθανά να έχουν σταλεί με το trap. Τα ζεύγη αυτά είναι τα variable binding που είδαμε παραπάνω στη μορφή του trap πακέτου. Μας δίνουν πληροφορίες σχετικές με την κατάσταση της συσκευής και το λόγο που στάλθηκε. Για να δούμε ακόμα περισσότερες πληροφορίες μπορούμε να κάνουμε double click στο επιθυμητό trap από τη λίστα. Τότε, ένα νέο παράθυρο εμφανίζεται.



Μπορούμε επιπλέον να δούμε το udp port από το οποίο στάλθηκε το trap, το community string του trap, το enterprise ID της συσκευής, την έκδοση του SNMP trap (version 1, version 2) και μια λίστα με όλα τα ζεύγη MIB αντικειμένου-τιμής που στάλθηκαν με το trap.

4.3.16. **Αποθήκευση των** Traps

Έχοντας λάβει μια σειρά από traps, μπορούμε πατώντας το κουμπί «Save to DB» να σώσουμε τα δεδομένα που μας παρέχουν σε βάση δεδομένων. Η αποθήκευση γίνεται σε αρχείο τύπου MS Access, του οποίου το όνομα και ο προορισμός αποθήκευσης επιλέγεται από το χρήστη. Η βάση δεδομένων αποτελείται από δυο πίνακες, τον «Traps» και τον «mibOIDValues». Ο πίνακας Traps περιέχει τα παρακάτω πεδία:

- «host», τύπου string, όπου αποθηκεύεται η IP διεύθυνση της συσκευής που έστειλε το trap.
- «port», τύπου integer, όπου αποθηκεύεται το udp port από όπου στάλθηκε το trap.
- «community», τύπου string, όπου αποθηκεύεται το community string που χρησιμοποιήθηκε.
- «enterprise», τύπου string, όπου αποθηκεύεται το enterprise ID της συσκευής που έστειλε το trap.
- «genTrap», τύπου string, όπου αποθηκεύεται ο κωδικός του generic trap. Παίρνει τιμές από 0 έως 6 που αντιστοιχούν στα: 0: «coldStart», 1: «warmStart», 2: «linkDown», 3: «linkUp», 4: «AuthenticationFailure», 5:

«EgpNeighborLoss» και 6: «Enterprise specific trap» (δηλαδή κάποιο trap που ορίζεται σε MIB συγκεκριμένου κατασκευαστή).

- «specTrap», τύπου string, όπου αποθηκεύει τον κωδικό του Enterprise specific trap, αν το generic trap έχει τιμή 6.
- «version», τύπου integer, που αποθηκεύει την έκδοση του SNMP που χρησιμοποιήθηκε. Πιθανές τιμές: «v1», «v2c» και «v3».
- «timeTicks», τύπου integer, που αποθηκεύει ένα timestamp που στέλνεται μαζί με το trap. Συνήθως είναι η διάρκεια, σε εκατοστά του δευτερολέπτου, που η συσκευή ήταν σε λειτουργία όταν εξέδωσε το trap.
- «arTime», τύπου string, που αποθηκεύει τη χρονική στιγμή που λήφθηκε το trap.

Πρωτεύον κλειδί του πίνακα είναι ο συνδυασμός των πεδίων «host» και «arTime», καθώς δεν επιτρέπεται η ίδια συσκευή να στείλει περισσότερα από ένα traps την ίδια χρονική στιγμή.

Ο δεύτερος πίνακας, με όνομα «mibOIDvalues», αποτελείται από τα παρακάτω πεδία:

- «host», τύπου string, που είναι η IP διεύθυνση του αποστολέα του trap.
- «arTime», τύπου string, που είναι η χρονική στιγμή που λήφθηκε το trap.
- «mibOID»,τύπου string, που είναι το object ID ενός από τα MIB αντικείμενα που στάλθηκαν μαζί με το trap.
- «mibValue», τύπου string, που είναι η τιμή του παραπάνω αντικειμένου που στάλθηκε μαζί με το trap.

Ο πίνακας αυτός χρησιμοποιείται για να αποθηκευτούν όλα τα ζεύγη MIB αντικειμένου-τιμής που στέλνονται μαζί με το trap, των οποίων δε γνωρίζουμε από πριν τον αριθμό. Έτσι, μπορούν να υπάρχουν πολλές εγγραφές στον πίνακα αυτό με ίδιες τιμές στα «host» και «arTime» (που προσδιορίζουν μοναδικά ένα trap του πίνακα «Traps»), με διαφορετικά όμως τα «mibOID» και «mibValue».

4.3.17. **Διαγραφή των** Traps

Επιλέγοντας το πλήκτρο «clear» διαγράφεται η λίστα με τα traps που έχουν ληφθεί.

4.3.18. **Κατάσταση λογισμικού**

Τέλος, στο κάτω μέρος του κύριου παραθύρου υπάρχει το status του NMS που περιγράφει κάθε στιγμή την κατάσταση στην οποία βρίσκεται το λογισμικό.

5. **Βιβλιογραφία**

1. Δικτύωση Υπολογιστών, James F. Kurose & Keith W. Ross
2. Δίκτυα Επικοινωνιών, Jean Walrand
3. Δίκτυα και διαδίκτυα υπολογιστών, Douglas E. Comer
4. Essential SNMP, Douglas R. Mauro & Kevin J. Schmidt
5. Mastering Delphi 7, Marco Cantù
6. Essential Delphi, Marco Cantù
7. Θεμελιώδεις Αρχές Συστημάτων Βάσεων Δεδομένων, R. Elmasri & S. B. Navathe
8. Σημειώσεις μαθήματος «Ηλεκτρονικές Υπηρεσίες», Φθινόπωρο 2003, Δημήτρης Ζησιάδης

7. Links

SNMP

1. www.snmplink.org
2. www.dart.com/powertcp/snmp.asp
3. www.mibdepot.com

Delphi

1. delphi.about.com
2. www.delphibasics.co.uk
3. www.programmersheaven.com/zone2/index.htm
4. www.borland.com

Vendors

1. www.cisco.com
2. www.3com.com
3. www.d-link.com
4. www.alvarion.com

Other

1. www.iana.org
2. net-snmp.sourceforge.net
3. nino.sourceforge.net
4. www.opennms.org
5. www.tools4ever.com/products/monitormagic
6. www.castlerock.com
7. www.forthnet.gr
8. www.uth.gr

Newsgroups

1. borland.public.delphi.database.interbaseexpress
2. borland.public.interbase.opensource
3. borland.public.delphi.internet.winsock