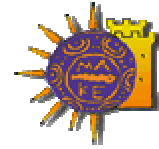




Survey of Tools for Monitoring and Managing a Network:

- **LinkView Pro,**
- **IP Manager,**
- **pcAnywhere,**
- **NeoTrace,**
- **Select-a-Net,**
- **Security Manager,**
- **SwitchIP,**
- **IP Ultra Monitor,**
- **Netcop Scanner,**
- **Timbuktu Pro,**
- **Monet LAN Analyzer,**
- **RemotelyAnywhere,**
- **sFLOW (InMon Co.),**
- **Ntop,**
- **NeTraMet,**



Επισκόπηση Εργαλείων για Εποπτεία και Διαχείριση ενός Δικτύου:

- LinkView Pro,
- IP Manager,
- pcAnywhere,
- NeoTrace,
- Select-a-Net,
- Security Manager,
- SwitchIP,
- IP Ultra Monitor,
- Netcop Scanner,
- Timbuktu Pro,
- Monet LAN Analyzer,
- RemotelyAnywhere,
- sFLOW (InMon Co.),
- Ntop,
- NeTraMet,

Abstract

In any network, the control of its proper operation constitutes a considerable chapter that must be taken into consideration during its design, implementation and management. In order to achieve that, we use various programs-tools, some of which will be presented in this project. Many of them enable us to remotely monitor what happens inside a computer or even inside the total number of computers found in the network. Specifically we can check the programs running in a computer as well as the user who runs them. Moreover we can view statistics about the network traffic as well as the used protocols by analyzing in low level the flow of data frames. Apart from the mere monitoring there are also programs (especially those produced by well known software companies) enabling system administrators to interfere remotely in the operation of the computer up to the point of entering commands or running programs as if they were standing in front of it. A very significant factor of these monitoring and managing programs is the security level they provide. The more functional such a programs is, the more difficult is to ensure total security in every level.

Περίληψη

Σε ένα δίκτυο ο έλεγχος της σωστής λειτουργίας του αποτελεί ένα σημαντικό κεφάλαιο που πρέπει να εξετάσουμε κατά τη διάρκεια του σχεδιασμού, της υλοποίησης αλλά και κατά τη διάρκεια της διαχείρισής του. Για να γίνει αυτό χρησιμοποιούμε διάφορα προγράμματα-εργαλεία, ορισμένα από τα οποία παρουσιάζουμε στην παρούσα εργασία. Πολλά από αυτά παρέχουν τη δυνατότητα να παρακολουθούμε από μακριά το τι συμβαίνει σε κάποιον υπολογιστή ή και σε όλους τους υπολογιστές που βρίσκονται στο δίκτυο. Συγκεκριμένα μπορούμε να ελέγξουμε από το τι προγράμματα τρέχουν σε έναν υπολογιστή και ποιος χρήστης είναι αυτός που τα τρέχει μέχρι να δούμε σε χαμηλό επίπεδο τα πακέτα των δεδομένων που διακινούνται και να πάρουμε στατιστικές πληροφορίες για το φόρτο του δικτύου ή για τα πρωτόκολλα που χρησιμοποιούνται. Εκτός όμως από την απλή παρακολούθηση υπάρχουν προγράμματα (κυρίως αυτά των μεγάλων εταιρειών παραγωγής software) που δίνουν τη δυνατότητα στους διαχειριστές των συστημάτων να μπορούν από μακριά να παρεμβαίνουν στη λειτουργία ενός υπολογιστή, στο βαθμό του να δίνουν εντολές ή να τρέχουν προγράμματα, σαν να βρίσκονται μπροστά στο συγκεκριμένο υπολογιστή. Πολύ σημαντικός παράγοντας σε αυτά τα προγράμματα παρακολούθησης και διαχείρισης ενός δικτύου είναι ο βαθμός της ασφάλειας την οποία παρέχουν. Όσο πιο λειτουργικό είναι ένα τέτοιο πρόγραμμα τόσο πιο δύσκολο είναι να μας εγγυηθεί πλήρη ασφάλεια σε όλα τα επίπεδα.

Contents - Περιεχόμενα

Abstract - Περίληψη	3
Contents - Περιεχόμενα	4
Introduction - Εισαγωγή	5
Reviews - Περιγραφή των Προγραμμάτων	
LinkView.....	6
Cisco IP Manager	7
pcAnywhere	9
NeoTrace Pro	13
Select-a-Net.....	15
Security Manager	16
SwitchIP Professional	18
IP Ultra Monitor 2000	19
Netcop Scanner	21
Timbuktu Pro 2000	23
Monet LAN Analyzer	25
RemotelyAnywhere.....	27
sFLOW	29
Ntop.....	31
NeTraMet	35
Conclusion - Συμπεράσματα.....	36
References - Αναφορές	37

Εισαγωγή

Τα προγράμματα για την παρακολούθηση και τη διαχείριση ενός δικτύου είναι πολλά. Οι δυνατότητές τους ξεκινάνε από κάποιες μεμονωμένες και απλές λειτουργίες και καταλήγουν σε ολοκληρωμένες λύσεις μεγάλων πακέτων που εξασφαλίζουν πλήρη έλεγχο της λειτουργίας του δικτύου σε οποιοδήποτε επίπεδο. Από όλα αυτά τα προγράμματα θα εξετάσουμε αντιπροσωπευτικά 15.

Ορισμένα από αυτά δίνουν απλώς χρήσιμες πληροφορίες για το δίκτυο χωρίς να υπάρχει η δυνατότητα παρέμβασης σε αυτό. Στις περιπτώσεις αυτές τα προγράμματα είναι χαμηλού κόστους, ή είναι ελεύθερα καθώς μπορεί να προέρχονται από ερευνητικά προγράμματα πανεπιστημίων ή διατίθενται για διαφημιστικούς σκοπούς από κάποιες εταιρείες προκειμένου να γίνουν γνωστές και να προωθήσουν άλλα μεγαλύτερα προϊόντα.

Θα δούμε όμως και τα σημαντικότερα ολοκληρωμένα πακέτα των μεγάλων εταιρειών Software που συνήθως έχουν αρκετά μεγάλη τιμή και απευθύνονται αποκλειστικά και μόνο στους διαχειριστές μεγάλων δικτύων. Οι δυνατότητες αυτών των προγραμμάτων είναι μεγάλες και υπάρχει περιθώριο για προσθήκη νέων επιλογών από την πλευρά των διαχειριστών

Για κάθε πρόγραμμα, θα δούμε τον τρόπο με τον οποίο εκλαμβάνει τις πληροφορίες μέσα από το δίκτυο και μέχρι πιο επίπεδο μπορεί να το επιτύχει αυτό. Επιπλέον θα δούμε μέχρι πιο βαθμό μπορούν να γίνουν επεμβάσεις και κατά πόσον η παρακολούθηση και διαχείριση μπορεί να γίνει από μακριά.

Τέλος θα εξετάσουμε για όλα τα προγράμματα το βαθμό της ασφάλειας στην οποία χρειάζεται να δοθεί μεγάλη έμφαση. Υπάρχει κίνδυνος, μέσω αυτών των προγραμμάτων να γίνει από τρίτους ανάκτηση σημαντικών πληροφοριών αλλά και επεμβάσεις σε συστήματα εφόσον δεν προσεχθεί ιδιαίτερα το θέμα της ασφάλειας.

Η σειρά των προγραμμάτων που ακολουθεί είναι τυχαία. Για το κάθε πρόγραμμα δίνουμε αρχικά ορισμένα στοιχεία όπως την εταιρεία που το προωθεί, την έκδοση την οποία εξετάσαμε καθώς και μια ενδεικτική τιμή για το πρόγραμμα όπου αυτή υπάρχει.

	LinkView Classic Network Analyzer for Local Area Network Analysis	 
Έκδοση	7.2 (2000)	
Εταιρεία	Wavetek Wandel & Goltermann Acterna	
Τιμή	US \$995.00	

Χαρακτηριστικά

- Ανάλυση φόρτου δικτύου και Internet
- Ανάλυση σφαλμάτων
- Στατιστικά δικτύου
- Ευέλικτες αναφορές
- Δημιουργία φόρτου (traffic generator)
- Διαχείριση συμβάντων

Περιγραφή

Το LinkView είναι ένα πολύ καλό πρόγραμμα για παρακολούθηση και ανάλυση του φόρτου ενός τοπικού δικτύου σε πραγματικό χρόνο. Από τη στιγμή που γίνει η σύνδεση με το δίκτυο όλα τα πλαίσια δεδομένων που λαμβάνει η κάρτα δικτύου περνούν και στο LinkView. Για κάθε πλαίσιο εξετάζεται

- η διεύθυνση προορισμού
- η διεύθυνση προέλευσης
- τα πρωτόκολλα που το συνοδεύουν και
- ο τύπος του

Το LinkView πραγματοποιεί ανάλυση του φόρτου και της ροής των δεδομένων στο δίκτυο και εμφανίζει στατιστικές για όλο το δίκτυο αλλά και για συγκεκριμένους σταθμούς εργασίας μέσα σε αυτό. Παρέχει σε πραγματικό χρόνο συλλογή δεδομένων και εμφανίζει στατιστικά κίνησης όπως ρυθμούς πλαισίων, ρυθμούς σφαλμάτων και χρήση του εύρους ζώνης. Χρησιμοποιώντας το πρωτόκολλό του “discoverer/decoder” εμφανίζει και αποκωδικοποιεί τα πρωτόκολλα που βρίσκει στο δίκτυο. Ακόμα παρέχει φίλτρα που μπορούν να εφαρμοστούν στα πλαίσια που περνούν από το πρόγραμμα και έχουν κρατηθεί στον buffer. Για διάφορα χρονικά διαστήματα - αυτό μπορεί να ρυθμιστεί - συγκεντρώνει στοιχεία από αυτά τα πλαίσια και δίνει πληροφορίες για αυτά. Όλα τα αποτελέσματα εμφανίζονται σε ένα αρκετά απλό και κατανοητό γραφικό περιβάλλον

Πρόκειται για ένα αυτοδύναμο πρόγραμμα όπου μόνο με software αναλύει το δίκτυο είτε αυτό στηρίζεται σε Ethernet είτε σε Token Ring κάρτες.

Στα υπέρ του προγράμματος θα μπορούσαμε να πούμε το ότι:

- Μειώνει δραματικά το χρόνο που απαιτείται για να λυθούν επίμονα αλλά και περιοδικά εμφανιζόμενα προβλήματα στο δίκτυο
- Παρέχει στους διαχειριστές και τεχνικούς του δικτύου την ικανότητα να έχουν πρόσβαση σε λειτουργίες και επιλογές που παραδοσιακά προσφέρονται μόνο από πολύ ακριβά hardware εργαλεία.
- Βοηθά τους διαχειριστές του κάθε δικτύου στο δυναμικό σχεδιασμό και ανάλυση με σκοπό τη βελτιστοποίησή του.

Λειτουργικό σύστημα - Απαιτήσεις

Το πρόγραμμα μπορεί να τρέξει σε περιβάλλον Windows 95/NT καθώς και στις νεότερες εκδόσεις τους χωρίς ιδιαίτερα μεγάλες απαιτήσεις από πλευράς Hardware.

Αξιολόγηση

Το LinkView αν εξαιρέσουμε την τιμή του – η οποία είναι για αυτά που προσφέρει πολύ ακριβή - θα μπορούσε να χαρακτηριστεί πολύ καλό. Μπορεί κανείς εύκολα να το δοκιμάσει κατεβάζοντας τη δοκιμαστική έκδοση από το site της Acterna αλλά και από πολλά άλλα site που διακινούν shareware ή freeware προγράμματα.

	Cisco IP Manager (Lite)	
Έκδοση	2.0 (2000)	
Εταιρεία	Cisco Systems	
Τιμή	\$75,000	

Χαρακτηριστικά

- Ρυθμίσεις καθοδηγούμενες από φόρμες που μπορούν εύκολα να δημιουργηθούν
- Έλεγχος πρόσβασης στα αρχεία ρυθμίσεων
- Δυνατότητα upload και download των αρχείων ρυθμίσεων
- Έλεγχος της κατάστασης των στοιχείων του δικτύου (όπως το ping και το show)
- Καταγραφή δραστηριοτήτων

Περιγραφή

Το IP Manager της Cisco αποτελεί ένα τμήμα του Cisco Service Management (CSM) που είναι μια συλλογή από εργαλεία για τους παροχείς υπηρεσιών και για τους διαχειριστές μεγάλων δικτύων. Το IP Manager σε συνδυασμό με τα άλλα εργαλεία του CSM προσφέρει άμεση, ολοκληρωμένη και υψηλής ποιότητας δυνατότητα διαχείρισης των συστημάτων σε οποιοδήποτε επίπεδο επιθυμούν οι διαχειριστές τους.

Συνήθως οι απαιτήσεις των επιχειρήσεων είναι στο 3ο αξιόπιστο επίπεδο για τα πολύ μεγάλα δίκτυα όπου το IP Manager:

- Επιτρέπει γρήγορη, υψηλής ποιότητας ανάπτυξη υπηρεσιών μέσω αυτοματοποιημένου και δομημένου συστήματος
- Υποστηρίζει νέες end-to-end υπηρεσίες δικτύου
- Επιτρέπει καταμερισμό του ελέγχου των αρμοδιοτήτων ώστε να υπάρχει συμφωνία με τις απαιτήσεις της επιχείρησης

Οι χειριστές μπορούν να χρησιμοποιήσουν το πρόγραμμα είτε για να ρυθμίσουν νέες συσκευές πριν ακόμα μπουν σε on line λειτουργία, είτε για να αλλάξουν υπάρχουσες ρυθμίσεις σε στοιχεία που βρίσκονται σε λειτουργία προκειμένου να υποστηρίξουν νέες υπηρεσίες. Έτσι μπορεί κανείς να γράφει τις τρέχουσες παραμέτρους των συσκευών σε αρχεία ρυθμίσεων πριν έρθουν στο δίκτυο νέα δεδομένα ρυθμίσεων οπότε υπάρχει η δυνατότητα να επανέλθουμε στις αρχικές ρυθμίσεις αν χρειαστεί

Μπορούν να κατασκευαστούν πολλαπλά αρχεία ρυθμίσεων τα οποία να κατανεμηθούν στο δίκτυο ώστε να δημιουργηθούν τυποποιημένες ρυθμίσεις που

μπορούν να αφορούν ονοματολογία διευθυνσιοδότηση δικτύων και υποδικτύων. Η όλη διαδικασία δημιουργίας και κατανομής των αρχείων ρυθμίσεων γίνεται τόσο απλά που θυμίζει τη συγχώνευση αλληλογραφίας που κάνει ένα πρόγραμμα επεξεργασίας κειμένου. Μπορούν να οργανωθούν έτσι με αυτόν τον τρόπο domains, subdomains, user groups, και να καθοριστούν αρμοδιότητες και δικαιώματα είτε σε διαχειριστές είτε σε απλούς χρήστες.

Σε πλήρη έκδοση το IP Manager περιλαμβάνει τα παρακάτω στοιχεία:

- ADMServer— (Administration Server)
- CTMServer— (Configuration Template Manager Server)
- Event Server
- GUI application — (Εφαρμογή των βασικών λειτουργιών σε γραφικό περιβάλλον)



- LOGServer
- Name Server
- NEMServer— (Network Element Manager Server – κανονίζει την επικοινωνία μεταξύ του προγράμματος με τα στοιχεία του δικτύου είτε μέσω του TGServer είτε μέσω του SGServer ανάλογα με την περίπτωση)
- Oracle database— (για την αποθήκευση στοιχείων)
- SGServer— (SNMP Gateway Server – γνωστός και σαν SGS)
- TGServer— (Telnet Gateway Server – χρησιμοποιεί το Telnet πρωτόκολλο για να επικοινωνεί με τα στοιχεία του δικτύου)
- VCMServer— (Version Control Manager Server – αρχειοθετεί τα στοιχεία του δικτύου και κρατά ιστορικό για τις αλλαγές των ρυθμίσεών τους).

Αν το επιτρέπει το Hardware όλα αυτά μπορούν να εγκατασταθούν στο ίδιο μηχάνημα. Μπορούμε όμως να έχουμε και καταμερισμό.

