ΣΤΗΡΙΖΩ | Υποστήριξη Ψηφιακού Σχολείου και νέες υπηρεσίες Πανελλήνιου Σχολικού Δικτύου

**Επιχειρησιακό Πρόγραμμα: «ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ» 2007-2013**

**ΠΡΑΞΗ:** «ΣΤΗΡΙΖΩ – Οριζόντιο Έργο Υποστήριξης Σχολείων, Εκπαιδευτικών και Μαθητών στο Δρόμο για το ΨΗΦΙΑΚΟ ΣΧΟΛΕΙΟ, νέες υπηρεσίες Πανελλήνιου Σχολικού Δικτύου και Στήριξη του ΨΗΦΙΑΚΟΥ ΣΧΟΛΕΙΟΥ (ΟΡΙΖΟΝΤΙΑ ΔΡΑΣΗ)»

**ΔΡΑΣΗ Α2: Βασικές (κρίσιμες) υπηρεσίες ΠΣΔ**

**εσίας**
**έτη**

| | |
|---|---|
| Κατάσταση Έκδοσης | **Υπό έγκριση από ΙΤΥΕ** |
| Ημερομηνία | **30/7/2012** |
| Περιγραφή Αρχείου | |
| Συμπράττων Φορέας | **ΕΠΙΣΕΥ** |
| Υπεύθυνος Παραδοτέου | **Σακκά Κωνσταντίνα** |
| Αριθμός Σελίδων | |
| Ημ/νια παραλαβής από Φορέα | **30/7/2012** |
| Ημ/νια παραλαβής από ΙΤΥΕ | |

**Ινστιτούτο Τεχνολογίας Υπολογιστών και Εκδόσεων «Διόφαντος» (ΙΤΥΕ)**

ΙΤΥΕ "ΔΙΟΦΑΝΤΟΣ" ινστιτούτο τεχνολογίας υπολογιστών & εκδόσεων

Ευρωπαϊκή Ένωση Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2007-2013 ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

## Ομαδα Εκπονησης Παραδοτεου

1. Καθ. Ευσταθιος Συκας
2. Δρ. Δημητριος Καλογερας
3. Κωνσταντινα Σακκα
4. Κωνσταντινος Καλευρας

# 1. ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΔΙΚΤΥΟΥ ΤΟΥ ΠΣΔ

## 1.1 ΣΧΟΛΙΚΕΣ ΜΟΝΑΔΕΣ

Το Πανελλήνιο Σχολικό δίκτυο, στην σημερινή μορφή με την οποία λειτουργεί, είναι από πολλές πλευρές ένα τυπικό δίκτυο πρόσβασης που παρέχει συνδεσιμότητα σε αρκετές χιλιάδες απομακρυσμένα σημεία. Τα σημεία αυτά είναι στην πλειοψηφία τους Ελληνικά σχολεία που ανήκουν είτε στην ***πρωτοβάθμια,*** είτε στην ***δευτεροβάθμια*** βαθμίδα του Ελληνικού εκπαιδευτικού συστήματος, ενώ συμπεριλαμβάνονται και ***διοικητικές*** μονάδες που εξυπηρετούν διοικητικούς και λοιπούς. Στο υπόλοιπο του παρόντος κειμένου, με την έννοια ***μονάδα*** ή ***σχολική μονάδα*** θα εννοείται οποιαδήποτε **διοικητική** υποδιαίρεση η οποία συνδέεται με το διαδίκτυο μέσω του δικτύου πρόσβασης του ΠΣΔ. Στις περισσότερες περιπτώσεις, μια διοικητική υποδιαίρεση του ΠΣΔ συμπίπτει με ένα συγκεκριμένο κτίριο, οπότε υπάρχει συνήθως ταύτιση ανάμεσα σε διοικητικές και γεωγραφικές μονάδες. Στις περιπτώσεις, όπως π.χ. κτιριακών συγκροτημάτων που στεγάζουν πολλά διαφορετικά σχολεία, η έννοια *μονάδα* θα αναφέρεται ξεκάθαρα στην διοικητική υποδιαίρεση, εκτός κι αν ρητά αναφέρεται το αντίθετο.

Σύμφωνα με στοιχεία του 2012, το ΠΣΔ περιλαμβάνει περίπου 17.000 μονάδες στις οποίες παρέχει δικτυακή πρόσβαση και όλες τις συναφείς υπηρεσίες δεδομένων στα μέλη τους. Όπως αναφέρθηκε προηγουμένως, οι κατηγορίες στις οποίες υποδιαιρούνται είναι:

1. Πρωτοβάθμιες μονάδες, περιλαμβάνουν περίπου του 60% των χρηστών του ΠΣΔ.
2. Δευτεροβάθμιες μονάδες, περιλαμβάνουν περίπου του 30% των χρηστών του ΠΣΔ.
3. Διοικητικές μονάδες, περιλαμβάνουν το υπόλοιπο 10%.

## 1.2 ACCESS CONCENTRATORS

Κάθε μονάδα του ΠΣΔ είναι συνδεδεμένη με το δίκτυο κορμού του ΠΣΔ μέσω ενός ακραίου δρομολογητή (Customer Premises Equipment, CPE) ο οποίος παρέχει συνδεσιμότητα στους διάφορους υπολογιστές και άλλες συνδεδεμένες συσκευές των μελών της ομάδας. Στις περιπτώσεις σύνδεσης DSL, ο ακραίος δρομολογητής συνδέεται και αποκαθιστά συνεδρία PPP με κάποιον δρομολογητή συγκέντρωσης (broadband aggregator, BRAS) του ΠΣΔ. Το ΠΣΔ χρησιμοποιεί επί του παρόντος 7 διαφορετικούς BRASs τύπου Cisco 7xxx (π.χ. 7301),

αλλά στο μέλλον το σχήμα αυτό πρόκειται να αλλάξει, με την εισαγωγή στην παραγωγή ενός Cisco ASR1000 ο οποίος θα δρα σαν το μοναδικό σημείο συγκέντρωσης συνόδων PPP του ΠΣΔ, συμπεριλαμβανομένων και των συνόδων PPP που θα προέρχονται από συνδέσεις VDSL.

## 1.3 ΑΚΡΑΙΟΙ ΔΡΟΜΟΛΟΓΗΤΕΣ

Οι διαμορφώσεις CPE που βρίσκονται σε χρήση σήμερα από ΠΣΔ είναι επιγραμματικά οι εξής:

1. Δρομολογητές **Cisco 876** (annex B) και **877** (annex A) οι οποίες διαθέτουν DSL interface και συνδέονται απευθείας μέσω PPP με το ΠΣΔ. Η μνήμη τους είναι **116 Mbytes**, διαθέτουν αποθηκευτικό χώρο flash **28 Mbytes** και η έκδοση λογισμικού είναι **12.3.4T4**.

2. Δρομολογητές **Cisco 831** χωρίς DSL interface οι οποίες συνδέονται μέσω PPPoE με το ΠΣΔ. Η μνήμη τους είναι **43 Mbytes**, διαθέτουν αποθηκευτικό χώρο **12 Mbytes** και η έκδοση λογισμικού είναι επίσης η **12.3.4T4**. Το bridging CPE που εκτελεί χρέη PPPoE bridge (RFC 1483) είναι ένα **Alcatel Speedtouch** με DSL interface (annex B ή A).

3. Συσκευές **Alcatel SpeedTouch** οι οποίες συνδέονται μέσω PPPoE με το ΠΣΔ και δίνουν απευθείας ή μέσω switch συνδεσιμότητα στις συσκευές της σχολικής μονάδας.

4. Δρομολογητές **λοιπής προέλευσης** οι οποίες έχουν αγοραστεί από τις μονάδες απευθείας και για τις οποίες το ΠΣΔ δεν είχε ανάμιξη στην επιλογή τους. Στις περισσότερες περιπτώσεις οι συσκευές αυτές ανήκουν στους τύπους που προμηθεύει ο ΟΤΕ στους συνηθισμένους πελάτες του.

5. Δρομολογητές που συνδέονται μέσω Metro Ethernet (αντί για DSL) με κάποιον κεντρικό δρομολογητή του ΠΣΔ.

## 1.4 ΈΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ΓΙΑ ΜΟΝΑΔΕΣ ΚΑΙ ΧΡΗΣΤΕΣ

Με εξαίρεση τις μονάδες που συνδέονται μέσω Metro Ethernet, οι ακραίοι δρομολογητές των σχολείων (Customer Premises Equipment – CPE) χρησιμοποιούν επιλεγόμενη πρόσβαση είτε μέσω τεχνολογίας ISDN είτε μέσω ADSL με χρήση συνθηματικών. Στην πλειοψηφία των περιπτώσεων, ο δρομολογητής συγκέντρωσης δέχεται μέσω του

πρωτοκόλλου PPP (Point to Point Protocol) από κάθε CPE τα συνθηματικά χρήσης. Ο δρομολογητής συγκέντρωσης προωθεί στην υποδομή AAA τα συνθηματικά για έλεγχο και αποδοχή ή απόρριψη της σύνδεσης.

Παρόμοια οι απομακρυσμένοι χρήστες του ΠΣΔ που χρησιμοποιούν επιλεγόμενη πρόσβαση (dialup) χρησιμοποιούν συνθηματικά χρήσης.

# 2. ΠΕΡΙΓΡΑΦΗ ΥΠΗΡΕΣΙΑΣ - AAA

Το περιβάλλον του Πανελλήνιου Σχολικού Δικτύου λειτουργεί ως ένα κλειστό δημόσιο δίκτυο (campus network) με δυνατότητες απομακρυσμένες πρόσβασης (Dial-in) για τα σχολεία του ΥΠ. ΠΔΒΜ. Οι απαιτήσεις λειτουργίας των υπηρεσιών του ΠΣΔ δεν είναι ίδιες για όλες τις υπηρεσίες. Η υπηρεσία Πιστοποίησης, Εξουσιοδότησης και Καταγραφής (ΠΕΚ) (Authentication Authorization Accounting- AAA)/ του Πανελλήνιου Σχολικού είναι εξαιρετικά κρίσιμη δεδομένου οτι σε αυτήν βασίζεται η πρόσβαση ΟΛΩΝ ΤΩΝ ΜΟΝΑΔΩΝ (δημοτικών/γυμνασίων/λυκείων) του ΥΠ. ΠΔΒΜ.

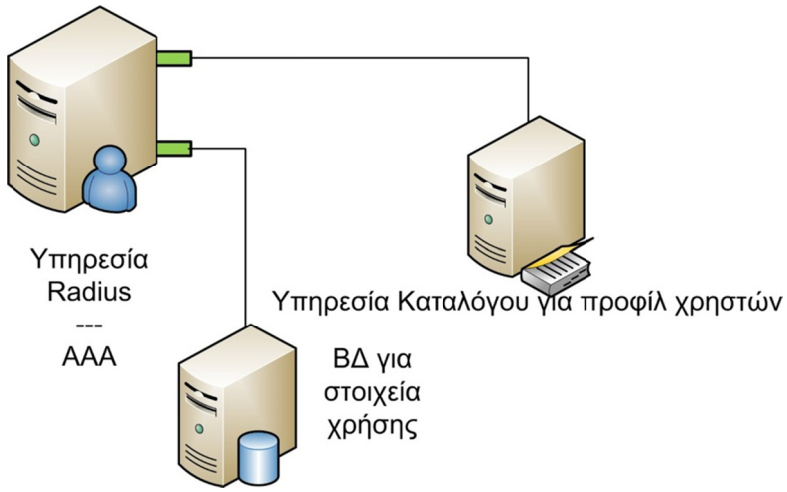
Η υπηρεσία ΑΑΑ/ΠΕΚ του ΠΣΔ βασίζεται στο πρωτόκολλο RADIUS [1](Remote Authentication Dial In User Service - RADIUS) το οποίο αναπτύχθηκε αρχικά από την Livingston το 1991 και το οποίο αργότερα ενσωματώθηκε στα πρότυπα του Internet Engineering Task Force (IETF). Το RADIUS είναι ένα πρωτόκολλο client/server το οποίο χρησιμοποιεί πακέτα UDP για την πιστοποίηση χρηστών από δικτυακές συσκευές και υπηρεσίες (π.χ. Network Access Server, Remote Access Server, Virtual Private Network - VPNs). Στο περιβάλλον του Πανελλήνιου Σχολικού Δικτύου (ΠΣΔ) η υποδομή ΑΑΑ/ΠΕΚ είναι υλοποιημένη στην ελεύθερη πλατφόρμα λογισμικού FreeRADIUS [FR].

## 2.1 ΓΕΝΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΗΣ ΥΠΗΡΕΣΙΑΣ

Η απομακρυσμένη πρόσβαση (Dial-in) στο πανελλήνιο σχολικό δίκτυο γίνεται κατόπιν ταυτοποίησης. Η απομακρυσμένη πρόσβαση γίνεται για τα μέλη του σχολικού δικτύου ( π.χ. καθηγητές) και τις απομακρυσμένες μονάδες (π.χ. σχολικές μονάδες). Ο μεγάλος αριθμός των προηγούμενων οντοτήτων (καθηγητών και σχολικών μονάδων) και η απαίτηση για διαφοροποιημένη παροχή της υπηρεσίας έχει οδηγήσει στην αποτύπωση ενός διαφορετικού προφίλ χρήσης για να υπάρχει μια προσωποποιημένη υπηρεσία η οποία με την σειρά της οδήγησε στην αποθήκευση των προφίλ χρήσης σε αποθετήριο καταλόγου (Directory Service).

[1] **Remote Authentication Dial In User Service (RADIUS)** http://www.ietf.org/rfc/rfc2865.txt

Επιπλέον η απαίτηση για καταγραφή της χρήσης της υπηρεσίας επέβαλε την καταγραφή των δεδομένων χρήσης (accounting) σε βάση δεδομένων. Ως εκ τούτου η υπηρεσία ΑΑΑ αλληλεπιδρά με τρία υποσυστήματα α) την πλατφόρμα FreeRadius β) την υποδομή καταλόγου (Directory Server) και γ) την υποδομή αποθετηρίου (Data Base) των στατιστικών χρήσης.




**Σχήμα 1 Διασύνδεση υπηρεσίας ΑΑΑ με υπηρεσία καταλόγου και ΒΔ[2]**

## 2.2 ΕΠΙΛΟΓΗ ΤΗΣ ΠΛΑΤΦΟΡΜΑΣ FREERADIUS ΓΙΑ ΧΡΗΣΗ RADIUS

Η πλατφόρμα λογισμικού FreeRADIUS πρωτοεμφανίστηκε τον Ιούνιο του 1999 από τον Miquel van Smoorenburg και τον Alan DeKok. Η πρώτη έκδοση (alpha) βγήκε τον Αύγουστο του 1999 με νεώτερες εκδόσεις να ακολουθούν σε διάστημα λίγων μηνών. Σήμερα η πλατφόρμα FreeRADIUS ισχυρίζεται ότι είναι η πιο διαδεδομένη στην αγορά με 50.000 εγκαταστάσεις ταυτοποιώντας περίπου το ⅓ των χρηστών στο Διαδίκτυο.

[2] Η χρήση εικονιδίων server στο παραπάνω σχήμα δεν υπονοεί και συγκεκριμένη πληθύσμωση τους.

Η πλατφόρμα FreeRADIUS περιλαμβάνει ένα RADIUS server, μια βιβλιοθήκη προγραμμάτων πελάτη και βιβλιοθήκη με modules - Pluggable Authentication Modules (PAM). Η πλατφόρμα FreeRADIUS έχει την άδεια λογισμικού GNU General Public License (GPL) version 2, ενώ η βιβλιοθήκη των προγραμμάτων πελάτη είναι υπό την άδεια του Berkeley Software Distribution (BSD). Σαν ανοιχτό λογισμικό προσφέρει τα γνωστά προνόμια της ελευθερίας χρήσης και τροποποίησης και της ποιότητας του κώδικα. (http://freeradius.org/).

## 2.3 ΕΠΙΛΟΓΗ ΠΛΑΤΦΟΡΜΑΣ ΑΠΟΘΕΤΗΡΙΟΥ ΚΑΤΑΛΟΓΟΥ

Στο ΠΣΔ το αποθετήριο καταλόγου είναι μια υφιστάμενη υποδομή και ως εκ τούτου δεν απαιτείται η προδιαγραφή και κατασκευή της εκ του μηδενός για την υπηρεσία ΑΑΑ/ΠΕΚ. Η υπηρεσία καταλόγου περιγράφεται αναλυτικά στο παραδοτέο [XXXX]. Η υποδομή καταλόγου βασίζεται στο ελεύθερο λογισμικό OpenLDAP [OD] το οποίο αποτελεί το λογισμικό αναφοράς για την ανάπτυξη της τεχνολογίας καταλόγου.

