Παν/μιο Μακεδονίας
ΠΜΣ Πληροφοριακά Συστήματα
Τεχνολογίες Τηλεπικοινωνιών και Δικτύων
Καθηγητής : Α. Οικονομίδης

Φοιτητής : Κυριαζίδης Ιωάννης
Α/Μ: Μ 25/99

Εργασία # 2:
Web based Software for Network Traffic Monitoring, Measurement & Auditing

24/01/1999

Web Based Software for Network Traffic Monitoring ,Measurment & Auditing

Εισαγωγή

Αποτελεί κοινός τόπος ότι όσο αναπτύσσεται η τάση δικτύωσης μεταξύ των υπολογιστών , τόσο μεγαλύτεη είναι η και σημασία της ανάλυσης και παρακολούθης της κίνησης και της μετάδοσης των δεδομένων που διακινούνται μέσω των δικτύων. Τα υφιστάμενα εργαλεία παρακολούθησης και ανάλυσης της μετάδοσης δεδομένων εστιάζουν στην παρακολούθηση της κίνησης σε μεμονομένα τμήματα του δικτύου. Επιπρόσθετα διαθέτουν περίπλοκα user interfaces. Δεδομένου ότι η μετάδοση δεδομένων μέσω Internet και Intranet συνεχώς αυξάνει λόγω αύξησης της χρήσης του WWW και άλλων εφαρμογών , η εξακρίβωση για το ποιος Host και ποια εφαρμογή προκαλεί το αντίστοιχο φόρτο αποτελεί κρίσιμος παράγοντας στην αποτελεσματική διαχείρηση και χρήση των διαθεσίμων συστημάτων.

Η τεχνολογία βασισμένη στο Web απελευθερώνει τους χρήστες από περίπλοκα και δύσχρηστα user interfaces , επιτρέποντας παράλληλα την προβολή των αποτελεσμάτων παρακολούθησης και ανάλυσης από οποιοδήποτε Web Browser, και σε οποιαδήποτε τοποθεσία.

Τι εννοούμε παρακολούθηση του φόρτου ενός δικτύου

Όταν μιλάμε για παρακολούθηση της μετάδοσης δεδομένων ενός δικτύου (network traffic monitoring) εννοούμε τη συλλογή και ανάλυση πρωτογενών δεδομένων μετάδοσης. Τα δεδομένα αυτά συλλέγονται από το Probing των πακέτων του δικτύου και η ανάλυση παρέχει εκτεταμένες πληροφορίες που βασίζονται σε αυτά τα πρωτογενή δεδομένα.

Προκειμένου να γίνει αποτελεσματική διαχείριση των διαθεσίμων συστημάτων του δικτύου , είναι απαραίτητη η λήψη πληροφοριών όσον αφορά την κίνηση στο δίκτυο όπως :

- Πόσα δεδομένα διακινούνται μέσω του δικτύου ;
- Τι είδους πληροφορία μεταδίδεται ;
- Πόση κίνηση μεταδίδεται από το κάθε επιμέρους σύστημα ;
- Ποιο σύστημα η ποια εφαρμογή προκαλεί συμφόρηση ;
- Πόση είναι η κίνηση στην ώρα αιχμής και πότε λαμβάνει χώρα η ώρα αιχμής ;

Εάν οι διαχειριστές ενός δικτύου δεν μπορούν να απαντήσουν σε αυτά τα ερωτήματα , τότε πολύτιμοι πόροι του δικτύου ενδεχομένως δεν αξιοποιούνται αποτελεσματικά.

Μεθοδοι μέτρησης φόρτου του δικτύου (Network Measurement)

Οι μέθοδοι συλλογής δεδομένων και παρακολούθησης του φόρτου μπορούν να κατηγοριοποιηθούν σε δύο κατηγορίες : **intrusive measurement (active probing) και non intrusive measurement (passive watch)**

Η πρώτη μέθοδος μέτρησης αναπαράγει πολλά probe πακέτα σε τακτά διαστήματα, τα αποστέλλει στο δίκτυο, και λαμβάνει πακέτα από το δίκτυο. Τα πακέτα αυτά χαρακτηρίζονται σαν ICMP echo packets, UDP echo port packets και άλλα πακέτα σε επίπεδο εφαρμογής. Τα πακέτα αυτά μεταδίδονται μέσω του δικτύου , και επηρεάζονται από την κατάσταση του δικτύου.

Το πλεονέκτημα αυτής της μεθόδου είναι ότι τα αποτελέσματα των μετρήσεων μπορούν να είναι διαθέσιμα όποτε ζητηθούν. Το μειονέκτημα είναι ότι τα αποτελέσματα δεν αντανακλούν την πραγματική εικόνα του δικτύου , διότι τα probed πακέτα συνδέονται έμμεσα με την τρέχουσα κατάσταση του δικτύου , και όχι άμεσα με την πραγματική κατάσταση. Επομένως τα αποτελέσματα θα πρέπει να διορθωθούν και επαληθευθούν μετά από τις μετρήσεις

Η δεύτερη μέθοδος (passive measurement) παρακολουθεί όλα τα μεταδοθέντα πακέτα στο δίκτυο , και αντιγράφει τα πακέτα αυτά μέσα στο σύστημα όπου καταγράφει και το χρόνο σύλληψης των δεδομένων. Τα πακέτα αυτά αναλύονται βάση ορισμένων παραμέτρων που παρατίθενται από το σύστημα. Ο ακριβής αριθμός των πακέτων σωρεύονται και αναλύονται με την πιο πάνω μέθοδο. Το σημείο μέτρησης θα πρέπει να καθοριστεί με προσοχή για την παρακολούθηση του φόρτου. Ο φόρτος του Internet γενικά θα μπορούσε να παρακολουθηθεί στο επίπεδο του backbone network.

Το πλεονέκτημα αυτής της μεθόδου είναι ότι τα δεδομένα του δικτύου μπορούν να αναλυθούν άμεσα. Το μειονέκτημα είναι ότι εάν δεν υπάρχει κίνηση στο δίκτυο , τότε δεν υπάρχει καμία ένδειξη της συμπεριφοράς του δικτύου.

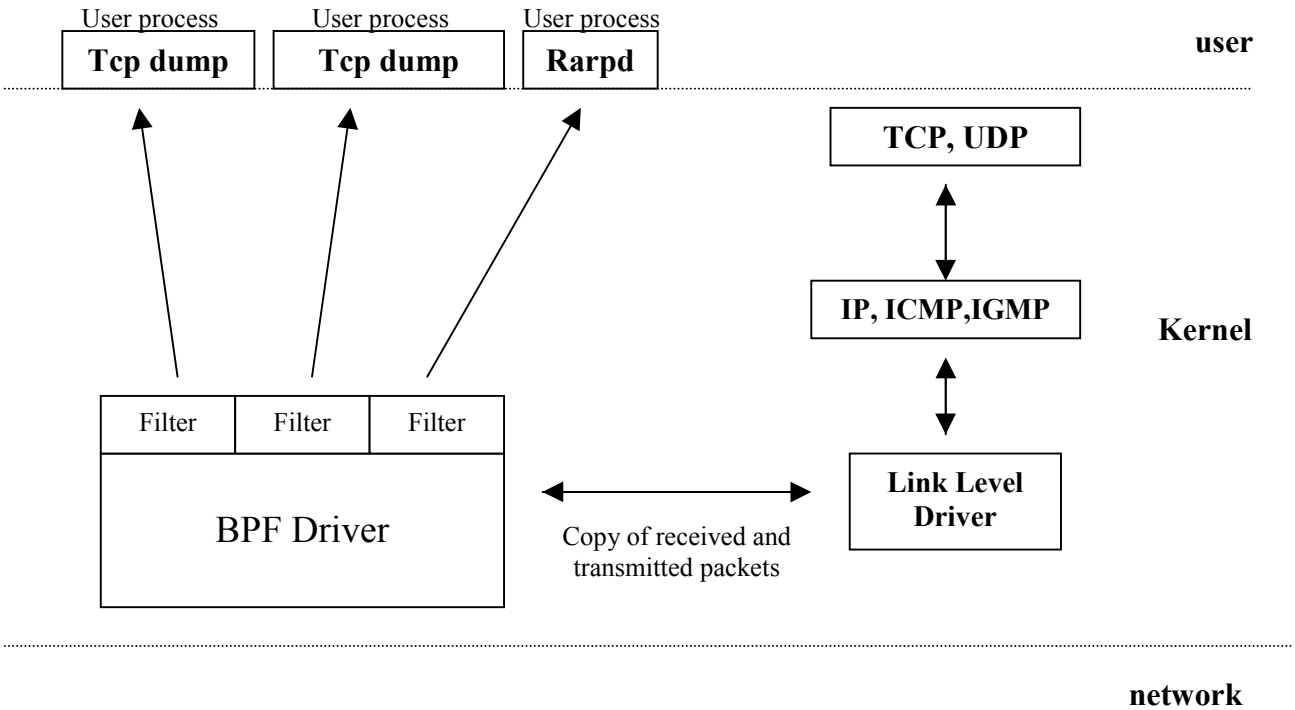
Σύλληψη πακέτων και το φίλτρο πακέτων BSD.