Λειτουργικό σύστημα - Απαιτήσεις

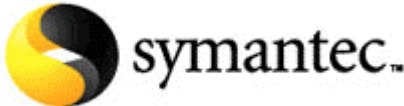
Για να δουλέψει το IP Manager, χρειαζόμαστε μαζί με το λειτουργικό και κάποια επιπλέον εργαλεία. Συγκεκριμένα απαιτούνται:

- Solaris 2.6 με Common Desktop Environment (CDE) ή άλλο γραφικό πρόγραμμα διαχείρισης που να υποστηρίζει Java run-time environment (JRE)
- Solaris SUNWspot και SUNWbtool packages
- Oracle Enterprise Server, version 8.0.5, που πρέπει να περιλαμβάνει:
 - Oracle UNIX Installer
 - ORACLE8 Server (RDBMS)
 - Oracle Net8 8.0.5.0.0
 - SQL*Plus
 - TCP/IP Protocol Adapter (V2)

Συνήθως η Cisco θα είναι αυτή που θα επιλέξει και το απαραίτητο υλικό πάνω στο οποίο θα δουλέψουν τα προγράμματά της χωρίς όμως βέβαια αυτό να αποτελεί κανόνα. Σε κάθε περίπτωση όμως απαιτείται σύγχρονο και αξιόπιστο υλικό.

Αξιολόγηση

Πανίσχυρο πρόγραμμα με την εγγύηση της Cisco. Από την τιμή του καταλαβαίνουμε ότι αφορά μόνο μεγάλες επιχειρήσεις και οργανισμούς που υποστηρίζονται από μεγάλα δίκτυα υπολογιστών και απασχολούν μεγάλο αριθμό χρηστών. Για την χρήση του προγράμματος ασφαλώς απαιτούνται έμπειροι διαχειριστές συστημάτων.

	pcAnywhere	
Έκδοση	10.5	
Εταιρεία	Symantec	
Τιμή	\$179.95	

Χαρακτηριστικά

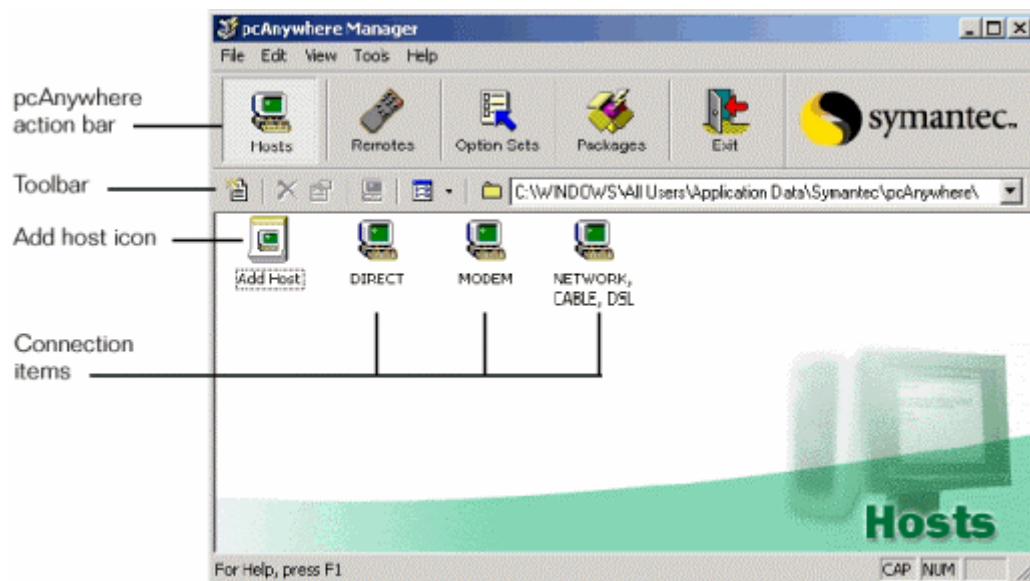
- Ανίχνευση σφαλμάτων υπολογιστών
- Υποστήριξη και συντήρηση servers σε δίκτυα
- Ανάκτηση αρχείων από το σπίτι ή από το χώρο εργασίας
- Εργασία από απόσταση.
- Δυνατότητα ιδιαίτερων παρεμβάσεων από τους χρήστες
- Αυξημένη λειτουργικότητα

Περιγραφή

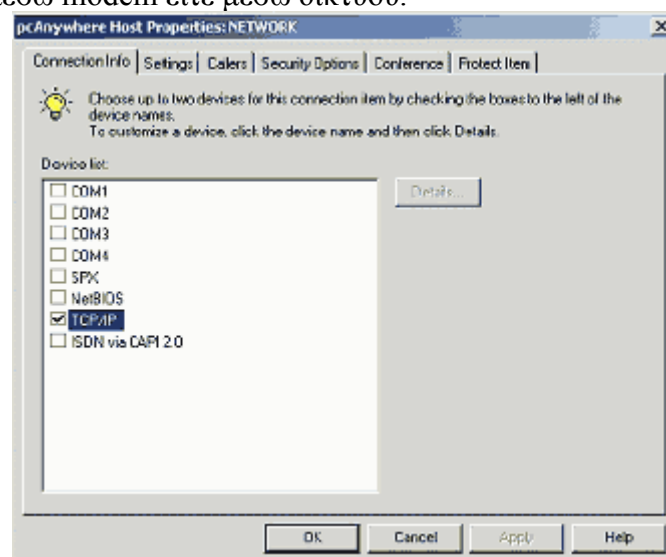
Το pcAnywhere της Symantec είναι το δημοφιλέστερο και πιο αξιόπιστο πρόγραμμα για απομακρυσμένο έλεγχο και διαχείριση υπολογιστών. Με το pcAnywhere μπορούμε να συνδεθούμε σε έναν απομακρυσμένο υπολογιστή στον οποίο έχουμε πρόσβαση, να τρέξουμε προγράμματα σε αυτόν και να βλέπουμε την εικόνα που θα είχε ο συγκεκριμένος υπολογιστής μέσα σε ένα παράθυρο στον δικό μας υπολογιστή. Μπορούμε ακόμα, να ανοίξουμε και να τροποποιήσουμε αρχεία ή ρυθμίσεις αλλά και να έχουμε πρόσβαση σε συσκευές που είναι συνδεδεμένες με τον απομακρυσμένο υπολογιστή σαν να βρισκόμαστε και εμείς εκεί. Έτσι μας δίνετε η δυνατότητα να διαχειριστούμε έναν server οπουδήποτε και αν βρισκόμαστε με μια απλή σύνδεση (Dial-Up ή LAN ή μέσω Internet) αρκεί φυσικά να έχουμε ορίσει σωστά τα δικαιώματα πρόσβασης και να τα προστατεύσουμε με κατάλληλους κωδικούς.

Το συγκεκριμένο πρόγραμμα χρησιμοποιείται από υπηρεσίες εξυπηρέτησης πελατών, διαχειριστές δικτύων, και άλλους επαγγελματίες στον τομέα των επικοινωνιών και δικτύων επειδή μπορούν να συνδεθούν από το χώρο της δουλειάς τους σε ένα άλλο υπολογιστή και να επιλύουν πιθανά προβλήματα χωρίς να μετακινηθούν. Με τον ίδιο τρόπο μπορεί να γίνετε και ο περιοδικός έλεγχος απομακρυσμένων υπολογιστών από τους διαχειριστές των δικτύων.

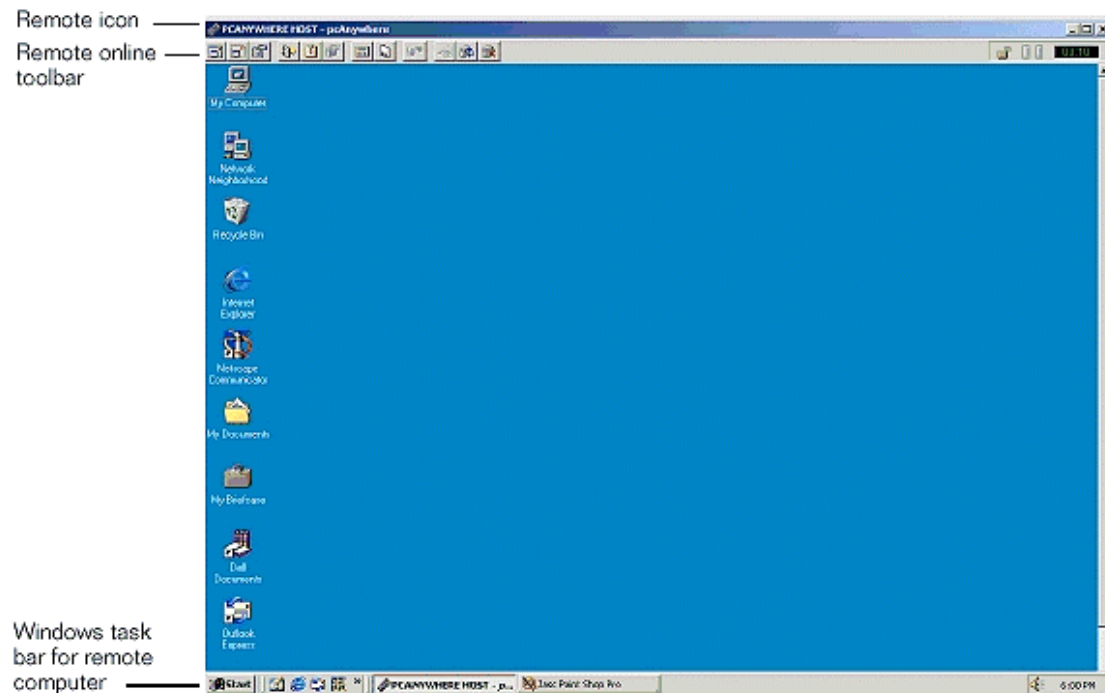
Στο βασικό μενού του pcAnywhere Manager υπάρχουν επιλογές για καθορισμένες συνδέσεις, δημιουργία νέων συνδέσεων, μεταφορά αρχείων, ρύθμιση των επιλογών καθώς και άλλες επιλογές προβολής και επεξεργασίας.



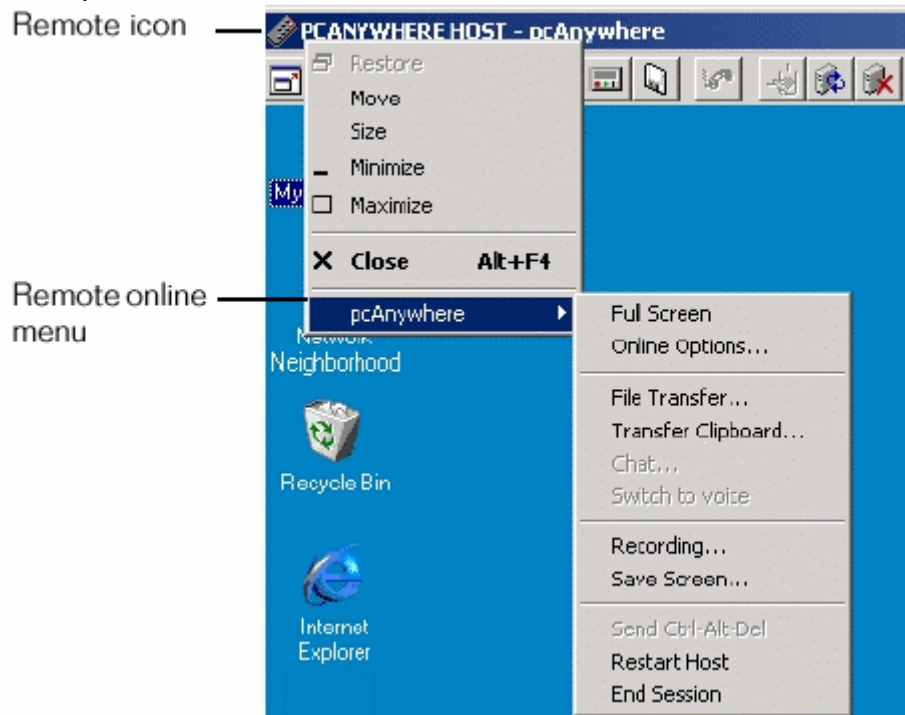
Υπάρχουν ακόμα επιλογές που καθορίζουν αν ο υπολογιστής πρόκειται να παίζει το ρόλο του host ή του remote. Σε κάθε εικονίδιο σύνδεσης αποθηκεύονται όλες οι παράμετροι που χρειάζονται για να λειτουργήσει σωστά η σύνδεση είτε αυτή είναι απευθείας είτε μέσω modem είτε μέσω δικτύου.



Από τη στιγμή που γίνει η σύνδεση η επιφάνεια εργασίας εμφανίζεται σε παράθυρο στον υπολογιστή που βρισκόμαστε. Στο συγκεκριμένο παράθυρο εμφανίζεται και μια γραμμή εργαλείων του pcAnywhere με επιλογές για τη σύνδεση.

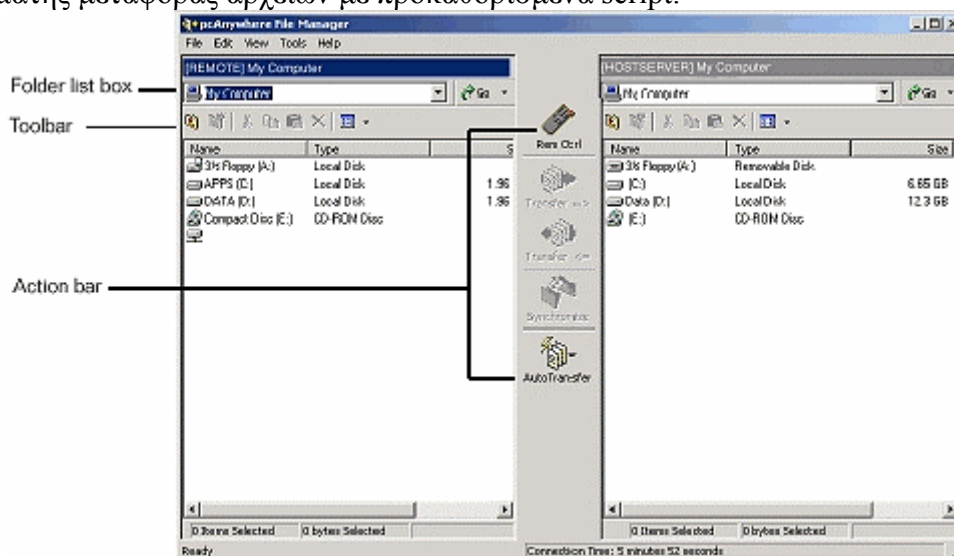


Μερικές από αυτές είναι μεταφορά αρχείων, συνομιλία με τον χρήστη (εφόσον υπάρχει εκείνη τη στιγμή) του απομακρυσμένου υπολογιστή, αλλά και καταγραφή όλων των λειτουργιών της σύνδεσης σε αρχείο το οποίο μπορεί να εκτελεστεί σε μια άλλη σύνδεση.



Τον έλεγχο της σύνδεσης μπορεί να έχει είτε το βασικό είτε το απομακρυσμένο σύστημα και μπορούν να δουλεύουν παράλληλα χειριστές και στους δύο υπολογιστές για την ίδια επιφάνεια εργασίας! Συνήθως βέβαια έχει γίνει ρύθμιση στον απομακρυσμένο υπολογιστή για αυτόματη αποδοχή κλήσεων σύνδεσης και μετά την επιβεβαίωση των κωδικών υπάρχει σχεδόν πλήρης πρόσβαση σε όλο το απομακρυσμένο σύστημα.

Ειδικότερα για τη μεταφορά αρχείων υπάρχει ξεχωριστός File Manager που επιτρέπει γρήγορη και εύκολη διαχείριση αρχείων και καταλόγων, μεταφορά τους από τον ένα υπολογιστή στον άλλο, συγχρονισμό καταλόγων αλλά και δυνατότητα αυτόματης μεταφοράς αρχείων με προκαθορισμένα script.



Μπορούμε επίσης να έχουμε εκτύπωση αρχείων είτε σε απομακρυσμένους εκτυπωτές είτε σε εκτυπωτές που βρίσκονται κοντά μας αρκεί να ρυθμίσουμε στο απομακρυσμένο σύστημα τις παραμέτρους και τις διευθύνσεις για τους εκτυπωτές αυτούς στους οποίους έχουμε πρόσβαση.

