Υπηρεσία Dial-up

Πιστοποίηση, εξουσιοδότηση, λογιστική (AAA - Authentication, Authorization, Accounting) για τη σύνδεση στο δίκτυο

Η υπηρεσία dialup λειτουργεί με τη χρήση του πρωτοκόλλου RADIUS και στηρίζεται στο ελεύθερο λογισμικό freeradius. Ο radius server αυτός παρέχει πολύ μεγάλες δυνατότητες, ευελιξία και ταχύτητα και ικανοποιεί με τον καλύτερο τρόπο τις απαιτήσεις μεγέθους από πλευράς χρηστών του Πανελλήνιου Σχολικού Δικτύου.

Η διαχείριση των λειτουργιών αυτών καθώς και η καθημερινή επόπτευση της καλής λειτουργίας του freeradius γίνεται από το dialup admin το οποίο αποτελεί ουσιαστικά μια συλλογή από ειδικά φτιαγμένες για τον σκοπό αυτό σελίδες οι οποίες είναι γραμμένες σε PHP. Για την χρήση του dialup-admin απαιτείται μονάχα ένας browser ο οποίος να έχει την δυνατότητα απεικόνισης frames.

1. Δυνατότητες

- **Authentication μέσω LDAP:** Η πιστοποίηση των χρηστών γίνεται με τη χρήση κατάλληλων LDAP ερώτησεων.
- **Authorization LDAP**: Το authorization των χρηστών γίνεται και αυτό μέσω LDAP πρωτοκόλλου. Μέσω ενός attribute στον LDAP καθορίζεται η δυνατότητα πρόσβασης στην υπηρεσία τηλεφωνικής πρόσβασης.
- **Reply-Items στον LDAP:** οι παράμετροι σύνδεσης των χρηστών προσδιορίζονται από attributes που περιέχονται στο entry του χρήστη στον διακομιστή LDAP.
- **Ημερήσια, Εβδομαδιαία Όρια:** Μετρητές χρησιμοποιούνται για τον έλεγχο και επιβολή ημερήσιων και εβδομαδιαίων ορίων χρήσης του dial-up.
- **Υποστήριξη των μηχανισμών PAP, CHAP και MS-CHAP:** Υποστηρίζονται και οι τρεις μέθοδοι αποστολής του συνθηματικού του χρήστη
- **Login-Time:** Καθορισμός του επιτρεπόμενου χρόνου σύνδεσης των χρηστών
- **Double logins:** Ανίχνευση double-login (πολλαπλή πρόσβαση) των χρηστών
- **Authorization** με βάση τα Caller-Ids των χρηστών και τα IP addresses του access server στον οποίο συνδέονται (τοπική πρόσβαση)
- **Multi-threaded :** Ο ίδιος ο server καθώς και τα βασικά modules (ldap,sql κτλ) είναι πλήρως multithreaded με αποτέλεσμα τη δυνατότητα υποστήριξης σχεδόν απεριόριστου αριθμού αιτήσεων
- **Accounting σε mySQL βάση**
- **Web-based σύστημα διαχείρισης (dialup-admin)**

2. Λειτουργίες βασισμένες σε DAP

2.1 Πιστοποίηση - Authentication

Η πιστοποίηση των χρηστών γίνεται μέσω ενός bind request στον διακομιστή LDAP με το login/password που παρέχει ο χρήστης κατά την σύνδεση. Κατά αυτόν τον τρόπο υποστηρίζονται όλοι οι τρόποι κρυπτογράφησης του password του χρήστη τους οποίους υποστηρίζει ο διακομιστής LDAP. Παρέχεται η δυνατότητα η αποστολή του login και του password στον ldap server να γίνει μέσω ασφαλούς σύνδεσης SSL.

2.2 Εξουσιοδότηση - Authorization

Για το authorization των χρηστών χρησιμοποιείται το objectclass **radiusprofile**, το οποίο παρέχει τα διάφορα attributes που σχετίζονται με το authorization. Οι ρυθμίσεις που αφορούν τον κάθε χρήστη ορίζονται με τον συνδυασμό τεσσάρων προφίλ, του **User-Profile**, του **Default-Profile**, του **Regular-Profile** και του **προσωπικού προφίλ** του κάθε χρήστη.