Πολλές εκδόσεις του UNIX παρέχουν εργαλεία για τη σύλληψη πακέτων σε επίπεδο χρήστη, καθιστώντας εφικτή την παρακολούθηση του φόρτου του δικτύου μέσα από σταθμούς εργασίας γενικής χρήσης. Τα συλληφθέντα πακέτα αρχικά αποθηκεύονται σε ένα πρόχειρο αρχείο και έπειτα αναλύονται offline. Μια τέτοια διαδικασία "παντρεύει" τις εργασίες της συλλογής και ανάλυσης δεδομένων σε μια διαδικασία . Ενας κεντρικός διαχειριστής (Kernel agent), που ονομάζεται φίλτρο πακέτων (packet filter), μπορεί να χρησιμοποιηθεί για την επιλεκτική αντιγραφή των πακέτων από τον κυρίως και ουσιαστικό χώρο και το χώρο του χρήστη.

Ένα κοινά αποδεκτό φίλτρο πακέτων είναι το BSD packet filter (BPF). Το BPF αποτελείται από μια τάπα δικτύου και έναν αριθμό από φίλτρα πακέτων. Η τάπα δικτύου συγκεντρώνει αντίγραφα πακέτων από οδηγούς των συσκευών του δικτύου και τα μεταφέρει σε φίλτρα πακέτων σε εφαρμογές που εκτελούν τις εργασίες παρακολούθησης και μέτρησης της απόδοσης του δικτύου. Το φίλτρο πακέτου αποφασίζει εάν το πακέτο θα γίνει αποδεκτό, και ένα ναι, τον αριθμό των bytes του πακέτου που θα αντιγραφούν στην εφαρμογή που παρακολουθεί και μετρά την απόδοση του δικτύου.

Στο ακόλουθο σχήμα φαίνετα ο τρόπος λειτουργίας του BPF και τη σχέση που έχει με τις διαδικασίες μέτρησης εφαρμογών και οδηγούς συσκευών. Σε επίπεδο κανονικής επεξεργασίας πρωτοκόλλου, όταν ένα πακέτο φθάνει σε ένα interface του δικτύου, ο οδηγός συσκευής link level το αποστέλλει στη σωρό του συστήματος πρωτοκόλλου. Αλλά όταν το BPF "ακούσει " σε αυτό το Interface , ο οδηγός θέτει πρώτα σε λειτουργία το BPF όταν καταφθάνει το πακέτο. Το BPF τροφοδοτεί το πακέτο σε κάθε φίλτρο επεξεργαστή που συμμετέχει. Το καθοριζόμενο από το χρήστη φίλτρο αποφασίζει εάν το πακέτο θα γίνει αποδεκτό και πόσα bytes του πακέτου θα αντιγραφούν. Για κάθε φίλτρο που αποδέχεται το πακέτο, το BPF αντιγράφει τα αιτούμενα δεδομένα στο buffer που σχετίζεται με το φίλτρο.

Επειτα ο οδηγός συσκευής παραλαμβάνει τον έλεγχο αφού το BPF ολοκληρώσει την επεξεργασία του πακέτου. Εάν το πακέτο δεν διευθυνσιοδοτηθεί στον τοπικό εξυπηρετητή, ο οδηγός επιστρέφει από την διακοπή. Αλλιώς η κανονική επεξεργασία πρωτοκόλλου συνεχίζεται κανονικά.



Αρχιτεκτονική BPF

Τυπικά μονάχα ένα υποτμήμα του φόρτου ενός δικτύου χρειάζεται από μια διαδικασία μέτρησης, και μια δραματική βελτίωση μπορεί να επιτευχθεί από το φιλτράρισμα των ανεπιθύμητων πακέτων. Για να ελαχιστοποιήσει το φόρτο της μνήμης, το BPF φιλτράρει τα πακέτα "επί της θέσης τους" και δεν τα αντιγράφει σε κάποιο άλλο χώρο πριν το φιλτράρισμα. Ετσι εάν το πακέτο γίνει αποδεκτό , μονάχα τα bytes (κεφαλίδες) που χρειάζονται από τη διαδικασία φιλτραρίσματος αναφέρονται από τον εξυπηρετητή.

Συμπερασματικά το BPF αποτελεί αποτελεσματικό εργαλείο για τη σύλληψη πακέτων.

Ξεπερνά το SunOS Network Interface Trap (NIT) όσον αφορά τη διαχείριση του Buffer και το Stanford Packet Filter (CSPF) σε ότι αφορά το μηχανισμό φιλτραρίσματος. Είναι ιδιαίτερα μεταφέρσιμο και συμβατό με διάφορα επίπεδα data links. Επιπρόσθετα, το συνολικό σύστημα BPF είναι μικρό και εύκολο στην εφαρμογή και υλοποίηση του.

Μέθοδοι παρακολούθησης του Internet.

Σήμερα γίνονται προσπάθειες για την κατασκευή ενός ολικού μοντέλου μέτρησης του φόρτου στο Internet. Ένα τέτοιο μοντέλο θα παρέχει πληθώρα από υπηρεσίες σχετιζόμενες με την απόδοση του δικτύου. Ωστόσο λόγω του εύρους αλλά και της πολυπλοκότητας του Internet ένα τέτοιο μοντέλο έχει ελάχιστες πιθανότητες υλοποίησης στο άμεσο μέλλον.

Απαιτήσεις που θα πρέπει να καλύπτει ένα σύστημα παρακολούθησης φόρτου

Οι σημαντικότερες απαιτήσεις που θα πρέπει να καλύπτει ένα σύστημα παρακολούθησης και ανάλυσης φόρτου (traffic monitoring and analysis) είναι τα ακόλουθα :

1.Ανεξαρτησία από την πλατφόρμα λειτουργίας (platform independence)

Η σύλληψη πακέτων δεδομένων σε χαμηλό επίπεδο θα πρέπει να είναι εξαρτώμενοι από την πλατφόρμα λειτουργίας. Επειδή κάθε πλατφόρμα παρέχει και διαφορετικό επίπεδο δικτύωσης χαμηλού επιπέδου θα πρέπει να υφίσταται διαφοροποίηση από το βασικό επίπεδο δικτύωσης. Εάν το πρόγραμμα κατασκευάστηκε για μια πλατφόρμα , το porting του προγράμματος σε διαφορετικές πλατφόρμες θα ήταν δύσκολη, και οι χρήστες για τις πλατφόρμες αυτές δεν θα μπορούσαν να χρησιμοποιήσουν το πρόγραμμα. Για συστήματα UNIX , ο κώδικας δικτύωσης BSD αποτελεί κοινός τόπος κάθε προτεύοντος λειτουργικού συστήματος.

Ετσι οι λειτουργίες σύλληψης πακέτων μπορούν να βασιστούν σε κοινό κώδικα. Το porting αυτού του προγράμματος σε μια πλατφόρμα PC Windows θα απαιτούσε επιπρόσθετη προσπάθεια διότι σε χαμηλό επίπεδο δικτύωσης οι πλατφόρμες των Windows και UNIX δεν έχουν σχεδόν κανένα κοινό σημείο.

2. Ισχυρά εργαλεία διεπαφής για το χρήστη (user interfaces)

Τα στοιχεία του User Interface θα πρέπει να είναι εύκολα στη χρήση και κατανόηση τους .

Γι' αυτό η καλύτερη λύση ίσως είναι ένα Interface βασισμένο στο Web (Web based Interface), τα οποία είναι εύκολα στη χρήση και ευρέως διαδεδομένα διότι το Web δεν στηρίζεται σε συγκεκριμένο λειτουργικό σύστημα. Επιπλέον οι Web Browsers είναι διαθέσιμοι για όλα τα λειτουργικά συστήματα. Ένα Web based user Interface έχει ακόμη ένα πλεονέκτημα. Για τη χρήση ενός συστήματος βασισμένου στο Web , το μονο που απαιτείται

είναι η πρόσβαση στο δίκτυο και η χρήση ενός Web Browser. Οπουδήποτε , οποτεδήποτε και οποιοσδήποτε θα μπορεί να έχει πρόσβαση στο σύστημα χρησιμοποιώντας ένα κοινό Web Browser.

3. Εγγυημένη σύλληψη πακέτων

Σε ένα δίκτυο υψηλών ταχυτήτων η ταχύτητα μετάδοσης πακέτων ανά δευτερόλεπτο μπορεί να είναι αστρονομική. Η ανάλυση αυτών των δεδομένων απαιτεί μεγάλο χρόνο για την επεξεργασία τους. Επομένως η αποτελεσματικότητα και η ταχύτητα σύλληψης των πακέτων από το πρόγραμμα-software είναι σημαντικός παράγοντας.

