University of Macedonia
Master's in Information Systems

Networking Technologies

Case-studies of Accounting Management in Internet Service Providers

Prof. Oikonomidis Anastasios
Prof. Pombortsis Andreas

Charalampos Douvletis hdoublet@ccf.auth.gr

Vassiliki Koustsonikola vkoutson@ccf.auth.gr

Thessaloniki, 12/01/2003

Πανεπιστήμιο Μακεδονίας
Μεταπτυχιακό Πρόγραμμα Σπουδών στα Πληροφοριακά Συστήματα

Τεχνολογίες Δικτύων

Case-studies of Accounting Management in Internet Service Providers

Καθ. Οικονομίδης Αναστάσιος
Καθ. Πομπόρτσης Ανδρέας

Δουβλετής Χαράλαμπος hdoublet@ccf.auth.gr

Κουτσονικόλα Βασιλική vkoutson@ccf.auth.gr

Θεσσαλονίκη, 12/01/2003

Abstract

The purpose of this text is to present issues related to Network Accounting management, implemented by modern Internet Service Providers (ISPs). At the beginning, this study presents applications and solution technologies for Network Accounting according to the needs of ISPs and large enterprises. Some of the most important applications of Network Accounting are usage and application based billing, security analysis, VoIP billing, classification of traffic and users and quality of services (QoS). Then, technologies for the implementation of Network Accounting are presented, such as Call Details Recording (CDR), Netflow, RADIUS, TACACS+, RMON and SNMP. Most of these technologies are supported by the corresponding network devices. In the second part of study, there is an analysis of case studies of ISPs, which have developed Network Accounting infrastructure based on commercial or open source software tools. Because of the necessity for better quality of services and more efficient design and network monitoring, the ISPs were led inevitably to the development and application of Network Accounting systems. At the end, there is a reference of the most popular tools for Network Accounting systems.

Περίληψη

Σκοπός του κειμένου αυτού είναι να παρουσιάσει θέματα που σχετίζονται με τη διαχείριση δικτύου και ειδικότερα με την καταγραφή και ανάλυση δικτυακής δραστηριότητας (Network Accounting) στους σύγχρονους παροχείς δικτυακών υπηρεσιών. Αρχικά γίνεται συνοπτική παρουσίαση των εφαρμογών και αναφορά των κατάλληλων τεχνολογιών του Network Accounting σε συνδυασμό με τις ανάγκες των παροχέων δικτυακών υπηρεσιών και μεγάλων εταιριών. Από τις σημαντικότερες εφαρμογές του Network Accounting είναι η χρέωση βάσει της κίνησης και της εφαρμογής, η ανάλυση ασφαλείας, η χρέωση του VoIP, η κατηγοριοποίηση της κίνησης και των χρηστών και η παροχή εγγυήσεων για την ποίοτητα των υπηρεσιών (QoS). Στη συνέχεια παρουσιάζονται οι τεχνολογίες που χρησιμοποιούνται για την υλοποίηση του Network Accounting οι σημαντικότερες από τις οποίες είναι τα συστήματα καταγραφής στοιχείων κλήσης (CDR), Netflow, RADIUS, TACACS+, RMON και SNMP. Οι περισσότερες τεχνολογίες υποστηρίζονται από το κατάλληλο υλικό. Στο δεύτερο μέρος του κειμένου, γίνεται ανάλυση συγκεκριμένων περιπτώσεων παροχέων οι οποίοι ανέπτυξαν υποδομή Network Accounting βασισμένοι είτε σε εμπορικά είτε σε ανοιχτού λογισμικού εργαλεία. Λόγω της αναγκαιότητας για καλύτερη ποιότητα υπηρεσιών και αποδοτικότερη σχεδίαση και παρακολούθηση του δικτύου, οι παροχείς, οδηγήθηκαν αναπόφευκτα στην ανάπτυξη και εφαρμογή συστημάτων Network Accounting. Τέλος γίνεται αναφορά των πιο διαδεδομένων εργαλείων Network Accounting.

CONTENTS

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΕΣ

ΣΧΗΜΑΤΑ

1 ΥΠΗΡΕΣΙΕΣ ΚΑΤΑΓΡΑΦΗΣ ΚΑΙ ΑΝΑΛΥΣΗΣ ΔΙΚΤΥΑΚΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ

1.1 ΕΙΣΑΓΩΓΗ

Στο σημερινό επιχειρησιακό περιβάλλον, όπου υπάρχει μια αυξανόμενη έμφαση στην αποδοτικότητα, τα δίκτυα εμφανίζονται όλο και περισσότερο ως μέσα για τη μείωση του κόστους και την αύξηση των εσόδων και της παραγωγικότητας. Για να επιτευχθεί αυτό, απαιτείται ο έλεγχο και η γνώση για την κυκλοφορίας μέσα στο δίκτυό της επιχείρησης ή του οργανισμού. Οι λύσεις καταγραφής και ανάλυσης δικτυακής δραστηριότητας (network accounting) βοηθούν τους πάροχους δικτυακών υπηρεσιών στο σχεδιασμό, στη παρακολούθηση και στη χρέωση διαφόρων υπηρεσιών, χωρίς συμβιβασμούς στην αφθονία των δυνατοτήτων, στην απόδοση των υπηρεσιών, στην προτεραιότητα των πακέτων, και στη κλιμάκωση των δικτύων τους. Ανάλογα με τις ιδιαιτερότητες των δικτύων, τις απαιτήσεις των πελατών, και το επιχειρησιακό μοντέλο, η μια τεχνολογία μπορεί να είναι καλύτερη από άλλη ή ένας συνδυασμός τεχνολογιών μπορεί να είναι η απάντηση στο σύνθετο αυτό θέμα.

Στα κεφαλαία που ακολουθούν παρουσιάζονται τρόποι και λόγοι χρήσης εφαρμογών network accounting, καθώς και οι πιο διαδεδομένες τεχνολογίες για την υλοποίηση των συστημάτων αυτών.

1.2 ΠΑΡΟΥΣΙΑΣΗ ΕΦΑΡΜΟΓΩΝ NETWORK ACCOUNTING

Ανάλογα με το πλαίσιο και τη χρήση, ο όρος "καταγραφή και ανάλυση δικτυακής δραστηριότητας (Network Accounting)" μπορεί να σημαίνει οτιδήποτε από τη χρέωση βάσει της χρήσης του δικτύου μέχρι τον χαρακτηρισμό και κατηγοριοποίηση της κίνησης του δικτύου.

Σε αυτό το κείμενο, ο όρος καταγραφή και ανάλυση δικτυακής δραστηριότητας χρησιμοποιείται με την ευρύτερη έννοιά του, για να περιλάβει τον σχεδιασμό (planning) δικτύων, την διαχείριση της κίνησης, την παρακολούθηση δικτύων, την παρακολούθηση εφαρμογών, την παρακολούθηση χρηστών, τη χρέωση με βάση την υπηρεσία και τον όγκο κίνησης, τις συμφωνίες μεταξύ ομότιμων οντοτήτων (peering agreements) και την ανάλυση της ασφάλειας δικτύων.

Τεχνολογίες /Λύσεις	BGP Policy Accounting/ DSB	CDR	IP Accounting	NetFlow	RADIUS & TACACS+	RMON	Service Assurance Agent	SNMP
Traffic Chara-cterization			X	X		X		X
Security Analysis				X				
Application-specific accounting				X	X	X	X	
Voice over IP		X			x		x	
Usage-based billing	X	X	X	X	X	X		X
Service-level agreements				X		X	X	X
Peering and transit	X		X	X				X

Πίνακας 1 **Αντιστοίχηση λύσεων με τεχνολογίες Network Accounting**

Οι διάφορες λύσεις που παρέχει το network accounting περιγράφονται παρακάτω. Ο ακόλουθος πίνακας παρουσιάζει μια επισκόπηση των μεθόδων network accounting που παρέχουν χρήσιμες πληροφορίες για τους διάφορους σκοπούς της διαχείρισης ενός δικτύου. Ο Πίνακας 1 συνοψίζει τις

λύσεις και τις τεχνολογίες που καλύπτονται σε αυτό το κείμενο και μπορεί να χρησιμοποιηθεί ως αρχικό σημείο για την εξερεύνηση των κατάλληλων λύσεων και τεχνολογιών.

1.3 ΣΕΝΑΡΙΑ ΛΥΣΕΩΝ

1.3.1 Χαρακτηρισμός και προτυποποίηση κίνησης χρηστών

Η τάση, για το δίκτυο που χρησιμοποιείται όλο και περισσότερο για κρίσιμες εφαρμογές, είναι εμφανής. Το VoIP, τα VPNs και η τηλεδιάσκεψη, χρησιμοποιούν όλο και περισσότερο τους πόρους του δίκτυο. Εντούτοις, μερικοί χρήστες κάνουν κακή χρήση του δικτύου κατεβάζοντας κινηματογραφικές ταινίες, ακούγοντας μουσική μέσω δικτύου, καθώς και με άλλου είδους δραστηριότητες που έχουν μεγάλες απαιτήσεις σε πόρους δικτύου.

Είναι περισσότερο σημαντικό από κάθε άλλη φορά, οι διαχειριστές δικτύων να κατανοούν με ακρίβεια την κίνηση και τους χρήστες του δικτύου. Οι πληροφορίες που προκύπτουν από το network accounting μπορούν να χρησιμοποιηθούν:

- για την παρακολούθηση και την προτυποποίηση (profiling) χρηστών
- για την ακριβή αναγνώριση της χρήσης του δικτύου ανά χρήστη
- για την καταγραφή των τάσεων χρήσης ανά χρήστη
- για την αναγνώριση ευκαιριών πώλησης επιπλέον υπηρεσιών προστιθέμενης αξίας σε συγκεκριμένους πελάτες με αναμενόμενο ενδιαφέρον

Τέτοιες πληροφορίες, μπορούν να χρησιμοποιηθούν για να δοθούν απαντήσεις στις παρακάτω ερωτήσεις:

- Ποιοι είναι οι N πρώτοι χρήστες με τη μεγαλύτερη εξερχόμενη κίνηση;
- Ποιο είναι το ποσοστό της κίνησης που προκαλούν;
- Πόσοι χρήστες χρησιμοποιούν το δίκτυο κάθε στιγμή;
- Για πόσο χρόνο χρησιμοποιούν το δίκτυο οι χρήστες;
- Τι συνδέσεις κάνουν και με ποιους;
- Πότε οι αναβαθμίσεις θα επηρεάσουν τον ελάχιστο αριθμό χρηστών στο δίκτυο;

Τεχνολογικές λύσεις για τον χαρακτηρισμό της κίνησης και την προτυποποίηση χρηστών περιλαμβάνουν:

- IP Accounting
- NetFlow
- RMON
- SNMP

1.3.2 Ανάλυση Ασφάλειας

Οι ίδιες τεχνολογίες που χρησιμοποιούνται για να δώσουν λεπτομερείς πληροφορίες για τα πακέτα που διακινούνται στο δίκτυο, μπορούν να χρησιμοποιηθούν για την παρακολούθηση της ασφάλειας. Πρόσφατα έχει παρατηρηθεί μια αυξανόμενη έμφαση στην ασφάλεια και την πρόληψη των επιθέσεων, ειδικά του τύπου Άρνησης-Υπηρεσίας (Denial-Of-Service - DOS), που έχουν προκαλέσει τη διακοπή της λειτουργίας των ιστοσελίδων της Yahoo και της Ebay. Όταν

πραγματοποιούνται τέτοιες επιθέσεις DOS, οι διαδικασίες των παραπάνω τεχνολογιών μπορούν να σημάνουν συναγερμό στο αντίστοιχο Κέντρο Λειτουργίας Δικτύου, μόλις ανιχνευτούν απόπειρες "smurf", "fraggle" και πλημμύρες SYN (SYN flooding) στο δίκτυο. Τα στοιχεία που συλλέχθηκαν μπορούν να χρησιμοποιηθούν αργότερα για την ανάλυση και τον εντοπισμό του τρόπου και της προέλευσης της επίθεσης. Αυτές οι τεχνολογίες μπορούν επίσης να χρησιμοποιηθούν για να επιβάλουν μια πολιτική αποδοχής χρηστών (AUP – Acceptable User Policy).

Τεχνολογικές λύσεις για την ανάλυση ασφάλειας είναι:

- IP Accounting
- NetFlow
- RMON
- SNMP

1.3.3 Χρέωση βάσει της εφαρμογή

Με την αύξηση των προστιθεμένης αξίας λύσεων, όπως το VoIP, το βίντεο, οι αποθήκες δεδομένων (data warehousing), η διαχείριση σχέσεων με τους πελάτες (Customer Relationship Management - CRM), η διαχείριση ανθρώπινων πόρων (Human Resource Management - HRM) και άλλου περιεχομένου, απαιτούνται λύσεις που επιτρέπουν τη χρέωση των πελατών σύμφωνα με την εφαρμογή που χρησιμοποιήθηκε.

Και οι πάροχοι υπηρεσιών εφαρμογών (Application Service Providers - ASPs) και οι εταιρίες φιλοξενίας ιστοσελίδων (Web-Hosting companies) χρεώνουν τους πελάτες για την πρόσβαση στην υπηρεσία που προσφέρουν. Αυτή η υπηρεσία είναι μεγαλύτερης αξίας και μερικές φορές ουσιαστική και αναγκαία στους πελάτες τους, και είναι πιο κερδοφόρα για τον πάροχο υπηρεσιών εάν μπορεί να τις συσχετίσει με ένα ορισμένο επίπεδο ποιότητας υπηρεσιών.

Σε πολλές περιπτώσεις, οι πάροχοι υπηρεσιών εφαρμογών συνεργάζονται με τους παρόχους δικτυακών υπηρεσιών, για να παρέχουν ολοκληρωμένη λύση στον πελάτη. Σε ποιόν ανήκει ποιο μέρος του δικτύου, διαφέρει ανάλογα με το σενάριο, αλλά η ανάγκη για εγγυήσεις στην ποιότητα της υπηρεσίας (Quality of Service - QoS), στο εύρος ζώνης του δικτύου και στους χρόνους απόκρισης δεν αλλάζει. Ομοίως, οι εταιρίες φιλοξενίας ιστοσελίδων μπορούν να ταξινομήσουν την πρόσβαση στους εξυπηρετητές και τα δίκτυά τους στις κατηγορίες υπηρεσιών που προσδιορίζονται από τις συμφωνίες επιπέδου παροχής υπηρεσιών (Service Level Agreements - SLAs). Για την υλοποίηση τέτοιον επιχειρηματικών μοντέλων, απαιτούνται από τις τεχνολογίες που αναπτύσσονται, και συμφωνίες παροχής υπηρεσιών και χρέωση με βάση τη χρήση.

