ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ

ΠΑΡΑΡΤΗΜΑ ΧΑΝΙΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

"Διαχείριση και ασφάλεια δικτύων Η/Υ "

ΠΛΑΤΙΑΣ ΔΗΜΗΤΡΗΣ

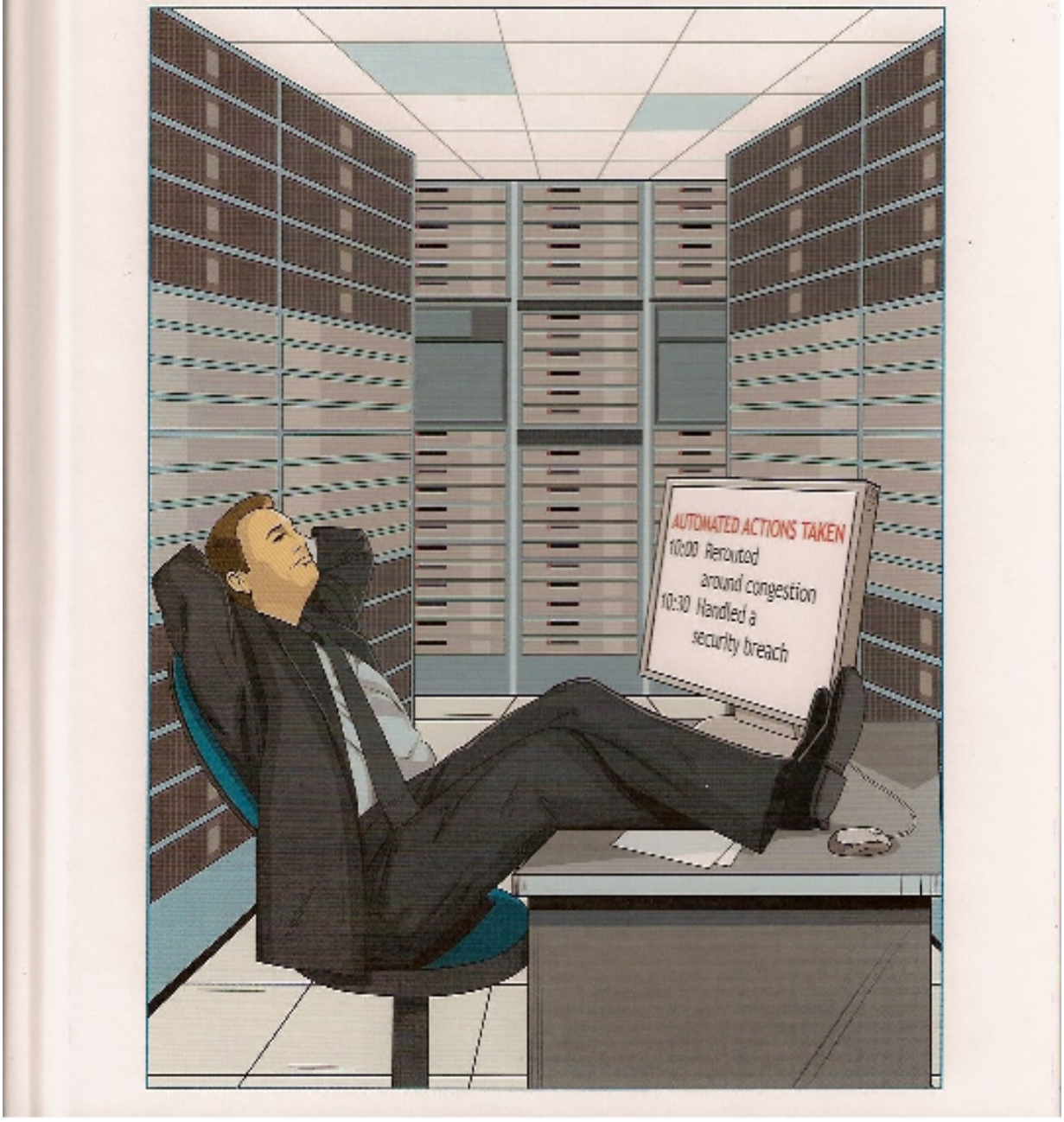
Επιβλέπων καθηγητής

Αντώνιος Ι. Ζερβουδάκης

ΧΑΝΙΑ 2010

Automated Network Management Systems

Current and Future Capabilities



ABSTRACT

Η διαχείριση δικτύων αναφέρεται στη διατήρηση και διαχείριση μεγάλων δικτύων υπολογιστών και τηλεπικοινωνιακών δικτύων στο ανώτατο επίπεδο .
Η διαχείριση δικτύων είναι η εκετελεση του συνόλου των λειτουργιών που απαιτούνται για τον έλεγχο, το σχεδιασμό, την κατανομή, την ανάπτυξη και την παρακολούθηση των πόρων του δικτύου.

Στη διαχείριση δικτύων υπάρχει ένας μεγάλος αριθμός πρωτοκόλλων για την διαχείριση και την υποστηρίξει του δικτύου και του δικτύου διαχείρισης της συσκευής
Κοινά πρωτοκολλά περιέχουν το SNMP (simple network management protocol)
CMIP (common management information protocol)
WEBMD (Web-Based Enterprise Management)
JAM (Java Management Extensions Technology)
NETCONG (Network Configuration Protocol)
Τα δεδομένα στο δίκτυο συγκεντρώνονται μεσώ διάφορων μηχανισμών συμπεριλαμβανόμενων των αντιπρόσωπων (agents) για παρακολούθηση και καταγραφή της δικτυακής κίνησης καθώς και για έλεγχο σε τερματικού σε πραγματικό χρόνο.
Σημείωση: η διαχείριση δικτύου δεν μπορεί να γίνει από χρηστή τερματικής συσκευής.

Στη παρούσα πτυχιακή εργασία θα ασχοληθούμε με τη διαχείριση του δικτύου του ΤΕΙ ΧΑΝΙΩΝ. Θα ξεκινήσουμε περιγράφοντας βασικές έννοιες πάνω στη διαχείριση δικτύων και τι τεχνολογίες χρησιμοποιούνται θα δούμε αναλυτικά το πρόγραμμα SOLARWINDS ENGINEER EDITION V8.2 το πως στήνετε το software μέρος του, την επεκτασιμότητα του καθώς και τα υπέρ και τα κατά της χρήσης του.

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1
1 Εισαγωγή στη διαχείριση δικτύων
1.1 Διαχείριση δικτύου
1.1.1 Διαχείριση παραμέτρων
1.1.2 Διαχείριση επίδοσης
1.1.3 Διαχείριση σφαλμάτων
1.1.4 Διαχείριση κόστους
1.1.5 Διαχείριση ασφάλειας
1.2 Τα μέρη που απαρτίζουν ένα σύστημα διαχείρισης
1.3 Αρχιτεκτονικές διαχείρισης δικτύων
1.3.1 Κεντρική αρχιτεκτονική
1.3.2 Ιεραρχική αρχιτεκτονική
1.3.3 Κατανεμημένη αρχιτεκτονική
1.4 Δικτυωμένο σύστημα διαχείρισης

Κεφάλαιο 2
2.Πρωτοκολλα διαχείρισης δικτύων
2.1 Το πρωτόκολλο SNMP
2.2 Το πρωτόκολλο RMON
2.3 Το πρωτόκολλο CMIP
2.4 Σύγκριση πρωτοκόλλων

Κεφάλαιο 3
3 Η πλατφόρμα solarwinds
3.1 IP address management
3.2 IP network browser
3.2.1 Scan device
3.2.2 Scan subnet
3.2.3 Scan range IP
3.3 Mac address discovery
3.4 port scanner
3.5 switch port mapper
3.6 bandwidth gauges
3.7 CPU gauge

ΕΙΣΑΓΩΓΗ

ΚΕΦΑΛΑΙΟ 1
1.Εισαγωγή στη διαχείριση δικτύων

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 είναι απαραίτητη η λεγόμενη διαχείριση δικτύου (network management).

Η διαχείριση δικτύου ορίζεται ως ένα σύνολο από λειτουργίες ενέργειες, διαδικασίες και εργαλεία που χρησιμοποιούνται για τον έλεγχο της λειτουργίας και για την εκμετάλλευση του δικτύου.
Γενικά θα μπορούμε να διαχειριστούμε

· την ελαχιστοποίηση του λειτουργικού κόστους συντήρησης.

· τη μεγιστοποίηση της απόδοσης.

· την εξασφάλισης της αξιοπιστίας στην αδιάλειπτη λειτουργία του.

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.

1.1 Διαχείριση δικτύου

Ο διεθνής οργανισμός προτυποποίησης (international organization for standardization, ISO) έχει ορίσει το πλαίσιο εργασίας(framework) για το μοντέλο διαχειρίσεις δικτύων OSI.
Με βάση το μοντέλο αυτό έχουν ορίσει πέντε περιοχές διαχείρισης:

- Διαχείριση παραμέτρων του δικτύου (configuration management)
- Διαχείριση επίδοσης του δικτύου (performance management)
- Διαχείριση σφαλμάτων (fault management)
- Διαχείριση του κόστους των υπηρεσιών (accounting management)
- Διαχείριση ασφάλειας (security management)

1.1.1Διαχείριση παραμέτρων (configuration management)

Με τον όρο διαχείριση παραμέτρων αινούμε τη διαδικασία αλλαγής της τοπολογίας του δικτύου καθώς και τη ρύθμιση των παραμέτρων των συσκευών που το αποτελούν, είτε σε επίπεδο υλικού είτε σε επίπεδο λογισμικού προκείμενου να διασφαλίσουμε τη σωστή λειτουργία του δικτύου ανάλογα με τις εκάστοτε απαιτήσεις. Η αρχική εγκατάσταση του δικτύου καθώς και η ρύθμιση των παραμέτρων των συσκευών που το αποτελούν δεν συνιστούν με βάση τον επίσημο ορισμό του μοντέλου OSI μέρος της διαχειρίσεις δικτύου Παρόλα αυτά είναι συνηθισμένο να χρησιμοποιούμε τα ίδια εργαλεία (εφαρμογές λογισμικό) για την αρχική εγκατάσταση του δικτύου όσο και για τη μετέπειτα παρακολούθηση και διαχείριση του. Γι' αυτό λόγο συχνά και η αρχική διαμόρφωση του δικτύου θεωρείτε μέρος της διαχείρισης του.

Ένα από τα σημαντικότερα έργα είναι και η τεκμηριώσει του δικτύου. Τεκμηρίωση τόσο των συσκευών με τις ρυθμίσεις που έχουν (πρωτοκολλά που χρησιμοποιούν αριθμός ενεργών θυρών φίλτρα κ.ο.κ.) όσο και της τοπολογίας του δικτύου και του τρόπου λειτουργίας του.

Η τεκμηριώσει του δικτύου βοηθάται σημαντικά από την ύπαρξη λογισμικού που ανακαλύπτει και καταγράφει σε βάση δεδομένων κατάλογου υλικών (inventory database) όλες τις συσκευές ενός δικτύου καθώς και τον τρόπο διασύνδεσης τους .συνήθως γίνεται καταγραφή όλων των ενεργών συσκευών που απαρτίζουν ένα δίκτυο όπως δρομολογητές μεταγωγεις (switches) γέφυρες επαναληπτες (hubs) τα είδη των τοπικών δικτύων όπως τμήματα Ethernet token ring κ.ο.κ, καθώς επίσης και τυχών wan γραμμές οπός ppp μισθωμένες η επιλεγόμενες (isdn) συνδέσεις x.25 frame relay κ.ο.κ.

Αν το λογισμικό που διαθέτουμε χρησιμοποιείται και για διαχείριση συστημάτων τότε γίνετε ανακάλυψη μέσο του δικτύου και των Η/Υ, εκτυπωτών και γενικότερα κάθε συσκευής που είναι συνδεμένη με το δίκτυο. Οι εφαρμογές που διαχειρίζονται το δίκτυο μπορούν να σχηματίσουν γραφικές απεικονίσεις των συσκευών του δικτύου και τη μεταξύ τους συνδεσμολογία.

1.1.2 Διαχείριση επίδοσης του δικτύου (performance management)

Για την διαχείριση της απόδοσης του δικτύου πρέπει πρώτα να ορίσουμε τι θέλουμε να μετράμε, να σχεδιάσουμε, τον τρόπο που θα γίνονται οι μετρήσεις και στη συνεχεία να υλοποιήσουμε τις μετρήσεις μας. Σε ένα δίκτυο είναι λογικό να μετρώνται σε τακτά χρονικά διαστήματα διάφορα χαρακτηριστικά όπως:

- Το ποσοστό χρησιμοποίησης των WAN γραμμών η των διάφορων τμημάτων του τοπικού δικτύου.
- Η ανάλυση του ποσοστού κίνησης ανά πρωτόκολλο π.χ. ip, NetBIOS.
- Το ποσοστό λαθών σε σχέση με όλη τη κίνηση.
- Ο χρόνος καθυστερήσεις διαφόρων σημείων του δικτύου.
- Ο χρόνος απόκρισης κάποιον συσκευών.
- Ο καθορισμός κατωφλίων σε μερικές μετρούμενες παραμέτρους. Όταν οι τιμές των παραμέτρων υπερβαίνουν τις τιμές που έχουν κριθεί ως κατώφλια τότε θα πρέπει να δημιουργούνται κάποιοι συναγερμοί (alarm).

Είναι δυνατόν να αποθηκευτούν οι μετρήσεις επίδοσης για μελλοντική επεξεργασία. Οι διαχειριστές του δικτύου θα πρέπει να αναλύουν τις μετρήσεις και να μπορούν να εντοπίσουν σημεία συμφόρησης η προβληματικής λειτουργίας του δικτύου. Με βάση τα συμπεράσματα από την ανάλυση των μετρήσεων είναι πιθανό να χρειαστεί να πραγματοποιηθεί η ανασχεδιάσει μερικών σημείων του δικτύου.
Όταν πραγματοποιούνται αλλαγές στο δίκτυο με βάση τις μετρήσεις που θα ληφθούν θα πρέπει να ελέγχεται στο κατά πόσο πέτυχαν το σκοπό για τον οποίο έγιναν.
Συνήθως η μετρήσεις μπορούν να καταγράφουν σε πίνακες η και σε γραφήματα.

1.1.3 Διαχείριση Σφαλμάτων

Το έργο της διαχείρισης σφαλμάτων είναι η αναγνώριση ύπαρξης προβλήματος / δυσλειτουργίας, ο εντοπισμός του σημείου, που υπάρχει το πρόβλημα, η επίλυση του προβλήματος ή η τεκμηρίωσή του και η προώθηση της περιγραφής του προβλήματος σε άλλη ομάδα. Συνήθως γίνεται και καταγραφή των προβλημάτων (τύπος λάθους, τοποθεσία, βαθμός κρισιμότητας κ.λ.π.) και τι λύση δόθηκε, για μελλοντική χρήση, όπως για παράδειγμα δημιουργία στατιστικών στοιχείων για κάποιες συσκευές. Μερικά προβλήματα είναι εύκολο να εντοπιστούν, όπως για παράδειγμα η μη λειτουργία συσκευής, η διακοπή σύνδεσης. Ο στόχος, όμως, της διαχείρισης δεν πρέπει να σταματά εκεί, αλλά να μπορεί να προβλέπει τη δημιουργία πιθανόν προβλημάτων πριν αυτά επηρεάσουν τους χρήστες του δικτύου. Το κομμάτι πρόβλεψης πιθανών προβλημάτων σχετίζεται άμεσα με τη διαχείριση επίδοσης του δικτύου.
Τα προβλήματα έρχονται με τη μορφή συναγερμού (alarm) και συνήθως γίνεται καταγραφή σε αρχεία (tags) ή και με μορφή αλλαγής της χρωματικής ένδειξης σε κάποιες γραφικές απεικονίσεις του δικτύου. Η λύση των προβλημάτων διαφέρει κάθε φορά και όπως είναι φυσικό εξαρτάται από το πρόβλημα. Μερικές φορές χρειάζεται η αποσύνδεση προβληματικών συσκευών από το δίκτυο, ή αντικατάσταση ελαττωματικού υλικού ή ρύθμιση παραμέτρων στο λογισμικό των συσκευών.

1.1.4 Διαχείριση κόστους (Accounting Management)

Το έργο της διαχείρισης κόστους ενός δικτύου περιλαμβάνει την παρακολούθηση της χρήσης των πόρων του δικτύου, την ανάλυση των διαθέσιμων επιπέδων των πόρων του δικτύου για συγκεκριμένες ομάδες χρηστών, την αντιστοίχηση του κόστους της χρήσης, την καταγραφή της χρήσης των δικτυακών πόρων από τις διάφορες ομάδες χρηστών και την εξασφάλιση ότι οι χρήστες δεν κάνουν χρήση υπηρεσιών, που δεν είναι συμφωνημένες.

1.1.5 Διαχείριση ασφάλειας (Security Management)

Η διαχείριση ασφάλειας περικλείει τον έλεγχο πρόσβασης σε συσκευές, δεδομένα και προγράμματα, απέναντι σε κάθε μη εξουσιοδοτημένη χρήση ηθελημένη ή μη, την επίβλεψη για προσπάθειες παραβίασης των κανόνων ασφάλειας και λήψη των απαραίτητων μέτρων προκειμένου να εξασφαλισθεί η ασφάλεια των πόρων του δικτύου. Η εξασφάλιση ασφάλειας σε πόρους του συστήματος αποτελεί πολύπλοκο και δύσκολο θέμα και αναλυτικότερη αναφορά σε μεθόδους επίτευξή της θα γίνει σε επόμενες παραγράφους.

Τα μέτρα ασφάλειας για κατανεμημένο πληροφορικό σύστημα δεν πρέπει σε καμία περίπτωση να είναι αποσπασματικά σε ένα τομέα, αλλά να περιλαμβάνουν όλους τους τομείς που συγκροτούν το πληροφορικό σύστημα. Θα μπορούσαμε να πούμε, ότι ο οργανισμός, που έχει εγκαταστήσει και χρησιμοποιεί πληροφορικό σύστημα, θα πρέπει να δεσμευτεί για την οργάνωση και τήρηση κανόνων ασφάλειας. Τα μέτρα ασφάλειας πρέπει να αφορούν:

- Τη φυσική προστασία των πόρων του συστήματος από πρόσβαση μη εξουσιοδοτημένων ατόμων.
- Την ασφάλεια των συστημάτων που συνδέονται σε δίκτυο. Το κομμάτι αυτό ανήκει επίσης στη διαχείριση ασφάλειας των συστημάτων (για παράδειγμα μηχανισμοί ασφάλειας σε επίπεδο λειτουργικού συστήματος)
- Την ασφάλεια του δικτύου και την προστασία των δεδομένων, που μεταφέρονται με αυτό.

1.2 Τα μέρη που απαρτίζουν ένα σύστημα διαχειρίσεις

• Network Management Console:

Ο σταθμός εργασίας που 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(router, bridge, hub, etc).

• Τα διαχειριζόμενα στοιχεία δικτύου (Network Elements - NE):

Όπως δικτυακές συσκευές (routers, bridge, modems, server applications)
Αρκετές από αυτές τις συσκευές έχουν τη δυνατότατα απομακρυσμένης Διαχείρισης (remote management) έτσι μπορούμε για παράδειγμα να κλείσουμε μια πόρτα (port) σε ένα router.

• Network Management Agent:

Το software που εγκαθίσταται στην δικτυακή συσκευή για χρήση του πρωτοκόλλου διαχείρισης.
Είναι δηλαδή το λογισμικό εκείνο που είναι υπεύθυνο για τι σωστή επικοινωνία και διαχείριση από τον διαχειριστή (μεσώ του πρωτοκόλλου διαχείρισης δικτύου (NMP)

• Network Management Protocol (NMP):

Το πρωτόκολλο με το οποίο θα επικοινωνεί με τις δικτυακές συσκευές.
Τα πρωτόκολλα διαχείρισης δικτύου (NMP, Network Management Protocols) είναι τα πρωτόκολλα που χρησιμοποιούνται για την επικοινωνία μεταξύ διαχειριστή και

αντιπροσώπων (ή πληρεξούσιων αντιπροσώπων) με σκοπό την ανταλλαγή πληροφοριών που έχουν να κάνουν με την διαχείριση των συσκευών του δικτύου. Τα ποιο γνωστά πρωτόκολλα αυτής της κατηγορίας είναι το SNMP για δίκτυα TCP/IP και το CMIP για δίκτυα που βασίζονται στο πρότυπο OSI. Τα πρωτόκολλα διαχείρισης δικτύου καθορίζουν:
Τον ακριβή τρόπο επικοινωνίας διαχειριστή – αντιπροσώπου.
Τη μορφή και την σημασία των μηνυμάτων που ανταλλάσσονται.