Μια πολύ χρήσιμη λειτουργία που έχει προστεθεί στις τελευταίες εκδόσεις του pcAnywhere είναι και η περιμετρική έρευνα για συστήματα απομακρυσμένης πρόσβασης (Remote Access Perimeter Scanner - RAPS) Επειδή είναι πολύ εύκολο σε τέτοια συστήματα να εισέλθουν διάφοροι ανεπιθύμητοι χρήστες και εκτός από το να δουν απόρρητες πληροφορίες, μπορούν να καταστρέψουν και ολόκληρα συστήματα, το RAPS σαρώνει όλο το δίκτυο και βρίσκει τα επικίνδυνα σημεία πρόσβασης. Μπορεί να ελέγξει και με dial-up κλήσεις τηλεφωνικά νούμερα που αντιστοιχούν σε remote access servers. Για κάθε pcAnywhere host με χαμηλό επίπεδο ασφάλειας που ανακαλύπτει μπορεί αυτόματα να διακόψει τη λειτουργία του. Μετά από κάθε έλεγχο του δικτύου το RAPS εμφανίζει ένα log-file με όλους τους απομακρυσμένους servers είτε αυτοί τρέχουν κάποια έκδοση του pcAnywhere είτε κάποιο άλλο αντίστοιχο software άλλων (ανταγωνιστών της Symantec) εταιρειών όπως:

- LapLink 2000, version 3.01
- Carbon Copy, version 5.5
- Timbuktu Pro 32, version 3.0
- ReachOut, version 8.3
- NetSupport/PcDuo, version 5.03
- NetMeeting, version 3.01
- VNC, version 3.3.3
- NetBus Pro, version 2.0.
- PPP Ras Server
- Windows Dial-Up Server
- Terminal Server for NT4
- Citrix Server
- X Server, version 11

Γενικά γίνεται πολύ μεγάλη προσπάθεια στο θέμα της ασφάλειας γιατί από τη φύση τους αυτά τα προγράμματα έχουν ριψοκίνδυνες επιλογές. Το pcAnywhere χρησιμοποιεί ένα συνδυασμό τριών μεθόδων αποκρυπτογράφησης για να μπορέσει να πετύχει αυξημένη ασφάλεια, αξιοπιστία και ταχύτητα

Λειτουργικό σύστημα - Απαιτήσεις

Το pcAnywhere τρέχει σε Windows 9x, Windows Millennium Edition (ME), Windows NT, and Windows 2000 και χρειάζεται μόνο αυτούς τους πόρους για να λειτουργήσει σωστά.

Αξιολόγηση

Αναμφίβολα είναι το καλύτερο πρόγραμμα στο είδος του. Φυσικά και η εταιρεία που το διαθέτει (Symantec) τώρα είναι ανάμεσα στις πρώτες στον κόσμο εταιρείες στην παραγωγή software. Η δοκιμαστική έκδοση του προγράμματος με περιορισμένες δυνατότητες και χρονολογική ισχύ διατίθεται από το site της Symantec και είναι περίπου 35 Mbytes! Η τιμή του εμπορικού πακέτου αν λάβουμε υπ' όψιν τη φήμη του προγράμματος αλλά και την αξιοπιστία της Symantec θα τη χαρακτηρίζαμε φυσιολογική.

	NeoTrace Pro	
Έκδοση	3.25 (2001)	
Εταιρεία	NeoWorx McAfee	
Τιμή	\$29.95	

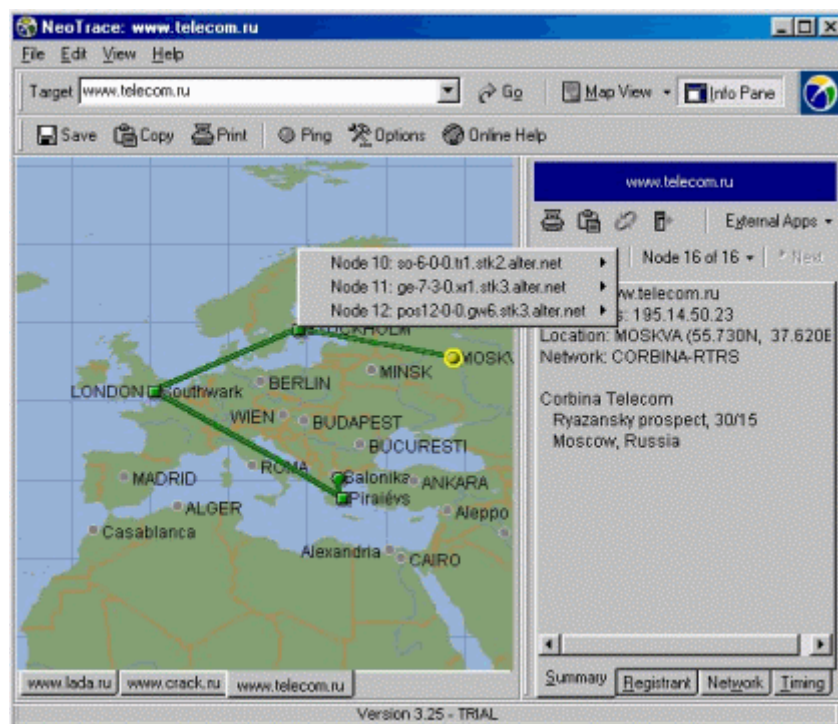
Χαρακτηριστικά

- Tracerouting
- Απεικόνιση σε χάρτη
- Ανάκτηση επιπλέον πληροφοριών για κάθε κόμβο

Περιγραφή

Το NeoTrace είναι ένα διαγνωστικό και διερευνητικό πρόγραμμα. Ακολουθεί όλη τη διαδρομή από υπολογιστή σε υπολογιστή (trace) μέσω internet από τον host στον οποίο βρισκόμαστε και εκτελούμε το πρόγραμμα μέχρι οποιοδήποτε (target) σύστημα οπουδήποτε στον κόσμο αρκεί να είναι online συνδεδεμένο στο internet. Αυτό που πρέπει να ξέρουμε είναι είτε το IP είτε το domain name του target συστήματος.

Βέβαια όλα αυτά τα κάνει οποιοδήποτε αντίστοιχο πρόγραμμα όπως και σε λειτουργικά συστήματα τύπου UNIX μια απλή εντολή τύπου «trace» σε command line. Αυτό όμως που κάνει το NeoTrace να ξεχωρίζει είναι το γεγονός ότι για κάθε ενδιαμέσο υπολογιστή (IP) μπορεί να ανακαλύψει διάφορα καταχωρημένα στοιχεία για τον ιδιοκτήτη ή τον διαχειριστή του συγκεκριμένου υπολογιστή. Μπορεί λοιπόν να δώσει πληροφορίες όπως όνομα, διεύθυνση, τηλέφωνο ή email του διαχειριστή ή του οργανισμού στον οποίο έχει καταχωρηθεί το κάθε “node IP”. Επιπλέον συνδέει τον τόπο (πόλη) που βρίσκεται ο υπολογιστής με έναν παγκόσμιο χάρτη και δείχνει έτσι πολύ παραστατικά τη διαδρομή αλλά και τις σχετικές καθυστερήσεις που μπορεί να υπάρχουν σε κάποια πιο “αργά” τμήματά της.



Μπορούμε έτσι να δούμε τις διαδρομές που μας υποχρεώνουν να ακολουθήσουμε οι διάφοροι DNS servers που πολλές φορές δεν είναι και οι καλύτερες δυνατότες. Το NeoTrace είναι δημοφιλές σε απλούς χρήστες που προσπαθούν να διαγνώσουν μόνοι τους διάφορα προβλήματα σύνδεσης που τους παρουσιάζονται. Εξάλλου πολλοί Internet Service Providers το συστήνουν στους πελάτες τους και το χρησιμοποιούν και οι ίδιοι. Σύμφωνα με την ίδια την NeoWorx το πρόγραμμα χρησιμοποιείται από διάφορες υπηρεσίες δίωξης εγκλήματος σε όλον τον κόσμο, από την τελωνιακή υπηρεσία των Ηνωμένων Πολιτειών και το NATO. Διδάσκεται σε κύκλους σπουδών της ακαδημίας του FBI και είναι το πρόγραμμα με το οποίο πολλοί τηλεοπτικοί σταθμοί παρουσιάζουν τα προβλήματα διακίνησης παράνομου υλικού μέσω Internet.

Η δοκιμαστική έκδοση του προγράμματος με περιορισμένη και χρονολογική ισχύ διατίθεται από το site της NeoWorx και της McAfee που την έχει αγοράσει πρόσφατα.

Λειτουργικό σύστημα – Απαιτήσεις

Ένας κοινός υπολογιστής που δουλεύει σε περιβάλλον Windows 95, 98, 98SE, NT4, 2000, ME ή XP αρκεί να έχει μια non-proxy σύνδεση στο Internet. Αυτή μπορεί να είναι dial-up, cable, DSL ή LAN. Σε περίπτωση που η σύνδεση γίνεται πίσω από κάποιο firewall πρέπει αυτό να ρυθμιστεί στο να επιτρέπει traceroute και ping.

Πρέπει επίσης να είναι εγκατεστημένος και το Internet Explorer έκδοσης 4.0 ή νεώτερης, χωρίς κατ' ανάγκη να έχει οριστεί σαν βασικός, διότι το πρόγραμμα χρησιμοποιεί κάποιους πόρους του.

Αξιολόγηση

Πέρα, πάντως, από το γεγονός ότι πρόκειται απλά για ένα monitoring tool με αρκετά συγκεκριμένες δυνατότητες το NeoTrace αποτελεί έναν γρήγορο τρόπο να πάρουμε μια σύντομη περιγραφή μιας σύνδεσης και με την ευκολία της αυτόματης ανάκτησης πληροφοριών που το διακρίνει, έχει γίνει ένα πολύ καλό εργαλείο και για έμπειρους αλλά και για νέους χρήστες.

	Select-a-Net	
Έκδοση	3.2.0 (2001)	
Υπεύθυνος	Jeffrey S. Bramwell Ut-Zone	
Τιμή	\$8.00	

Χαρακτηριστικά

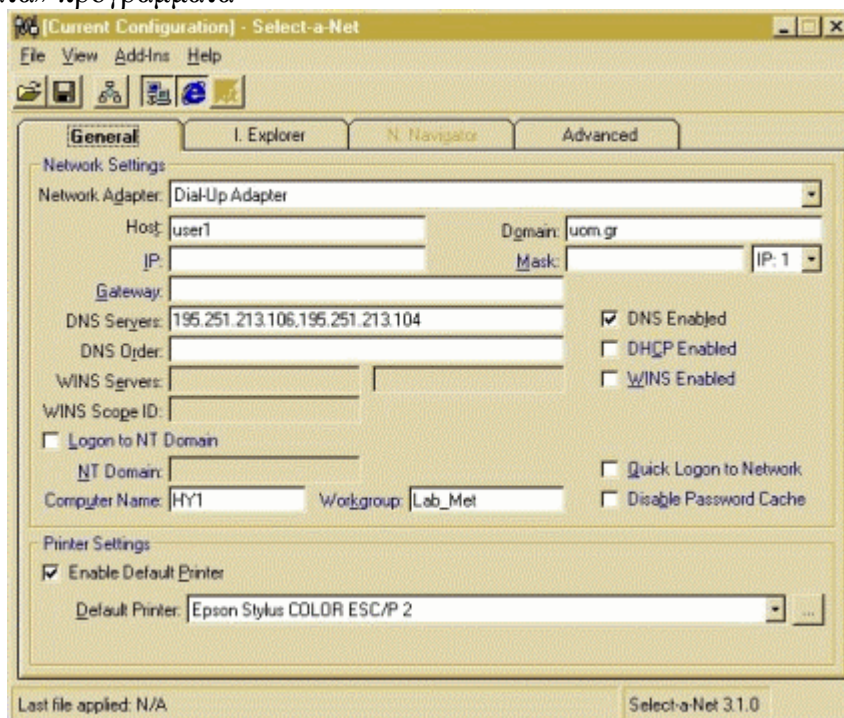
- Γρήγορη εναλλαγή ρυθμίσεων δικτύου
- Πολύ χρήσιμο για φορητούς υπολογιστές
- Εύκολη αποθήκευση των set των ρυθμίσεων στους browsers

Περιγραφή

Το Select-a-Net είναι ένα πρόγραμμα που μπορεί να εναλλάσσει τις ρυθμίσεις στους browsers και σε άλλα εργαλεία του internet πολύ εύκολα. Αυτό γίνεται αποθηκεύοντας τις εκάστοτε ρυθμίσεις των προγραμμάτων σε ειδικά αρχεία από τα οποία εύκολα μπορούν να ξαναφορτωθούν στα συγκεκριμένα προγράμματα. Έτσι δεν είναι υποχρεωτικό να επανεκκινήσουμε τον υπολογιστή για να ισχύσουν οι αλλαγές των ρυθμίσεων.

Αυτό είναι πολύ χρήσιμο για φορητούς υπολογιστές που συνδέονται σε διαφορετικά δίκτυα και πρέπει κάθε φορά να εναλλάσσουν τις ρυθμίσεις σε πολλά προγράμματα και στο ίδιο το λειτουργικό σύστημα για να μπορέσουν να «δουν» το δίκτυο. Υποστηρίζει τα Windows 95/98/NT κυρίως στο TCP/IP πρωτόκολλο.

Απλό πρόγραμμα με εύκολο γραφικό περιβάλλον χωρίς τις πολλαπλές λειτουργίες που είχαν κάποια από τα προηγούμενα προγράμματα που περιγράψαμε παραπάνω αλλά και χωρίς επιπλέον άλλες δυνατότητες monitoring η managing που είδαμε στα πιο «δυνατά» προγράμματα



Λειτουργικό σύστημα – Απαιτήσεις

Δουλεύει σε Windows 95/98/NT 4.0, ενώ αναμένεται και η έκδοση που θα δουλεύει και στις νεότερες εκδόσεις των Windows. Άλλες ιδιαίτερες απαιτήσεις σε Hardware ή Software δεν υπάρχουν

Αξιολόγηση

Ο σκοπός για τον οποίο έγινε το Select-A-Net είναι από μόνος του ένας βασικός παράγοντας για να είναι ένα περιζήτητο εργαλείο. Εξάλλου είναι στις πρώτες προτιμήσεις των χρηστών στα μεγάλα site διακίνησης software όπως το tucows και το ZDnet. Πέρα από αυτό όμως οι δυνατότητες του είναι περιορισμένες και συγκεκριμένες και δεν μπορεί να συγκριθεί με τα μεγάλα προγράμματα που περιγράψαμε παραπάνω.