## 2.4 ΑΠΑΙΤΗΣΕΙΣ – ΛΕΙΤΟΥΡΓΙΑ - ΣΥΓΚΡΟΤΗΣΗ ΥΠΗΡΕΣΙΑΣ ΚΑΤΑΛΟΓΟΥ ΓΙΑ ΤΗΝ ΥΠΗΡΕΣΙΑ ΑΑΑ

Αναφορικά με την υπηρεσία ΑΑΑ/ΠΕΚ, η υπηρεσία καταλόγου αποθηκεύει για κάθε οντότητα (π.χ. τελικός χρήστης, σχολική μονάδα κλπ) ένα *εξέχων όνομα* (Distinguished Name-DN). Κάθε *εξέχων όνομα* συνοδεύεται από απλά χαρακτηριστικά όπως π.χ όνομα (χρήστη) *username* της οντότητας, το συνθηματικό (*password*) ή/και πιο σύνθετα χαρακτηριστικά όπως το προφίλ χρήσης διαφόρων υπηρεσιών, εν προκειμένω *radius profile attributes*. Ως εκ τούτου, ελάχιστη απαίτηση είναι να προστεθεί η κλάση radiusprofile με τα αντίστοιχα attributes στο LDAP schema. Επιπλέον προτείνεται το attribute uid να είναι indexed προκειμένου να γίνονται γρήγορα οι αναζητήσεις για χρήστες.

Ειδικότερα για κάθε απομακρυσμένο χρήστη ο οποίος αιτείται ταυτοποίηση και παρουσιάζει ένα συνδυασμό ονόματος χρήστη (username) και συνθηματικού (password) η υπηρεσία ΑΑΑ/ΠΕΚ μέσω της υπηρεσία καταλόγου χρειάζεται να:

1. ανακαλέσει (search) με βάση το username το συνθηματικό του και το προφίλ του.

2. να ταυτοποίησει (ελέγξει) την εγκυρότητα του συνθηματικού του. Αυτό γίνεται μέσω των ενδογενών μηχανισμών ταυτοποίησης της υπηρεσίας καταλόγου (ldap bind)

3. να ανακαλέσει τα χαρακτηριστικά του προφίλ του κάθε χρήστη. Το προφίλ αναζητείται με κλειδί το username του χρήστη από το οποίο προσδιορίζεται στο (Distinguished Name-DN) της εγγραφής του και στην συνέχεια εξάγονται τα αντίστοιχα radius attributes περιέχονται στην εγγραφή. Σε περίπτωση που έχουν ενεργοποιηθεί επιπλέον δυνατότητες πραγματοποιούνται επιπλέον αναζητήσεις για τα *Default/User/Regular Profiles*. Κατά συνέπεια κάθε access-request συνεπάγεται το λιγότερο μία αναζήτηση στον εξυπηρετητή ldap ενώ μπορεί τελικά να πραγματοποιηθούν μέχρι και άλλες δύο επιπλέον αναζητήσεις.

Δεδομένου οτι η υπηρεσία καταλόγου είναι μια από τις υφιστάμενες υποδομές του ΠΣΔ η απαίτηση της υπηρεσία ΑΑΑ/ΠΕΚ με όρους υποδομής έχει να κάνει με την συγκρότηση (configuration) του προφίλ των χρηστών και την λειτουργία (operation) της υπηρεσίας καταλόγου για υψηλή διαθεσιμότητα και χαμηλό χρόνο απόκρισης.

Η συγκρότηση του προφίλ του χρηστών γίνεται σε δύο στάδια:

1. ορισμός και εισαγωγή του κατάλληλου σχήματος δεδομένων με μια κλάση (object class) radiusprofile με τα αντίστοιχα attributes στο LDAP schema καθώς επίσης και τα απαραίτητα indices στα attribute uid στο όνομα του group (συνήθως το cn). Πληροφορίες για αυτό το σχήμα

2. και πληθύσμωση των χρηστών με τα κατάλληλά χαρακτηριστικά radius από την εφαρμογή διαχείρισης χρηστών (η οποία στο ΠΣΔ είναι η εφαρμογή diaupadmin).

Τα χαρακτηριστικά του radius δεν είναι ομογενή για όλες τις οντότητες του ΠΣΔ. Αυτό οφείλεται στη διαφορετική φύση των οντοτήτων που χρειάζονται υπηρεσίες ΑΑΑ/ΠΕΚ. Συνοπτικά υπάρχουν τέσσερις διαφορετικές κατηγορίες προφίλ χρήσης:

- **Dialup User Profiles:** Για κάθε σχολική μονάδα που ανήκει στο ΠΣΔ (και στο μέλλον για ένα μεγάλο μέρος της εκπαιδευτικής κοινότητας) καταχωρείται ένας

dialup λογαριασμός (ο οποίος ενσωματώνεται στην εγγραφή του χρήστη στην υπηρεσία καταλόγου).

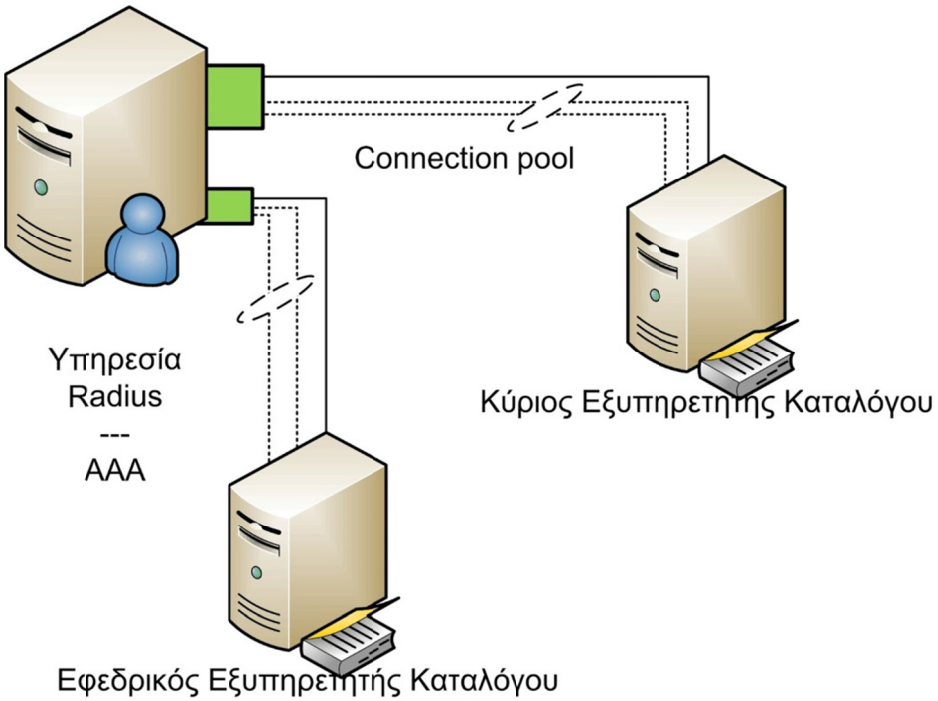
- **Router Profiles:** Για τους routers με τους οποίους συνδέονται τα σχολικά αργαστήρια στο ΠΣΔ. Για κάθε τέτοιο router δημιουργείται μία εγγραφή μορφής r-<router-name> (με το <router name> να προκύπτει κατά βάση από το DNS της μονάδας). Η διαφορά με το προηγούμενο προφίλ είναι οτι το παρόν προφίλ χρησιμοποείται από δρομολογητές αποκλειστικά και δεν έχει πρόσβαση σε άλλες υπηρεσίες (πχ email).
- **Outbound Route Profiles:** Για την υλοποίηση εξερχόμενων κλήσεων προς κάθε δρομολογητή σχολικής μονάδας από τους κεντρικούς συγκεντρωτές πρόσβασης απαιτείται η ύπαρξη ενός outbound route profile.
- **Large Scale Dialout**: προφίλ για συσχετισμό πληροφοριών δρομολόγησης με εξερχόμενες κλήσεις χρησιμοποιώντας κατά ακολουθία το προηγούμενο προφίλ.

Οι λειτουργικές απαιτήσεις της υπηρεσίας ΑΑΑ/ΠΕΚ περιορίζονται σε:

1. τουλάχιστον διπλή φυσική διασύνδεση με την υπηρεσία καταλόγου για επίτευξη υψηλής διαθεσιμότητας προς την υπηρεσία καταλόγου.

2. μια ομάδα ανοικτών συνδέσων (connection-pool) προς τους εξυπηρετητές καταλόγου για μείωση του χρόνου (connection overhead) εγκατάστασης σύνδεσης (establishment time).

Συνοπτικά αυτό φαίνεται στο παρακάτω σχήμα:

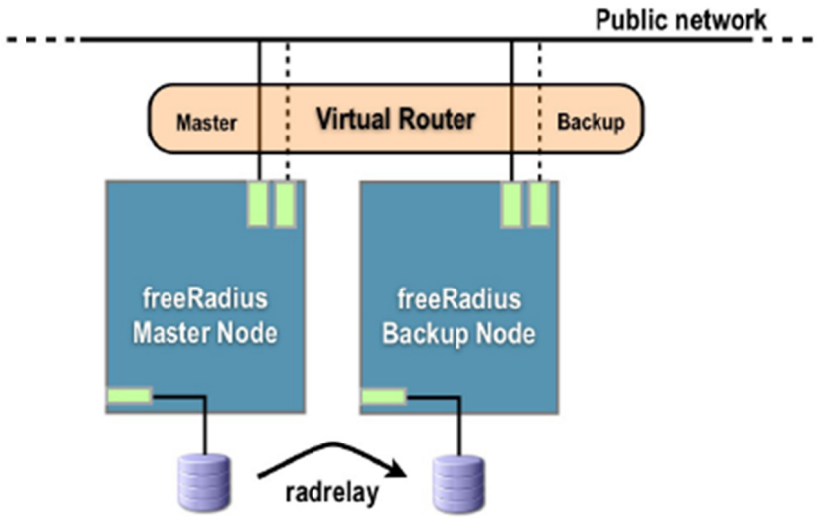



**Σχήμα 2 Συγκρότηση Υπηρεσίας Καταλόγου**

## 2.5 ΕΠΙΛΟΓΗ ΠΛΑΤΦΟΡΜΑΣ ΓΙΑ ΑΠΟΘΕΤΗΡΙΟ ΣΤΑΤΙΣΤΙΚΩΝ ΧΡΗΣΗΣ (ACCOUNTING) ΥΠΟΔΟΜΗΣ ΠΕΚ/AAA

Το πρωτόκολλο Radius υλοποιώντας μια υποδομή ταυτοποίησης και καταγραφής χρησιμοποιεί πακέτα (Radius) ταυτοποίησης (auth-requests) και πακέτα στατιστικών (accounting packets). Η διαδικασία της καταχώρησης (accounting) ξεκινά μετά την επιτυχή πιστοποίηση ενός χρήστη με την καταγραφή του νέου session, η οποία επικαιροποιείται μετά την έναρξη της σύνδεσης (στην μεριά του access servers) κατά την οποία ο access server στέλνει ένα πακέτο τύπου Accounting-Start στο radius server περιέχοντας βασικές πληροφορίες για τη σύνδεση. Η καταγραφή των στατιστικών χρήσης γίνεται υπό μορφή πληροφορίας σε υποδομή βάση δεδομένων (ΒΔ). Τα καταχωρημένα στοιχεία ανακαλούνται είτε σε ενεργό χρόνο (online) π.χ. για την αποφυγή διπλο-εγγραφών ενεργών χρηστών είτε για την δημιουργία απαραίτητων στατιστικών μετρικών π.χ. μέσος/μέγιστος χρόνος χρήσης/αναμονής και περαιτέρω δημιουργίας πολιτικών χρήσης. Επειδή η εφαρμογή των πιλοτικών χρήσης της υπηρεσίας πρόσβασης και η εξαγωγή στοιχείων χρήσης είναι απαραίτητη προτείνεται η διασφάλιση της υποδομής δεδομένων χρήσης με τεχνικές υψηλής

διαθεσιμότητας. Στην γενικότερη μορφή, αυτό σημαίνει την ύπαρξη τουλάχιστον δύο εξυπηρετητών (server) για μια συστοιχία ταυτοποίησης (radius) για την υψηλή διαθεσιμότητα του αρχείου καταγραφής όπως φαίνεται στο σχήμα, συνεπικουρούμενη από μια συστοιχία υποδομής ΒΔ (Βάση δεδομένων).




**Σχήμα 3 Τυπικό περιβάλλον υψηλής διαθεσιμότητας ΑΑΑ/ΠΕΚ για υψηλή διαθεσιμότητα αρχείου χρήσης (accounting detail)**

Στο παραπάνω σχήμα φαίνονται δύο εξυπηρετητές FreeRADIUS οι οποίοι έχουν διπλές δυνδέσεις (κύριες-master και εφεδρικές-backup) στους οποίους έχει ενεργοποιηθεί μια δυναμική διεύθυνση με χρήση του πρωτοκόλλου Virtual Redundancy Router Protocol (VRRP) ή του CARP[3]. Η ενεργοποίηση του εν λόγω πρωτοκόλλου δημιουργεί μια τοπολογία (Active/standby) η οποία μοιράζεται δυναμικά μια διεύθυνση IP πάνω στην οποία ενεργοποιείται η διαδικασία FreeRADIUS.

[3] CARP (Common Address Redundancy Protocol) είναι μια εναλλακτική τεχνολογία υψηλής διαθεσιμότητας διεύθυνσης IP (αντί της χρήσης του VRRP) το οποίο υποστηρίζει πλήρως IPv6 και επιπρόσθετα χρησιμοποιεί κρυπτομηχανισμούς για τις ανακοινώσεις. Αναπτύχθηκε από την ομάδα του OpenBSD εξαιτίας των προβλημάτων με τα δικαιώματα χρήσης του HSRP και VRRP από την CISCO.

Σε επίπεδο δεδομένων χρήσης (accounting data) η διασφάλιση των δεδομένων εξασφαλίζεται από το γεγονός ότι η βάση SQL θα λειτουργεί σε δύο αντίτυπα, με λογική master-slave replication. Η καταγραφή θα γίνεται σε μία από τις δύο βάσεις (η οποία θα θεωρείται master) και θα γίνεται online replication στη slave. Σε περίπτωση απώλειας του master η καταγραφή θα γίνεται αυτόματα στο slave. Για το σκοπό αυτό θα χρησιμοποιηθεί ένα κοινό resource (IP), το οποίο θα αποδίδεται στον master με χρήση λογισμικού heartbeat.

## 2.6 Υψηλη διαθεσιμοτητα υποδομης ΒΔ για ΑΑΑ/ΠΕΚ

Όπως αναφέρθηκε παραπάνω η διαδικασία καταγραφής (accounting) αποθηκεύει στοιχεία χρήσης σε μια μόνιμη υποδομή ΒΔ. Ειδικότερα ο πίνακας **radacct** αποθηκεύει πληροφορίας για κάθε dial-up/dsl session σε κάθε γραμμή πίνακα (row) ως εξής. Μια επιτυχής πιστοποίηση ενός χρήστη δημιουργεί μια νέα γραμμή (row) στον πίνακα radacct ο οποίος περιέχει τις διαθέσιμες πληροφορίες της σύνδεσης. Μετά την επιτυχή σύνδεση, ο access server στέλνει και Accounting-Start με επιπλέον στοιχεία της σύνδεσης που δεν ήταν γνωστά κατά την αρχικοποίησης π.χ. δ/νση IP. Μετά την αποσύνδεση του χρήστη ενημερώνεται η γραμμή του με πλήθος πληροφοριών για τη σύνδεση όπως τα bytes που παραλήφθηκαν και στάλθηκαν, ip address, κτλ.

Η διασφάλιση δεδομένων καταγραφής μιας υποδομής ΑΑΑ/ΠΕΚ σε Βάση Δεδομένων (ΒΔ) γίνεται σε δύο φάσεις: α) με συγχρονισμό, φροντίζοντας για αξιόπιστη αντιγραφή των πινάκων μεταξύ ενός κύριου (master) ενός ή περισσοτέρων slave και β) με τον μηχανισμό μετάπτωσης.