• Management Information Base - MIB)

Είναι μια βάση δεδομένων που μοιράζονται μεταξύ τους οι διαχειριστές και αντιπρόσωποι και η οποία περιέχει πληροφορίες σχετικά με τα διαχειριζόμενα στοιχεία δικτύου 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.

1.3 Αρχιτεκτονικές Διαχείρισης Δικτύων

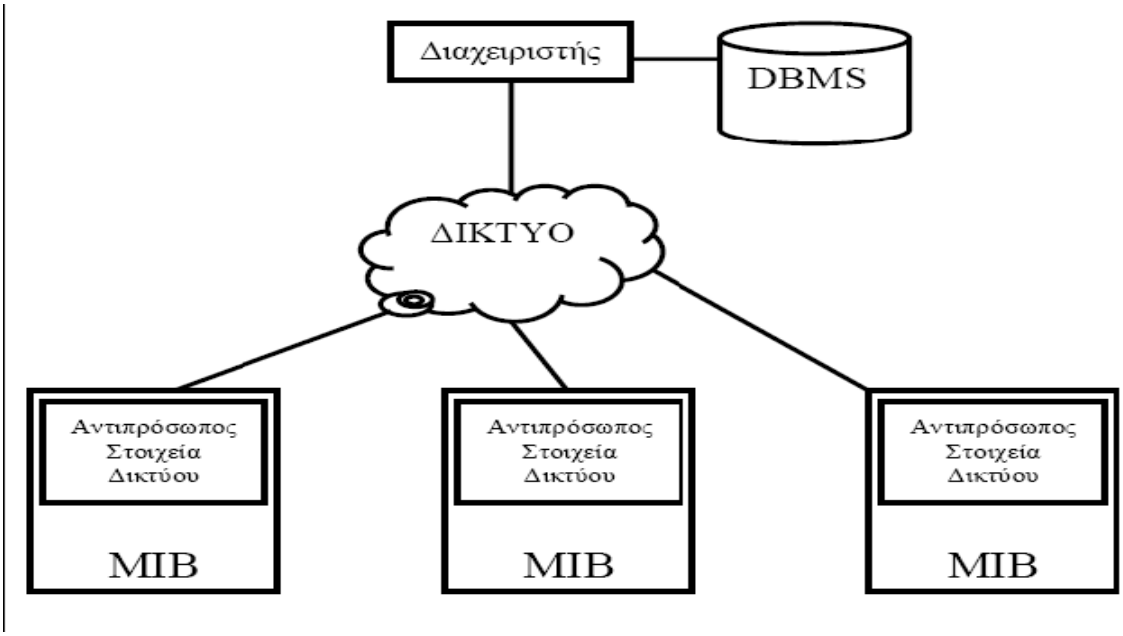
Για να μπορεί μια πλατφόρμα διαχείρισης δικτύου να εκτελεί τις λειτουργίες που περιγράφηκαν προηγουμένως, θα πρέπει να χρησιμοποιεί κάποια αρχιτεκτονική διαχείρισης. Οι αρχιτεκτονικές διαχείρισης του δικτύου που υπάρχουν είναι η **Κεντρική, η Ιεραρχική και η Κατανεμημένη.** Οι διαφορές αυτών των αρχιτεκτονικών 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.
Επίσης ο συνδυασμός της κεντρικής και της κατανεμημένης αρχιτεκτονικής μας δίνει το δικτυωμένα σύστημα διαχειρίσεις δικτύου.
Γενική περιγραφή των τεσσάρων αρχιτεκτονιών και των πλεονεκτημάτων και μειονεκτημάτων θα περιγράψουμε παρακάτω.

1.3.1 Κεντρική Αρχιτεκτονική Διαχείρισης

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 μεσώ 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 μεσώ κατάλληλου περιβάλλοντος επικοινωνίας με το χρήστη.

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.



ΣΧΗΜΑ 1: Κεντρική Αρχιτεκτονική Διαχείρισης Δικτύου

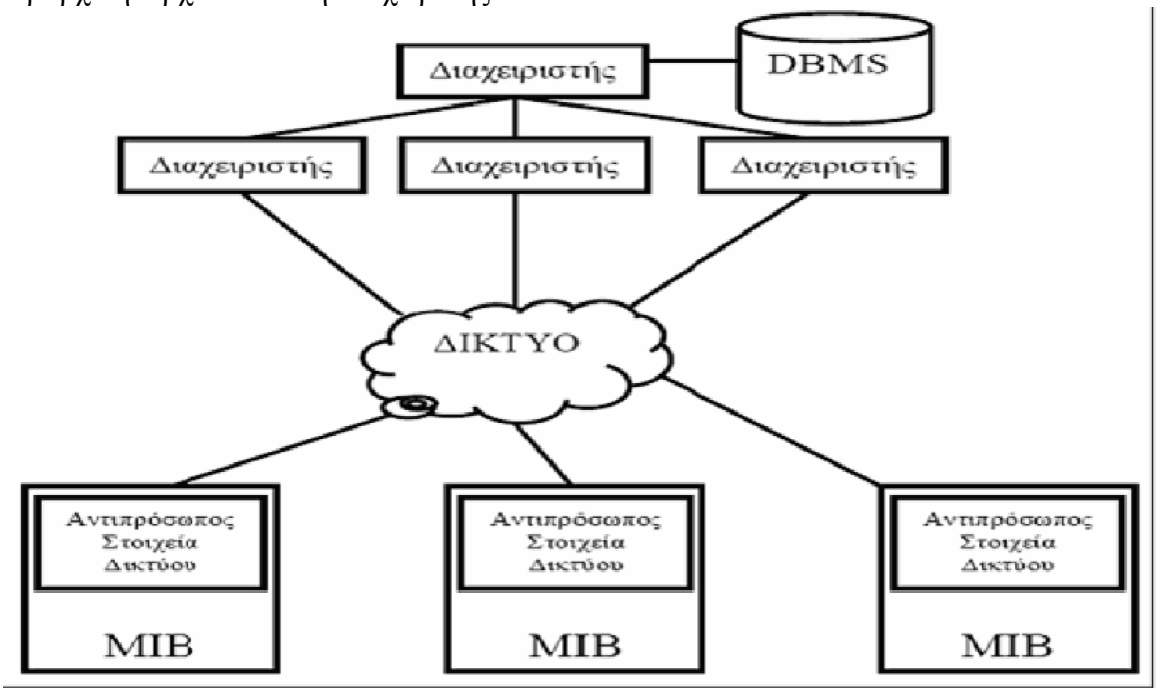
1.3.2 Ιεραρχική Αρχιτεκτονική Διαχείρισης (Hierarchical)

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.

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 u948 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 :

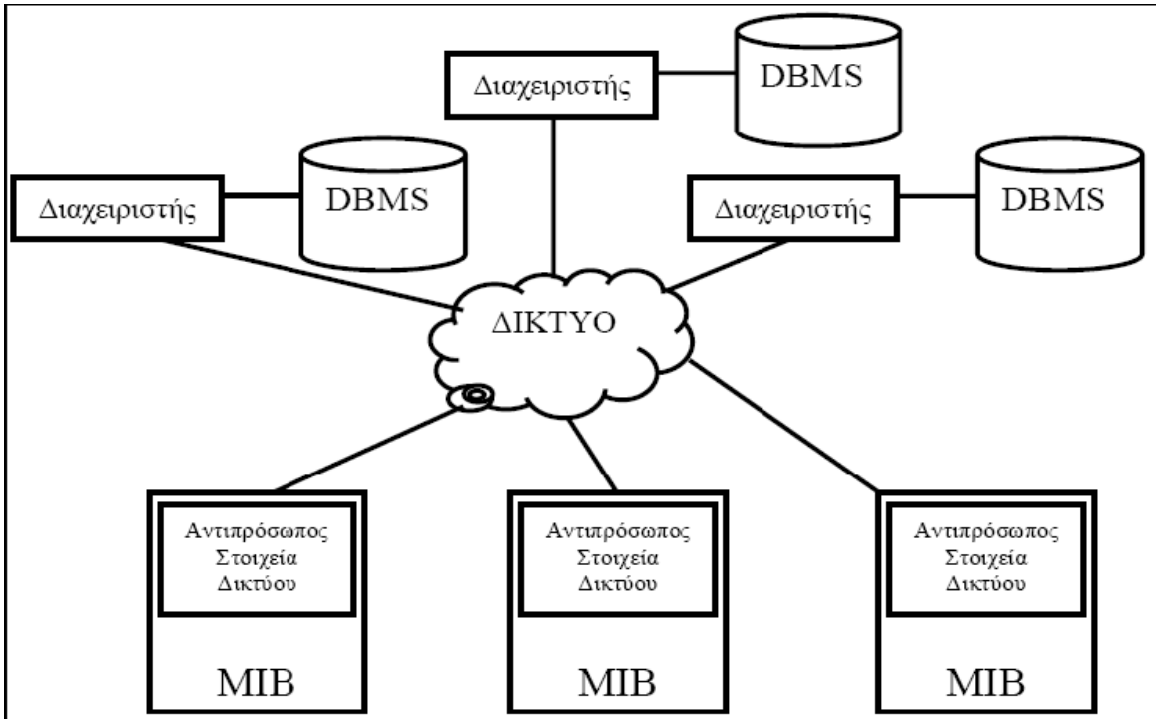
• Προσφέρει καλύτερο έλεγχο και επίδοση στο διαχειριστή του δικτύου
• Προσφέρεται για ετερογενή δίκτυα
• Βρίσκει εφαρμογή και σε δίκτυα που υπάρχει ανάγκη διαίρεσης του διαχειριζόμενου περιβάλλοντος
• Παρέχει: Ολοκληρωμένο διαχειριστικό περιβάλλον, Ενοποιημένη αναπαράσταση ετερογενούς δικτύου, Κοινό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



ΣΧΗΜΑ 2 : Ιεραρχική Αρχιτεκτονική Διαχείρισης Δικτύου

1.3.3 Κατανεμημένη Αρχιτεκτονική Διαχείρισης (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).
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.



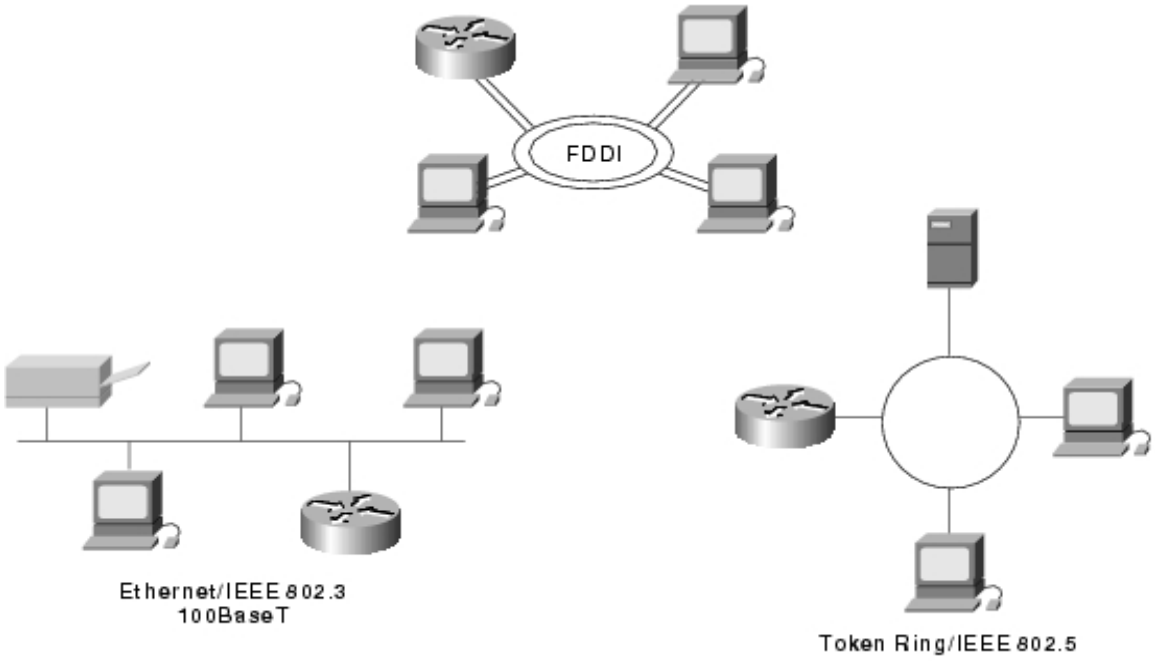
ΣΧΗΜΑ 3 :Κατανεμημένη Αρχιτεκτονική Διαχείρισης Δικτύου

1.4 Δικτυωμένο σύστημα διαχειρίσεις

Η αρχιτεκτονική αυτή συνδυάζει στοιχεία από τις αρχιτεκτονικές του κατανεμημένου και ιεραρχικού. Εδώ έχουμε περισσότερους από ένα MOM (Integrated Managers), ο καθένας από τους οποίους διαχειρίζεται μια ομάδα managers, κάθε ένας από τους οποίους διαχειρίζεται με την σειρά του μια ομάδα κόμβων (έννοια manager domain). Η αρχιτεκτονική αυτή ενθαρρύνεται από το γεγονός ότι όλο και περισσότερα διαχειριστικά συστήματα αναπτύσσουν τυποποιημένα interface, διευκολύνοντας έτσι την επικοινωνία με άλλα συστήματα. Το OSI Network Management Forum υποστηρίζει την προσπάθεια να επιτευχθεί ένα ευέλικτο και ισχυρό σύστημα που να ακολουθεί αυτή την αρχιτεκτονική. Η αρχιτεκτονική του δικτυωμένου συστήματος συνδυάζει τα πλεονεκτήματα των κατανεμημένων και ιεραρχικών συστημάτων που παρουσιάστηκαν παραπάνω. Το βασικότερο μειονέκτημα είναι ότι αυξάνει τον αριθμό των διαχειριστικών συστημάτων που χρησιμοποιεί, γεγονός που αυξάνει το κόστος. Βέβαια, ο ιεραρχικός χαρακτήρας αυτής της αρχιτεκτονικής μπορεί να οδηγήσει στην μείωση του αριθμού των χειριστών στο κέντρο διαχείρισης, αλλά δεν μειώνει τον αριθμό των διαχειριστικών συστημάτων που πρέπει να αγοραστούν και να συντηρηθούν. Όπως προαναφέρθηκε, μια τεχνική που οδηγεί σε μείωση του αριθμού των συστημάτων, είναι η μέθοδος της πλατφόρμας διαχείρισης. Τέλος, αξίζει να σημειωθεί ότι οι τρεις προηγούμενες αρχιτεκτονικές προσφέρουν λύσεις στα προβλήματα της ολοκληρωμένης διαχείρισης σε ετερογενή δίκτυα Ειδικότερα η ιεραρχική και κατανεμημένη (peer-to-peer) αντιμετώπιση έχουν προταθεί για χρήση στην διαχείριση multi domain δικτύων.

Τέτοια δίκτυα είναι σαφώς χωρισμένα σε ξεχωριστά τμήματα (domains) που διαχειρίζονται από τοπικούς διαχειριστές (εξαρτώμενοι από τους κατασκευαστές των τμημάτων). Τα προβλήματα που αντιμετωπίζονται είναι η έλλειψη ολοκληρωμένης πληροφορίας και η περιορισμένη δυνατότητα ελέγχου των τοπικών διαχειριστών. χουν προταθεί αλγόριθμοι που αντιμετωπίζουν αυτά τα προβλήματα και εφαρμόζονται στην κατανεμημένη αρχιτεκτονική, όπου ο κάθε διαχειριστής "βλέπει" τα άλλα τμήματα ως μοναδικούς κόμβους μεσώ των τοπικών διαχειριστών.

1.5 Τοπολογίες δικτύων



ΣΧΗΜΑ 4: Αρχιτεκτονικές δικτύων

Παραπάνω φαίνονται οι 3 βασικές μέθοδοι δικτυώσεις
1)FDDI
2) ETHERNET/IEEE
3)TOKEN RING

Οι τρεις παραπάνω αρχιτεκτονικές δικτυώσεις είναι οι πιο ευρέως χρησιμοποιούμενες. Είναι σημαντικό ότι και στις τρεις μπορούμε να κάνουμε διαχείριση δικτύου σχεδόν Παρόμοια. Με λίγα λόγια η διαχείριση δικτύου δεν μας περιορίζει ανάλογα με τι αρχιτεκτονική δικτύου έχουμε.

ΚΕΦΑΛΑΙΟ 2
Πρωτόκολλα Διαχείρισης Δικτύων.

Τα πρωτόκολλα διαχείρισης δικτύου καθορίζουν τον τρόπο με τον οποίο οι διαχειριστές (managers) επικοινωνούν με τους αντιπροσώπους (agents) για να γίνει η διαχείριση των διαχειριζόμενων στοιχείων δικτύου (Network Elements). Συγκεκριμένα, τα πρωτόκολλα αυτά καθορίζουν:

- Τον ακριβή τρόπο επικοινωνίας διαχειριστή – αντιπροσώπου.
- Τη μορφή και την σημασία των μηνυμάτων που ανταλλάσσονται.

Στο πρωτόκολλο TCP/IP χρησιμοποιούμε ένα συνδυασμό των παρακάτω για μια απλή και αποτελεσματική διαχείριση:

• Το πρωτόκολλο απλής διαχείρισης δικτύου SNMP (Simple Network Management Protocol).

• Την δομή πληροφοριών διαχείρισης (SMI, Structure of Management Information).

• Την βάση πληροφοριών διαχείρισης (MIB, Management Information Base).

Γενικά ωστόσο, σε δίκτυα που χρησιμοποιούν την αρχιτεκτονική OSI (π.χ. μεγάλα ετερογενή δίκτυα) χρησιμοποιούμε τα παρακάτω:

Το πρωτόκολλο κοινής διαχείρισης πληροφοριών CMIP (Common Management Information Protocol).

• Την υπηρεσία κοινής διαχείρισης πληροφοριακών στοιχείων (CMISE, Common Management Information Service Element).

Τα πρωτόκολλα SNMP και CMIP αποτελούν αυτή τη στιγμή τα σημαντικότερα πρωτόκολλα διαχείρισης δικτύων.

2.1Το πρωτόκολλο SNMP

• Στο πρωτόκολλο SNMP (Simple Network Management Protocol) που χρησιμοποιείται στο TCP/IP κάθε αντιπρόσωπος διαθέτει μια σειρά από *μεταβλητές* των οποίων οι τιμές μπορεί να αλλάζουν. Ο αντιπρόσωπος πρέπει να είναι σε θέση να παρουσιάσει αυτές τις τιμές σε κάποιο διαχειριστή που θα τις ζητήσει.

Μεταβλητές: Στη συγκεκριμένη περίπτωση, είδη πληροφοριών των οποίων η τιμή μπορεί να αλλάζει ανάλογα με την κατάσταση του δικτύου. Για παράδειγμα, έστω ότι ένας αντιπρόσωπος παρακολουθεί τα λάθη του δικτύου που παρατηρούνται σε μια πόρτα ενός δρομολογητή. Η μεταβλητή είναι «Λάθη δικτύου στο δρομολογητή» και η τιμή της είναι αυτή που κάθε φορά μετράει ο αντιπρόσωπος.