	Security Manager	
Έκδοση	3.3 (2001)	
Εταιρεία	NetIQ	
Τιμή	\$900	

Χαρακτηριστικά

- Κεντρική διαχείριση από ένα σημείο για την ασφάλεια του συστήματος
- Διαχείριση θεμάτων ασφαλείας σε πραγματικό χρόνο (με έλεγχο σε πραγματικό χρόνο και αυτοματοποιημένη ανταπόκριση συμβάντων)
- Αναφορές ασφαλείας των Firewall
- Host-based έλεγχος παραβιάσεων ασφαλείας
- Διαχείριση πολιτικών ασφαλείας
- Αναγνώριση ευπρόσβλητων σημείων
- Διαχείριση ασφάλειας χρηστών
- Διαχείριση ασφάλειας αρχείων

Περιγραφή

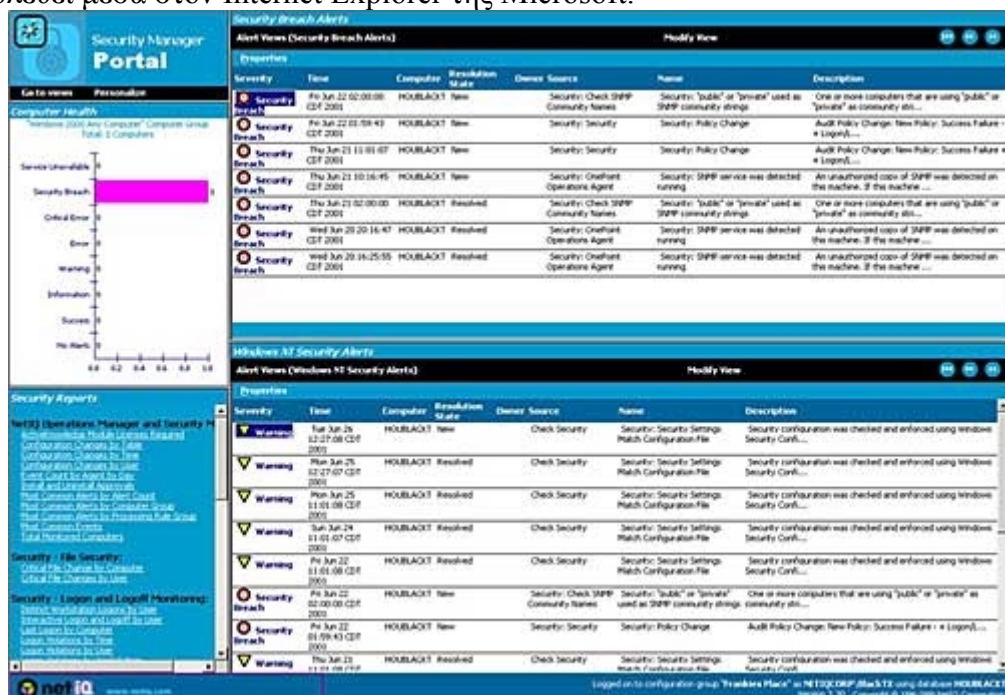
Σχεδιάστηκε για τα Windows 2000/NT και είναι ένα πολύ καλό εργαλείο που παρέχει εκτενείς αναφορές που βοηθούν στην τεκμηρίωση και έρευνα ρηγμάτων ασφαλείας σε πραγματικό χρόνο. Διαχειρίζεται το ίδιο καλά θέματα ασφαλείας χρηστών όπως και αρχείων.

Έχει αρκετές επιλογές πάνω σε θέματα ασφάλειας των δικτύων που είναι βασισμένα σε Windows λειτουργικά συστήματα. Αποτελείται από πολλά τμήματα το βασικότερο από αυτά εγκαθίσταται στον κεντρικό Windows NT/2000 server και τα υπόλοιπα agent managers εγκαθίστανται στους υπόλοιπους servers που θέλουμε να παρακολουθήσουμε.

Μας επιτρέπει να μαζέψουμε να συγκρίνουμε και να αξιολογήσουμε πληροφορίες θεμάτων ασφαλείας που προέρχονται από άλλα προγράμματα όπως anti-virus ή firewall έχοντας έτσι έναν κεντρικό έλεγχο για την ασφάλεια του συστήματός μας.

Χρησιμοποιεί τον Microsoft SQL server για να υποστηρίξει όλη τη δουλειά της βάσης δεδομένων που δημιουργείται εξασφαλίζοντας έτσι την δυνατότητα επεκτασιμότητας για μεγάλα συστήματα.

Η εγκατάσταση του προγράμματος μπορεί να γίνει αυτοματοποιημένα και πού γρήγορα και το ίδιο απλός φαίνεται να είναι και ο χειρισμός του. Αυτός βασίζεται στο Microsoft Management Console (MMC) που μοιάζει πολύ με Web περιβάλλον και δουλεύει μέσα στον Internet Explorer της Microsoft.



Σύμφωνα με την τεχνολογία ActiveKnowledge module που υποστηρίζει υπάρχουν με την εγκατάσταση προκαθορισμένες επιλογές, scripts, ομάδες αναφορών και επισημάνσεων, έτσι όλο το σύστημα μπορεί να ανταποκριθεί πολύ γρήγορα σε οποιοδήποτε πρόβλημα ασφαλείας προκύψει κάνοντας από μόνο του τις απαραίτητες ενέργειες που χρειάζονται σε κάθε περίπτωση. Φυσικά ο καθορισμός όλων αυτών των ενεργειών μπορεί να τροποποιηθεί από το διαχειριστή του συστήματος ο οποίος βέβαια βοηθιέται πολύ από την υπάρχουσα αυτοματοποίηση.

Συμφωνά με τις προδιαγραφές του Security Manager μπορεί να ελέγξει μέχρι και 30 εκατομμύρια συμβάντα ημερησίως με χρονική διαφορά συλλογής λιγότερο του δευτερολέπτου αποδεικνύοντας έτσι την άμεση και ταχύτατη ανταπόκρισή του.

Η δοκιμαστική έκδοση του προγράμματος είναι αρκετά μεγάλη (101Mb) και διατίθεται από το site της NetIQ είναι όμως προστατευμένη και αυτή με password το οποίο δίνεται μετά από τηλεφωνική επικοινωνία με την εταιρεία μαζί με κάποιες σύντομες οδηγίες για την εγκατάσταση και σωστή λειτουργία του προγράμματος.

Λειτουργικό σύστημα – Απαιτήσεις

Ελάχιστες απαιτήσεις για έναν server που να μπορεί να υποστηρίξει πάνω από 25 agents είναι 300MHz Pentium III με 256Mb RAM και 800Mb ελεύθερο σκληρό δίσκο, που να τρέχει NT4 P6a ή Windows 2000. Μελλοντικοί στόχοι της εταιρείας είναι να βγάλει σύντομα έκδοση που να τρέχει και σε Sun Solaris, HP-UX, AIX και Red Hat Linux

Αξιολόγηση

Το γεγονός ότι δεν μπορεί να υποστηρίξει Unix συστήματα είναι ίσως το μόνο μειονέκτημα του κατά τα άλλα πολύ καλού προγράμματος για έλεγχο και ενημέρωση σε θέματα ασφαλείας δικτύου. Η αυτοματοποίηση που το διακρίνει γλιτώνει από πού

δουλειά τους διαχειριστές των συστημάτων και με αυτόν το τρόπο η διαχείριση μπορεί να γίνει και από έναν απλό χρήστη.

	SwitchIP Professional TCP/IP Network Switch for Windows 98/95/NT/2000	
Έκδοση	2.1 (2000)	
Σχεδίαση Ανάπτυξη	Michael S. Andrews, Dasz Garncarz	
Τιμή	\$19.95	

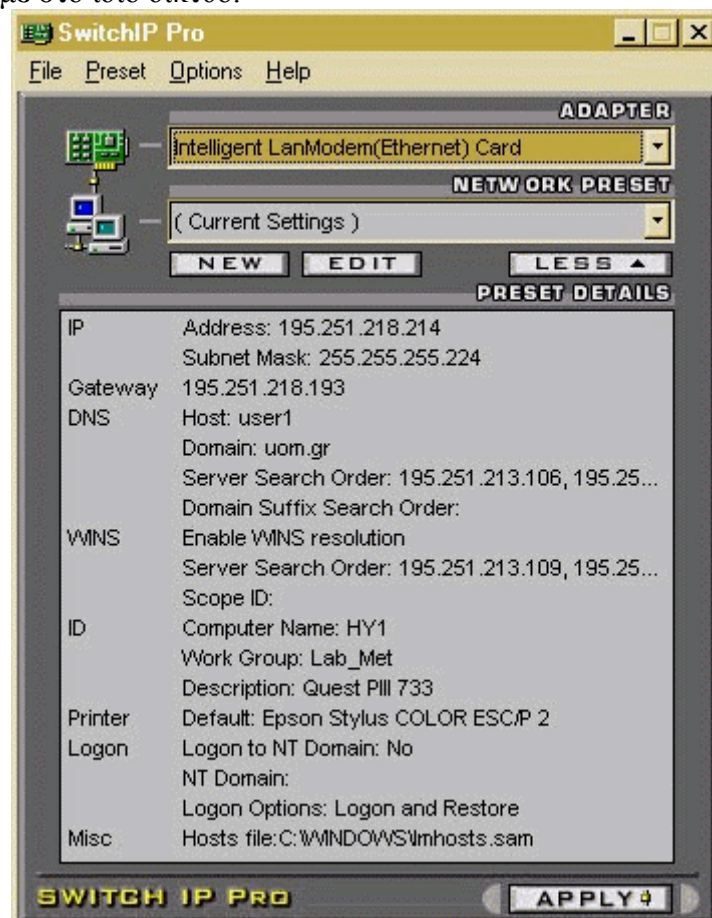
Χαρακτηριστικά

- Αποθήκευση ρυθμίσεων δικτύου
- Χρήσιμο για υπολογιστές που συνδέονται σε διαφορετικά δίκτυα

Περιγραφή

Το SwitchIP είναι ένα ακόμα πολύ χρήσιμο εργαλείο που γλιτώνει από πολύ βαρετή δουλειά διαχειριστές αλλά και απλούς χρήστες δικτύων όταν αλλάζουν συχνά δίκτυο και πρέπει να ξαναρυθμίζουν από τη αρχή IP διευθύνσεις, ονόματα χρηστών, ομάδων εργασίας και υπολογιστών, εκτυπωτές, password κλπ.

Με ένα πολύ απλό μενού κάθε φορά που πρωτορυθμίζονται όλες οι παραπάνω λεπτομέρειες, φτιάχνεται ένα αρχείο ρυθμίσεων το οποίο φορτώνεται αυτόματα όταν ξανασυνδεθούμε στο ίδιο δίκτυο.



Απλό πρόγραμμα με εύκολο γραφικό περιβάλλον χωρίς τις πολλαπλές λειτουργίες που είχαν κάποια από τα προηγούμενα προγράμματα που περιγράψαμε παραπάνω αλλά και χωρίς επιπλέον άλλες δυνατότητες monitoring η managing που είδαμε στα πιο «δυνατά» προγράμματα.

Η δοκιμαστική του έκδοση υπάρχει στο ομώνυμο site αλλά και στα περισσότερα site με shareware προγράμματα

Λειτουργικό σύστημα – Απαιτήσεις

Δουλεύει σε Windows 95/98/NT/2000 και μόνο με βάση το TCP/IP πρωτόκολλο. Ειδικότερα για τα NT/2000 πρέπει ο χρήστης να έχει το δικαίωμα πρόσβασης read/write στο μητρώο (registry). Από πλευράς hardware το πρόγραμμα μπορεί να δουλέψει σε οποιοδήποτε Pentium ή νεώτερο υπολογιστή

Αξιολόγηση

Έχουμε και εδώ (όπως στο Select-A-Net) ένα εργαλείο χρήσιμο σε διαχειριστές δικτύου που δεν έχει όμως άλλες δυνατότητες πέρα από την εναλλαγή ρυθμίσεων δικτύου που είναι και ο σκοπός του. Όσο καλό και να είναι το SwitcIP, η διαχείριση ενός δικτύου δεν μπορεί να γίνει μόνο με ένα τέτοιο πρόγραμμα

	IP Ultra Monitor 2000
Έκδοση	2.4.4 (2000)
Εταιρεία	Ultrajones software
Τιμή	FREEWARE

Χαρακτηριστικά

- Προβολή σε γραφικό περιβάλλον της κατάστασης συσκευών του δικτύου
- Έλεγχος TCP υπηρεσιών (FTP, NNTP, SMTP, HTTP) απομακρυσμένων συσκευών.
- Καταγραφή αποτυχημένων συνδέσεων
- Έξοδος σε HTML μορφή
- Υποστήριξη βάσης δεδομένων σε Microsoft Access για καταγραφή και επεξεργασία των στοιχείων που καταγράφονται
- Δυνατότητα ping σε απομακρυσμένες συσκευές πολλές φορές για προσδιορισμό της κατάστασης
- Υποστήριξη με Wizards για τον έλεγχο νέων συσκευών

Περιγραφή

Το IP Ultra Monitor 2000 είναι ένα πρόγραμμα για παρακολούθηση σε γραφικό περιβάλλον των TCP/IP ports (π.χ. http, ftp, smtp, dns) σε απομακρυσμένους servers με τη βοήθεια του Πρωτοκόλλου Διασυνδεδετικού Μηνύματος Ελέγχου (Interface Control Message Protocol - ICMP) ping.



Για κάποια απομακρυσμένη συσκευή μπορούμε να καθορίσουμε τα ports που θέλουμε να ελέγξουμε και να έχουμε μια σαφή εικόνα του τι συμβαίνει σε καθένα από αυτά. Για παράδειγμα αν ορίσουμε το TCP port 80 μπορούμε να ελέγξουμε αν δουλεύει σωστά ένας web server.



Ένα από τα δυνατά σημεία του προγράμματος είναι η δυνατότητα να ελέγχει απομακρυσμένες συσκευές κάθε 1 έως 60 λεπτά (αυτό καθορίζεται από το χρήστη). Αποτυπώνει τα τελευταία μηνύματα λάθους καθώς και τον αριθμό των επιτυχημένων και αποτυχημένων συνδέσεων. Υπάρχει επιλογή για να ξαναστέλνει μηνύματα e-mail που απέτυχαν ανά τακτά χρονικά διαστήματα τα οποία μπορεί επίσης να καθορίσει ο χρήστης. Με τη χρήση κατάλληλων wizards μπορούμε να δημιουργήσουμε λίστες με συσκευές και ports που θέλουμε να παρακολουθήσουμε. Έτσι πολλά προβλήματα μπορούν να ανιχνευθούν και να εμφανιστούν σε HTML έξοδο. Το πρόγραμμα χρησιμοποιεί την τεχνολογία Microsoft Agent και είναι γραμμένο σε Visual Basic 6.0

Λειτουργικό σύστημα – Απαιτήσεις

Απαραίτητη είναι μια Internet ή Intranet σύνδεση οποιασδήποτε μορφής (dial-up / cable modem / ISDN κλπ.) και λειτουργικό Windows 95, 98, NT 4 ή 2000 με εγκατεστημένα το TCP/IP και τις βασικές βιβλιοθήκες της Visual Basic 6.0 και το Microsoft Agent 2.0 (Τα παραπάνω συνήθως είναι ήδη εγκατεστημένα στα

περισσότερα Windows συστήματα από άλλα προγράμματα, ή μπορούν να κατεβαστούν ελεύθερα από το site της Microsoft)

Αξιολόγηση

Αρκετά καλό εργαλείο για monitoring μέσω internet χρήσιμο όχι μόνο για διαχειριστές δικτύων αλλά και για απλά περιέργους χρήστες. Το γεγονός ότι είναι ακόμα freeware σημαίνει ότι η πρώτη κανονική έκδοσή του θα είναι πολύ καλύτερη και θα αποτελεί ένα πολύ ανταγωνιστικό στο είδος του πρόγραμμα

	Netcop Scanner	
Έκδοση	2.0 (1998)	
Εταιρεία	Netcop Software	
Τιμή	FREWARE	

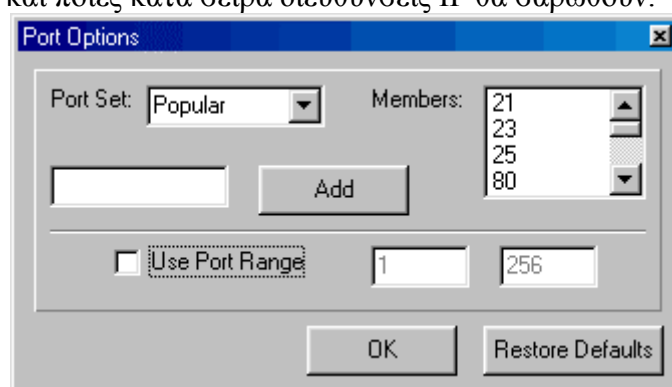
Χαρακτηριστικά

- Αναγνώριση προβλημάτων ασφαλείας σε servers ή οποιοδήποτε άλλο IP-συνδεδεμένο σύστημα.
- Δυνατότητα επιλογής ταχύτητας του δικτύου
- Δυνατότητα πολλαπλής έρευνας υπολογιστών και δικτύων.
- Χρήσιμες αναφορές.