Η υποδομή αποθήκευσης της ΒΔ και των πινάκων της είναι εξαιρετικής σημασίας για την διαδικασία καταγραφής και ως εκ τούτου απαιτείται η διασφάλιση της υποδομής με αντίγραφα ασφαλείας, ιδανικά, σε πραγματικό χρόνο. Η διαδικασία αντιγράφων βάσης ονομάζεται replication και δημιουργεί σχεδόν συγχρονισμένα πανομοιότυπα αντίγραφα μια ΒΔ και των πινάκων της σε μια άλλη ΒΔ.

Εν προκειμένω χωρίς την ύπαρξη κεντρικών οδηγιών/επιλογών θα περιοριστούμε στην επιλογή MySQL για σχεσιακή ΒΔ η οποία έχει δοκιμαστεί εκτεταμένα τα τελευταία χρόνια και η οποία υποστηρίζει συγχρονισμό (replication) αντιγράφων.

Τα βασικά βήματα για MySQL replication (τα οποία μπορεί να διαφέρουν στις λεπτομέρειες ανάλογα με την έκδοση που χρησιμοποιείται) είναι:

- Ρύθμιση ενός μοναδικού Server Id και περαιτέρω ενεργοποίηση binary logging (με πιθανή επανεκκίνηση του server) στον κόμβο Master.
- Σε κάθε κόμβο Slave ρύθμιση ενός μοναδικού Server Id ((με πιθανή επανεκκίνηση του server).
- Προαιρετικά δημιουργία χρηστών με τα απαραίτητα διαπιστευτήρια για την ταυτοποίηση τους στην διαδικασία αντιγραφής.
- Δημιουργία στιγμιότυπου (sqldump) και αποτύπωση της θέσης εκκίνησης (replication point) για την αντιγραφή στο Master.
- Ρύθμιση των Slave με τα χαρακτηριστικά της διαδικασίας αντιγραφής (χρήστες, συνθηματικά, διευθύνσεις) καθώς και το σημείο εκκίνησης αντιγραφής.

Η διαδικασία MySQL replication είναι εξ' ορισμού ασύγχρονη. Ο master γράφει γεγονότα (events) στο binary log αλλά δεν γνωρίζει εάν ο/οι slave έχει/ουν καταφέρει να γράψουν τις εγγραφές επιτυχώς. Με το ασύγχρονο replication, εάν ο master πάθει βλάβη δεν είναι σίγουρο οτι λειτουργίες που έχει εκτελέσει θα έχουν καταφέρει να μεταδοθούν στον/στους slave και το αντίστροφο. Ως εκ τούτου μετάπτωση από τον master στο slave μπορεί να επιφέρει ελλειμματικές πληροφορίες. Με την υπόθεση ότι υπάρχουν επικαιροποιημένα αντίγραφα ΒΔ απαιτείται η διαδικασία καταγραφής του FreeRadius να μπορεί να στέλνει τα δεδομένα στο σωστό αντίγραφο. Αυτό επιτυγχάνεται με μηχανισμούς μετάπτωσης. Θα εξεταστεί ο μηχανισμός Heartbeat ο οποίος είναι εξαιρετικά διαδεδομένος και ο μηχανισμός Distributed Replicated Block Device (DRBD).

## 2.7 HEARTBEAT [HA]

Η τεχνική λύση Heartbeat είναι αποτέλεσμα του project Linux-HA [HA] το οποίο προσφέρεται σε διάφορα λειτουργικά συστήματα και μπορεί να χρησιμοποιηθεί εκτός από εφαρμογές ΒΔ όπως η Mysql και σε εφαρμογές mail, DNS κλπ. Η τεχνική Heartbeat υλοποιεί ένα πρωτόκολλο μηνυμάτων heartbeat τα οποία στέλνονται σε τακτά χρονικά

διαστήματα μεταξύ ενός κύριου (master) και ενός ή περισσότερων slave κόμβων. Εάν ένα μήνυμα δεν ληφθεί εντός χρονικού διαστήματος, αυτό σημαίνει ότι ο κόμβος έχει πρόβλημα και θα χρειαστεί μετάπτωση σε ένα δευτερεύον κόμβο. Ο κύριος κόμβος (master) μοιράζεται με τους δευτερεύοντες μια ιδεατή διεύθυνση IP (με μεταβλητή διεύθυνση ARP) η οποία αποδίδεται σε μια πόρτα δικτύου. Αυτή είναι η διεύθυνση (σταθερή IP, μεταβλητή ARP) μέσω της οποίας αποκτούν πρόσβαση εξωτερικές εφαρμογές στην MySQL. Εάν ο κύριος κόμβος υποστεί βλάβη ένας δευτερεύον κόμβος θα αναλάβει την διεύθυνση σε μια άλλη πόρτα δικτύου και με την χρήση "gratuitous ARP" θα διασφαλίσει ότι όλη η κίνηση για την εν λόγω δυναμική διεύθυνση θα παραληφθεί από το συγκεκριμένο σταθμό.

Αυτή η μέθοδος μετάπτωσης ονομάζεται συχνά "IP Address Takeover" επειδή οι ιδεατές διευθύνσεις θεωρούνται αγαθά. Τα αγαθά αυτά ενσωματώνονται συνήθως μέσα σε scripts (π.χ. init) το οποίο σημαίνει οτι μπορεί να ξεκινήσουν/σταματήσουν ανάλογα με την κατάσταση του πρωτοκόλλου heartbeat.

Στην περίπτωση της MySQL και προκειμένου να αποφευχθούν προβλήματα στο replication:

1. Το replication είναι της μορφής multi-master (κάθε εξυπηρετητής μπορεί να λειτουργήσει ως master και να πραγματοποιούνται απευθείας εγγραφές σε αυτόν).

2. Δεν αποδεσμεύονται τα αγαθά του κοινού resource από τον βοηθητικό εξυπηρετητή αυτόματα μετά την επιδιόρθωση (π.χ. αποκατάσταση δικτυακού προβλήματος) στον αρχικό εξυπηρετητή αν αυτός επανέλθει.

## 2.8 (DISTRIBUTED REMOTE BLOCK DEVICE) [DRBD]

Για την παροχή υψηλής διαθεσιμότητας στην υποδομή ΒΔ του ΑΑΑ/ΠΕΚ αντί του μηχανισμού αντιγραφής/συγχρονισμού των πινάκων είναι εφικτό να επιτευχθεί ο ίδιος στόχος στο επίπεδο της υποδομής αποθήκευσης. Ειδικότερα η μέθοδος DRBD (Distributed Remote Block Device) καταφέρνει το συγχρονισμό στο επίπεδο της στοιχειώδους μονάδας αποθήκευσης.

Τα κατανεμημένα αντίγραφα block συσκευών αποτελούν ένα μηχανισμό κατανεμημένης αποθήκευσης με αντίγραφα παρόμοια με αυτό του RAID-1 αλλά υλοποιημένα πάνω σε υποδομή δικτύου. Οι συσκευές block αποτελούν την μικρότερη δομική μονάδα περιγραφής

συσκευής αποθήκευσης. Το λειτουργικό σύστημα γράφει/διαβάζει από τις συσκευές block κομμάτια δεδομένων τα οποία ονομάζονται blocks. Οι συσκευές block χρησιμοποιούν buffers για ανάγνωση και γράψιμο. Όταν μια εφαρμογή αιτείται εγγραφή/ανάγνωση δεδομένων, κάθε χαρακτήρας αποθηκεύεται σε buffer και όταν γεμίσει ο buffer ολοκληρώνεται η λειτουργία. Τα λειτουργικά συστήματα χρησιμοποιούν συσκευές αποθήκευσης block στις περιπτώσεις συσκευών αποθήκευσης τυχαίας πρόσβασης. Στην πιο απλή μορφή οι συσκευές block είναι δίσκοί ή partition δίσκων. Σε πιο σύνθετες περιπτώσεις μπορεί να είναι μια συστάδα (stack) συσκευών ή ιδεατές συσκευές.

Κάθε συσκευή η οποία έχει ρυθμιστεί σε DRBD cluster έχει μια κατάσταση η οποία μπορεί να είναι είτε πρωτεύουσα είτε δευτερεύουσα. Το DRBD δημιουργεί και στους δύο κόμβους ένα δεσμό μεταξύ μιας ιδεατής συσκευής και ενός τοπικού partition. Όλες οι εγγραφές γίνονται αρχικά στον πρωτεύοντα κόμβο και μέσω των κατανεμημένων συσκευών block μεταφέρονται στον/στους δευτερεύοντες. Οι δευτερεύοντες κόμβοι στην συνέχεια πραγματοποιούν τις αλλαγές στις χαμηλότερες συσκευές block. Εάν γίνει βλάβη στον πρωτεύοντα κόμβο η διαδικασία του cluster θα προβιβάσει τον δευτερεύοντα κόμβο σε κύριο. Όταν γίνει επαναφορά του κατεστραμμένου κόμβου το σύστημα διαχείρισης ανάλογα με τις ρυθμίσεις του διαχειριστή θα ξαναπροβιβάσει ή θα αφήσει τον κόμβο σε δευτερεύοντα ρόλο.

Οι συσκευές block χρησιμοποιούνται συνήθως από τα συστήματα αρχείων (ΣΑ). Όταν ένα ΣΑ χρησιμοποιεί συσκευές block (DRBD) αποκτά υψηλή διαθεσιμότητα. Ο μηχανισμός Linux-HA χρησιμοποιείται για τον χειρισμό των καταστάσεων μετάβασης καθώς επίσης και για την ενεργοποίηση του μηχανισμού mounting των ΣΑ πάνω από τις ιδεατές συσκευές που δημιουργούνται από το DRBD.

Είναι αξιοσημείωτο ότι το DRBD είναι διαθέσιμο κατά την διάρκεια συγχρονισμού επειδή μόνο τα τμήματα τα οποία έχουν υποστεί αλλαγές χρειάζονται συγχρονισμό.

Ένα σημαντικό στοιχείο αντοχής του DRBD είναι ότι χειρίζεται καταστάσεις “split-brain” η οποία συμβαίνει όταν χαθεί η δικτυακή σύνδεση μεταξύ των μελών ενός cluster αλλά οι κόμβοι είναι ενεργοί. Το DRBD έχει την δυνατότητα να ανιχνεύει τέτοιες καταστάσεις επειδή έχει υιοθετήσει ένα μηχανισμό μεταβολής καταστάσεων (Finite state machine). Στις

περιπτώσεις “split-brain” είναι σύνηθες ότι και οι δύο κόμβοι αντιλαμβάνονται ότι είναι οι μοναδικοί επιζήσαντες και αναλαμβάνουν την ιεραρχία του cluster με την ενεργοποίηση των αγαθών τοπικά. Στο DRBD αυτή η κατάσταση δημιουργεί αποκλίνοντα σετ δεδομένων στα οποία είναι δυνατόν να επιτευχθεί σύγκλιση υιοθετώντας αυτόματες ή χειροκίνητες πολιτικές ανάκαμψης.

Όταν η MySQL χρησιμοποιείται σε συνδυασμό με DRBD τα δεδομένα του ΣΑ αντιγράφονται μεταξύ του Master και του slave χρησιμοποιώντας τις συσκευές DRBD έχοντας την MySQL [MYSQL] ενεργοποιημένη μόνο στον master. Όταν ο master πάθει βλάβη οι συσκευές DRBD του slave γίνονται οι κύριες (primary), τα ΣΑ γίνονται mount και ξεκινά η MySQL. Ο αρχικός master έχει τα αγαθά του απενεργοποιημένα με τις συσκευές DRBD σε δευτερεύουσα κατάσταση και την MysQL απενεργοποιημένη.

Στην παρούσα φάση δεν έχει αποφασιστεί κεντρικά από το ΠΣΔ εάν θα προσφερθεί υποδομή ΒΔ με χαρακτηριστικά υψηλής διαθεσιμότητας σε λογική λειτουργίας cluster κατά την πρώιμη φάση λειτουργίας των datacenters. Όταν και εφόσον αποφασιστεί η λειτουργία κεντρικής υποδομής ΒΔ θα επικαιροποιηθεί το παρόν παραδοτέο.

## 2.9 ΑΠΑΙΤΗΣΕΙΣ ΛΕΙΤΟΥΡΓΙΑΣ -ΠΕΡΙΒΑΛΛΟΝ ΛΕΙΤΟΥΡΓΙΑΣ ΣΥΝΝΕΦΟΥ

Οι γενικές απαιτήσεις υποδομής που έχουν γνωστοποιηθεί από τον κύριο του Έργου (Ε.Α.ΙΤΥ) είναι για ένα ιδεατό περιβάλλον σύννεφου (cloud). Η λειτουργία της υπηρεσίας ΠΕΚ/ΑΑΑ με λογισμικό FreeRadius σε περιβάλλον cloud δεν είναι κάτι καινούργιο. Η ομάδα ανάπτυξης της υπηρεσίας έχει εμπειρία από την υποστήριξη και λειτουργία υποδομής ΠΕΚ/ΑΑΑ στο περιβάλλον του Φοιτητικού DSL του ΕΔΕΤ. (Εν τούτοις χρειάζεται να επιβεβαιωθεί και να ελεγχτεί η λειτουργία μετάπτωσης από κύριο σε εφεδρικό κόμβο με χρήση των ενδογενών μηχανισμών μετάπτωσης του σύννεφου π.χ. vmotion [VMWARE] για περιβάλλον vmware, xenmotion [XEN] για περιβάλλον Xen, live migration για kvm [KVM]. Εναλλακτικά μπορούν να χρησιμοποιηθούν οι γενικές οδηγίες που δόθηκαν στην ενότητα για το περιβάλλον υψηλής διαθεσιμότητας)

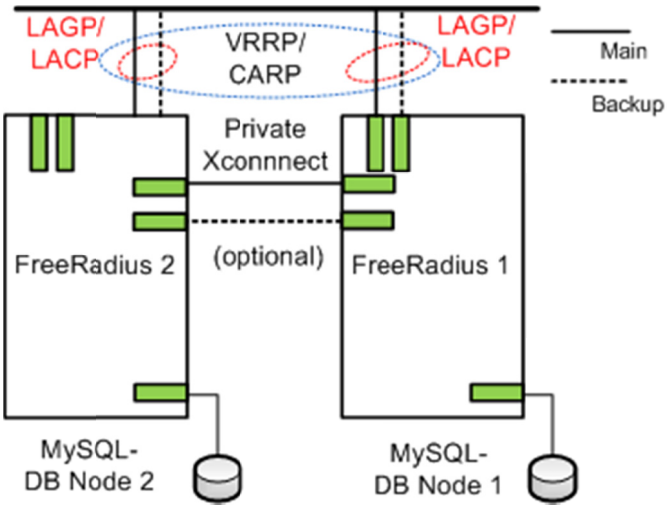
Γενικά δεν υπάρχουν ποσοτικές εκτιμήσεις των απαιτήσεων για την νέα υπηρεσία π.χ. Μέγιστο/μέσο αριθμό κλήσεων, μέγιστο/μέσο αριθμό ρυθμό κλήσεων κλπ εκτός από τον μέγιστο χρόνο απόκρισης σε μια κλήση radius ο οποίος έχει οριστεί σε 20 sec (4

συνεχόμενες φορές με άνω όριο 5 sec ανά φορά). Η νέα υποδομή της υπηρεσίας θα εξυπηρετήσει εκτός από τις υφιστάμενες κλήσεις και την νέα υπηρεσία WiFi στην οποία θα πιστοποιούνται όλοι οι Η/Υ οι οποίοι συνδέονται με ασύρματη τεχνολογία στο ΠΣΔ. Οι απαιτήσεις λειτουργίας είναι υπολογιστικοί πόροι με 1GB RAM, 20 GB για αποθηκευτικό χώρο του λειτουργικού συστήματος και 40 GB αποθηκευτικό χώρο ποιότητας βάσης δεδομένων.

Στην φάση της υπάρχουσας προμελέτης της υπηρεσίας WiFi εκτιμάται οτι η ελεγχόμενη πρόσβαση θα έχει πολύ μεγαλύτερες απαιτήσεις από οτι πριν δεδομένου οτι ο αριθμός των τερματικών σταθμών είναι πολύ μεγαλύτερος. Εάν υποθέσουμε οτι σε κάθε σχολείο θα υπάρχουν 3-5 ασύρματοι σταθμοί και κατά μέγιστο 10 σταθμοί με ρυθμό διπλασιασμού για κάθε χρόνο. Αυτό που μπορεί να γίνει για την ώρα είναι να γίνει μια διαστασιολόγηση ανάλογη με αυτή που υπάρχει στο Φοιτητικό DSL.