Πληροφορίες που θα πρέπει να καταγράφονται είναι:

- Αριθμός Αυτόνομου Συστήματος (Autonomous System Number - ASNs)
- Εξυπηρετητές, εφαρμογών και δικτυακές πόρτες υπηρεσιών
- Κίνηση δικτύου (εύρος ζώνης, όγκος σε bytes, χρονικός προσδιορισμός)

Τεχνολογικές λύσεις για χρέωση βάσει εφαρμογής είναι:

- NetFlow
- RADIUS/TACACS+
- RMON
- Service Assurance Agent (SAA)

1.3.4 Χρέωση VoIP

Η χρέωση της μετάδοσης φωνής έχει πολλές προκλήσεις, καθώς πολλά και διαφορετικά θέματα θα πρέπει να ληφθούν υπόψιν:

1) Χρέωση του τελικού χρήστη (πάγια χρέωση, ανά κλήση, ανά χαρακτηριστικό κλήσης, ανά κατηγορία υπηρεσίας (Class of Service - CoS), ανάλογα με την απόσταση και τον χρόνο χρήσης του δικτύου)
2) Χρέωση για εξυπηρέτηση κλήσεων από το δημόσιο τηλεφωνικό δίκτυο (PSTN) (ανά κλήση, ανά τελικό όγκο κλήσης)
3) Χρέωση για την εξυπηρέτηση κλήσεων προς άλλους παρόχους υπηρεσιών VoIP (ανάλογα με το εύρος ζώνης, την ποιότητα της υπηρεσίας (QoS) και τον χρόνο)
4) Μελέτη της κίνησης για τη μετάδοση φωνής (τύπος κλήσης, χαρακτηριστικά χρήσης)

Ο τρόπος και το είδος των δεδομένων που θα πρέπει να συλλεχθούν εξαρτώνται από το επιχειρηματικό μοντέλο του παρόχου (δηλαδή, πάγια χρέωση ή χρέωση ανά κλήση, προπληρωμένη ή πληρωμή μετά τη χρήση της υπηρεσίας) καθώς και τις λεπτομέρειες της υπηρεσίας οι οποίες χρεώνονται (δηλαδή, η χρονική διάρκεια, το έυρος ζώνης, η ποιότητα της υπηρεσίας, η χρήση διάφορων χαρακτηριστικών). Η καταγραφή στοιχείων κλήσης (Call Detail Records - CDRs), οι οποίες περιγράφουν τα παραπάνω στοιχεία, παράγονται και συλλέγονται από το δίκτυο.

Χρέωση του τελικού χρήστη: Οι CDRs παρέχουν τις απαραίτητες λεπτομέρειες για τη χρέωση με βάση τη χρήση. Αν το εύρος ζώνης ή η παρεχόμενη ποιότητα της υπηρεσίας είναι απαραίτητες για χρέωση, το χαρακτηριστικό Netflow μπορεί να παρέχει κάποιες από τις πληροφορίες αυτές, αν και θα πρέπει να γίνει διεξοδική συσχέτιση με τις CDRs. Αν χρησιμοποιείται το μοντέλο προπληρωμένης χρέωσης, τότε η υπηρεσία RADIUS (Remote Authentication Dial-In User Service) παρέχει την απαιτούμενη υποδομή.

Πάροχοι υπηρεσιών ή δημόσιου τηλεφωνικού δικτύου: Οι απαραίτητες πληροφορίες μπορούν να προέλθουν από τις CDRs (από τους πράκτορες κλήσεων (call agents) ή τις πύλες Secure System 7 (SS7)). Σχετικά με την χρέωση μεταξύ ομότιμων παρόχων υπηρεσιών, οι αναγκαίες πληροφορίες για τον υπολογισμό του κόστους μπορούν να προέλθουν από το Netflow. Στις περιπτώσεις αυτές ενδιαφέρει περισσότερο η καταγραφή της χρήσης του διαθέσιμου εύρου ζώνης παρά κάθε μιας κλήσης.

Traffic studies: Οι CDRs μπορούν να χρησιμοποιηθούν για λεπτομερή ανάλυση θεμάτων των τηλεφωνικών υπηρεσιών (πρότυπα κλήσεων και χρησιμοποίηση χαρακτηριστικών) ενώ το Netflow μπορεί να παρέχει λεπτομερή ανάλυση της χρήσης του εύρους ζώνης.

Τεχνολογικές λύσεις για χρέωση του VoIP:

- CDR
- Radius/TACACS+
- SAA

1.3.5 Χρέωση βάσει της χρήσης

Τα κεφάλαια που είχαν δαπανηθεί την προηγούμενη δεκαετία για την υποδομή πληροφοριακών συστημάτων από επιχειρήσεις και παρόχους δικτυακών υπηρεσιών είχαν παρουσιάσει σταθερό ρυθμό αύξησης και οι επενδύσεις αυτές θα πρέπει τώρα να επιφέρουν εισοδήματα. Επιπλέον, η εξάρτηση των επιχειρήσεων και των οργανισμών από τις τεχνολογίες δικτύων αυξάνεται συνεχώς. Τέλος, η τρέχουσα τεχνολογία έχει κάνει τη χρέωση βάσει της χρήσης και πρακτικά εφικτή. Επομένως, οι τεχνολογίες αυτές δίνουν τη δυνατότητα σε έναν πάροχο να υλοποιήσει τα εξής:

- Χρέωση των επιμέρους τμημάτων μιας επιχείρησης ή πελατών

- Δίκαιη δέσμευση πόρων μεταξύ των τμημάτων μιας επιχείρησης ή πελατών
- Ανάλυση χρήσης του δικτύου από τους πελάτες ή τα τμήματα της επιχείρησης
- Χρέωση του τελικού χρήστη
- Στρατηγική δέσμευση πόρων του δικτύου
- Μείωση του κόστους
- Προσαρμογή επιπρόσθετων υπηρεσιών στο διαθέσιμο εύρος ζώνης

Τεχνολογίες που μπορούν να χρησιμοποιηθούν για τη χρέωση βάσει της χρήσης είναι:

- Border Gateway Protocol Policy Accounting (BGP PA)/Destination Sensitive Billing (DSB)
- Καταγραφή στοιχείων κλήσης (CDR)
- Σύστημα καταγραφής και ανάλυσης δικτυακής κίνησης (IP Accounting, MAC Accounting, Precedence Accounting)
- NetFlow
- Radius
- TACACS+
- RMON
- SNMP

1.3.6 Εγγυήσεις σε επίπεδο υπηρεσίας (Service-Level Agreements - SLA)

Η χρέωση από έναν πάροχο δικτυακών υπηρεσιών βάσει της χρήσης είναι σίγουρα ένα πλεονέκτημα σε σχέση με την πάγια χρέωση των υπηρεσιών κάποιου άλλου παρόχου. Επιπλέον, οι πάροχοι παρέχουν νέες δυνατότητες ευέλικτης χρέωσης για διάφορες υπηρεσίες και εφαρμογές προστιθέμενης αξίας. Για την αποδοτικότερη ανάπτυξη υψηλότερου επιπέδου ποιότητας υπηρεσιών χρησιμοποιούνται τα Service-Level Agreements, τα οποία είναι συμβάσεις βάσει των οποίων οι πάροχοι είναι υποχρεωμένοι να παρέχουν συγκεκριμένες εγγυήσεις ανάλογα με το επίπεδο που επιλέγεται. Οι εγγυήσεις σχετίζονται με τον μέγιστο χρόνο που η υπηρεσία μπορεί να μην είναι διαθέσιμη, το εύρος ζώνης ή τους χρόνους απόκρισης. Επομένως, χρειάζεται ένας μηχανισμός παρακολούθησης από την πλευρά του παρόχου, αλλά κυρίως από την πλευρά του πελάτη, ώστε να εξακριβωθεί ότι οι εγγυήσεις της σύμβασης τηρούνται. Ανεξάρτητα όμως από τις εγγυήσεις των υπηρεσιών, η χρέωση πρέπει να είναι ακριβής και επομένως είναι απαραίτητη και πολύ μεγάλης σημασίας.

Συνοπτικά, τα Service-Level Agreements δίνουν τη δυνατότητα στον πάροχο δικτυακών υπηρεσιών να πετύχει τα εξής:

- Παροχή υψηλού επιπέδου υπηρεσιών
- Υλοποίηση ανταγωνιστικών πακέτων υπηρεσιών

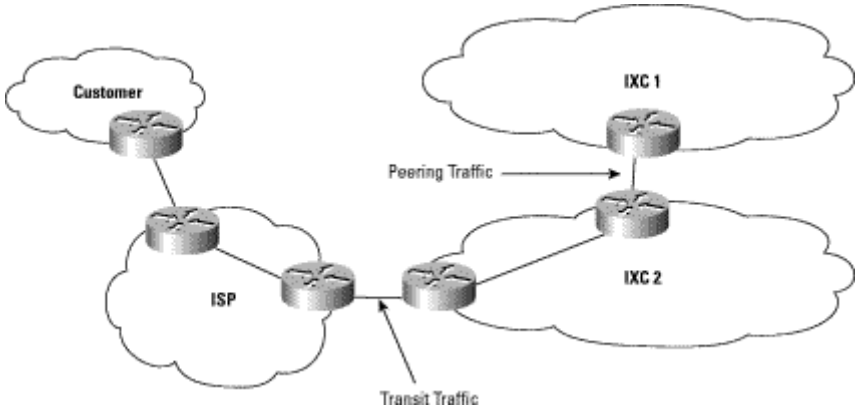
Τεχνολογίες που μπορούν να χρησιμοποιηθούν είναι:

- NetFlow
- RMON
- Service Assurance Agents (SAA)

- SNMP

1.3.7 Peering και Transit κίνηση

Peering χαρακτηρίζεται η κίνηση που ανταλλάσσεται μεταξύ ομότιμων παρόχων δικτυακών υπηρεσιών ενώ Transit ονομάζεται η κίνηση που διέρχεται από το δίκτυο ενός παρόχου και ανήκει σε κάποιον από τους παρόχους πελάτες του (Σχήμα 1). Όπως είναι προφανές οι πάροχοι και στις δύο περιπτώσεις χρεώνουν με βάση τον όγκο της κίνησης και τις συμφωνίες που έχουν συνάψει.



Σχήμα 1) Peering και Transit κίνηση

Στις περιπτώσεις αυτές, τα εργαλεία καταγραφής και ανάλυσης δικτυακής κίνησης μπορούν να χρησιμοποιηθούν για να δώσουνς απαντήσεις σε καίρια ερωτήματα που σχετίζονται με:

- Τον υπολογισμό της χρέωσης
- Την επαλήθευση της χρέωσης
- Την αξιολόγηση μιας συμφωνίας
- Την ανεύρεση εναλλακτικών λύσεων
- Τη διάκριση της κίνησης σε Peering και Transit
- Την ανάπτυξη και σχεδίαση του δικτύου

Τεχνολογίες που μπορούν να χρησιμοποιηθούν είναι:

- BGP Policy Accounting / DSB
- IP Accounting
- NetFlow
- SNMP

1.4 ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΤΑΓΡΑΦΗΣ ΚΑΙ ΑΝΑΛΥΣΗΣ ΔΙΚΤΥΑΚΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ (NETWORK ACCOUNTING)

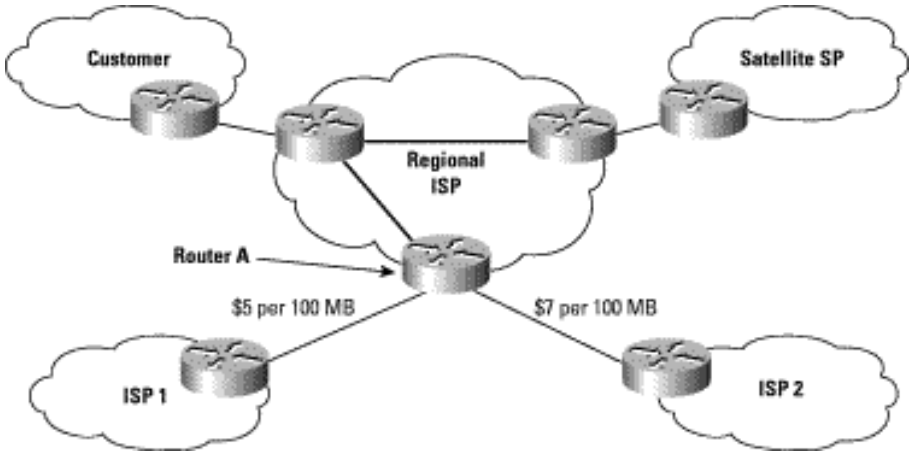
1.4.1 Border Gateway Protocol Policy Accounting (BGP PA)/Destination Sensitive Billing (DSB)

Το BGP policy accounting μετρά και κατηγοριοποιεί την κίνηση από και προς τις διάφορες ομότιμες οντότητες του δικτύου. Δίνει στους παρόχους δικτυακών υπηρεσιών ένα μέσο για τη χρέωση των πελατών τους με βάση τη δικτυακή διαδρομή που θα ακολουθήσει η κίνηση του

δικτύου τους και όταν απαιτηθεί μπορεί να κάνει διάκριση μεταξύ της εσωτερικής ή τοπικής κίνησης μέσα σε ένα τομέα δικτύου (domain) και της εξωτερικής κίνησης (εκτός του τομέα).

Η κατηγοριοποίηση της κίνησης μπορεί να γίνει με βάση τον αριθμό αυτόνομου συστήματος (Autonomous System Number - ASN), τη διαδρομή των αυτόνομων συστημάτων ή άλλες ιδιότητες και μπορεί να υλοποιηθεί από τους δρομολογητές. Τα δεδομένα που συλλέγουν οι δρομολογητές μπορούν στη συνέχεια να ανακτηθούν για να επεξεργαστούν μέσω του SNMP.

Επομένως, το BGP policy accounting μπορεί να χρησιμοποιηθεί για την καταγραφή και χρέωση της κίνησης των πελατών, ανάλογα με τη δικτυακή διαδρομή που αυτή ακολουθεί. Για παράδειγμα, μπορεί να υπάρξει διαφορετική πολιτική χρέωσης ανάλογα με το αν η κίνηση δρομολογείται μέσω ενός εγχώριου, διεθνούς ή δορυφορικού δικτύου, όπως παρουσιάζεται στο Σχήμα 2.



Σχήμα 2) Χρέωση πελατών ανάλογα με το δίκτυο δρομολόγησης

Το Destination Sensitive Billing (DSB) έχει το χαρακτηριστικό ότι συνδυάζει τη λειτουργικότητα του BGP policy accounting με χαρακτηριστικά του QoS. Με τον τρόπο αυτό οι πελάτες μπορούν να χρεωθούν όχι μόνο με βάση τον όγκο και τη διαδρομή δρομολόγησης της κίνησης, αλλά και με την ποιότητα υπηρεσιών που έχουν ζητήσει.