Περιγραφή

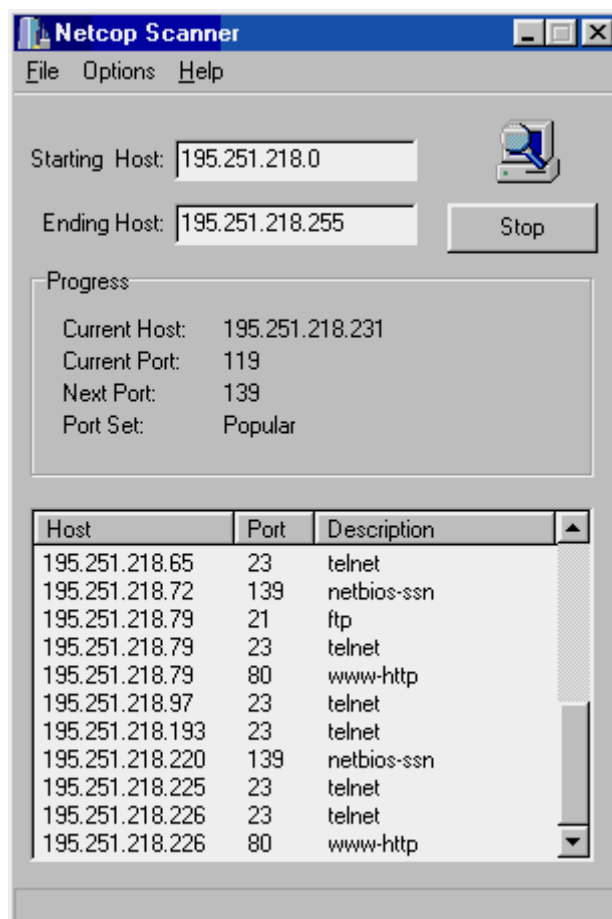
Το Netcop Scanner είναι ένα εργαλείο ανάλυσης της ασφάλειας συστημάτων και χρησιμοποιείται από τους διαχειριστές αλλά και από απλούς χρήστες (πιθανόν και από hackers) για να ανακαλύπτει κενά ασφαλείας σε servers και PCs..

Έχει την ικανότητα να σαρώνει πολλούς υπολογιστές και δίκτυα ελέγχοντας όλα τα ports που είναι ενεργά. Υπάρχει επιλογή για το ποια (αν όχι όλα) τα ports που θα ελεγχθούν αλλά και ποιες κατά σειρά διευθύνσεις IP θα σαρωθούν.



Εμφανίζεται έτσι μια λίστα με τα ενεργά ports με τις αντίστοιχες λειτουργίες τους και τις IP διευθύνσεις στις οποίες ανήκουν.

Έτσι ένας διαχειριστής μπορεί να ελέγξει εξονυχιστικά όλα τα ports όλων των υπολογιστών του δικτύου αλλά και ένας home-user (ενώ είναι συνδεδεμένος στο internet) όλα τα ports του δικού του υπολογιστή για να διαπιστώσουν αν υπάρχουν πιθανότητες παραβίασης της ασφάλειας των συστημάτων τους.



Υπάρχει η δυνατότητα αποθήκευσης σε φόρμα των επιλογών που κάνουμε κάθε φορά ώστε να μην επιλέγουμε συνέχεια τι έλεγχο θέλουμε να κάνουμε. Μπορούμε επίσης να αποθηκεύουμε και τα αποτελέσματα που παίρνουμε σε ένα απλό αρχείο κειμένου ή με μορφή στοίχισης για περαιτέρω ανάλυση και επεξεργασία.

Λειτουργικό σύστημα – Απαιτήσεις

Φτιάχτηκε για γραφικό περιβάλλον Windows95/98/NT. Τρέχει όμως και στις νεώτερες εκδόσεις των Windows, ένας λόγος για το ότι δεν έχει βγει νεώτερη έκδοση από αυτή του 1998.

Αξιολόγηση

Ένα Freeware πρόγραμμα από μια εταιρεία (Netcop) που κατά τα άλλα προωθεί στην αγορά πολλά δυνατότερα προγράμματα για ασφάλεια και διαχείριση δικτύου. Σίγουρα είναι πολύ χρήσιμο εργαλείο για τον έλεγχο της ασφάλειας των συστημάτων μας, αυτό όμως μπορεί να γίνει boomerang γιατί και οι άλλοι μπορούν να ελέγξουν μέσω αυτού του εργαλείου την ασφάλεια των συστημάτων μας πριν από εμάς.

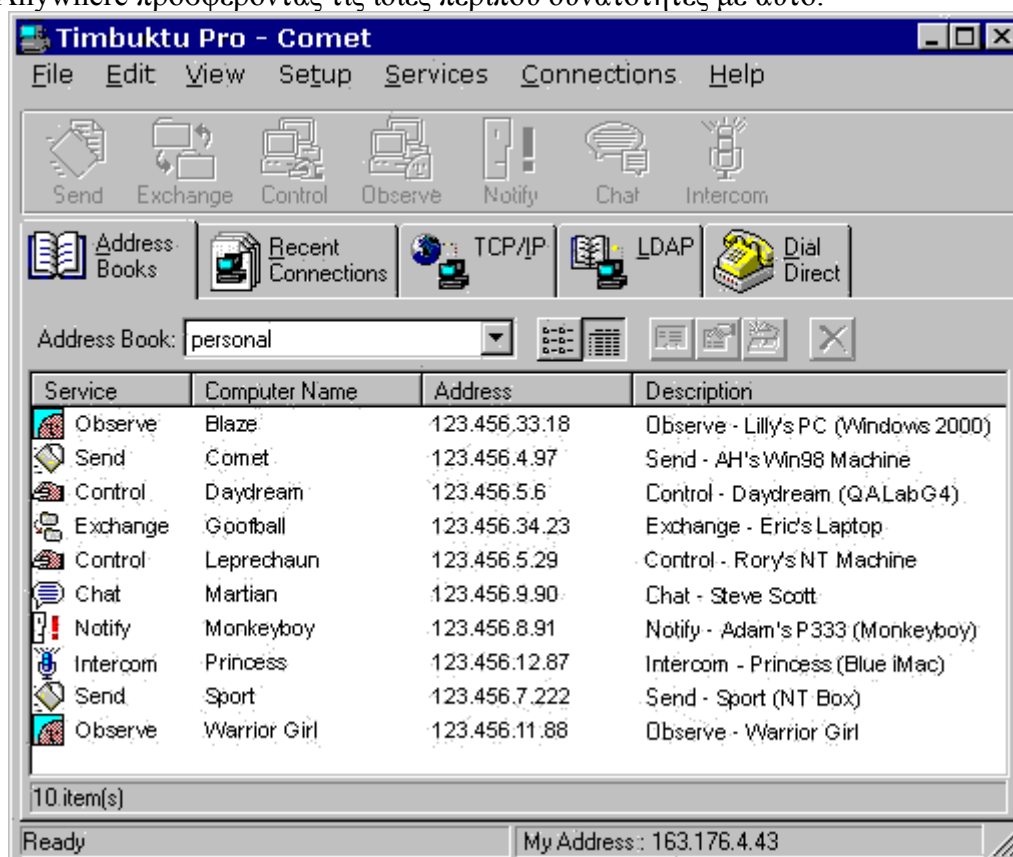
	Timbuktu Pro 2000	
Έκδοση	(2001)	
Εταιρεία	Netopia	
Τιμή	159.95 (έκδοση για Windows2000) και για δύο υπολογιστές	

Χαρακτηριστικά

-  Αποστολή (send) μηνυμάτων με επισυναπτόμενα αρχεία σε απομακρυσμένο υπολογιστή
-  Πρόσβαση σε άλλους σκληρούς δίσκους – ακόμα και Macintosh – και Διαχείριση αρχείων (αντιγραφή, μεταφορά, διαγραφή) μεταξύ διαφορετικών υπολογιστών από οποιονδήποτε από αυτούς (exchange)
-  Έλεγχος (control) ή απλή παρατήρηση απομακρυσμένου υπολογιστή από άλλη επιφάνεια εργασίας
-  Ειδοποίηση (notify) όταν κάποιος απομακρυσμένος υπολογιστής έχει γίνει ενεργός
-  Επικοινωνία (chat) ή
-  συνομιλία (voice) με το χρήστη του απομακρυσμένου υπολογιστή (intercom)

Περιγραφή

Το Timbuktu Pro 2000 της Netopia έχει γίνει ένας πολύ σημαντικός αντίπαλος του pcAnywhere προσφέροντας τις ίδιες περίπου δυνατότητες με αυτό.

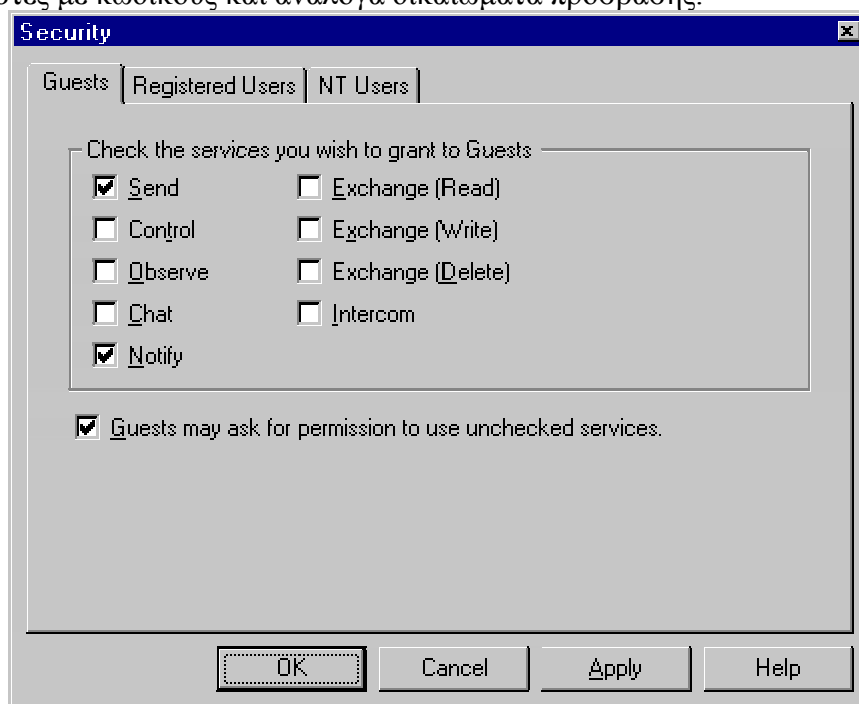


Με ένα λίγο διαφορετικό Interface μπορούμε και εδώ να συνδεθούμε σε απομακρυσμένους υπολογιστές και να έχουμε την επιφάνεια εργασίας τους στην

οθόνη του δικού μας υπολογιστή μέσα σε ένα παράθυρο. Μπορούμε να ανταλλάξουμε, αρχεία να τρέξουμε προγράμματα, και να αλλάξουμε ρυθμίσεις στον απομακρυσμένο υπολογιστή όπως και να συνομιλήσουμε με το χρήστη του ακόμα και με ήχο κάνοντας χρήση του ανάλογου hardware που συνήθως έχουν και οι δύο υπολογιστές. Όλα αυτά γίνονται σε πραγματικό χρόνο (ή περίπου πραγματικό όταν τα πρωτόκολλα και οι συνδέσεις δεν το επιτρέπουν).

Υπάρχει βιβλίο διευθύνσεων με τα χαρακτηριστικά κάθε σύνδεσης που έχει γίνει ή σκοπεύει να γίνει στο μέλλον και ειδική επιλογή για διερεύνηση άλλων συνδέσεων που είναι δυνατόν να επιτευχθούν.

Για το θέμα της ασφάλειας υπάρχουν αρκετές ρυθμίσεις ώστε να υπάρχει σε πολλά επίπεδα και να μπορεί να επιλέγει ο χρήστης το βαθμό της. Μπορούν να καθοριστούν έτσι χρήστες με κωδικούς και ανάλογα δικαιώματα πρόσβασης.



Υπάρχουν οι δυνατότητες από το χρήστη του απομακρυσμένου υπολογιστή να μπορεί να ελέγχει τις συνδέσεις που έχουν γίνει στο δικό του υπολογιστή, να απαγορεύει αν το θελήσει συνδέσεις που πρόκειται να γίνουν ή να διακόπτει αυτήν που είναι ήδη σε εξέλιξη.

Η δοκιμαστική για 30 ημέρες διατίθεται και εδώ από το site της και εταιρείας και από τα γνωστά site που είδη έχουμε αναφέρει.

Λειτουργικό σύστημα – Απαιτήσεις

Εκτός από όλα τα Windows λειτουργικά συστήματα υπάρχει και έκδοση για υπολογιστές Macintosh. Μπορεί μάλιστα μέσω του Timbuktu Pro να γίνει και σύνδεση PC-MAC υπολογιστών με πολύ ενδιαφέροντα και εντυπωσιακά αποτελέσματα.

Η επικοινωνία των υπολογιστών δεν προϋποθέτει την ύπαρξη δικτύου εφόσον μπορεί να γίνει και με κατευθείαν modem-to-modem σύνδεση.

Αξιολόγηση

Ακόμα ένα πολύ καλό πρόγραμμα για έλεγχο και διαχείριση απομακρυσμένων υπολογιστών. Συγκρινόμενο με το pcAnywhere που παρουσιάσαμε παραπάνω έχει πολλά κοινά και βρίσκεται πολύ κοντά αλλά μάλλον το ακολουθεί. Αυτό συμβαίνει και στην τιμή τους αλλά όχι και στον όγκο του προγράμματος (Η δοκιμαστική έκδοση του Timbuktu Pro 2000 είναι μόνο 6.5Mbytes ενώ όπως έχουμε αναφέρει η αντίστοιχη για το pcAnywhere 10.5 είναι 35Mbytes)

	Monet LAN Analyzer	
Έκδοση	V2.21 PD (packet driver) (1997)	
Εταιρεία	MG-SOFT (Slovenia) ABIT (Japan)	
Τιμή	\$900,00	

Χαρακτηριστικά

- Παρακολούθηση σε πραγματικό χρόνο
- Αποκωδικοποίηση πολλών πρωτοκόλλων
- Κατηγοριοποίηση πακέτων (με διαγράμματα)
- Δημιουργία τεχνητού φόρτου
- Φιλτράρισμα σε πολλαπλά επίπεδα

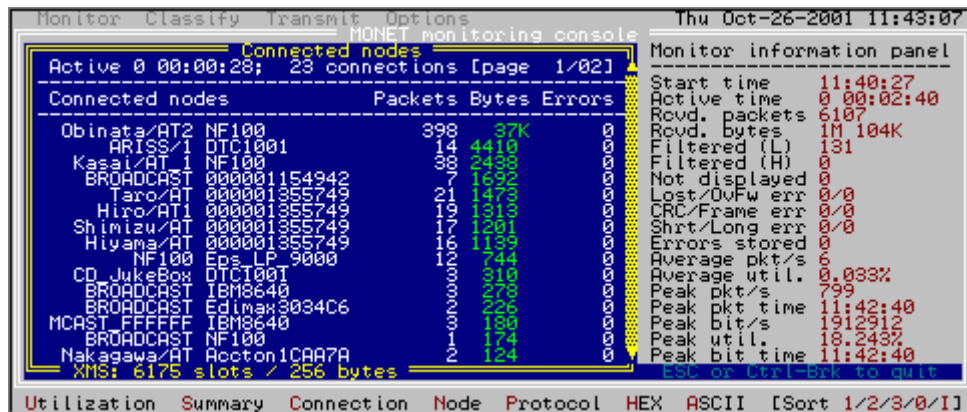
Περιγραφή

Το Monet LAN Analyzer είναι ένα από τα παλαιότερα και σπουδαία πακέτα εργαλείων για τον έλεγχο της ροής των δεδομένων σε ένα τοπικό δίκτυο. Περιέχει αρκετά ισχυρά εργαλεία που προσφέρουν πλήρη υποστήριξη στους διαχειριστές και τεχνικούς δικτύων καθώς επίσης και στους προγραμματιστές εφαρμογών δικτύου. Έτσι βοηθά στη αύξηση της παραγωγικότητας και στη βελτίωση της λειτουργίας του δικτύου μειώνοντας αισθητά το χρόνο που χάνεται όταν το δίκτυο δε δουλεύει σωστά.