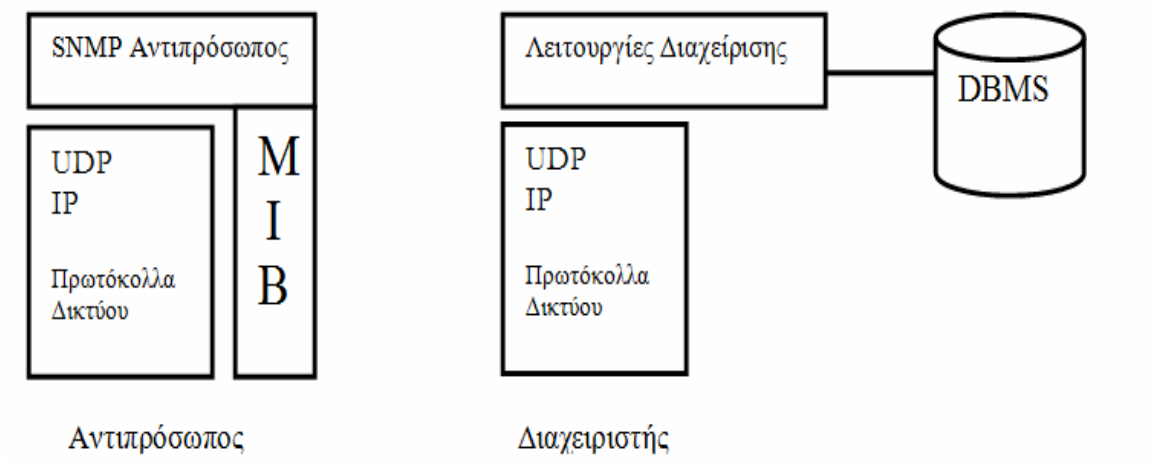
Οι μεταβλητές μπορεί να είναι απεικονίσεις διάφορων αντικειμένων (διευθύνσεις, μετρητές κ.α.). Καθεμία από αυτές τις απεικονίσεις μπορεί να μην δίνει πλήρη εικόνα της

κατάστασης του αντικειμένου που αναφέρεται, αφού ένα πολύπλοκο αντικείμενο μπορεί να έχει περισσότερες από μια απεικονίσεις και κάθε μία να αναφέρεται σε μια διαφορετική ιδιότητα ή στοιχείο του. (Για παράδειγμα, σε μια σύνδεση TCP υπάρχουν πολλά μετρήσιμα χαρακτηριστικά και καθένα από αυτά είναι μια απεικόνιση, αλλά κανένα από μόνο του δεν αρκεί για να κρίνουμε την κατάσταση της σύνδεσης συνολικά)

Σε κάθε περίπτωση, οι απεικονίσεις αυτές συγκεντρώνονται σύμφωνα με το SNMP και αποθηκεύονται σε ένα πίνακα. Το σύνολο τώρα όλων αυτών των μεταβλητών αποτελεί τελικά την βάση πληροφοριών διαχείρισης (MIB). Ένας σταθμός διαχείρισης στο SNMP έχει την δυνατότητα να ελέγχει (διαβάζει) αυτές τις τιμές και να βγάζει έτσι συμπεράσματα για την κατάσταση στην οποία βρίσκεται το διαχειριζόμενο στοιχείο του δικτύου που αναφέρεται. Όμως ο διαχειριστής έχει επίσης δυνατότητα να μεταβάλλει τις τιμές αυτές και με αυτό τον τρόπο να παρεμβαίνει στις ρυθμίσεις του δικτύου. Γενικά ο διαχειριστής:

- Παρακολουθεί την απόδοση του δικτύου.
- Ελέγχει τις παραμέτρους που αφορούν την κατάσταση και λειτουργία του δικτύου.
- Μπορεί να αναλύσει και να απομονώσει σφάλματα καθώς και να πάρει βήματα για την αποκατάσταση τους.

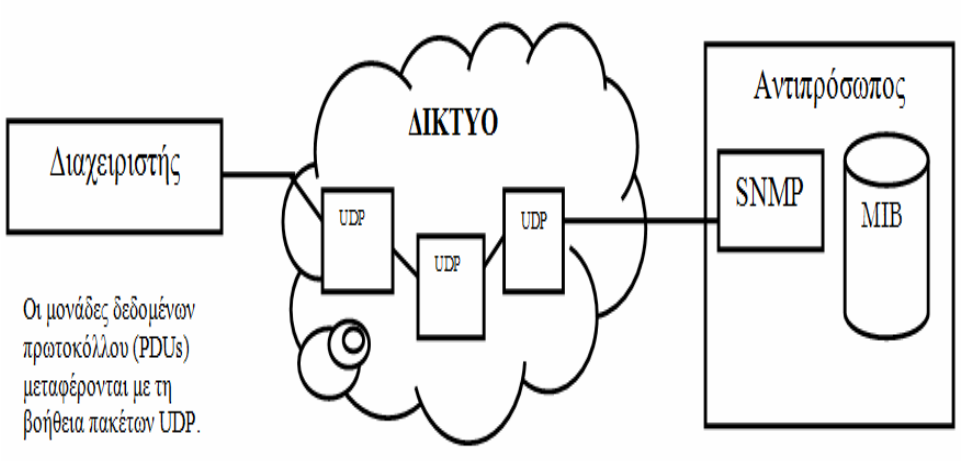
Ο κάθε αντιπρόσωπος κρατάει πληροφορίες που αναφέρονται μόνο σε ένα υποσύνολο της βάσης πληροφοριών διαχείρισης (MIB View, απεικόνιση της βάσης) και οι πληροφορίες αυτές είναι ανάλογες με τα πρωτόκολλα (IP, TCP, UDP) που χρησιμοποιούνται στο μηχάνημα που εκτελείται. Κάθε διαχειριστής διαθέτει διαφορετικό τρόπο πρόσβασης για κάθε απεικόνιση της MIB. Κάποιοι διαχειριστές έχουν δικαιώματα μόνο ανάγνωσης ενώ άλλοι έχουν δυνατότητα μεταβολής (εγγραφής) στη βάση. Προφανώς οι διαχειριστές που έχουν δυνατότητα εγγραφής μπορούν με τον τρόπο αυτό να μεταβάλλουν τις ρυθμίσεις του δικτύου. Με το σύστημα αυτό των δικαιωμάτων, υλοποιείται ένα μοντέλο ασφαλείας.



ΣΧΗΜΑ 5: Διαχειριστής - Αντιπρόσωπος στο πρωτόκολλο SNMP

Αν ένας αντιπρόσωπος κρατάει δεδομένα στο μηχάνημα του που δεν αφορούν το ίδιο το μηχάνημα που εκτελεί την διαχείριση αλλά κάποιο άλλο, τότε ο αντιπρόσωπος δρα για λογαριασμό άλλου και είναι *πληρεξούσιος – αντιπρόσωπος (proxy agent)*.

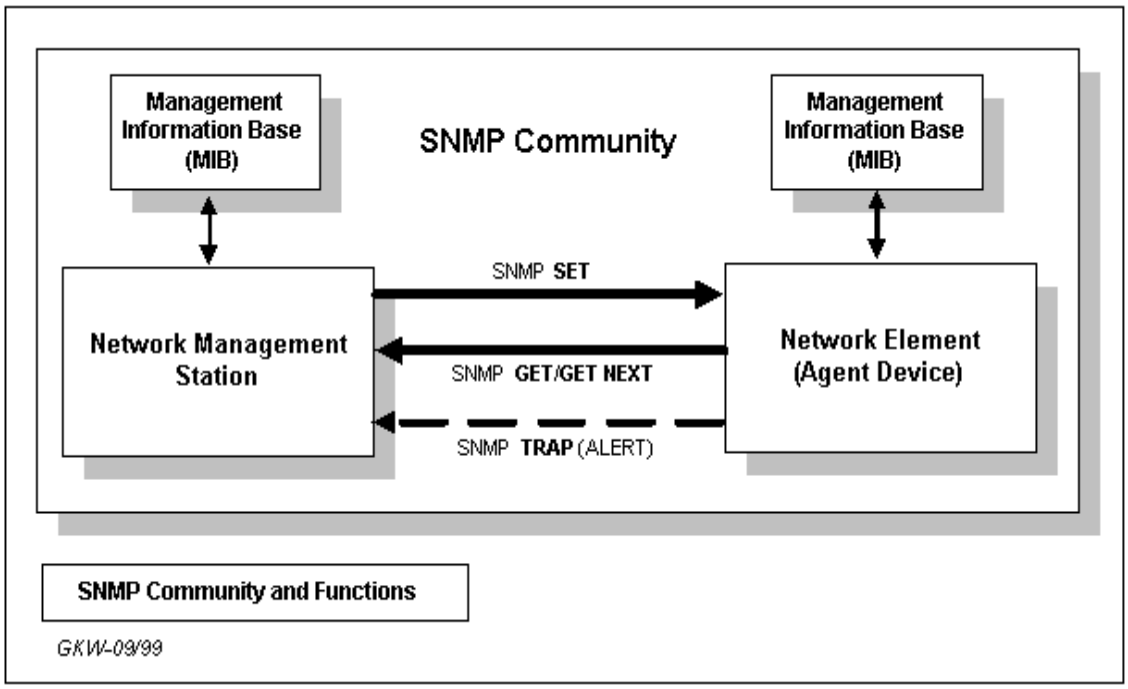
Το πρωτόκολλο SNMP δίνει ένα πολύ μικρό ποσοστό από πληροφορίες στις εφαρμογές διαχείρισης σχετικά με τον έλεγχο ή τις αλλαγές τιμών που έκαναν οι αντιπρόσωποι στις τιμές των απεικονίσεων MIB. Η επικοινωνία μεταξύ διαχειριστών και αντιπροσώπων γίνεται με την ανταλλαγή *μονάδων δεδομένων πρωτοκόλλου (PDU, Protocol Data Units)*. Κάθε μία από τις μονάδες αυτές κωδικοποιείται μέσα σε *ένα και μοναδικό πακέτο UDP* (User Datagram, αυτοδύναμο πακέτο) και ανταλλάσσεται με την χρήση του πρωτοκόλλου UDP. Το SNMP είναι δομημένο με τέτοιο τρόπο ώστε να εφαρμόζεται ακριβώς πάνω από το UDP.



ΣΧΗΜΑ6: Μονάδες δεδομένων πρωτοκόλλου στο SNMP

Το πρότυπο SNMP v2 (δεύτερη έκδοση) αποτελεί εξέλιξη του αρχικού SNMP και έχει σκοπό να εξαλείψει κάποια από τα σημαντικά μειονεκτήματα της πρώτης έκδοσης αλλά και να επεκτείνει το πρότυπο ώστε να μπορεί να χρησιμοποιηθεί (εκτός από το TCP/IP) και σε πρωτόκολλα που ακολουθούν το πρότυπο OSI. Τα πρόσθετα στοιχεία / βελτιώσεις του SNMP v2 είναι:

- Καλύτερη δομή πληροφοριών διαχείρισης.
- Νέες λειτουργίες πρωτοκόλλου.
- Νέες MIB.
- Μεγαλύτερη ασφάλεια.



ΣΧΗΜΑ 7: Εντολές που ανταλλάσσονται στο πρότυπο διαχείρισης SNMP

2.2Το πρωτόκολλο RMON

RMON1

Έκδοση: 1

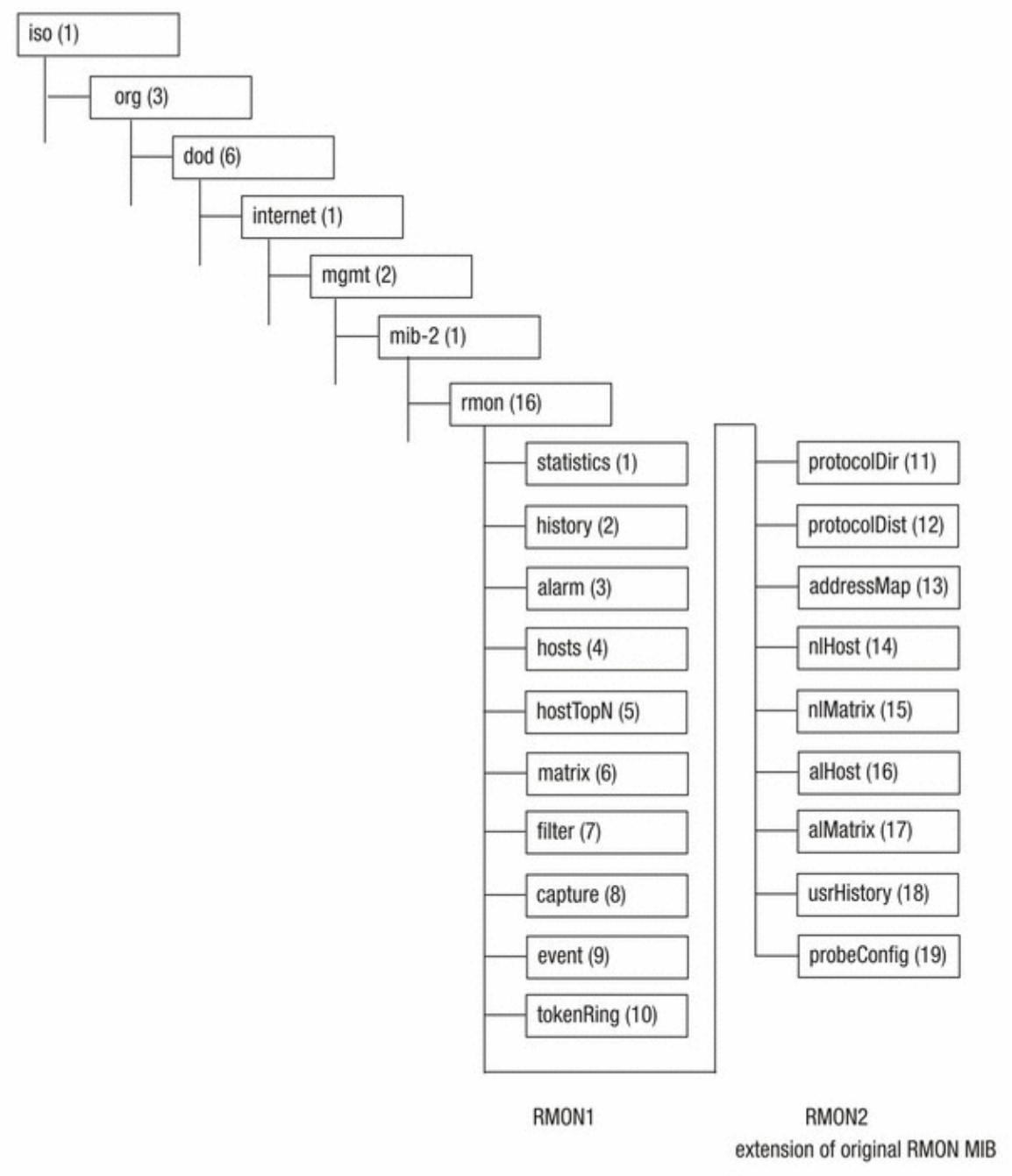
Με το RMON1 MIB, οι διαχειριστές δικτύων μπορούν να συλλέξουν τις πληροφορίες από τα μακρινά τμήματα δικτύων για τους σκοπούς της ανίχνευσης λαθών και του ελέγχου απόδοσης. Το RMON1 MIB παρέχει:

Τρέχουσες και ιστορικές στατιστικές κυκλοφορίας για ένα τμήμα δικτύων, για ένα συγκεκριμένο σύστημα σε ένα τμήμα, και μεταξύ των συστημάτων (πίνακας)

Έναν προσαρμόσιμο μηχανισμό συναγερμών και γεγονότων για τον ορισμό κατώτατων ορίων και την ειδοποίηση του διαχειριστή για τις αλλαγές στη συμπεριφορά δικτύων

Ένα ισχυρό, ευέλικτο εργαλείο ορισμού φίλτρων και σύλληψης πακέτων που μπορούν να χρησιμοποιηθούν για να δημιουργήσουν ένα πλήρες, διανεμημένο σύστημα ανάλυσης πρωτοκόλλων

Στο ακόλουθο σχήμα φαίνεται μια λίστα με τα γκρουπ του RMON και η ένταξη τους μέσα στα στάνταρ του International Standards Organization (ISO).



ΣΧΗΜΑ 8: Ομάδες πληροφοριών RMON 1 &RMON 2

Στη συνέχεια θα αναφερθούμε στις ομάδες παραμέτρων RMON για δίκτυα τύπου Ethernet. Το RMON μπορεί να υποστηρίζεται από δικτυακή συσκευή που συνδέεται σε Ethernet δίκτυο. Ο! ομάδες είναι:

1.Statistics: παρέχει πληροφορίες, που απαιτούνται για την κατανόηση της επίδοσης τμήματος δικτύου. Τα στατιστικά περιλαμβάνουν μετρήσεις σε αληθινό χρόνο πακέτων, οκτάδων, πακέτα πολλαπλών εκπομπών, πακέτα, που απορρίφθηκαν, λάθη κ.ο.κ.

2.History: παρέχει ιστορικά δεδομένα για διάφορες παραμέτρους τμήματος δικτύου, που βοηθούν στην καλύτερη ανάλυση της συμπεριφοράς του.
3.Host Table: παρέχει πληροφορίες για την κίνηση, που δημιουργούν οι διάφοροι σταθμοί, που συνδέονται στο τμήμα του δικτύου, που μετράμε. Παρέχει τη δυνατότητα εντοπισμού της συσκευής, που δημιουργεί την περισσότερη κίνηση μέσα στο δίκτυο.
4.HostTopN: παρέχει στατιστικά στοιχεία ταξινομημένα με βάση τους σταθμούς που δημιουργούν την περισσότερη κίνηση στο δίκτυο.
5.Traffic Matrix: παρέχει στοιχεία για την κίνηση και τα λάθη για όλους τους δυνατούς συνδυασμούς ζευγαριών επικοινωνίας μεταξύ των σταθμών εργασίας μέσα στο δίκτυο.
6.Alarm: αναφέρει αλλαγές στα χαρακτηριστικά λειτουργίας δικτύου. Συνήθως alarm δημιουργούνται από την ενεργοποίηση κατωφλίων για διάφορες παραμέτρους του MIB.
7.Event: καταγράφει συμβάντα στο δίκτυο. Και στην περίπτωση αυτή η καταγραφή γεγονότων προέρχεται, συνήθως, από την ενεργοποίηση κατωφλίων από το διαχειριστή του δικτύου.
8.Filters: παρέχει τη δυνατότητα ενεργοποίησης φίλτρων, που βασίζονται σε λογικούς κανόνες (π.χ. and, or, not). Όταν ικανοποιούνται οι κανόνες φίλτρου, μπορεί να ενεργοποιούνται μηχανισμοί όπως καταγραφής (log) συμβάντος, ή δημιουργίας alarm κ.λ.π.
9.Packet Capture: είναι η μόνη από τις ομάδες, που περιλαμβάνει και τα επτά επίπεδα του μοντέλου OSI. Με τη λειτουργία αυτή είναι δυνατή η αντιγραφή των πακέτων που κυκλοφορούν μέσα στο δίκτυο καθώς και η δυνατότητα ανάλυσή τους. Η ενεργοποίηση της αντιγραφής μπορεί να ελεγχθεί, επίσης, με βάση την ικανοποίηση κριτηρίων όπως ο τύπος του πρωτοκόλλου επικοινωνίας κ.ο.κ.

