Πανεπιστήμιο Μακεδονίας

ΠΜΣ Πληροφοριακά Συστήματα

Τεχνολογίες Τηλεπικοινωνιών & Δικτύων

Καθηγητές: Α.Α. Οικονομίδης & Α. Πομπόρτσης

ΘΕΜΑ:

«ΣΥΓΚΡΙΣΗ ΔΩΡΕΑΝ ΕΡΓΑΛΕΙΩΝ ΓΙΑ ΔΙΑΧΕΙΡΙΣΗ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΔΙΚΤΥΩΝ»

ΚΑΛΥΒΑ ΕΛΕΝΗ

Α.Μ. 02/2006

email: mis062@uom.gr

Θεσσαλονίκη, 2006

University of Macedonia
Master Information Systems
Networking Technologies
Professors: A.A. Economides & A. Pomportsis

SUBJECT:

«Comparison of Free Tools for Network Monitoring & Management»

KALIVA ELENI
R.N. 02/2006
email: mis062@uom.gr

Thessaloniki, 2006

ΠΕΡΙΛΗΨΗ

Τα τελευταία χρόνια τα δίκτυα υπολογιστών 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. Η πολυπλοκότητα αυτών των δικτύων κάνει αναγκαία τη χρήση εργαλείων αυτόματης διαχείρισης.

Το δίκτυο κάθε οργανισμού / επιχείρησης είναι σχεδιασμένο και υλοποιημένο με τέτοιο τρόπο ώστε να καλύπτονται οι ανάγκες του. Έτσι, στα σύγχρονα δίκτυα παρατηρείται μεγάλη ποικιλομορφία τόσο στις τοπολογίες δικτύων όσο και στους τύπους των συσκευών που χρησιμοποιούνται για τη διαδικτύωση. Σήμερα, υπάρχει στην αγορά μεγάλη πληθώρα πακέτων λογισμικού για διαχείριση δικτύων τα οποία καλύπτουν διαφορετικούς τύπους δικτύων και είναι εστιασμένα σε διάφορους τομείς της διαχείρισης δικτύων.

Σκοπός της παρούσας εργασίας είναι η εκπόνηση μιας συγκριτικής μελέτης για τα δωρεάν εργαλεία διαχείρισης δικτύων. Έχουν επιλεγεί εφαρμογές οι οποίες ανταποκρίνονται σε διαφορετικές ανάγκες ενός συστήματος διαχείρισης. Γίνεται μια συνοπτική παρουσίαση των εφαρμογών και των πλεονεκτημάτων / μειονεκτημάτων που αυτές διαθέτουν. Στη συνέχεια πραγματοποιείται συγκριτική μελέτη μεταξύ των εξεταζόμενων εφαρμογών. Τέλος, σκιαγραφούνται οι μελλοντικές τάσεις των συστημάτων διαχείρισης δικτύων.

ABSTRACT

Recently, computer networks have undergone a great development. The trend in developing such networks is along the axis of bigger and more complicate networks that supports more and more users and applications. The complexity of those systems makes more than necessary the use of automatic management tools.

The network of each organization / enterprise is designed and materialized in such a way that satisfy its needs. Therefore, great diversity in network topologies as well as in network devices that are used in networks is observed in the up-to-date networks. Today, a great number of network management software packages that satisfy the needs of different types of networks and focus on different network management areas, are presented in the market

The current assignment aims at the materialization of a comparative review of free network management and monitoring tools. The applications that have been chosen correspond to different needs of a network management system. The selected tools together with their advantages/ disadvantages are briefly presented. The comparative review of the selected applications follows. Finally, the future trends in network management systems are sketched out.

ΠΕΡΙΕΧΟΜΕΝΑ

CONTENTS

1 Παρουσίαση του Προβλήματος

1.1 Εισαγωγή στην 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. Γενικότερα, τα δίκτυα και όλα τα σχετικά με αυτά και τις κατανεμημένες εφαρμογές τους γίνονται απαραίτητα για τον καθένα που τα χρησιμοποιεί[1].

Αυξάνοντας η πολυπλοκότητα και το μέγεθος των δικτύων τόσο αυξάνει η πιθανότητα να συμβεί κάποιο λάθος και έτσι ολόκληρο το δίκτυο ή ένα μέρος του να τεθεί εκτός λειτουργίας, ή να μειωθεί η αξιοπιστία του.

Πολλά προβλήματα δικτύου προκύπτουν όχι από ξαφνική δυσλειτουργία των μηχανημάτων αλλά από βαθμιαίες διαβρώσεις εκτέλεσης που θα μπορούσαν να είχαν ανιχνευθεί νωρίτερα. Άλλα πάλι δεν σχετίζονται καθόλου με λάθη, αλλά προέρχονται από προβλήματα χωρητικότητας που αναπτύσσονται με το χρόνο ή σαν αποτέλεσμα ενός ασυνήθιστου γεγονότος.

Σκοπός της διαχείρισης του δικτύου είναι :

- Η διατήρηση της ικανοποιητικής και αξιόπιστης λειτουργίας ακόμη και κάτω από συνθήκες υπερφόρτωσης ή βλάβης, καθώς επίσης και κάτω από αλλαγές της διαμόρφωσης του δικτύου (εισαγωγή νέων συσκευών ή υπηρεσιών).

- Η βελτίωση της απόδοσης του δικτύου, η οποία σχετίζεται με την ποιότητα και την ποσότητα των υπηρεσιών που παρέχονται στους χρήστες.

Ένα μεγάλο δίκτυο είναι δύσκολο να διαχειριστεί μόνο με ανθρώπινη προσπάθεια. Η πολυπλοκότητα αυτών των δικτύων κάνει αναγκαία τη χρήση αυτόματης διαχείρισης. Η απαίτηση για την ανάπτυξη εργαλείων που θα βοηθήσουν στη διαχείριση των δικτύων επιτείνεται τα τελευταία χρόνια με τη χρήση στα δίκτυα συσκευών που ανήκουν σε διαφορετικούς κατασκευαστές. Έτσι έχουν αναπτυχθεί πρωτόκολλα, βάσεις διαχείρισης πληροφοριών και συνοδευτικές υπηρεσίες.

1.2 Απαιτήσεις από το Σύστημα Διαχείρισης

Οι πιο σημαντικές λειτουργικές περιοχές στη διαχείριση ενός δικτύου όπως ορίζονται από το Διεθνή Οργανισμό Προτυποποίησης (ISO) είναι οι ακόλουθες [2]:

1.2.1 Διαχείριση Σφαλμάτων (Fault Management)

Για τη διατήρηση της σωστής λειτουργίας ενός σύνθετου δικτύου πρέπει να υπάρχει μέριμνα για την καλή λειτουργία τόσο ολόκληρου του δικτύου όσο και των επιμέρους στοιχείων του. Όταν συμβεί κάποιο σφάλμα είναι αναγκαίο όσο το δυνατόν συντομότερα να:

- Προσδιορισθεί που βρίσκεται το σφάλμα.

- Απομονωθεί το υπόλοιπο του δικτύου έτσι ώστε να μπορεί να λειτουργεί χωρίς παρεμβολές.

- Αναδιαμορφωθεί το δίκτυο έτσι ώστε να ελαχιστοποιηθεί η επίδραση από τη βλάβη σε κάποιο ή κάποια στοιχεία του.

- Επισκευαστεί ή να αντικατασταθεί το στοιχείο με τη βλάβη έτσι ώστε να επανέλθει το δίκτυο στην αρχική του κατάσταση.

Για να μπορεί να επιτευχθεί γρήγορη επίλυση του προβλήματος χρειάζεται να γίνει γρήγορη και αξιόπιστη ανίχνευση και διάγνωση σφαλμάτων που θα έχει τη μικρότερη δυνατή επιβάρυνση στη λειτουργία του δικτύου.

1.2.2 Διαχείριση Κοστολόγησης (Accounting Management)

Σε πολλές επιχειρήσεις και οργανισμούς υπάρχει χρέωση για τις προσφερόμενες υπηρεσίες του δικτύου. Ο διαχειριστής του δικτύου απαιτείται να παρακολουθεί τη χρήση των πόρων του δικτύου από τον τελικό χρήστη ή ομάδα χρηστών για τους παρακάτω λόγους:

- Ο τελικός χρήστης ή ομάδα χρηστών παραβιάζουν τα δικαιώματα πρόσβασης και επιβαρύνουν το δίκτυο.
- Ο τελικός χρήστης μπορεί να κάνει μη αποτελεσματική χρήση του δικτύου και ο διαχειριστής μπορεί να βοηθήσει ώστε να βελτιωθεί η απόδοση.
- Ο διαχειριστής μπορεί εύκολα να σχεδιάσει την επέκταση του δικτύου.

Θα πρέπει η διαχείριση του δικτύου να μπορεί να ορίσει τις παραμέτρους που θα καταγράφονται στους διάφορους κόμβους, τα χρονικά διαστήματα στα οποία θα αποστέλλονται αυτές οι πληροφορίες σε ανώτερους κόμβους καθώς επίσης και τον αλγόριθμό που θα χρησιμοποιηθεί για την κοστολόγηση.

1.2.3 Διαχείριση Διαμόρφωσης (Configuration Management)

Τα μοντέρνα δίκτυα δεδομένων αποτελούνται από μεμονωμένα στοιχεία και λογικά υποσυστήματα που μπορούν να διαμορφωθούν για να εκτελέσουν διάφορες εφαρμογές (πχ. Η ίδια συσκευή μπορεί να διαμορφωθεί και να λειτουργήσει είτε σαν router είτε σαν τελικός κόμβος ή και τα δύο). Όταν αποφασιστεί το πώς θα χρησιμοποιηθεί μια συσκευή, η διαχείριση διαμόρφωσης μπορεί να επιλέξει το κατάλληλο λογισμικό και να ορίσει το σύνολο των χαρακτηριστικών και τις τιμές τους για τη συσκευή.

Η διαχείριση διαμόρφωσης ασχολείται με την εκκίνηση και την παύση λειτουργίας τμήματος ή ολόκληρου του δικτύου. Επίσης ασχολείται με τη συντήρηση, προσθήκη και ενημέρωση των σχέσεων ανάμεσα στα στοιχεία καθώς και την κατάσταση των στοιχείων κατά τη λειτουργία του δικτύου.

Η αναδιαμόρφωση ενός δικτύου είναι συχνά αναγκαία για τη βελτίωση της απόδοσης ενός δικτύου, την αναβάθμιση του δικτύου, την ανίχνευση λαθών ή την ασφάλεια του δικτύου.

1.2.4 Διαχείριση Απόδοσης (Performance Management)

Τα μοντέρνα δίκτυα δεδομένων αποτελούνται από πολλά και διαφορετικά στοιχεία, τα οποία πρέπει να επικοινωνούν μεταξύ τους και να μοιράζονται δεδομένα και πόρους του δικτύου. Η διαχείριση απόδοσης χωρίζεται σε δύο τομείς- την παρακολούθηση της δραστηριότητας του δικτύου και τον έλεγχο που επιτρέπει ρυθμίσεις με σκοπό τη βελτίωση της απόδοσης. Μερικά από τα θέματα που ασχολείται η διαχείριση απόδοσης είναι:

- Ποιο είναι το επίπεδο χωρητικότητας χρήσης
- Υπάρχει αυξημένη κυκλοφορία?
- Μήπως έχει πέσει ο ρυθμός απόδοσης σε μη αποδεκτά επίπεδα?
- Υπάρχει κάπου συνωστισμός
- Έχει αυξηθεί ο χρόνος απόκρισης

Για την αντιμετώπιση αυτών των θεμάτων ο διαχειριστής του δικτύου πρέπει να επικεντρώσει την προσοχή του στην παρακολούθηση κάποιων επιλεγμένων πόρων του δικτύου για να μπορέσει να εκτιμήσει την κατάσταση. Για το σκοπό αυτό είναι απαραίτητες οι στατιστικές

απόδοσης που βοηθούν στο σχεδιασμό, τη διαχείριση και τη συντήρηση μεγάλων δικτύων. Μακροχρόνια τέτοιες στατιστικές μπορούν να χρησιμοποιηθούν για το σχεδιασμό της χωρητικότητας του δικτύου φυσικά την επέκταση των γραμμών σε κάποιο τομέα.

1.2.5 Διαχείριση Ασφάλειας (Security Management)

Η διαχείριση ασφάλειας ασχολείται με τη διαχείριση πληροφοριών ασφάλειας και αυτό συνεπάγεται τη δημιουργία, διανομή και αποθήκευση κλειδιών κρυπτογράφησης. Επίσης ασχολείται με την παρακολούθηση και τον έλεγχο της πρόσβασης σε τμήματα ή και σε όλο το δίκτυο. Η πρόσβαση στο δίκτυο είναι μια πληροφορία που καταγράφεται στους διάφορους κόμβους του δικτύου. Για το σκοπό αυτό χρησιμοποιούνται ημερολόγια (logs) τα οποία είναι από τα βασιμότερα εργαλεία ελέγχου.

1.3 Πρωτόκολλα Διαχείρισης Δικτύου

Τα πρωτόκολλα διαχείρισης δικτύου καθορίζουν τον τρόπο με τον οποίο οι διαχειριστές (managers) επικοινωνούν με τους αντιπροσώπους (agents) για να γίνει η συλλογή των απαιτούμενων πληροφοριών – δεικτών της απόδοσης του δικτύου καθώς και η διαχείριση των στοιχείων δικτύου (Network Elements – δικτυακές συσκευές). Συγκεκριμένα, τα πρωτόκολλα αυτά καθορίζουν [1]:

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

Τα ποιο ευρέως χρησιμοποιούμενα πρωτόκολλα διαχείρισης δικτύου είναι [3]:

- **SNMP** (Simple Network Management Protocol): είναι το βασικό πρωτόκολλο για συλλογή παραμέτρων χωρητικότητας και χρήσης του δικτύου. Χρησιμοποιείται για την παρακολούθηση της χρήσης των δρομολογητών και μεταγωγέων (routers and switches) καθώς και για την παρακολούθηση χρήσης των παραμέτρων των συσκευών δικτύου (servers) όπως χρήση μνήμης, ποσοστό χρήση της CPU κ.α. Είναι κατάλληλο για το δίκτυο TCP/IP
- **Packet Sniffing**: Το πρωτόκολλο αυτό προσφέρει εποπτεία και παρακολούθηση όλων των πακέτων που διακινούνται στο υπο παρακολούθηση δίκτυο. Με τον τρόπο αυτό υπολογίζεται η χρήση του δικτύου (bandwidth usage)
- **NetFlow protocol**: είναι το πιο ισχυρό πρωτόκολλο για μέτρηση της χρήσης της χωρητικότητας του δικτύου (bandwidth usage). Είναι κατάλληλο για δίκτυα με ιδιαίτερα υψηλή κίνηση.
- **Remote Monitoring (RMON)**: Χρησιμοποιείται για απομακρυσμένη διαχείριση δικτύου. Με το RMON, οι διαχειριστές δικτύων μπορούν να συλλέξουν τις πληροφορίες από τα μακρινά τμήματα δικτύων.

2 ΕΡΓΑΛΕΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΕΠΟΠΤΕΙΑΣ ΔΙΚΤΥΩΝ

Στην ενότητα αυτή παρουσιάζουμε δωρεάν εργαλεία για διαχείριση και παρακολούθηση δικτύων. Τα εργαλεία αυτά χωρίζονται σε:

- εργαλεία ανοιχτού κώδικα
- εργαλεία ελεύθερης διανομής
- εμπορικά εργαλεία ελεύθερης διανομής με περιορισμένα χαρακτηριστικά ως προς την πλήρη εμπορική τους έκδοση.

Παρακάτω παρουσιάζονται εργαλεία διαχείρισης και παρακολούθησης δικτύων τα οποία ανήκουν και στις τρις προαναφερόμενες κατηγορίες. Τα πακέτα που παρουσιάζονται επιλέχθηκαν από τις πηγές [4], [5] και [6].

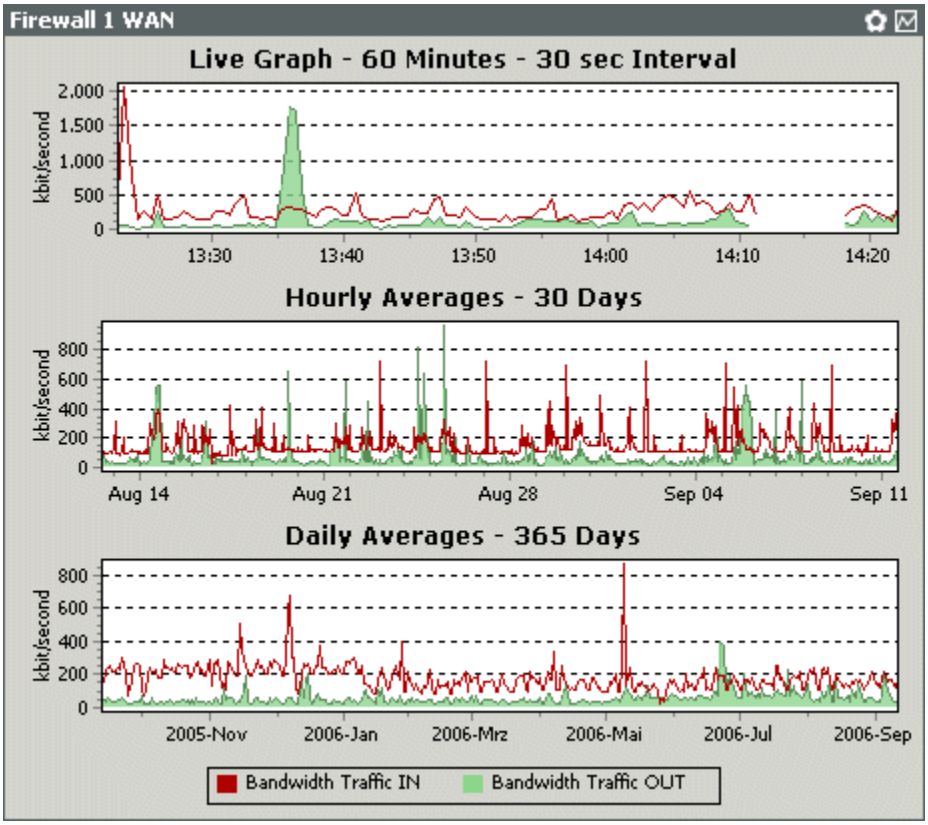
2.1 PRTG Traffic Grapher (version 6.0.5.417)

2.1.1 Παρουσίαση [7]

Είναι ένα εύχρηστο γραφικό εργαλείο, **ελεύθερης διανομής**, για παρακολούθηση δικτύου, το οποίο λειτουργεί κάτω από το λειτουργικό σύστημα Windows. Μέσω του εργαλείου αυτού οι διαχειριστές μπορούν να παρακολουθούν σε πραγματικό χρόνο και σε 24-ωρη βάση τις παραμέτρους χρήσης του δικτύου (πχ χρήση της χωρητικότητας του δικτύου - bandwidth usage) [7].

Οι παρακολουθούμενοι παράμετροι αποθηκεύονται σε βάση δεδομένων για να μπορούν να ανακτηθούν από το σύστημα με σκοπό την παραγωγή στατιστικών αποτελεσμάτων.

Το σύστημα διαθέτει δυνατότητες γραφικής απεικόνισης των αποτελεσμάτων χρήσης:



Εικόνα 1 – Ενδεικτικές Γραφικές Παραστάσεις στο PRTG

Επιπρόσθετα, το σύστημα μέσω ενός ιδιαίτερα φιλικού περιβάλλοντος, επιτρέπει τη ρύθμιση των εποπτευόμενων παραμέτρων του δικτύου, την παραγωγή γραφημάτων κατ' απαίτηση καθώς και την παραγωγή αναφορών κατ' απαίτηση.

Υποστηρίζει πολλά διαδεδομένα πρωτόκολλα για συλλογή παραμέτρων παρακολούθησης δικτύου: (SNMP, Packet Sniffing, NetFlow). Ειδικά για το Packet Sniffer και το NetFlow το πρόγραμμα υπολογίζει τη χρήση χωρητικότητας ανά IP διεύθυνση ή port και δίνει τη δυνατότητα για παραγωγή στατιστικών στοιχείων (Top Talkers, Top Connections, Top Protocols, κα) [7].

2.1.2 Αξιολόγηση

Το PRTG είναι ένα πρόγραμμα παρακολούθησης της κίνησης του δικτύου, κατάλληλο για αρχάριους διαχειριστές δικτύων, μια και είναι ιδιαίτερα απλό στη χρήση.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Γραφική αναπαράσταση αποτελεσμάτων Παρακολούθηση σε πραγματικό χρόνο Ρύθμιση εποπτευόμενων παραμέτρων Υποστήριξη πολλών πρωτοκόλλων διαχείρισης δικτύων Παραγωγή γραφημάτων και αναφορών χρήσης κατ' απαίτηση Κατάλληλο για απλούς χρήστες, ιδιαίτερα απλό στη χρήση	Διατίθεται μόνο για Windows Δεν διαθέτει δυνατότητες για ανάλυση της κίνησης (drill down) Προσφέρει λειτουργικότητες μόνο για παρακολούθηση δικτύου, δεν διαθέτει δυνατότητες για ανίχνευση σφαλμάτων Παρακολούθηση παραμέτρων μόνο για κίνηση και χρήση του δικτύου, όχι για τα χαρακτηριστικά των δικτυακών συσκευών κ.α.

2.2 MRTG - Multi Router Traffic Grapher (version 2.14.7)

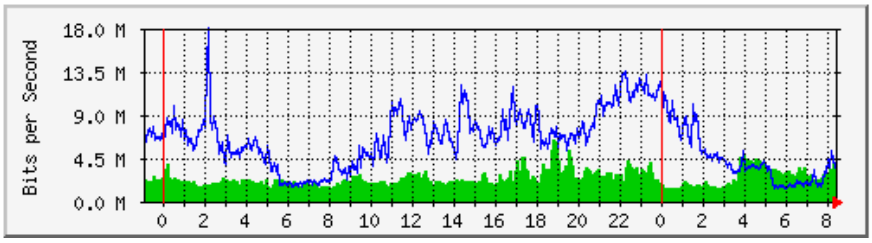
2.2.1 Παρουσίαση [8]

Είναι ένα εργαλείο ανοιχτού λογισμικού για παρακολούθηση της κίνησης των δικτύων. Διατίθεται σε εκδόσεις για Unix, Linux και Windows. Παρέχει δυνατότητα γραφικής απεικόνισης των αποτελεσμάτων χρήσης (διαγράμματα). Επίσης, παρέχει τη δυνατότητα τήρησης και ανάκτησης (γραφικής αναπαράστασης) ιστορικών στοιχείων του δικτύου για χρονικό διάστημα έως δύο ετών[8].

Αναλυτικότερα, οι υποστηριζόμενες λειτουργικότητες του προγράμματος είναι:

- Προσβάσιμο μέσω διαδικτύου
- Γραφικό περιβάλλον εργασίας
- Χρήση SNMP για συλλογή δεδομένων κίνησης δικτύου
- Γραφική απεικόνιση αποτελεσμάτων
- Εξαγωγή γραφημάτων σε html μορφή για προβολή μέσω διαδικτύου
- Παρακολούθηση κίνησης σε πραγματικό χρόνο
- Ιδιαίτερα γρήγορο; πολλές ρουτίνες απεικόνισης παραμέτρων σε γραφικές παραστάσεις είναι γραμμένες σε C
- Δυνατότητες διασύνδεσης με πολλά προγράμματα συλλογής δεδομένων, του πρωτοκόλλου SNMP.

- Δυνατότητα ενσωμάτωσης δεδομένων από διαφορετικές πηγές (διαφορετικές εφαρμογές συλλογής δεδομένων) σε ένα γράφημα [8]



Εικόνα 2 Τυπική Γραφική Παράσταση του MRTG

2.2.2 Αξιολόγηση

Το MRTG είναι ένα πρόγραμμα κατάλληλο για παρακολούθηση δικτύων σε πραγματικό χρόνο μια και διαθέτει πολύ γρήγορες ρουτίνες για γραφική απεικόνιση των παρακολουθούμενων παραμέτρων.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Υποστήριξη πολλών λειτουργικών συστημάτων Προσβάσιμο μέσω web-browser Γραφική αναπαράσταση αποτελεσμάτων Κατάλληλο για παρακολούθηση σε πραγματικό χρόνο, ιδιαίτερα γρήγορο Δυνατότητα ενσωμάτωσης δεδομένων από διαφορετικές πηγές (διαφορετικές εφαρμογές συλλογής δεδομένων) σε ένα γράφημα	Υποστήριξη μόνο του πρωτοκόλλου SNMP Διαθέτει μόνο προτυποποιημένες γραφικές παραστάσεις, δεν προσφέρει γραφικές παραστάσεις κατ' απαίτηση (οριζόμενες από τον χρήστη) Δεν διαθέτει δυνατότητες για ανάλυση της κίνησης (drill down) Προσφέρει λειτουργικότητες μόνο για παρακολούθηση δικτύου, δεν διαθέτει δυνατότητες για ανίχνευση σφαλμάτων Παρακολούθηση παραμέτρων μόνο για κίνηση και χρήση του δικτύου, όχι για τα χαρακτηριστικά των δικτυακών συσκευών κ.α. Περιορισμένες δυνατότητες γραφικής αναπαράστασης; Παραγωγή απλών μορφών γραφημάτων

2.3 VisualSniffer (version 2.0)

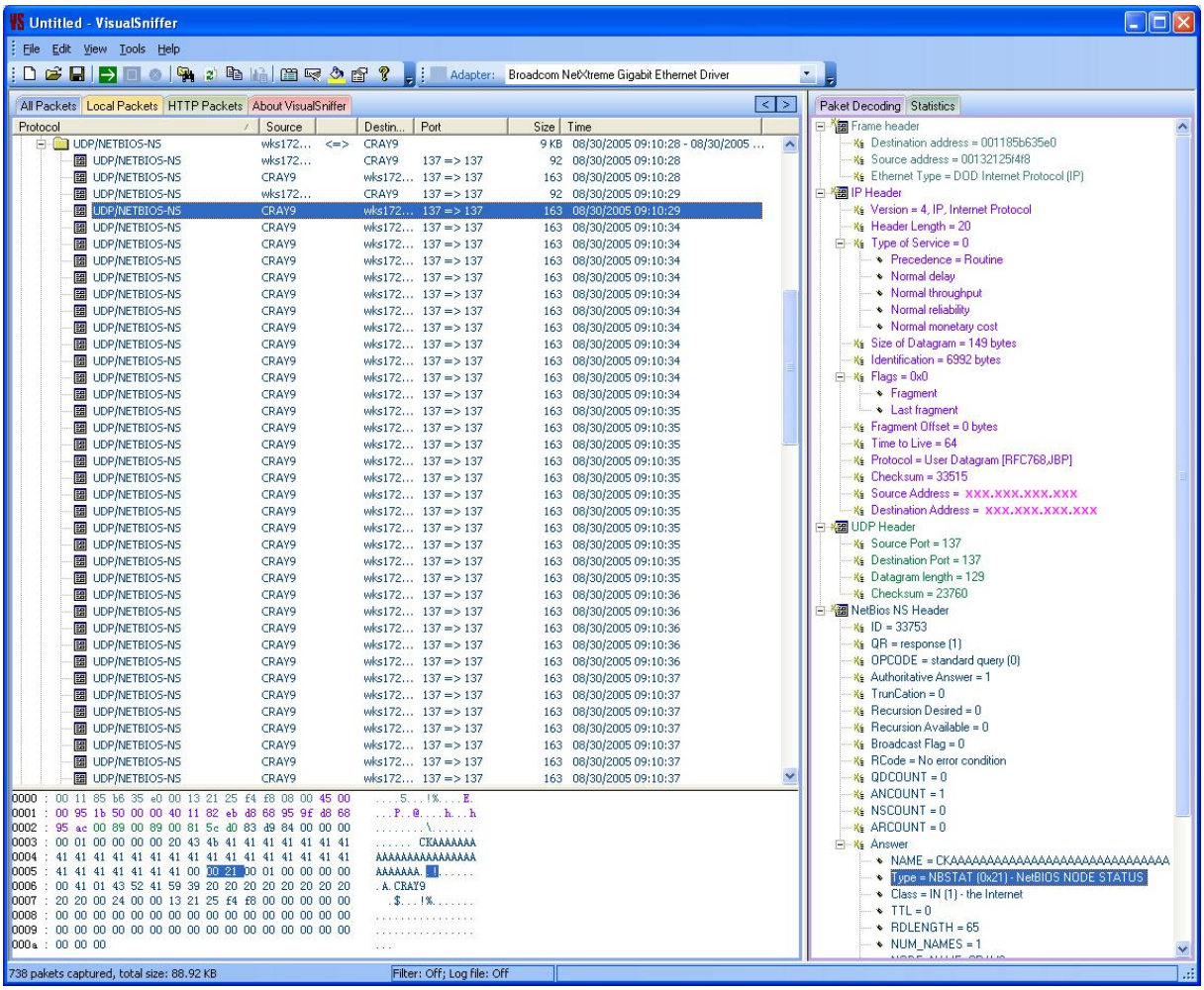
2.3.1 Παρουσίαση [9]

Είναι ένα εργαλείο ανοιχτού λογισμικού το οποίο χρησιμοποιεί τη μέθοδο packet sniffing για παρακολούθηση και διαχείριση των παραμέτρων του δικτύου. Προσφέρει στους διαχειριστές δικτύου δυνατότητα για παρακολούθηση του δικτύου, ανίχνευση εισβολών (intrusion detection) και τήρηση αρχείου για κίνηση του δικτύου (network traffic logging). Διατίθεται μόνο σε έκδοση για Windows.