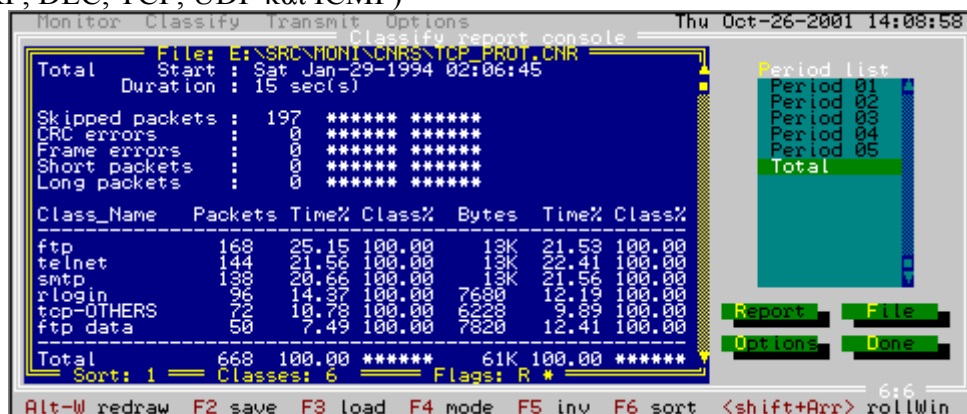
Μερικά από τα εργαλεία που υπάρχουν στο πακέτο της κανονική έκδοσης είναι τα παρακάτω:

- ADMIN – Το βασικό πρόγραμμα διαχείρισης του Monet LAN Analyser
- SPY – Εργαλείο για έλεγχο των Ethernet κόμβων
- NEWALIAS, ETH2CCS, IP2CCS – Διάφοροι μετατροπείς αρχείων
- MGREP, MTYPE – Browsers αρχείων δεδομένων
- MGP - MONET Graph Painter – Πρόγραμμα γραφικών παρουσιάσεων
- MLOG - LAN – Πρόγραμμα καταγραφής συμβάντων

Η παρακολούθηση γίνεται σε πραγματικό χρόνο με διάφορους τρόπους. Ανάλογα με τις παραμέτρους που θα δώσουμε μπορούμε να έχουμε ανά πολύ μικρά χρονικά διαστήματα πληροφορίες όπως τον όγκο της ροής των δεδομένων και πού αυτός αντιστοιχεί, τις χρονικές στιγμές που συμβαίνουν συγκεκριμένα γεγονότα, τις καθυστερήσεις που παρουσιάζονται, τις μέσες και ανώτερες τιμές χαρακτηριστικών μεγεθών καθώς και την καταμέτρηση των σφαλμάτων που παρουσιάζονται.



Υποστηρίζει τα πρωτόκολλα IEEE 802.2 (LLC and SNAP), IEEE 802.3 (Novell IPX) και Ethernet II και μπορεί έτσι να ανιχνεύει και να κατηγοριοποιεί τα πλαίσια που αντιστοιχούν σε αυτά. Με κατάλληλα φίλτρα ελέγχει όλα τα πακέτα και παρουσιάζει χρήσιμα στατιστικά για το περιεχόμενό τους. Συγκεκριμένα μπορεί να αποκωδικοποιήσει πακέτα από διάφορα επίπεδα με πρωτόκολλα όπως (IP, ARP, RARP, DLC, TCP, UDP και ICMP)



Μια ακόμα ενδιαφέρουσα λειτουργία του είναι το «Traffic generation» με το οποίο κατασκευάζει μόνο του διάφορα πακέτα, το είδος των οποίων το καθορίζει ο χρήστης, και το πρόγραμμα τα στέλνει από μόνο του σε διάφορα σημεία του δικτύου ή φορτώνει από διαφορετικά σημεία του δικτύου μεγάλους όγκους δεδομένων δημιουργώντας έτσι με τεχνητή ροή δεδομένων που είναι όμως πολύ χρήσιμη στον έλεγχο του δικτύου για τα προβλήματα που μπορεί να παρουσιάσει σε καταστάσεις αυξημένου φόρτου. Σύμφωνα με τις προδιαγραφές του προγράμματος το Traffic Generator μπορεί να γεμίσει το δίκτυο μέχρι και 99,6% οπότε χρειάζεται αρκετή προσοχή για να μην κολλήσουμε από μόνοι μας το δίκτυο.

Εκτός από τη βασική και πλήρη έκδοση του προγράμματος υπάρχει και η έκδοση LITE με λιγότερες δυνατότητες, η οποία διατίθεται ελεύθερα από την MG-SOFT και την ABIT

Λειτουργικό σύστημα – Απαιτήσεις

Το Monet LAN Analyzer δουλεύει και σε παλαιότερους υπολογιστές με πολύ χαμηλές προδιαγραφές (IBM PC/AT ή συμβατό, επεξεργαστή 386, DOS V3.30, XMS RAM 4Mbyte με κατάλληλο διαχειριστή μνήμης τύπου "himem.sys")

Ασφαλώς δουλεύει και στα νεότερα συστήματα των Windows 95/98/2000/ME/NT αρκεί να εγκαταστήσουμε το κατάλληλο πακέτο με τους 32-bit drivers που υπάρχει στην τελευταία έκδοση του προγράμματος ή στα site των δύο εταιρειών που προωθούν το πρόγραμμα.

Αξιολόγηση

Πολύ καλό πρόγραμμα αλλά για χρήστες παλαιότερων γενεών. Το command prompt περιβάλλον του είναι πολύ αποκρουστικό για κάθε νέο χρήστη. Οι διαχειριστές των δικτύων που το χρησιμοποιούν βέβαια το βρίσκουν ιδανικό για αυτό που κάνει αλλά σίγουρα δε θα έλεγαν όχι και για ένα παρόμοιο πρόγραμμα σε περιβάλλον Windows.

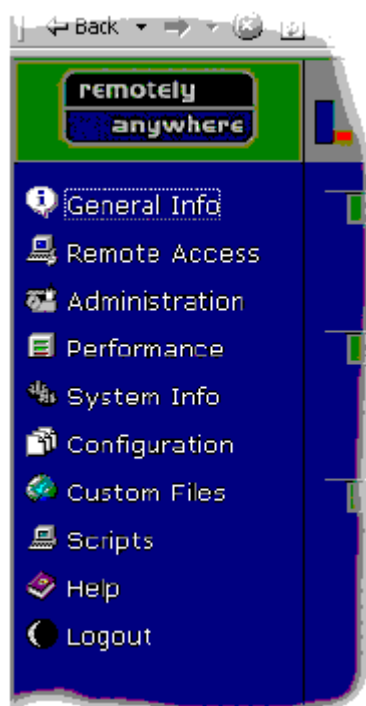
Η τιμή του που παραμένει η ίδια εδώ και κάποια χρόνια θεωρείται τώρα μάλλον ακριβή.

	RemotelyAnywhere	
Έκδοση	3.21.261 (2000)	
Εταιρεία	3am Laboratories PL, Hungary Marton Anka	
Τιμή	\$99	

Χαρακτηριστικά

- Απομακρυσμένη πρόσβαση σε web περιβάλλον
- Διαχείριση αρχείων – χρηστών
- Προβολή συμβάντων
- Αλλαγή ρυθμίσεων - Επανεκκίνηση
- Προγραμματισμός εργασιών
- Εκτέλεση και έλεγχος προγραμμάτων
- Προβολή της επιφάνειας εργασίας
- Telnet
- Σύνδεση μέσω war

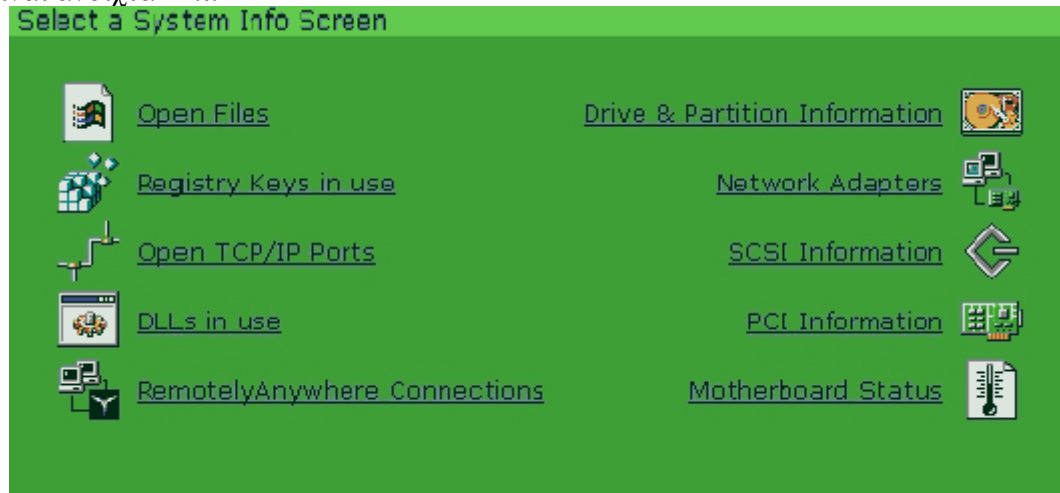
Περιγραφή



Ένα πολύ καλό πρόγραμμα για διαχείριση από μακριά υπολογιστών μέσα από τον απλό περιβάλλον ενός κοινού browser. Αφού εγκαταστήσουμε το πρόγραμμα σε ένα υπολογιστή που τρέχει κάποιο Windows λειτουργικό αυτό παραμένει σαν ένα μικρό daemon utility και υποστηρίζει ένα είδος web-server. Μέσω internet ή intranet και με τη βοήθεια του πρωτοκόλλου TCP/IP μπορούμε να εισέλθουμε στον συγκεκριμένο υπολογιστή από οποιοδήποτε σημείο και να ενεργοποιήσουμε το πρόγραμμα.

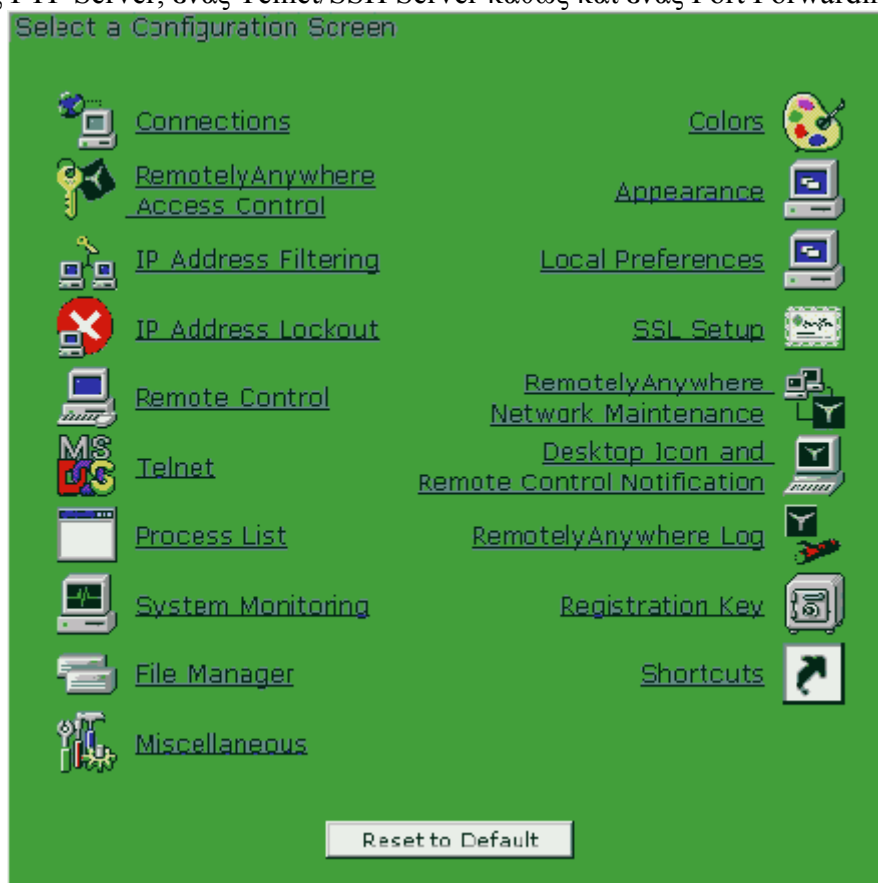
Αν και όλες οι επιλογές εμφανίζονται μέσα από τις σελίδες που διαβάζει ο browser που χρησιμοποιούμε παρόλα αυτά το πρόγραμμα είναι τόσο λειτουργικό που μοιάζει να είναι εγκατεστημένο και στον δικό μας υπολογιστή. Στην πραγματικότητα το μόνο που χρειάζεται είναι υποστήριξη JavaScript από το browser και δε υπάρχει καμία δέσμευση για το ποιος θα είναι αυτός και σε τι λειτουργικό σύστημα θα τρέξει.

Ο αριθμός των επιλογών που έχουμε είναι μεγάλος και αφορά μεταξύ άλλων διαχείριση αρχείων αλλαγή ρυθμίσεων hardware, εκτέλεση προγραμμάτων και προβολή της επιφάνειας εργασίας του απομακρυσμένου υπολογιστή. Μπορούμε ακόμα να ελέγξουμε το βαθμό χρήσης της CPU και της μνήμης, τα προγράμματα και DLLs που τη χρησιμοποιούν, τους πόρους του συστήματος, τα αρχεία και ports που είναι ανοιχτά κλπ.



Υπάρχει μάλιστα η δυνατότητα να επέμβουμε και να τερματίσουμε προγράμματα ακόμα και τη λειτουργία του απομακρυσμένου υπολογιστή.

Ανάμεσα στις νέες δυνατότητες που έχουν προστεθεί στην τελευταία έκδοση είναι και ένας FTP Server, ένας Telnet/SSH Server καθώς και ένας Port Forwarding Server.



Ίσως η πιο πρωτοποριακή καινοτομία η οποία δικαιολογεί πλήρως το δεύτερο συνθετικό (Anywhere) του ονόματος του προγράμματος είναι η πρόσβαση στον απομακρυσμένο υπολογιστή μέσω war από κάποιο κινητό τηλέφωνο υποστηρίζει το συγκεκριμένο πρωτόκολλο (Wireless Application Protocol - WAP).



Μόλις γίνει η σύνδεση ζητούνται οι απαραίτητοι κωδικοί και εφόσον δωθούν σωστά ο χρήστης του κινητού μπορεί να ελεγξει βασικά μόνο στοιχεία ή να δώσει κάποιες απλές εντολές στο απομακρυσμένο σύστημα.

Στον τομέα της ασφάλειας υιοθετεί τις δυνατότητες των Windows NT που θεωρείται ότι παρέχει ασφαλείς συνδέσεις σε όλα τα επίπεδα.

Και το RemotelyAnywhere υπάρχει σε δοκιμαστική έκδοση 5Mbytes η οποία έχει χρονική ισχύ αλλά είναι κατά τα άλλα πλήρης και διατίθεται από το ομώνυμο site που ανήκει στη εταιρεία 3am Laboratories PL.

Λειτουργικό σύστημα – Απαιτήσεις

Όλες οι λειτουργίες δουλεύουν σε υπολογιστές με Windows 9x και οι περισσότερες από αυτές δουλεύουν και σε Windows NT 3.51.4/2000.

Βέβαια η πρόσβαση μπορεί να γίνει όπως είπαμε από οποιοδήποτε λειτουργικό σύστημα αρκεί αυτό να διαθέτει browser με ενεργοποιημένο το JavaScript ή από κάποιο κινητό τηλέφωνο που υποστηρίζει war.