Στη συνέχεια θα αναφερθούμε στις ομάδες παραμέτρων RMON2 για δίκτυα τύπου Ethernet. Το RMON2 μπορεί να υποστηρίζεται από δικτυακή συσκευή, που συνδέεται σε Ethernet δίκτυο. Οι ομάδες παραμέτρων είναι:

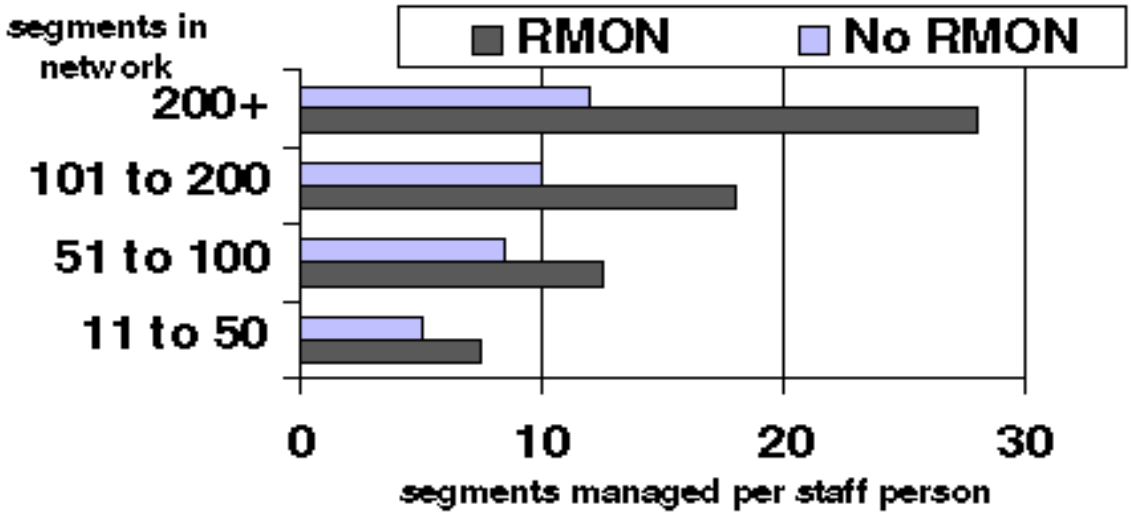
1.Protocol Directory Group: περιέχει σε κατάλογο όλα τα πρωτόκολλα, που μπορεί να καταλάβει η συσκευή, που υποστηρίζει το RMON2.
2.Protocol Distribution: κρατά στατιστικά στοιχεία για το ποσοστό της κίνησης, που δημιουργεί το κάθε πρωτόκολλο ανά τμήμα LAN ή ανά επίπεδο στο μοντέλο OSI.
3.Address Mapping: συσχετίζει τον αριθμό θύρας συσκευής με τη φυσική της διεύθυνση (MAC address) και τη διεύθυνση δικτύου (π.χ. IP address).
4.Network Layer Host: περιέχει στατιστικά στοιχεία για την κίνηση συγκεκριμένων σταθμών μέσα στο δίκτυο, βασισμένα στη διεύθυνση δικτύου που έχουν.
5.Network Layer Matrix: περιέχει στατιστικά στοιχεία για την κίνηση μεταξύ ζευγαριών επικοινωνίας από σταθμούς μέσα στο δίκτυο, βασισμένα στη διεύθυνση δικτύου, που έχουν.
6.Network Layer TopN Matrix: περιέχει στατιστικά στοιχεία του τρίτου επιπέδου του μοντέλου OSI, για τις πλέον ενεργές συνομιλίες μεταξύ των σταθμών μέσα στο δίκτυο.
7.Application Layer Host: περιέχει στατιστικά στοιχεία για την κίνηση ανά σταθμό στο δίκτυο σε επίπεδο εφαρμογής.
8.Application Layer Matrix: περιέχει στατιστικά στοιχεία για την κίνηση, που δημιουργούν στο δίκτυο, οι σταθμοί εργασίας στις μεταξύ τους συνομιλίες σε επίπεδο εφαρμογής.
9.User History: κρατά στατιστικά ιστορικά στοιχεία για μεταβλητές (32 bit ακέραιες μεταβλητές) που έχει ορίσει ο ίδιος ο χρήστης.
10. Probe Configuration:περιέχει τις καθιερωμένες ρυθμίσεις της συσκευής δι¬κτύου,

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 στο χρήστη. Οι "εξυπηρετητές" είναι οι συσκευές ελέγχου που διανέμονται σε όλα τα μακρινά δίκτυα και συλλέγουν τις πληροφορίες για το RMON και αναλύουν τα πακέτα δικτύων. Η συσκευή ελέγχου καλείται συνήθως "probe" και τρέχει ένα πρόγραμμα λογισμικού, αποκαλούμενο γενικά RMON "πράκτορας". Οι πράκτορες RMON μπορούν να βρεθούν σε αφοσιωμένες συσκευές ή και να ενσωματωθούν στις συσκευές υποδομής δικτύων όπως τα hubs και τα switches. Η εφαρμογή και ο πράκτορας επικοινωνούν μέσω του δικτύου χρησιμοποιώντας το Simple Network Management Protocol (SNMP).

Τα οφέλη RMON1 είναι σαφή. Χωρίς να εγκαταλείψει το γραφείο, ένας διαχειριστής δικτύων μπορεί να δει την κυκλοφορία σε ένα τμήμα του τοπικού LAN, είτε εκείνο το τμήμα βρίσκεται στο διπλανό δωμάτιο ή οπουδήποτε σε όλο τον κόσμο. Οπλισμένος με αυτήν την γνώση κυκλοφορίας, ο διαχειριστής δικτύων μπορεί να προσδιορίσει τις τάσεις, τα bottlenecks, και τα hotspots του δικτύου. Όταν ένα πρόβλημα προκύπτει, το RMON1 περιλαμβάνει επίσης έναν ισχυρό αναλυτή πρωτοκόλλου έτσι ώστε ο διαχειριστής να έχει τα εργαλεία ανίχνευσης λαθών άμεσα προσιτά. Δεδομένου ότι η συσκευή RMON1 είναι μόνιμα συνδεμένη με το τμήμα δικτύων, συλλέγει ήδη τα στοιχεία για το μακρινό τοπικό LAN και είναι έτοιμη να τα διαβιβάσει σε έναν κεντρικό διαχειριστικό σταθμό όποτε απαιτείται. Όλος αυτός ο έλεγχος και η ανίχνευση λαθών στο δίκτυο μπορεί να γίνει χωρίς τα έξοδα του χρόνου και του ταξιδιού που απαιτούνται για να σταλούν οι ακριβοί εμπειρογνώμονες δικτύων με τις συσκευές ανάλυσης πρωτοκόλλου σε μια μακρινή περιοχή.

Τα κέρδη που προσφέρει το RMON στην ικανότητα διαχείρισης του δικτύου φαίνονται στο σχήμα:



ΣΧΗΜΑ 9: Σύγκριση με RMON και χωρίς RMON

2.3 Το πρωτόκολλο CMIP

Το CMIP είναι ένα πρωτόκολλο διαχείρισης δικτύου βασισμένο στο OSI μοντέλο, το οποίο υποστηρίζει ανταλλαγή πληροφοριών μεταξύ των εφαρμογών διαχείρισης δικτύου και των αντίστοιχων πρακτόρων. Σχεδιάστηκε για να αντικαταστήσει το SNMP.

Το CMIP καθορίζει πως οι πληροφορίες διαχείρισης ανταλλάσσονται μεταξύ εφαρμογών διαχείρισης και αντίστοιχων πρακτόρων. Χρησιμοποιεί έναν ISO μηχανισμό, προσανατολισμένο προς σύνδεση και έχει ένα ενσωματωμένο σύστημα ασφαλείας το οποίο υποστηρίζει έλεγχο πρόσβασης, εξουσιοδότηση και ημερολόγιο ασφαλείας. Οι πληροφορίες διαχείρισης ανταλλάσσονται μεταξύ των εφαρμογών διαχείρισης και των αντίστοιχων πρακτόρων μέσο των διαχειριζόμενων αντικειμένων. Τα διαχειριζόμενα αντικείμενα είναι χαρακτηριστικά μιας διαχειριζόμενης συσκευής και μπορούν να παρακολουθούνται, τροποποιούνται και να ελέγχονται και τα οποία μπορούν να χρησιμοποιηθούν για την εκτέλεση διάφορων εργασιών.

Το CMIP δεν καθορίζει τη λειτουργικότητα της εφαρμογής διαχείρισης δικτύου, απλά ορίζει το μηχανισμό ανταλλαγής πληροφοριών και όχι το πώς θα χρησιμοποιηθούν ή θα μεταφραστούν.

Τα πλεονεκτήματα του CMIP σε σχέση με το SNMP είναι:

- Οι μεταβλητές του CMIP δεν συσχετίζουν απλά τις πληροφορίες αλλά χρησιμοποιούνται για την εκτέλεση λειτουργιών. Αυτό είναι αδύνατο με το SNMP.
- Το CMIP είναι πιο ασφαλές σύστημα, εφόσον έχει ενσωματωμένη ασφάλεια.
- Το CMIP προσφέρει μεγάλες δυνατότητες που επιτρέπουν στις εφαρμογές διαχείρισης να εκτελούν ταυτόχρονα πάνω από μία εργασίες.
- Το CMIP αναφέρει με καλύτερο τρόπο τα προβλήματα που παρουσιάζονται στο δίκτυο.

2.4 Σύγκριση πρωτοκόλλων

SNMP

Πλεονεκτήματα

• Είναι ευρέως δοκιμασμένο και αποδεκτό
• Είναι απλό στη δομή του και στις λειτουργίες του
• Έχει χαμηλό κόστος υλοποίησης,
• Βγήκε πρώτο χρονικά στην αγορά

Μειονεκτήματα

Είναι connectionless, άρα όχι τόσο αξιόπιστο όσο το connection oriented CMIP.
• Οι πληροφορίες SNMP δεν φιλτράρονται. Ο Manager παίρνει όλες τις πληροφορίες για να επιλέξει αυτήν που τον ενδιαφέρει.

• Το polling που χρησιμοποιεί καταλαμβάνει πολύτιμο bandwidth του δικτύου, ιδίως όταν αυτό γίνεται μέσο δικτύου ευρείας ζώνης WAN όπου οι ταχύτητες είναι χαμηλές.

CMIP

Πλεονεκτήματα

• Είναι πολύ ισχυρότερο,
• Είναι πρότυπο του ISO, που σημαίνει ότι είναι σχεδιασμένο για ανοικτά συστήματα και όχι μόνο για περιπτώσεις όπως του internet.
• Είναι connection oriented και κατά συνέπεια αξιόπιστο
• Το CMIP εξετάζει (φιλτράρει) το κατά πόσον θα σταλεί μία πληροφορία από τον Agent στον Manager και δεν τις στέλνει όλες ανεξαιρέτως.

Μειονεκτήματα
• Βγήκε αργότερα στην αγορά
• Δεν έχει μεγάλη εγκατεστημένη βάση
• Απαιτεί για κάθε agent περί τα 400 Kbytes μνήμη ενω το SNMP απαιτεί μόλις 10.kbytes

ΚΕΦΑΛΑΙΟ 3

Η ΠΛΑΤΦΟΡΜΑ SOLARWINDS ENGINEER EDITION V8.2

Το SOLARWINDS ENGINEER EDITION είναι ένα ισχυρό πρόγραμμα Διαχείρισης δικτύων με πάρα πολλές επιλογές και εργαλεία διαχείρισης Τα οποία μπορούν να προσεγγιστούν εύκολα μεσώ γραφικών παραθύρων ελέγχου και παρατήρησης. Στο solarwinds θα δούμε αναλυτικά τα εξής:

NETWORK DISCOVERY	PERFORMANCE MONITORING
Ip address management	**Bandwidth gauges**
Ip network browser	**Cpu gauge**
Mac address discovery	
Port scanner	
Switch port mapper	

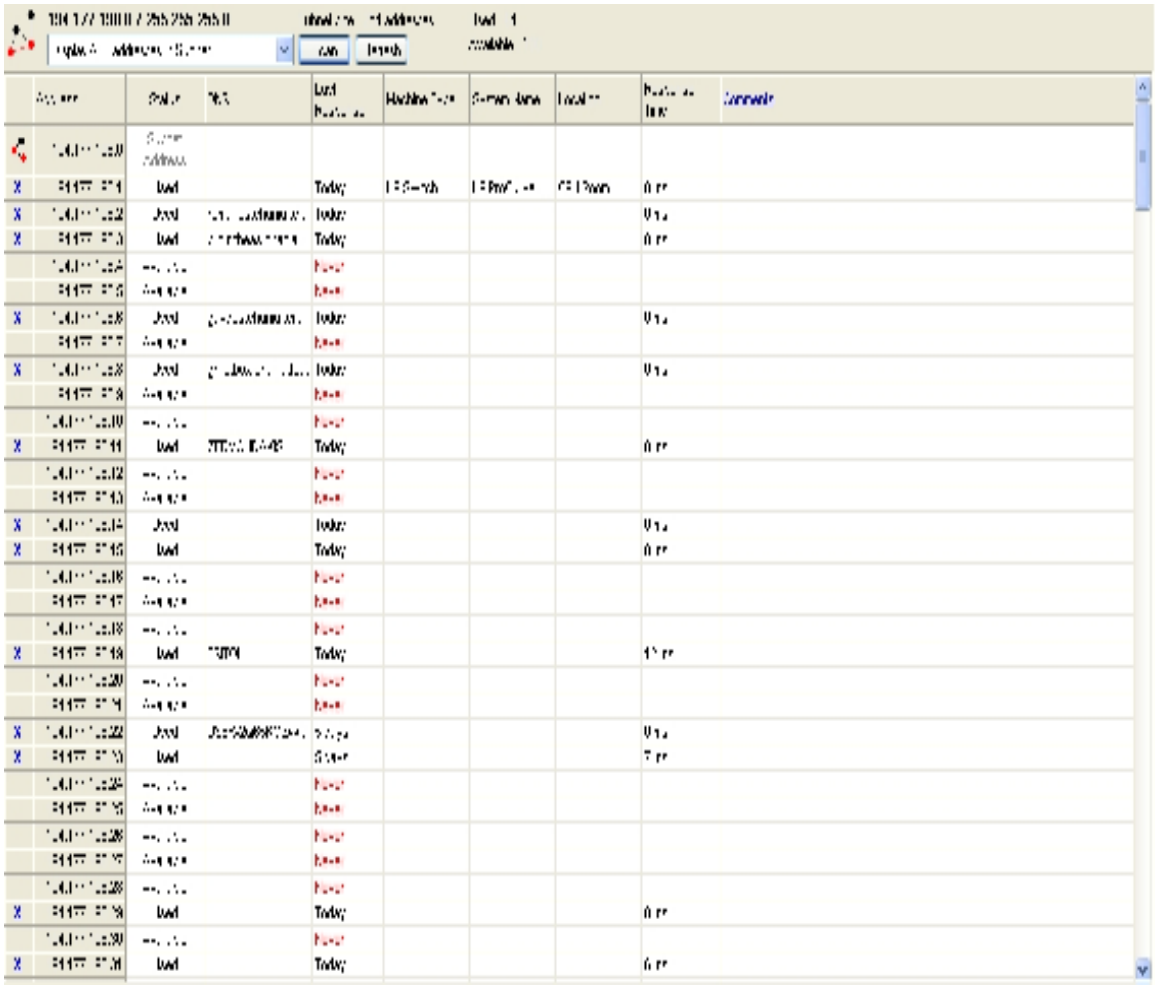
NETWORK DISCOVERY

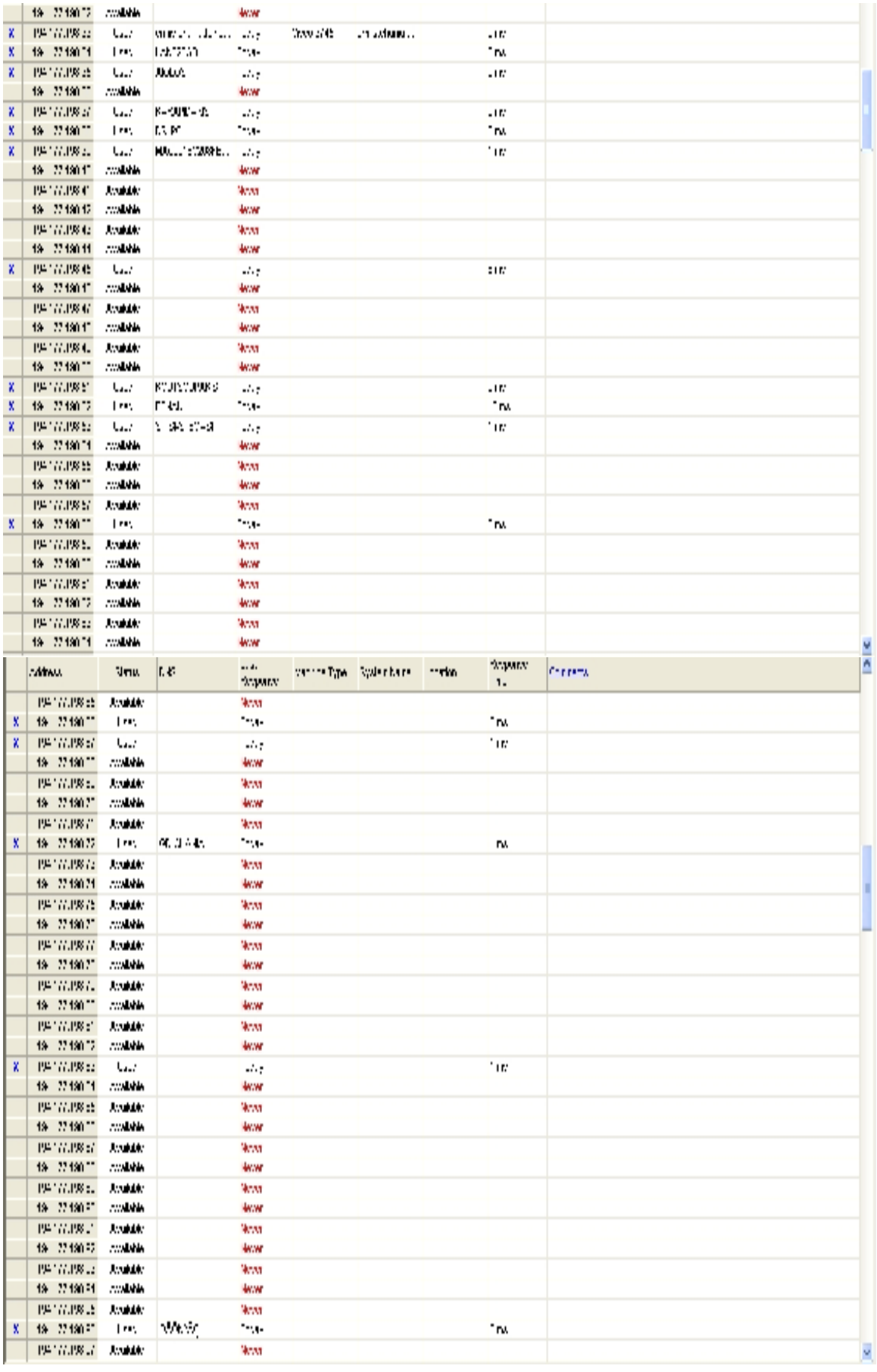
Σε αυτό το κεφαλαίο θα κάνουμε μια παρουσίαση των επιλογών του solarwinds που αναφέραμε πιο πάνω, οι συγκεκριμένες μετρήσεις έγιναν στο ΤΕΙ ΧΑΝΙΩΝ στις 15-3-2010.
Για να μπορέσουμε να έχουμε αμφίδρομη επικοινωνία από router-station και station router ενεργοποιήσαμε το πρωτόκολλο TFTP όπου μας παρέχει ασφαλή επικοινωνία προς το router μόνο με μια συγκεκριμένη διεύθυνση ip αυτή που ορίσαμε εμείς μέσα από το router ώστε να μπορούμε να έχουμε πλήρη πρόσβαση σε αυτό στην προκείμενη περίπτωση ενεργοποιήσαμε την διεύθυνση ip 194.177.198.11 να είναι full accessible.

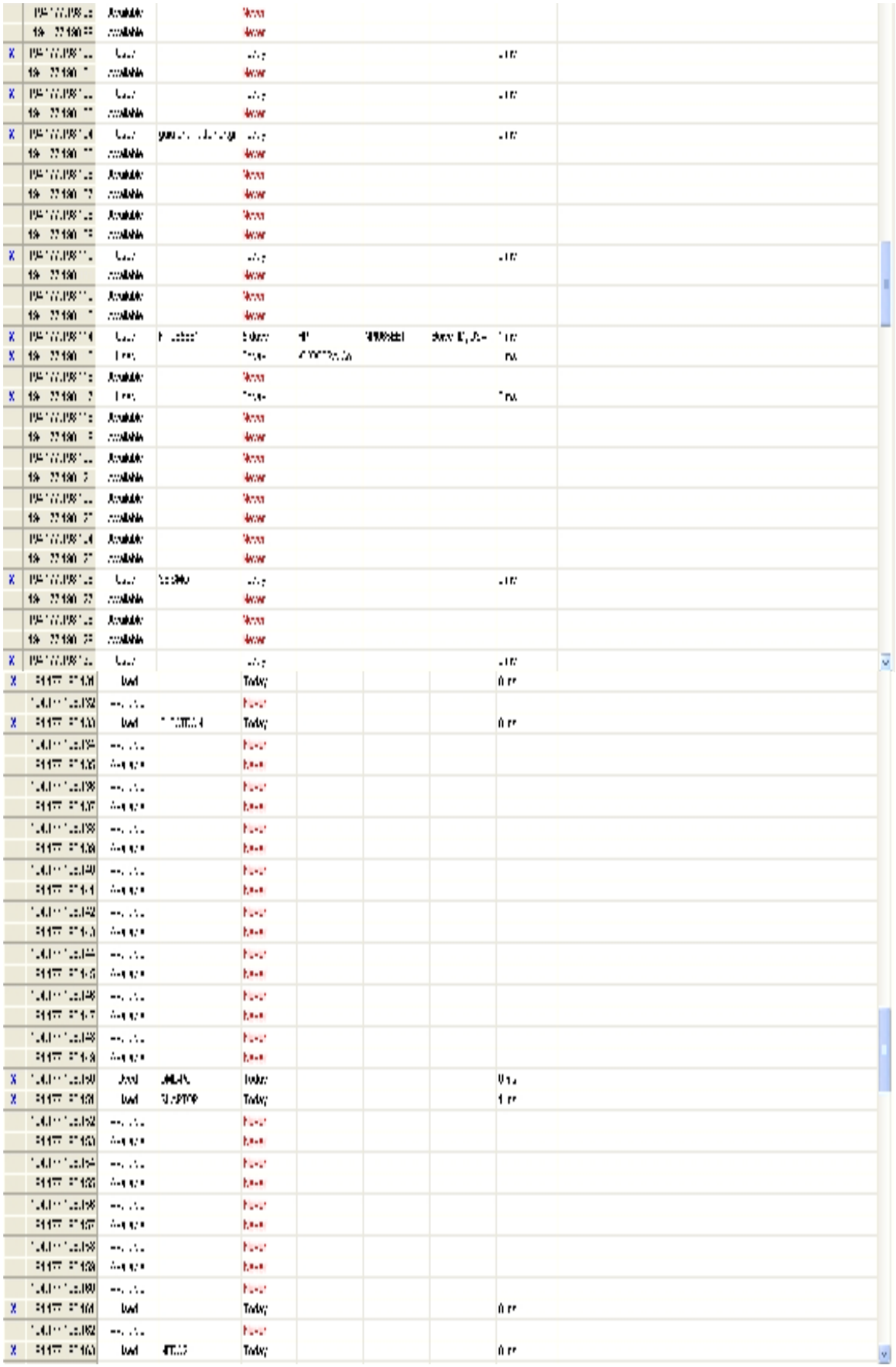
3.1IP Address Management

Η πρώτη μας επιλογή ήταν το **IP Address Management.** Δημιουργήσαμε το δίκτυο μας δίνοντας της κατάλληλες τιμές σε ip address & subnet mask.
Μόλις του δώσαμε τα απαραίτητα αυτά στοιχεία το πρόγραμμα άρχισε να σαρώνει το δίκτυο μας και να μας βγάζει ένα-ένα όλα τα τερματικά που είναι συνδεδεμένα στο δίκτυο. Στα παρακάτω screenshot φαίνονται οι τερματικοί σταθμοί που εντόπισε το solarwinds καθώς και κάποιες επιπρόσθετες πληροφορίες όπως την DNS address, την τελευταία φορά που ήταν ενεργή μια ip (Last Response), τον τύπο της κάθε συσκευής(machine type), την τοποθεσία της στο μέσα στο δίκτυο(μεταβλητή η οποία δίνετε από τον διαχειριστή του δικτύου για κάθε τερματικό) και το χρόνο που χρειάστηκε να απαντήσει το κάθε τερματικό επίσης μας δίνετε και η επιλογή να σημειώσουμε συγκεκριμένα πράγματα για κάθε τερματικό στα comments.