Αναλυτικότερα, οι υποστηριζόμενες λειτουργικότητες του προγράμματος είναι:

- Ανάλυση της κίνησης (παρακολούθηση πακέτων)
- Παρακολούθηση της κίνησης σε πραγματικό χρόνο; η μέτρηση της κίνησης του δικτύου πραγματοποιείται βάσει της κίνησης των πακέτων

- Τήρηση των παρακολουθούμενων παραμέτρων για μελλοντική χρήση (πχ παραγωγή στατιστικών)
- Καταγραφή πακέτων σε αρχείο (log file) και ανάκτηση πακέτων από το αρχείο αυτό
- Υποστήριξη πολλών πρωτοκόλλων επικοινωνίας (ARP, DNS, EGP, GGP, GRE, ICMP, IGMP, IGRP, IPv4, IPv6, NetBIOS, PIM, RDP, RSVP, SNAP, SNMP, TCP, UDP)
- Αναζήτηση πακέτων βάσει διαφόρων κριτηρίων αναζήτησης (IP διεύθυνσης, πρωτοκόλλου επικοινωνίας, περιεχομένου, μεγέθους κτλ)
- Ρύθμιση κανόνων για την παρακολούθηση πακέτων (πχ βάσει IP διεύθυνσης, πρωτοκόλλου επικοινωνίας, περιεχομένου, μεγέθους του πακέτου, χρόνου μετάδοσης κα)
- Παραγωγή γραφημάτων και στατιστικών πινάκων
- Παραγωγή γραφημάτων και στατιστικών κατ' απαίτηση, βασισμένων σε παραμέτρους που επιλέγει ο χρήστης (IP διεύθυνσης, πρωτοκόλλου επικοινωνίας, περιεχομένου, μεγέθους κτλ)
- Προγραμματισμός εργασιών παρακολούθησης (ρύθμιση χρονικού διαστήματος κτλ)



Εικόνα 3 Περιβάλλον Εργασίας του Visual Sniffer(Παρακολούθηση Πακέτων)

2.3.2 Αξιολόγηση

Το VisualSniffer είναι ένα πρόγραμμα κατάλληλο για ανάλυση της κίνησης του δικτύου μια και προσφέρει μεγάλο βαθμό ανάλυσης (drill-down) της κίνησης (παρακολούθηση μεταδιδόμενων πακέτων).

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Γραφική αναπαράσταση αποτελεσμάτων Ρύθμιση εποπτευόμενων παραμέτρων Παραγωγή γραφημάτων κατ' απαίτηση χρονοπρογραμματισμός εργασιών Ανάλυση κίνησης (λόγω παρακολούθησης των πακέτων), δυνατότητες drill down Υποστήριξη πολλών πρωτοκόλλων επικοινωνίας	Διατίθεται μόνο για Windows Υποστήριξη μόνο του packet sniffing και όχι άλλων πρωτοκόλλων συλλογής δεδομένων Προσφέρει λειτουργικότητες μόνο για παρακολούθηση δικτύου, δεν διαθέτει δυνατότητες για ανίχνευση σφαλμάτων Παρακολούθηση παραμέτρων μόνο για κίνηση και χρήση του δικτύου, όχι για τα χαρακτηριστικά των δικτυακών συσκευών κτλ Περιορισμένες δυνατότητες γραφικής αναπαράστασης; Παραγωγή απλών μορφών γραφημάτων

2.4 OpManager (Free Edition, version 5.5)

2.4.1 Παρουσίαση [10]

Πρόκειται για εμπορικό πακέτο, το οποίο προσφέρεται σε ελεύθερη διανομή με περιορισμένα χαρακτηριστικά σε σχέση με το πλήρες εμπορικό πακέτο (παρακολούθηση και διαχείριση 20 δικτυακών συσκευών το πολύ). Προσφέρεται σε εκδόσεις για Windows, Linux και Solaris.

Ο OpManager είναι ένα ολοκληρωμένο πακέτο διαχείρισης και παρακολούθησης δικτύου για τοπικά και ευρείας περιοχής δίκτυα (LANs, WANs). Υποστηρίζει την καταγραφή γεγονότων σε αρχείο (Log).

Το πρόγραμμα προσφέρει μια ολοκληρωμένη πλατφόρμα διαχείρισης συσκευών δικτύου, εφαρμογών, σφαλμάτων και απόδοσης. Το πρόγραμμα ανιχνεύει αυτόματα τις δικτυακές συσκευές και παρουσιάζει μια ολοκληρωμένη όψη του δικτύου στην κονσόλα διαχείρισης. Διαθέτει τη δυνατότητα αυτόματης ειδοποίησης των διαχειριστών (με email) σε περίπτωση ανίχνευσης σφαλμάτων.

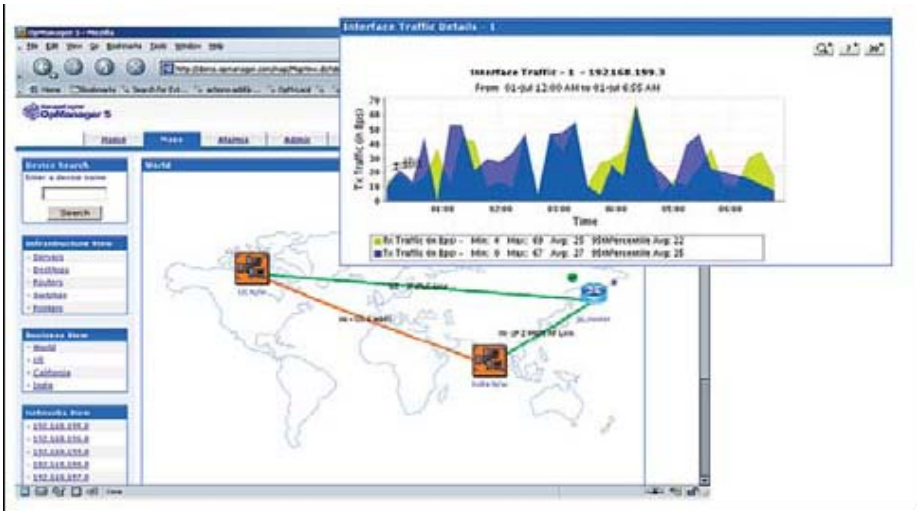
Η εποπτεία δικτύου βασίζεται στο πρωτόκολλο SNMP και ο χρήστης μπορεί να παραμετροποιήσει κατάλληλα το γραφικό περιβάλλον παρακολούθησης και διαχείρισης των δικτυακών συσκευών (routers) ώστε να μπορεί να παρακολουθεί/διαχείρίζεται οποιαδήποτε SNMP παράμετρο. Επιπρόσθετα, υποστηρίζει το πρωτόκολλο NetFlow για παραγωγή αναφορών και αποτελεσμάτων σχετικά με τη χρήση του δικτύου.

Επιπρόσθετα, προσφέρει δυνατότητες παραγωγής γραφικών αναπαραστάσεων και αναφορών κατ' απαίτηση για τις παρακολουθούμενες παραμέτρους. Προσφέρει δυνατότητες παρακολούθησης σε πραγματικό χρόνο καθώς και παραγωγής στατιστικών αποτελεσμάτων (κρατά ιστορικό των παραμέτρων).

Αναλυτικότερα, οι προσφερόμενες λειτουργικότητες είναι:

Εποπτεία Δικτύου:

- Παρακολούθηση των παραμέτρων του δικτύου σε πραγματικό χρόνο
- Γραφική απεικόνιση των αποτελεσμάτων
- Ανίχνευση διαθεσιμότητας των δικτυακών συσκευών
- Παρακολούθηση δικτυακών εφαρμογών
- Παραγωγή ειδοποιήσεων σε περιπτώσεις σφάλματος
- Στατιστικά διαθεσιμότητας των δικτυακών συσκευών
- Στατιστικά κίνησης και χρήσης του δικτύου
- Στατιστικά χρόνων απόκρισης των δικτυακών συσκευών / εφαρμογών
- Στατιστικά λαθών
- Ρύθμιση και παρακολούθηση παραμέτρων των δικτυακών συσκευών / εφαρμογών
- Υποστήριξη του NetFlow για παραγωγή αναφορών και αποτελεσμάτων σχετικά με την κίνηση δικτύου
- Υποστήριξη πολλών πρωτοκόλλων επικοινωνίας
- Υποστηρίζει πολλές τοπολογίες δικτύων (LANs, WANs)



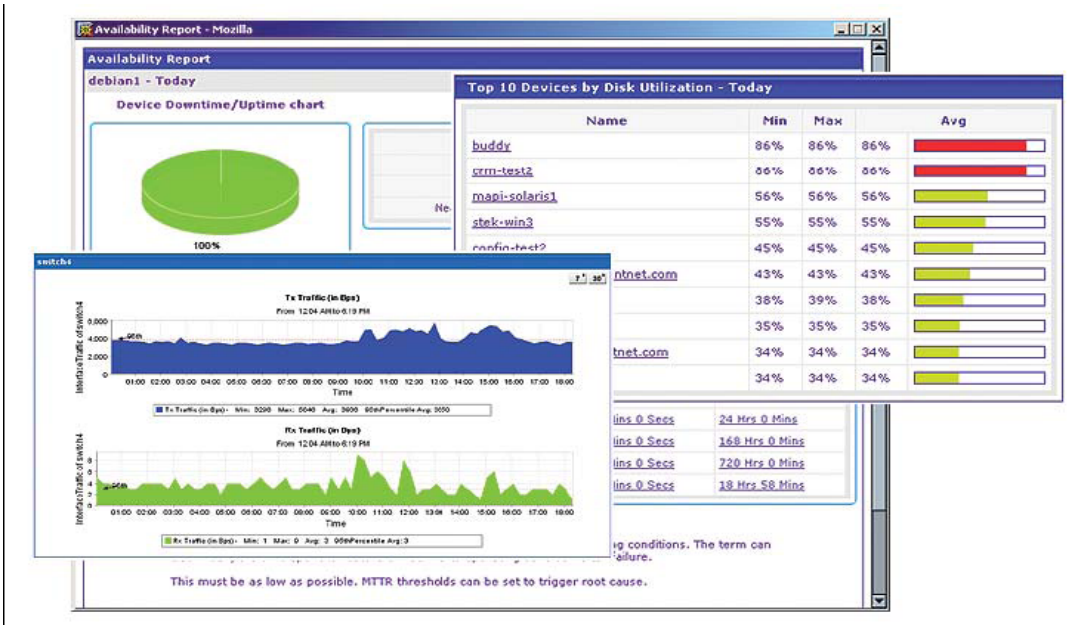
Εικόνα 4 Περιβάλλον Εργασίας του OpManager

Διαχείριση Δικτυακών Συσκευών:

- Δυνατότητα παρακολούθησης πολλαπλών παραμέτρων απόδοσης των εξυπηρετητών (χρήση CPU, μνήμης, δίσκων)
- Διαχείριση και παρακολούθηση εφαρμογών των εξυπηρετητών (Application Management)
- Διαχείριση μεταγωγέων και των θυρών αυτών
- Διαχείριση δικτυακών εκτυπωτών
- Ανίχνευση προβλημάτων στις συσκευές και αυτόματη ειδοποίηση του διαχειριστή
- Ανίχνευση διαθεσιμότητας των συσκευών

Διαχείριση Σφαλμάτων:

- Αυτόματες ειδοποιήσεις σε περιπτώσεις ανίχνευσης σφαλμάτων
- Παρουσίαση σφαλμάτων με γραφικό τρόπο (χρωματικές κωδικοποιήσεις κατηγοριών, ιεραρχική κατηγοριοποίηση)
- Αυτόματη εκτέλεση scripts σε περίπτωση ανίχνευσης συγκεκριμένων σφαλμάτων



Εικόνα 5 Παραγωγή Στατιστικών στο OpManager

Διαχείριση Απόδοσης:

- Παραγωγή προτυποποιημένων γραφημάτων και αναφορών
- Παραγωγή αναφορών και γραφημάτων κατ' απαίτηση
- Παρακολούθηση παραμέτρων δικτύου (κίνηση, χρήση, σφάλματα)
- Παρακολούθηση παραμέτρων δικτυακών συσκευών (CPU, Memory and Disk)
- Παρακολούθηση διαθεσιμότητας και χρόνων απόκρισης
- Προγραμματισμός παραγωγής αναφορών (ημερήσια, εβδομαδιαία, μηνιαία βάση ή ορισόμενη από το χρήστη)
- Εξαγωγή αναφορών σε HTML, PDF, CSV formats

2.4.2 Αξιολόγηση

Το OpManager είναι μια ολοκληρωμένη πλατφόρμα διαχείρισης και εποπτείας δικτύου και μπορεί να χρησιμοποιηθεί για ολοκληρωμένη διαχείριση δικτύου, μια και καλύπτει όλα τα χαρακτηριστικά ενός συστήματος διαχείρισης, έτσι όπως αναφέρονται στην παράγραφο 1.2 – Απαιτήσεις από το σύστημα διαχείρισης.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Ολοκληρωμένη πλατφόρμα διαχείρισης και εποπτείας δικτύου Υποστηρίζει Windows, Linux και Solaris Παρακολούθηση σε πραγματικό χρόνο; Ρύθμιση παρακολουθούμενων παραμέτρων Διαχείριση και παρακολούθηση δικτυακών συσκευών/εφαρμογών Διαχείριση σφαλμάτων; Ειδοποίηση διαχειριστών; Αυτόματη εκτέλεση scripts	Η ελεύθερη έκδοση υποστηρίζει μέχρι 20 δικτυακές συσκευές Δεν διαθέτει δυνατότητες για ανάλυση της κίνησης (drill down) Υποστηρίζει μόνο SNMP και NetFlow

Γραφική αναπαράσταση αποτελεσμάτων , παραγωγή γραφημάτων και αναφορών κατ' απαίτηση Χρονοπρογραμματισμός εργασιών Υποστήριξη πολλών πρωτοκόλλων επικοινωνίας Παρακολούθηση σε πραγματικό χρόνο Υποστηρίζει πολλές τοπολογίες δικτύων Υποστηρίζει πάνω από ένα πρωτόκολλο διαχείρισης (SNMP και NetFlow)	

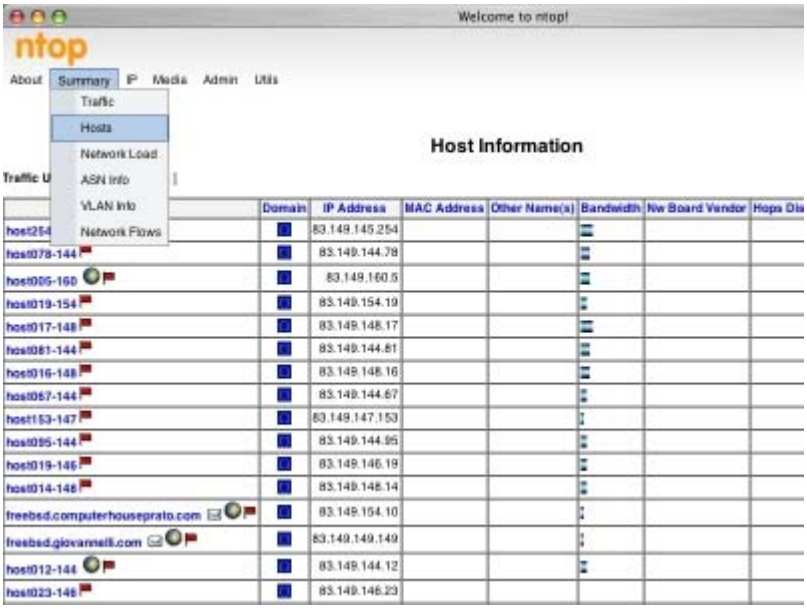
2.5 NTop (version 3.2)

2.5.1 Παρουσίαση [11]

Είναι ένα εργαλείο ανοιχτού λογισμικού, για παρακολούθηση δικτύων το οποίο προσφέρεται σε εκδόσεις για Windows, Linux, BSD, Solaris, and MacOSX.