Αξιολόγηση

Ένα πολύ καλό και έξυπνο πρόγραμμα που βασίζεται στις δυνατότητες της java αλλά και στους βασικούς πόρους που παρέχουν τα Windows. Όλα αυτά τα εκμεταλλεύεται σε ένα πολύ μεγάλο βαθμό με αρκετά εντυπωσιακά αποτελέσματα. Επειδή και τα ίδια τα Windows στον τομέα της ασφάλειας δεν είναι και πολύ ανθεκτικά αυτό είναι ίσως το μόνο μειονέκτημα που θα σημειώναμε για το πρόγραμμα.

	sFLOW	
Έκδοση	Hardware/Software	
Εταιρεία	(InMon Co.)	
Τιμή	FREE (to Software probe)	

Χαρακτηριστικά

- Ακρίβεια
- Επεκτασιμότητα
- χαμηλό κόστος
- αμεσότητα

Περιγραφή

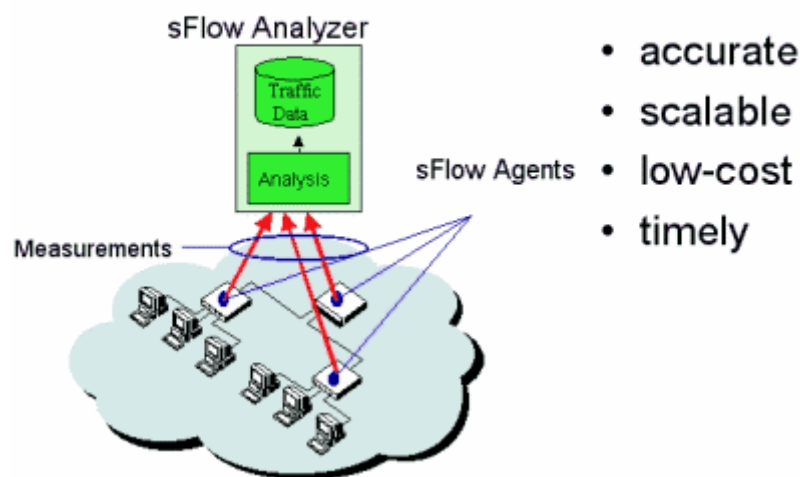
Το sflow probe της InMon (Internet Monitoring) είναι μια hardware συσκευή που κατασκευάζεται εδώ και αρκετό καιρό σε συνεργασία με την Foundry Networks και

αποτελεί ένα σημείο από όπου περνούν και ελέγχονται όλα τα πακέτα δεδομένων πριν εισέλθουν ή εξέλθουν από το δίκτυο

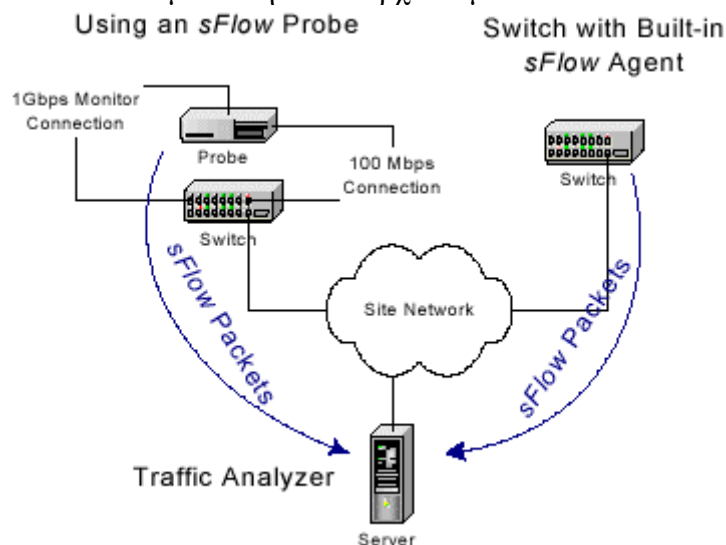


Τοποθετώντας έτσι ένα ή περισσότερα probe σε βασικούς κόμβους του δικτύου μπορούμε να πάρουμε γρήγορα, εύκολα και αξιόπιστα διάφορα στατιστικά στοιχεία που αφορούν το φόρτο και τη ροή προς κάθε κατεύθυνση των δεδομένων που διακινούνται μέσα, από και προς το δίκτυο

sFlow Traffic Monitoring System



Με τη βοήθεια των διακοπών της Foundry Networks μπορούμε να επιλύσουμε προβλήματα που παρουσιάζονται όταν οι ταχύτητες είναι πολύ μεγάλες (10Gbps) και δεν μπορούμε να αναλύσουμε οτιδήποτε διέρχεται μέσα από το δίκτυο.



Πέρα όμως από την Hardware υλοποίηση η InMon έχει προχωρήσει και στη δημιουργία ενός Software Probe με το ίδιο όνομα (sFlow Software Probe)

Αυτό είναι ένα πρόγραμμα μέσα από το οποίο περνάει όλη η ροή των δεδομένων από και προς το δίκτυο και υπολογίζει στοιχεία σχετικά με αυτά με τη βοήθεια του Switched Port Analyzer (SPAN) Βασισμένο στην ίδια τεχνολογία το πρόγραμμα μπορεί να δουλέψει σε συνεργασία με τα εργαλεία της ίδιας εταιρείας sflowtool, ή InMon Traffic Server

Λειτουργικό σύστημα – Απαιτήσεις

Το InMon Software Probe μπορεί να εγκατασταθεί σε ένα PC που τρέχει RedHat Linux και χρειάζεται να είναι εγκατεστημένα τα net-snmp tools.

Αξιολόγηση

Ενώ η Hardware υλοποίηση έχει αυξημένες δυνατότητες για την εποπτεία του φόρτου του δικτύου, το Software Probe δεν μπορεί να εγγυηθεί αυξημένες αποδόσεις για πολύ μεγάλες ταχύτητες κίνησης δεδομένων ώστε να συμβαίνουν συχνά υπερφόρτωση και απώλειες πακέτων δεδομένων. Αυτό φυσικά εξαρτάται από το σύστημα στο οποίο τρέχει το πρόγραμμα. Η InMon βέβαια δίνει ελεύθερα το sFLOW Software probe αλλά προτείνει εγγυημένα την Hardware υλοποίηση.

	Ntop
Έκδοση	2.0 (2001)
Υπεύθυνος	Luca Deri University of Pisa, Italy.
Τιμή	Distributed free software

Χαρακτηριστικά

- μέτρηση φόρτου δικτύου
- έλεγχος φόρτου δικτύου
- βελτιστοποίηση σχεδιασμού δικτύου
- έλεγχος για παραβιάσεις ασφαλείας δικτύου
- ταξινόμηση του φόρτου σύμφωνα με πολλά πρωτόκολλα
- εμφάνιση στατιστικών φόρτου και με γραφικά
- ενσωματωμένος HTTP server με υποστήριξη password
- υποστήριξη CGI
- αποθήκευση στοιχείων σε βάση δεδομένων με υποστήριξη SQL
- πολυπλεξία
- διασύνδεση για Perl
- υποστήριξη wap

Περιγραφή

Το ntop είναι ένα εργαλείο που δείχνει τη χρήση του δικτύου όπως ακριβώς κάνει και η γνωστή εντολή top του Unix. Το πρόγραμμα έχει δύο βασικές εφαρμογές: το «κλασικό» ntop που ενεργοποιεί έναν web server και το intop (interactive ntop) που ουσιαστικά είναι ένα shell βασισμένο στο ntop engine.

Το ntop παρέχει ένα ισχυρό και ευέλικτο interface στον εκλεκτή των πακέτων του ntop. Από τη στιγμή που ο ρόλος του ntop έχει μεγαλώσει και δεν μπορεί να απλά να θεωρείται ένας network-browser, το πρόβλημα του ελέγχου και εμφάνισης της χρήσης του δικτύου έχει μοιραστεί. Έτσι όπως στις προηγούμενες εκδόσεις το ntop engine αιχμαλώτιζε πακέτα, πραγματοποιούσε ανάλυση φόρτου και αποθήκευση πληροφοριών, έρχεται τώρα το ntop με ένα λιτό command line interface με πλήρη όμως λειτουργικότητα καθώς και σχεδίαση για μελλοντικές εργασίες

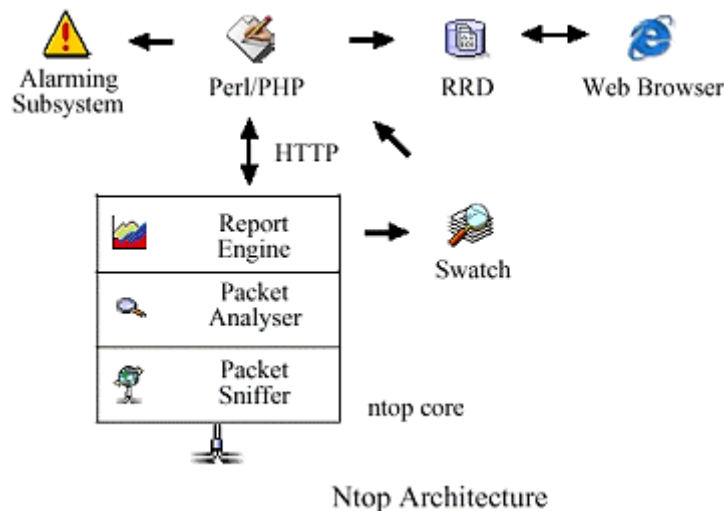
```

ntop 0.0.1 (May 19 2000) listening on [hme0]
6606 Pkts/770.7 Kb [IP 703.7 Kb/Other 67.1 Kb] Thpt: 211.9 Kbps/349.7 Kbps

```

Host	Act	-Rcvd-	Sent	TCP	UDP	ICMP
more	B	257.4 Kb	281.9 Kb	256.6 Kb	769	0
zetant	B	204.2 Kb	232.3 Kb	204.2 Kb	0	0
tar	B	42.9 Kb	19.5 Kb	42.9 Kb	0	0
ibook	B	32.7 Kb	4.7 Kb	32.7 Kb	0	0
tecserv	R	791	0	0	595	196
bugnoli	B	602	1.4 Kb	0	602	0
urano	B	496	5.1 Kb	0	496	0
utlrout	R	98	0	0	0	98
mis	S	0	212	0	0	0
fiorella	S	0	486	0	0	0
piutltst02	S	0	1.4 Kb	0	0	0
mostardi	S	0	952	0	0	0
193.43.104.55	S	0	588	0	0	0
itest1	S	0	928	0	0	0
rally	S	0	46	0	0	0
itin2	S	0	92	0	0	0
3comhub1	S	0	610	0	0	0
re	S	0	5.6 Kb	0	0	0
pi100	S	0	1.2 Kb	0	0	0
lcardini	S	0	546	0	0	0
mbeng	S	0	602	0	0	0
itest2	S	0	600	0	0	0
fossati-a	S	0	960	0	0	0
hpwsutl	S	0	3.1 Kb	0	0	0
catlc	S	0	120	0	0	0
aut01b	S	0	243	0	0	0
biu	S	0	542	0	0	0
artico2	S	0	226	0	0	0

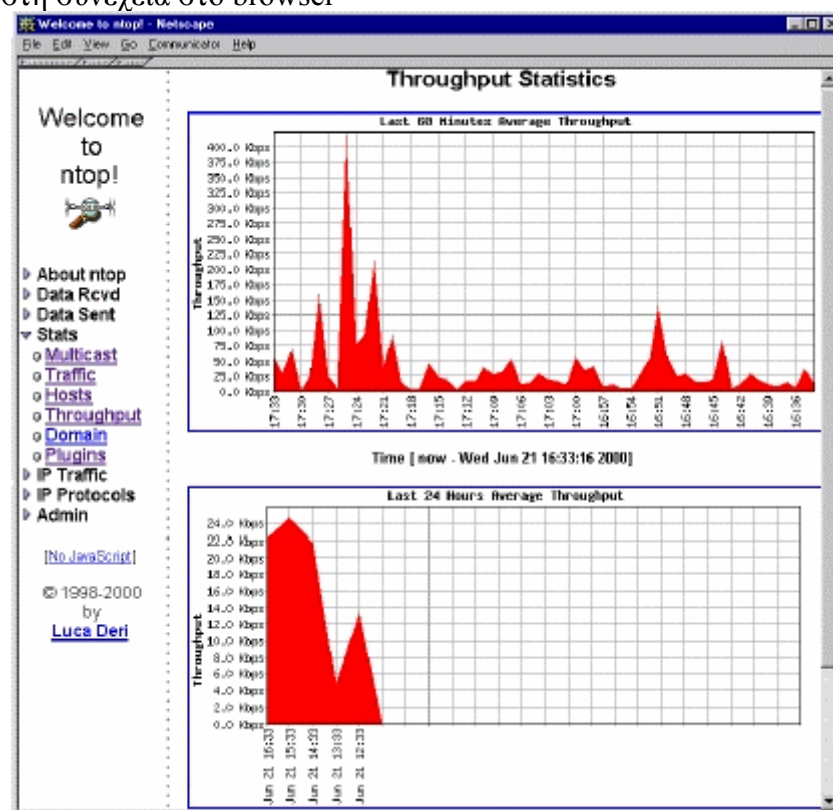
Η επόμενη εικόνα δείχνει την παρούσα σχεδίαση του ntop:



Το ntop είναι υπεύθυνο για τη συλλογή και ανάλυση των πακέτων από το δίκτυο. Οι περισσότερες πληροφορίες παραμένουν στη μνήμη και μια μικρότερη ποσότητα από αυτές περνάει και στο σκληρό δίσκο με η μορφή cash. Το Ntop εμπεριέχει έναν HTTP-based report engine που επιτρέπει τους χρήστες να δουν στατιστικά που αφορούν το φόρτο του δικτύου με τη χρήση ενός απλού web browser.



Έχουν ενσωματωθεί πολλές δυνατότητες για να ελεγχθούν ουσιαστικά οι ανωμαλίες που μπορούν να εμφανιστούν στη ροή των δεδομένων. Για χάρη της ευελιξίας των επιλογών ρυθμίσεων και επειδή κάθε διαχειριστής μπορεί να έχει διαφορετικές προτιμήσεις επιλογών, οι διευκολύνσεις για το χειρισμό των προβλημάτων που έχουν ανακαλυφθεί και των επισημάνσεων που δημιουργούνται, δεν αποτελούν μέρους του πυρήνα του ntop αλλά εκτελούνται μέσω HTTP με Perl και PHP στοιχεία. Αυτές οι γλώσσες έχουν επιλεγεί επειδή είναι interpreted, εύκολες στην εκμάθηση, αποδοτικές, λειτουργικές και συμβατές σχεδόν με τα περισσότερα λειτουργικά συστήματα με internet εφαρμογή. Έτσι κάθε φορά οι πληροφορίες που αναζητούμε μέσα από τον web browser, κωδικοποιούνται σε ένα ξεχωριστό URL με αποτέλεσμα να εμφανιστεί μια σελίδα σε Perl ή PHP μορφή, την οποία διαβάζει και προβάλλει στη συνέχεια στο browser



Το παραπάνω σχήμα δείχνει το συνολικό φόρτο ενός δικτύου για μεγάλα χρονικά διαστήματα ανά 60 λεπτά και ανά 24 ώρες. Με τη χρήση τέτοιων αναφορών μπορεί να γίνει πολύ εύκολα ο μελλοντικός σχεδιασμός και προγραμματισμός των επόμενων εργασιών πάνω στο δίκτυο εφόσον μπορούμε να ξέρουμε τις ώρες αιχμής καθώς και το πότε το σύστημα είναι διαθέσιμο. Μπορούμε επίσης να ελέγξουμε ποιοι πόροι δεσμεύουν περισσότερο το δίκτυο αλλά και ποιοι χρήστες το χρησιμοποιούν περισσότερο, οπότε να ξέρουμε πού θα πρέπει να καθορίσουμε προτεραιότητες και πού όχι.

Με το `wap plunging` που έχει προστεθεί στην τελευταία έκδοση υπάρχει δυνατότητα να πάρουμε στατιστικά σε `wap` μορφή τα οποία βέβαια θα είναι πολύ συνοπτικά και χωρίς γραφικά εφόσον στις οθόνες των κινητών μπορούμε να έχουμε (προς το παρόν τουλάχιστον) μόνο χαρακτήρες και ένα χρώμα.. Είναι και αυτή μια ευκολία που προσφέρεται για τους κατόχους κινητών τηλεφώνων που υποστηρίζουν το πρωτόκολλο `wap`



- ntop's WAP plug-in - accessing 'top receivers' from a WAP device

Λειτουργικό σύστημα – Απαιτήσεις

Αν και πρόκειται για ένα κλασικό Unix πρόγραμμα, υπάρχει και σε εκδόσεις για Win32 και Mac (και πάλι όμως σε command prompt περιβάλλον) Βέβαια ο χειρισμός μπορεί να γίνει όπως είπαμε μέσα από οποιοδήποτε web (ή wap) browser οπότε η δυσκολία στο χειρισμό του επικεντρώνεται κυρίως στον υπολογιστή πάνω στον οποίο θα εγκατασταθεί

Υποστηρίζει Loopback, Ethernet, Token Ring, PPP, Raw IP και FDDI καθώς και τα πρωτόκολλα IP, IPX, DecNet, AppleTalk, Netbios, OSI, και DLC,

Αξιολόγηση

Αναμφίβολα ένα από τα καλύτερα προγράμματα για τον έλεγχο του φόρτου του δικτύου και τη διαχείριση των πόρων του. Απευθύνεται αποκλειστικά σε διαχειριστές δικτύων και το γεγονός ότι είναι ελεύθερο προς χρήση δε μειώνει την αξία του. Απεναντίας μπορούν να προστεθούν από τον καθένα επιπλέον επιλογές που να το προσαρμόζουν κάθε φορά στις ξεχωριστές απαιτήσεις που παρουσιάζονται.