Σε δίκτυο υψηλών ταχυτήτων , το σύστημα ενδεχομένως να μην μπορεί να διαχειριστεί όλα τα πακέτα εγκαίρως. Εάν η ταχύτητα επεξεργασίας , η το ίδιο το σύστημα , δρα σε επίπεδα ταχύτητας που δεν επαρκούν για τη σύλληψη όλων των πακέτων, τότε τα αποτελέσματα της ανάλυσης θα είναι αναξιόπιστα. Η διασφάλιση ότι όλα τα πακέτα δεδομένων λαμβάνονται κανονικά αποτελεί σημαντικός παράγοντας για την αξιολόγηση του προγράμματος.

4. Κατηγοριοποίηση -Ταξινόμηση όλων των πληροφοριών για τα πρωτόκολλα

Σε ένα δικτυακό τοπίο συναντώνται πολλών ειδών πρωτόκολλα επικοινωνίας. Για παράδειγμα σήμερα υπάρχουν πολλά πρωτόκολλα εφαρμογών όπως είναι HTTP, Ftp, Telnet, SNMP, MP3,Real Audio , Real Video κλπ. Όλα τα πακέτα δεδομένων μεταφέρονται μέσω του πρωτοκόλλου και το πρωτόκολλο μπορεί να ταξινομηθεί σε συγκεκριμένο στρώμα - επίπεδο. Ένα ιδεατό εργαλείο παρακολούθησης θα πρέπει να μπορεί να ταξινομεί και π να προβάλλει όλα τα πιθανά πρωτόκολλα σε κάθε στρώμα .

5. Μεταφερσιμότητα - Συμβατότητα

Ένα εργαλείο σύλληψης πακέτων θα πρέπει να είναι εύκολο στην εγκατάσταση και στη χρήση σε κάθε τμήμα του δικτύου. Εάν κάποιος θέλει να παρακολυθήσει ένα συγκεκριμένο τμήμα του δικτύου , θα πρέπει να είναι σε θέση να εγκαταστήσει το σύστημα παρακολούθησης σε έν φόρητο Η/Υ η ένα PC και να το συνδέσει με το τμήμα αυτό με ευκολία.

6. Ασφάλεια

Η ασφάλεια αποτελεί κρίσιμος παράγοντας. Η ασφάλεια των δεδομένων είναι απαραίτητη για την αποφυγή παράνομης πρόσβασης και ενδεχομένων ζημιών στα δεδομένα. Πολλοί χάκερς παραβιάζουν συστήματα που παρουσιάζουν κενά στα ζητήματα ασφαλείας. Επομένως η πρόσβαση θα πρέπει να περιοριστεί σε εξουσιοδοτημένους χρήστες. Ενας συμβατικός μηχανισμός ασφαλείας του Web (όπως ένα username και έλεγχο του password) μπορεί να χρησιμοποιηθεί για την παροχή πρόσβασης στο σύστημα ανάλυσης και παρακολούθησης.

7. Προβολή δεδομένων σε πραγματικό χρόνο (real time) και ιστορικά στοιχεία.

Το σύστημα θα πρέπει να είναι σε θέση να προβάλλει On line και σε πραγματικό χρόνο τα δεδομένα για την κατάσταση του συστήματος καθώς και σωρευμένα ιστορικά στοιχεία εύκολα. Από τα ιστορικά στοιχεία ο χρήστης θα μπορεί να αναλύσει μακροπρόθεσμες τάσεις όσον αφορά το φόρτο του συστήματος και από τα real time δεδομένα να εξετάσει τις βραχυπρόθεσμες τάσεις. Αυτό διευκολύνει το χρήστη να εντοπίσει τα προβλήματα πιο εύκολα και γρήγορα.

Διαθέσιμα Εργαλεία

Στη συνέχεια παρουσιάζονται τα ακόλουθα εργαλεία για την παρακολούθηση και ανάλυση της μετάδοσης δεδομένων στα δίκτυα.

1. Multi Router Traffic Grapher
2. Argus
3. Etherfind
4. NF Swatch
5. TCP Dump
6. Etherload
7. Web Technology

Multi Router Traffic Grapher (MRTG)

Το MRTG αποτελεί εργαλείο για την παρακολούθιηση του δικτυακού φόρτου πάνω σε δεσμούς δικτύων (network links) . Παράγει σελίδες σε HTML που περιέχουν εικόνες GIF και παρέχουν μια ζωντανή οπτική παρουσίαση του δικτυακού φόρτου. Υλοποιείται με τη χρήση γλωσσών προγραμματισμού όπως Perl και C και μπορεί να λειτουργήσει κάτω από διάφορα συστήματα UNIX και Windows NT. Το πρόγραμμα MRTG χρησιομοποιείται με επιτυχία σε πολλά sites ανά τον κόσμο.

Ωστόσο το MRTG δεν περιορίζεται μονάχα στην παρακολούθηση της κίνησης τιου δικτύου. Μπορεί να χρησιμοποιηθεί για την παρακολούθηση κάθε SNMP MIB μεταβλητής. Το MRTG μπορεί να παρέχει αποτελέσματα αναλύσεων από δεδομένα που συγκεντρώνονται από εξωτερικά προγράμματα. Χρησιμοποιείται για την παρακολούθηση πληροφοριών όπως είναι ο φόρτος του συστήματος , για τις εισόδους των χρηστών (login sessions) , τη διαθεσιμότητα των modems και άλλα. Το MRTG μπορεί να περιλάβει δύο οι περισσότερες πηγές δεδομένων σε ένα γράφημα.

Παρόλο τα σημαντικά πλεονεκτήματα του συστήματος , το MRTG δεν παρέχει πληροφόρηση που να υποδεικνύει ποιος εξυπηρετητής η ποια εφαρμογή προκαλεί συμφόρηση στο σύστημα (bottleneck). Οι μεταβλητές SNMP MIB δεν ενδικνύονται για τέτοια χρήση και μπορούν μονάχα να δείχνουν το φόρτο κίνησης. Επίσης το MRTG δεν παρέχει πληροφορίες για τον τυπο του φόρτου ούτε στατιστικά για τα πρωτόκολλα.

Ετσι ενώ το MRTG αποτελεί εξαίρετο εργαλείο με Web Based Interface και είναι εύκολο στη χρήση , οι διαχειριστές δικτύων χρειάζονται πιο φιλικά και εξεζητημένα εργαλεία για την ανάλυση των δεδομένων από την κίνηση στα δίκτυα.

Etherfind

Το Etherfind παρέχεται από το λειτουργικό σύστημα SunOS. Το λογισμικό ανοίγει την κάρτα δικτύου σε πρόχειρη λειτουργία και αντιγράφει μια συνοπτική γραμμή για κάθε πακέτο σε ένα αρχείο. Τα δεδομένα αυτά αφορούν τον τύπο του πρωτοκόλλου, το μέγεθος καθώς και τη διεύθυνση αποστολής και παραλαβής. Το εργαλείο αυτό λαμβάνει πληροφορίες από κάθε πακέτο. Τα δεδομένα παρέχονται με τη μορφή ενός text based user interface και μονάχα οι εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στο εργαλείο.

NF Swatch

Παρκολουθεί κάθε εισερχόμενη μετάδοση δικτύου που κατευθύνεται προς NFS File Servers , και τα διαιρεί σε ορισμένες κατηγορίες. Το ποσό και ποσοστό των πακέτων κάθε κατηγορίας προβάλλεται απευθείας στην οθόνη και ενημερώνεται συνεχώς. Εξ ορισμού το NFSwatch παρακολουθεί όλα τα πακέτα που κατευθύνονται για το τρέχον εξυπηρετητή. Κάθε εναλλακτικός εξυπηρετητής προορισμού προς παρακολούθηση μπορεί να καθοριστεί με τη χρήση μιας εσωτερικής παραμέτρου. Εάν ο εξυπηρετητής που αποτελεί την πηγή καθοριστεί με την παραμετρο src , τότε μονάχα παρακολουθούνται τα πακέτα που καταφθάνουν στον εξυπηρετητή προορισμού τα οποία στάλθηκαν από τον εξυπηρετητή -πηγή

Το εργαλείο αυτό όπως και το Etherfind δεν αποτελεί βέλτιστη λύση διότι σχεδιάστηκε για την παρακολούθηση ενός μονάχα εξυπηρετητή.

TCP Dump

Το TCPDump αρχικά υλοποιηθηκε για την έρευνα και την βελτίωση του TCP και την απόδοση του Internet Gateway. Το TCPDump αποτυπώνει τις κεφαλίδες των πακέτων σε ένα interface του δικτύου. Οι χρήστες αναλύουν την κατάσταση του δικτύου διαχειριζόμενοι οι ίδιοι τις πληροφορίες τις κεφαλίδας. Παρόλο που το σύτημα παρέχει πολλές επιλογές για την παρακολούθηση πρωτογενών δεδομένων, δεν παρέχει καμμία δυνατότητα ανάλυσης των δεδομένων αυτών.