3. Χρέωση - Accounting

Για το accounting χρησιμοποιείται μία βάση mysql η οποία αποθηκεύει την σχετική πληροφορία. Πιο συγκεκριμένα, για τον σκοπό αυτό χρησιμοποιείται ο πίνακας **radacct** ο οποίος αποθηκεύει ένα row πληροφορίας για κάθε dial-up session. Αμέσως μετά την επιτυχή πιστοποίηση του χρήστη ο access server στέλνει ένα Accounting-Start πακέτο στο radius server το οποίο περιέχει βασικές πληροφορίες για τη σύνδεση (την πόρτα στην οποία συνδέθηκε ο χρήστης, ο αριθμός τηλεφώνου απο τον οποίο συνδέθηκε κτλ) το οποίο και χρησιμοποιείται για τη δημιουργία ενός νέου row στον πίνακα radacct το οποίο και περιέχει τις πληροφορίες αυτές. Μετά την αποσύνδεση του χρήστη ο access server στέλνει ένα Accounting-Stop πακέτο το οποίο περιέχει πλήθος πληροφοριών για τη σύνδεση όπως την ip address, τα bytes που παραλήφθηκαν και στάλθηκαν κτλ.

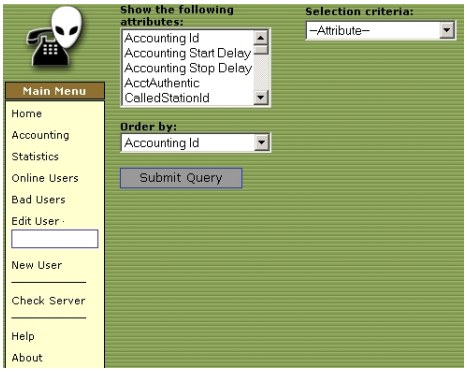
4. Μετρητές

Το σύστημα παρέχει δυνατότητα μετρητών για authorization και accounting χρήση σε ωριαία, ημερήσια, εβδομαδιαία και μηνιαία βάση. Αυτή την στιγμή χρησιμοποιούνται μόνο ημερήσιοι και εβδομαδιαίοι μετρητές. Ο κάθε ένας από αυτούς τους μετρητές χρησιμοποιεί ένα attribute (**Max-Daily-Session, Max-Weekly-Session** αντίστοιχα) που ορίζει το μέγιστο όριο ημερισίου/εβδομαδιαίου χρόνου που δικαιούται ο κάθε χρήστης, το οποίο και περιέχεται στο entry του χρήστη στον LDAP.

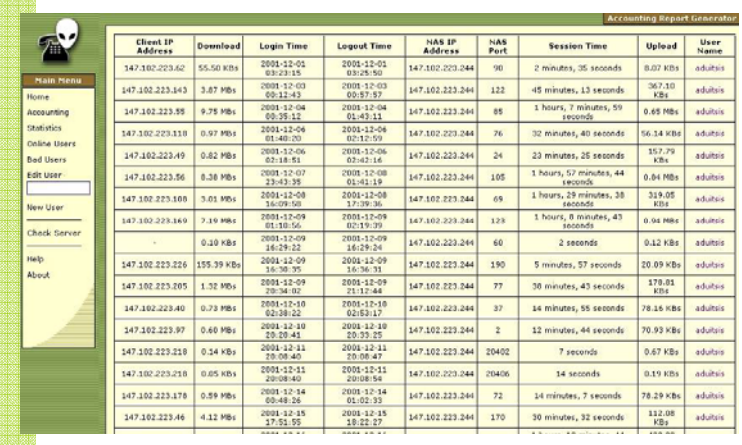
5. Εφαρμογή διαχείρισης (dialup-admin)

Η διαχείριση των λειτουργιών της υπηρεσίας dialup καθώς και η καθημερινή επόπτευση της καλής λειτουργίας του freeradius γίνεται από το dialup admin το οποίο αποτελεί ουσιαστικά μια συλλογή από ειδικά φτιαγμένες από το ΠΣΔ για τον σκοπό αυτό σελίδες οι οποίες είναι γραμμένες σε PHP. Παραθέτουμε ενδεικτικά μερικές από τις λειτουργίες που παρέχει το περιβάλλον του dialupadmin

Accounting: Με τη λειτουργία αυτή μπορεί κανείς να αναζητήσει πληροφορίες σχετικά με τις συνδέσεις sessions τα οποία έχουν καταγραφεί μέχρι το παρόν χρονικό σημείο στην βάση δεδομένων.