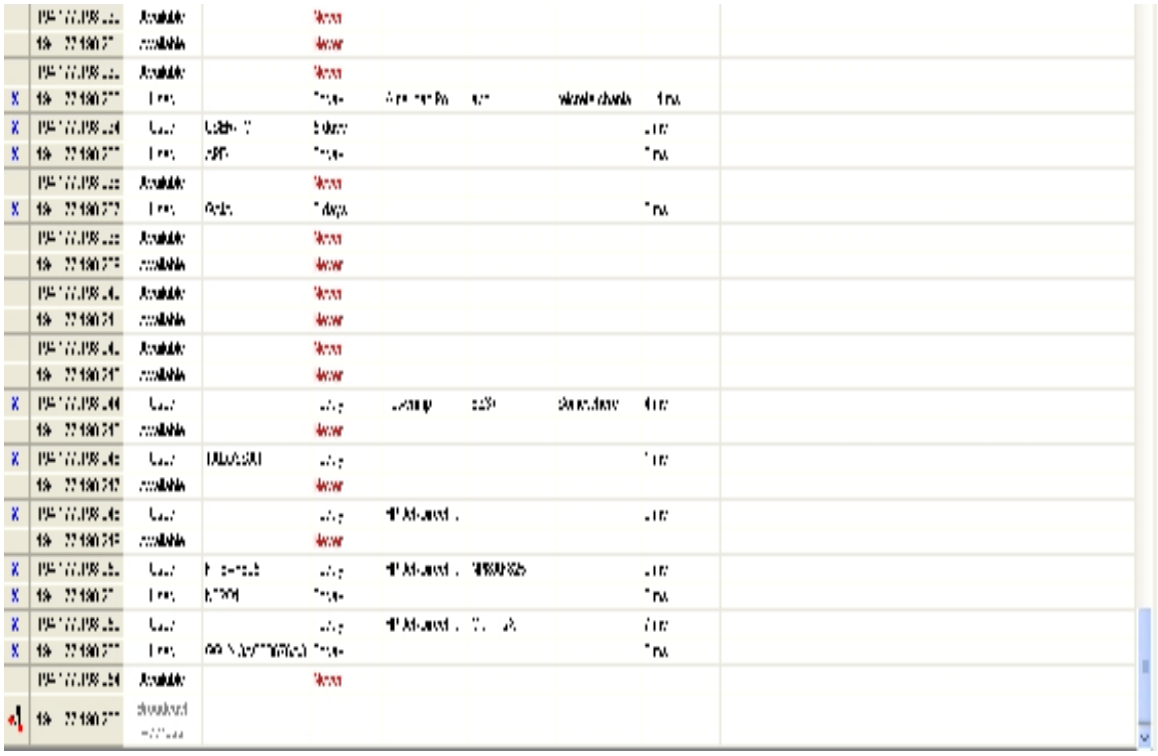
Επίσης διαπιστώνουμε ότι το **ip address management** βρίσκει όλες τις ip ακόμα και αν τη συγκεκριμένη στιγμή δεν είναι ενεργές.
Τα στοιχεία που περιγράψαμε φαίνονται παρακάτω η μάσκα υποδικτυου που βάλαμε ήταν το 255.255.255.0 όποτε αναμενόμενο να πάρουμε και 254 διευθύνσεις ip(class c)





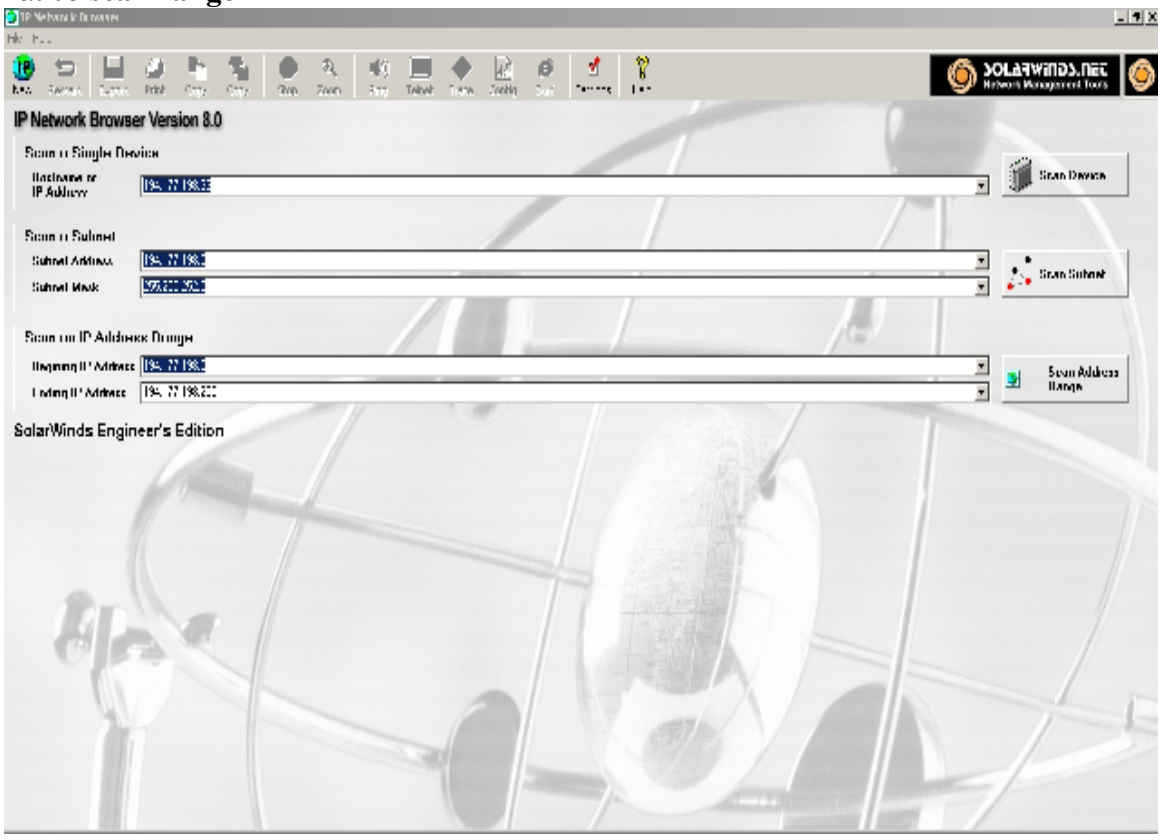






3.2 IP Network Browser

Ανοίγοντας το IP network browser βλέπουμε 3 επιλογές το **scan device** το **scan subnet** και **το scan range IP**

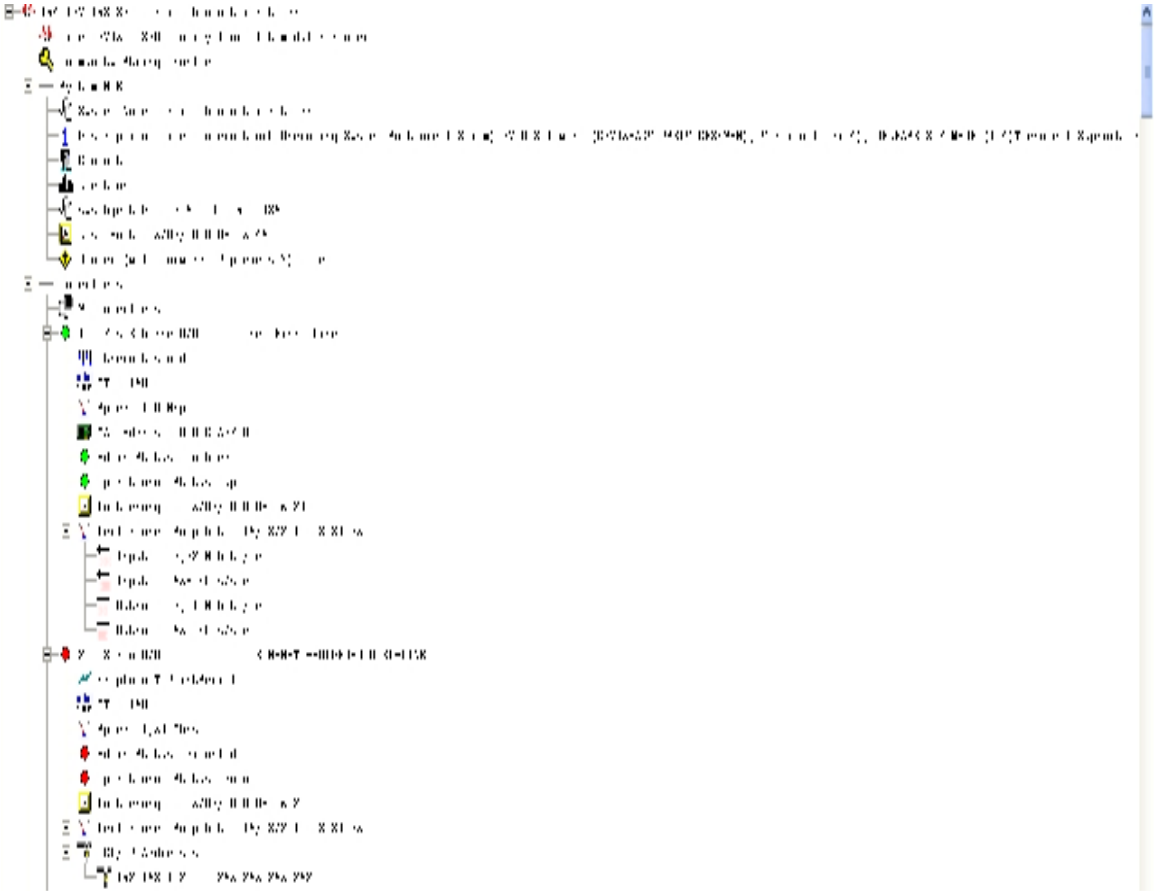


3.2.1 Scan device

Στο scan device μπορούμε να πάρουμε πληροφορίες μιας συγκεκριμένης συσκευής του δικτύου, εμείς πήραμε πληροφορίες για το Cisco router 3745(ο router του δικτύου μας) παρατηρούμε τα αποτελέσματα στα παρακάτω screenshot.
Ίσως είναι από τις σημαντικότερες πληροφορίες που μπορούμε να πάρουμε από το **solarwinds** και εδώ φαίνετε η δύναμη των πρωτοκόλλων διαχειρίσεις.
Τα αποτελέσματα που περνούμε είναι πράγματι παρά πολλά και αφορούν όλα το Cisco router 3745

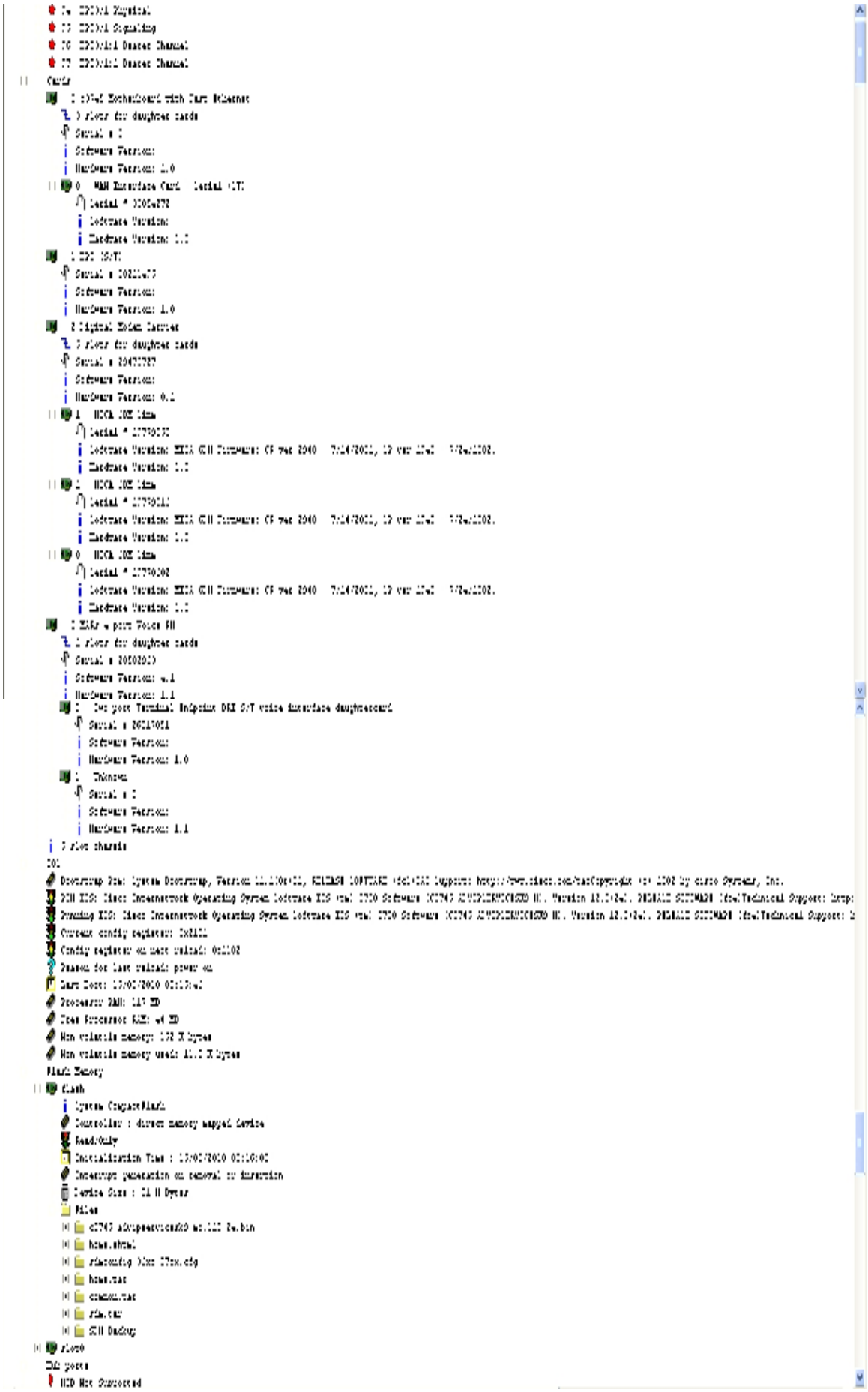
Cisco 3745 information

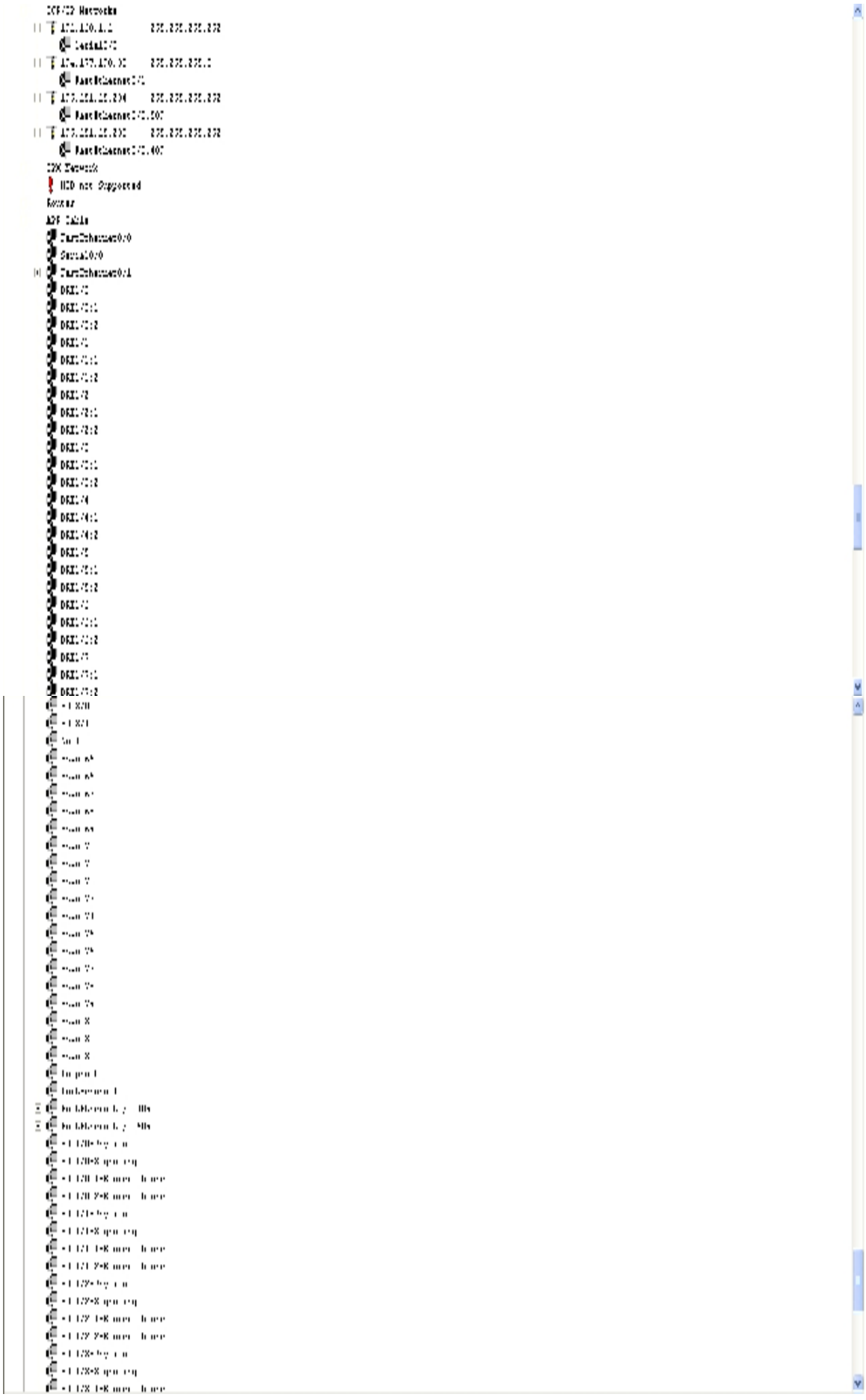
Ο δρομολογητής του Παραρτήματος Χανίων του ΤΕΙ ΚΡΗΤΗΣ είναι ο παρακάτω στον οποίο φαίνετε και η σύνθεση σε κάρτες και εξοπλισμό. Θα μπορούσαμε να πούμε ότι πρόκειται για ένα manual της συσκευής καθώς μας περιέχει πολλές πληροφορίες.
Φυσικά θα πρέπει κάποιος να είναι εξοικειωμένος με όλους τους παραιτώ όρους ώστε να εκμεταλλευτεί στο μέγιστο την σπουδαία αυτή δυνατότητα του solarwinds.