Τα πλεονεκτήματα της χρώσης με βάση τις δυνατότητες που παρέχει το BGP είναι τα εξής:

- Εύκολη υλοποίηση (υποστήριξη από το υλικό)
- Ανάκτηση των στοιχείων κίνησης μέσω του SNMP
- Δυνατότητα εύκολης διάκρισης της κίνησης ανάλογα με τον αριθμό αυτόνομου συστήματος (ASN)

1.4.2 Σύστημα καταγραφής στοιχείων κλήσης (Call Detail Recording – CDR)

Το σύστημα καταγραφής στοιχείων κλήσης (Call Detail Recording - CDR) είναι ένας γενικός όρος που χρησιμοποιείται κυρίως στα τηλεφωνικά δίκτυα και στις υπηρεσίες μετάδοσης φωνής των δικτύων, για να περιγράψει πληροφορίες κάθε κλήσης και χρησιμοποιούνται στην πλειοψηφία των περιπτώσεων για σκοπούς χρέωσης. Τα συστήματα αυτά είναι ιδιαίτερα σημαντικά στη σύγχρονη εποχή όπου επιχειρείται αλλά και χρησιμοποιείται στην πράξη η ολοκλήρωση της μετάδοσης φωνής και δεδομένων.

Στα συστήματα CDR, τα στοιχεία συλλέγονται κατά τη διάρκεια της κλήσης και η τελική εγγραφή που περιγράφει την κλήση (σταθερού ή μεταβλητού μήκους) παράγεται στο τέλος της κλήσης. Τα στοιχεία που καταγράφονται μπορεί να είναι ο αριθμός του καλούμενου και του καλούντα, τα ονόματα του τοπικού και του απομακρυσμένου κόμβου, χρονικές διάρκειες, χρονικές στιγμές διαφόρων γεγονότων, πληροφορίες για την περίπτωση αποτυχίας της κλήσης (Call Failure Class

fields) κτλ.

Για την υλοποίηση των τεχνολογιών ολοκλήρωσης μετάδοσης φωνής και δεδομένων μπορούν να χρησιμοποιηθούν εξειδικευμένες συσκευές ή και δρομολογητές οι οποίοι παρέχουν υπηρεσίες ελέγχου και διασύνδεσης μεταξύ δικτύων δεδομένων και τηλεφωνικών δικτύων. Η καταγραφή των CDRs γίνεται από τις συσκευές αυτές

Θα πρέπει να αναφερθεί ότι τα CDRs περιγράφουν μια έννοια και όχι ένα συγκεκριμένο πρότυπο, αν και υπάρχουν ορισμένα σχετικά πρότυπα. Χρησιμοποιούνται κυρίως για τη χρέωση τόσο τελικών χρηστών όσο και παρόχων υπηρεσιών. Ορισμένες επιχειρήσεις χρησιμοποιούν τα CDRs και για την ανάλυση του δικτύου και της χρήσης των υπηρεσιών.

Στα πλεονεκτήματα των CDRs θα αναφερθεί ότι αποτελούν μια καλή και δοκιμασμένη τεχνολογία για την ανάπτυξη υπηρεσιών φωνής, όμως σημαντικό μειονέκτημά τους είναι η έλλειψη προτύπων. Αυτό σημαίνει ότι απαιτείται δυνατότητα υποστήριξης δικτύων διαφορετικών κατασκευαστών.

1.4.3 Σύστημα καταγραφής και ανάλυσης δικτυακής κίνησης (IP Accounting)

Η υλοποίηση του IP accounting βασίζεται στη δυνατότητα του δρομολογητή να συλλέγει πληροφορίες για την κίνηση που δρομολογεί με βάση την IP διεύθυνση του αποστολέα και του παραλήπτη των πακέτων. Ο δρομολογητής διατηρεί μετρητές για το πλήθος των πακέτων και των bytes που δρομολογούνται και οι οποίοι αυξάνονται συνεχώς.

Υπάρχουν διάφορες παρόμοιες υλοποιήσεις του IP Accounting, όπως IP MAC address accounting και IP Precedence accounting.

Το IP MAC address accounting των δρομολογητών έχει τη ίδια φιλοσοφία με το IP Accounting με τη διαφορά ότι η κίνηση κατηγοριοποιείται με βάση τη MAC (Medium Access Control) διεύθυνση του αποστολέα και του παραλήπτη των πακέτων. Ο δρομολογητής διατηρεί μετρητές των πακέτων και των bytes που σχετίζονται με κάθε μοναδική διεύθυνση MAC. Το χαρακτηριστικό αυτό μπορεί να χρησιμοποιηθεί για να διαπιστωθεί πόση κίνηση διακινήθηκε από και προς κόμβους και υπολογιστές που είναι συνδεδεμένοι στον δρομολογητή.

Το χαρακτηριστικό IP Precedence accounting παρέχει τη δυνατότητα παρακολούθησης του όγκου της κίνησης, όπως και τα παραπάνω, αλλά η κατηγοριοποίηση γίνεται με βάση την διεπαφή (interface) του δρομολογητή από το οποίο δρομολογείται η κίνηση.

Βασικό πλεονέκτημα των παραπάνω χαρακτηριστικών είναι η απλότητα και η ευκολία υλοποίησής τους. Σε όλες τις περιπτώσεις η λειτουργία υποστηρίζεται από τον δρομολογητή. Επίσης, θετικό είναι και το γεγονός ότι η ανάκτηση των αντίστοιχων δεδομένων γίνεται μέσω του SNMP. Μειονέκτημα είναι ίσως, ανάλογα και με τις ανάγκες που καλούνται να καλύψουν, η μικρή λεπτομέρεια στοιχείων κίνησης, σε σχέση τουλάχιστο και με άλλες μεθόδους.

1.4.4 NetFlow

Το NetFlow είναι ένα υψηλής απόδοσης χαρακτηριστικό το οποίο υλοποιείται μόνο από ορισμένα μοντέλα δρομολογητών και στοιχείων μεταγωγής της εταιρίας CISCO. Παρέχει τη δυνατότητα συλλογής ενός πλούσιου συνόλου στατιστικών κίνησης από τους δρομολογητές, ταυτόχρονα με τη δρομολόγηση των πακέτων. Τα στατιστικά που συλλέγονται, αποτελούνται από στοιχεία περιγραφής ροών κίνησης (flows), οι οποίες είναι μονής κατεύθυνσης ακολουθίες από πακέτα ανάμεσα σε ένα ζεύγος αποστολέα και παραλήπτη, που χρησιμοποιούν το ίδιο πρωτόκολλο. Οι πληροφορίες που συλλέγονται μπορούν να χρησιμοποιηθούν σε μια πληθώρα περιπτώσεων όπως ανάλυση και σχεδίαση δικτύων, διαχείριση δικτύων, χρέωση κτλ.

Λόγω του ότι τα flows περιγράφουν κίνηση μονής κατεύθυνσης, τα flows από έναν πελάτη προς ένα εξυπηρετητή είναι διαφορετική για την αντίθετη φορά. Επίσης, τα flows διακρίνονται και με βάση το πρωτόκολλο. Για παράδειγμα, πακέτα HTTP που αποστέλλονται σε ένα πελάτη από έναν

συγκεκριμένο εξυπηρετητή αποτελούν διαφορετικό σύνολο από flows στην περίπτωση που μεταδίδονται πακέτα FTP μεταξύ των δύο ίδιων υπολογιστών και προς την ίδια κατεύθυνση.

Τα χαρακτηριστικά της κίνησης που μπορεί να καταγράφει ένας δρομολογητής με ενεργοποιημένο το χαρακτηριστικό NetFlow είναι τα εξής:

- IP αποστολέα και παραλήπτη
- Αριθμός δικτυακής θύρας αποστολέα και παραλήπτη
- Τύπος πρωτοκόλλου
- Τύπος υπηρεσίας (Type of Service - ToS)
- Διεπαφή (interface) εισόδου δρομολογητή

Τα παραπάνω πεδία προσδιορίζουν ένα μοναδικό flow. Αν ένα flow έχει ένα από τα παραπάνω πεδία διαφορετικό, τότε θεωρείται διαφορετικό flow. Ένα flow περιλαμβάνει και άλλα πεδία στατιστικών τα οποία είναι:

- Πλήθος πακέτων και bytes
- Χρονικές στιγμές έναρξης και λήξης
- Διεπαφή (interface) εισόδου δρομολογητή
- Πληροφορίες δρομολόγησης (next-hop address, αριθμός αυτόνομου συστήματος (ASN) αποστολέα και παραλήπτη, source prefix mask, destination prefix mask)

Το NetFlow είναι μια λύση η οποία αποτελείται από τρία μέρη:

1. Αποστολέας στοιχείων κίνησης

Η υλοποίηση του NetFlow από τον δρομολογητή εξαρτάται από τον τύπο του δρομολογητή και την έκδοση του NetFlow που χρησιμοποιείται. Ο δρομολογητής χρησιμοποιεί μνήμη εναποθήκευσης μέσα στην οποία γίνεται ως ένα βαθμό συγχώνευση των flows με βάση τα ταυτοτικά τους χαρακτηριστικά. Στη συνέχεια τα στοιχεία κίνησης που έχει οργανώσει ο δρομολογητής αποστέλλονται σε προκαθορισμένο υπολογιστή που τρέχει το κατάλληλο λογισμικό για την καταγραφή σε αρχεία και την επεξεργασία των δεδομένων.

Τα στοιχεία και ο όγκος των δεδομένων που αποστέλλει ο δρομολογητής εξαρτώνται από τις δυνατότητες του δρομολογητή και από το σχήμα συγχώνευσης (aggregation scheme) που έχει επιλεγεί να υλοποιήσει ο δρομολογητής. Κάθε σχήμα συγχώνευσης υποστηρίζει διαφορετικά πεδία στα στοιχεία κίνησης. Επίσης, ο όγκος των στοιχείων κίνησης είναι μια πολύ σημαντική παράμετρος. Ιδίως σε μεγάλα δίκτυα απαιτείται να γίνεται από τον δρομολογητή συγχώνευση των flows σε μεγάλο βαθμό, ώστε να μειωθεί ο όγκος τους που επηρεάζει τόσο την απόδοση του λογισμικού καταγραφής σε αρχεία των στοιχείων κίνησης όσο και την παραπέρα απαιτούμενη επεξεργασία. Οι τελευταίες προτάσεις της CISCO σχετικά με το NetFlow και τον όγκο των δεδομένων σχετίζονται κυρίως με δειγματοληπτική συλλογή των flows.

Μια άλλη σημαντική παράμετρος είναι η επιλογή του δρομολογητή του δικτύου που θα αναλάβει την αποστολή των flows. Συνήθως είναι προτιμότερο να ενεργοποιείται το χαρακτηριστικό NetFlow στους συνοριακούς δρομολογητές του δικτύου, αντί για τους δρομολογητές του δικτύου κορμού. Η τελική επιλογή εξαρτάται από το είδος του accounting που απαιτείται να γίνει και τις δυνατότητες των δρομολογητών.

2. Ενδιάμεσες συσκευές (Cisco NetFlow FlowCollector)

Ο Cisco NetFlow FlowCollector είναι μία UNIX εφαρμογή που συλλέγει δεδομένα NetFlow που αποστέλλουν ένα σύνολο από δρομολογητές με το χαρακτηριστικό NetFlow ενεργοποιημένο. Ο NetFlow FlowCollector έχει επίσης τη δυνατότητα να υλοποιεί συγχώνευση των δεδομένων σε

δεύτερο επίπεδο με σκοπό τη μείωση του όγκου τους. Τελικός σκοπός του είναι η δημιουργία αρχείων με τα στοιχεία κίνησης που απέστειλα οι δρομολογητές για την περαιτέρω επεξεργασία τους. Έχει πολλές άλλες δυνατότητες όπως δυνατότητα επιλογής σχήματος συγχώνευσης, δημιουργία φίλτρων κίνησης, συμπίεσης των παραγόμενων αρχείων, ορισμού πρωτοκόλλων κτλ.

3. Εργαλεία ανάλυσης στοιχείων κίνησης (Cisco Network Data Analyzer)

Σκοπός του Network Data Analyzer είναι η ανάλυση και παρουσίαση των στοιχείων κίνησης που έχει αποθηκεύσει ο NetFlow FlowCollector μέσω γραφικού περιβάλλοντος. Επιτρέπει τη σχεδόν σε πραγματικό χρόνο ανάλυση και παρουσίαση της κίνησης του δικτύου παράγοντας γραφήματα και αναλύσεις τάσεις. Στο Σχήμα 3 παρουσιάζεται παράδειγμα χρήσης του Network Data Analyzer.

Εκτός από το Network Data Analyzer, υπάρχουν πλήθος άλλων εφαρμογών που παρέχουν τη δυνατότητα ανάλυσης των στοιχείων κίνησης του NetFlow Collector και μάλιστα με διαφορετικές προσεγγίσεις (ασφάλεια, αντιμετώπιση προβλημάτων, σχεδίαση δικτύου κτλ.).

Σχήμα 3) Παράδειγμα χρήσης του Network Data Analyzer

Μια επέκταση του NetFlow είναι η καταγραφή flows και με βάση τις ετικέτες MPLS (Multi Protocol Layer Switching) κατά τη δρομολόγηση και ονομάζεται NetFlow MPLS Egress. Κύριο πλεονέκτημα είναι η καταγραφή της κίνησης από και προς ιδεατά ιδιωτικά δίκτυα (Virtual Private Networks - VPNs).

1.4.5 RADIUS

Το RADIUS είναι ένα πρωτόκολλο πιστοποίησης εξουσιοδότησης και καταγραφής δραστηριότητας (Authentication Authorization Accounting - AAA) που χρησιμοποιείται στους εξυπηρετητές πρόσβασης (access servers) και είναι πολύ δημοφιλές στους παρόχους δικτυακών υπηρεσιών και της μεγάλες εταιρίες.

Οι εξυπηρετητές πρόσβασης παρέχουν τη δυνατότητα απομακρυσμένης σύνδεσης στο Διαδίκτυο ή το εσωτερικό δίκτυο εταιρίας ή οργανισμού μέσω modem συνήθως. Η καταγραφή στοιχείων σχετικά με τις συνδέσεις των χρηστών και τις δραστηριότητές τους είναι πολύ σημαντική για την ασφάλεια, τη χρέωση και την ποιότητα των υπηρεσιών που προσφέρει ο πάροχος δικτυακών υπηρεσιών. Επίσης, το RADIUS παρέχει τη δυνατότητα ορισμού συγκεκριμένων ρυθμίσεων ανά χρήστη ανώ η πιστοποίησή τους γίνεται με τη βοήθεια βάσης δεδομένων, γεγονός που βοηθάει σημαντικά σε θέματα διαχείρισης.