Argus

Αποτελεί ένα γενικευμένο IP εργαλείο ελέγχου για τις κινήσεις του δικτύου και χρησιμοποιείται από πολλά sites παγκοσμίως , εκτελώντας πολλές εργασίες διαχείρησης δικτύου. Λειτουργεί σε επίπεδο εφαρμογής , διαβάζοντας πακέτα του δικτύου από ένα προκαθορισμένο interface.

Επειτα αναπαράγει εγγραφές ελέγχου των κινήσεων για τη δραστηριότητα του δικτύου που συναντά. Ο τρόπος με τον οποίο το Argus κατηγοριοποιεί και παρουσιάζει τα αποτελέσματα για τη δραστηριότητα του δικτύου κάνει το εργαλείο αυτό μοναδικό στο είδος του και ισχυρό.

Πρώτον ανακτά πληροφορίες από κάθε πακέτο και στη συνέχεια αποθηκεύει την πληροφορία αυτή σε ένα αρχείο το οποίο αργότερα και αναλύει. . Το εργαλείο αυτό παρουσιάζει πληροφορίες όσον αφορά τα πρωτόκολλα , αλλά δεν δείχνει τον εξυπηρετητή πηγής και προορισμού . Επιπρόσθετα παρέχει μονάχα ένα text based user interface.

Etherload

Αποτελεί εργαλείο ανάλυσης κίνησης σε LAN για συστήματα MS DOS με ελεγκτή Ethernet η Token Ring. Όπως λέει και το όνομα του προγράμματος , το πρόγραμμα αναπτύχθηκε αρχικά για τη μέτρηση του φόρτου σε τμήματα Ethernet. Η βασική του λειτουργία είναι να συλλαμβάνει κάθε πακέτο που περνά από το LAN και παρέχει ορισμένες πληροφορίες για το πακέτο. Η διαθέσιμη πληροφορία καλύπτει αρκετά είδη πρωτοκόλλων όπως TCP/IP , DECnet, OSI,Novell,NetyBEUI της Microsoft κλπ. Το πρόγραμμα απεικονίζει σημαντικές παραμέτρους, γεγονότα και ποσό φόρτου για τα πρωτόκολλα καθώς επίσης και τα συνολικά στατιστικά φόρτου.

Το Etherload μπορεί να χρησιμοποιηθεί για να ελεγχθεί ποιος εξυπηρετητής δημιουργεί τη μεγαλύτερη μετάδοση δεδομένων , ποιος εξυπηρετητής αποστέλλει σε ποιόν εξυπηρετητή, και ποια είδη πρωτοκόλλων βρίσκονται σε χρήση σε ένα συγκεκριμένο τμήμα του Ethernet. Παρέχει λεπτομερή πληροφόρηση όλων των παραμέτρων και στατιστικά δεδομένα. Ειδικά για το TCP/IP δίκτυο, το Etherload είναι σε θέση να αναλύσει και ταξινομήσει την κίνηση μέσω TCP/UDP port numbers, τα οποία δίδουν στατιστικά δεδομένα για ποικίλες εφαρμογές TCP/IP. Δεδομένου ότι το Etherload στηρίζεται σε περιβάλλον MS DOS , παρέχει ένα interface τύπου χαρακτήρων (character based) για την παρουσίαση των αποτελεσμάτων. Κάθε πληροφορία για τα πρωτόκολλλα προβάλλεται σε διαφορετική οθόνη και οι χρήστες μπορούν να μετακινούνται μεταξύ των οθονών μέσω ειδικών εντολών.

Web Technology

Το WWW σχεδιάστηκε αρχικά από ερευνητές του ιδρύματος CERN.Το Web αποτελεί μέσο για την πρόσβαση σε on line περιεχόμενα μέσα από σχέσεις υπερσυνδέσμων στο Internet. Το χρησιμοποιούμενο πρωτόκολλο είναι το HTTP το οποίο χρησιμοποιείται από το 1990. Το HTTP αποτελεί πρωτόκολλο που λειτουργεί σε επίπεδο εφαρμογής και χρησιμοποιείται για κατανεμημένα, πολυμεσικά συστήματα. Το HTML είναι στην ουσία μετατροπή των δεδομένων για τη δημιουργία κειμένων υπερσυνδέσμων (Hypertext documents) τα οποία είναι διαθέσιμα από την μια πλατφόρμα στην άλλη.

Το Web στηρίζεται στην αρχιτεκτονική client server και λειτουργεί ως ακολούθως . Κέιμενα υπερσυνδέσμου τα οποία προτίθενται να κυκλοφορήσουν στο Web κατασκευάζονται σε μορφή HTML και γίνονται προσβάσιμα από τον Web Server.Οι χρήστες που επιθυμούν να διαβάσουν τα κείμενα μπορούν να έχουν πρόσβαση χρησιμοποιώντας ένα web client (τους Web Browsers όπως Netscape Navigator η Microsoft Explorer) για να συνδεθούν στο Web Server που περιέχει το κείμενο.

Το Common Gateway Interface (CGI) αποτελεί την πιο δημοφιλή λύση για την παρακολούθηση εξωτερικών εφαρμογών με Web Servers. Το κείμενο HTLM βρίκεται σε

στατική μορφή με την έννοια ότι υπάρχει σε μια σταθερή μορφή : ένα αρχείο κειμένου που δεν μεταβάλλεται. Ένα πρόγραμμα CGI ωστόσο εκτελείται σε πραγματικό χρόνο , ώστε να είναι σε θέση να μεταδώσει δυναμική πληροφορία. Εάν κανείς επιθυμεί να συνδέσει μια βάση δεδομένων στο Web ώστε διάφοροι χρήστες να μπορούν να πάρουν πληροφόρηση από αυτή, τότε κανείς χρειάζεται ένα CGI πρόγραμμα. Το πρόγραμμα αυτό θα επιτρέπει στο Web Sever να μεταδώσει πληροφορίες στη μηχανή της βάσης δεδομένων , να πάρει τις αιτούμενες πληροφορίες και να τις προβάλλει στον πελάτη -client.

Στο παρακάτω σχήμα φαίνεται η αρχιτεκτονική του Web με το πρόγραμμα CGI.

Με τα προγράμματα αυτά , μπορεί κυριολεκτικά να μεταφεθεί στο Web οτιδήποτε.

Κύρια αρχιτεκτονική κοινού gateway inteface

Παρυσίαση του προγράμματος Web Traf Mon

Το Web Traf Mon αποτελεί εργαλείο βασιζόμενο στο Web για την παρακολούθηση και ανάλυση της μετάδοσης δεδομένων στο δίκτυο. Το πρόγραμμα αυτό προβάλλει το φόρτο ενός δικτύου σε πλήρη λεπτομέρεια, επιτρέποντας στους χρήστες να έχουν πληροφόρηση σε κάθε επίπεδο επικοινωνίας (communication layer), δηλαδή στο επίπεδο της πηγής αλλά και του προορισμού των δεδομένων, τον αριθμό των πακέτων που μεταδόθηκαν και άλλα στοιχεία. Το Web Traf Mon λειτουργεί δια μέσου των Web Interfaces έτσι ώστε οι χρήστες να έχουν πρόσβαση στο πρόγραμμα από τους ήδη υπάρχοντες και εύκολους στη χρήση Web Browsers. Οι Web Interfaces είναι ο ευκολότερος τρόπος για το τρέξιμο του WebTrafMon δεδομένου ότι οι χρήστες χρειάζονται μονάχα μια σύνδεση στο Internet και έναν κοινό Web Browser. Δεν χρειάζεται καμμία προσθήκη άλλου προγράμματος η ρύθμισης από την πλευρά του πελάτη. Οποιοσδήποτε μπορεί να έχει πρόσβαση στην πληροφόρηση και τα στοιχεία ανάλυσης, αν και είναι δυνατός ο περιορισμός της πρόσβασης χρησιμοποιώντας κάποιο μηχανισμό ελέγχου της πρόσβασης σε εξιουσιοδοτημένα μονάχα άτομα.

Το Web Traf Mon αποσπά την πληροφορία κάνοντας χρήση των πακέτων του δικτύου από τις κεφαλίδες στο πιο χαμηλό επίπεδο πρόσβασης ελέγχου (Medium access control) σε αυτό

του ανώτερου επιπέδου της εφαρμογής. Καμία άλλη συναλλαγή η λήψη πακέτων δεν χρειάζεται για να παρθεί η απαιτούμενη πληροφορία. Η πληροφορία αποσπάται σε πραγματικό χρόνο , ώστε οι χρήστες να μπορούν να παρακολουθήσουν τη δραστηριότητα του δικτύου , και να διαπιστώσουν ποιο επιμέρους σύστημα η πρωτόκολλο προκαλεί επιπλοκές, από τη πρώτη στιγμή που θα χρησιμοποιήσουν το WebTrafMon.

