



Πανελλήνιο Σχολικό Δίκτυο – www.sch.gr

Το δίκτυο στην υπηρεσία της εκπαίδευσης

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 Πανελληνίου 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 ερωτήσεων.
- **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 επίβλεψη 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.

Show the following attributes:
Accounting Id
Accounting Start Delay
Accounting Stop Delay
AcctAuthentic
CalledStationId

Selection criteria:
-Attribute-

Order by:
Accounting Id

Main Menu
Home
Accounting
Statistics
Online Users
Bad Users
Edit User
New User
Check Server
Help
About

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".

Accounting Report Generator

Client IP Address	Download	Login Time	Logout Time	NAS IP Address	NAS Port	Session Time	Upload	User Name
147.102.223.62	55.50 Kbits	2008-12-01 03:21:15	2008-12-01 03:26:50	147.102.223.244	90	2 minutes, 35 seconds	0.07 Kbits	aduitsis
147.102.223.343	3.87 MBs	2008-12-03 00:12:43	2008-12-03 00:57:57	147.102.223.244	122	45 minutes, 13 seconds	367.10 Kbits	aduitsis
147.102.223.85	9.75 MBs	2008-12-04 00:35:15	2008-12-04 01:43:11	147.102.223.244	85	1 hours, 7 minutes, 59 seconds	0.65 MBs	aduitsis
147.102.223.118	0.97 MBs	2008-12-06 01:40:20	2008-12-06 02:12:59	147.102.223.244	76	32 minutes, 40 seconds	56.14 Kbits	aduitsis
147.102.223.49	0.82 MBs	2008-12-06 03:18:51	2008-12-06 03:42:16	147.102.223.244	24	23 minutes, 25 seconds	157.79 Kbits	aduitsis
147.102.223.56	0.38 MBs	2008-12-07 23:03:39	2008-12-08 03:41:19	147.102.223.244	105	1 hours, 57 minutes, 44 seconds	0.04 MBs	aduitsis
147.102.223.108	3.01 MBs	2008-12-08 01:10:56	2008-12-08 02:19:39	147.102.223.244	65	1 hours, 8 minutes, 38 seconds	319.05 Kbits	aduitsis
147.102.223.189	7.19 MBs	2008-12-09 01:10:56	2008-12-09 02:19:39	147.102.223.244	129	1 hours, 8 minutes, 43 seconds	0.94 MBs	aduitsis
-	0.10 Kbits	2008-12-09 16:30:35	2008-12-09 16:30:35	147.102.223.244	60	2 seconds	0.12 Kbits	aduitsis
147.102.223.226	155.39 Kbits	2008-12-09 20:34:02	2008-12-09 21:17:44	147.102.223.244	190	5 minutes, 57 seconds	20.09 Kbits	aduitsis
147.102.223.205	1.32 MBs	2008-12-09 20:34:02	2008-12-09 21:17:44	147.102.223.244	77	38 minutes, 47 seconds	170.81 Kbits	aduitsis
147.102.223.40	0.73 MBs	2008-12-10 02:29:22	2008-12-10 02:53:17	147.102.223.244	37	14 minutes, 55 seconds	78.16 Kbits	aduitsis
147.102.223.97	0.60 MBs	2008-12-10 20:30:45	2008-12-10 20:30:25	147.102.223.244	2	12 minutes, 44 seconds	70.93 Kbits	aduitsis
147.102.223.218	0.14 Kbits	2008-12-11 20:06:40	2008-12-11 20:06:47	147.102.223.244	20402	7 seconds	0.67 Kbits	aduitsis
147.102.223.218	0.05 Kbits	2008-12-11 20:08:56	2008-12-11 20:08:56	147.102.223.244	20406	14 seconds	0.19 Kbits	aduitsis
147.102.223.178	0.59 MBs	2008-12-14 00:48:26	2008-12-14 01:02:33	147.102.223.244	72	14 minutes, 7 seconds	78.29 Kbits	aduitsis
147.102.223.46	4.12 MBs	2008-12-15 17:51:55	2008-12-15 18:22:27	147.102.223.244	170	30 minutes, 32 seconds	112.98 Kbits	aduitsis

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.