Κάθε μια από τις τρεις υπηρεσίες του RADIUS μπορούν να χρησιμοποιηθούν και ανεξάρτητα. Στην καταγραφή στοιχείων (accounting), γίνεται καταγραφή των δεδομένων στην αρχή και το τέλος της συνόδου. Τα δεδομένα αυτά αναφέρονται στους πόρους του δικτύου που χρησιμοποιήθηκαν (χρόνος σύνδεσης, πακέτα, bytes, ιστορικό ενεργειών κτλ)

Το πρωτόκολλο RADIUS βασίζεται στο μοντέλο πελάτη – εξυπηρετητή. Ο εξυπηρετητής πρόσβασης δικτύου αποτελεί τον πελάτη ο οποίος αποστέλλει στοιχεία για κάθε σύνοδο στον

εξυπηρετητή RADIUS, ο οποίος είτε καταγράφει στατιστικά στοιχεία, είτε υλοποιεί την πιστοποίηση και εξουσιοδότηση του χρήστη, δίνοντας την εντολή στον εξυπηρετητή πρόσβασης δικτύου να αποδεχθεί ή να απορρίψει τη σύνδεση. Επίσης, διατηρεί τη βάση δεδομένων των χρηστών και των ρυθμίσεών τους. Το RADIUS μπορεί να χρησιμοποιηθεί και για τη χρέωση και έλεγχο εφαρμογών VoIP.

1.4.6 TACACS+

Ένα άλλο πρωτόκολλο παρόμοιο με το RADIUS είναι το TACACS (Terminal Access Control Access Control System). Έχουν την ίδια λειτουργικότητα και η βασική τους διαφορά είναι στον τρόπο επικοινωνίας του εξυπηρετητή πρόσβασης δικτύου και τον εξυπηρετητή TACACS. Στην περίπτωση του RADIUS χρησιμοποιείται το πρωτόκολλο UDP (connectionless), ενώ το TACACS χρησιμοποιεί το TCP (connection oriented), γεγονός που το καθιστά περισσότερο αξιόπιστο.

1.4.7 RMON

Το RMON είναι ένα πρωτόκολλο παρακολούθησης δικτύου. Η πρώτη έκδοσή του (RMON1) όριζε την παρακολούθηση δικτυακής κίνησης στο επίπεδο MAC. Η δεύτερη έκδοση ορίζει τις προδιαγραφές για την παρακολούθηση του δικτύου μέσω του επιπέδου εφαρμογής του OSI. Το RMON αναγνωρίζει τη δραστηριότητα ανεξάρτητων κόμβων του δικτύου, εξετάζοντας κάθε πλαίσιο που διακινείται στο τοπικό δίκτυο.

Βασικά πλεονεκτήματα του RMON είναι τα εξής:

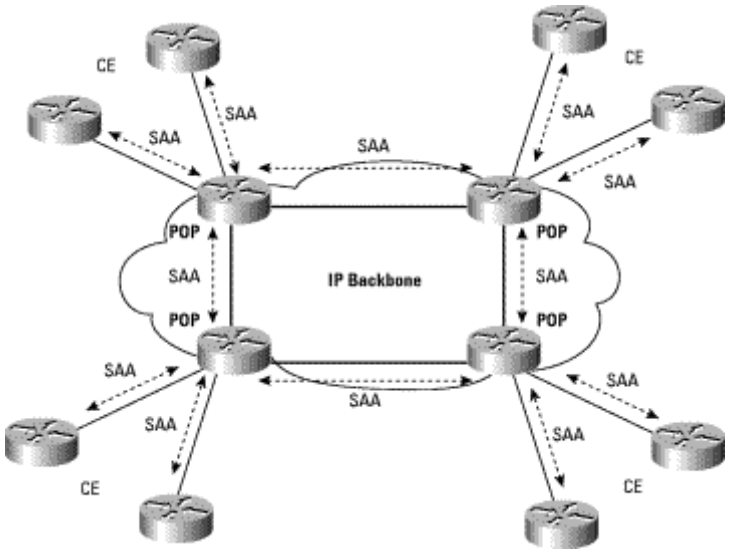
- Συλλογή στατιστικών για τα επίπεδα 2-7 του μοντέλου OSI
- Παρακολούθηση και άλλων πρωτοκόλλων εκτός του IP (για παράδειγμα IPX)
- Το RMON1 έχει χαμηλές απαιτήσεις σε επεξεργαστική ισχύ (σε αντίθεση με το RMON2)
- Είναι πολύ ισχυρό εργαλείο για το επίπεδο MAC

1.4.8 Πράκτορας εγγύησης υπηρεσιών (Service Assurance Agent)

Ο πράκτορας εγγύησης υπηρεσιών (Service Assurance Agent - SA Agent) είναι ένα εργαλείο που υλοποιείται από τους δρομολογητές της εταιρίας CISCO και σκοπός του είναι η συλλογή πληροφοριών σχετικά με την απόδοση του δικτύου, όπως χρόνοι απόκρισης, απώλεια πακέτων, χρόνοι φόρτωσης ιστοσελίδων καθώς και άλλα στατιστικά στοιχεία σε πραγματικό χρόνο. Ακόμη, παρέχει μηχανισμούς για την παρακολούθηση ανά κατηγορία κίνησης πάνω από την ίδια σύνδεση.

Η λειτουργία των Service Assurance Agents βασίζεται στην κατασκευή και αποστολή πακέτων σε προκαθορισμένες συσκευές προορισμού. Η απόδοση μετράται με βάση τον χρόνο που απαιτείται για την επιστροφή των πακέτων και το πλήθος των πακέτων που επιστρέφουν (λειτουργεί όπως το PING). Αν ο προορισμός είναι συσκευή της CISCO μπορεί να ρυθμιστεί ως SA Responder, παράγοντας ακριβέστερα αποτελέσματα. Τα στατιστικά από την παραπάνω διαδικασία μπορούν να ανακτηθούν μέσω SNMP.

Βασικά πλεονεκτήματα των Service Assurance Agents είναι η ακριβής μέτρηση της απόδοσης σε πραγματικό χρόνο, η παρακολούθηση κατηγοριών κίνησης από άκρο σε άκρο και η υποστήριξη του SNMP. Ένα μειονέκτημα ίσως είναι ότι στο δίκτυο διακινούνται πακέτα για την παρακολούθηση του δικτύου που ίσως επηρεάσουν την απόδοσή του.



Σχήμα 4) Η λειτουργία των Service Assurance Agents

1.4.9 Simple Network Management Protocol (SNMP)

Το SNMP μπορεί να χαρακτηριστεί περισσότερο ως μία μέθοδο ανάκτησης δεδομένων από συσκευές δικτύου, παρά ως μία τεχνολογία για accounting. Παρολαυτά, οι δυνατότητες που παρέχει και το πλήθος των πληροφοριών που μπορούν να ανακτηθούν από διαφόρων τύπων και κατασκευαστών συσκευές είναι πολύ μεγάλο και συναγωνίζεται όλες τις παραπάνω τεχνολογίες.

Είναι ένα πρωτόκολλο του επιπέδου εφαρμογής που χρησιμοποιείται για την ανταλλαγή πληροφοριών διαχείρισης μεταξύ συσκευών δικτύου. Επιτρέπει στους διαχειριστές τη βελτιστοποίηση του δικτύου, τον εντοπισμό και επίλυση βλαβών και τέλος τη σχεδίαση της ανάπτυξης ενός δικτύου.

Το SNMP αποτελείται από τα εξής μέρη:

i) SNMP manager: Αποτελεί μέρος της πλατφόρμας διαχείρισης ενός δικτύου (NMS).

ii) SNMP agent: Ο agent βρίσκεται εγκατεστημένος στις συσκευές που παρακολουθούνται. Μπορεί να αποστέλλει αυτόβουλα πληροφορίες στον manager για να δηλώσει κάποιο γεγονός ή να ανταποκρίνεται σε αιτήματα του manager.

iii) MIB: Αποτελεί ένα ιδεατό σύνολο από διαχειριστικές πληροφορίες που παρακολουθεί ο agent και οι οποίες μπορούν να ανακτηθούν για οποιονδήποτε διαχειριστικό σκοπό. Τα αντικείμενα που περιλαμβάνει μια MIB (Management Information Base) είναι οργανωμένες σε δενδρική δομή και άλλες είναι τυποποιημένες και άλλες προστίθενται από τον εκάστοτε κατασκευαστή.

Οι επιτρεπόμενες λειτουργίες στα αντικείμενα της MIB είναι :

- Get – Ανάγνωση της τιμής ενός αντικειμένου
- GetNext – Ανάγνωση του επόμενου αντικειμένου
- GetResponse – Επιστροφή απάντησης σε ερώτημα Get
- Set – Ορισμός τιμής αντικειμένου
- Trap – Αποστολή τιμής αντικειμένου στον manager για να δηλώσει κάποιο γεγονός

2 ΜΕΛΕΤΗ ΕΦΑΡΜΟΓΩΝ

Στο κεφάλαιο αυτό αναφέρονται περιπτώσεις Παρόχων δικτυακών υπηρεσιών που προκειμένου να εξασφαλίσουν στους χρήστες τους την ποιότητα υπηρεσιών, χρησιμοποιούν διάφορα εργαλεία καταγραφής και ανάλυσης της δικτυακής δραστηριότητας (network accounting). Για κάθε μια από τις περιπτώσεις παρουσιάζεται και το αντίστοιχο εργαλείο που χρησιμοποιείται.

2.1 MANNET

Το γραφείο υπολογιστών (MCB) ιδρύθηκε το 1970 στο νησί Man, αρχικά ως γραφείο κατανομής χρόνου για τις βιομηχανίες μισθοδοτικών καταστάσεων, λογιστικής και τραπεζικών εργασιών. Σχεδόν 6 έτη πριν την ίδρυση του, ο καπετάνιος Stuart McKenzie που ήταν και ο ιδρυτής της MCB ίδρυσε τον πρώτο Πάροχο Δικτυακών υπηρεσιών στο νησί με το όνομα Mannet και τον 26^{ο} της Βρετανίας. Η μοναδική κατάσταση που επικρατούσε στο νησί σήμαινε την ακμή των επιχειρήσεων μέσα σε ένα εντελώς διαφορετικό περιβάλλον από ότι στην ηπειρωτική χώρα. Τις υπηρεσίες του Mannet δεν χρησιμοποιούσαν μόνο οι τοπικές επιχειρήσεις αλλά η εταιρία προσέλκυε σημαντικό ποσοστό των εταιριών σε παγκόσμιο επίπεδο εξαιτίας της ενιαίας της δομής και της γενικότερης πολιτικής σταθερότητας που υπήρχε στο νησί.

Για την Mannet το πρόβλημα της διαχείρισης εύρους ζώνης συχνοτήτων θα μπορούσε ενδεχομένως να περιπλεχτεί περαιτέρω από το γεγονός ότι, αντίθετα από ότι συνέβαινε στην ηπειρωτική χώρα, η μη μετρήσιμη πρόσβαση στο δίκτυο υπήρχε από την 1^{η} Αυγούστου. Οι οργανισμοί τηλεπικοινωνίας του νησιού πρόσφεραν την υπηρεσία στους συνδρομητές για £6 μηνιαίως για ιδιωτική χρήση και £15 μηνιαίως για επαγγελματική χρήση συν το Φ.Π.Α.

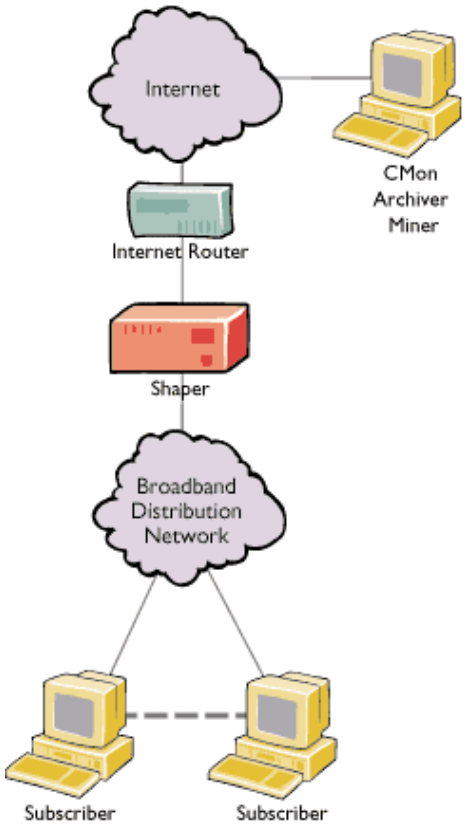
Με τον καιρό όλο και περισσότερες εταιρίες στρέφονται στο Internet για τις διάφορες επιχειρησιακές τους ανάγκες, με αποτέλεσμα να διακινούνται μεγάλες ποσότητες δεδομένων και να χρησιμοποιούνται εφαρμογές με μεγάλες απαιτήσεις σε εύρος ζώνης. Οι παροχείς στην προσπάθεια τους να αντιμετωπίσουν τις εφαρμογές μεγάλων απαιτήσεων σε εύρος ζώνης, οδηγούνται στην δημιουργία πολύπλοκων δικτύων, πλατφόρμων και διεπαφών με αποτέλεσμα να παρέχουν τελικά μη αξιόπιστες υπηρεσίες στους χρήστες τους. Είναι επομένως απαραίτητο ο Παροχέας να μπορεί να ελέγχει αποδοτικά τη διάθεση του εύρους ζώνης. Ο μόνος τρόπος για να γίνει αυτό είναι να ελέγχεται το εύρος ζώνης σε πραγματικό χρόνο.

«Προσπαθούσαμε να ελέγχουμε τη χρήση του εύρους ζώνης από την πλευρά των χρηστών μας με το NetScan το οποίο παρόλο που μας έδινε αρκετά λεπτομερείς πληροφορίες της κίνησης, δεν μας τις έδινε σε πραγματικό χρόνο. Αν υπήρχε πρόβλημα στους χρήστες μας εξαιτίας της κακής χρήσης του δικτύου από έναν και μόνο χρήστη τότε αυτό μπορούσαμε απλά να το διαπιστώσουμε εκ των υστέρων και όχι τη στιγμή που συνέβαινε. Χρειαζόμασταν κάποια λύση που θα περιόριζε αυτόματα και θα έλεγχε τη χρήση μέσα σε προκαθορισμένα πλαίσια, ώστε όλες μας οι υπηρεσίες να παρέχονται χωρίς πρόβλημα στους χρήστες μας.»