	NeTraMet
Έκδοση	4.3(1999)
Υπεύθυνος	Nevil Brownlee Information Technology Systems & Services The University of Auckland New Zealand
Τιμή	Distributed free software

Χαρακτηριστικά

- Μέτρηση ροής και φόρτου
- Ανάλυση ροής και φόρτου
- Παράλληλη συλλογή δεδομένων από πολλούς μετρητές

Περιγραφή

Το NeTraMet ή Network Traffic Meter είναι μια δουλειά του τμήματος Πληροφορικής Τεχνολογίας Συστημάτων και Υπηρεσιών του Πανεπιστημίου του Auckland στη Νέα Ζηλανδία.

Πρόκειται για μια σειρά από εντολές σε command prompt περιβάλλον, που υπολογίζουν και δίνουν στοιχεία σχετικά με το φόρτο του δικτύου παρέχοντας έτσι πολύ χρήσιμες πληροφορίες για τη ροή των δεδομένων μέσα στο δίκτυο με τέτοιο τρόπο ώστε να κατανοήσουμε καλύτερα τη χρήση του δικτύου.

Κάνει καταμέτρηση της ροής των πακέτων και των bytes από και προς διευθύνσεις οι οποίες μπορεί να είναι διευθύνσεις Ethernet, διευθύνσεις πρωτοκόλλου (IP, DECnet, EtherTalk, IPX or CLNS), διευθύνσεις «μεταφοράς» (IP port numbers, κλπ) ή οποιοσδήποτε συνδυασμός τους. Το τι θα παρατηρήσουμε καθορίζεται από ένα set κανόνων που μπορούν να περάσουν στο NeTraMet από το «manager» πρόγραμμα. Τα στοιχεία του φόρτου συγκεντρώνονται μέσω SNMP από το NeTraMet και από το «collector» πρόγραμμα. Το «manager» και το «collector» βρίσκονται στο NeMaC που είναι ένα πρόγραμμα το οποίο δίνεται μαζί με το NeTraMet. Η μορφή με την οποία το NeMaC συλλέγει τις πληροφορίες είναι πολύ γενική και οι γραμμές των αρχείων με τα δεδομένα αυτά μπορούν να καθοριστούν από τον χρήστη.

Το NeTraMet/NeMaC διατίθεται ελεύθερα από πολλά FTP site και επειδή είναι ανοιχτό για βελτιώσεις και επεκτάσεις μπορούν να βρεθούν ελεύθερα και πολλά άλλα εργαλεία που βασίζονται σε αυτό.

Λειτουργικό σύστημα – Απαιτήσεις

Σχεδιάστηκε για λειτουργικά συστήματα τύπου UNIX (Solaris, SunOS, Irix ή Linux) υπάρχει όμως και μια έκδοση για DOS που μπορεί να τρέξει και μέσα σε ένα παράθυρο των windows. Οι απαιτήσεις σε Hardware είναι μικρές (επεξεργαστή 386 ή ανώτερο) και τρέχει βέβαια σε οποιοδήποτε Pentium σύστημα.

Αξιολόγηση

Το γεγονός ότι δουλεύει σε τέτοιο περιβάλλον, κάνει το πρόγραμμα δύσκολο στη χρήση κυρίως σε χρήστες που δεν έχουν πείρα σε τέτοιου είδους λειτουργικά συστήματα. Παρόλα αυτά βρίσκει μεγάλη ανταπόκριση σε φοιτητές και ερευνητές που το βρίσκουν αρκετά χρήσιμο και χωρίς κανένα τίμημα.

Συμπεράσματα

Ασφαλώς τα προγράμματα τα οποία εξετάσαμε δεν είναι και τα μοναδικά στο είδος τους. Μπορούμε να βρούμε δεκάδες (ή καλύτερα εκατοντάδες) από προγράμματα με παρόμοιες ή και άλλες ξεχωριστές δυνατότητες σε σχέση με την παρακολούθηση και διαχείριση ενός δικτύου. Πιστεύουμε όμως ότι το δείγμα αυτών των 15 προγραμμάτων ήταν αρκετά αντιπροσωπευτικό για να αποκτήσουμε μια γενική ιδέα πάνω σε αυτού του είδους τα εργαλεία.

Έτσι προγράμματα σαν το LinkView Pro, το Monet LAN Analyzer, το sFLOW ή το NeTraMet δίνουν λεπτομερή ανάλυση των δεδομένων που διακινούνται και παρέχουν χρήσιμες στατιστικές σε πραγματικό χρόνο για τη ροή και το φόρτο του δικτύου. Τέτοιες πληροφορίες είναι πολύ χρήσιμες στους διαχειριστές του δικτύου στη φάση του ελέγχου της λειτουργίας αλλά και στη φάση του σχεδιασμού για την μελλοντική επέκταση του δικτύου.

Παρόμοια προγράμματα είναι και τα IP Ultra Monitor και Netcop Scanner, που δίνουν με ένα πολύ περιγραφικό τρόπο στοιχεία για τα ports και τα πρωτόκολλα που χρησιμοποιούνται για συνδέσεις με άλλους υπολογιστές μέσω internet. Μια πολύ λεπτομερή εικόνα της διαδρομής που ακολουθείται σε internet συνδέσεις μας δίνει το NeoTrace, σχεδιάζοντάς την πάνω σε χάρτη και δίνοντας στοιχεία για κάθε ενδιαμέσο κόμβο.

Το pcAnywhere, και το Timbuktu Pro δίνουν την εντυπωσιακή δυνατότητα να μπορεί κάποιος να χειριστεί έναν υπολογιστή βρισκόμενος μπροστά σε κάποιον άλλον υπολογιστή αλλά έχοντας την εικόνα της επιφάνειας εργασίας του απομακρυσμένου υπολογιστή μέσα σε ένα παράθυρο στην δική του οθόνη.

Εντυπωσιακά είναι επίσης και τα προγράμματα όπως το RemotelyAnywhere και το Ntop, τα οποία εκτός από απομακρυσμένη διαχείριση μπορούν να υποστηρίξουν και σύνδεση μέσω war από τα κινητά τηλέφωνα που υποστηρίζουν το συγκεκριμένο πρωτόκολλο.

Είδαμε ακόμα τα μεγάλα προγράμματα IP Manager και Security Manager που παρέχουν ολοκληρωμένη υποστήριξη στο θέμα της παρακολούθησης και διαχείρισης δικτύου.

Τέλος είδαμε και μικρά αλλά χρήσιμα εργαλεία όπως το Select-a-Net και το SwitchIP δίνουν τη δυνατότητα αποθήκευσης ρυθμίσεων δικτύου για υπολογιστές που συνδέονται σε περισσότερα του ενός δίκτυα.

Αναφορές - References

(Όλες οι πηγές είναι από το internet. Οι πρώτες 15 αφορούν τα site των εταιρειών ή οργανισμών που προωθούν τα προγράμματα που παρουσιάστηκαν. Σε αυτά τα site υπάρχουν εγχειρίδια, reviews αλλά και δοκιμαστικές ή πλήρεις εκδόσεις των προγραμμάτων.)

1. <http://www.acterna.com> ή <http://www.wg.com> ή <http://www.linkview.com>
Η Wandel & Goltermann's που είναι ο δημιουργός του LinkView Pro αποτελεί πλέον ένα τμήμα της Acterna η οποία δραστηριοποιείται παγκοσμίως στο χώρο των τηλεπικοινωνιών και δικτύων
2. <http://www.cisco.com/warp/public/cc/pd/nemns/ipmn/index.shtml>
Στη συγκεκριμένη διεύθυνση της Cisco, υπάρχουν αρκετές πληροφορίες για το IPManager που είναι απλώς ένα από τα πάρα πολλά προϊόντα της
3. <http://www.symantec.com/pcanywhere>
Το τμήμα της Symantec που αφορά το pcAnywhere. Στην αρχική σελίδα <http://www.symantec.com> μπορούμε να βρούμε και τα κλασικά Norton Utilities, το Norton Antivirus και πολλά άλλα δημοφιλή εργαλεία.
4. <http://mcafeestore.beyond.com/Product/0,1057,3-18-SN107878,00.html>
Σε αυτή τη διεύθυνση του <http://www.mcafee.com> (γνωστό κυρίως από το ομώνυμο antivirus) υπάρχει το NeoTrace που αρχικά κατασκευάστηκε από την NeoWorx (<http://www.neoworx.com>) η οποία είναι πλέον τμήμα της McAfee.
5. <http://ut-zone.com/selectanet>
Η διεύθυνση του Select-a-Net όπου υπάρχει το πρόγραμμα και αρκετά στοιχεία για αυτό.
6. <http://www.netiq.com/products/sm/default.asp>
Η σελίδα του Security Manager. Από βασική σελίδα <http://www.netiq.com> μπορούμε να δούμε όλα τα προϊόντα μιας ακόμα πολύ μεγάλης εταιρείας (NetIQ)
7. <http://www.switchip.com>
Η διεύθυνση του SwitchIP.
8. <http://members.home.com/ultraj>
Η διεύθυνση της Ultrajones Software η οποία εκτός από το IP Ultra Monitor προωθεί και άλλα προγράμματα για δίκτυα
9. <http://www.netcop.com>
Η διεύθυνση της Netcop με πολλά προγράμματα που προωθεί. Δεν βρίσκεται εκεί όμως και το Netcop Scanner το οποίο όμως σαν freeware μπορεί να βρεθεί σε πολλά άλλα sites στο internet
10. <http://www.netopia.com/software/products/tb2/2000>
Η σελίδα του Timbaktu Pro 2000 της Netopia. Αν και αυτό είναι το πιο γνωστό πρόγραμμα της, η εταιρεία αυτή προωθεί και άλλα προγράμματα και δραστηριοποιείται γενικά στον τομέα των ολοκληρωμένων πακέτων παροχής λύσεων σε δικτυακές υποδομές.
11. <http://www.mg-soft.si/monetlt.html>
Η σελίδα του Monet LAN Analyzer από την Σλοβένικη MG Soft. Το ίδιο πρόγραμμα το διακινεί και η ABIT (<http://www.abit.co.jp>) από την Ιαπωνία.
12. <http://remotelyanywhere.com>
Η σελίδα του RemotelyAnywhere από την Ουγγρική 3am Laboratories PL,
13. <http://www.inmon.com/probes.htm>
Η διεύθυνση της InMon Co. για το sFlow.

14. <http://www.ntop.org/ntop.html>
Η βασική σελίδα για την προώθηση του Ntop από το Πανεπιστήμιο της Πίζας στην Ιταλία.
15. <http://www2.auckland.ac.nz/net/Accounting/ntm.Release.note.html> ή <http://www.netramet.ah.net> Η σελίδα του NeTraMet από το Πανεπιστήμιο του Auckland στη Νέα Ζηλανδία.

(Ακολουθούν οι διευθύνσεις των site από όπου μπορεί να κατεβάσει κανείς αμέτρητο αριθμό shareware προγραμμάτων αλλά και πλήθος από άρθρα, κριτικές και αξιολογήσεις για όλα αυτά τα προγράμματα. Δίνονται επίσης και συγκεκριμένες διευθύνσεις που οδηγούν σε reviews που αφορούν κάποια από τα προγράμματα που παρουσιάσαμε)
16. <http://www.tucows.com>
Παγκόσμιο site με πολλαπλά mirrors σε όλον το κόσμο, που διακινεί τις δοκιμαστικές εκδόσεις όλων σχεδόν των προγραμμάτων που σχετίζονται με οποιονδήποτε τρόπο με το δίκτυο
17. <http://www.zdnet.com> ή <http://www.cnet.com> ή <http://www.download.com>
Ηλεκτρονικά περιοδικά με πληθώρα παρουσιάσεις προγραμμάτων, αξιολογήσεις, άρθρα, δοκιμαστικές εκδόσεις και συγκριτικά στοιχεία.
18. <http://www.programfiles.com>
Ακόμα ένα site με πολλά shareware προγράμματα κάθε κατηγορίας και αντίστοιχα reviews
19. <http://www.scmagazine.com>
Το περιοδικό Security Magazine στην ηλεκτρονικά του μορφή. Υπάρχει και εδώ μεγάλο αρχείο από δημοσιεύματα όπου μπορούν να βρεθούν κριτικές και σχόλια για διάφορα προγράμματα
20. <http://www.alw.nih.gov/Security/prog-network.html>
Μια σελίδα με links για έναν μεγάλο αριθμό προγραμμάτων σχετικά με Network και Network Monitoring
21. <http://www.davecentral.com/projects/netcopscanner>
Review από το DaveCentral (Ένα ακόμα site για διακίνηση shareware προγραμμάτων) για το NetCop Scanner.
22. <http://www.networkmagazine.com/article/NMG20000517S0100>
Άρθρο από το Network Magazine για το pcAnywhere
23. <http://www.ehsco.com/reading/19980817ir1.html>
Μια πολύ καλή παρουσίαση του LinkView Pro από το site της EHS Company η οποία εκτός των άλλων κάνει ελέγχους σε νέα προγράμματα που κυκλοφορούν και εκφράζει κριτικές και παρατηρήσεις για αυτά

(Τέλος δίνουμε και κάποια άρθρα σε περιοδικά καθώς και κάποιες εργασίες πάνω σε θέματα σχετικά με την εποπτεία των δικτύων ή σχετικά με κάποια από τα προγράμματα που είδαμε.)
24. *Network Meter-Reading - Network Monitoring Software, Russell Iwanchuk*
PC Magazine, June 24, 1997 Vol. 16, No. 12
Μια αναλυτική παρουσίαση (παλαιότερων) προγραμμάτων για παρακολούθηση του δικτύου
25. *Design and Implementation of an Anomaly Detection System: an Empirical Approach, Luca Deri, Stefano Suin, Gaia Maselli, Univ. of Pisa*
Εργασία για την αναγνώριση σφαλμάτων δικτύων από τους δημιουργούς του Ntop με πολύ συχνές αναφορές για το συγκεκριμένο πρόγραμμα

26. Monitoring Networks Using ntop
L. Deri and others, Proc. of IM 2001, Seattle, May 2001
Αναλυτικός οδηγός για τη χρήση και λειτουργία του ntop.
27. NTOP – Network TOP An Overview
University of Twente, The Netherlands (Report) João Paulo Almeida, Yohannes Albertino Ramlie - June 2000
Ακόμα μία εργασία που περιγράφει τη λειτουργία του ntop.
28. SYMANTEC pcANYWHERE 9.0: Πώς το PC σας θα σας ακολουθεί... παντού!
Γιάννη Νινιού, περιοδικό PCmaster-Αριθ. Τεύχ.: 116 15/2/2000
Άρθρο για την προηγούμενη έκδοση του pcAnywhere
29. Εποπτεία Δικτύων με την XML (XML for Network Monitoring) Πανεπιστήμιο Μακεδονίας ΠΜΣ Πληροφοριακά Συστήματα, Τεχνολογίες Τηλεπικοινωνιών και Δικτύων Υπεύθυνος: Α. Α. Οικονομίδης, Αθανάσιος Πετρίδης Ιανουάριος 2001
Εργασία για Monitoring μέσω XML με αρκετά καλή τη θεωρητική του παρουσίαση
30. Web based Software for Network Traffic Monitoring, Measurement & Auditing
Παν/μιο Μακεδονίας ΠΜΣ Πληροφοριακά Συστήματα, Τεχνολογίες Τηλεπικοινωνιών και Δικτύων Καθηγητής: Α. Οικονομίδης, Κυριαζίδης Ιωάννης 24/01/1999
Εργασία που αναφέρεται στους τρόπους που γίνεται η εποπτεία του φόρτου του δικτύου μέσω web.