DIALUP ADMIN

Online Users

Tuesday, 14 September 2004, 17:27:11 EEST

cas.aitsch.gr
Cisco 3640 access server
14 users connected 16 free lines

#	user	ip address	callerid	name	duration
1	r-tee-vonits	194.63.160.156	643023280	Router Dialup	03:17:52
2	r-lyk-empes	194.63.160.132	647031503	Router Dialup	01:08:23
3	sdeagr	81.186.76.61	641056100	ΣΧΟΛΕΙΟ ΔΕΥΤΕΡΗΣ ΕΚΠΑΙΔΕΥΣΗΣ ΑΓΡΙΝΙΟΥ	00:40:40
4	ppapagn	81.186.76.66	641057899	ΠΑΠΑΓΕΩΡΓΙΟΥ ΠΑΝΑΓΙΩΤΑ	00:44:47
5	pesinisb	81.186.76.95	641022296	ΠΕΛΙΝΗΣ ΒΑΣΙΛΕΙΟΣ	00:24:39
6	tlavidis	81.186.76.48	641022279	ΛΥΔΗΣ ΘΑΛΕΜΑΧΟΣ	00:22:05
7	theostam	81.186.76.12	641028360	ΣΤΑΜΑΤΗΣ ΘΕΟΔΩΡΟΣ	00:14:26
8	apapapanou	81.186.76.106	-	ΠΑΠΑΠΑΝΟΥ ΑΓΓΕΛΙΚΗ	00:13:06
9	michait	81.186.76.81	641048431	ΜΗΧΑΝΟΡΓΑΝΩΣΗ του ΓΡΑΦΕΙΟΥ Δ.Ε. ΑΙΤΙΟΛΟΓΟΚΑΡΝΑΓΙΑΣ	00:09:01
10	kyvritas	81.186.76.58	641024493	ΜΠΟΥΡΑΣ ΚΥΡΙΑΚΟΣ	00:07:04
11	oetsoukaras	81.186.76.46	-	ΤΣΟΥΚΑΡΑΣ ΚΩΝΣΤΑΝΤΙΝΟΣ	00:05:44
12	r-0pm-frisson	194.63.160.130	646022708	Router Dialup	00:04:49
13	Vgalias	81.186.76.107	641023902	ΓΑΛΑΤΙΑΣ ΒΑΣΙΛΕΙΟΣ	00:03:03
14	r-0pm-kendil	194.63.160.170	646051093	Router Dialup	00:00:35



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 μενού "password" είναι δυνατόν ο διαχειριστής να επαληθεύσει αν το password του χρήστη είναι πράγματι αυτό που ο τελευταίος ισχυρίζεται.

DIALUP ADMIN

SHOW | EDIT | ACCOUNTING | BADUSERS | DELETE | TEST

Connection Status for aduitsis (Athanasios Douitsis)

User is	not online now
Last Connection Time	2002-01-10 22:59:42
IP Address	ppp238.dialup.ntua.gr (147.102.223.238)
Online Time	1 minutes, 25 seconds
NAS Server	prometheus.dialup.ntua.gr (147.102.223.244)
NAS Port	188
Upload	5.61 KBs
Download	34.24 KBs
Allowed Session	user can login for 11 days, 11 hours, 46 minutes, 7 seconds
Usefull User Description	-

Check Password

Password

Account Status For The Last 7 Days

Connections	8
Online time	4 hours, 36 minutes, 16 seconds
Upload	2.18 MBs
Download	23.68 MBs
Average Time	34 minutes, 32 seconds
Average Upload	278.40 KBs
Average Download	2.96 MBs

6. Μεγέθη

Εξυπηρετητές AAA	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