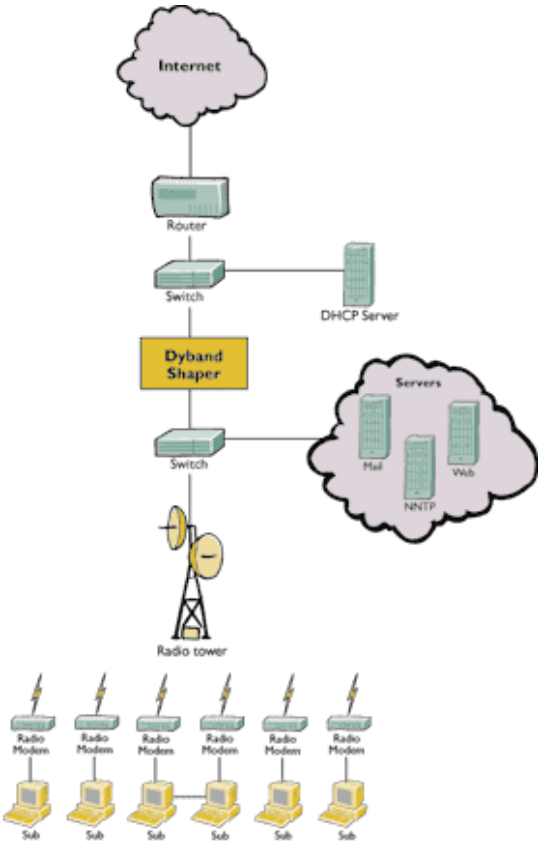
Το Dyband ήταν η λύση στο πρόβλημα της εταιρίας καθώς διαχειρίζεται δυναμικά την κατανάλωση εύρους ζώνης, παρέχει εγγυήσεις για την ποιότητα των υπηρεσιών (Quality of Service) μειώνοντας το κόστος συντήρησης του δικτύου.

Μπορεί κανείς να προμηθευτεί από το δίκτυο το Dyband το οποίο προσφέρεται για δοκιμή για 30 μέρες. Η εταιρία προμηθεύτηκε τη δοκιμαστική έκδοση του πακέτου και αφού πραγματοποίησε με ευκολία την παραμετροποίηση του ώστε να προσαρμοστεί στις ανάγκες του συγκεκριμένου δικτύου, προχώρησε στη χρησιμοποίηση του.

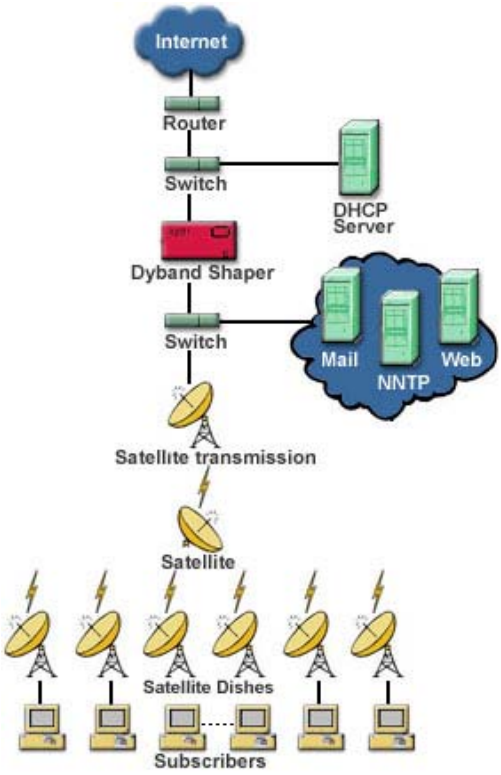
Το Dyband είναι απόλυτα κλιμακωτό δίνοντας τη δυνατότητα στην εταιρία να μπορεί να αντεπεξέρχεται στις απαιτήσεις των χρηστών της. «Το Dyband είναι το μόνο προϊόν που έχω συστήνει ανεπιφύλακτα στα 30 χρόνια που βρίσκομαι στο χώρο των υπολογιστών» δήλωσε ο ιδρυτής της εταιρίας McKenzie. Και συνεχίζει λέγοντας «Για την αποτελεσματική διαχείριση του εύρους ζώνης και τον έλεγχο της κίνησης, είναι το μόνο προϊόν στην αγορά που προσφέρεται με ικανοποιητικό κόστος και αξίζει να επενδύσει κάποιος σε αυτό».



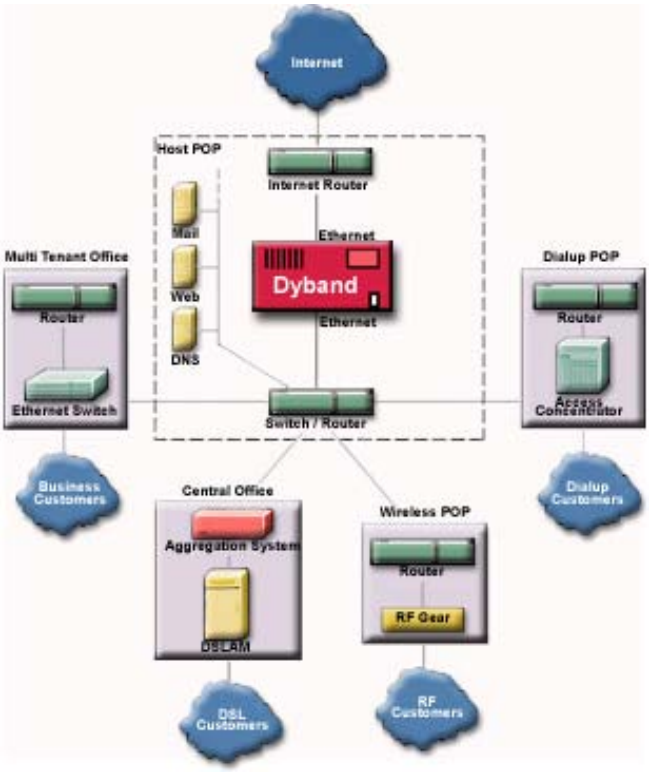
Σχήμα 5) Το Dyband σε ενσύρματο δίκτυο



Σχήμα 6) Το Dyband σε ασύρματο δίκτυο



Σχήμα 7) Το Dyband σε δορυφορικό δίκτυο



Σχήμα 8) Το Dyband σε δίκτυο πολλαπλής πρόσβασης

Το λογισμικό του Dyband είναι το αποτέλεσμα της έρευνας εκατομμυρίων δολαρίων και της προσπάθειας που πραγματοποιήθηκε από τον Ιούνιο του 2001. Τα προϊόντα της Dyband χρησιμοποιούνται σήμερα από πολλούς διεθνείς, εθνικούς και τοπικούς Παροχείς Δικτυακών υπηρεσιών. Το Dyband μετρά και ελέγχει την χρησιμοποίηση του εύρους ζώνης από άτομα και ομάδες, επιτρέποντας στους Παροχείς να ελέγχουν τους «κακούς» χρήστες, να ελαχιστοποιούν την δικτυακή συμφόρηση και να μειώνουν την απώλεια πακέτων. Επίσης, τους δίνει τη δυνατότητα να παρακολουθούν τις υπηρεσίες πρόσβασης σε πραγματικό χρόνο ενώ παράλληλα συλλέγουν τα δεδομένα για ανάλυση με σκοπό τη βελτίωση των υπηρεσιών.

Όταν το Dyband εφαρμόζεται σε ασύρματα δίκτυα, ο ανιχνευτής της κίνησης τοποθετείται μεταξύ του τοπικού δικτύου και του δρομολογητή του Διαδικτύου. Είναι υπεύθυνο για την παρακολούθηση όλης της κίνησης και την παραγωγή στατιστικών στοιχείων σε πραγματικό χρόνο.

Cmon είναι το εργαλείο διεπαφής που χρησιμοποιεί ο διαχειριστής του δικτύου για να βλέπει και να μεταβάλλει την τοπολογία των χρησιμοποιούμενων αντικειμένων και να παρακολουθεί τα στατιστικά σε πραγματικό χρόνο.

Το Dyband χρησιμοποιεί δομή δέντρου για την παρουσίαση των διαχειριζόμενων αντικειμένων. Το σύστημα ανιχνεύει αμέσως τους νεοεισελθόντες στο δίκτυο και τους τοποθετεί στην κατάλληλη θέση στο δέντρο. Το σύστημα αναγνωρίζει τους χρήστες είτε μέσω του DNS server ή του LDAP server ή του RADIUS server και ξεκινά την παρακολούθηση της κίνησης που προκαλούν στο δίκτυο.

Το Dyband κοστίζει ανάλογα με το ποσό του εύρους ζώνης που διαχειρίζεται. Ο πελάτης έχει έκπτωση 90% του κόστους της αρχικής χρέωσης όταν αναβαθμίζει το πρόγραμμα ώστε να διαχειρίζεται μεγαλύτερο ποσό εύρους ζώνης. Για παράδειγμα ένας πελάτης θα έχει έκπτωση 90% του κόστους της χρέωσης που είχε για τα 5Mbs όταν κάνει αναβάθμιση στα 20Mbs. Στον παρακάτω πίνακα φαίνεται η χρέωση του πακέτου με βάση το ποσό εύρους ζώνης που θα αυτό θα επεξεργάζεται.

128 Kbps	$ 500
512 Kbps	$1,000
1 Mbps	$1,800
2 Mbps	$3,000
5 Mbps	$6,000
10 Mbps	$10,000
20 Mbps	$16,000
35 Mbps	$21,000
45 Mbps	$25,000
100 Mbps	$30,000

Πίνακας 2 **Κόστος του Dyban με βάση το εύρος ζώνης**

2.2 CRISS CROSS

Η Criss Cross ήταν η πρώτη εταιρία που διέθετε υπολογιστές της Apple και χρησιμοποίησε το NetEnforcer για έλεγχο της ποιότητας υπηρεσιών και εφαρμογή της καταγραφής και ανάλυσης της δικτυακής δραστηριότητας.

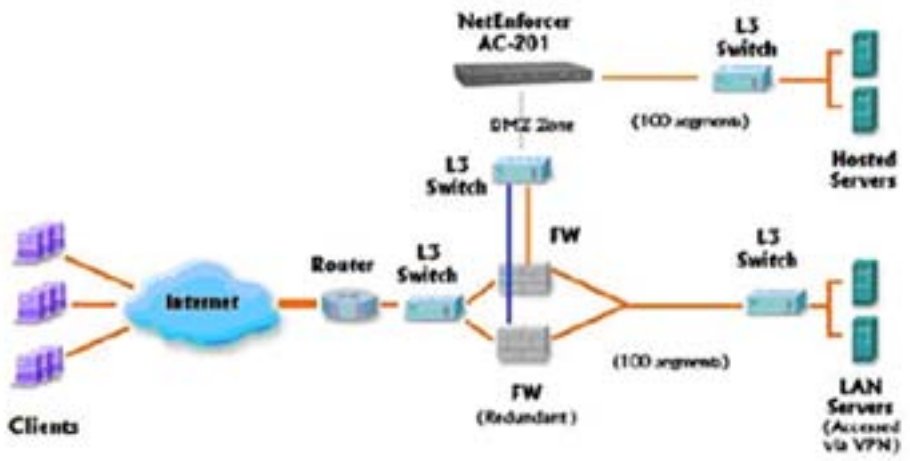
Το δικτυακό περιβάλλον της εταιρίας αποτελούνταν από:

- 64 Apple G4 υπολογιστές με λειτουργικό σύστημα MacOSX

- Macs, Allied Telesyn δρομολογητές και μεταγωγείς (switches)
- Apache και Webstar web servers
- Sorenson Broadcaster (webcast) servers
- Ένα νέο σύστημα accounting της BMC
- 1 GB οπτικής ίνας για σύνδεση στο Internet

Ο Rob Visser ίδρυσε την εταιρία Criss Cross στην Ολλανδία, δημιουργώντας ένα δίκτυο Mac υπολογιστών, με τη συμβολή χρηστών, ειδικών στο Unix και στα δίκτυα. Το 2001 η Criss Cross ίδρυσε το δικό της Κέντρο Λειτουργίας Δικτύου το οποίο διέθετε την κατάλληλη υποδομή συμπεριελαμβανομένων αιθουσών με κλιματισμό, UPS, συστημάτων ασφαλείας, server racks, συστήματος δημιουργίας αντιγράφων ασφαλείας (data backup) και συστήματα καταγραφής και ανάλυσης της δικτυακής δραστηριότητας και υπολογισμού του κόστους της χρήσης των δικτυακών πόρων. Η Criss Cross πρόσφερε χώρο στους χρήστες της τάξης των 10GB και ταχύτητα 2MB για πρόσβαση στο δίκτυο.

Η μεγάλη επιτυχία της Criss Cross οφείλεται στην αποτελεσματική κατανομή του εύρους ζώνης για την κάλυψη των αναγκών των εφαρμογών με μέγαλες απαιτήσεις σε εύρος ζώνης όπως για παράδειγμα το video streaming ή η μεταφορά μεγάλων αρχείων. Μεγάλης σημασίας ήταν για την εταιρία η δυνατότητα χρέωσης των υπηρεσιών που χρησιμοποιούνται από τους τελικούς χρήστες που έχουν πρόσβαση στους εξυπηρέτες της εταιρίας. Επομένως η εταιρεία χρειαζόταν ένα σύστημα καταγραφής και ανάλυσης της δικτυακής δραστηριότητας που θα της έδινε τη δυνατότητα του σχεδιασμού του πλάνου χρέωσης. Η χρέωση θα βασίζεται στην ροή δεδομένων, στο «κατέβασμα» αρχείων κτλ.



Σχήμα 9) Εφαρμογή καταγραφής και ανάλυσης της δικτυακής δραστηριότητας με χρήση του NetEnforcer

Η Criss Cross μελέτησε αρκετά εργαλεία ελέγχου της ποιότητας υπηρεσιών για να καταλήξει τελικά στο NetEnforcer. Η εφαρμογή του NetEnforcer εγγυάται συγκεκριμένα ποσά εύρους ζώνης ανά IP διεύθυνση και η ίδια η Criss Cross εγγυάται κατά 99,99% τη λειτουργικότητα όσο δηλαδή και το ποσοστό εγγύησης που παρέχεται από την γερμανική εταιρεία τηλεπικοινωνιών KPN η οποία παρέχει την οπτική ίνα του 1 GB.Οι χρήστες πολυμεσικών εφαρμογών μπορούν να δεσμεύσουν 2 MB ή και περισσότερο προκειμένου να ικανοποιηθούν οι ανάγκες των εφαρμογών τους. Υπάρχουν επίσης πολιτικές που εξασφαλίζουν προτεραιότητες για τις διάφορες εφαρμογές. Για παράδειγμα, οι εφαρμογές video, έχουν μεγαλύτερη προτεραιότητα σε σχέση με τις εφαρμογές MP3. Επίσης, οι HTTP εφαρμογές έχουν μεγαλύτερη προτεραιότητα από τις FTP εφαρμογές.