Το συγκεκριμένο εργαλείο διαφέρει από τα άλλα προγράμματα διότι μπορεί να παρουσιάσει το φόρτο του δικτύου είτε από τη σκοπιά της πηγής και του προορισμού του εξυπηρετητή από οποιοδήποτε Web Interface. Μπορεί επίσης να προβάλλει το φόρτο σε επίπεδο κάθε πρωτοκόλλου, από το επίπεδο της εφαρμογής μέχρι το επίπεδο του δικτύου. Συνήθως όταν τα δίκτυα διακρίνονται από βαρύ φόρτο , τότε ο φόρτος προέρχεται από ένα αριθμό ορισμένων εξυπηρετητών. Οι διαχειριστές δικτύων θα πρέπει να είναι σε θέση να εξακριβώνουν γρήγορα ποιος εξυπηρετητής προκαλεί το μεγαλύτερο φόρτο ,ώστε να είναι σε θέση να επέμβουν και να διορθώσουν την κατάσταση.

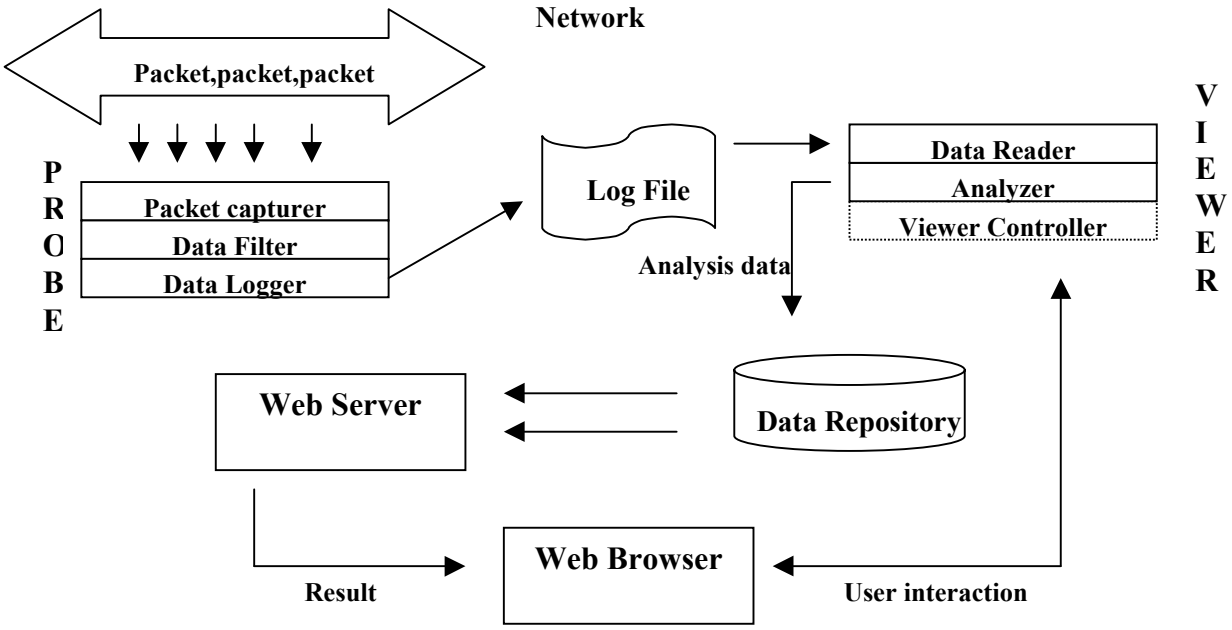
Τα παραδοσιακά εργαλεία παρακολούθησης και ανάλυσης δεδομένων δεν μπορούν να δείξουν το φόρτο εργασίας ανά εξυπηρετητή, παρόλο που η πληροφόρηση αυτή ανά εξυπηρετητή στις μέρες μας είναι σημαντική. Για παράδειγμα μονάχα ένας εξυπηρετητής Video on Demand η Audio on Demand μπορεί να φέρει σε επίπεδο αιχμής ένα υποτμήμα του δικτύου. Σήμερα όλο και πιο πολλές υπηρεσίες πολυμέσων προσφέρονται μέσω του Internet , μερικά από τα οποία χρησιμοποιούν μεγάλα επίπεδα του εύρους ζώνης. Ετσι η πληροφόρηση περί πρωτοκόλλων από κάθε επίπεδο είναι καθοριστικός παράγοντας, όπως επίσης και τα δεδομένα φόρτου από τον εξυπηρετητή γίνονται ολοένα και πιο κρίσιμα στοιχεία .

Το Web Traf Mon χωρίζεται σε δύο τμήματα.

- Ο probe και,
- Ο viewer (προβολέας)

Ο probe αποσπά δεδομένα από τα πακέτα του δικτύου και συντάσσει μικρά αρχεία (log files). Τα δεδομένα των αναλύσεων βασίζονται σε αυτά τα μικρά αρχεία. Ο προβολέας βρίσκεται σε άμεση αλληλεπίδραση με τον χρήστη, προβάλλοντας τα δεδομένα των αναλύσεων διαμέσου ενός Web Browser.

Στη συνέχεια ακολουθεί η αρχιτεκτονική σχεδίασης του Web Traf Mon



Αρχιτεκτονική συστήματος παρακολούθησης και ανάλυσης βασισμένη στο Web

Όπως προαναφέρθηκε το σύστημα αποτελείται από δύο μέρη : το Probe και το viewer.

Ο probe αποσπά δεδομένα από τα πακέτα του δικτύου σε κάθε επίπεδο και τα αποθηκεύει σε ένα προκαθορισμένο αρχείο. Το αρχείο αυτό στη συνέχεια επεξεργάζεται από το τμήμα του analyzer του viewer. Ο χρήστης αλληλεπιδρά με τα δεδομένα ανάλυσης τα οποία αποθηκεύονται στο Data Repository , και ο Web Server τα αποστέλλει στο Web Browser του χρήστη μέσω του view controller.

Probe

Ο probe χρησιμοποιείται για την ανάκληση δεδομένων από κάθε πακέτο και αποθηκεύει τα δεδομένα σε ένα πρόχειρο αρχείο για μετέπειτα επεξεργασία. Για να πιάσει όλα τα πακέτα λειτουργεί σε promiscuous mode. Αυτό οφείλεται και στην ίδια την φύση του Ethernet : Εκπομπή πακέτων (packet broadcasting) . Η σύλληψη όλων των πακέτων αποτελεί την πιο σημαντική και ουσιαστική δουλειά του probe. Ετσι θα πρέπει να λειτουργήσει χρησιμοποιώντας ανεξάρτητο κώδικα λειτουργικού συστήματος. Λεπτομερής περιγραφή της δομής του probe για κάθε επίπεδο επικοινωνίας ακολουθεί στη συνέχεια.

Πρωτίστως αναφέρεται ότι τα επιμέρους συστατικά του probe κάνουν τις ακόλουθες εργασίες. Ο λήπτης πακέτων ευθύνεται για τη σύλληψη όλων των πακέτων από το δίκτυο. Το φίλτρο δεδομένων αποσπά την πληροφορία από κάθε πακέτο. Ο καταγραφέας δεδομένων αντιγράφει τα δεδομένα που το φίλτρο δεδομένων απέσπασε από το log file.

Medium Access Control Layer

Τα πακέτα σε αυτό το επίπεδο θα πρέπει να συλλαμβάνονται με τη μέγιστη δυνατή ταχύτητα. Ωστόσο είναι πρακτικά αδύνατο να συλλάβει κανείς όλα τα πακέτα αξιόπιστα διότι δεν αποτελεί θέμα hardware αλλά software, όπου θα πρέπει η διαδικασία σύλληψης των πακέτων να είναι ακριβής και αποτελεσματική.

Στο επίπεδο αυτό , η αφαίρεση ορισμένων οδηγών του hardware (όπως η κάρτα Ethernet) είναι σημαντικός παράγοντας. Εάν ο κώδικας σύλληψης των πακέτων χρησιμοποιεί ορισμένους οδηγούς συσκευών του δικτύου, το porting του κώδικα σε άλλη συσκευή του δικτύου πιθανώς να χρειαστεί επιπρόσθετη εργασία.

Το probe αποσπά κάθε σχετική με το φόρτο πληροφορία από το επίπεδο αυτό καθώς και το μέγεθος του πακέτου από την κεφαλίδα.

Network Layer.

Το επίπεδο αυτό σχετίζεται με το IP, το ARP (Address Resolution Protocol) κλπ. Εάν ένα πακέτο είναι IP based , συνεχίζεται η επεξεργασία του ώστε να εξακριβωθεί ο εξυπηρετητής πηγής αλλά και προορισμού. Εάν δεν είναι IP Based τότε δεν χρειάζεται παραπέρα ανάλυση διότι δεν εμπεριέχει πληροφορίες για τον εξυπηρετητή πηγής και προορισμού. Στη συνέχεια ο viewer θα πρέπει να ενημερωθεί ότι το πακέτο δεν είναι IP Based ώστε να γνωρίζει ότι ο εξυπηρετητής πηγής και προορισμού δεν είναι διαθέσιμος.