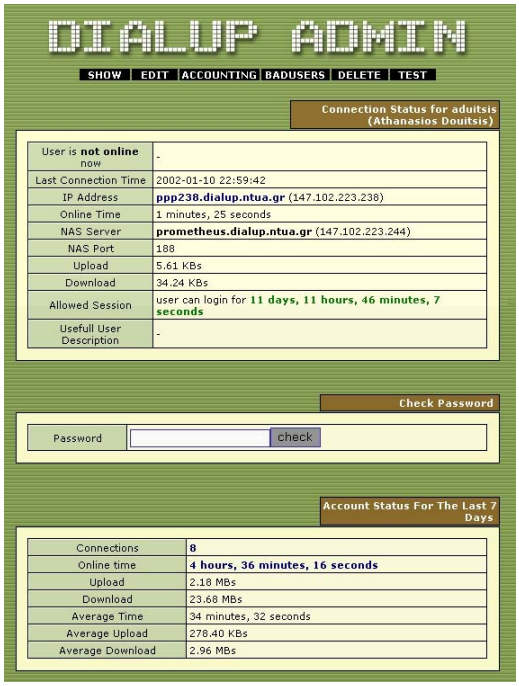


Παρακάτω φαίνεται το αποτέλεσμα της αναζήτησης "username=aduitsis". Στο παράδειγμα έχουν ζητηθεί τα πεδία client ip address, download, login time, logout time, NAS ip address, NAS port, session time, upload, user name. Επίσης έχει επιλεγεί "sort by login time".



Online users: Σκοπός της εντολής αυτής είναι η απεικόνιση της τρέχουσας κατάστασης του συστήματος και συγκεκριμένα ποιων χρηστών είναι συνδεδεμένοι σε κάποιον access server του συστήματος την στιγμή της εκτέλεσης της εντολής.

Edit User: Με το στοιχείο αυτό γίνεται έκθεση και τροποποίηση των στοιχείων ενός χρήστη στον LDAP. Έχει αναφερθεί προγενέστερα ότι το μοντέλο του dialup-admin χρησιμοποιεί την παραδοχή ότι η κύρια μέθοδος ταυτοποίησης που χρησιμοποιεί ο freeradius είναι μέσω LDAP.



Γράφοντας το username του χρήστη στο αντίστοιχο κουτάκι και πιέζοντας Enter ο διαχειριστής έχει πρόσβαση στην οθόνη που φαίνεται παρακάτω.

Ο πίνακας "Account Status for the last 7 days" φανερώνει στατιστικά στοιχεία για τις συνδέσεις του εν λόγω χρήστη τις τελευταίες 7 ημέρες. Τα συγκεκριμένα δεδομένα παρέχονται σαν διευκόλυνση, αφού όπως περιγράφηκε ήδη τα στοιχεία αυτά είναι διαθέσιμα και από άλλα μενού.

Σε περίπτωση που κάποιος χρήστης δεν μπορεί να συνδεθεί λόγω λανθασμένου password, με το menu "password" είναι δυνατόν ο διαχειριστής να επαληθεύσει αν το password του χρήστη είναι πράγματι αυτό που ο τελευταίος ισχυρίζεται.

6. Μεγέθη

Εξυπηρετητές ΑΑΑ	2

7. Υλοποίηση

Η υπηρεσία έχει υλοποιηθεί και συντηρείται από το **Ερευνητικό Πανεπιστημιακό Ινστιτούτο Συστημάτων Επικοινωνιών και Υπολογιστών (ΕΠΙΣΕΥ)** http://www.iccs.ece.ntua.gr **του Εθνικού Μετσοβείου Πολυτεχνείου (ΕΜΠ)** **www.ntua.gr**.

8. Πληροφορίες

URL: http://www.sch.gr, email: info@sch.gr