Η επιλογή του NetEnforcer εξασφάλισε στην εταιρία τα παρακάτω πλεονεκτήματα:

- **Εγγυημένο εύρος ζώνης**

Το NetEnforcer έδωσε τη δυνατότητα στην εταιρία να εγγυάται σε κάθε χρήστη ένα ελάχιστο ποσό εύρους ζώνης ανάλογα με τις εκάστοτε δικτυακές του ανάγκες.

- **Διαχείριση της κίνησης του δίκτυου μέσω ενός Java περιβάλλοντος**

Το NetEnforcer καθώς βασιζόταν στην τεχνολογία της Java δεν απαιτούσε την εγκατάσταση οποιουδήποτε άλλου λογισμικού προκειμένου να λειτουργήσει η εφαρμογή σε περιβάλλον Macintosh.

- **Ανεκτικότητα σε σφάλματα**

Το NetEnforcer παρείχε ανεκτικότητα σε σφάλματα έχοντας μηχανισμούς που μπορούσαν, σε περίπτωση κάποιας δυσλειτουργίας, να στηρίξουν τη λειτουργικότητα της εφαρμογής.

- **Προϊόντα καταγραφής και ανάλυσης της δικτυακής δραστηριότητας**

Το NetEnforcer προσφέρει μια ποικιλία επιπλέον προϊόντων που έχουν να κάνουν με το accounting του συστήματος όπως είναι για παράδειγμα το NetAccountant.

Στο Σχήμα 10 φαίνεται ο τρόπος λειτουργίας του NetEnforcer, όπου η διαδιακασία του accounting πραγματοποιείται σε τρεις φάσεις.

1. **Εντοπισμός νεοεισελθέντων χρηστών**

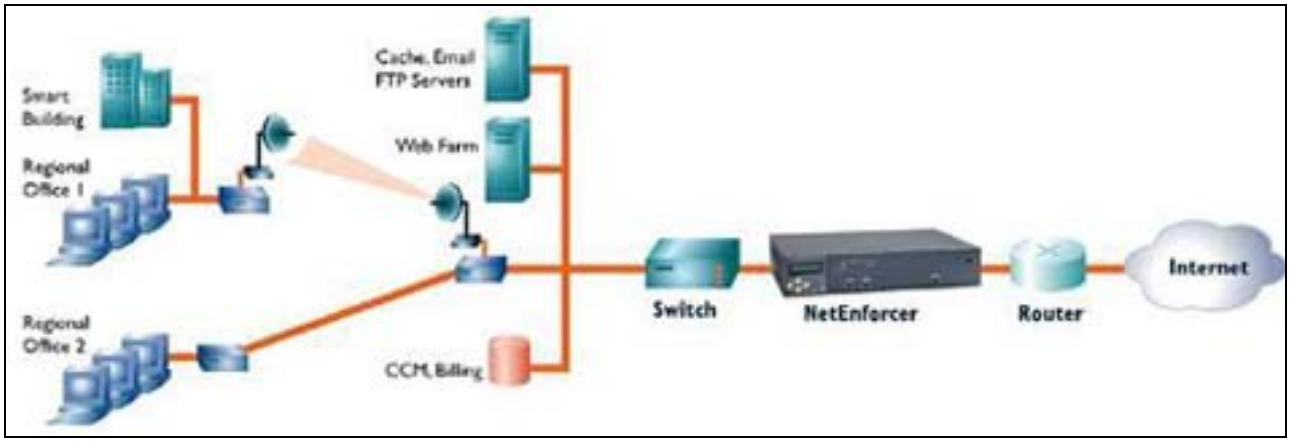
Το NetEnforcer αντλεί τις πληροφορίες από το σύστημα χρέωσης (Customer Care and Billing System CCB) ή μια λίστα πελατών σε μορφή αρχείου. Κατά το στάδιο αυτό το NetEnforcer αντλεί αυτόματα τις απαραίτητες πληροφορίες σχετικά με το χρήστη και θέτει τους κατάλληλους περιορισμούς σχετικά με το εύρος ζώνης που θα αποδοθεί στο χρήστη.

2. **Επιβολή περιορισμών**

Το NetEnforcer προωθεί τα πακέτα σύμφωνα με τους περιορισμούς σχετικά με το εύρος ζώνης.

3. **Χρέωση**

Το NetEnforcer στέλνει λεπτομερείς αναφορές στο σύστημα κοστολόγησης αναφέροντας τις διευθύνσεις που επισκέφτηκε ο χρήστης, τις εφαρμογές που χρησιμοποιήσε και τη συνολική ποσότητα εξερχόμενης κίνησης.



Σχήμα 10) NetEnforcer

Τεχνικά χαρακτηριστικά του NetEnforcer

Ακολουθεί αναφορά σε κάποια από τα χαρακτηριστικά του NetEnforcer που εξασφαλίζουν την αποδοτική του λειτουργία.

Συνδέσεις διεπαφής:

- AC-202/302/401: Τρεις 10/100BASE-T half/full duplex autosense Ethernet διεπαφές, συμπεριελαμβανομένης μιας διεπαφής διαχείρισης, όλες διασυνδεδεμένες με RJ-45 connectors.
- AC-701/SP-C: Δύο 1000BASE-T half/full duplex Ethernet διεπαφές και μια 10/100BASE-T διαχειριστική επαφή, όλες διασυνδεδεμένες με RJ-45 connectors.
- AC-701/SP-F: Δύο 1000BASE-SX οπτικές διεπαφές με connectors τύπου SC και μια 10/100BASE-T διεπαφή με έναν RJ-45 connector.

Ταξινόμηση κίνησης

Με βάση:

- Τις IP/MAC διευθύνσεις. Η ανάκτηση των στοιχείων γίνεται μέσω LDAP ή text αρχείου.
- Τα πρωτόκολλα δικτύου και τις εφαρμογές
- Τις εφαρμογές δυναμικών θυρών (πχ H.323, FTP, AudioGalaxy, Oracle, RTSP κτλ)
- Το πρωτόκολο πιστοποίησης (πχ HTTP)
- Το VLAN
- Την ακριβή ημερομηνία

Εξασφάλιση ποιότητας υπηρεσιών:

Μέσω

- Της επιβολής κανόνων ιεραρχίας σχετικά με την κίνηση στο δίκτυο
- Ελάχιστου/μέγιστου ορίου ανά flow/VC/Pipe
- Δέκα επίπεδα προτεραιότητας ανά VC/Pipe
- Δικαιοσύνη όσο αφορά τη ροή δεδομένων ίσων προτεραιοτήτων
- Διαχείριση των full/half dublex συνδέσεων

Ασφάλεια Δικτύου:

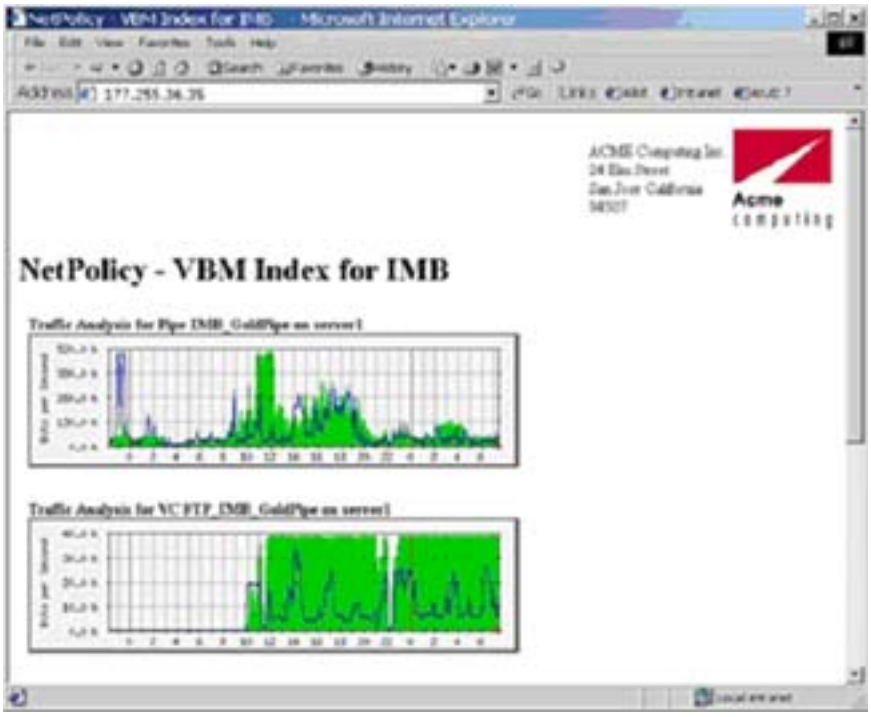
Μέσω

- Ελέγχου πρόσβασης
- Προστασίας από DoS (Denial of Service) επιθέσεις
- Φιλτράρισμα των διευθύνσεων και των επεκτάσεων των αρχείων (πχ για τον ιό Nimda)
- Έλεγχος αριθμού και ρυθμού συνδέσεων

Στο Σχήμα 11 φαίνεται η διαχειριστική κονσόλα της εφαρμογής ενώ στο σχήμα 12 ένα στιγμιότυπο

των αποτελεσμάτων.

Σχήμα 11) Γραφικό περιβάλλον διαχείρησης του NetEnforcer



Σχήμα 12) Αποτελέσματα ανάλυσης δεδομένων από το NetEnforcer

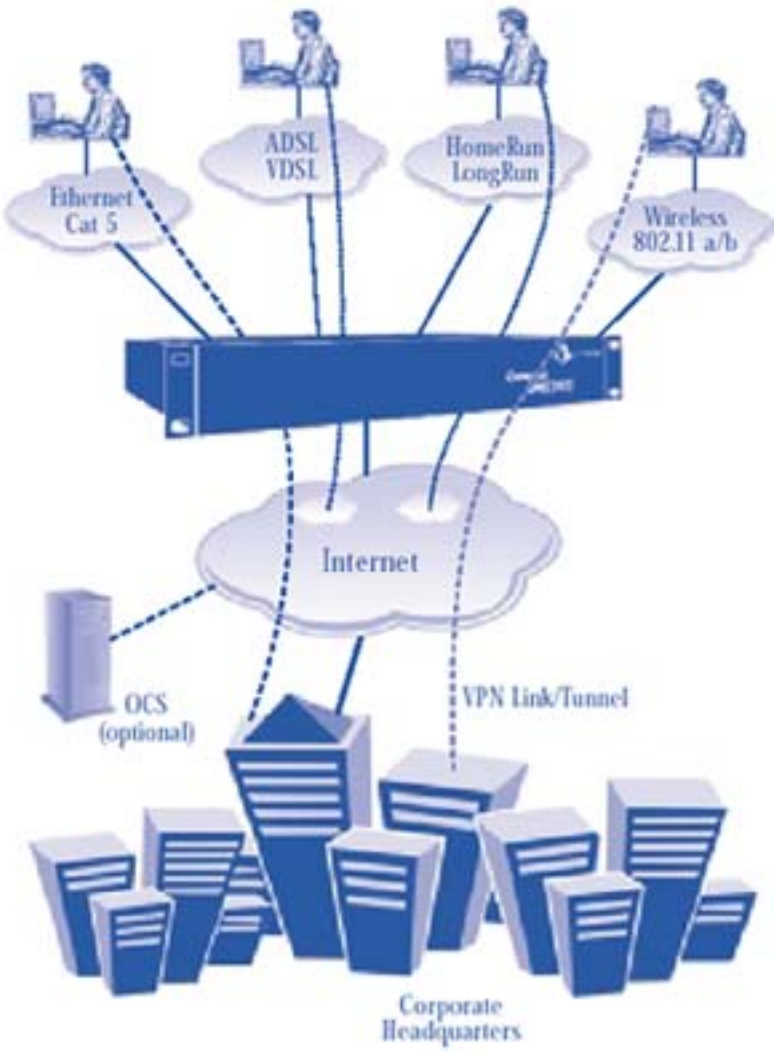
2.3 ΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΟΥ ILLINOIS

Με την αύξηση των αγορών laptop από τους φοιτητές μια νέα ανάγκη πρόβαλλε στους χώρους των πανεπιστημίων. Η ανάγκη πρόσβασης στο Internet με την εξασφάλιση υψηλών ταχυτήτων από οποιοδήποτε σημείο του χώρου του πανεπιστημίου. Το πανεπιστήμιο του Illinois ήρθε αντιμέτωπο

με αυτό το πρόβλημα καθώς διαθέτοντας πάνω από 35000 φοιτητές το ποσοστό αυτών που διέθεταν laptop αυξανόταν συνεχώς, δημιουργώντας το εξής ερώτημα στους υπεύθυνους του πανεπιστημίου: Πώς γίνεται να προσφερθούν συνδέσεις υψηλών ταχυτήτων και παράλληλα να διατηρηθεί σε υψηλά επίπεδα η ασφάλεια του δικτύου;

Την άνοιξη του 1999, η υπεύθυνη ομάδα του πανεπιστημίου για θέματα δικτύου άρχισε να ψάχνει για μια λύση στις νέες ανάγκες που δημιουργήθηκαν. Σε καμιά περίπτωση δεν επιθυμούσαν να μπορεί ο οποιοσδήποτε βρισκόταν στο χώρο του πανεπιστημίου να μπορεί να συνδεθεί στο δίκτυο και να κάνει χρήση των δικτυακών πόρων. Αυτό που επιθυμούσαν είναι η εξουσιοδοτημένη πρόσβαση στο δίκτυο, όπου ο κάθε χρήστης θα έχει το δικό του username και password.

Αφού διερευνήθηκαν διάφορες λύσεις, τελικά προτιμήθηκε το Expresso SMS/OCS. Πρόκειται για ένα σύστημα διανομής των δικτυακών υπηρεσιών σε ταχύτητες 1 Mbps που εφαρμόζεται κυρίως σε κτιριακά συγκροτήματα όπως, διαμερίσματα, ξενοδοχεία και πανεπιστημιακές εστίες. Το Expresso SMS/OCS υποστηρίζει την διαχείριση IP διευθύνσεων, firewalls, πιστοποίηση, accounting καθώς επίσης παρέχει στους τελικούς χρήστες τη δυνατότητα plug-and-play σύνδεσης στο δίκτυο χωρίς να είναι απαραίτητη κάποια αλλαγή στο λογισμικό του υπολογιστή τους.



Σχήμα 13) Το Expresso SMS/OCS

Η εταιρία παραγωγής του προϊόντος προμηθεύει τους Παροχείς με εργαλεία διαχείρισης και κοστολόγησης των συνδέσεων των χρηστών. Το Expresso SMS/OCS εφαρμόστηκε αρχικά στην βιβλιοθήκη του πανεπιστημίου, όπου όπως υπολογίστηκε στο τέλος της πρώτης εβδομάδας εφαρμογής, πάνω από 100 φοιτητές συνδέονταν στο δίκτυο χρησιμοποιώντας το laptop τους.