Για τον καθορισμό του ποιος εξυπηρετητής έστειλε το πακέτο, γίνεται χρήση δεδομένων από το επίπεδο αυτό. Ένα δεδομένο πακέτο IP έχει μέσα του δύο διευθύνσεις IP. της πηγής και του προορισμού. Το σύστημα χρησιμοποιεί αυτή την πληροφόρηση για την ανάλυση του φόρτου ανά εξυπηρετητή.

Transport Layer

Το επίπεδο αυτό αποτελεί και το επίπεδο εξυπηρετητή προς εξυπηρετητή. Τα δυο κυρίαρχα πρωτόκολλα στο επίπεδο αυτό είναι το TCP και το UDP (User Diagram Protocol). Το TCP παρέχει αξιόπιστες υπηρεσίες μεταφοράς δεδομένων με δυνατότητα εξακρίβωσης και διόρθωσης των σφαλμάτων, ενώ UDP παρέχει low overhead.

Το probe αποσπά το πρωτόκολλο που χρησιμοποιήθηκε στο επίπεδο αυτό για κάθε δεδομένο πακέτο , και αποθηκεύει την πληροφορία σε ένα log file για παραπέρα χρήση από το viewer.

Application Layer

Το επίπεδο αυτό συνδέεται άμεσα με τις θύρες πηγής και προορισμού, και παρέχει πληροφορίες για τα πρωτόκολλα των εφαρμογών και τη θύρα προορισμού που περιέχει το πακέτο. Για παράδειγμα η θύρα με αριθμό 23 χρησιμοποιείται από το Telnet. Αυτός ο αριθμός θύρας δεσμεύεται για χρήση μονάχα του Telnet. Κάθε αριθμός θύρας μικρότερος του 1023 έχει παρακρατηθεί. Το RFC 1700 καθορίζει τη χρήση των θυρών κάτω του 1023 και αποκαλούνται "Ανατιθέμενοι αριθμοί". Από τα δεδομένα αυτά , μπορεί να γίνει

εκκαθάριση του πακέτου και να γνωρίζουμε ποιο πρωτόκολλο σε επίπεδο εφαρμογής έχει χρησιμοποιηθεί.

Υπάρχει σήμερα μεγάλος αριθμός από πρωτόκολλα σε επίπεδο εφαρμογής.

Μεταξύ αυτών, ο φόρτος που σχετίζεται με το HTTP έχει αυξηθεί σημαντικά λόγω της διάδοσης του WWW. Το HTTP αποτελεί πρωτόκολλο βασιζόμενο στο MIME (Multipurpose Internet Mail Exchange). Οποιαδήποτε δεδομένα μπορούν να αποσαφηνιστούν από το MIME μπορούν να μεταφερθούν μέσω HTTP. Το γεγονός αυτό οδήγησε στην άνθηση των υπηρεσιών πολυμέσων στο Διαδίκτυο, που ουσιαστικά χρειάζονται ένα μεγάλο εύρος ζώνης για να λειτουργήσουν. Τέτοιες υπηρεσίες έχουν προσελκύσει πολλούς χρήστες στο Internet με φυσικό επακόλουθο την αύξηση του αντίστοιχου φόρτου. Νεα συστήματα στο Internet εισάγονται με ταχύς ρυθμούς. Ένα σύστημα παρακολούθησης θα πρέπει να είναι σε θέση να εντοπίζει τέτοια νέα πρωτόκολλα εφαρμογών και να μπορεί να τα αναλύει.

Viewer

Ο viewer αποτελείται από τρία συστατικά μέρη: το data reader , το analyzer και το controller.

Ο data reader διαβάζει τις πληροφορίες των πακέτων από το Log file που προήλθε από το probe. Ο analyzer αναλύει τις πληροφορίες που ζήτησε ο view controller. Τέλος ο view controller αλληλεπιδρά με τον χρήστη για την παροχή των πληροφοριών που αυτός θα ζητήσει.

Ο viewer αναλύει το αρχείο κίνησης (log file) που προήλθε από το Probe και απεικονίζει όλες τις πιθανές πληροφορίες. Εδώ περιλαμβάνονται πληροφορίες για τα πρωτόκολλα που χρησιμοποιούνται στο δίκτυο , αλλά κυρίως οι πληροφορίες αφορούν τη χρήση του εύρους ζώνης του δικτύου από:

- Κάθε πρωτόκολλο σε επίπεδο δικτύου
- Κάθε πρωτόκολλο σε επίπεδο μετάδοσης
- Κάθε πρωτόκολλο σε επίπεδο εφαρμογής
- Το φόρτο ανάμεσα σε κάθε πηγή και προορισμό
- Το φόρτο από κάθε εξυπηρετητή-πηγή
- Το φόρτο σε κάθε εξυπηρετητή προορισμού

Για λόγους ευκολίας και αποτελεσματικότητας, έχει χρησιμοποιηθεί ένα interface βασιζόμενο στο Web , παρόλο που μπορεί να χρησιμοποιηθεί οποιοδήποτε Interface . Ένα Web based interface εξαλείφει τα προβλήματα του porting, ενώ ένα script παρέχει ενοποιημένα αποτελέσματα , ανεξάρτητα από το λειτουργικό σύστημα, οπουδήποτε και εάν βρίσκεται ο χρήστης

Ο viewer διαβάζει το αρχείο κίνησης που προήλθε από το Probe και αλληλεπιδρά με το χρήστη για να διαπιστώσει τι θέλει να δει ο χρήστης. Ανάλογα με τις επιθυμίες του χρήστη ο viewer επεξεργάζεται τις πληροφορίες των πακέτων και φανερώνει τα αποτελέσματα στο χρήστη μέσω του Web Browser,

Στο σχεδιασμό του viewer , έχουν ληφθεί υπόψη κάθε πιθανά προβλήματα ασφαλείας που ενδεχομένως προκύψουν. Αυτό σημαίνει ότι το WebTraf Mon θα πρέπει να επαληθεύει τον κάθε χρήστη ώστε μονάχα οι εξουσιοδοτημένοι χρήστες να έχουν πρόσβαση στο σύστημα.

Εφαρμογή -Υλοποίηση

Στο τμήμα αυτό παρατίθενται οι λεπτομέρειες εφαρμογής του Web Traf Mon

Εφαρμογή Probe

Το συστατικό μέρος για τη σύλληψη των πακέτων που χρησιμοποιήθηκε είναι το Libcap , ένα ανεξάρτητο interface για σύλληψη πακέτων σε επίπεδο χρήστη. Το γενικευμένο Libcap api καθιστά το porting σε συστήματα multi vendor εύκολη υπόθεση. Το Libcap Interface υποστηρίζει ένα μηχανισμό φιλτραρίσματος που βασίζεται στην αρχιτεκτονική του BPF το οποίο αναλύθηκε παραπάνω. Τα συστήματα που δεν υποστηρίζουν το BPF διαβάζουν όλα τα πακέτα που εισέρχονται στο χώρο του χρήστη. Στη συνέχεια τα φίλτρα BPF αξιολογούνται στη βιβλιοθήκη του Libcap.

Για την ανάλυση των πακέτων , προκαθορίστηκε μια μορφή αρχείου σύμφωνα με το επίπεδο του Tcp/Ip πρωτοκόλλου και το μέγεθος του κάθε πακέτου. Στον πίνακα 1 φαίνεται ένα δείγμα ενός αρχείου κίνησης (log file) . Η σημασία κάθε γραμμής και στήλης έχει ως ακολούθως

Δείγμα ενός log file				
346	164.124.96.18	141.223.82.4	Udp	telnet
64	141.223.82.4	141.223.82.26	Tcp	http
112	Rarp			
64	Arp			
74	141.223.99.99	141.223.82.28	icmp	

Η κάθε γραμμή αντιπροσωπεύει ένα πακέτο , με το πρώτο πεδίο να δείχνει το μέγεθος , σε bytes , του κάθε πακέτου. Η πληροφορία αυτή αποσπάται από το επίπεδο του MAC. Για πακέτα Ethernet , η πληροφορία αυτή εμφανίζεται κάτω από την κεφαλίδα Ethernet.

Το δεύτερο πεδίο αντιπροσωπεύει τον εξυπηρετητή πηγή του πακέτου, εάν είναι πακέτο IP based. Εάν δεν είναι IP based τότε μπορεί να βασίζεται είτε σε ARP, RARP η άλλα πρωτόκολλα σε αυτό το επίπεδο. Για παράδειγμα οι γραμμές 3 και 4 αποτελούν τέτοιες περιπτώσεις. Η πληροφορία αυτή αποσπάται από το επίπεδο του δικτύου (network layer).