## 2.10 ΛΕΙΤΟΥΡΓΙΑ RADIUS ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΜΕ ΕΝΑ DATA CENTER

Η λειτουργία της υπηρεσίας σε περιβάλλον data center επιτρέπει την ύπαρξη κύριου και εφεδρικού εξυπηρετητή της υπηρεσίας χωρίς να απασχολείται ο διαχειριστής για την διαθεσιμότητα των φυσικών πόρων (κλιματισμός, παροχή ηλεκτρικής ενέργειας) με αποτέλεσμα να μειώνεται το λειτουργικό κόστος υψηλής διαθεσιμότητας της υπηρεσίας. Ειδικότερα για την υπηρεσία ΑΑΑ/ΠΕΚ ο κύριος και ο εφεδρικός εξυπηρετητής έχουν ανεξάρτητες διαδικασίες για την εξυπηρέτηση του Radius αλλά μοιράζονται την ίδια στοίβα λογισμικού για την βάση δεδομένων. Πρακτικά η ΒΔ τρέχει και στους δύο εξυπηρετητές σε τοπολογία master-slave. Ο ορισμός του master εξαρτάται από την ανταλλαγή heart-bit (όπως περιγράφτηκε προηγουμένως) μέσω απ' ευθείας ανεστραμμένου καλωδίου (Xconnect) μεταξύ των δύο εξυπηρετητών. Η ύπαρξη της άμεσης σύνδεσης συνίσταται για να αποφευχθεί η περίπτωση split-brain στην οποία είναι επιρρεπής η τεχνική heart-bit.




**Σχήμα 4 Τυπικό περιβάλλον υψηλής διαθεσιμότητας FreeRadius σε ένα data center**

Στο παραπάνω σχήμα έχει υιοθετηθεί η λειτουργία επιπλέον πρωτόκολλων τα οποία επιτυγχάνουν υψηλή διαθεσιμότητα σε διαφορετικά επίπεδα το καθένα. Το πρωτόκολλο LACP/LAGP (IEEE 802.1ag) είναι διαθέσιμο σε λειτουργικά Freebsd και επιτρέπει καταμερισμό φορτίου και αντοχή στις δικτυακές συνδέσεις μεταξύ τερματικού σταθμού και μεταγωγέα Ethernet. Στην παραπάνω περίπτωση χρησιμοποιείται στις συνδέσεις που έχουν ενεργοποιημένη την διαδικασία του radius στην κύρια και εφεδρική σύνδεση και προαιρετικά μεταξύ της κύριας και εφεδρικής ανεστραμένης σύνδεσης.

Η ενεργοποίηση του πρωτοκόλλου VRPP/CARP επιτρέπει την χρήση μιας δυναμικής διεύθυνσης μεταξύ των δύο σταθμών. Ορίζεται ένα σταθμός σαν master ο οποίος έχει στην κατοχή του την δυναμική διεύθυνση και ο εφεδρικός ο οποίος την ανακτά σε περίπτωση βλάβης. (Το υποδίκτυο της δυναμικής διεύθυνσης είναι το ίδιο με το δίκτυο της συνάρθροισης (δηλ. το δίκτυο που παράγεται από το LACP)). Με αυτό τον τρόπο για τον εξωτερικό κόσμο δλδ. τους radius clients υπάρχει μια δ/ση εξυπηρετητή. Εάν είναι επιθυμητή υψηλότερη διαθεσιμότητα (node-protection) αναφορικά με τις διπλές φυσικές οδεύσεις των εξυπηρετητών προτείνεται η χρήση Multi-chassis-LACP)

Εναλλακτικά εάν η υποδομή του Datacenter υποστηρίζει μεταγωγείς επιπέδου 7 είναι εφικτή η ενσωμάτωση της λειτουργίας SLB (service load balancing) είτε στο foundry - brocade

(http://www.brocade.com/support/Product_Manuals/ServerIron_SLBGuide/health.pdf) switch

είτε στο Cisco switch ( http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxf7.html#wp2435940) για την παροχή υψηλής διαθεσιμότητα στην διαδικασία radius.

Οι γενικές οδηγίες για service load balancing και για τους δύο κατασκευαστές είναι οτι συγκροτείτειται μια ομάδα από real servers οι οποίοι αποτελούν την φάρμα. Στην συνέχεια συγκροτείται ένας virtual server ο οποίος (ο οποίος λειτουργεί εντός του Layer 7 switch) προωθεί τις κλήσεις/αιτήσεις στην φάρμα με βάση κάποια πολιτική (τυχαία, round-robin, με βάρη κλπ) προώθηση. Ο τρόπος με τον οποίο καθορίζονται η διαθεσιμότητα των πραγματικών εξυπηρετητών μέσω του ιδεατού είναι με την συγκρότηση health-checks ή probes ανάλογα με τον κατασκευαστή. Στην περίπτωση της cisco τα probes τα οποία ελέγχουν την διαθεσιμότητα της υπηρεσίας με χρήση udp ή icmp packet. Στην περίπτωση του server-iron ορίζεται μια κλήση (με χρήση user-name κάποιο τυχαίο password και του σωστού radius-key) για έλεγχο της διαθεσιμότητας της υπηρεσίας με χρήση του πρωτοκόλλου radius. Σε περίπτωση απάντησης συμπεραίνεται η λειτουργία του πρωτοκόλλου του πραγματικού εξυπηρετητή. Σε περίπτωση απάντησης με icmp port unreachable προκύπτει οτι δεν εξυπηρετείται το εν λόγο πρωτόκολλο.

### 2.10.1 Λειτουργία σε περιβάλλον με εφεδρικό data center

Το ΠΣΔ έχει προδιαγράψει την λειτουργία δύο data center ένα εκ των οποίων θα βρίσκεται στην Κωλλέτη και το δεύτερο στο υπολογιστικό κέντρο του ΕΑΙΤΥ στην Πάτρα ή στο Υπ. Παιδείας. Ανεξάρτητα της φυσικής τοποθεσία θα παρουσιάσουμε ένα υποθετικό σενάριο λειτουργίας το οποίο μένει να επιβεβαιωθεί όταν λειτουργήσουν τα δύο data center.

Η βασική υπόθεση είναι οτι οι radius clients έχουν ρυθμισμένους δύο radius servers για την αποστολή αιτήσεων/κλήσεων και θα ήταν επιθυμητό αυτή η ρύθμιση να κρατηθεί σε αυτό το επίπεδο. Στο νέο σενάριο κάθε μία διεύθυνση θα παραπέμπει σε ένα virtual server σε ξεχωριστό data center. Σε αυτή την περίπτωση θα χρειαστεί να μειωθεί ο χρόνος

μετάπτωσης των clients από τον κύριο στον εφεδρικό σε τιμή που να καθορίζεται από το χρόνο μετάπτωσης της δρομολόγησης από το κεντρικό στο εφεδρικό εξυπηρετητή.

Πρέπει να διευκρινιστεί οτι η λειτουργία της υπηρεσίας radius στον εφεδρικό datacenter δεν είναι απόλυτα συμμετρική αφού οι βάσεις δεν είναι απόλυτα συγχρονισμένες. Δεν έχει διευκρινιστεί ακόμα πως θα επιτευχθεί ο συγχρονισμός σε σχεδόν πραγματικό χρόνο και τα απαιτούμενα αγαθά που συνεπάγεται μια τέτοια απαίτηση. Στην παρούσα φάση ο σχεδιασμός για το εφεδρικό site παρέχει την δυνατότητα για ταυτοποίηση (radius authentication) χωρίς έλεγχο ζωντανής διπλής εγγραφής (double login detection) και κλασματική ενημέρωση των στοιχείων χρήσης (accounting data).

### 2.10.2 Περιγραφή των ενεργών RADIUS profile στο ΠΣΔ - Authorization

Η λειτουργία της ΑΑΑ/ΠΕΚ στο ΠΣΔ αφορά κατά βάση το περιβάλλον συγκρότησης δηλαδή το σύνολο των λειτουργικών χαρακτηριστικών των συνδέσεων με χρήση προφίλ που αποθηκεύονται στο αποθετήριο καταλόγου. Τα χαρακτηριστικά του προφίλ των χρηστών ρυθμίζονται με χρήση πρωτυποποιημένου λεξικού Radius. Ένα τέτοιο attribute για παράδειγμα είναι το dialupaccess, το οποίο εάν είναι FALSE ο χρήστης δεν επιτρέπεται να χρησιμοποιήσει την υπηρεσία.

Στην υποδομή καταλόγου τα profile των χρηστών περιγράφονται από την δομή objectclass. Το objectclass επίσης περιέχει attributes, τα οποία είναι είτε check items τα οποία ελέγχονται κατά το authorization του χρήστη, είτε reply items με παραμέτρους σύνδεσης που επιστρέφονται στον access server εάν το authentication επιτύχει (π.χ., session-timeout, idle-timeout). Για το authorization των χρηστών χρησιμοποιείται το objectclass **radiusprofile**, το οποίο παρέχει τα διάφορα attributes που σχετίζονται με το authorization.

Ο αναλυτικός ορισμός του radiusprofile παρουσιάζεται παρακάτω:

| **LDAP Attribute** | **Περιγραφή** | **Τύπος (check/reply)** |
|---|---|---|

| | | |
|---|---|---|
| radiusSimultaneousUse | Ορίζει τον μέγιστό αριθμό από ταυτόχρονες συνδέσεις (όχι multilink) που μπορούν να γίνουν από ένα συγκεκριμένο χρήστη. Συνήθως λαμβάνει την τιμή 1 προκειμένου να αποκλείονται περιπτώσεις double login | check |
| radiusAuthType | Ορίζει τον τύπο του authentication που θα εκτελεστεί από τον radius server αλλά δε χρησιμοποιείται πλέον στην πράξη ιδιαίτερα. | check |
| radiusExpiration | Ορίζει την ημερομηνία κατά την οποία θα λήξει η πρόσβαση του χρήστη (είναι της μορφής 20 May 2002) | check |
| dialupaccess | Ορίζει το κατα πόσο ο χρήστης έχει πρόσβαση στην υπηρεσία dialup. Αν έχει την τιμή FALSE τότε η πρόσβαση του χρήστη στην υπηρεσία δεν επιτρέπεται. Αν έχει οποιαδήποτε άλλη τιμή τότε η πρόσβαση επιτρέπεται | check |
| radiusHint | | check |
| radiusLoginTime | Ορίζει το χρονικό διάστημα (σε UUCP format) κατά το οποίο μπορεί να συνδεθεί ο αντίστοιχος χρήστης στην υπηρεσία | check |
| radiusarapfeatures | | |
| radiusarapsecurity | | |

| | | |
|---|---|---|
| radiusarapzoneaccess | | |
| radiuscallbackid | | |
| radiuscallbacknumber | | |
| radiuscalledstationid | Το τηλέφωνο στο οποίο καλεί ο χρήστης (DNIS) | check |
| radiuscallingstationid | Το τηλέφωνο από το οποίο γίνεται η κλήση (CLID) | check |
| radiusclass | | |
| radiusfilterid | | |
| radiusframedappletalklink | | |
| radiusframedappletalknetwork | | |
| radiusframedappletalkzone | | |
| radiusframedcompression | Το πρωτόκολλο συμπίεσης το οποίο θα εφαρμοστεί στη σύνδεση. Το πλέον διαδεδομένο και συνηθισμένο πρτόκολλο είναι το Van-Jacobson-TCP-IP | reply |
| radiusframedipaddress | Η διεύθυνση IP η οποία θα αποδωθεί στον χρήστη | reply |
| radiusframedipnetmask | Η IP netmask που θα αποδωθεί στο χρήστη | reply |

| | | |
|---|---|---|
| radiusframedipxnetwork | | reply |
| radiusframedmtu | Το MTU της σύνδεσης | reply |
| radiusframedprotocol | Το πρωτόκολλο της σύνδεσης (συνήθως είναι PPP) | reply |
| radiusframedroute | | reply |
| radiusframedrouting | | reply |
| radiusidletimeout | Ο μέγιστος χρόνος για τον οποίο επιτρέπεται η σύνδεση του χρήστη να μείνει ανενεργή (idle) | reply |
| radiusloginiphost | | reply |
| radiusloginlatgroup | | reply |
| radiusloginlatnode | | reply |
| radiusloginlatport | | reply |
| radiusloginlatservice | | reply |
| radiusloginservice | | reply |
| radiuslogintcpport | | reply |
| radiuspasswordretry | | reply |
| radiusportlimit | Ο μέγιστος αριθμός απο διαθέσιμα κανάλια | reply |

| | | |
|---|---|---|
| | στον access server τα οποία μπορεί να ανοίξει ταυτόχρονα ο χρήστης σε μία mutlink σύνδεση | |
| radiusprompt | | reply |
| radiusservicetype | Ο τύπος της σύνδεσης του χρήστη. Συνηθισμένες τιμές είναι Framed-User εφόσον η σύνδεση είναι τύπου Framed, Outbound-User για εξερχόμενες (από την πλευρά του access server) συνδέσεις και Login-User για συνδέσεις telnet | reply |
| radiussessiontimeout | Ο μέγιστος χρόνος που μπορεί να διαρκέσει η σύνδεση | reply |
| radiusterminationaction | | reply |
| radiustunnelassignmentid | | reply |
| radiustunnelclientendpoint | | reply |
| radiustunnelmediumtype | | reply |
| radiustunnelpassword | | reply |
| radiustunnelpreference | | reply |
| radiustunnelprivategroupid | | reply |
| radiustunnelserverendpoint | | reply |

| | | |
|---|---|---|
| radiustunneltype | | reply |
| radiusvsa | | reply |
| radiuscheckitem | Γενικής φύσης attribute το οποίο μπορεί να χρησιμοποιηθεί για την αποθήκευση οποιουδήποτε check item. Η τιμή του πρέπει να είναι της μορφής <RADIUS attribute> <operator> <value> (πχ NAS-IP-Address := "194.63.239.238") | check |
| radiusreplyitem | Γενικής φύσης attribute το οποίο μπορεί να χρησιμοποιηθεί για την αποθήκευση οποιουδήποτε reply item. Η τιμή του πρέπει να είναι της μορφής <RADIUS attribute> <operator> <value> (πχ Cisco-AVPair := "lcp:send-secret=XXXXXX") | reply |

**Πίνακας 1 Αναλυτικός ορισμός του radiusprofile**

Οι ρυθμίσεις που αφορούν τον κάθε χρήστη ορίζονται με τον συνδυασμό τεσσάρων προφίλ, του **Default-Profile, User-Profile**, **Regular-Profile** και του **προσωπικού προφίλ** του κάθε χρήστη με αύξουσα σειρά προτεραιότητας.

Το Default-Profile που ορίζεται στο αρχείο διαμόρφωσης του radius server και το οποίο (το default-profile entry) περιέχει attributes που προσδιορίζουν τις προκαθορισμένες (default) ρυθμίσεις των χρηστών. Το User-Profile συνήθως ορίζεται μέσα στο αρχείο users με βάση ελέγχους στα radius attributes που περιέχονται στα πακέτα τύπου Access-Request. Το αρχείο ορίζει το DN ενός entry το οποίο περιέχει ρυθμίσεις για μία συγκεκριμένη κατηγορία χρηστών. Σε αυτή την περίπτωση δεν λαμβάνεται υπόψη το Default-Profile. Κατά αυτό τον τρόπο μπορεί να επιλέγεται ένα γενικό profile για τους χρήστες αναλόγως με τον τύπο της αιτούμενης σύνδεσης ή με βάση άλλα κριτήρια τα οποία μπορεί να ορίσει ο διαχειριστής της

υπηρεσίας. Το Regular-Profile είναι ένα attribute που περιέχεται στα entries των χρηστών και το οποίο δείχνει σε κάποιο DN με ρυθμίσεις που αφορούν την ομάδα χρηστών στην οποία ανήκει ο χρήστης. Τέλος, το entry του κάθε χρήστη μπορεί να περιέχει attributes που διαφοροποιούν το προφίλ του συγκεκριμένου χρήστη από τις default ρυθμίσεις ή τις ρυθμίσεις ομάδας.