Τεχνικά χαρακτηριστικά του Expresso SMS/OCS:

- Διαχείριση των IP διευθύνσεων (NAT, DHCP, DNS, Static IP, Proxy)
- Πρωτόκολλα που υποστηρίζονται: PPTP, L2TP, IPsec, HTTP, FTP, H323
- Απόδοση: 100 Mbps, 800 ταυτόχρονες συνδέσεις
- Ευκολία παραμετροποίησης
- Πολλαπλές επιλογές ελέγχου πρόσβασης και κοστολόγησης συνδέσεων καθώς υποστηρίζεται το RADIUS AAA (Authentication, Authorization, Accounting)
- Ασφάλεια και προστασία χρηστών
- Δυνατότητα διαχείρισης εύρους ζώνης
- Πλήρης υποστήριξη ηλεκτρονικού ταχυδρομείου
- Συμβατότητα με Windows NT και Linux
- Περιέχεται Apache web server
- Συμβατότητα με PostgreSQL server και MS SQL server.

2.4 AARNET2

Το AARNET2 είναι ένα ATM δίκτυο ακανόνιστης τοπολογίας που συνδέει τις οχτώ πολιτείες της Αυστραλίας όπως φαίνεται και στο Σχήμα 14.

Σχήμα 14) Το δίκτυο AARNet2

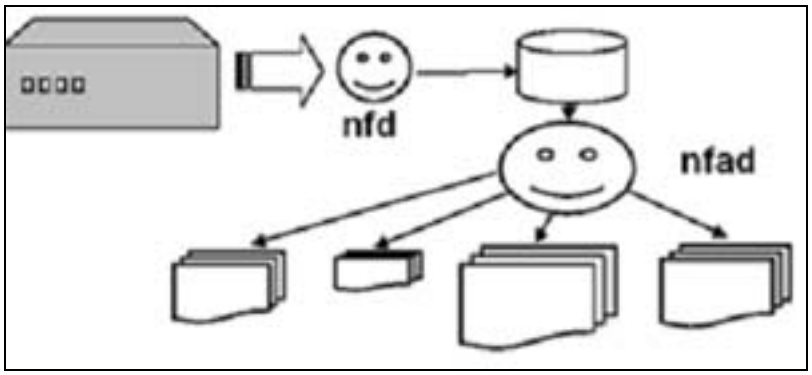
Αρχικά η παρακολούθηση του δικτύου γινόταν χρησιμοποιώντας:

- SNMP
- NNStat
- NetraMet

Αυτές οι μέθοδοι προϋπόθεταν δειγματοληψία με υψηλούς ρυθμούς και περιείχαν πολλά κρυμμένα κόστη. Έτσι κατά το σχεδιασμό του AARNet2 επιλέχθηκε να χρησιμοποιηθεί το Netflow της Cisco. Ο σκοπός ήταν να γίνει πιο αποτελεσματική η καταγραφή και η ανάλυση της δικτυακής δραστηριότητας για το δίκτυο AARNet2 και να παρέχονται ακριβείς πληροφορίες για τις συνδέσεις του κάθε ιδρύματος που συμμετείχε στο δίκτυο.

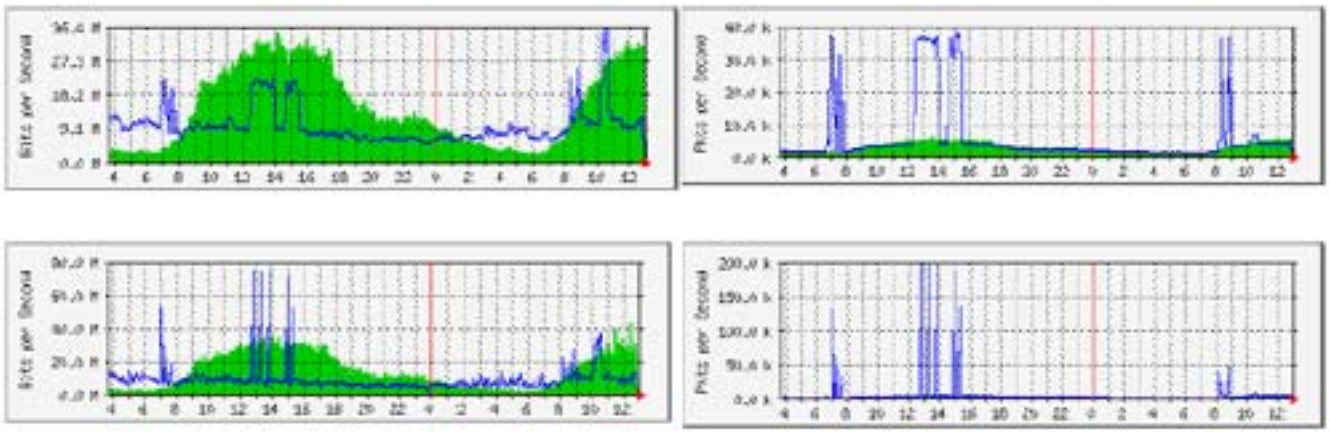
Το σύστημα συνολικά λειτουργεί ως εξής:

- Υπάρχει ένας δρομολογητής που εξάγει τα δεδομένα κίνησης
- Ένας ακροατής που γράφει τα δεδομένα σε δίσκο
- Πρόγραμμα που αναλύει τα δεδομένα σε ομάδες προορισμού (destination groups)



Σχήμα 15) Δομή συστήματος Netflow

Συνολικά, για την υλοποίηση της ανάλυσης της δικτυακής δραστηριότητας χρησιμοποιούνται οκτώ κατανεμημένοι συλλέκτες δεδομένων (collectors). Στο δίκτυο κάθε μέρα διακινούνται κατά μέσο όρο 1.5 TBytes (περίπου 5000 flows το λεπτό) και αναλύονται περίπου 12 GBytes δεδομένων ενώ χρησιμοποιούνται γύρω στα 500 GBytes δίσκου.



Σχήμα 16) Αποτελέσματα από το Netflow

Σε κάθε ίδρυμα αποδίδεται μια πλήρης ανάλυση της κίνησης του σε καθημερινή βάση για λόγους καταγραφής της δικτυακής δραστηριότητας, διαχείρισης καθώς επίσης και για λόγους ασφαλείας. Στο Σχήμα 16 φαίνεται ο τρόπος παρουσίασης των αποτελεσμάτων.

2.5 VERMONT

Το εργοστάσιο παραγωγής ημιαγωγών της IBM Vermont, απασχολεί γύρω στους 8000 υπαλλήλους και το σύνολο των υπαλλήλων έχουν πρόσβαση στο τοπικό δίκτυο της εταιρίας. Το δίκτυο διαθέτει πάνω από 50 δρομολογητές, 250 τμήματα και 12000 συσκευές συνδεδεμένες στο δίκτυο. Σκοπός της εταιρίας ήταν:

- Η συλλογή πληροφοριών από το δίκτυο που θα είχε σα στόχο τη δημιουργία ενός συστήματος πληροφοριών χρέωσης, το οποίο θα εντόπιζε όλες τις θύρες, τους σταθμούς εργασίας και τα καλώδια του δικτύου.
- Η χρησιμοποίηση του συστήματος πληροφοριών χρέωσης για την χρέωση των χρηστών του δικτύου
- Η χρησιμοποίηση του συστήματος πληροφοριών χρέωσης για την αντιμετώπιση προβλημάτων ανάλυσης
- Η συλλογή των δεδομένων σε καθημερινή βάση και η επεξεργασία τους σε μηνιαία βάση

Το σύστημα πληροφοριών χρέωσης ξεκίνησε τον Ιούνιο του 1997 και ολοκληρώθηκε τον Ιανουάριο του 1998.

2.5.1 Συλλογή δεδομένων

Τα δεδομένα που συλλέγονται είναι τόσο δυναμικά όσο και στατικά. Τα δυναμικά δεδομένα συλλέγονται από συσκευές της IBM όπως είναι οι κατανεμητές (μοντέλα 8250 και 8224), οι δρομολογητές δικτύου, οι ελεγκτές επικοινωνίας 3745 της IBM και ο διαχειριστής του τοπικού δικτύου.

Οι βάσεις δεδομένων που συλλέγουν τα δυναμικά δεδομένα είναι:

Α. Η NEWRP – Μια λίστα δρομολογητών

Β. Η VTMA – Μια λίστα διευθύνσεων καρτών δικτύου και πληροφορίες αρχιτεκτονικών συστημάτων δικτύων.

Τα στατικά δεδομένα που συλλέγονται είναι:

Γ. PRINTERS - Μια λίστα εκτυπωτών

Δ. MAC - Μια λίστα διευθύνσεων καρτών δικτύου, θυρών και τμημάτων

Ε. NETBIOS - Μια λίστα ονομάτων υπολογιστών και διευθύνσεων καρτών δικτύου

Ζ. COAX - Μια λίστα σταθμών εργασίας

Η. NEWNAME - Το αρχείο DNS που περιέχει τις IP διευθύνσεις και τα ονόματα των υπολογιστών

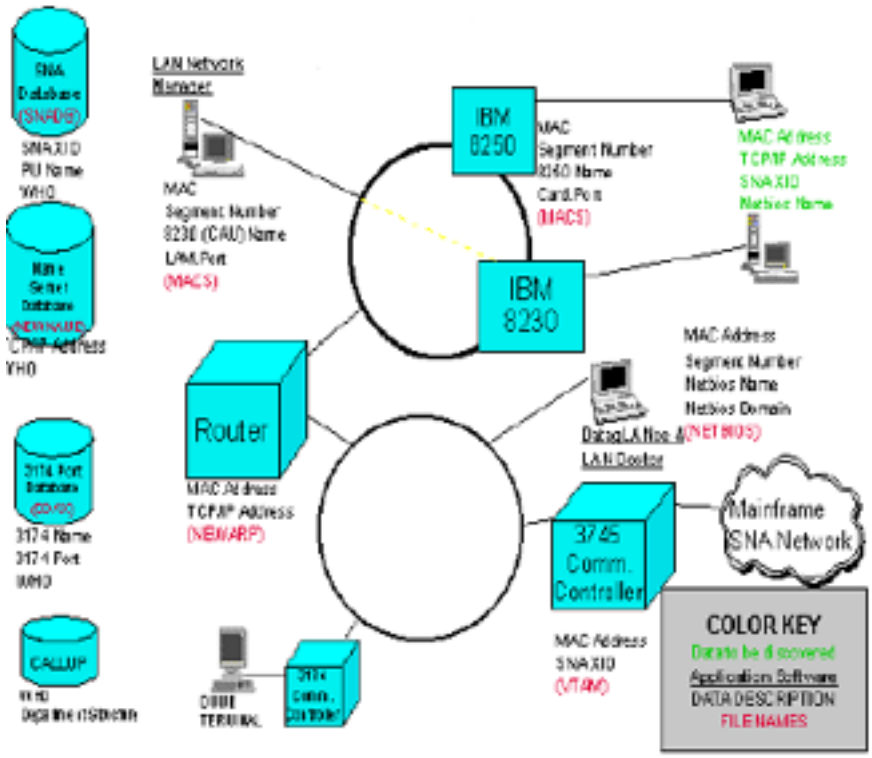
Θ. CALLUP - Τα στοιχεία των υπαλλήλων.

Όλα αυτά τα αρχεία αποθηκεύονται με τη μορφή κειμένου. Στη συνέχεια τα δεδομένα συγχωνεύονται, αναλύονται και παράγονται αναφορές. Λόγω της διαφορετικών χαρακτηριστικών των πελατών δημιουργούνται διαφόρων ειδών αναφορές οι οποίες περιέχουν:

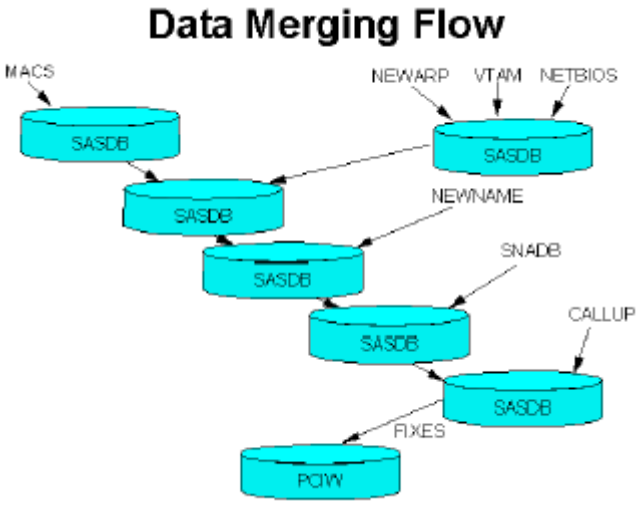
- Το συνολικό αριθμό των συνδέσεων, τις θύρες που χρησιμοποιήθηκαν, τη δικτυακή δραστηριότητα κτλ
- Λίστα συνδέσεων ανά χρήστη, τμήμα, κτίριο κτλ.
- Αναφορές ανά θύρα
- Αναφορές χρέωσης της χρήσης των δικτυακών πόρων

- Λίστα IP διευθύνσεων που δεν παρουσίασαν δραστηριότητα για τους τρεις τελευταίους μήνες και επομένως μπορούν να διαγραφούν από το DNS.

Στο Σχήμα 18 παρουσιάζεται ο τρόπος με τον οποίο συγχωνεύονται τα αρχεία.



Σχήμα 17) Δομή συστήματος πληροφοριών χρέωσης



Σχήμα 18) Συγχώνευση αρχείων δεδομένων

Το σύστημα πληροφοριών χρέωσης είναι μια web εφαρμογή που απευθύνεται:

- Στους διαχειριστές του δικτύου – οι διαχειριστές μπορούν να παρακολουθούν στοιχεία χωρητικότητας και φόρτου του δικτύου.

- Στους διαχειριστές λογαριασμών - αυτή η κατηγορία χρηστών παρακολουθεί την δικτυακή κίνηση του κάθε τμήματος και αποδίδει την ανάλογη χρέωση

- Στους τεχνικούς του δικτύου – αυτή η κατηγορία χρηστών εξάγει συμπεράσματα σχετικά με την αποδοτική λειτουργία του δικτύου και εντοπίζει πιθανά προβλήματα που υπάρχουν.

Η χρησιμοποίηση του συστήματος πληροφοριών χρέωσης βοήθησε σε σημαντικό βαθμό και την ανάπτυξη της ίδιας της IBM.

3 ΕΡΓΑΛΕΙΑ ΚΑΤΑΓΡΑΦΗΣ ΚΑΙ ΑΝΑΛΥΣΗΣ ΔΙΚΤΥΑΚΗΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ

Στη συνέχεια παρουσιάζονται συνοπτικά κάποια από τα σπουδαιότερα εργαλεία καταγραφής και ανάλυσης της δικτυακής δραστηριότητας.