Το τρίτο πεδίο αντιπροσωπεύει τον εξυπηρετητή προορισμού του πακέτου εάν είναι IP based. Οι πληροφορίες που αφορούν τον εξυπηρετητή πηγή και προορισμού πάνε "χέρι-χέρι". Η πληροφορία αυτή είναι ιδιαίτερα σημαντική ώστε να διαπιστωθεί από ποιόν εξυπηρετητή προήλθε ο φόρτος.

Το τέταρτο πεδίο περιέχει την πληροφορία του transport layer protocol. Εάν είναι TCP-based τότε τυπώνεται το flag με την ένδειξη Tcp. Εάν είναι UDP -based τότε τυπώνεται το flag με την ένδειξη "Udp". Εάν δεν βασίζεται σε TCP η UDP τότε τυπώνεται το αντίστοιχο όνομα του πρωτοκόλλου. Η τελευταία σειρά αποτελεί τέτοια χαρακτηριστική περίπτωση.

Εφαρμογή viewer

Ο viewer αναλύει τα αρχεία κίνησης που αναπαράγονται από το Probe.

Για την ανάλυση του αρχείου κίνησης χρησιμοποιείται Perl script , και για την προβολή των αποτελεσμάτων στο browser του χρήστη χρησιμοποιείται το CGI. Για κάθε στήλη η Perl Script ανακτά πληροφορίες για κάθε επίπεδο δικτύου και το αναπαριστά γραφικά .Ολα τα scripts συγκεντρώνουν πληροφορίες του εξυπηρετητή -πηγή , του εξυπηρετητή προορισμού, η πληροφορίες περί πρωτοκόλλων και μεγέθους των πακέτων. Η προβολή αυτών των πληροφοριών είναι σχετικά εύκολη υπόθεση. Το μόνο που χρειάζεται είναι η προσθήκη του κώδικα HTML. Το Web Traf Mon μπορεί να εμφανίσει την ακόλουθη πληροφόρηση για ένα δεδομένο αρχείο κίνησης :

- Εξυπηρετητή πηγή
- Εξυπηρετητή προορισμός
- Ζευγος εξυπηρετητή πηγής και προορισμού
- Πρωτόκολλο σε επίπεδο δικτύου
- Πρωτόκολλο σε επίπεδο μετάδοσης
- Πρωτόκολλο σε επίπεδο εφαρμογής

Ο viewer στην ουσία αποσπά ένα η δύο πεδία που χρειάζεται από το αρχείο κίνησης, και το ταξινομεί σύμφωνα με το συνολικό φόρτο. Η πληροφορία που σχετίζεται με το φόρτο και το εύρος ζώνης προέρχεται από το πρώτο πεδίο του αρχείου κίνησης, δηλαδή το μέγεθος του δεδομένου πακέτου.

Τελικές διαπιστώσεις

Στα επόμενα σχήματα απεικονίζεται η πληροφόρηση που παρέχεται στο χρήστη από το Web Traf Mon έτσι όπως εμφανίζεται μέσα από το Web Browser. Στη δεξί παράθυρο φαίνεται το είδος της πληροφορίας που μπορεί να εμφανίσει το Web Traf Mon. Η επιλογή "Data received" απεικονίζει τις πληροφορίες του εξυπηρετητή προορισμού. Η επιλογή "data sent" απεικονίζει τις πληροφορίες του εξυπηρετητή πηγή. Η επιλογή "data Exchanged" απεικονίζει το φόρτο στη μετάδοση των δεδομένων σύμφωνα με τον εξυπηρετητή πηγής αλλά και προορισμού. Η επιλογή "Protocol Information" απεικονίζει τις πληροφορίες πρωτοκόλλου σύμφωνα με το κάθε επίπεδο του δικτύου. Η επιλογή "Real Time Monitotring" χρησιμοποιείται για να εμφανίσει την κίνηση σε πραγματικό χρόνο.

Χρησιμοποιώντας το Web Browser οι χρήστες μπορούν να επιλέξουν ένα συγκεκριμένο διάστημα παρακολούθησης η να ανατρέξουν στην υφιστάμενη κατάσταση του δικτύου.

Στο σχήμα Α παρατίθενται ενδεικτικές μετρήσεις τύπου "Data Sent ". Απεικονίζει μαζί την πιο πρόσφατη μέτρηση του φόρτου αλλά και σωρευμένα το συνολικό φόρτο ημέρας.

Στο σχήμα Β φαίνεται ο πίνακας ελέγχου για την παρακολούθηση σε πραγματικό χρόνο. Οι χρήστες μπορούν να ελέγξουν την κατάσταση του δικτύου από το user interface επιλέγοντας ένα από τα ακόλουθα κουμπιά.

- Data sent : Δείχνει ποιος εξυπηρετητής απέστειλε τα περισσότερα πακέτα
- Data received : Δείχνει ποιος εξυπηρετητής έλαβε τα περισσότερα πακέτα
- Data Exchanged : Δείχνει το φόρτο ανάμεσα στον εξυπηρετητή πηγή αλλά και προορισμού
- Network Layer : Δείχνει το φόρτο αναφορικά με τα διάφορα επίπεδα του δικτύου
- Tansport Layer :Δείχνει πληροφορίες του φόρτου σε επίπεδο μετάδοσης
- Application Layer : Δείχνει τα πρωτόκολλα σε επίπεδο εφαρμογής

Συμπερασματικά ολοκληρώνουμε τονίζοντας ότι το Web Traf Mon παρέχει στους διαχειριστές δικτύων δυνατότητες παρακολούθησης σε πραγματικό η μη πραγματικό χρόνο καθώς επίσης και δυνατότητες παρακολούθησης βασισμένες στον εξυπηρετητή προορισμού , πηγής καθώς και προορισμού πηγής αλλά και σε επίπεδο δικτύου , επίπεδο μετάδοσης και πρωτοκόλλου εφαρμογής. Μπορεί να απαντήσει σε ερωτήματα όπως "ποια εφαρμογή αναλώνει τους περισσότερους πόρους του δικτύου ; ", η "ποιοί εξυπηρετητές αναλώνουν τους περισσότερους πόρους του δικτύου ",και " ποια ζεύγη εξυπηρετητών παράγουν το μεγάλυτερο φόρτο στο δίκτυο"

Βιβλιογραφία -Πηγές

Internet

1.Τίτλος : An emperical study of the characteristics of Internet traffic
WWW: www.elsevier.com/locate/comcom
Περιγραφή : Το άρθρο περιγράφει το σχεδιασμό και ανάπτυξη ενός συστήματος μέτρησης του φόρτου στο Internet καθώς και τα χαρακτηριστικά που διακρίνουν το φόρτο του Internet. Τα αποτελέσματα των μετρήσεων που προέρχονται από το συγκεκριμένο σύστημα για την κίνηση στο backbone χαρακτηρίζονται από παραμέτρους όπως τον αριθμό των πακέτων , τον όγκο των δεδομένων που μεταδόθηκαν, το χρόνο σύνδεσης, το χρόνο έναρξης, και τον αριθμό των πακέτων που μεταδόθηκαν πάνω από μια φορές.

2.Τίτλος : Multi Router Traffic Grapher
WWW: ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html
Περιγραφή : Το άρθρο περιγράφει το Multi Router Traffic Grapher σαν εργαλείο παρακολούθησης του φόρτου του δικτύου. Ξεκινά με μια σύντομη παρουσίαση του προγράμματος , ένα σύντομο ιστορικό και ασχολείται με τον τρόπο εγκατάστασης και ρύθμισης του εν λόγω προγράμματος σε συστήματα UNIX και Windows NT. Καταλήγει με ορισμένες συμβουλές για την καλύτερη παραμετροποίηση του προγράμματος και με ορισμένες χρήσιμες διευθύνσεις στο WWW για περισσότερες πληροφορίες.

3.Τίτλος : Network and Network Monitoring Software
WWW: www.alw.nih.gov/security/prog-network .html
Περιγραφή : Πρόκειται για μια σελίδα του National Institutes of Health, Center for Information Technology, η οποία περιέχει μια λίστα αρκετών προγραμμάτων παρακολούθησης φόρτου στο δίκτυο μαζί με μια σύντομη περιγραφή καθώς και χρήσιμα links που οδηγούν σε περισσότερες πληροφορίες για κάθε επιμέρους πρόγραμμα καθώς και ftp sites για το download του κάθε προγράμματος

4.Τίτλος : Web Traf Mon : Web based Internet network traffic monitoring and analysis system
WWW:www.elsevier.com/locate
Περιγραφή : το άρθρο παρουσιάζει και αναλύει τα χαρακτηριστικά του προγράμματος Web Traf Mon , ενός συστήματος παρακολούθησης της κίνησης στο Web και το οποίο λειτουργεί πάνω από κάθε κοινό Web Browser που κυκλοφορούν σήμερα στην αγορά. Τα άρθρο κάνει μια συγκριτική αντιπαράθεση και με άλλα παρόμοια συστήματα Web Monitoring τονίζοντας τα πλεονεκτήματα και μειονεκτήματα του καθενός .