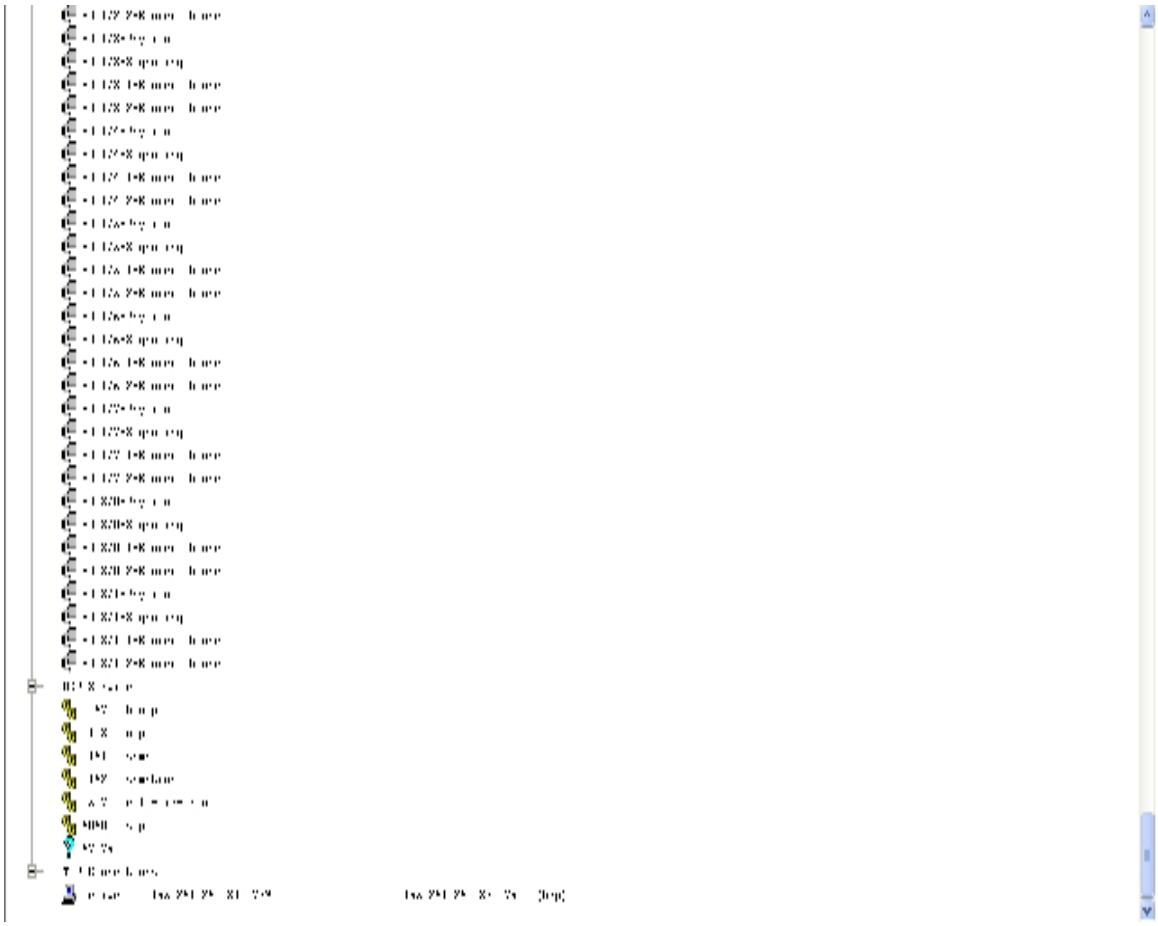










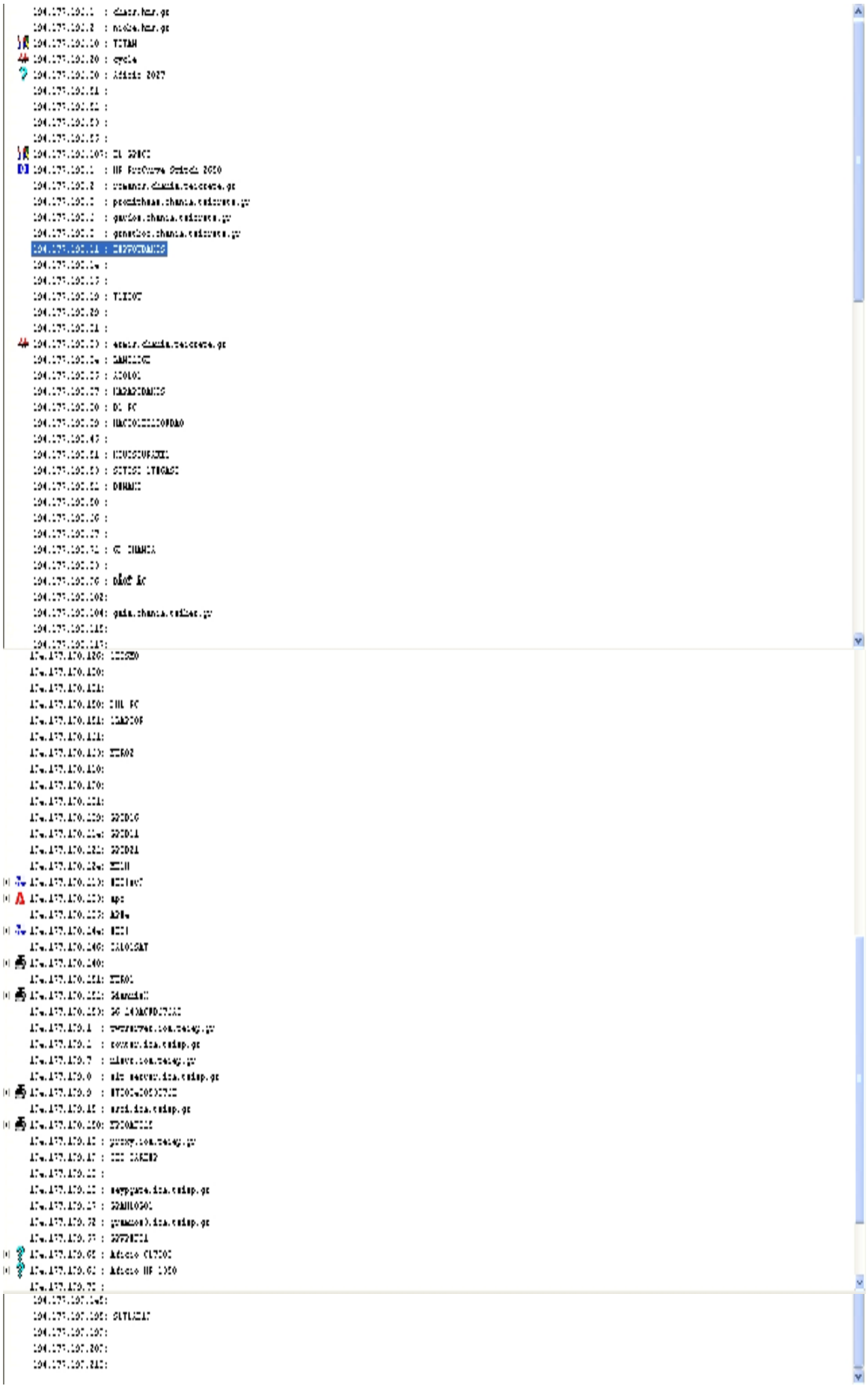


3.2.2 Scan subnet

Στο **scan subnet** μπορούμε να δούμε το δίκτυο μας η και το υποδικτυο που μπορεί να βρίσκετε μέσα στο κεντρικό δίκτυο.

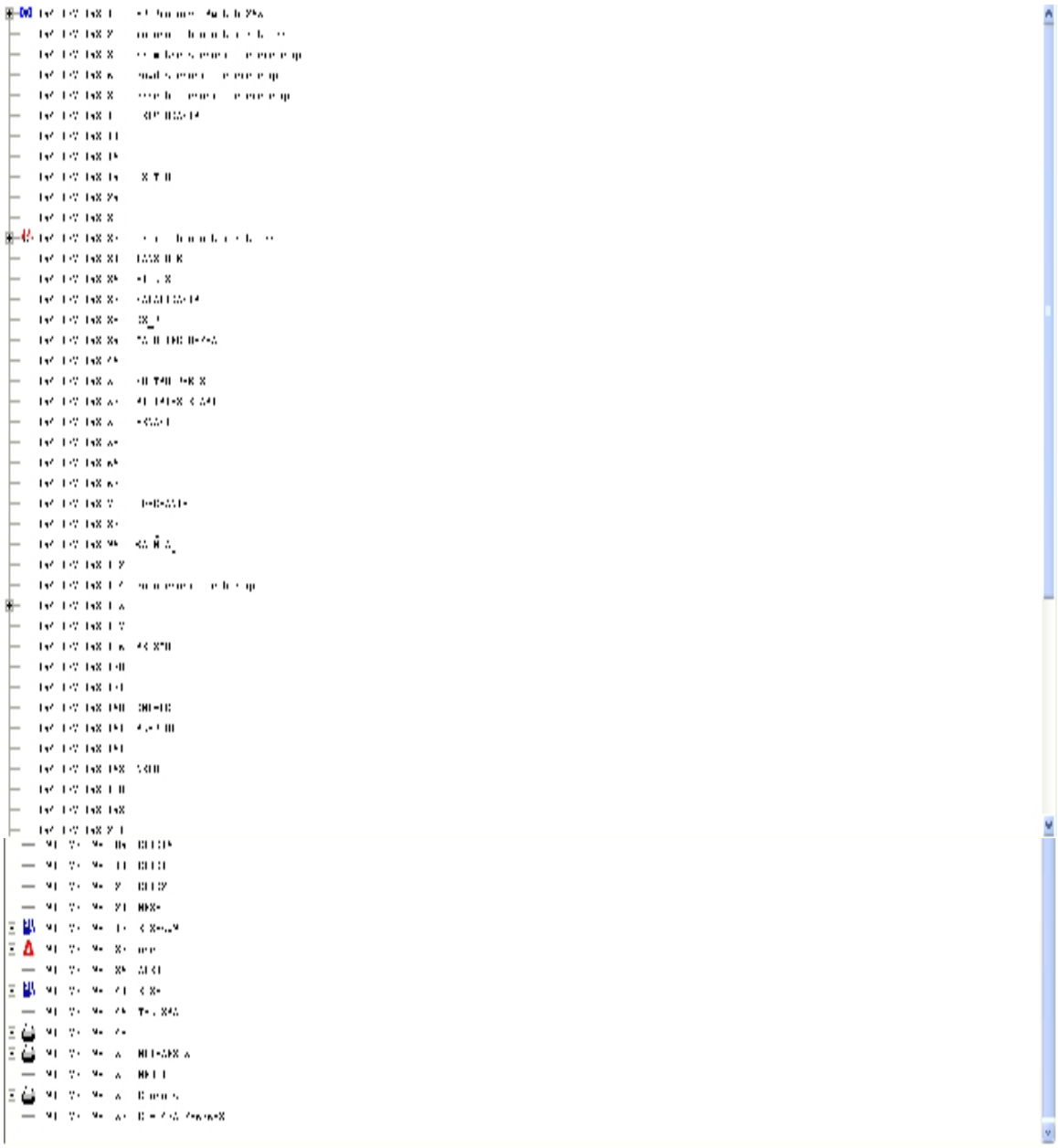
Όπως βλέπουμε στα παρακάτω screenshot το πρόγραμμα έχει βρει το δίκτυο μας τα τερματικά που είναι συνδεμένα όπως και επιπρόσθετες πληροφορίες γι' αυτα.

Το **scan subnet** είναι μια γρήγορη διεργασία για να δούμε από ποσά τερματικά απαρτίζετε το δίκτυο μας και κάποιες πληροφορίες για το καθένα .Σημαντικό είναι ότι στο συγκεκριμένο εργαλείο οι επιλογές μας είναι πολύ περισσότερες απ' ότι στο **IP Address Management** καθώς μας δίνει την δυνατότητα να επέμβουμε στη κάθε συσκευή σαν διαχειριστές δικτύου πλέον π.χ. μπορούμε να αποκλείσουμε μια συγκεκριμένη IP η οποία δεν πλήρη τα κριτήρια του δικτύου μας .



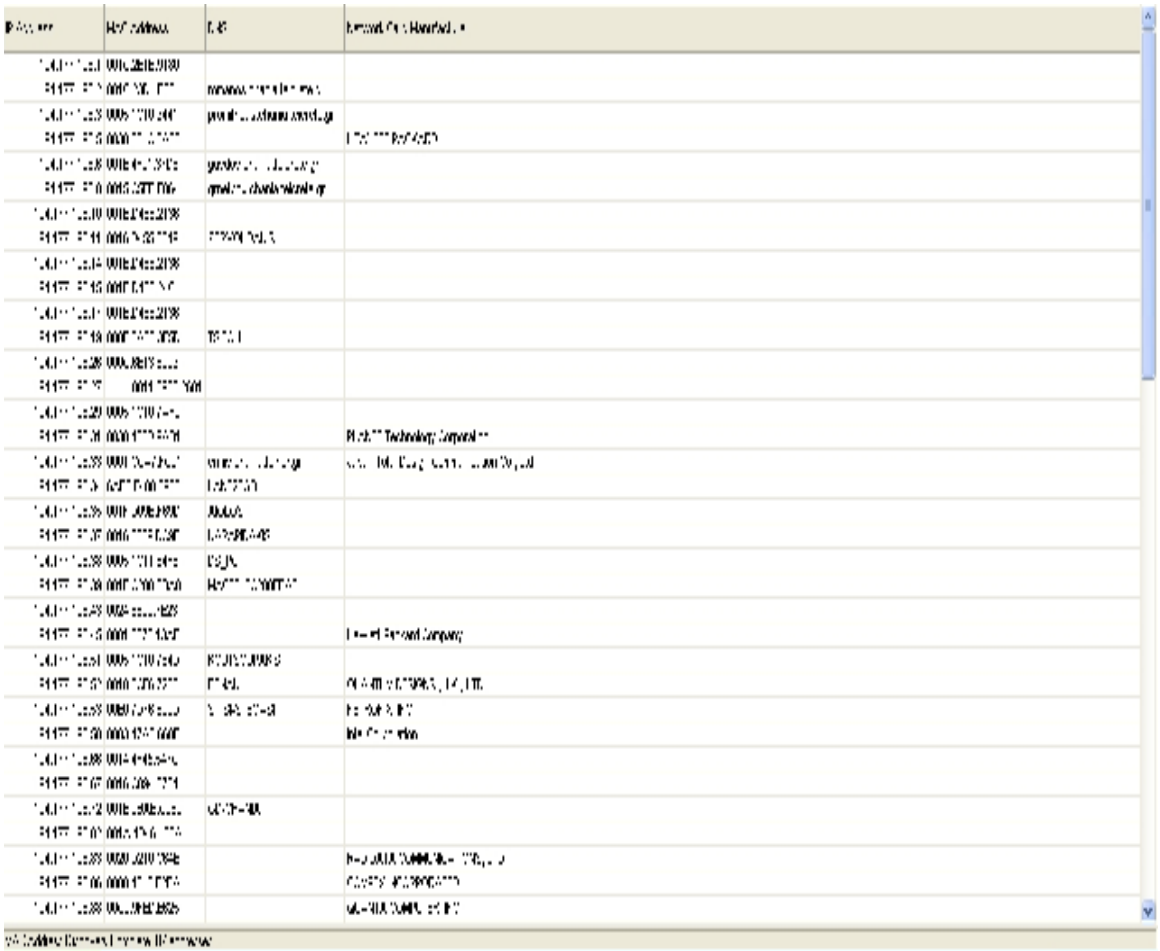
3.2.3 scan range IP

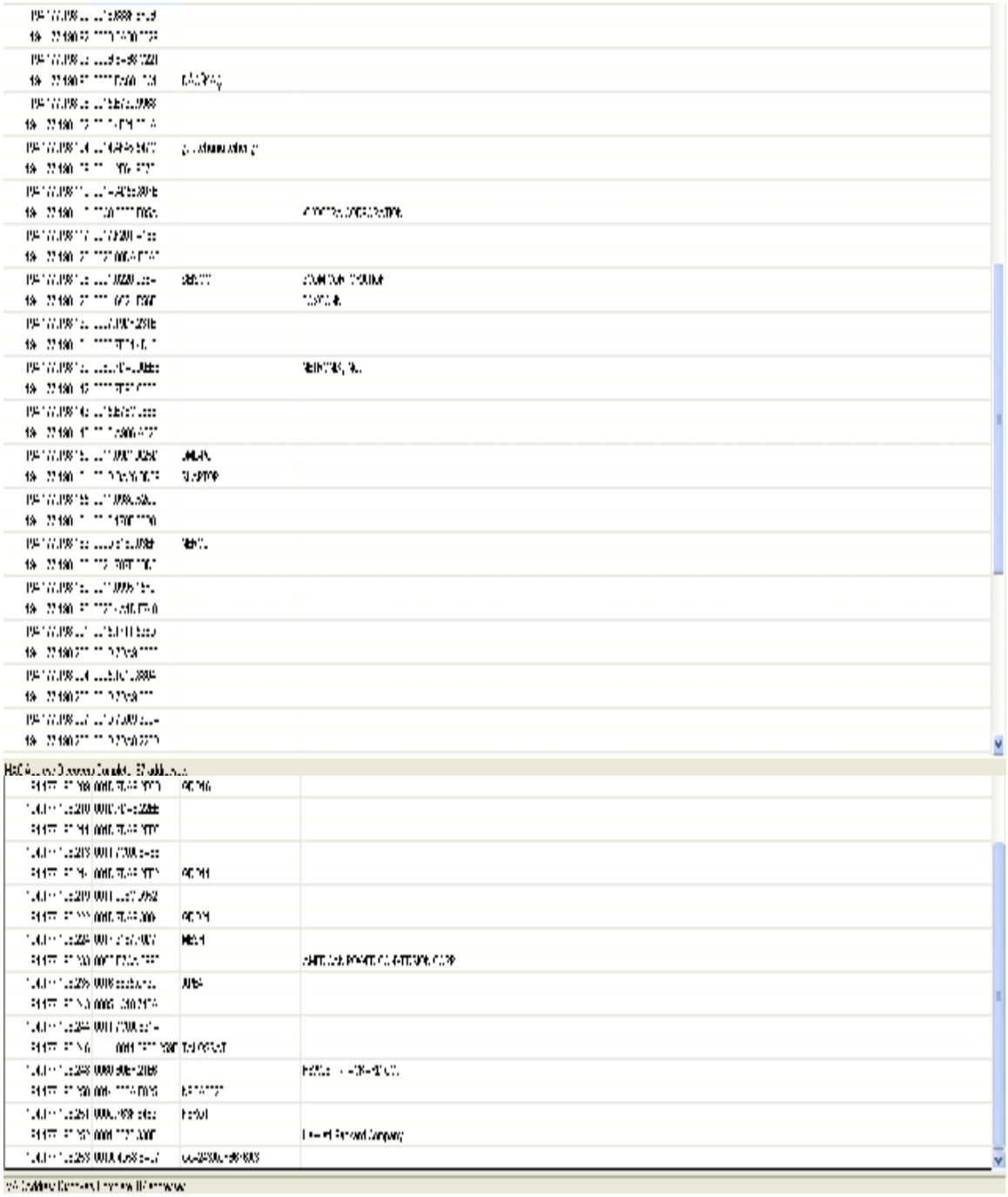
Το **scan range IP** πραγματοποιεί ένα απλό σάρωμα του δικτύου το οποίο μας πληροφορεί άμεσα ποσά τερματικά βρίσκονται στο δίκτυο μας σίγουρα αυτές τις πληροφορίες μπορούμε να τις πάρουμε και από αλλού αλλά το **scan range IP** μας τις δίνει **πολύ γρήγορα**



3.3 Mac address discovery

Το **Mac address discovery** χρησιμοποιείται για να ανακάλυψη την Mac address της κάθε κάρτας διεπαφης που είναι στο δίκτυο. Η Mac address συνδέετε άμεσα με την κάθε IP μεσώ του πρωτοκόλλου TCP/IP, DCHP
Το **Mac address discovery** μας επιτρέπει να κάνουμε αποκοπή μιας IP η μιας Mac address η ακόμα να κάνουμε μια **IP reserve**. (αποκλειστική).
Σε πολλές περιπτώσεις θα θέλαμε να ξέρουμε την Mac address κάθε συσκευής καθώς αυτή είναι μοναδική σε ολόκληρο τον διαδικτυακό τόπο. Για παράδειγμα θα μπορούσαμε να αποκλείσουμε μια συγκεκριμένη Mac address σαν κακόβουλη.
Σίγουρα πρόκειται για μια πόλη σημαντική λειτουργία καθώς μπορούμε από απόσταση να βρούμε όλες τις Mac του δικτύου μας και ανάλογα να χειριστούμε την Mac όπου μας ενδιαφέρει π.χ. θα μπορούσαμε να επιτρέψουμε η να αποκλείσουμε σε μια Mac μεσώ φιλτραρίσματος του router την πρόσβαση στο internet η ακόμα και την συμμετοχή στο τοπικό δίκτυο.