3.1 ΛΟΓΙΣΜΙΚΟ ΑΝΟΙΧΤΟΥ ΚΩΔΙΚΑ

- FlowScan: Πρόκειται για μια Perl εφαρμογή η οποία αναλύει τα δεδομένα που συλλέγονται από εργαλεία όπως το cflowd, το lfapd και το flow-tools. Η έξοδος του συστήματος περιέχει γραφήματα όπως επίσης και λίστες ανακοινώσεων και συζητήσεων. Διάφορα εργαλεία που αναπτύχθηκαν από χρήστες έχουν κατά καιρούς ενσωματωθεί στην εφαρμογή.

- Flow –tools: είναι παρόμοιο με το cflowd μόνο που υλοποιείται σαν ένα σύνολο απλούστερων εργαλείων που εξασφαλίζουν επιπλέον την συμπίεση των καταγεγραμμένων δεδομένων με αποτέλεσμα μεγαλύτερος όγκος δεδομένων να μπορεί να αποθηκευτεί στο δίσκο. Η εφαρμογή αυτή γενικά χρησιμοποιείται ευρέως και υπάρχουν κάποια επιπλέον εργαλεία που μπορούν να ενσωματωθούν όπως για παράδειγμα το flow – extract το οποίο χρησιμοποιείται για το φιλτράρισμα των δεδομένων που διακινούνται στο δίκτυο.

- F.L.A.V.I.O: ένας συλλέκτης δεδομένων ο οποίος αποθηκεύει τα δεδομένα σε πίνακες της MySQL και δημιουργεί γραφήματα σε καθημερινή, εβδομαδιαία, μηνιαία και ετήσια βάση.

- CAIDA cflowd: Αρκετά πολύπλοκο σύστημα το οποίο χρησιμοποιεί πολλούς κατανεμημένους εξυπηρετητές αρχείων καταγραφής (log files). Διατέθηκε το 1998 και ήταν το πρώτο open-source λογισμικό που επεξεργαζόταν τη ροή δεδομένων του δικτύου αλλά δεν συντηρείται πλέον.

- UDP Samplicator: Ένα μικρό πρόγραμμα που δέχεται UDP πακέτα και τα αναδιανέμει σε ένα σύνολο παραληπτών. Είναι χρήσιμο για να κατανέμει τη δικτυακή κίνηση σε διαφορετικά προγράμματα επεξεργασίας και να στέλνει συγκεκριμένα ποσοστά πακέτων σε κάθε παραλήπτη. Στις τελευταίες εκδόσεις του προγράμματος έχει προστεθεί η δυνατότητα του “spoofing”, δηλαδή της δυναμικής αλλαγής της IP διεύθυνσης του αποστολέα.

- Fluxoscope: Λογισμικό που χρησιμοποιείται για την χρέωση, την παρακολούθηση και την ανάλυση στης κίνησης σε επίπεδο μεταγωγέα (Switch). Περιέχει τον δικό του NetFlow παραλήπτη ο οποίος μετατρέπει τα δεδομένα κίνησης σε πολυδιάστατους πίνακες. Το μεγαλύτερο μέρος του λογισμικού είναι γραμμένο σε LISP.

- Panoptis: Εφαρμογή που αναπτύχθηκε από τον Κ. Κοτσοκάλη του GRNET. Χρησιμοποιεί τα δεδομένα του NetFlow για να ανιχνεύει DoS επιθέσεις (Denial of Service). Υποστηρίζει τις εκδόσεις 1 και 5 του NetFlow σαν εισόδους ενώ βρίσκεται υπό ανάπτυξη ώστε να επεκταθούν οι δυνατότητες του.

- MHTG: Χρησιμοποιεί το NetFlow για να παράγει γραφήματα της δικτυακής κίνησης ανά υπολογιστή. Ένα αρκετά λειτουργικό περιβάλλον διαχείρισης έχει αναπτυχθεί σε Java. Το πρόγραμμα περιέχει επίσης τμήματα γραμμένα σε C++ για την επεξεργασία των δεδομένων κίνησης και MySQL υποστήριξη για την αποθήκευση των δεδομένων.

3.2 ΕΜΠΟΡΙΚΑ ΠΑΚΕΤΑ

- Apogee Networks: Αποτελείται από το NetCountant που πραγματοποιεί τη χρέωση, το NetScope που είναι το εργαλείο παρακολούθησης του δικτύου σε πραγματικό χρόνο και ανάλυσης και υποστηρίζει NetFlow, RMON2, RADIUS, άλλα και SNMP MIBS και εφαρμογές επιπέδου 7.
- Cisco: NetFlow FlowCollector/ Network Data Analyzer: Είναι παρόμοιο με το cflowd αλλά ενσωματώνει και ένα γραφικό περιβάλλον σε Java ενώ παρέχει περισσότερες δυνατότητες ορισμού φίλτρων και σχημάτων ομαδοποίησης των δεδομένων.
- Concord: Δικτυακές εφαρμογές ιατρικής χρησιμοποιούν πληροφορίες του NetFlow και του RMON2 για να καθορίζουν το απαιτούμενο εύρος ζώνης και το ποσοστό χρησιμοποίησης του εξυπηρετητή.
- Diqiquant: Σύστημα καταγραφής, ανάλυσης και χρέωσης δικτυακής δραστηριότητας του IMT που χρησιμοποιεί την Oracle 8i και τρέχει σε Unix.
- Hewlett- Packard: Τα Internet Billing Solution και OpenView Performance Insight for Networks (OVPI) είναι συστήματα χρέωσης που χρησιμοποιούν τα δεδομένα του NetFlow σαν δεδομένα εισόδου.
- InMon Traffic Server: Πρόκειται για μια εμπορική web εφαρμογή που τρέχει σε Linux και προσφέρει ανάλυση δυναμικών και στατικών δεδομένων από τα Flows και NetFlow. Τα ερωτήματα μέσω της εφαρμογής παρέχουν εύκολη πρόσβαση στα δεδομένα που έχουν καταχωρηθεί. Τα γραφήματα της ανάλυσης φανερώνουν τα σημεία συμφόρησης στο δίκτυο.
- RODOPI: Σύστημα χρέωσης που προσφέρεται στους Παρχοχείς Δικτυακών Υπηρεσιών.
- XACCT: Εμπορικό πακέτο για την καταγραφή, ανάλυση και χρέωση της δικτυακής δραστηριότητας που έχει τη δυνατότητα να επεξεργάζεται δεδομένα του NetFlow.
- Micromuse: Προϊόν της Cisco Info Center USM το οποίο συγκεντρώνει, αναλύει και εμφανίζει τα δεδομένα χρήσης του Internet
- Portal Software: Λογισμικό διαχείρισης και χρέωσης τοπικών δικτύων.

4 ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ

Τόσο για τους παροχείς δικτυακών υπηρεσιών όσο και για τις μεγάλες επιχειρήσεις, η κατανόηση του δικτύου και της κίνησής του είναι απαραίτητα. Κρίσιμες αποφάσεις θα πρέπει να ληφθούν με βάσει τις πληροφορίες που συλλέγονται από το δίκτυο. Για τους παροχείς δικτυακών υπηρεσιών, τα συστήματα υποστήριξης λειτουργιών (Operations Support Systems - OSS) είναι ζωτικής σημασίας. Η πιθανότητα αποτυχίας μοντέλων υπηρεσιών βασισμένων στην αντίληψη και σε μαθηματικές θεωρίες έχει οδηγήσει τους παροχείς δικτυακών υπηρεσιών και τις μεγάλες επιχειρήσεις στην ανάπτυξη μοντέλων που θα βασίζονται σε λειτουργικά ακριβείς πληροφορίες που προέρχονται απευθείας από το ίδιο το δίκτυο. Στόχος επομένως των συστημάτων καταγραφής και ανάλυσης δικτυακής δραστηριότητας (Network Accounting) είναι η συλλογή στοιχείων που θα απεικονίζουν την πραγματικότητα είτε χρησιμοποιώντας εμπορικά είτε ανοιχτού κώδικα (open source) εργαλεία και τεχνολογίες. Ιδιαίτερη σημασία θα πρέπει να δοθεί στον γεγονός ότι η συλλογή των δεδομένων δεν είναι αρκετή για να οδηγήσει σε σωστές αποφάσεις. Απαιτείται η παραγωγική ανάλυση και παρουσίαση των στοιχείων προκειμένου να αποτελέσουν χρήσιμα εφόδια στη λειτουργία, ανάπτυξη και σχεδίαση ενός δικτύου.

Όπως μπορεί κανείς να διαπιστώσει από την παραπάνω ανάλυση του θέματος του Network Accounting, για τις διάφορες κατηγορίες αναγκών ενός ISP υπάρχει πληθώρα πρωτοκόλλων, εργαλείων και προτύπων τα οποία μάλιστα υλοποιούνται με διαφορετικό τρόπο από τον κάθε κατασκευαστή. Υπάρχουν βέβαια οργανισμοί όπως η CAIDA που προσπαθούν να συντονίσουν τις προσπάθειες για την υλοποίηση εργαλείων συμβατων μεταξύ τους, τα οποία είναι ανοιχτού λογισμικού. Θα πρέπει να υπαρξει συντονισμός των κατασκευαστών συσκευών δικτύου και λογισμικού προκειμένου να υπάρξει προτυποποίηση των τεχνολογιών που χρησιμοποιούνται στη διαχείριση των δικτύων.

ΠΑΡΑΡΤΗΜΑ

http://www.allot.com/html/solutions_Case_Studies_main1.shtm

Η Allot Communications είναι μια εταιρία που εξειδικεύεται σε προϊόντα διαχείρισης δικτύου (λογισμικό και υλικό). Στο συγκεκριμένο σύνδεσμο υπάρχουν πολλά case studies ανά κατηγρία παροχέα υπηρεσιών και για διάφορες κατηγορίες δικτύων (wireless, wireline, satellite)

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/nwact_wp.pdf

Το άρθρο αυτό είναι μια πολύ καλή εισαγωγή στις υπηρεσίες του Network Accounting και στις τεχνολογίες που χρησιμοποιούνται.

http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.pdf

Το άρθρο αυτό αποτελεί μια λεπτομερή παρουσίαση της τεχνολογίας NetFlow της CISCO.

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/nfc/

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/nfa/

Στους συνδέσμους αυτούς της εταιρίας CISCO, υπάρχουν τα εγχειρίδια του λιγισμικού της εταιρίας για την τεχνολογία NetFlow. Ο $1^{ος}$ σύνδεσμος αναφέρεται στο λογισμικό συλλογής των στοιχείων κίνησης από τους δρομολογητές (NetFlow Collector) και ο $2^{ος}$ στο λογισμικό ανάλυσης NetFlow Analyzer.

http://www.dyband.net

Η Dyband είναι εταιρία ανάπτυξης λογισμικού διαχείρισης δικτίου και Network Accounting. Στον σύνδεσμο αυτό υπάρχους αρκετά case studies για υλοποιήσεις Network Accounting

http://www.snmplink.org/

Η ιστοσελίδα αυτή είναι αφιερωμένη στο SNMP. Παρέχει πληθώρα πληροφοριών, βιβλίων, εργαλείων, MIBs κτλ. Αποτελεί πηγή αναφοράς για το SNMP.

http://www.switch.ch/tf-tant/floma/software.html

Στην ιστοσελίδα αυτή παρουσιάζεται μια σειρά εργαλείων σχετικά με το NetFlow αλλά και άλλες τεχνολογίες.

http://www.ixiacom.com/support/techinfo/

Μεγάλη συλλογή από άρθρα, papers και case studies σχετικά με network management.

http://www.caida.org/

Η ιστοσελίδα ενός οργανισμού που ασχολείται με την ανάπτυξη εργαλείων για τη διαχείριση δικτύων. Πολλά από τα εργαλεία της χρησιμοποιούνται εκτενώς από

ISPs. Ιδιαίτερο ενδιαφέρον παρουσιάζει η λίστα ηλεκτρονικού ταχυδρομείου της.

Από τα πιο γνωστά εργαλεία της είναι το cflowd το οποίο έχει παρόμοιες δυνατότητες με το αντίστοιχο εργαλείο της CISCO NetFlow Collector.

http://computer.org/internet/v3n6/w6onwire.htm

Πολύ ενδιαφέρουσα ιστοσελίδα που περιγράφει τις αρχές λειτουργίας των πρωτοκόλλων AAA (Authentication Authorization Accounting).

http://www.isp-planet.com/

Η ιστοσελίδα αυτή περιέχει υλικό για το σύνολο των θεμάτων που αφορούν τη λειτουργία ενός ISP.

http://www.cisco.com/en/US/products/hw/univgate/ps501/products_implementation_design_guide_chapter09186a00800ea875.html

Παρέχει πληροφορίες για τον τρόπο οργάνωση ενός ISP για την ανάπτυξη μιας συγκεκριμένης υπηρεσία. Αποτελεί ένα case study.

http://inet2002.org/CD-ROM/lu65rw2n/papers/p06.pdf

Η περιγραφή ενός εργαλείου ανάλυσης για την παρακολούθηση του εύρους ζώνης και τη διαχείριση του δικτύου.

http://www.proxim.com/learn/library/casestudies/index.html

Μεγάλη συλλογή από case studies για διάφορα θέματα δικτύων, για μεγάλες εταιρίες και πανεπιστήμια.

An Innovative Internet Architecture for Application Service Providers

Borko Furht, Florida Atlantic University, Boca Raton, Florida

Chris Phoenix, Citrix Systems, Fort Lauderdale, Florida

John Yin, Daleen Technologies, Boca Raton, Florida

Zijad Aganovic, CyLex Systems, Boca Raton, Florida

Traffic Flow Measurements within IP Network : Requirement, Technologies and Standardization

Jurgen Quittek, Network Laboratories,NEC Europe Ltd.

Tanja Zseby,Georg Carle,Sebastian Zander, FhI FOKUS

Enterprise Network Traffic Monitoring, Analysis and Reporting using Web Technology

James W. Hong, Young Min-Kang, CSD Department, POSTECH

Analyzing Network Management Data with the SAS System

Tracy L. Lord / Charles E. Keeler IBM Global Services Essex Junction, Vermont

MBA: A Tool for Multicast Billing and Accounting

Lakshminath Dondeti, Brian Haberman, Haldon Sandick, Thomas Hardjono, Haixiang He

Accounting Management in Communication Networks: Concepts and Architecture

Theodore K. Apostolopoulos

Department of Informatics, Athens University of Economics and Business

Statistical Characterization of Wide-Area IP Traffic

Matthew T. Lucas, Dallas E. Wrege, Bert J. Dempsey, Alfred C. Weaver

Department of Computer Science, University of Virginia