Το NTop είναι και προσβάσιμο μέσω web browser χωρίς να απαιτείται εγκατάσταση του προγράμματος. Η δικτυακή όμως έκδοση της εφαρμογής παρέχει περιορισμένες λειτουργικότητες.

Αναλυτικότερα, υποστηρίζονται οι ακόλουθες λειτουργικότητες:

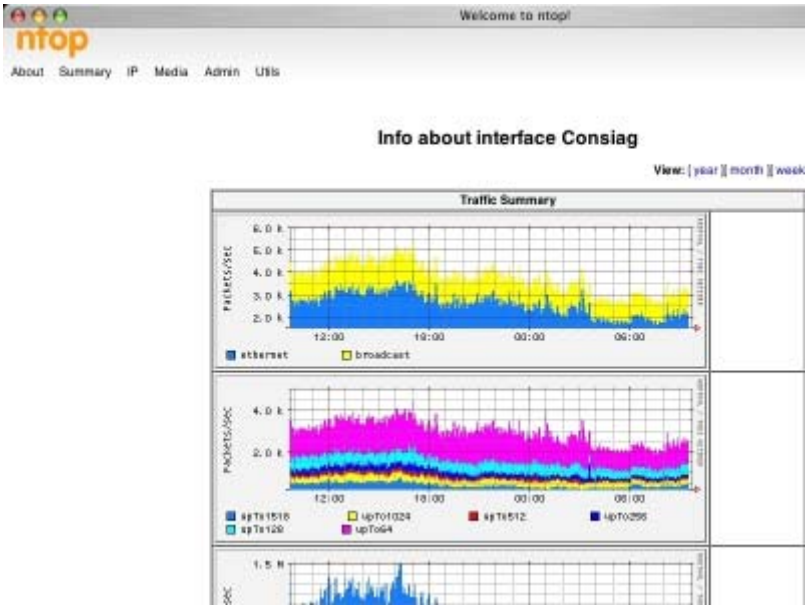


Εικόνα 6 Περιβάλλον Εργασίας του Ntop

Παρακολούθηση δικτύου

- Γραφική απεικόνιση εποπτευόμενων παραμέτρων
- Παρακολούθηση εποπτευόμενων παραμέτρων σε πραγματικό χρόνο
- Παρακολούθηση της κίνησης του δικτύου
- Παρακολούθηση κατανομής της κίνησης του δικτύου
- Η ταξινόμηση της κίνησης του δικτύου σύμφωνα με διάφορα κριτήρια

- Η ανάλυση της IP κυκλοφορίας σύμφωνα με πηγή-παραλήπτη
- Παρακολούθηση διαθεσιμότητας δικτυακών συσκευών
- Παραγωγή στατιστικών αποτελεσμάτων
- Τήρηση εποπτευόμενων παραμέτρων σε βάση δεδομένων για μελλοντική χρήση
- Υποστήριξη NetFlow για εξελιγμένα στατιστικά κίνησης του δικτύου
- Υποστήριξη RMON



Εικόνα 7 Γραφικές Παραστάσεις στο NTop

Ανίχνευση προβλημάτων διαμόρφωσης δικτυακών συσκευών

- Διπλοκαταχώρηση IP διευθύνσεων
- Ανίχνευση Κατάχρησης υπηρεσιών:hosts που δεν χρησιμοποιούν τους προκαθορισμένους proxies
- Ανίχνευση Κατάχρησης Πρωτοκόλλων: hosts που δεν χρησιμοποιούν προκαθορισμένα πρωτόκολλα
- Ανίχνευση λανθασμένων δρομολογητών: σταθμοί εργασίας που λειτουργούν ως δρομολογητές
- Ανίχνευση περιπτώσεων κατάχρησης της χωρητικότητας του δικτύου
- Ανίχνευση λανθασμένης διαμόρφωσης εφαρμογών των εξυπηρετητών

Βελτιστοποίηση Σχεδιασμού Δικτύου

Μέσω των εκτεταμένων δυνατοτήτων παρακολούθησης των παραμέτρων του δικτύου (απόδοση, κίνηση, χρήση χωρητικότητας, κατανομή κίνησης), ο διαχειριστής έχει τη δυνατότητα να διαχειριστεί με το βέλτιστο τρόπο τις δικτυακές συσκευές και να σχεδιάσει έτσι το δίκτυο με βέλτιστο τρόπο.

Διαχείριση Ασφαλείας Δικτύου

Η εφαρμογή παρέχει δυνατότητες ανίχνευσης επιθέσεων (πχ trojan horses, portscan επιθέσεις, επιθέσεις άρνησης εξυπηρέτησης, IP spoofing, promiscuous στοιχεία δικτύου). Σε περιπτώσεις παραβιάσεων το σύστημα παρέχει μηχανισμό αυτόματης ειδοποίησης των

διαχειριστών (mail, SNMP traps ή Short Messaging Systems). Επίσης, παρέχει δυνατότητα αυτόματη; εκτέλεση scripts σε περίπτωση ανίχνευσης συγκεκριμένων σφαλμάτων.

2.5.2 Αξιολόγηση

Το NTop είναι ένα πρόγραμμα κατάλληλο για παρακολούθηση και διαχείριση της ασφάλειας των δικτύων, μια και προσφέρει δυνατότητες για ανίχνευση πολλών κατηγοριών σφαλμάτων και επιθέσεων.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

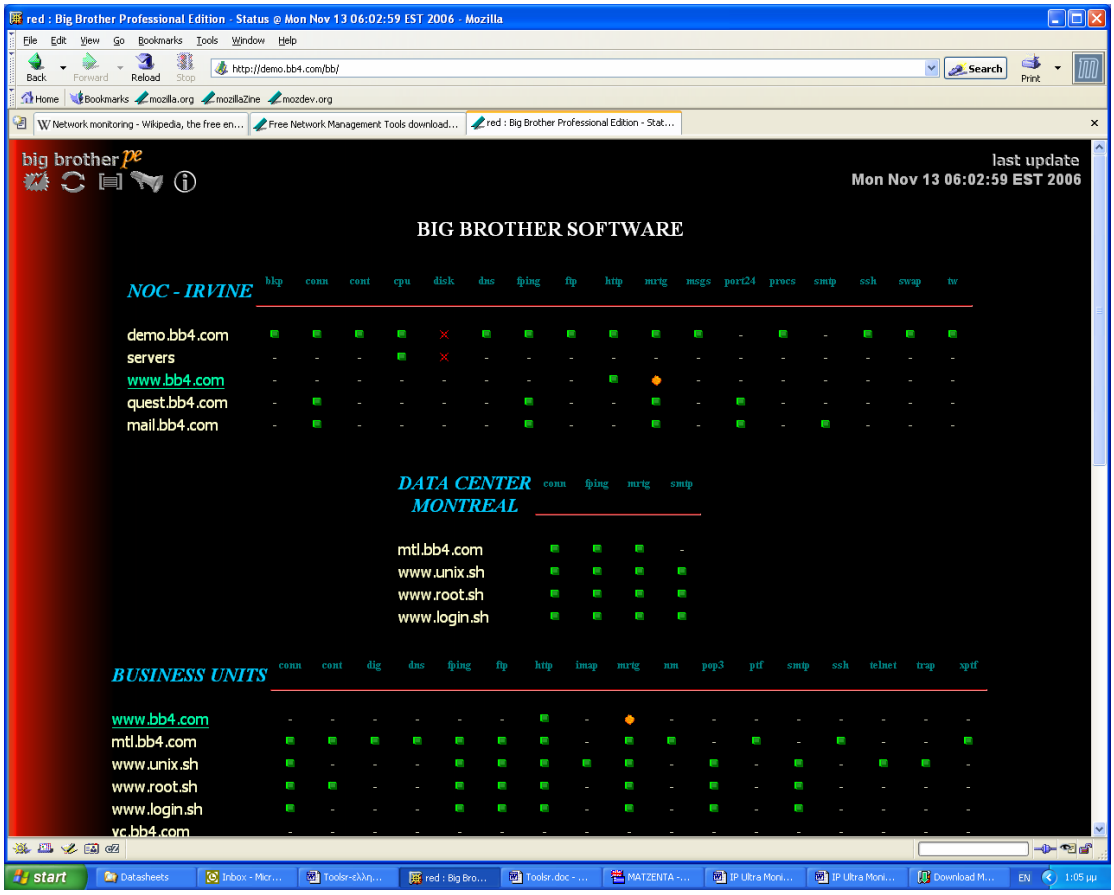
ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Εποπτεία της ασφάλειας του δικτύου Υποστηρίζει μεγάλο αριθμό λειτουργικών συστημάτων Διαχείριση διαμόρφωσης δικτυακών συσκευών Διαχείριση σφαλμάτων; Ειδοποίηση διαχειριστών; Αυτόματη εκτέλεση scripts Γραφική αναπαράσταση αποτελεσμάτων Υποστήριξη SNMP και NetFlow, RMON Πρόσβαση μέσω διαδικτύου	Διαθέτει μόνο προτυποποιημένες γραφικές παραστάσεις, δεν προσφέρει γραφικές παραστάσεις κατ' απαίτηση (οριζόμενες από τον χρήστη) Δεν παράγει αναφορές χρήσης Δεν διαθέτει δυνατότητες για ανάλυση της κίνησης (drill down)

2.6 Big Brother (personal edition, version 3.1)

2.6.1 Παρουσίαση [12]

Το Big Brother είναι ένα πρόγραμμα ανίχνευσης και παρακολούθησης δικτυακών συσκευών και εφαρμογών διαδικτύου. Αποτελεί ελεύθερη διανομή του εμπορικού λογισμικού Big Brother Professional Edition και προσφέρεται ελεύθερα για μη εμπορική χρήση. Προσφέρεται σε εκδόσεις για Unix, Linux,, Windows. Στηρίζεται στο πρωτόκολλο SNMP και παρέχει τις ακόλουθες λειτουργικότητες:

- Γραφικό περιβάλλον εργασίας
- Πρόσβαση μέσω διαδικτύου
- Παρακολούθηση σε πραγματικό χρόνο
- Παρακολούθηση δικτυακών συσκευών.
- Παρακολούθηση δικτυακών εφαρμογών.
- Γραφική απεικόνηση της κατάστασης των παρακολουθούμενων δικτυακών στοιχείων; Χρωματικές κωδικοποιήσεις.
- Τήρηση ιστορικών στοιχείων. Ο διαχειριστής μπορεί να έχει πρόσβαση στα ιστορικά στοιχεία
- Ανίχνευση Σφαλμάτων.Όταν κάποιο πρόβλημα ανιχνευθεί, ο διαχειριστής ειδοποιείται αμέσως με ηλεκτρονικό ταχυδρομείο, μπίπερ, ή μήνυμα SMS.
- Διασυνδεσιμότητα με άλλες εφαρμογές για διαχείριση σφαλμάτων (με την εφαρμογή Spotlight της ίδιας εταιρίας)



Εικόνα 8 Περιβάλλον Εργασίας του Big Brother

2.6.2 Αξιολόγηση

Το Big Brother είναι ένα πρόγραμμα κατάλληλο για παρακολούθηση δικτυακών συσκευών και δικτυακών εφαρμογών σε πραγματικό χρόνο.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

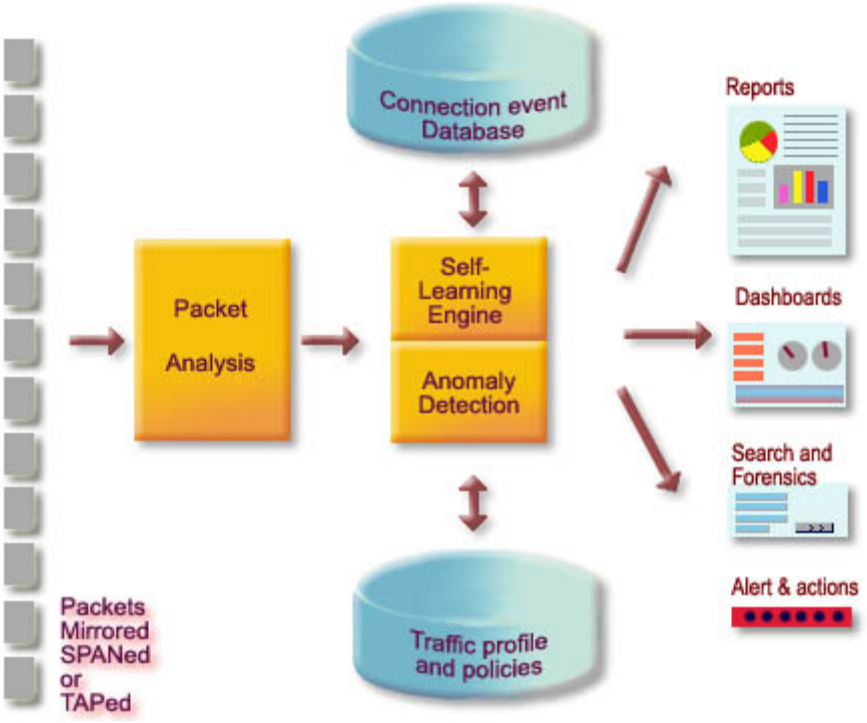
ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
24 ωρη και σε πραγματικό χρόνο παρακολούθηση συσκευών/εφαρμογών Φιλικό περιβάλλον εργασίας Προσβάσιμο μέσω διαδικτύου Ανίχνευση σφαλμάτων	Περιορισμένες λειτουργικότητες: δεν διαθέτει ενσωματωμένο module για διαχείριση σφαλμάτων. Υπάρχει όμως η δυνατότητα για διασύνδεση με εφαρμογές διαχείρισης. Περιορισμένες λειτουργικότητες: δεν διαθέτει module για παρακολούθηση κίνησης του δικτύου. Δεν παράγει στατιστικά στοιχεία. Δεν παράγει γραφήματα

2.7 nLive Core (free edition, version 2.4)

2.7.1 Παρουσίαση [13]

Πρόκειται για εμπορικό πακέτο, το οποίο προσφέρεται σε ελεύθερη διανομή με περιορισμένα χαρακτηριστικά (παρακολούθηση έως 360 γεγονότων/ λεπτό, τήρηση ιστορικών στοιχείων έως επτά μέρες). Διατίθεται μόνο σε έκδοση για Linux.