Η συνήθης πρακτική για το ΠΣΔ είναι η χρήση της υποδομής ΑΑΑ/ΠΕΚ για συνδέσεις τύπου PPP από χρήστες ή δρομολογητές το οποίο μεταφράζεται σε συνδέσεις τύπου Framed-User αναφορικά με το συντακτικό Radius. Ως εκ τούτου εφαρμόζεται πάντα το ακόλουθο Regular Profile (default-dialup):

| | |
|---|---|
| radiusFramedIPNetmask: 255.255.255.255 | Ελεύθερη απόδοση δ/νσης |
| radiusFramedCompression: Van-Jacobson-TCP-IP | Επιλογή για συμπίεση δεδομένων |
| radiusFramedProtocol: PPP | Χρήση πρωτοκόλλου PPP |
| radiusServiceType: Framed-User | Χρήση πρωτ/λου Framed |
| radiusFramedMTU: 1500 | MTU =1500 bytes |

Επιπλέον η υπηρεσία υποστηρίζει τις παρακάτω βασικές κατηγορίες χρηστών:

**Dialup User Profiles:** Για κάθε σχολική μονάδα (και στο μέλλον για ένα μεγάλο μέρος της εκπαιδευτικής κοινότητας) παραχωρείται κανονικός dialup λογαριασμός. Για το λογαριασμό αυτό ισχύουν τα εξής:

- **PAP authentication:** Δεν επιτρέπεται CHAP authentication για τους dialup λογαριασμούς παρά μόνο PAP
- **Παραχώρηση δυναμικής IP Address:** Σε όλους τους dialup κωδικούς παραχωρείται δυναμική διεύθυνση IP
- **Caller-Id Authentication:** Στο άμεσο μέλλον θα ενεργοποιηθεί callerid authentication και για τους dialup κωδικούς των μονάδων. Για τους προσωπικούς λογαριασμούς των εκπαιδευτικών κάτι τέτοιο δε θα ισχύει.

- **Double login detection:** Για όλους τους dialup λογαριασμούς (εφόσον δεν έχει ενργοποιηθεί callerid authentication) πραγματοποιείται double login detection.
- **default-user-dialup Regular Profile:** Το regular profile αυτό παρατίθεται παρακάτω:

  *radiusPortLimit: 2*

  *npSessionsAllowed: 1*

  *radiusIdleTimeout: 600*

  *radiusReplyItem: Cisco-AVPair := "ip:addr-pool=dialin_pool"*

**Router Profiles:** Πρόκειται για εγγραφές που αντιστοιχούν στους routers με τους οποίους συνδέονται τα σχολικά αργαστήρια στο ΠΣΔ. Για κάθε τέτοιο router δημιουργείται μία εγγραφή μορφής r-<router-name>. Για τους λογαριασμούς αυτούς ισχύουν τα εξής:

- **Caller-Id Authentication:** Για κάθε router αντιστοιχεί ένας αριθμός από τον οποίο επιτρέπεται να πραγματοποιηθεί η κλήση προς το ΠΣΔ. Επιπλέον στις εγγραφές προστίθονται και επιπλέον Allowed Caller-Id το 8962488888 προκειμένου να επιτρέπονται οι εξερχόμενες κλήσεις προς τους δρομολογητές των σχολείων.
- **Ελεύθερη χρήση δύο καναλιών ISDN**
- **PAP ή CHAP authentication:** Στις περιπτώσεις των router profiles επιτρέπεται είτε η σύνδεση μέσω CHAP (υλοποιείται με τη χρήση του chappassword ldap attribute) είτε μέσω PAP (υλοποιείται με LDAP BIND).
- **default-router-edunet Regular Profile:** Το profile παρατίθεται παρακάτω:

  *radiusIdleTimeout: 250*

  *radiusSessionTimeout: 14400*

  *radiusFramedIPAddress: 255.255.255.254*

*chappassword: educhap1603*

*radiusPortLimit: 2*

*radiusReplyItem: Cisco-AVPair := "lcp:send-secret=<SECRET>"*

**Outbound Route Profiles:** Για την υλοποίηση του Large Scale Dialout απαιτείται η ύπαρξη ενός outbound route profile για κάθε δρομολογητή. Για τους λογαριασμούς αυτούς ισχύουν τα εξής:

- **Συνδέσεις μόνο τύπου Outbound-User** με PAP authentication (password cisco).
- **Caller-Id Authentication:** Για κάθε router επιτρέπονται συνδέσεις μόνο με callerid "Dial out" το callerid το οποίο προσθέτει αυτόματα ο κεντρικός δρομολογητής όταν κάνει αίτηση για το outbound profile.
- **Ειδικά attributes:** Σε κάθε outbound profile προστίθενται δύο επιπλέον attributes. Το ένα περιέχει το τηλέφωνο στο οποίο θα πρέπει να γίνει η κλήση (το τηλέφωνο με άλλα λόγια του δρομολογητή του σχολείου) και το άλλο την IP η οποία θα παραχωρηθεί στο τοπικό interface του access server μετά την επιτυχή σύνδεση. Τα attributes αυτά έχουν τη μορφή που φαίνεται παρακάτω:

  *radiusReplyItem: Cisco-AVPair := "outbound:addr*255.255.255.254"*

  *radiusReplyItem: Cisco-AVPair := "outbound:dial-number=2xxxxxx"*
- **default-router-edunet-dialup Regular Profile:** Το regular profile αυτό παρατίθεται παρακάτω:

  *radiusCallingStationId: "Dial out"*

  *radiusReplyItem: Cisco-AVPair := "outbound:send-secret=educhap1603"*

**LSD Profiles:** Για κάθε δρομολογητή διατηρούνται LSD profiles όπως αυτά περιγράφηκαν στο τμήμα του Large Scale Dialout. Για τους λογαριασμούς αυτούς ισχύουν τα εξής:

- **Συνδέσεις μόνο τύπου Outbound-User** με PAP authentication (password cisco).
- **Caller-Id Authentication:** Επιτρέπονται μόνο Access-Request που περιέχουν callerid "Dial out". Αυτό προστίθεται αυτόματα από τον κεντρικό δρομολογητή όταν κάνει την αντίστοιχη αίτηση.

# 3. ΠΕΡΙΦΕΡΕΙΑΚΕΣ ΕΦΑΡΜΟΓΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΣΤΑΤΙΣΤΙΚΩΝ.

## 3.1 DIALUPADMIN

Ενώ η υποδομή ΑΑΑ/ΠΕΚ παρέχει τις απαραίτητες λειτουργικότητες για ταυτοποίηση και έλεγχο πρόσβασης των χρηστών και έλεγχο των δεδομένων καταγραφής των χρηστών. Η διαχείριση των εγγραφών των χρηστών γίνεται από την εφαρμογή διαχείριση χρηστών (ΠΔΧ).

## 3.2 ΣΤΑΤΙΣΤΙΚΑ ΧΡΗΣΗΣ

Στα πλαίσια της παροχής στατιστικών από την υποδομή ΑΑΑ/ΠΕΚ προσφέρονται τα ακόλουθα στοιχεία:

- Ο πίνακας totacct που περιέχει ημερήσια συγκεντρωτικά στατιστικά ανά χρήστη. Για την εξαγωγή των στατιστικών υπεύθυνο είναι το εκτελέσιμο αρχείο tot_acct ( περιέχεται στον κατάλογο εκτελέσιμων του dialup_admin το οποίο εκτελείται καθημερινά μέσω cron και αναλαμβάνει την εξαγωγή της αντίστοιχης πληροφορία από τον πίνακα radacct τον προσθέσει στον πίνακα totacct. Η δομή του πίνακα totacct είναι όπως φαίνεται παρακάτω:

| **Πεδίο** | **Τύπος** | **Περιγραφή** |
|---|---|---|
| TotAcctId | bigint(21) | Το ID του κάθε row |
| UserName | varchar(64) | Το username του κάθε χρήστη |
| AcctDate | date | Η ημέρα στην οποία αναφέρεται το row |
| ConnNum | bigint(12) | Ο αριθμός των συνδέσεων που πραγματοποιήθηκαν από το συγκεκριμένο χρήστη |
| ConnTotDuration | bigint(12) | Η συνολική διάρκεια των συνδέσεων |

| | | |
|---|---|---|
| ConnMaxDuration | bigint(12) | Η μέγιστη διάρκεια των συνδέσεων του συγκεκριμένου χρήστη |
| ConnMinDuration | bigint(12) | Η μικρότερη διάρκεια των συνδέσεων |
| InputOctets | bigint(12) | Ο αριθμός των bytes που εισήλθαν στον access server από την πλευρά του χρήστη (upload) |
| OutputOctets | bigint(12) | Ο αριθμός των bytes που εξήλθαν από τον access server προς τον χρήστη (download) |
| NASIPAddress | varchar(15) | Η IP διεύθυνση του access server στον οποίο συνδέθηκε ο χρήστης. |

**Πίνακας 2 Totacct: περιέχει ημερήσια συγκεντρωτικά στατιστικά ανά χρήστη**

- Ο πίνακας mtotacct που διατηρεί τα μηνιαία συγκεντρωτικά ανά χρήστη με δομή ανάλογη με του totacct. Η παραγωγή στοιχείων γίνεται από το εκτελέσιμο monthly_tot_stats ( το οποίο εκτελείται κάθε μέρα μέσω cron. Η δομή του πίνακα mtotacct είναι όπως φαίνεται παρακάτω:

| **Πεδίο** | **Τύπος** | **Περιγραφή** |
|---|---|---|
| MtotAcctId | bigint(21) | Το ID του κάθε row |
| UserName | varchar(64) | Το username του κάθε χρήστη |
| AcctDate | date | Η πρώτη ημέρα του μήνα στον οποίο αναφέρεται το row |
| ConnNum | bigint(12) | Ο αριθμός των συνδέσεων που πραγματοποιήθηκαν από το συγκεκριμένο χρήστη |

| | | |
|---|---|---|
| ConnTotDuration | bigint(12) | Η συνολική διάρκεια των συνδέσεων |
| ConnMaxDuration | bigint(12) | Η μέγιστη διάρκεια των συνδέσεων του συγκεκριμένου χρήστη |
| ConnMinDuration | bigint(12) | Η μικρότερη διάρκεια των συνδέσεων |
| InputOctets | bigint(12) | Ο αριθμός των bytes που εισήλθαν στον access server από την πλευρά του χρήστη (upload) |
| OutputOctets | bigint(12) | Ο αριθμός των bytes που εξήλθαν από τον access server προς τον χρήστη (download) |
| NASIPAddress | varchar(15) | Η IP διεύθυνση του access server στον οποίο συνδέθηκε ο χρήστης. |

**Πίνακας 3 Mtotacct: διατηρεί τα μηνιαία συγκεντρωτικά ανά χρήστη**

- User Reports: παράγει στοιχεία χρήσης ανά κόμβο πρόσβασης (access server) με τον αριθμό των συνδέσεων που πραγματοποίησε ο κάθε χρήστης καθώς και τον αριθμό των τυχών αποτυχημένων συνδέσεων (bad logins). (Εκτελείται καθημερινά μέσω cron.) Η μορφή του είναι όπως παρακάτω:

```
Kombos: r.att.sch.gr


Data From Date: 2003-03-10 00:00:00

Data To   Date: 2003-03-11 00:00:00

*****************************
```

```
---------------------------------------------------------------------
Connections     Hours   MBytes  UserName
---------------------------------------------------------------------
*****************************
299             23.9  8.5   r-1tee-aigal
195             19.4  7.1   r-4lyk-athin
189             18.3  7.1   r-9lyk-perist
176             16.1  7.9   r-1lyk-ellin
175             15.2  7.5   r-5sek-a-peiraia

1               0.1   0.4     9teepeir
1               0.1   0.1   nkokkin
--
---------------------------------------------------------------------
                TOTAL STATISTICS
Connections    Hours  MBytes
-------------------------------------------------------------
8304            1537.4  4281.5

-------------------------------------------------------------
Failed Logins  UserName
-------------------------------------------------------------
89          r-3gym-kerats
```

60 r-1sek-v-ath

39 r-2sek-d-ath

25 r-1tee-asprop

1 lykglner

1 2gymtavr

1 5teechal

--

---

TOTAL STATISTICS

Failed Logins

---

571

# 4. ΥΠΟΔΟΜΗ ΑΑΑ/ΠΕΚ ΓΙΑ ΑΣΥΡΜΑΤΗ ΠΡΟΣΒΑΣΗ (WIFI)

Στο ΠΣΔ έχει αποφασιστεί να επιτραπεί η πρόσβαση στο διαδίκτυο σε σχολικές μονάδες μέσω ασύρματης τεχνολογίας WiFi. Παρ όλο που τα ειδικότερα τεχνικά και πολιτικά θέματα της ασύρματης πρόσβασης θα παρουσιαστούν σε επιμέρους παραδοτέα θα αναφερθούν τα ειδικότερα θέματα ελέγχου πρόσβασης. Σε γενικές αρχές τα σημεία ελέγχου πρόσβασης στα σχολεία θα αποτελείται από: α) ένα portal το οποίο δέχεται τα στοιχεία ταυτοποίησης (username και password) του κάθε μαθητή/χρήστη και β) ένα υποσύστημα έλεγχου ταυτοποίησης το οποίο βασίζεται στα πρότυπα IEEE [IEEE] 802.1X [IEEE-802.1X]. Εν γένη και οι δύο παραπάνω μέθοδοι είναι ευρέως διαδεδομένοι στο διαδίκτυο και δεν απαιτούν κάποια νέα τεχνολογία προς ανάπτυξη για το σχολικό δίκτυο. Το ιδιαίτερο χαρακτηριστικό του ελέγχου πρόσβασης για τα ασύρματα δίκτυα του σχολικού δικτύου είναι ο μεγάλος αριθμός των σημείων πρόσβασης με συνέπεια μεγάλο αριθμό ταυτοποιήσεων στην υποδομή ΑΑΑ/ΠΕΚ. Είναι εύκολο να φανταστούμε οτι σε κάθε σχολείο μπορεί να υπάρχει κατά μέσο όρο ένα σημείο ασύρματης πρόσβασης από το οποίο κάθε μέρα θα ταυτοποιούνται ένας σημαντικός αριθμός ταυτοποιήσεων με αποτέλεσμα να προκύπτει η σημαντικά υψηλότερη απαίτηση για αριθμό ταυτοποιήσεων που να προσεγγίσει τουλάχιστον διπλασιασμό ή και τετραπλασιασμό του φορτίου.

Δεδομένου ότι το πρωτόκολλο radius ρυθμίζεται να χρησιμοποιεί μια συνθηματική λέξη σε κάθε μεταφορά πληροφορίας προκύπτει ότι η κωδική λέξη θα πρέπει χρησιμοποιείται από ένα μεγάλο αριθμό από τερματικά σημεία ταυτοποίησης (~ 15.000) γεγονός που αποδυναμώνει την ασφάλεια μεταφορά δεδομένων. Προτείνεται είτε α) να δημιουργηθούν ασφαλής φράσεις ανά περιοχή ή/και β) να δημιουργηθεί μια επιπλέον υποδομή μεταφοράς δεδομένων τύπου radius με χρήση πληρεξούσιου (proxy) radius σε συνδυασμό με χρήση Extensible Authentication Protocol (EAP)[EAP] και 802.1X για ασφαλή πρόσβαση.

Εν γένη η χρήση proxy δεν είναι κάτι ριζοσπαστικό στο ΠΣΔ αφού έχει χρησιμοποιηθεί και στην υπηρεσία καταλόγου (LDAP) όταν απαιτείται η επικοινωνία της υπηρεσία με τους τελικούς χρήστες σε αντιδιαστολή με την χρήση της υπηρεσίας από κεντρικούς server.

Ο πληρεξούσιος radius δημιουργεί ένα πρόσθετο τοίχος ανάσχεσης των κλήσεων radius προς την κρίσιμη κεντρική υποδομή ετσι ώστε τυχόν επίθεση DDoS (Distributed Denial of

Service) να μπορέσει να ανασχεθεί στους radius proxy. Με αυτό τον τρόπο μπορεί να δημιουργηθούν κατάλληλες λίστες προστασίας (access lists -ACL) για την προστασία της κεντρική υποδομής, διαφορετικά η υποδομή θα ήταν ουσιαστικά δίχως προστασία στον τυχαίο κακόβουλο τελικό χρήστη. Σχηματικά αυτό φαίνεται ως εξής.