5.Τίτλος : A server based non intrusive measurement infrastructure for enterprise networks
WWW: www.elsevier.com/locate/peva
Περιγραφή : Το άρθρο αυτό προτείνει μια μέθοδο μέτρησης του φόρτου βασισμένη στο server (server based) ώστε να παρέχει τις υπηρεσίες του σε μεγάλο αριθμό πελατών στο Internet. Με βάση την προσέγγιση αυτή ο κάθε server εκτελεί τη εργασία μέτρησης και ανταλλάσσει την πληροφόρηση με ισοδύναμους εξυπηρετητές (peer servers). Η προσέγγιση αυτή αποτελείται από τρία βήματα : 1) non intrusive data collection 2) data analysis 3) exchange of performance metrics among peer servers

6.Τίτλος : Mobile agents for Web Based systems management

WWW:www. Emerald-library.com
Περιγραφή : Το άρθρο διαπραγματεύεται τις δυσκολίες που παρουσιάζει η διαχείρηση των συστημάτων σε συστήματα client server λόγω της ετερογένειας που διακρίνει τα συστήματα που βασίζονται στο Web. Περιγράφει το περιβάλλον που αποκαλείται MAMAS και ο τρόπος υλοποίησης του με τη χρήση της τεχνολογίας Mobile Agent. Στόχος του MAMAS είναι να παρακολουθεί ολόκληρο το σύστημα , εισάγοντας διορθωτικές ενέργειες κατά δυναμικό τρόπο και διαχειρίζοντας τις πολιτικές συστημάτων σε χρόνο run time.

7.Τίτλος : Benchmarking: A tool for Web Site Evaluation and improvement
WWW: www.emerald-library . com
Περιγραφή : Το άρθρο εισάγει την έννοια του Benchmarking για τη διαχείρηση του World Wide Web. Παρουσιάζει ένα case study για να δείξει πως μέσω του Benchmarking ένας οργανισμός μπόρεσε να συγκρίνει το δικό του Web Site με αυτόν ενός άλλου οργανισμού. Τα αποτελέσματα του Benchmarking αποκαλύπτουν πώς συγκρίνεται το Web Site ενός οργανισμού σε σχέση με έναν άλλον, παρέχει ιδέες για την παραπέρα βελτίωση του Web Site και τρόπους για παραπέρα αξιολόγηση του Web Site.

8.Τίτλος : Real Time Network Traffic Monitoring
WWW: www.cs.ukc.ac.uk/pubs/1999/897
Περιγραφή : Το άρθρο αυτό ασχολείται με τα προβλήματα της παρακολούθησης φόρτου σε πραγματικό χρόνο . Εξετάζονται μερικές από τις ηδη υφιστάμενες μεθόδους, όπως είναι τα απλά συστήματα φιλτραρίσματος και λοιποί μηχανισμοί που μπορούν να αναφέρουν συγκεκριμένα συμβάντα η να συλλάβουν δεδομένα κάτω από συγκεκριμένες περιστάσεις. Τέλος παρατίθενται και ορισμένες τεχνικές υλοποίησης αυτών των μηχανισμών

9.Τίτλος : Network Traffic Monitoring - an architecture using associative processing
WWW: www.cs.ukc.ac.uk/pubs/1999/904
Περιγραφή : Η εργασία αυτή εξετάζει τις πιθανές αρχιτεκτονικές συσχετιζόμενης επεξεργασίας για χρήση στην εφαρμογή της παρακολούθησης φόρτου σε πραγματικό χρόνο. Η προτεινόμενη λύση είναι ένας απλός συσχετιζόμενος μονο-επεξεργαστής που βασίζεται σε ένα μικρό αριθμό ηλεκτρικών στοιχείων Το σύστημα αυτό θα παραλαμβάνει μια σειρά από πακέτα δεδομένων ενός δικτύου και μπορεί να προγραμματιστεί να παράγει μηνύματα συμβάντων που αποτελούνται από επιλεκτικά δεδομένα του δικτύου η άλλες πληροφορίες

10.Τίτλος : Network Application Monitoring Software
WWW: www.layer7.com/probe-example.htm
Περιγραφή : Στο άρθρο αυτό γίνεται παρουσίαση του Net Layer7, , ενός προγράμματος παρακολούθησης φόρτου, το οποίο παρέχει πολλά διαφορετικά probes για την παρακολούθηση του δικτύου. Σε αντίθεση με άλλα συστήματα παρακολούθησης τα οποία κάνουν ping σε μια συσκευή hardware , το NetLayer7 διεισδύει μέσα στην εφαρμογή για να κάνει εξακρίβωση πέρα από το επίπεδο του Hardware , και να διαπιστώσει ότι οι εφαρμογές είναι πραγματικά λειτουργικές

11.Τίτλος : Transcend Traffix Manger V 3 For Windows NT
WWW: WWW.3com/news/releases/pr99/aug2399.html

Περιγραφή : Πρόκειται για την παρουσίαση ενός συστήματος παρακολούθησης φόρτου σε συστήματα Windows NT το οποίο έχει το ιδιαίτερο χαρακτηριστικό ότι παρέχει μια ολική εικόνα για τη ροή του φόρτου σε συστήματα end to end , γεγονός που βοηθά τους διαχειριστές δικτύου να κάνουν τις ανάλογες ρυθμίσεις ώστε να επιτύχουν υψηλά επίπεδα διαθεσιμότητας. Επίσης διαθέτει σύστημα ανάλυσης που εξετάζει τα δεδομένα του δικτύου για ασυνέπειες λειτουργίας και ειδοποιεί τους διαχειριστές εάν εμφανιστούν απρόβλεπτα γεγονότα στη διαχείριση των πόρων.

12.Τίτλος : Unix Network Monitoring Tools
WWW: ciac.llnl.gov/ciac/ToolsUnixNetMon.html
Περιγραφή : Στο κείμενο αυτό αναλύονται δύο σημαντικά εργαλεία παρακολούθησης φόρτου , το Argus και το Courtney. Το Argus είναι ένα γενικευμένο IP εργαλείο ελέγχου των μεταδόσεων το οποίο εκτελεί αρκετά σημαντικά καθήκοντα που δεν επιτυγχάνονται από άλλα παρόμοια εμπορικά πακέτα. Για τη λειτουργία του απαιτείται το libcap. Από την άλλη το Courtney παρακολουθεί το δίκτυο και εντοπίζει τα συστήματα των SATAN probes.

13.Τίτλος : TrafShow -Network Traffic Monitoring Utility
WWW: filewatcher.org/sec/trafshow/int_1month.html
Περιγραφή : Το TrafShow απεικονίζει την κίνηση του δικτύου με μεγάλη λεπτομέρεια. Απεικονίζει έναν πίνακα με την πηγαία διεύθυνση, την πηγαία θύρα, τη διεύθυνση και θύρα προορισμού, το IP πρωτόκολλο και το CPS. Οι μετρητές ενημερώνονται με την παραλαβή των πακέτων και η ταξινόμηση του πίνακα γίνεται με τον byte counter. Επίσης δέχεται φίλτρα όπως το TCPDump για να μπορεί ο διαχειριστής να επιθεωρήσει ορισμένο τμήμα του φόρτου του δικτύου.

Περιοδικά /Πρακτικά συνεδρίων / εγχειρίδια κλπ

1) Τίτλος : Network Monitoring software Network Meter reading
Συγγραφέας : Iwanchuk-Russel
Πηγή : PC Magazine Network Edition v16 p 24

2) Τίτλος : Network tools put on new interface : Vendors expect new browser based suppot to gratly increase the accessibility of network performance monitoring tools
Συγγραφέας : Sullivan Kristina
Πηγή : PC Week v 14 p 86 - 89

3) Τίτλος : Feel your networks pulse with network Vital Signs
Συγγραφέας : Bowden Eric
Πηγή : LAN Times v 9 p 42-43

4) Τίτλος : Intel expands net management effort
Συγγραφέας : Krohn-Nico
Πηγή : PC Week v 9 p 30

5) Τίτλος : Network monitoring software gives early warning of disasters
Συγγραφέας : Lehman cliff
Πηγή : Mac Week v 6 p 83-84

6) Τίτλος : LAN Management software system begins shipping
Συγγραφέας : Mardesiich-Jodi
Πηγή : Info World v 12 p 45

7) Τίτλος : Network General bolsters Sniffer with new monitoring software
Συγγραφέας : Morrisey -Jane
Πηγή : PC Week v 7 p 31,40

8) Τίτλος : Delivering the right amount of data on distributed nets
Συγγραφέας : Lowenski
Πηγή : Data communications v 28 p 25 - 26

9) Τίτλος : On the design of ATM interface for traffic monitoring
Συγγραφέας :
Πηγή : Journal of Network and Computer Applications

10) Τίτλος : Rethinking traffic management
Συγγραφέας : McQuillan,-John
Πηγή : Business-Communications-Review. v. 27 May '97 p. 14+