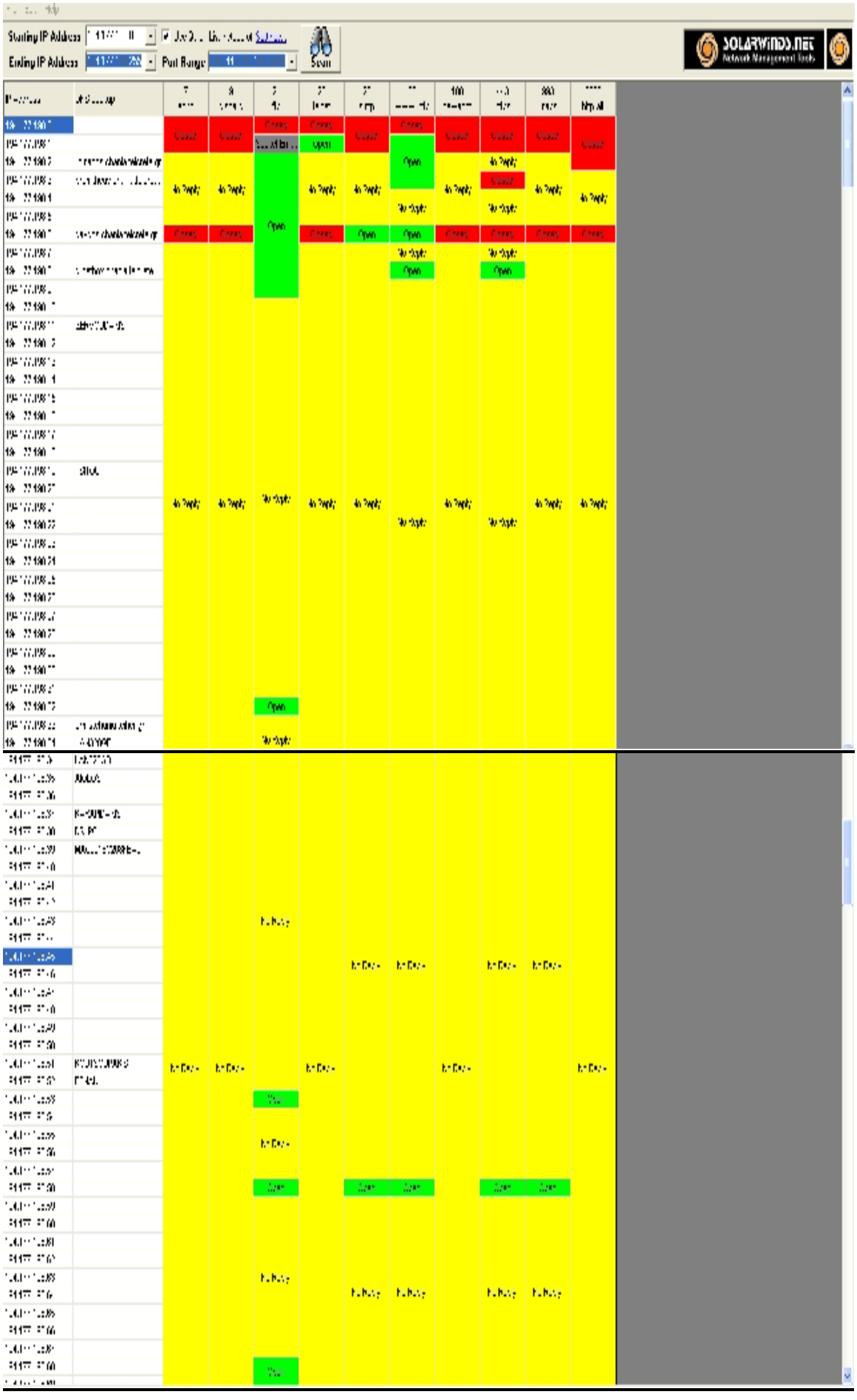


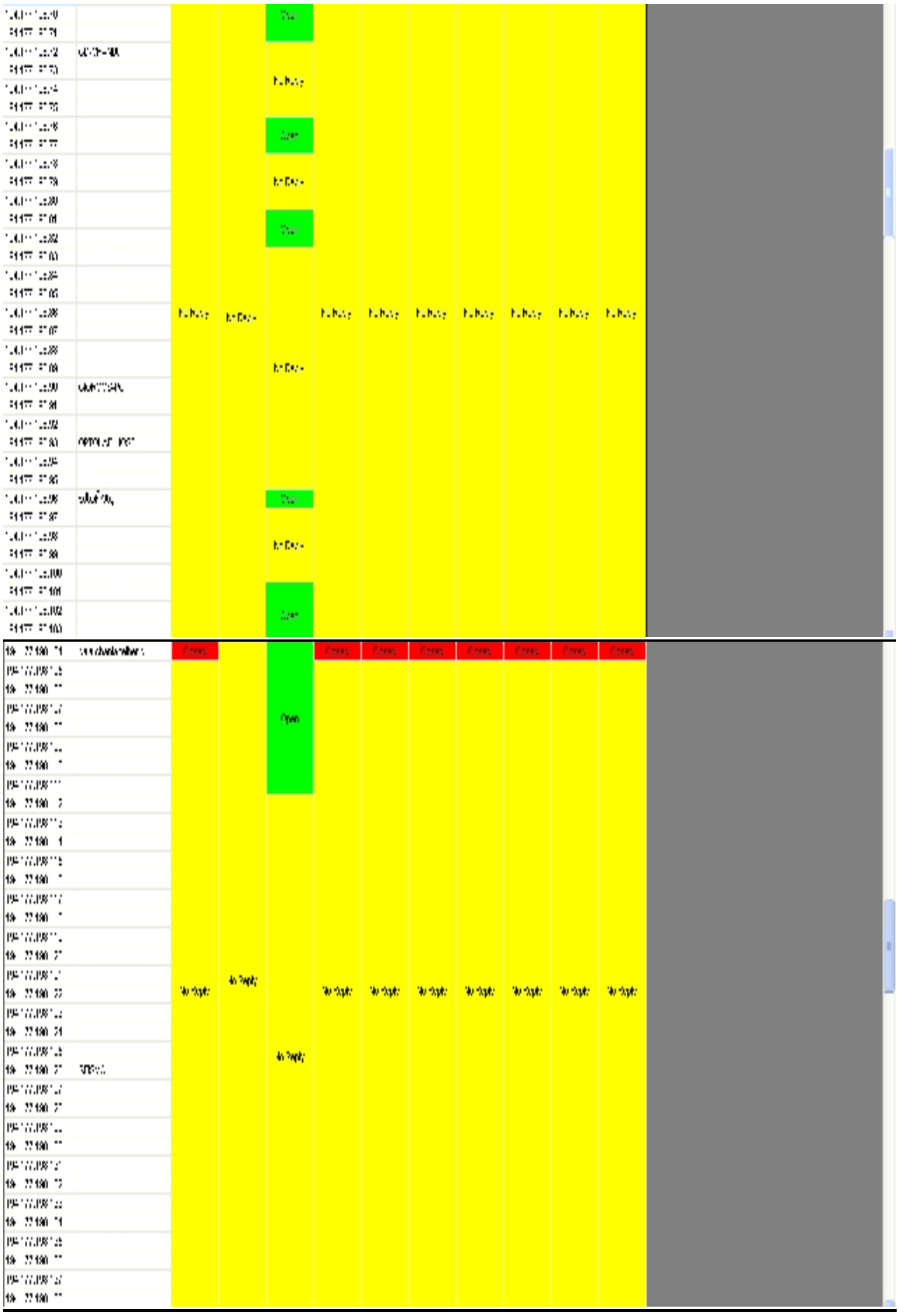


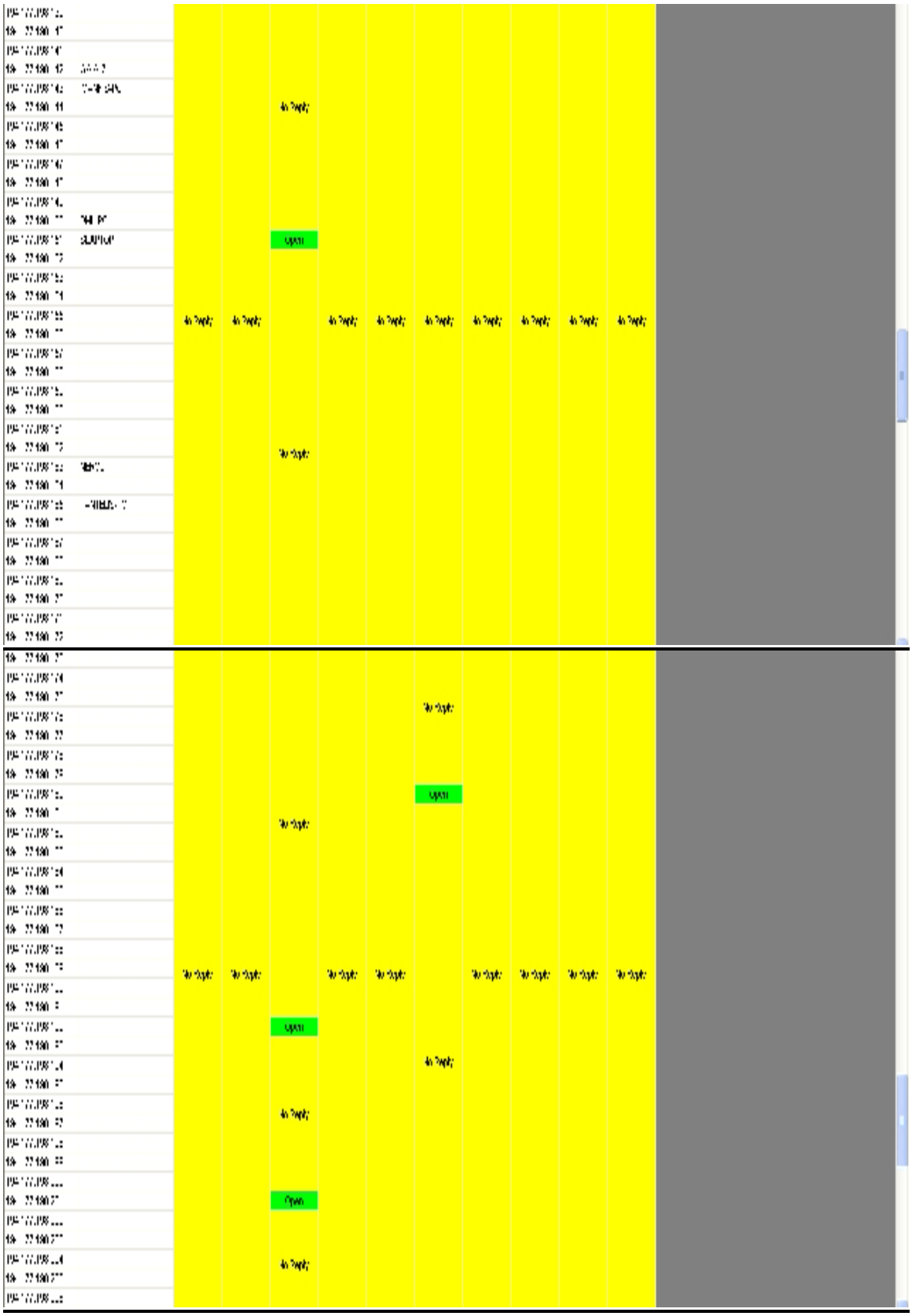
3.4 port scanner

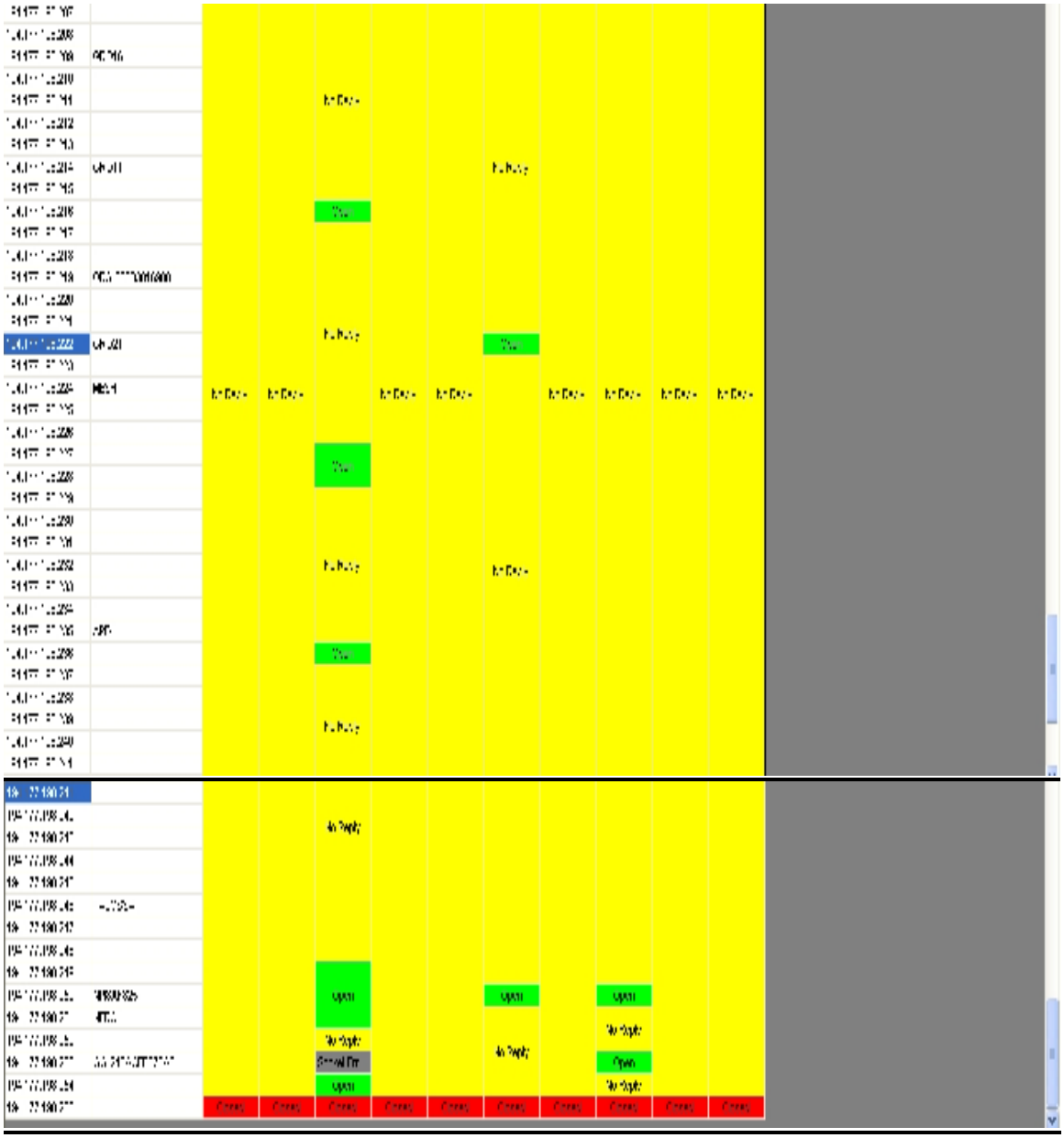
Κάθε Η/Υ έχει ένα σύνολο από Θύρες (Πόρτες) Δικτύου. Αυτές μπορεί να είναι κλειστές ή ανοικτές. Ο αριθμός των δικτυακών θυρών αυτών είναι 65536. Κάποιες Θύρες είναι αφιερωμένες σε ειδικούς σκοπούς όπως για παράδειγμα η μεταφορά αρχείων 21 (FTP), η θύρα 23 (Telnet) η περιήγηση στο ιντερνετ 80 (Web Browsing) κτλ. Κάποιες άλλες είναι ελεύθερες.

Το **port scanner** του solarwinds είναι μια διεργασία η οποία μπορεί να ανακαλύψει από μακριά την κατάσταση της κάθε IP σχετικά με ποιες πόρτες χρησιμοποιεί η κάθε συσκευή. Μπορούμε να σαρώσουμε μια περιοχή τιμών IP Και να δούμε ποιες πόρτες χρησιμοποιούνται επίσης μπορούμε να σαρώσουμε επιθυμητές πόρτες (π.χ. Port 80 μόνο) Που αντιστοιχεί στο πρωτόκολλο http. Έτσι με αυτό τον τρόπο έχουμε μια πλήρη άποψη για το ποιες πόρτες χρησιμοποιεί ο κάθε υπολογιστής.


Starting IP Address
Ending IP Address
Port Range
Scan
SOLARWINDS.NET
Network Management Tools