Το nLive Core παρακολουθεί την κίνηση του δικτύου και χρησιμοποιώντας αλγόριθμους μάθησης, μαθαίνει τις πολιτικές και τις συμπεριφορές του δικτύου κάτω από πολλές καταστάσεις. Με συνεχή σύγκριση της κίνησης του δικτύου μια δεδομένη στιγμή με τα αποθηκευμένα πρότυπα κίνησης, η εφαρμογή ανιχνεύει σφάλματα και παραβιάσεις του δικτύου.



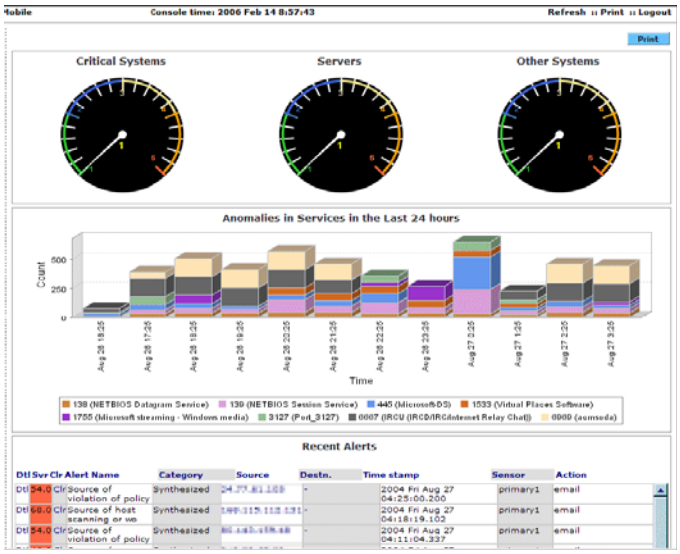
Εικόνα 9 Αρχιτεκτονική του nLive Core

Αναλυτικότερα, υποστηρίζονται οι ακόλουθες λειτουργικότητες:

Παρακολούθηση κίνησης δικτύου:

- Παρακολούθηση κίνησης σε πραγματικό χρόνο, 24χ7
- Δυνατότητα γραφικής απεικόνησης των αποτελεσμάτων (με χρήση γραφημάτων)
- Δυνατότητα παραμετροποίησης των παραγόμενων γραφημάτων
- Παρακολούθηση χρήσης του δικτύου (%χρήσης της χωριτικότητας, ρυθμοί μετάδοσης)
- Τήρηση ιστορικών στοιχείων
- Παραγωγή στατιστικών
- Παραγωγή αναφορών, προτυποποιημένων και κατ' απίτηση, δυνατότητες χρονοπρογραμματισμού παραγωγής αναφορών
- Δυνατότητες drill-down

- Παρακολούθηση και Ανίχνευση σφαλμάτων δικτυακών συσκευών (διαθεσιμότητα συσκευών, παρακολούθηση παραμέτρων δικτυακών συσκευών)
- Ανίχνευση αλλαγών στη συμπεριφορά των δικτυακών συσκευών
- Ανίχνευση ασυνήθιστης κίνησης δικτύου
- Ανίχνευση με εξουσιοδοτημένων προσπαθειών πρόσβασης στο δίκτυο: η εφαρμογή ανιχνεύει και καταγράφει προσπάθειες πρόσβασης σε πόρους του δικτύου (συσκευές, εφαρμογές, δεδομένα)



Εικόνα 10 Στατιστικά στο nLive Core

Διαχείριση Ασφάλειας

- Προστασία έναντι άγνωστων απειλών: βάσει των προτύπων συμπεριφοράς δικτύου, η εφαρμογή έχει τη δυνατότητα ανίχνευσης άγνωστων απειλών, συμπεριλαμβανόμενων zombie machines, botnets, trojans, spyware, keyloggers, probers, scans and distributed attacks.
- Η εφαρμογή παρέχει δυνατότητα αυτόματης εκτέλεση ορισμένων από το διαχειριστή ενεργειών σε περίπτωση ανίχνευσης συγκεκριμένων προτύπων συμπεριφοράς δικτύου.
- Παρέχει μηχανισμό αυτόματης ειδοποίησης των διαχειριστών σε περιπτώσεις ανίχνευσης μη αποδεκτών προτύπων συμπεριφοράς του δικτύου.
- Η ανίχνευση των σφαλμάτων γίνεται σε πραγματικό χρόνο και αυτόματα ειδοποιούνται οι διαχειριστές του συστήματος. Έτσι δίνεται η δυνατότητα μπλοκαρίσματος του σφάλματος, ώστε να μην εξαπλωθεί σε όλο το δίκτυο/

2.7.2 Αξιολόγηση

Το nLive Core είναι ένα πρόγραμμα κατάλληλο για παρακολούθηση και διαχείριση ασφάλειας δικτύων.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Πολύ ισχυρό εργαλείο διαχείρισης ασφάλειας Διαχείριση σφαλμάτων; Ειδοποίηση διαχειριστών; Αυτόματη εκτέλεση scripts Γρήγορη απόκριση σε περίπτωσεις	Περιορισμένη τηρηση ιστορικών στοιχείων (7 ημέρες) Διατίθεται μόνο έκδοση για Linux

σφαλμάτων Εξελιγμένη τεχνική παρακολούθησης δικτύου (πρότυπα συμπεριφοράς), αλγόριθμους μάθησης Χρονοπρογραμματισμός εργασιών 24 ωρη και σε πραγματικό χρόνο παρακολούθηση δικτύου Ευχρηστο περιβάλλον εργασίας Πολύ ισχυρό εργαλείο παραγωγής στατιστικών	

2.8 NCS Z-tools.he Suite (version 2.1)

2.8.1 Παρουσίαση [14]

Είναι μια σουίτα εργαλείων ελεύθερης διανομής για διαχείριση και παρακολούθηση δικτύου. Προσφέρεται μόνο σε έκδοση για Windows. Περιλαμβάνει τα ακόλουθα εργαλεία:

- NetClickLE
- AccountView
- ACLView
- ServiceView
- WhoIsConnected

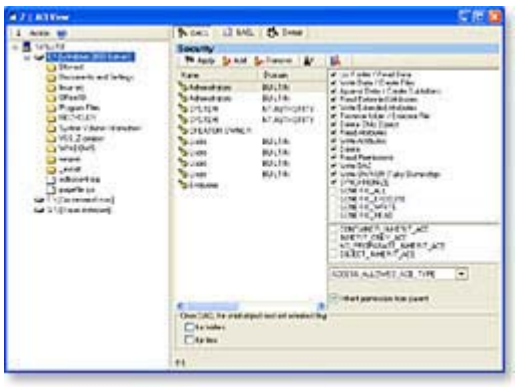
Αναλυτικότερα, υποστηρίζονται οι ακόλουθες λειτουργικότητες:

Διαχείριση Δικτύου(εργαλείο NetClickLE)

- Πλήρης διαχείριση διαδικασιών του συστήματος (process)
- Παρακολούθηση και καταγραφή (audit) προσπαθειών πρόσβασης στο σύστημα. Εξαγωγή αρχείου σε XML format
- Διαχείριση και παρακολούθηση παραμέτρων δικτυακών πόρων και δικτυακών συσκευών
- Διαχείριση χρηστών και δικαιωμάτων πρόσβασης στο δίκτυο και σε επιμέρους στοιχεία του δικτύου
- Παρακολούθηση χρήσης δικτυακών πόρων
- Διαχείριση απομακρυσμένων πόρων
- Παρακολούθηση σε πραγματικό χρόνο

Διαχείριση λίστας πρόσβασης (εργαλείο ACLView)

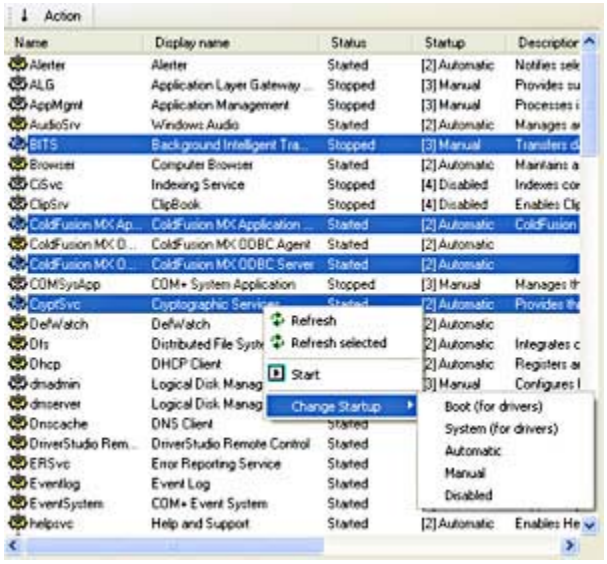
Η εφαρμογή αυτή παρέχει λειτουργικότητες διαχείρισης της λίστας πρόσβασης στο δίκτυο και σε επιμέρους στοιχεία του δικτύου. Αναλυτικότερα, ο διαχειριστής μπορεί να ορίσει ποιος χρήστης έχει πρόσβαση σε ποιους πόρους, καθώς και τα δικαιώματα πρόσβασης αυτού.



Εικόνα 11 Περιβάλλον εργασίας του ACLView

Διαχείριση Υπηρεσιών και Δικτυακών Συσκευών (εργαλείο ServiceView)

Παρέχεται παρακολούθηση και διαχείριση των δικτυακών υπηρεσιών και των δικτυακών συσκευών



Εικόνα 12 Περιβάλλον εργασίας του ServiceView

Διαχείριση και Παρακολούθηση Δικτυακών Συνδέσεων (εργαλείο Who Is Connected)

- Παρακολούθηση δικτυακών συνδέσεων
- Παρακολούθηση χρήσης των πόρων του δικτύου
- Δυνατότητα απαγόρευσης συνδέσεων σε πόρους του δικτύου
- Δυνατότητα κατάργησης συνδέσεων
- Παρακολούθηση IP ports

Διαχείριση Λογαριασμών(εργαλείο AccountView)

- Παρέχεται εργαλείο διαχείρισης των λογαριασμών των χρηστών του δικτύου

2.8.2 Αξιολόγηση

Η σουίτα NCS Z-tools.he είναι κατάλληλη για παρακολούθηση τοπικών δικτύων και προσφέρεται για αρχάριους διαχειριστές δικτύων.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Πλήρες πακέτο παρακολούθησης και διαχείρισης των δικτυακών συσκευών και εφαρμογών, καθώς και χρηστών Ιδιαίτερα φιλικό περιβάλλον εργασίας, κατάλληλο για αρχάριους διαχειριστές Παρακολούθηση σε πραγματικό χρόνο	Διατίθεται μόνο σε έκδοση για Windows Κατάλληλο μόνο για LANs Πολύ περιορισμένες δυνατότητες παρακολούθησης χρήσης του δικτύου Δεν παράγει στατιστικά χρήσης

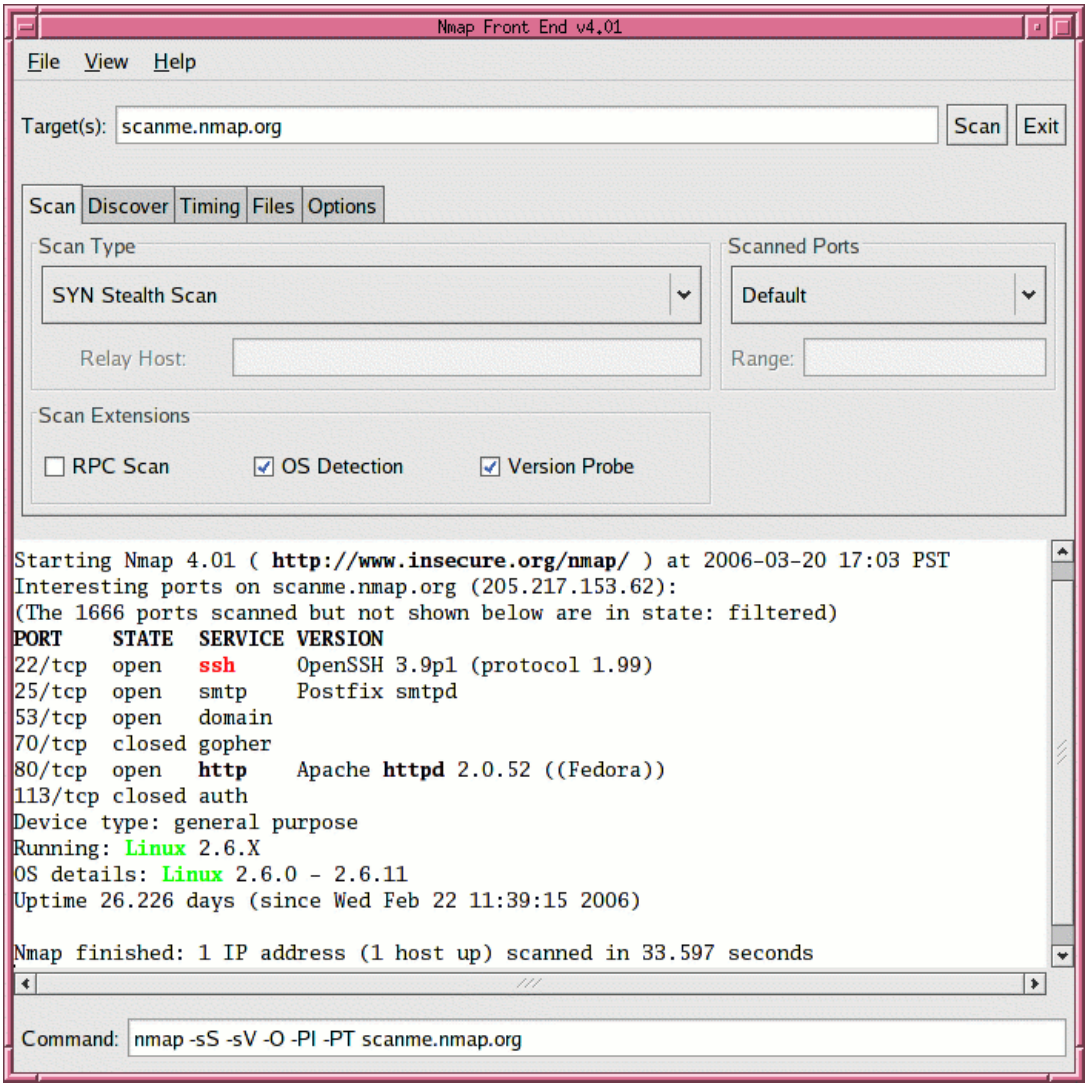
2.9 NMAP (version 4.20)

2.9.1 Παρουσίαση [15]

Το Nmap είναι ένα εργαλείο ανοιχτού λογισμικού το οποίο προσφέρεται σε εκδόσεις για Linux, Solaris Mac OS X,, AmigaOS. και Windows. Είναι κατάλληλο μεγάλα δίκτυα και χρησιμοποιείται κυρίως για διαχείριση ασφάλειας των δικτύων.