## 4.1 PROXY RADIUS

Το ενδιαφέρον χαρακτηριστικό της λειτουργίας του Proxy είναι ότι εκμεταλλεύεται τον ορισμό realm (χώρων περιγραφής π.χ. user@wireless.sch.gr, user@sch.gr) για χρήση διαφορετικού μηχανισμού ταυτοποίησης. Αυτό μπορεί να κριθεί απαραίτητο εάν χρησιμοποιηθούν διαφορετικοί μηχανισμοί αποθήκευσης των διαπιστευτηρίων κατά την χρήση Captive portal από ότι στο 802.1X.

Επιπλέον, η χρήση του Extensible Authentication Protocol (EAP) που περιγράφεται στην συνέχεια κάνει εφικτή την ασφαλή ταυτοποίηση των τερματικών ασύρματων σημείων (H/Y) στην υποδομή ΑΑΑ/ΠΕΚ.

## 4.2 EAP ΠΑΝΩ ΑΠΟ RADIUS

Το πρωτόκολλο Extensible Authentication Protocol (EAP) (αρχικά RFC 2284, και πλέον RFC 3748) αναπτύχθηκε αρχικά ως επέκταση για το PPP για την ανάπτυξη και μηχανισμών μηχανισμών ταυτοποίησης. Με το PPP οι μηχανισμοί ταυτοποίησης (PAP [PAP], CHAP [CHAP], MS-CHAP [MSCHAP], MS-CHAPv2 [MSCHAP2]) επιλέγονται από τις τερματικές συσκευές και συγκεντρωτή δικτύου (Network Access Server) από κοινού. Ως εκ τούτου όταν χρειάζεται να εισαχθεί ένας νέος μηχανισμός αυτός πρέπει να υλοποιηθεί και στους δύο οντότητες. Με το EAP αντίθετα οι μηχανισμοί ταυτοποίησης υλοποιούνται στην τερματική συσκευή και στο Radius Server. Ο φυγοκεντρωτής δικτύου κατά την φάση ταυτοποίησης δεν κάνει κανένα έλεγχο ταυτοποίησης αλλά ενθυλακώνει τα μηνύματα σε νέου τύπου πακέτα που λέγονται Radius EAP. Από άποψη αρχιτεκτονικής οι μέθοδοι ταυτοποίησης υλοποιούνται στα τερματικά σημεία και στον Radius server με τον μηχανισμό των plug-in modules.

Ο μηχανισμός του EAP προτείνεται να χρησιμοποιηθεί για την ταυτοποίηση ασύρματων συνδέσεων (IEEE 802.11b/g/n) σύμφωνα με το πρότυπο 802.1X. Με αυτό τον τρόπο δεν υπάρχουν περιορισμοί που τίθενται από τους ασύρματους σταθμούς (π.χ. laptops κλπ) αφού τα Access Points (AP) δεν βάζουν κανένα περιορισμό για την ταυτοποίηση.

Στην παρούσα φάση ο FreeRadius υποστηρίζει τους παρακάτω μηχανισμούς ενθυλάκωσης

- EAP-MD5 [EAPMD]
- EAP-TLS (Transport Layer Security) [EAPTL]
- EAP-PEAP (Protected EAP)
- EAP-TTLS (Tunneled Transport Layer Security) [TTLS]
- EAP-TTLS (Tunneled TLS)

Η μέθοδος EAP-MD5 δεν προτείνεται εξαιτίας προβλημάτων ασφάλειας του MD5. Η μέθοδος EAP-TLS χρησιμοποιείται κυρίως ταυτοποίηση των σημείων επικοινωνίας με certificates. Η μέθοδος EAP-PEAP χρησιμοποιείται για τερματικά σημεία (π.χ. windows clients) στα οποία η μέθοδος αποθήκευση του Password είναι MS-chapv2 το οποίο χρησιμοποιείται κατά βάση από Directory servers της MS. Η μέθοδος EAP-PEAP προσφέρει κρυπτογράφηση στα μηνύματα EAP που ανταλλάσσονται. Η μέθοδος EAP-TTLS παρέχει τα ίδια χαρακτηριστικά ασφαλείας αλλά αντί να μεταφέρει μηνύματα EAP μεταφέρει μηνύματα Radius EAP. Το πλεονέκτημα αυτής της επιλογής είναι με αυτό τον τρόπο εντός του καναλιού TLS μπορεί να οριστεί η μέθοδος ταυτοποίησης ανάλογα με τα μηνύματα radius.

Στο ΠΣΔ χρησιμοποιείται συνάρτηση κατακερματισμού (one way secure hash) μονής κατεύθυνσης για την αποθήκευση του password γεγονός που επιτρέπει την χρήση EAP-TTLS+PAP. Προτείνεται παράλληλα να χρησιμοποιηθεί και attribute αποθήκευσης του NT-Password (NTLM hash) για την παροχή δυνατότητας χρήσης του EAP-PEAP. Τέτοιο attribute υπάρχει ήδη διαθέσιμο στην κλάση radisprofile,το radiusntpassword.

Οι γενικές οδηγίες για την ενεργοποίηση του EAP στον Radius είναι:

1. εγκατάσταση βιβλιοθηκών SSL (π.χ. openssl) στην τελευταία σταθερή έκδοση

   a. (Προαιρετικά) Δημιουργία και εγκατάσταση ιδιωτικού/ δημόσιου κλειδιού και Certificate Authority εάν δεν υπάρχει ήδη.

   *mkdir /etc/ssl*

   *mkdir private*

   *mkdir newcerts*

   *touch index.txt*

   *echo '01' > serial*

   *Αλλαγή εντός του αρχείο /etc/pki/tls/openssl.cnf* για το dir σε dir=/etc/ssl

   *openssl req -new -x509 -extensions v3_ca -keyout private/cakey.pem -out cacert.pem -days 3650*

(Στην ερώτηση για pass phrase διαλέγουμε ένα αυθαίρετο. π.χ. *let-sch-in*

2. Δημιουργία Server certificate

   b. Δημιουργία αίτησης πιστοποιητικού server

   *openssl req -new -nodes -keyout server_key.pem -out server_req.pem -days 730*

   c. Δημιουργία επεκτάσεων πιστοποιητικού για χρήση ταυτοποίησης στο φάκελο /etc/ssl

   *# cat xpextensions*

   *[ xpclient_ext]*

   *extendedKeyUsage = 1.3.6.1.5.5.7.3.2*

   *[ xpserver_ext ]*

   *extendedKeyUsage = 1.3.6.1.5.5.7.3.1*

   d. Υπογραφή αίτησης και δημιουργία πιστοποιητικού

   *openssl ca -policy policy_anything -out server_cert.pem -extensions xpserver_ext -extfile /etc/ssl/xpextensions -infiles /etc/ssl/server_req.pem*

   e. Συμπτυξη πιστοποιητικού και κλειδιου σε ένα αρχείο

   *cat server_key.pem server_cert.pem > server_keycert.pem*

3. Δημιουργία client Sertificate

   f. Δημιουργία αίτησης πιστοποιητικού client (στο κατάλογο /etc/ssl) με pass phrase [π.χ. sch-wifi-client]

   *openssl req -new -nodes -keyout client_key.pem -out client_req.pem -days 730*

g. Δημιουργία επεκτάσεων πιστοποιητικού για χρήση ταυτοποίησης στο φάκελο /etc/ssl

*# cat xpextensions*

*[ xpclient_ext]*

*extendedKeyUsage = 1.3.6.1.5.5.7.3.2*

*[ xpserver_ext ]*

*extendedKeyUsage = 1.3.6.1.5.5.7.3.1*

h. Υπογραφή αίτησης και δημιουργία πιστοποιητικού (με χρήση pass phrase της CA)

*openssl ca -policy policy_anything -out client_cert.pem -extensions xpclient_ext -extfile /etc/ssl/xpextensions -infiles /etc/ssl/client_req.pem*

i. Δημιουργία του πιστοποιητικού client σε format (P12) κατάλληλο για XP:

*openssl pkcs12 -export -in client_cert.pem -inkey client_key.pem -out client_cert.p12 -clcerts*

Σε αυτή την φάση θα χρειστούν δύο μυστικές φράσεις ή μία που χρησιμοποιήθηκε στην αίτηση [δηλ. sch-wifi-client] και άλλη μία (π.χ. idontknow) που θα χρησιμοποιηθεί τον τελικό χρήστη οταν θα χρειαστεί να το εισάγει στον Η/Υ του.

j. Εξαγωγή του certificate της αρχής (CA) σε κατάλληλο format (DER) για Η/Υ τύπου XP:

*openssl x509 -setalias "ciitwifi@ciit" -outform DER -in cacert.pem -out cacert.der*

k. Τα αρχεία 'client_cert.p12' και 'cacert.der' μπορούν να μεταφερούν σε ένα κατάλογο στα XP clients.

4. Διαγραφή και αντικατάσταση των πιστοποιητικών εγκατάστασης με αυτά που έχουν ήδη δημιουργηθεί

*rm -Rf /etc/raddb/demoCA*

*mkdir /etc/raddb/certs*

*cp /etc/ssl/cacert.pem /etc/raddb/certs/ -v*

*cp /etc/ssl/server_keycert.pem /etc/raddb/certs/ -v*

5. Δημιουργία στοιχείων DH (Diffie Hellman) εντός του /etc/ssl

*openssl dhparam -check -text -5 512 -out dh*

6. Αντιγραφή του αρχείου "dh" στο κατάλογο /etc/raddb/certs :

*cp /etc/ssl/dh /etc/raddb/certs -v*

7. Δημιουργία ψευτοσειράς για το TLS και αλλαγή κυριότητας

```
dd if=/dev/urandom of=random count=2
chown -R radiusd /etc/raddb/certs
```

8. Τροποποίηση του /etc/raddb/eap.conf :

(Σημ: "let-sch-in" είναι το private key password του server certificate.)

```
 eap                                                    {
default_eap_type                        =              ttls
timer_expire                            =              60
ignore_unknown_eap_types                =              no
cisco_accounting_username_bug           =              no
md5                                                    {
}
leap                                                   {
}
gtc                                                    {
auth_type                               =              PAP
}
tls                                                    {
private_key_password                    =              let-sch-in
private_key_file                =       ${raddbdir}/certs/server_keycert.pem
certificate_file                =       ${raddbdir}/certs/server_keycert.pem
CA_file                         =       ${raddbdir}/certs/cacert.pem
dh_file                         =       ${raddbdir}/certs/dh
random_file                     =       ${raddbdir}/certs/random
}


ttls                                                   {
default_eap_type                        =              pap
use_tunneled_reply                      =              yes
}
peap                                                   {
default_eap_type                        =              mschapv2
}
mschapv2                                               {
}
}
```

9. Προσθήκη των radius client στο αρχείο /etc/raddb/clients.conf. Εν προκειμένω του Proxy radius:

Για τον proxy:

```
client 192.168.0.53 {
secret = <proxy secret phrase>
shortname = proxy
nastype = other
}
```

# 5. ΠΑΡΟΥΣΑ ΚΑΤΑΣΤΑΣΗ ΛΕΙΤΟΥΡΓΙΑΣ ΤΗΣ ΥΠΟΔΟΜΗΣ ΠΕΚ/ΑΑΑ ΤΟΥ ΠΣΔ (ΠΑΝΕΛΛΗΝΙΟΥ ΣΧΟΛΙΚΟΥ ΔΙΚΤΥΟΥ)

Στην παρούσα κατάσταση η υποδομή ΠΕΚ/ΑΑΑ του ΠΣΔ λειτουργεί σε δύο (2) εξυπηρετητές Sun Solaris v280 με 1GB RAM (αποκλειστική χρήση της υπηρεσίας) ενταγμένους στα datacenter του ΠΣΔ σε Αθήνα και Θεσσαλονική. Κάθε εξυπηρετητής περιλαμβάνει:

- Λογισμικό FreeRADIUS ver 1.6
- Βοηθητικό λογισμικό (γραμμένο κυρίως σε γλώσσα perl) κυρίως για την υποβοήθηση της λειτουργίας αποτροπής πολλαπλής σύνδεσης (double login detection) καθώς και για την εξαγωγή στατιστικών στοιχείων, backup δεδομένων κοκ.
- Βάση δεδομένων MySQL για την καταγραφή των στοιχείων accounting.
- Δύο τοποθεσίες λειτουργίας (Αθήνα και Θεσ/κη) για διαμοιρασμό του ρίσκου από την απώλεια μιας εκ των δύο κεντρικών υποδομών της υπηρεσίας σε περίπτωση καθολικής ή μερικής βλάβης

## 5.1 ΚΑΤΑΣΤΑΣΗ ΛΕΙΤΟΥΡΓΙΑΣ

Η τρέχουσα υλοποίηση της υπηρεσίας έχει φτάσει στα όρια της καθώς:

- Οι εξυπηρετητές είναι πεπαλαιωμένοι, με πολύ μικρό διαθέσιμο χώρο ενώ η υποστήριξη του λειτουργικού συστήματος Solaris με την μορφή packages για το freeradius καθυστερεί έναντι των επίσημων εκδόσεων του λογισμικού και αφετέρου δεν παρέχονται δωρεάν.
- Η έκδοση του λογισμικού FreeRADIUS που χρησιμοποιείται είναι παλαιά, με αποτέλεσμα να μην είναι διαθέσιμες ορισμένες επιπλέον λειτουργίες που παρέχονται στις νεότερες εκδόσεις. Παρόμοια κατάσταση ισχύει και για το λογισμικό MySQL.
- Η διαχείριση του λογισμικού (freeradius) δεν είναι εύκολη καθώς δεν υπάρχει κάποιο απλοποιημένο και λειτουργικό package management. Το κύριο λογισμικό έχει

εγκατασταθεί από source code distribution με συνέπεια τη δυσκολία ενσωμάτωσης νέας λειτουργικότητας και διαχείρισης της υπηρεσίας.

## 5.2 ΕΞΑΡΤΩΜΕΝΕΣ ΥΠΗΡΕΣΙΕΣ

Από την υπηρεσία εξαρτάται η παροχή πρόσβασης σε σχολικές και διοικητικές μονάδες στο ΠΣΔ μέσω τεχνολογίας ADSL (και ISDN dialup όπου χρησιμοποιείται ακόμα). Παράλληλα χρησιμοποιείται από την υπηρεσία VPN.

## 5.3 ΕΞΑΡΤΗΣΕΙΣ ΝΕΑΣ ΥΠΗΡΕΣΙΑΣ

Βασική εξάρτηση της νέας υπηρεσίας είναι η παροχή κατάλληλου υλικού (νέοι εξυπηρετητές) για την εγκατάσταση και διαμόρφωση της. Οι νέοι εξυπηρετητές πρέπει να επιτρέπουν την εύκολη διαχείριση τόσο του λειτουργικού, όσο και του λογισμικού που θα χρησιμοποιηθεί στη νέα υπηρεσία. Τα προτεινόμενα λειτουργικά είναι FreeBSD ή Linux.

Σε περίπτωση κατά την οποία η διαθεσιμότητα νέων εξυπηρετητών αργήσει, προτείνεται να γίνει δοκιμαστική εγκατάσταση της υπηρεσίας σε εξυπηρετητή της ομάδας ανάπτυξης του ΕΜΠ, στην οποία θα ενσωματωθούν όλες οι νέες λειτουργίες που προβλέπονται από τη φάση ανάπτυξης. Όταν οι νέοι εξυπηρετητές γίνουν διαθέσιμοι, θα υπάρξει άμεση εγκατάσταση (με χρήση του ήδη αναπτυγμένου configuration και εργαλείων λογισμικού) και ενεργοποίηση της.

# 6. ΠΕΡΙΓΡΑΦΗ ΑΝΑΠΤΥΞΗΣ

Βασικό συστατικό στοιχείο της ανάπτυξης είναι η μετάβαση της υπηρεσίας στην έκδοση FreeRADIUS 2.X. η οποία περιλαμβάνει πολλαπλές βελτιώσεις του λογισμικού οι οποίες θα υποβοηθήσουν την καλύτερη λειτουργία και διαχείριση της υπηρεσίας. Ανάμεσα στα άλλα:

- Καλύτερη διαμόρφωση της υπηρεσίας με σαφέστερο διαχωρισμό της διαμόρφωσης σε συστατικά στοιχεία και λειτουργία πολλαπλών virtual servers.
- Νέα, εξελιγμένη γλώσσα διαμόρφωσης με δυνατότητα conditional path selection στην παροχή της υπηρεσίας με βάση πολλαπλά κριτήρια.
- Online conditional debugging.
- Πλήρως λειτουργική και ώριμη υποστήριξη των τεχνολογιών Extensible Authentication Protocol) EAP.
- Πλήρως λειτουργική και ώριμη υποστήριξη IPv6 και απαιτούμενων attributes.
- Integration με την τεχνολογία πιστοποιητικών (certficates), το οποίο μπορεί να επιτρέψει, εφόσον είναι επιθυμητό, την αξιοποίηση αρχής πιστοποίησης του ΠΣΔ για την παροχή ελεγχόμενης πρόσβασης στο διαδίκτυο (με χρήση τεχνολογίας 802.1x/EAP-TLS).
- Βελτιωμένη ικανότητα post-logging, λειτουργία απαραίτητη για την καταγραφή αποτυχημένων και προβληματικών συνδέσεων.