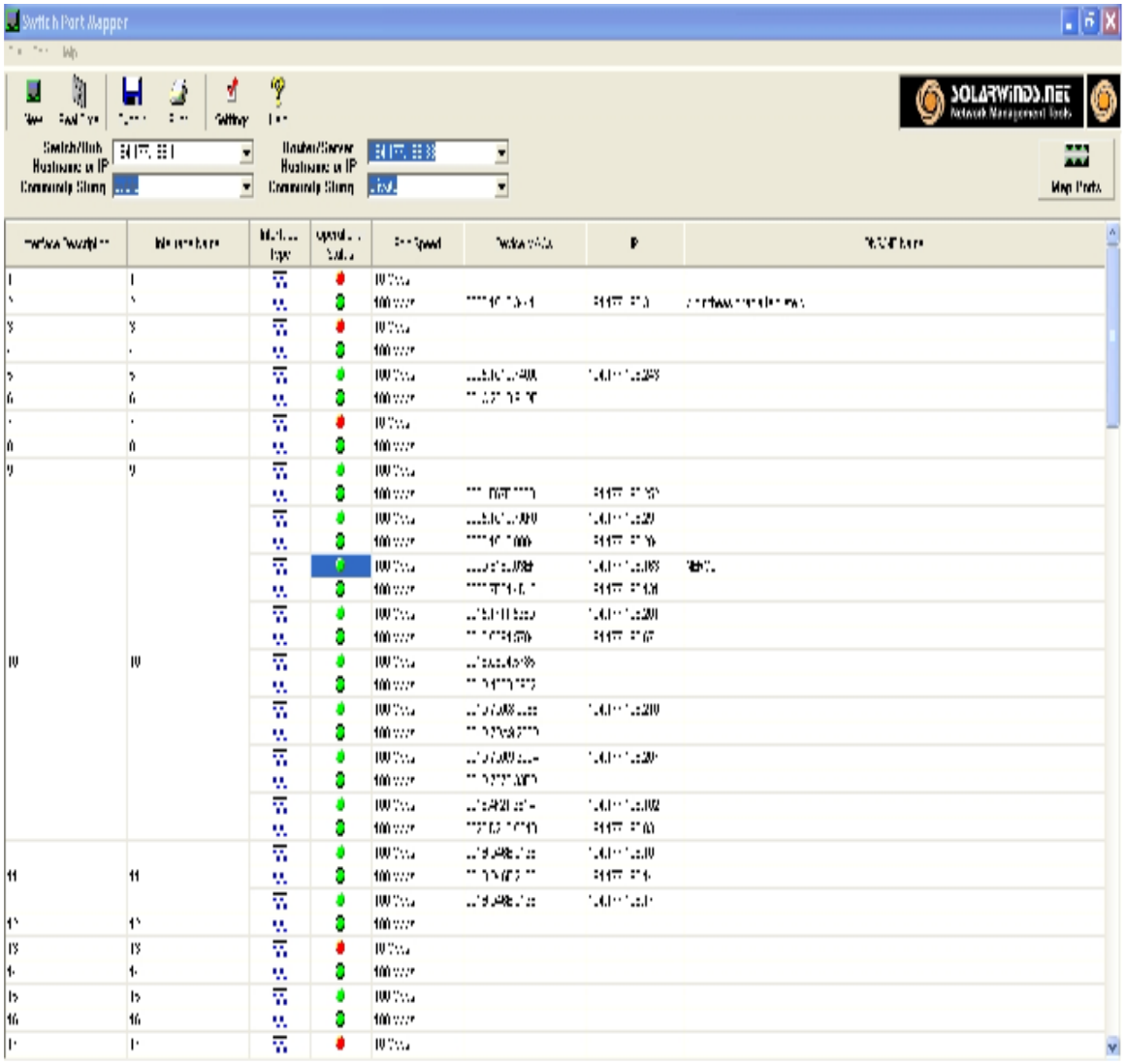


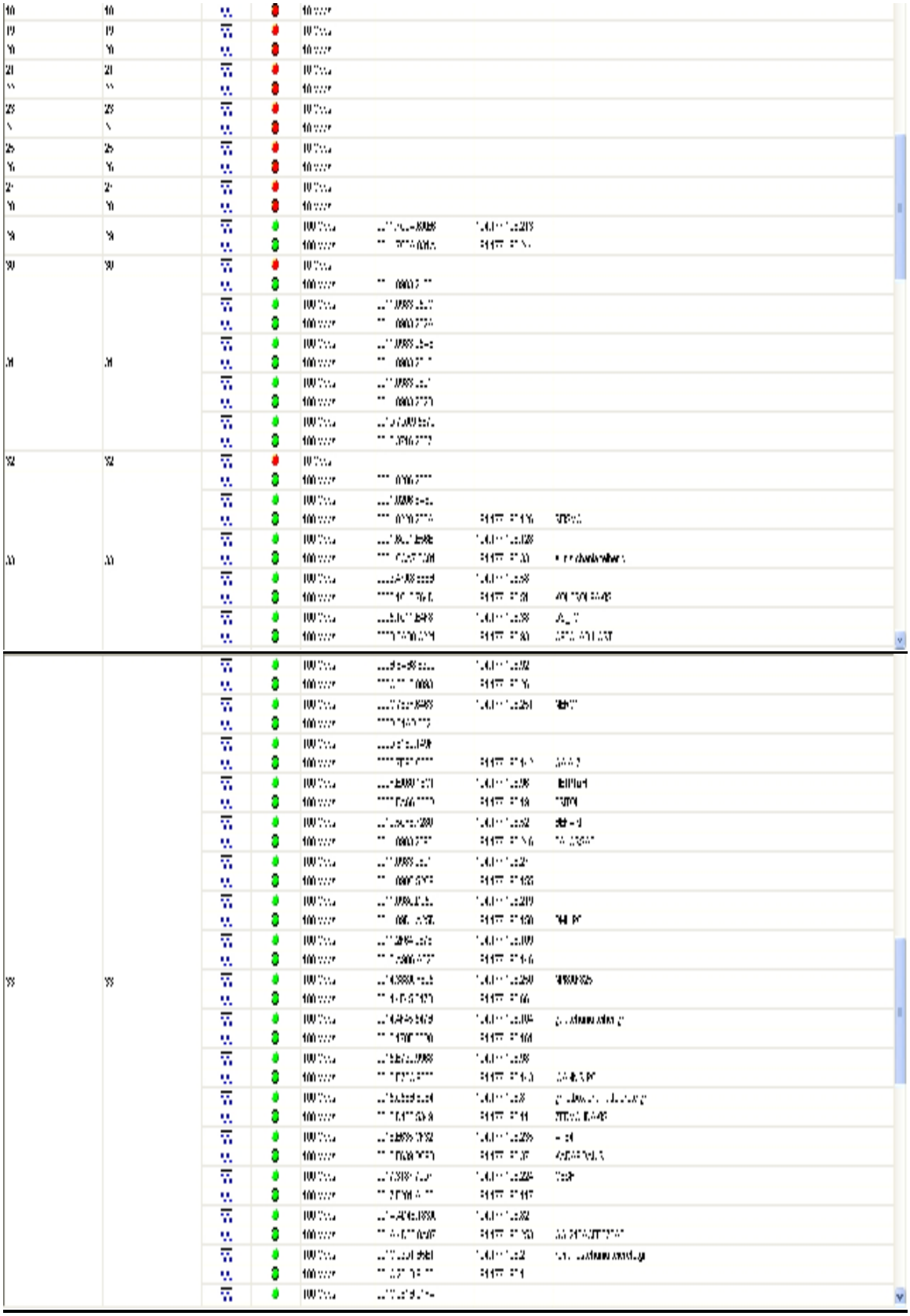


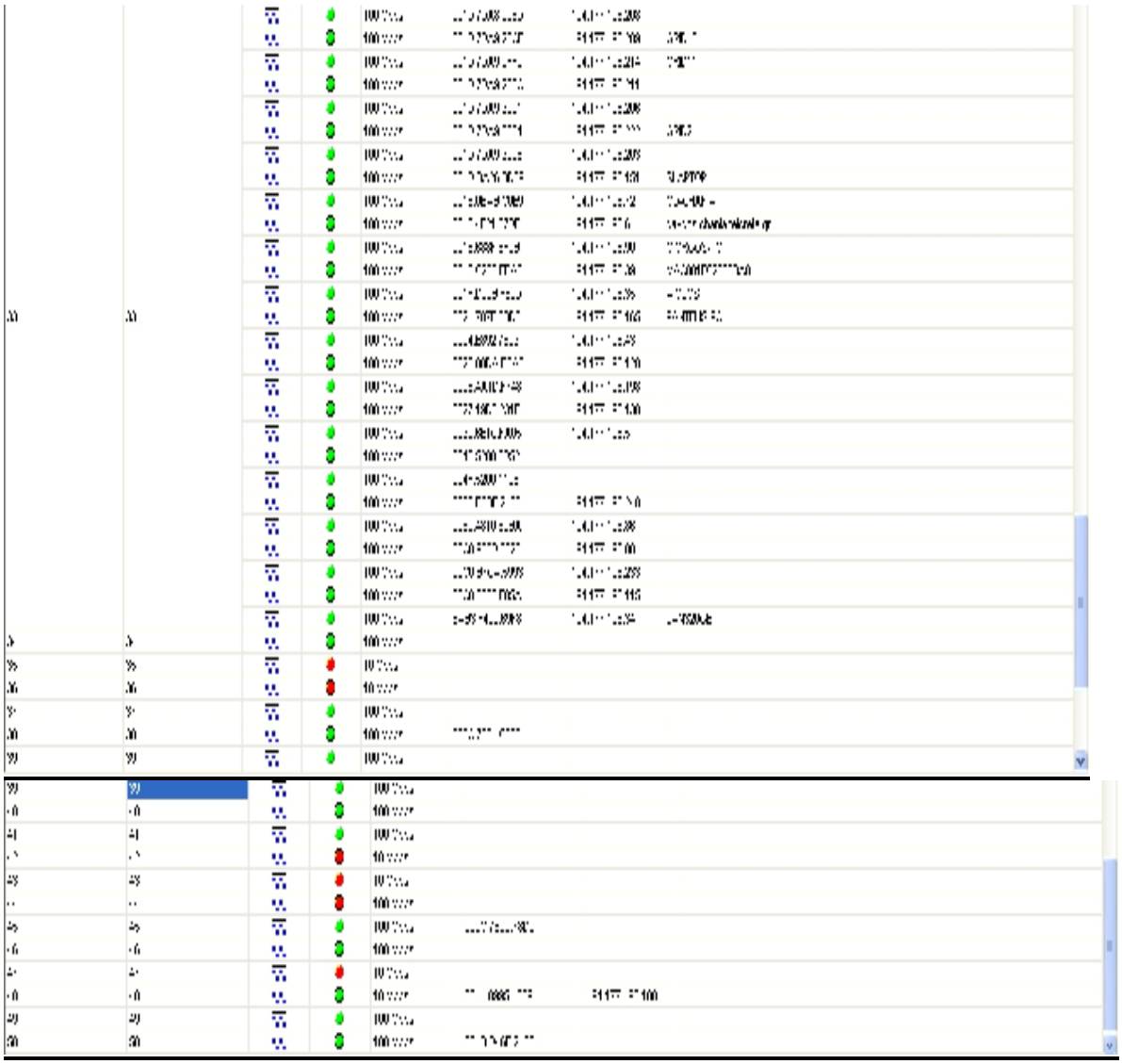


3.5 Switch port mapper

Το εργαλείο Switch port mapper μπορεί να προσδιορίσει ποιες θύρες του router μας χρησιμοποιεί ο κάθε υπολογιστής του δικτύου όπως και να μας δώσει πληροφορίες για την Ip την Mac address και γενικές πληροφορίες της πόρτας όπου χρησιμοποιεί μπορεί να ανακαλύψει και ξεχωριστά τμήματα δικτύου όπως routers/hubs στην ουσία κάνει μια χαρτογράφηση των θυρών της κάθε συσκευής του δικτύου. Σημαντικό πλεονέκτημα που μας δίνει το συγκεκριμένο εργαλείο είναι ότι μπορούμε να καταστήσουμε ενεργή η ανενεργή μια συγκεκριμένη πόρτα του router.
Πηγαίνοντας πάνω σε μια ενεργή πόρτα (πράσινη ένδειξη) μπορούμε κάνοντας δεξί κλικ να πατήσουμε την εντολή «shutdown interface» με αυτό τον τρόπο απενεργοποιούμε την πόρτα λογισμικά και τι καταστούμε μια ενεργή έτσι η ροή πληροφορίας από την συγκεκριμένη πόρτα παύει να υφίσταται.
Με πράσινο φαίνονται η ενεργές πόρτες και με κόκκινο η μη ενεργές πόρτες την συγκεκριμένη χρονική στιγμή, επίσης επιπρόσθετα μας εμφανίζει και την ταχύτητα της κάθε πόρτας σε Mbps αυτό φυσικά έχει να κάνει και με το φυσικό επίπεδο σύνδεσης (physical layer) καθώς και με την εγκατάσταση και τα χαρακτηριστικά της κάρτας διεπαφης δικτύου.
(10/100/1000 mbps)





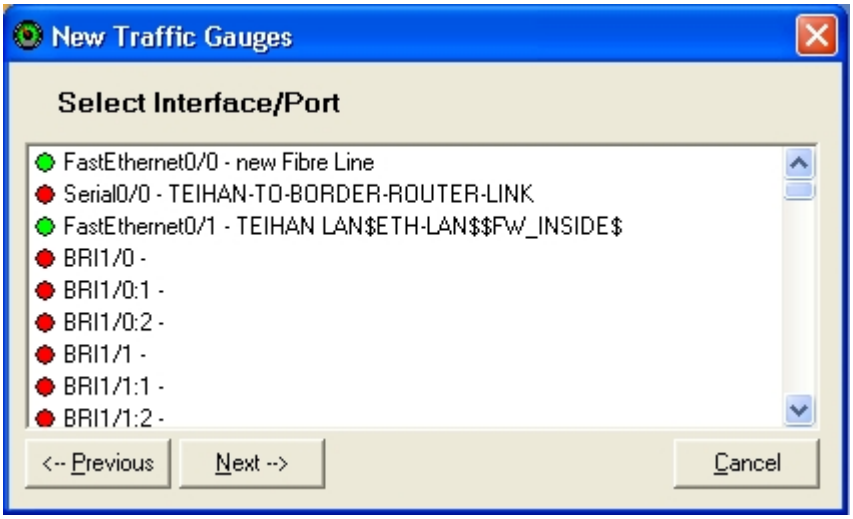


3.6 Bandwidth gauges

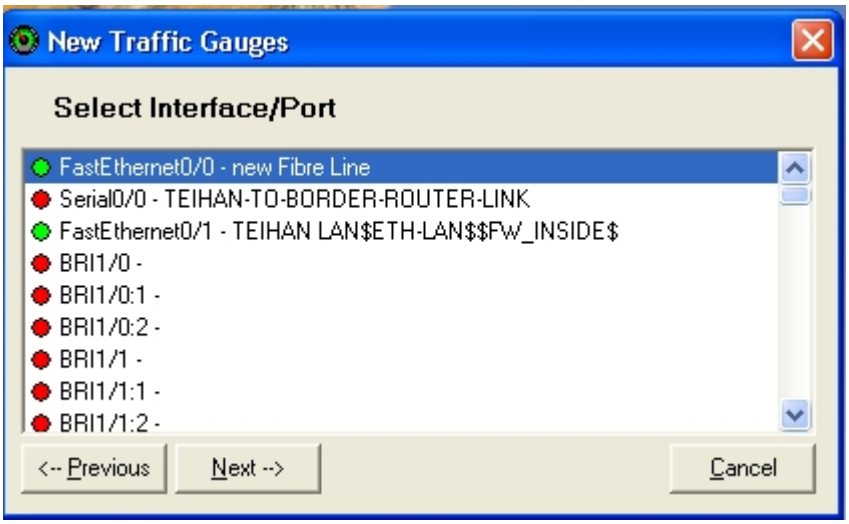
Σε κάθε δίκτυο καίριο ρόλο έχει το bandwidth της εισερχόμενης και εξερχόμενης γραμμής παροχής καθώς και ο διαμερισμός του στα επιμέρους τερματικά του δικτύου. Το Bandwidth gauges μπορεί να προσδιορίσει την ταχύτητα (bandwidth) Που εισέρχεται στο router καθώς και την εξερχόμενη ροή(download, upload)



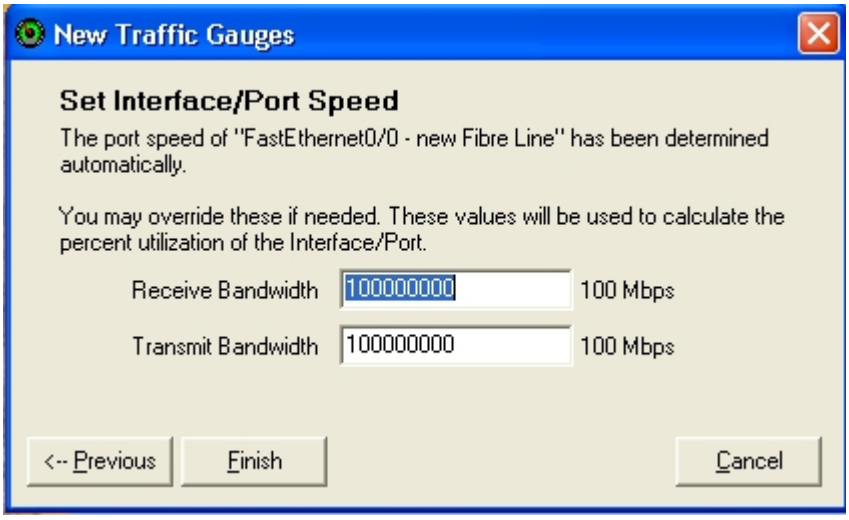
Βάζουμε την IP του router και το snmp community string: private



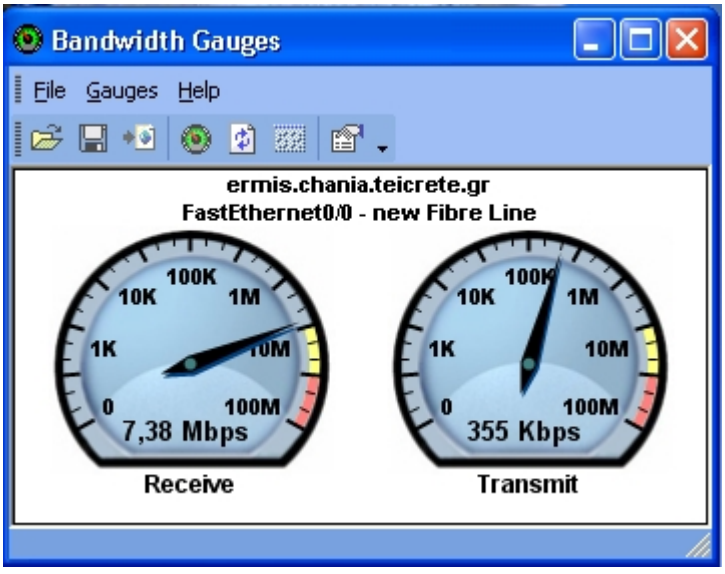
Το παράθυρο που μας ανοίγει μας περιέχει πληροφορίες σχετικά με τις συνδέσεις του router



Επιλέγουμε την πρώτη επιλογή όπου στην περίπτωση μας είναι η εισερχόμενη γραμμή internet μια οπτική ίνα .



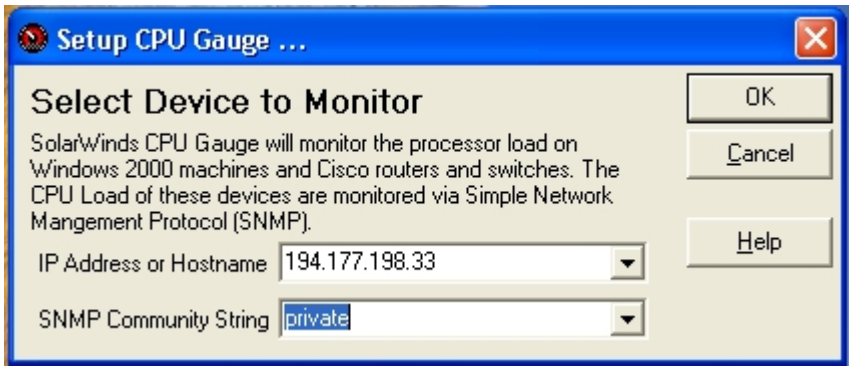
Βάζουμε τη επιθυμητή ταχύτητα Αποστόλης και λήψης



Τα αποτελέσματα της μέτρησης φαίνονται στο παρακάτω μετρητή όπου μας δείχνει την ταχύτητα Αποστόλης και λήψης την συγκεκριμένη στιγμή.

3.7 Cpu gauge

Το cpu gauge μπορεί να μετράει την χρησιμοποίηση της cpu (την καταπόνηση του επεξεργαστή του router/hub).χρησιμοποιεί το πρωτοκολλώ SNMP για να επικοινωνήσει με την συσκευή και να πάρει τα αποτελέσματα της κίνησης. Γενικά ta modem/router υπάρχει το πρόβλημα της συμφόρησης όπου υπάρχει μεγάλη κίνηση(traffic) με αποτέλεσμα ο router/modem να αρχίσει να μην συμπεριφέρεται σωστά ο μετρητής αυτός μας κρατάει ενήμερους για την κατάσταση της cpu.



Βάζουμε την IP του router και το snmp community string: private



Όπως βλέπουμε τη συγκεκριμένη χρονική στιγμή το cpu gauge μας πληροφορεί ότι ο router χρησιμοποιεί το 2% των δυνατοτήτων του.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα πτυχιακή εργασία ασχοληθήκαμε με τη διαχείριση δικτύου σε ένα σχετικά μεγάλο τοπικό δίκτυο.
Περιγράψαμε την σημασία και τον ρόλο που έχει η διαχείριση δικτύου στα σημερινά δίκτυα είδαμε τα πρωτοκολλά επικοινωνίας που είναι υπεύθυνα για την διαχείριση και τη σωστή μεταφορά δεδομένων καθώς τα υπέρ και κατά αυτών. Επίσης δείξαμε την λειτουργία του προγράμματος solarwinds σε πραγματικό χρόνο με πλήρη λειτουργία του δικτύου του ΤΕΙ ΧΑΝΙΩΝ παίρνοντας τις επιθυμητές μετρήσεις.
Το συμπέρασμα από την όλη λειτουργία του προγράμματος είναι ότι το solarwinds είναι ένα πολύ δυνατό και γρήγορο software όπου μπορεί να μας παρέχει όλες της πληροφορίες που χρειαζόμαστε ώστε να κάνουμε διαχείριση δικτύου. Φυσικά στο εμπόριο διατίθενται πολύ πιο ακριβά και αποδοτικά λογισμικά για διαχείριση δικτύων με μεγαλύτερες βάσεις δεδομένων πιο όμορφα παράθυρα και πιο εύκολα στη χρήση τους πέραν όμως τούτων το solarwinds έκανε τη δουλεία που εμείς θέλαμε χωρίς κανένα απολύτως πρόβλημα δηλαδή την διαχείριση του δικτύου του ΤΕΙ ΧΑΝΙΩΝ.

Η **επεκτασιμότητα** του προγράμματος είναι άμεση και έχει να κάνει με το υλικό μέρος ενός δικτύου εμείς ότι αλλαγές κάνουμε σε υλικό στο δίκτυο μας (προσθαφαίρεση συσκευών, τερματικών) θα ανακαλυφτεί αμέσως από το solarwinds μιας και αυτό τρέχει σε πραγματικό χρόνο και μπορεί να ανακαλύψει όλες τις λεπτομέρειες του δικτύου μας.