Αναλυτικότερα, η εφαρμογή διαθέτει τις ακόλουθες λειτουργικότητες:

- Προσδιορισμός των ενεργών συνδέσεων κάθε δικτυακής συσκευής (Host Discovery)
- Σκανάρισμα Θυρών (port scanning): Προσδιορισμός των ανοιχτών θυρών των δικτυακών συσκευών
- Έλεγχος δικτυακών συσκευών (firewalls, servers and workstations) για ευάλωτες TCP/IP θύρες.
- Εργαλείο ανίχνευσης λειτουργικών συστημάτων των δικτυακών συσκευών (OS Detection)
- Ping sweep, εργαλείο ανίχνευσης για το εάν ένα firewall μπλοκάρει pings
- Υποστήριξη απεριορίστου αριθμού δικτυακών συσκευών; Σταθερό για μεγάλα δίκτυα
- Υποστήριξη διαχείρισης απομακρυσμένων δικτυακών συσκευών
- Ανιχνευση ευάλωτων δικτυακών συσκευών



Εικόνα 13 Περιβάλλον εργασίας του NMAP

2.9.2 Αξιολόγηση

Το NMAP είναι ένα πρόγραμμα κατάλληλο για εποπτεία της ασφάλειας μεγάλων δικτύων.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Υποστήριξη μεγάλων δικτύων	Όχι και τόσο φιλικό περιβάλλον εργασίας
Υποστήριξη πολλών λειτουργικών συστημάτων	Δεν παράγει στατιστικά
Ισχυρά εργαλεία παρακολούθησης ασφάλειας; Εύκολη ανίχνευση ευάλωτων συσκευών; Προσδιορισμός ευάλωτων συνδέσεων	Δεν διαθέτει ενσωματωμένα modules για διαχείριση ασφάλειας

2.10 Ethereal (version 0.99)

2.10.1 Παρουσίαση [16]

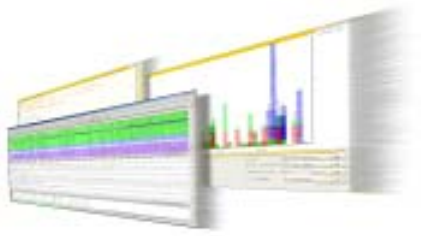
Το Ethereal είναι ένα εργαλείο ανοιχτού λογισμικού και προσφέρεται σε εκδόσεις για Unix Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X and Windows.

Είναι εργαλείο διαχείρισης και παρακολούθησης δικτύου. Μέσω του εργαλείου αυτού οι διαχειριστές μπορούν να παρακολουθούν την κίνηση του δικτύου συνολικά αλλά και σε μεγάλο βάθος ανάλυσης (ανά δικτυακή συσκευή κτλ).

Βασίζεται στο πολύ ισχυρό εργαλείο tcpdump (πολύ διαδεδομένο console-based εργαλείο για διαχείριση και παρακολούθηση δικτύου), αλλά παρέχει γραφικό περιβάλλον, καθώς και πολλές δυνατότητες οπτικοποίησης και ταξινόμησης των αποτελεσμάτων χρήσης.

Επίσης, υποστηρίζει πολλά προτόκολλα δικτύων (Ethernet, internet, ATM κτλ) καθώς και πολλά προτόκολλα επικοινωνίας (ftp. tcp/ip κτλ)

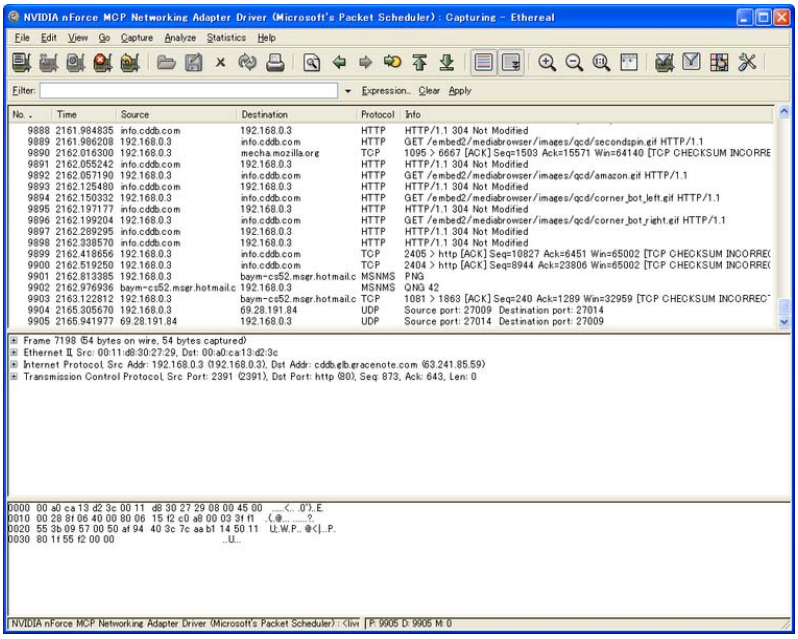
Χρησιμοποιεί τη μέθοδο packet sniffing για συλλογή δεδομένων για ανάλυση της κίνησης του δικτύου



Εικόνα 14 Στατιστικά στο Ethereal

Αναλυτικότερα, η εφαρμογή διαθέτει τις ακόλουθες λειτουργικότητες:

- Γραφική απεικόνηση αποτελεσμάτων
- Ταξινόμηση αποτελεσμάτων
- Φιλτράρισμα αποτελεσμάτων
- Συνεχής και σε πραγματικό χρόνοπαρακολούθηση δικτύου
- Χρωματική Κωδικοποίηση Αποτελεσμάτων
- Εξαγωγή γραφικών αποτελεσμάτων σε διάφορα formats (postscript κτλ)
- Υποστήριξη πολλών τύπων δικτύου (Ethernet, TCP/IP, ATM) για συλλογή real-time αποτελεσμάτων
- Υποστήριξη σχεδόν όλων των δικτυακών συσκευών από γνωστούς κατασκευαστές (Cisco, Toshiba, Lucent/Ascend κτλ)
- Διασύνδεση με πολλά προγράμματα συλλογής δεδομένων - packet sniffers (tcpdump-libcap, NAI's Sniffer, NetXray)



Εικόνα 15 Περιβάλλον εργασίας του Ethereal

2.10.2 Αξιολόγηση

Το Ethereal είναι ένα πρόγραμμα κατάλληλο για παρακολούθηση κίνησης μεγάλων δικτύων. Το συγκριτικό του πλεονέκτημα σε σχέση με τα άλλα προγράμματα εποπτείας δικτύων είναι ότι υποστηρίζει πολλούς τύπους δικτυακών συσκευών και πολλές τοπολογίες δικτύων.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Υποστήριξη πολλών προτοκόλλων επικοινωνίας δικτύου Υποστήριξη πολλών τύπων δικτύου Υποστήριξη σχεδόν όλων των δικτυακών συσκευών από γνωστούς κατασκευαστές Μεγάλες δυνατότητες ανάλυσης της κίνησης του δικτύου Γραφική απεικόνηση αποτελεσμάτων Υποστήριξη πολλών Λ.Σ.	Υποστήριξη μόνο της μεθόδου packet sniffing για συλλογή δεδομένων. Παρόλα αυτά όμως, υποστηρίζει διασύνδεση με πολλά προγράμματα συλλογής δεδομένων, μόνο τύπου packet sniffing. Προσφέρει λειτουργικότητες μόνο για παρακολούθηση δικτύου, δεν διαθέτει δυνατότητες για ανίχνευση και διαχείριση σφαλμάτων. Δεν προσφέρει λειτουργικότητες για παρακολούθηση δικτυακών συσκευών

2.11 Bello Network Monitoring (version 5.3.3.644)

2.11.1 Παρουσίαση [17]

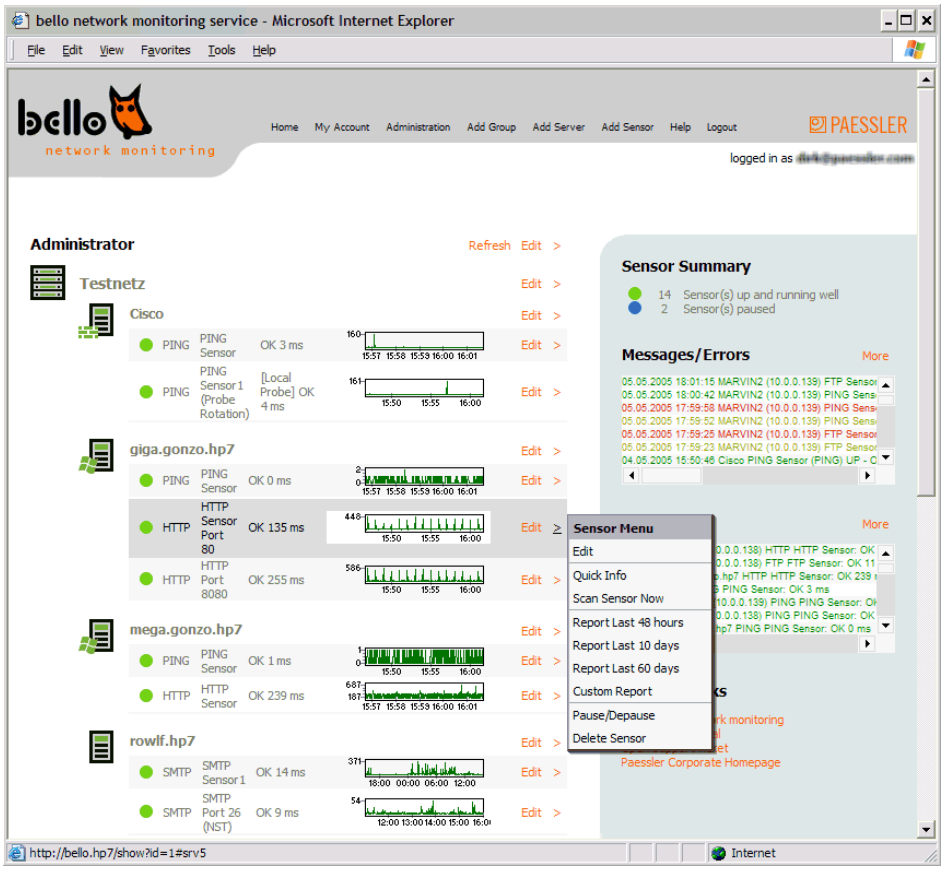
Πρόκειται για εμπορικό πακέτο, το οποίο προσφέρεται σε ελεύθερη διανομή με περιορισμένα χαρακτηριστικά σε σχέδη με το πλήρες εμπορικό πακέτο (Ταυτόχρονη παρακολυθηση μόνο 2 προωτοκόλλων επικοινωνίας, αυτόματος έλεγχος δικτύου κάθε 60 λεπτά). Προσφέρεται μόνο σε έκδοση για Windows και είναι προσβάσιμη τόσο μέσω διαδικτύου όσο και μέσω stand-alone διεπαφής.

Χρησιμοποιείται για παρακολούθηση δικτυακών εφαρμογών (websites) και για παρακολούθηση δικτυακών συσκευών (servers). Το πρόγραμμα ελέγχει περιοδικά την κατάσταση των δικτυακών συσκευών (η ελεύθερη έκδοση υποστηρίζει έλεγχο κάθε 60 λεπτά το ελάχιστο) και εφαρμογών και σε περιπτώσεις παραβίασης ειδοποιεί αυτόματα τον διαχειριστή του συστήματος (με email, CQ message)

Υποστηρίζει πολλά πρωτόκολλα δικτυακών επικοινωνιών (PING, PORT, HTTP, HTTPS, Advanced HTTP, HTTP Transaction, DNS, SMTP, POP3, FTP) και ο χρήστης μπορεί να επιλέξει ποια πρωτόκολλα επιθυμεί να παρακολουθεί. Η ελεύθερη έκδοση του προγράμματος υποστηρίζει ταυτόχρονη παρακολυθηση μόνο 2 πρωτοκόλλων επικοινωνίας.

Η εφαρμογή διαθέτει λειτουργικότητες γραφικής αναπαράστασης των συλλεγόμενων δεδομένων (γραφήματα) και παραγωγής αναφορών. Επίσης, διαθέτει εργαλείο παραγωγής στατιστικών.

Επιπρόσθετα, ενσωματώνει χρωματικές κωδικοποιήσεις για εύκολη παρακολούθηση της κατάστασης των δικτυακών συσκευών και εφαρμογών. Τέλος, διαθέτει βιβλιοθήκη λαθών, όπου περιέχονται κωδικοποιημένες οι πιο συχνες παραβιάσεις των TCP/IP δικτύων.



Εικόνα 16 Περιβάλλον εργασίας του Bello Network Monitoring

2.11.2 Αξιολόγηση

Το Bello Network Monitoring είναι ένα πρόγραμμα κατάλληλο για παρακολούθηση δικτυακών συσκευών και εφαρμογών και ανίχνευση σφαλμάτων σε TCP/IP δίκτυα. Αυτό που διαφοροποιεί την εφαρμογή από τις ομοειδείς της είναι η δυνατότητα για γραφική απεικόνηση των παραμέτρων παρακολούθησης.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
24 ωρη παρακολούθηση συσκευών/εφαρμογών Φιλικό περιβάλλον εργασίας Προσβάσιμο μέσω διαδικτύου Ανίχνευση σφαλμάτων Αναφορές, γραφήματα ανά συσκευή/εφαρμογή	Μόνο σε windows Ταυτόχρονη παρακολυθηση μόνο 2 προωτοκόλλων επικοινωνίας Μεγάλο χρονικό διάστημα μεταξύ περιοδικών ελέγχων (60 λεπτά), δεν υποστηρίζεται η παρακολούθηση σε πραγματικό χρόνο Υποστήριξη μόνο TCP/IP τύπων δικτύου

2.12 SysUpTime Network Monitor (personal edition, version 3.11)

2.12.1 Παρουσίαση [18]