Στα πλαίσια μετάβασης στη νέα έκδοση θα γίνει μετάβαση της υπάρχουσας διαμόρφωσης στο νέο σχήμα καθώς και αναβάθμιση των εργαλείων υποστήριξης (double login detection) με σκοπό την ακόμα πιο πλήρη και λειτουργική κάλυψη των απαιτήσεων του ΠΣΔ αλλά και την μείωση των απαιτήσεων διαχείρισης. Σε συνεργασία με τις ομάδες ανάπτυξης των υπηρεσιών Wi-Fi και IPv6, θα γίνουν όλες οι απαραίτητες ενέργειες και προσαρμογές στην υπηρεσία ώστε να υποστηρίζεται πλήρως τόσο η πρόσβαση στις νέες υπηρεσίες, όσο και η καταγραφή αναλυτικού ιστορικού πρόσβασης (accounting).

Σε συνεργασία με την ομάδα λειτουργίας του EduRoam (ΕΔΕΤ) θα επιδιωχθεί η σύνδεση της υπηρεσίας AAA με το δίκτυο του EduRoam, κάτι το οποίο θα επιτρέψει (ιδιαίτερα με

δεδομένη την επέκταση της δυνατότητας πρόσβασης με παροχή υπηρεσιών Wifi και IPv6) την πρόσβαση στο δίκτυο του ΠΣΔ σε όλη την ακαδημαϊκή κοινότητα, καθιστώντας το ΠΣΔ μέρος του ευρύτερου Ελληνικού ακαδημαϊκού δικτύου.

# 7. ΑΠΛΟΠΟΙΗΣΗ ACCOUNTING – ΒΕΛΤΙΩΣΗ DOUBLE LOGIN DETECTION

Στα πλαίσια βελτίωσης της υπηρεσίας θα υπάρξουν δύο βασικές διαφοροποιήσεις στο σχήμα καταγραφής χρήσης της υπηρεσίας:

1. Διαχωρισμός του μακροπρόθεσμου accounting από την καταγραφή των συνδεδεμένων χρήστων σε δύο πίνακες (το μακροπρόθεσμο accounting παράλληλα με το ιστορικό των συνδέσεων θα διατηρεί **και** τους συνδεδεμένους χρήστες, έχοντας ουσιαστικά μία μικρής έκτασης αλληλοεπικάλυψη). Κατά αυτόν τον τρόπο όλες οι λειτουργίες που έχουν να κάνουν με την ίδια την υπηρεσία (double login detection κτλ) θα πραγματοποιούνται σε έναν πίνακα σταθερού μεγέθους, με συνέπεια σταθερότητα στην απόκριση και μειωμένο χρόνο εξυπηρέτησης.

2. Το double login detection πρέπει να γίνεται με ερώτηση ΜΟΝΟ του πίνακα των συνδεδεμένων χρηστών. Ο έλεγχος για stale sessions θα πραγματοποιείται εξωτερικά από κατάλληλο script το οποίο θα εκτελείται κάθε μερικά λεπτά και θα ελέγχει τους συνδεδεμένους χρήστες (όπως φαίνονται στη βάση) με τους πραγματικά συνδεδεμένους στους LNS. Αυτό σημαίνει βέβαια ότι οι χρήστες δε θα έχουν τη δυνατότητα να συνδεθούν για μερικά λεπτά αλλά από την άλλη θα επιτρέψει την εξυπηρέτηση των χρηστών ακόμα και σε δύσκολες καταστάσεις μετά από reboots/πτώσεις κυκλωμάτων. Ταυτοχρόνως, ο χρόνος εξυπηρέτησης περιπτώσεων μαζικού double login θα εξαρτάται μόνο απο την απόδοση των εξωτερικών script. Τα script αυτά, καθώς θα τρέχουν συνεχώς, δε θα έχουν τα προβλήματα που συνδέονται με την επαναλαμβανόμενη εκτέλεση (φόρτωση) διεργασιών ενώ θα διαμορφωθούν με τέτοιο τρόπο ώστε η εκτέλεση εξωτερικών sql queries να είναι όσο πιο αποδοτική γίνεται αποφεύγοντας σειριακή εκτέλεση όπου είναι δυνατό.

Παράλληλα θα υπάρξει εκτεταμένη χρήση του sql_log module το οποίο επιτρέπει την καταγραφή σε κατάλληλο αρχείο sql statements στις φάσεις του accounting (accounting start, stop, alive) και του post-auth. Η καταγραφή αυτή στη συνέχεια διαβάζεται (σε συνεχή βάση) από κατάλληλη εξωτερική διεργασία η οποία και κάνει την τελική καταγραφή στη βάση δεδομένων. Έτσι, η υγεία της βάσης δεδομένων και η απόκριση της παύει να επηρεάζει την απόδοση της υπηρεσίας RADIUS. Ο εξυπηρετητής καταγράφει απλώς στο sql_log

αρχείο κατάλληλα statements και η εξωτερική διεργασία φροντίζει να καταγραφούν στη βάση δεδομένων με βάση τους ρυθμούς που μπορεί να εξυπηρετήσει η τελευταία.

Κατά συνέπεια, ο μοναδικός ουσιαστικά πίνακας στον οποίο καταγράφει άμεσα η υπηρεσία είναι ο πίνακας των συνδεδεμένων χρηστών ενώ οποιαδήποτε άλλη λειτουργία καταγραφής (accounting, failed logins και οτιδήποτε άλλο τυχόν απαιτηθεί στο μέλλον) γίνεται μέσω εξωτερικών διεργασιών χωρίς να επηρεάζεται η υπηρεσία.

## 7.1 ΠΙΝΑΚΑΣ RADSESSION

Για καταγραφή των online χρηστών θα χρησιμοποιηθεί ένας νέος πίνακας, διαθέσιμος στη βάση δεδομένων σε replicated/high availability, ο οποίος θα περιέχει τους online χρήστες. Στο επιτυχές authentication χρηστών θα χρησιμοποιείται η sql εντολή REPLACE για την προσθήκη (εφόσον δεν υπάρχει ήδη) της εγγραφής χρήστη στον πίνακα. Προτείνεται να χρησιμοποιηθεί το REPLACE αντί του INSERT προκειμένου να μειωθούν τυχόν προβλήματα λόγω duplicate keys στο replication. Σε περίπτωση που (λόγω στιγμιαίας δυσλειτουργίας του replication) η εγγραφή υπάρχει ήδη, το REPLACE θα εκτελέσει παρόμοια λειτουργία με το INSERT χωρίς όμως αποτυχία λόγω ύπαρξης του κλειδιού του row που αντιστοιχεί στην εγγραφή αυτή (όπως θα συνέβαινε με INSERT). Σε accounting-stop η εγγραφή θα γίνεται DELETE με συνέπεια να διατηρούνται μόνο οι συνδεδεμένοι χρήστες.

Η προσθήκη εγγραφής στον πίνακα στο επιτυχές authentication και όχι στο accounting-start είναι ηθελημένη καθώς η εμπειρία έχει δείξει ότι είναι προτιμότερο να έχουμε μία εγγραφή για χρήστη ο οποίος τελικά δεν μπόρεσε να συνδεθεί (η οποία μπορεί να διαγραφεί στη συνέχεια μέσω λειτουργιών stale sessions check/double login check) παρά να μην υπάρχει καθόλου εγγραφή για χρήστη ο οποίος είναι συνδεδεμένος. Το τελευταίο μπορεί να συμβεί λόγω σύντομης δικτυακής δυσλειτουργίας η οποία μπορεί να οδηγήσει σε απώλεια του αντίστοιχου Accounting-Start record με αποτέλεσμα την ανυπαρξία εγγραφής για το συνδεδεμένο χρήστη.

Το γενικό accounting θα συνεχίσει να διατηρείται στον πίνακα radacct. Προκειμένου να μειωθεί η εξάρτηση της υπηρεσίας από εξωτερικές βάσεις και για αύξηση της απόδοσης θα ακολουθηθεί μία λογική ενδιάμεσου buffer. Τα στοιχεία που προορίζονται για εγγραφή στον πίνακα radacct θα εγγράφονται σε ένα SQL statements αρχείο μέσω του FreeRADIUS module sql_log. Στη συνέχεια εξωτερική διεργασία radsqlrelay θα αναλαμβάνει την εκτέλεση τους στον πίνακα radacct.

## 7.2 ΒΕΛΤΙΩΣΗ DOUBLE LOGIN DETECTION

Στο τρέχων σχήμα του double login detection υπάρχει σημαντική χρήση ερωτημάτων προς τους access servers για τον προσδιορισμό των stale sessions. Ειδικότερα:

- Το double login detection εμπιστεύεται τον πίνακα με τους συνδεδεμένους χρήστες και δεν επιτρέπει τη σύνδεση χρήστη ο οποίος εμφανίζεται ήδη συνδεδεμένος.
- Αποτυχημένα logins καταγράφονται στη ΒΔ σε κατάλληλο table και εξωτερική διεργασία τα ελέγχει σε τακτά χρονικά διαστήματα με βάση snmpwalk στους access servers και αν απαιτείται αποστέλλει κατάλληλο fake accounting-stop.
- Κατά τη λήψη ενός Accounting-Update, ενημερώνεται κατάλληλο πεδίο (UpdateTime) στον πίνακα των συνδεδεμένων χρηστών. Εξωτερική διεργασία ελέγχει για χρήστες που φαίνονται 'stale' με βάση τη διαφορά μεταξύ του τρέχοντος χρόνου και του τελευταίου χρόνου ενημέρωσης (current time – update time) και εφόσον δε βρεθούν συνδεδεμένοι με βάση snmpwalk στον access server (στον οποίο εμφανίζονται συνδεδεμένοι), αποστέλλεται κατάλληλο fake accounting stop.

Παρότι η παραπάνω διαδικασία είναι πολύ πιο ευέλικτη και αποδοτική σε σχέση με τη χρήση του κλασσικού μηχανισμού (κλήση εξωτερική διεργασίας ελέγχου του χρήστη με χρήση snmpwalk σε περίπτωση που εμφανίζεται συνδεδεμένος) παρουσιάζει και πάλι σημαντικά θέματα:

- Η εύρεση 'stale sessions' με χρήση του update time είναι εγγενώς αργή και μπορεί να λειτουργήσει μόνο υποβοηθητικά σε ένα σχήμα που λειτουργεί ήδη σωστά.

- Η χρήση των double logins για την ενεργοποίηση του ελέγχου για 'stale sessions' έχει το πρόβλημα ότι σε περιπτώσεις όπως η μαζική αποσύνδεση χρηστών (λόγω πχ πτώσης κάποιου τοπικού κυκλώματος του ΟΤΕ), απαιτείται να γίνει μαζικός έλεγχος χρηστών, ο οποίος είναι μία αργή διαδικασία. Λόγω των συνδέσεων DSL από την άλλη, μονάδες οι οποίες δεν μπορούν να συνδεθούν θα συνεχίσουν να προσπαθούν μαζικά και συνεχόμενα να επιτύχουν τη δικτυακή τους σύνδεση, επιδεινώνοντας την κατάσταση.

Η νέα διαδικασία θα λειτουργεί ως εξής:

Στον πίνακα radsession προστίθεται ένα νέο πεδίο UpdateTime. Σε κάθε εξυπηρετητή θα εκτελούνται με μικρό sleep ανάμεσα στις εκτελέσεις διεργασίες snmpbulkwalk των LNS. Κατά την εκκίνηση κάθε εκτέλεσης θα διατηρείται το timestamp έναρξης. Κάθε χρήστης του πίνακα radsession ο οποίος βρίσκεται να είναι ενεργός θα ανανεώνεται στο πεδίο UpdateTime με την τιμή του timestamp εφόσον η τιμή του (η UpdateTime) είναι παλαιότερη.

Παράλληλα στον πίνακα των nas θα προστεθεί ένα επιπλέον πεδίο UpdateTime το οποίο θα περιέχει πάντα την νεότερη τιμή του UpdateTime για τον LNS αυτό. Η τιμή του θα ανανεώνεται μόνο εφόσον το snmpbulkwalk επέστρεψε χρήστες για τον αντίστοιχο LNS και αφού ολοκληρωθεί η διάσχιση του.

Σε δεύτερο στάδιο θα εκτελείται διεργασία stale sessions check. Για κάθε LNS η διεργασία θα λαμβάνει την τιμή του UpdateTime (απο τον πίνακα nas) και θα εκτελεί το ισοδύναμο του παρακάτω SQL query:

"*SELECT UserName, AcctSessionId, NASIPAddress, FROM radsession WHERE UpdateTime < '%{Update-Time}' AND NASIPAddress = '%{NAS-IP-Address}' AND AcctStartTime < '%{Update-Time}'*

Κατ' αυτόν τον τρόπο θα βρίσκονται απευθείας μέσω sql query οι χρήστες οι οποίοι έχουν συνδεθεί πριν το τελευταίο walk του αντίστοιχου LNS αλλά δεν ανανεώθηκε η εγγραφή τους (δηλαδή είναι stale). Με εκτέλεση του ίδιου query για όλους τους LNS θα πραγματοποιείται

απευθείας η ανεύρεση stale εγγραφών και θα αποστέλλονται κατάλληλα fake accounting stops.

# 8. ΚΑΤΑΓΡΑΦΗ BAD LOGINS

Στην τρέχουσα αρχιτεκτονική, υπάρχει εξωτερική διαδικασία η οποία διαβάζει συνεχώς το radius.log και φροντίζει ώστε να υπάρχει καταγραφή αποτυχημένων logins στη βάση του accounting.

Στη νέα αρχιτεκτονική θα γίνει εκμετάλλευση της δυνατότητας για conditional configuration και χρήση του sql_log module στο post-auth. Στο post-auth section, τυχόν αποτυχημένες προσπάθειες σύνδεσης θα καταγράφονται σε κατάλληλα sql statements σε sql_log αρχείο, το οποίο στη συνέχεια θα διαβάζεται από εξωτερική διεργασία radsqlrelay η οποία και θα τα καταγράφει τελικώς στη βάση δεδομένων, απλοποιώντας το σχήμα και επιτρέποντας πολύ μεγαλύτερο έλεγχο. Αναλόγως με το λόγο της αποτυχίας, τα statements θα περιέχουν διαφορετικά στοιχεία καταγραφής στο terminate-cause.

Παράλληλα, θα εξεταστεί η δυνατότητα καταγραφής μίας μόνο εγγραφής αποτυχημένης σύνδεσης ανά λογαριασμό (τα στοιχεία της οποίας θα ανανεώνονται σε κάθε νέα αποτυχημένη προσπάθεια), προκειμένου να ελαφρύνει το μέγεθος της καταγραφής accounting από πολλαπλές προσπάθειες αποτυχημένης πρόσβασης.

## 8.1 ΚΑΤΑΓΡΑΦΗ ΤΕΛΕΥΤΑΙΑΣ ΠΡΟΣΒΑΣΗΣ

Λόγω του πολύ μεγάλου αριθμού καθημερινών συνδέσεων και προκειμένου να είναι ευκολότερη η επισκόπηση των λογαριασμών των μονάδων, έχει επιλεγεί η πολιτική της διατήρησης ενεργού καταγραφής στη ΒΔ μόνο για τις τελευταίες δέκα ημέρες, με τις υπόλοιπες να διατηρούνται σε κατάλληλα sql dump αρχεία καταγραφής.

Κατόπιν επανειλημμένης ζήτησης από το helpdesk θα δημιουργηθεί πίνακας καταγραφής στον οποίο θα διατηρείται ο χρόνος της τελευταίας επιτυχημένης σύνδεσης για ένα λογαριασμό (ένα row ανά λογαριασμό), ανεξαρτήτως του χρόνου στον οποίο έγινε αυτή και ο οποίος θα παρουσιάζεται από το εργαλείο διαχείρισης dialupadmin, στην κεντρική σελίδα επισκόπησης ενός λογαριασμού.