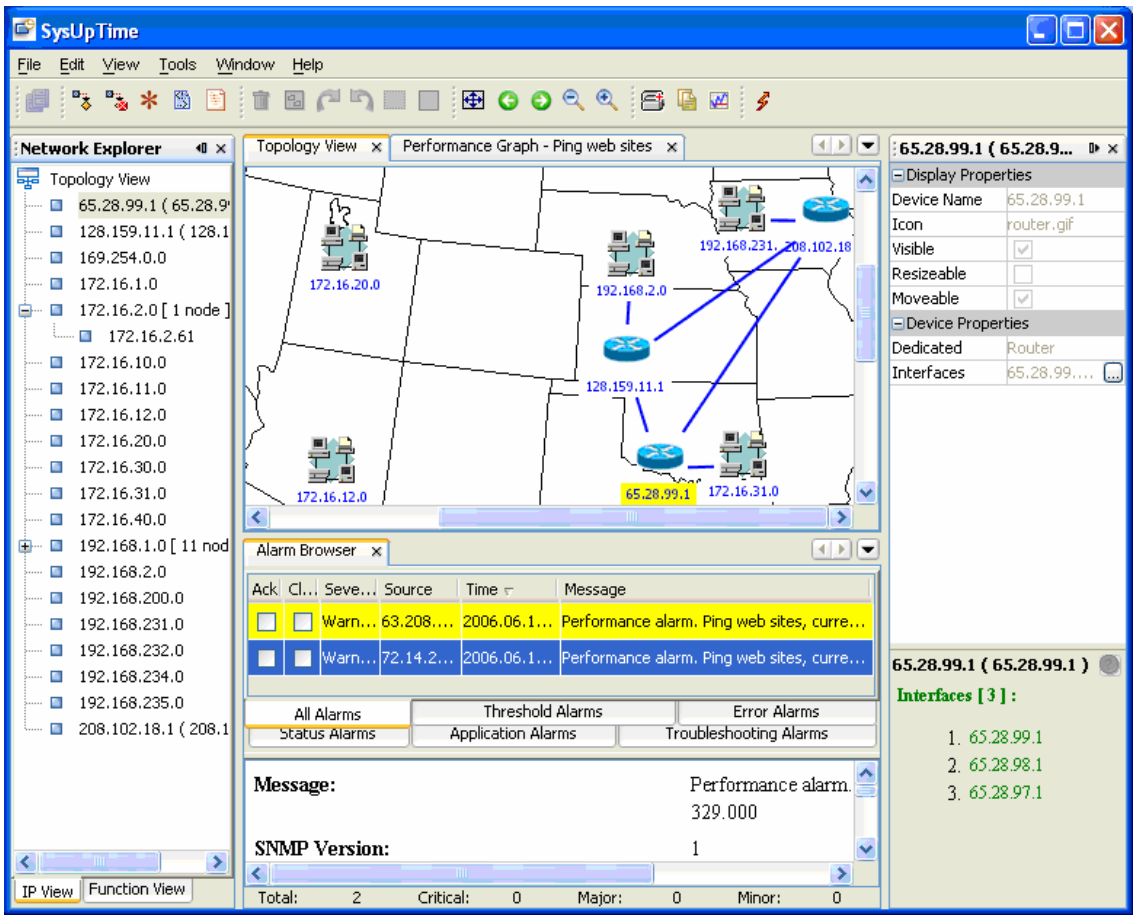
Πρόκειται για εμπορικό πακέτο, το οποίο προσφέρεται σε ελεύθερη διανομή με περιορισμένα χαρακτηριστικά σε σχέδη με το πλήρες εμπορικό πακέτο (παρακολούθηση και διαχείριση 20 δικτυακών συκευών το πολύ, δεν υποστηρίζει ταυτόχρονη πρόσβαση πάνω του ενός χρήστη). Προσφέρεται σε εκδόσεις για Windows and Linux/UNIX

Είναι ένα εύχρηστο εργαλείο παρακολούθησης και διαχείρισης δικτύου. Προσφέρει δυνατότητες παρακολούθησης της διαθεσιμότητας και της απόδοσης δικτυακών συσκευών (workstations, routers, switches). Σε περίπτωση ανίχνευσης σφαλμάτων το σύστημα ειδοποιεί αυτόματα τον διαχειριστή (με email). Μπορεί επίσης να παραμετροποιηθεί κατάλληλα ώστε σε περίπτωση σφαλμάτων να εκτελεί αυτόματα τα κατάλληλα scripts.

Αναλυτικότερα, οι προσφερόμενες λειτουργικότητες είναι:

Ανίχνευση της τοπολογίας του δικτύου

- Η εφαρμογή ανιχνεύει αυτόματα την τοπολογία του δικτύου και τις συνδέσεις μεταξύ των συσκευών και κατασκευάζει αυτόματα τον τοπολογικό χάρτη του δικτύου (διάγραμμα)
- Υποστηρίζει πολλούς τύπους δικτυακών συσκευών
- Εύκολη προσθήκη νέων συσκευών
- Ανίχνευση βάσει του πρωτοκόλλου SNMPv1/v2c/v3
- Χρονοπρογραμματισμός κατασκευής της δικτυακής τοπολογίας



Εικόνα 17 Περιβάλλον εργασίας του SysUpTime Network Monitor

Διαχείριση συσκευών

- Αυτόματη ανίχνευση δικτυακών συσκευών (ο τύπος των οποίων υπάρχει καταχωρημένος στο σύστημα)
- Εύκολη προσθήκη νέων τύπων δικτυακών συσκευών (πχ Cisco router)
- Δυνατότητα προσθήκης σημειώσεων στις συσκευές
- Αυτόνομη παρακολούθηση κάθε συσκευής

Παρακολούθηση Δικτύου

- Λεπτομερής παρακολούθηση της διαθεσιμότητας , της απόδοσης και της χρήσης του δικτύου
- Παρακολούθηση σε πραγματικό χρόνο
- Τήρηση στοιχείων παρακολούθησης για παραγωγή στατιστικών
- Γραφική απεικόνηση παρακολουθούμενων παραμέτρων
- Παραγωγή αναφορών; Εξαγωγή σε PDF format
- Χρονοπρογραμματισμός παραγωγής αναφορών
- Πλήθος προτυποποιημένων αναφορών και γραφημάτων
- Υποστήριξη πολλών προτοκόλλων επικοινωνίας (Ping, TCP/UDP, FTP, DNS/LDAP, SMTP/POP3)
- Υποστήριξη SNMPv1/v2c/v3

- Αυτόνομη παρακολούθηση συσκευών και εφαρμογών

Διαχείριση γεγονότων (events)

- Ανίχνευση γεγονότων
- Αυτόματη ειδοποίηση διαχειριστών σε περίπτωση ανίχνευσης συγκεκριμένου γεγονότος; Επισύναψη της περιγραφής του γεγονότος
- Κατηγοριοποίηση γεγονότων
- Χρωματική Κωδικοποίηση γεγονότων
- Αντιστοίχιση γεγονότων σε περιγραφές και μυνήματα λαθών
- Αυτόματη Εκτέλεση scripts

2.12.2 Αξιολόγηση

Το SysUpTime Network Monitor είναι μια ολοκληρωμένη πλατφόρμα διαχείρισης και εποπτείας δικτύου και μπορεί να χρησιμοποιηθεί για ολοκληρωμένη διαχείριση δικτύου, μια και καλύπτει όλα τα χαρακτηριστικά ενός συστήματος διαχείρισης, έτσι όπως αναφέρονται στην παράγραφο 1.2 – Απαιτήσεις από το σύστημα διαχείρισης.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Ολοκληρωμένη πλατφόρμα διαχείρισης και εποιπτείας δικτύου	Η ελεύθερη έκδοση υποστηρίζει έως 20 δικτυακές συκευές
Γραφική απεικόνηση της τοπολογίας του δικτύου	Διαθέτει μόνο προτυποποιημένες γραφικές παραστάσεις, δεν προσφέρει γραφικές παραστάσεις κατ' απαίτηση (οριζόμενες από τον χρήστη)
Ιδιαίτερα φιλικό προς τη χρήση	Υποστήριξη μόνο του SNMP προτοκόλου
Εξελιγμένες δυνατότητες οπτικής αναπαράστασης	Δεν διαθέτει δυνατότητες για ανάλυση της κίνησης (drill down)
Διαχείριση συσκευών και εφαρμογών	
Εκτεταμένες δυνατότητες διαχείρισης σφαλμάτων	
Υποστήριξη πολλών λειτουργικών συστημάτων	
Υποστήριξη πολλών πρωτοκόλλων επικοινωνίας	
Παρακολούθηση σε πραγματικό χρόνο	

2.13 NeTraMet (version 4.0)

2.13.1 Παρουσίαση [19]

Είναι ένα εργαλείο ανοιχτού λογισμικού το οποίο χρησιμοποιείται για παρακολούθηση και ανάλυση δικτύου. Διατίθεται μόνο σε εκδόσεις για UNIX Solaris, SunOS, Linux. Χρησιμοποιεί το πρωτόκολλο SNMP για συλλογή των παραμέτρων του δικτύου. Υποστηρίζει αρκετές τοπολογίες δικτύων (Ethernet, internet, οχι ATM).

Το πρόγραμμα δεν διαθέτει γραφικό περιβάλλον εργασίας. Είναι τύπου console-based και διαθέτει μεγάλη βιβλιοθήκη εντολών για παρακολούθηση δικτύου. Συγκεκριμένα προσφέρει λειτουργικότητες για:

- Παρακολούθηση σε πραγματικό χρόνο
- Παρακολούθηση χρήσης του δικτύου - μεταδιδόμενης πληροφορίας
- Αναλυση χρήσης του δικτύου – μεταδόσεις ανα δικτυακή θύρα, πρωτόκολλο κτλ (λειτουργικότητα nifty)
- Διαχείριση παρακολουθούμενων παραμέτρων -ποιες παράμετροι θα παρακολουθούνται, χρονικό διάστημα ανανέωσης (λειτουργικότητα NeMaC)
- Ταξινόμηση, και φιλτράρισμα αποτελεσμάτων (λειτουργικότητα fd_filter)
- Εξαγωγή στατιστικών αποτελεσμάτων (λειτουργικότητα fd_extract)
- Ιδιαίτερα γρήγορο

2.13.2 Αξιολόγηση

Το NeTraMet είναι ένα πρόγραμμα κατάλληλο για παρακολούθηση χρήσης του δικτύου σε πραγματικό χρόνο, μια και είναι ιδιαίτερα γρήγορο, αφού δεν διαθέτει λειτουργικότητες γραφικής απεικόνησης των αποτελεσμάτων.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Γρήγορο, κατάλληλο για παρακολούθηση σε πραγματικό χρόνο	Console-based, οχι φιλικό περιβάλλον εργασίας, δύσκολο στη χρήση
Διαχείριση παρακολουθούμενων παραμέτρων	Δεν υποστηρίζει Windows
Πολλές βιβλιοθήκες για ανάλυση και παρακολούθηση δικτύου	Παρουσίαση αποτελεσμάτων στην κονσόλα, όχι γραφική απεικόνηση
Εύκολη προσθήκη έξτρα λειτουργικοτήτων στον βασικό πυρήνα της εφαρμογής	Υποστήριξη μόνο του SNMP

2.14 RRDtool (version 1.2)

2.14.1 Παρουσίαση [20]

Είναι ένα εργαλείο ανοιχτού λογισμικού το οποίο διατίθεται σε εκδόσεις για UNIX, Linux,Windows. Χρησιμοποιείται για αποθήκευση παραμέτρων παρακολούθησης δικτύων και ανάλυση της συμπεριφοράς τους. Η εφαμρμογή διαθέτει ενσωματωμένη μια Round-Robin βάση δεδομένων στην οποία αποθηκεύονται οι παράμετροι παρακολούθησης με τη μορφή χρονοσειρών.

Η εφαρμογή δεν διαθέτει ενσωματωμένο module συλλογής παραμέτρων παρακολούθησης. Μπορεί όμως να διασυνδεθεί εύκολα με εφαρμογές παρακολούθησης παραμέτρων για καταγραφή των δεδομένων στην βάση της εφαρμογής και ανάλυση των δεδομένων. Αναλυτικότερα, υποστηρίζει συλλογή κα ιανάλυση δεδομένων απο πολλές διαφορετικές πηγές και ολοκλήρωση αυτών σε ένα γράφημα ή αναφορά.

Επιπρόσθετα, η εφαρμογή είναι εύκολα επεκτάσιμη. Παρέχεται δυνατότητα ενσωμάτωσης νέων εφαρμογών-modules. Διατίθενται πλατφόρμες για ανάπτυξη εφαρμογών και ενσωμάτωσή (σε Perl, Python, PHP) τους στο κυρίως εργαλείο.

Αναλυτικότερα, οι προσφερόμενες λειτουργικότητες είναι:

Συλλογή δεδομένων

- Συλλογή δεδομένων απο πολλές πηγές
- Καταγραφή σε βάση δεδομένων

- Παραγωγή μυνημάτων λάθους σε περιπτώσεις που οι τιμές μιας μεταβλητής ξεπερνούν συγκεκριμένα όρια (οριζόμενα από τον χρήστη)

Διαχείριση της δομής της βάσης δεδομένων

- Ορισμός των πεδίων της βάσης
- Ορισμός του χρονικού διαστήματος ανά το οποίο θα λαμβάνονται τιμές

Αρχειοθέτηση

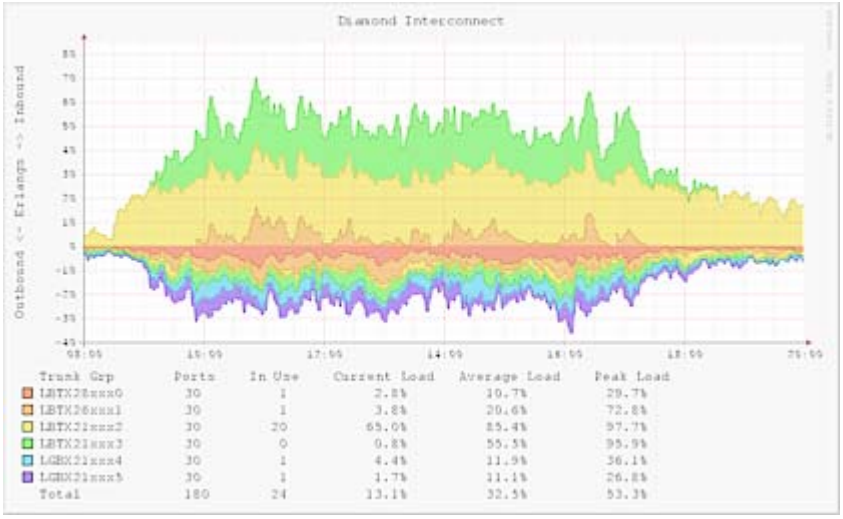
- Αρχειοθέτηση δεδομένων
- Καταγραφή απειριορίστου αριθμού records
- Ανάκτηση ιστορικών στοιχείων χωρίς περιορισμό

Στατιστική Επεξεργασία και Παρουσίαση

- Γραφική Αναπαράσταση Δεδομένων
- Γραφήματα, Πίνακες, Αναφορές
- Μεγάλες Δυνατότητες Στατιστικής Επεξεργασίας
- Γραφήματα/Αναφορές οριζόμενες από τον χρήστη

Ανάλυση Συμπεριφοράς Δικτύων

- Χρήση της Θεωρίας Ανάλυσης Χρονοσειρών
- Πρόβλεψη μελλοντικών τιμών βάσει των προηγούμενων τιμών μιας χρονοσειράς
- Ανάλυση απόκλισης (deviation) μεταξύ πραγματικών και προβλεπόμενων τιμών



Εικόνα 18 Ενδικτική Γραφική Παράσταση του RRDtool

2.14.2 Αξιολόγηση

Το RRDtool είναι ένα πρόγραμμα κατάλληλο για ανάλυση της συμπεριφοράς των δικτύων, σύγκριση δικτύων και εξαγωγή συγκριτικών αποτελεσμάτων.