# 9. Συνολο Πινακων Υπηρεσιας

Με βάση και την περιγραφή που έγινε προηγουμένως οι πίνακες στους οποίους θα βασίζεται η υπηρεσία θα είναι:

1. Πίνακας radsession στον οποίο θα γράφει απευθείας η υπηρεσία και θα περιλαμβάνει μόνο τους συνδεδεμένους χρήστες. Κατά την αποσύνδεση η αντίστοιχη καταγραφή θα διαγράφεται.
2. Πίνακας radacct στον οποίο θα καταγράφεται το ιστορικό συνδέσεων των τελευταίων δέκα ημερών αλλά και οι συνδεδεμένοι χρήστες. Η καταγραφή θα γίνεται μέσω sql_log και εξωτερικής διεργασίας. Καθημερινή διεργασία θα φροντίζει για τη διαγραφή στοιχείων παλαιότερων των δέκα ημερών αφού πρώτα λαμβάνεται αρχείο backup.
3. Πίνακας τελευταίας σύνδεσης και τελευταίας αποτυχημένης σύνδεσης. Στον πίνακα θα καταγράφεται η τελευταία επιτυχημένη και τελευταία αποτυχημένη σύνδεση ανά χρήστη για λόγους εύκολης επισκόπησης. Η καταγραφή θα γίνεται μέσω sql_log και εξωτερικής διεργασίας. Θα γίνουν κατάλληλες αλλαγές στο περιβάλλον επισκόπησης dialup_admin ώστε να υποστηρίζει το νέο σχήμα.
4. Πίνακες επισκόπησης ιστορικού οι οποίοι θα περιέχουν συγκεντρωτικά στοιχεία συνδέσεων ανά χρήστη. Οι πίνακες αυτοί είναι ήδη διαθέσιμοι στην τρέχουσα υπηρεσία και δημιουργούνται από κατάλληλα scripts τα οποία εκτελούνται σε καθημερινή βάση και η υπάρχουσα υποδομή δε θα αλλάξει σε αυτό το επίπεδο.

# 10. ΥΠΟΣΤΗΡΙΞΗ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΠΡΟΣΒΑΣΗΣ IPv6 ΑΠΟ ΤΗΝ ΥΠΟΔΟΜΗ ΑΑΑ/ΠΕΚ

## 10.1 IETF RADIUS ATTRIBUTES

Για την δυναμική ρύθμιση του NAS σχετικά με τις λειτουργίες πρόσβασης των δρομολογητών πρόσβασης, προβλέπεται από την μελέτη πρόσβασης IPv6 η χρήση των παρακάτω RADIUS attributes όπως καθορίζονται στο RFC3162 και στο draft-ietf-radext-ipv6-access-07 με ενσωμάτωση τους στην κλάση radiusprofile και χρήση τους κατά το authorization των μονάδων/χρηστών.

1. **Framed-IPv6-Prefix**
2. Καθορίζει το πρόθεμα IPv6 που ανατίθεται στον σύνδεσμο PPP του συνδρομητή. Στις περισσότερες περιπτώσεις, το prefix αυτό ενσωματώνεται μέσα στο Router Advertisement που μεταδίδεται από τον NAS προς το CPE μέσα από τον σύνδεσμο PPP.
3. **Framed-IPv6-Pool**
4. Η λειτουργία του συγκεκριμένου attribute είναι παρόμοια με του Framed-IPv6-Prefix, με την διαφορά ότι στην περίπτωση του Framed-IPv6-Pool το πρόθεμα ανασύρεται από ένα pool προθεμάτων που εδράζεται στον NAS, αντί να καθορίζεται ρητά από τον RADIUS. Οπότε, ο RADIUS καθορίζει το pool και ο NAS φροντίζει να επιλέξει ένα ελεύθερο (δεν το έχει δώσει αλλού) πρόθεμα μέσα από αυτό.
5. **Delegated-IPv6-Prefix (πολλαπλές τιμές)**
6. Καθορίζει το πρόθεμα IPv6 που είναι δυνατό να ανατεθεί στο CPE, αν το τελευταίο ζητήσει να λάβει πρόθεμα μέσω DHCPv6 Prefix Delegation. Στην γενική περίπτωση, το συγκεκριμένο attribute μπορεί να έχει πολλαπλές τιμές, με συνέπεια το CPE να μπορεί να λάβει πολλαπλά prefixes.
7. **Delegated-IPv6-Prefix-Pool**
8. Έχει την ίδια σχέση με το Delegated-IPv6-Prefix με την σχέση του Framed-IPv6-Pool με το Framed-IPv6-Prefix. Είναι δηλαδή η δεξαμενή προθεμάτων από την οποία μπορεί να γίνει απόδοση προθεμάτων στα CPEs μέσω του μηχανισμού DHCPv6 Prefix Delegation.

9. **Framed-Interface-ID**
10. Καθορίζει τα τελευταία 64 bits (Least Significant Bits) της διεύθυνσης IPv6 που θα έχει το CPE. Υπενθυμίζεται ότι με βάση τα 64 αυτά bits και την διαδικασία του SLAAC που θα καθορίσει τα πρώτα 64 bits (Most Significant Bits) μέσα από κάποιο router advertisement (RA) που θα περιέχει ένα πρόθεμα /64, το CPE μπορεί να καταλήξει σε μια πλήρη διεύθυνση IPv6 συνδυάζοντας τα δύο διαφορετικά κομμάτια.
11. **Framed-IPv6-Route (πολλαπλές τιμές)**
12. Μέσω του συγκεκριμένου attribute, είναι δυνατό να εγκατασταθεί στον NAS ένα IPv6 route που να οδηγεί προς το interface του συνδρομητή. Τυχόν υποδίκτυα ρυθμισμένα πίσω από το CPE (ήτοι μέσα στην μονάδα), μπορούν με αυτό τον τρόπο να αποκτήσουν συνδεσιμότητα με το υπόλοιπο δίκτυο. Για να γίνει αυτό πρέπει απαραίτητα να υπάρχει το σχετικό configuration στο CPE και παράλληλα το user profile του συγκεκριμένου CPE να περιλαμβάνει το αντίστοιχο Framed-IPv6-Route.
13. **DNS-Server-IPv6-Address (πολλαπλές τιμές)**
14. Δίνει την δυνατότητα να καθοριστεί ένα σύνολο από IPv6 recursive DNS servers που θα αποδοθούν στο CPE. Ο τρόπος με τον οποίο οι διευθύνσεις αυτών των servers θα μεταδοθούν στο CPE δεν καθορίζεται ρητά, αλλά επί του παρόντος προσφέρονται οι εξής τρόποι:
15. RFC5006 ή RFC6106 για την ενσωμάτωση των DNS servers στα Router Advertisements του NAS.
16. DHCPv6 Stateless Options
17. **Route-IPv6-Information.**
18. Δίνει την δυνατότητα στον NAS να συμπεριλάβει ένα ή περισσότερα προθέματα, routes προς τα οποία θα εγκατασταθούν εντός του CPE όταν επιτευχθεί η σύνδεση PPP. Ο μηχανισμός με τον οποίο επιτυγχάνεται το παραπάνω είναι η εισαγωγή από τον NAS ενός ή περισσοτέρων route information options (RFC4191, παρ. 2.3) στα router advertisements που στέλνει προς το CPE πάνω από τον σύνδεσμο PPP.
19. **Framed-IPv6-Address**
20. Διεύθυνση που θα δοθεί στο CPE από τον BRAS μέσω του μηχανισμού DHCPv6-NA.

21. **Stateful-IPv6-Address-Pool**
22. Δεξαμενή προθεμάτων από την οποία μπορεί να γίνει απόδοση διευθύνσεων στα CPEs μέσω DHCPv6-NA.

## 10.2 ΧΡΗΣΗ RADIUS ATTIBUTES ΓΙΑ ΤΑ ΠΡΟΦΙΛ ΤΩΝ ΜΟΝΑΔΩΝ ΤΟΥ ΠΣΔ.

## 10.3 CISCO VENDOR SPECIFIC ATTRIBUTES

Συνοπτικός πίνακας με τα σχετικά Cisco vendor specific attributes και το αντίστοιχο IETF RADIUS attribute δίνεται παρακάτω. Τονίζεται δυστυχώς ότι η τεκμηρίωση που προσφέρει η εταιρεία Cisco είναι ελλιπής και σε πολλές περιπτώσεις παραπλανητική ή λανθασμένη. Ο υλοποιητής θα πρέπει σε όλες τις περιπτώσεις που μπορεί να χρησιμοποιήσει τα IETF attributes να δείξει προτίμηση σε αυτά αντί για τα αντίστοιχα VSAs .

| Παράδειγμα Cisco-AVPair | IETF |
|---|---|
| **cisco-avpair = "ipv6:route=2001:DB8:2::/64"** | Αντίστοιχο με το Framed-IPv6-Route |
| **cisco-avpair = "ipv6:prefix=2001:DB8:2::/64 0 0 onlink autoconfig"** | Αντίστοιχο με το Framed-IPv6-Prefix |
| **cisco-avpair="ipv6:outacl#1=deny 2001:DB8::/10",** | (δεν υπάρχει αντίστοιχο IETF attribute) |
| **cisco-avpair="ipv6:inacl#1=permit 2001:DB8:1::/64 any"** | (δεν υπάρχει αντίστοιχο IETF attribute) |

## 10.4 ΑΝΤΙΣΤΟΙΧΙΣΗ RADIUS ΚΑΙ LDAP ATTRIBUTES.

Για λόγους απλότητας, η αποθήκευση των attributes στον LDAP θα γίνεται σε βάση ένα προς ένα, δηλαδή πλήρης αντιστοιχία του κάθε attribute με το αντίστοιχο LDAP attribute. Η μοναδική παρατήρηση που έχει σημασία από την πλευρά της υλοποίησης είναι ότι καθώς το

dictionary ενός εξυπηρετητή καταλόγου σε κάποιες περιπτώσεις δεν επιτρέπει την χρήση του χαρακτήρα '-' (παύλα), για την αποθήκευση στον κατάλογο θα χρησιμοποιείται η μορφή CamelCase (βλέπε: http://en.wikipedia.org/wiki/CamelCase) , αφού φυσικά αφαιρεθούν οι παύλες.

## 10.5 MULTIVALUED ATTRIBUTES

Υπενθυμίζεται τέλος ότι ορισμένα από τα παραπάνω attributes (π.χ. DNS-Server-IPv6-Address) μπορεί έχουν πολλαπλές τιμές (multivalued attributes). Η αποθήκευση των πολλαπλών τιμών ενός attribute που πρέπει να επιστραφεί από τον RADIUS γίνεται στην υπηρεσία καταλόγου με την αντίστοιχη χρήση LDAP multivalued attributes.

## 10.6 DNS-SERVER-IPV6-ADDRESS

Εξαίρεση αποτελεί το DNS-Server-IPv6-Address, που σε κάποιες περιπτώσεις θα χρειαστεί να καθορίζεται π.χ. από τον ίδιο τον NAS ή από τον RADIUS με στατικό τρόπο ή προγραμματιστικά. Ένα παράδειγμα που προκρίνεται σαν αρκετά αντιπροσωπευτικό είναι η χρήση του DNS για αποτελεσματικότερο content filtering στο ΠΣΔ. Στο παράδειγμα αυτό, οι πρωτοβάθμιες μονάδες θα χρησιμοποιούν ένα συνολο από «περιορισμένους» DNS servers οι οποίοι δεν επιστρέφουν απάντηση για domains που θεωρούνται από το ΠΣΔ σαν βλαβερά και απαγορεύονται. Αντίθετα, π.χ. οι διοικητικές μονάδες δεν υπόκεινται σε αυτόν τον περιορισμό, με αποτέλεσμα να πρέπει να λάβουν ένα άλλο σύνολο από DNS servers. Η υλοποίηση ενός τέτοιου σχήματος γίνεται καθορίζοντας στον RADIUS τα διαφορετικά σύνολα από διευθύνσεις των εξυπηρετητών DNS και προγραμματίζοντάς τον να επιστρέφει το κατάλληλο ανάλογα με το group κάτω από το οποίο η μονάδα είναι καταγεγραμμένη στην υπηρεσία καταλόγου. Περισσότερες πληροφορίες σχετικά με το συγκεκριμένο θέμα περιέχονται στην αντίστοιχη μελέτη για την υπηρεσία καταλόγου και τον RADIUS.

## 11. ΕΡΓΑΣΙΕΣ ΑΝΑΠΤΥΞΗΣ

- Εγκατάσταση νέου λογισμικού σε δοκιμαστικό εξυπηρετητή, μετάβαση υπάρχουσας διαμόρφωσης στη νέα έκδοση.
- Ανανέωση και βελτιστοποίηση βοηθητικού λογισμικού.
- Ενσωμάτωση επιπλέον λειτουργικότητας για παροχή υποστήριξης στις υπηρεσίες Wi-Fi, IPv6.
- Διαμόρφωση και δοκιμή της ικανότητας πιστοποίησης μέσω της ομάδας πρωτοκόλλου EAP.
- Σύνδεση με την υπηρεσία EduRoam.
- Δοκιμή της υπηρεσίας σε συνεργασία με άλλες ομάδες του ΠΣΔ (υπηρεσία πρόσβασης, VPN κτλ).

## 12. ΠΑΡΑΔΟΤΕΑ

- Λειτουργική υπηρεσία (η τελική φάση θα εξαρτηθεί από τη διαθεσιμότητα εξυπηρετητών).
- Τεκμηρίωση.

## 13. ΑΝΑΦΟΡΕΣ – ΠΗΓΕΣ

[FR] FreeRADIUS http://freeradius.org/

[OD] OpenLDAP http://www.openldap.org/

[HA] Linux High Availability http://www.linux-ha.org/wiki/Main_Page

[DRBD] Distributed Remote Block Device http://www.drbd.org/

[MySQL] MySQL Data Base http://www.mysql.com/

[VMWARE] VMware www.vmware.com

[XEN] xen.org

[KVM] kvm.org

[IEEE-802] Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Overview and Architecture", IEEE Standard 802, 1990.

[IEEE-802.1X] Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port-Based Network Access Control", IEEE Standard 802.1X, September 2001.

[EAP] Extensible Authentication Protocol (EAP) RFC 3748, http://tools.ietf.org/html/rfc3748

[PAP] Password authentication protocol (PAP) PPP authentication protocols www.ietf.org/rfc/rfc1334.tx

[CHAP] Challenge Handshake Authentication Protocol, www.ietf.org/rfc/rfc1994.txt

[MSCHAP] Microsoft PPP CHAP Extensions, http://tools.ietf.org/html/rfc2433

[MSCHAP2] Microsoft PPP CHAP Extensions, Version 2, http://tools.ietf.org/html/rfc2759

[EAPMD] RFC 2284 Extensible Authentication Protocol http://www.ietf.org/rfc/rfc2284.txt

[EAPTL] PPP EAP TLS Authentication Protocol, http://www.ietf.org/rfc/rfc2716.txt

[PEAP] Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, http://www.ietf.org/rfc/rfc4017.txt

[PEAP] Palekar, A., et al., "Protected EAP Protocol (PEAP)", Work in Progress, July 2004

[TTLS] Funk, P. and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)", Work in Progress, August 2004

Delivering Massively Scalable & Highly Available Authentication Services:

http://www.mysql.com/why-mysql/white-papers/mysql_wp_ha_auth_account.php

**http://www.sown.org.uk/wiki/FreeRadius**

MySQL Cluster on the web: http://www.mysql.com/products/database/cluster/

MySQL Cluster Datasheet:

23. http://www.mysql.com/products/database/cluster/mysql-cluster-datasheet.pdf

MySQL Cluster Architecture and New Features Whitepaper:

24. http://www.mysql.com/why-mysql/white-papers/mysql_wp_cluster7_architecture.php

MySQL Cluster Evaluation Guide:

25. http://www.mysql.com/why-mysql/white-papers/mysql_cluster_eval_guide.php

Πηγές από το Διαδίκτυο

http://rackerhacker.com/redundant-cloud-hosting-configuration-guide/setting-up-a-redundant-database-and-caching-layer/

http://dba.stackexchange.com/questions/5153/mysql-replication-1-slave-multiple-masters

http://dba.stackexchange.com/questions/9424/best-way-to-setup-master-to-multi-master-replication

http://www.slideshare.net/KrisBuytaert/mysql-ha-alternatives-2010

http://www.clusterlabs.org/wiki/DRBD_MySQL_HowTo