Αναλυτικότερα, τα πλεονεκτήματα και τα μειονεκτήματα της εφαρμογής είναι:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Ολοκλήρωση με εφαρμογές παρακολούθησης δεδομένων για καταγραφή των δεδομένων	Δεν προσφέρει λειτουργικότητες για

στην βάση της εφαρμογής και ανάλυση των δεδομένων Εύκολη επέκταση με scripts - διατίθενται πλατφόρμες για ανάπτυξη εφαρμογών και ενσωμάτωσή (σε Perl, Python, PHP) τους στο κυρίως εργαλείο Μελέτη Συμπεριφοράς Δικτύων Πρόβλεψη συμπεριφοράς δικτύων Συγκριτικές Αναλύσεις Τήρηση μεγάλου αριθμού ιστορικών στοιχείων	παρακολούθηση σε πραγματικό χρόνο

3 ΣΥΜΠΕΡΑΣΜΑΤΑ – ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ

3.1 Σύνοψη Εργαλείων

Στην παρούσα εργασία παρουσιάστηκαν 14 δωρεάν εργαλεία για διαχείριση και παρακολούθηση δικτύων. Τα εργαλεία αυτά, όπως έχει αναφερθεί στο κεφ.2 χωρίζονται σε: ανοιχτού λογισμικού (open source), ελεύθερης διανομής (freeware) και ελεύθερης διανομής εμπορικές εφαρμογές με περιορισμένα χαρακτηριστικά (freeware, limited commercial editions). Οι εφαρμογές που εξετάστηκαν φαίνονται συνοπτικά στον παρακάτω πίνακα:

A/A	Εφαρμογή	OPEN SOURCE	FREEWARE	LIMITED EDITION
1	PRTG Traffic Grapher		**X**	
2	Multi Router Traffic Grapher	**X**		
3	VisualSniffer	**X**		
4	OpManager			**X**
5	NTop	**X**		
6	Big Brother		**X**	
7	nLive Core			**X**
8	NCS Z-tools.he Suite		**X**	
9	NMAP	**X**		
10	Ethereal	**X**		
11	Bello Network Monitoring			**X**
12	SysUpTime Network Monitor			**X**
13	NeTraMet	**X**		
14	RRD Tool	**X**		
	ΣΥΝΟΛΟ	***7***	***3***	***4***

Οι εφαρμογές που παρουσιάστηκαν προσφέρουν λειτουργικότητες που εξηπηρετούν διαφορετικά θέματα διαχείρισης και εποπτείας δικτύων. Αναλυτικότερα, τα εξεταζόμενα προγράμματα μπορούν να χωριστούν στις κατηγορίες που φαίνονται στον επόμενο πίνακα:

ΚΑΤΗΓΟΡΙΑ	ΕΦΑΡΜΟΓΕΣ
Παρακολούθηση Κίνησης Δικτύου	PRTG Traffic Grapher
	Multi Router Traffic Grapher
	VisualSniffer
	Ethereal
	NeTraMet
Παρακολούθηση Δικτυακών Συσκευών και Εφαρμογών	Big Brother
	Bello Network Monitoring
	NCS Z-tools.he Suite

Παρακολούθηση Ασφάλειας Δικτύου	NTop
	nLive Core
	NMAP
Ολοκληρωμένες Πλατφόρμες Διαχείρισης Δικτύου	OpManager
	SysUpTime Network Monitor
Ανάλυση Συμπεριφοράς Δικτύων	RRD Tool

3.2 Σύγκριση Εργαλείων

Σημειώνεται εδώ ότι κρίνουμε σκόπιμο να συγκρίνουμε ομοειδή εργαλεία, δηλαδή εργαλεία τα οποία ανήκουν στην ίδια από τις προαναφερόμενες κατηγορίες.

3.2.1 Εργαλεία Παρακολούθησης Κίνησης Δικτύου

Στην παρούσα εργασία εξετάστηκαν 5 εφαρμογές της κατηγορίας αυτής. Το Ethereal είναι κατάλληλο για παρακολούθηση της κίνησης μεγάλων και πολύπλοκων δικτύων, μια και υποστηρίζει πολλούς τύπους δικτυακών συσκευών και πολλές τοπολογίες δικτύων. Το MRTG είναι κατάλληλο για παρακολούθηση δικτύου σε πραγματικό χρόνο, μια και διαθέτει πολύ γρήγορες ρουτίνες για οπτικοποίηση των παρακολουθούμενων παραμέτρων. Ακόμη πιο γρήγορο είναι το NeTraMet, το οποιο όμως είναι consoled-based και δεν διαθέτει δυνατότητες για οπτική αναπαράσταση των αποτελεσμάτων. Κατάλληλο για ανάλυση της κίνησης σε πολύ μεγάλο βάθος (drill down) είναι το Visual Sniffer, το οποίο χρησιμοποιεί τη μέθοδο packet sniffing για μέτρηση και ανάλυση της κίνησης του δικτύου. Τέλος, πολύ εύχρηστο εργαλείο και ιδιαίτερα κατάλληλο για αρχάριους διαχειριστές συστημάτων είναι το PRTG.

3.2.2 Εργαλεία Παρακολούθησης Δικτυακών Συσκευών και Εφαρμογών

Εξετάστηκαν 3 εφαρμογές της κατηγορίας αυτής. Το BigBrother είναι κατάλληλο για παρακολούθηση της κατάστασης των δικτυακών πόρων (συσκευών και εφαρμογών) σε πραγματικό χρόνο. Το Bello Network Monitoring υποστηρίζει μόνο TCP/IP δίκτυα, δεν ενδείκνειται για παρακολούθηση σε πραγματικό χρόνο, αλλά διαθέτει λειτουργικότητες οπτικοποίησης των παρακολουθούμενων παραμέτρων. Τέλος, το NCS Z-tools.he Suite διαθέτει περιορισμένες λειτουργικότητες παρακολούθησης – προσφέρεται για παρακολούθηση της χρήσης των πόρων του δικτύου - και υποστηρίζει μόνο LAN. Λόγω της ιδιαίτερα φιλικής του διεπαφής είναι κατάλληλο για αρχάριους χρήστες.

3.2.3 Εργαλεία Παρακολούθησης Ασφάλειας Δικτύου

Εξετάστηκαν 3 εφαρμογές της κατηγορίας αυτής. Το Ntop είναι ένα ολοκληρωμένο πρόγραμμα παρακολούθησης της ασφάλειας του δικτύου. Προσφέρει λειτουργικότητες για ανίχνευση και διαχείριση σφαλμάτων. Το nLiveCore είναι επίσης ένα ολοκληρωμένο πρόγραμμα διαχείρισης ασφάλειας, και προσφέρει τις προαναφερόμενες δυνατότητες, όμως διατίθεται μόνο σε έκδοση για Linux. Βασίζεται σε εξελιγμένη τεχνική ανίχνευσης σφαλμάτων, χρησιμοποιώντας αλγόριθμους μάθησης και σύγκριση με πρότυπα συμπεριφοράς. Προσφέρει επίσης πολλές δυνατότητες παραγωγής στατιστικών και οπτικοποίησης αυτών. Δεν τηρεί όμως ιστορικά στοιχεία για μεγάλο χρονικό διάστημα – έως 7 ημέρες. Τέλος, το NMAP προσφέρεται για παρακολούθηση της ασφάλειας μεγάλων δικτύων χωρίς να διαθέτει όμως λειτουργικότητες ανίχνευσης και διαχείρισης σφαλμάτων.

3.2.4 Ολοκληρωμένες Πλατφόρμες Διαχείρισης Δικτύου

Παρουσιάστηκαν 2 ολοκληρωμένα συστήματα διαχείρισης δικτύων, τα οποία όμως είναι ελεύθυρες εκδόσεις εμπορικών προγραμμάτων και διαθέτουν περιορισμένα χαρακτηριστικά. Συγκεκριμένα, και οι 2 εφαρμογές υποστηρίζουν δίκτυα με 20 συσκευές το πολύ και έτσι δεν ενδείκνυνται για διαχείριση μεγάλων δικτύων. Και οι δύο εφαρμογές ικανοποιούν όλες τις απαιτήσεις των συστημάτων διαχείρισης δικτύων - έτσι όπως παρουσιάστηκαν στην ενότητα 1.2. Το OpManager διαθέτει περισσότερες λειτουργικότητες διαχείρισης ενώ το Network Monitor διαθέτει περισσότερες δυνατότητες οπτικοποίησης των παρακολουθούμενων παραμέτρων.

3.2.5 Εργαλεία Ανάλυσης Συμπεριφοράς Δικτύων

Θα μπορούσε κανείς να ισχυριστεί ότι στην κατηγορία αυτή ανήκουν τα προγράμματα των κατηγοριών τα οποία διαθέτουν modules για στατιστική επεξεργασία των παρακολυθούμενων παραμέτρων. Κανένα όμως από αυτά δεν διαθέτει τις δυνατότητες ανάλυσης του RRDtool. Συγκεκριμένα, το εργαλείο αυτό μπορεί να συλλέξει δεδομένα από πολλές διαφορετικές πηγές και να τα αποθηκεύσει στη βάση δεδομένων που διαθέτει. Υπάρχει δυνατότητα αποθήκευσης απεριορίστων εγγραφών. Διαθέτει δυνατότητες για στατιστική επεξεργασία δεδομένων και εκπόνηση συγκριτικών αναλύσεων, με παραμέτρους οριζόμενες από τον χρήστη. Διαθέτει επίσης δυνατότητες οπτικοποίησης των παραγόμενων αποτελεσμάτων. Τέλος, διαθέτει λειτουργικότητα για πρόβλεψη μελλοντικής συμπεριφοράς των δικτύων. Τα προαναφερόμενα χαρακτηριστικά καθιστούν το RDDtool απαραίτητο εργαλείο για εκπόνηση μελετών συμπεριφοράς δικτύων και παραγωγή στατιστικών αναλύσεων.

3.3 Μελλοντικές Επεκτάσεις

Ο δικτυακός τόπος [6] παρουσιάζει μια σύντομη ιστορική αναδρομή των εργαλείων διαχείρισης δικτύου από την προηγούμενη δεκαετία μέχρι και σήμερα. Από την αναδρομή αυτή μπορεί να εξαχθεί το συμπέρασμα ότι τα σύγχρονα πακέτα διαχείρισης δικτύων προσανατολίζονται προς τα ακόλουθα:

- **Ασφάλεια Δικτύων**. Ιδιαίτερη σημασία δίνεται από τους κατασκευαστές στην ανάπτυξη ισχυρών εργαλείων διαχείρισης της ασφάλειας των δικτύων. Τα σύγχρονα πακέτα τα οποία επικρατούν στον χώρο της διαχείρισης δικτύων διαθέτουν πολύ ισχυρά εργαλεία ανίχνευσης και διαχείρισης εξωτερικών επιθέσεων καθώς και προστασίας δεδομένων, εφαρμογών και συσκευών από τις επιθέσεις αυτές.
- **Συμβατότητα με πολλούς τύπους συσκευών**. Ιδιαίτερη σημασία δίνεται στην ανάπτυξη εφαρμογών διαχείρισης δικτύων οι οποίες θα είναι συμβατές με πολλούς τύπων δικτυακών συσκευών διαφορετικών κατασκευαστών.
- **Διαλειτουργικότητα μεταξύ εφαρμογών**. Επειδή το θέμα της διαχείρισης δικτύων είναι ιδιαίτερα πολύπλοκο και με πολλές απαιτήσεις, η κατασκευή/αγορά μιας ολοκληρωμένης πλατφόρμας διαχείρισης είναι οικονομικά ασύμφορη. Η σύγχρονη τάση προσανατολίζεται στην ανάπτυξη ισχυρών προγραμμάτων σε υποπεριοχές της διαχείρισης δικτύων (με την εφαρμογή ανοιχτών προτύπων), με στόχο ολοκλήρωση αυτών σε μία ενοποιημένη πλατφόρμα διαχείρσης.
- **Packet sniffing**. Όσον αφορά τα πρωτόκολλα διαχείρισης δικτύων, ιδιαίτερα προτιμάται το Packet sniffing, το οποίο προσφέρει μεγάλες δυνατότητες ανάλυσης της κίνησης του δικτύου.

4 ΒΙΒΛΙΟΓΡΑΦΙΑ

Συγγράμματα:

[1] **Dr Αμαλία Μήλιου, Σημειώσεις μαθήματος «Διαχείριση Επικοινωνιακών Συστημάτων»**, Τμήμα Πληροφορικής, ΑΠΘ (http://agent.csd.auth.gr/lesson12.html.el) – Σημειώσεις σχετικές με τις θεωρητικές αρχές και την αρχιτεκτονική σχεδιασης συστημάτων διαχείρισης δικτύου.

[2] **Cicso Technical Documentation: Internetworking Technology Handbook, chapter 6: Network Management Basics** (http://www.cisco.com/univercd/cc/td/doc/cisintwk/index.htm) – Σύγγραμμα της εταιρίας Cisco σχετικά με τις θεωρητικές αρχές των συστημάτων διαχείρισης δικτύων. Αναλυτική παρουσίαση του μοντέλου ISO για τα συστήματα διαχείρισης δικτύων.

Διαδίκτυο:

[3] http://www.wikipedia.com/ - online εγκυκλοπαίδεια τεχνολογικών όρων

[4] http://www.tucows.com/ - μη εμπορικός δικτυακός τόπος για κατέβασμα (downloading) ελεύθερων και δοκιμαστικών εργαλείων λογισμικού

[5] http://www.freedownloads.com/ - μη εμπορικός δικτυακός τόπος για κατέβασμα (downloading) ελεύθερων και δοκιμαστικών εργαλείων λογισμικού

[6] http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html - δικτυακή περιοχή του πανεπιστημίου του Stanford, όπου παρουσιάζονται επιλεγμένα εργαλεία διαχείρισης δικτύων.

[7] http://www.paessler.com/prtg - επίσημο site του εργαλείου PRTG

[8] http://oss.oetiker.ch/mrtg/ - επίσημο site του εργαλείου MRTG

[9] http://www.biovisualtech.com/vindex.htm - επίσημο site του εργαλείου Visual Sniffer

[10] http://manageengine.adventnet.com/products/opmanager/ - επίσημο site του εργαλείου Opmanager

[11] http://www.ntop.org/ntop.html - επίσημο site του εργαλείου NTOP

[12] http://www.bb4.org/ - επίσημο site του εργαλείου BigBrother

[13] http://www.vigiliti.com/ - επίσημο site του εργαλείου nLive Core

[14] http://www.nativecs.com/index.en.php - επίσημο site των εργαλείων NCS Z-tools.he Suite

[15] http://insecure.org/nmap/ - επίσημο site του εργαλείου nmap

[16] http://www.ethereal.com/ - επίσημο site του εργαλείου ethereal

[17] http://www.bello-monitors-the.net/about/ - - επίσημο site του εργαλείου Bello Network Monitoring

[18] http://www.ireasoning.com/network_monitor.shtml - - επίσημο site του εργαλείου SysUpTime Network Monitor

[19] http://www.auckland.ac.nz/net/NeTraMet/ - επίσημο site του εργαλείου NeTraMet

[20] http://oss.oetiker.ch/rrdtool/ - - επίσημο site του εργαλείου RRDtool