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)»

Δράση Α3 Προηγμένες υπηρεσίες ΠΣΔ

υ

Κατάσταση Έκδοσης	**Υπό έγκριση από ΙΤΥΕ**
Ημερομηνία	**30/7/2012**
Περιγραφή Αρχείου	
Συμπράττων Φορέας	**ΕΠΙΣΕΥ**
Υπεύθυνος Παραδοτέου	**Δρ. Δημήτριος Καλογεράς**
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

ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Ομαδα Εκπονησης Παραδοτεου

1. **Καθ. Ευσταθιος Συκας**
2. **Δρ. Δημητριος Καλογερας**
3. **Σπυριδων Παπαγεωργιου**

1. Περιγραφη Υπηρεσιας- WiFi

Στόχος της υπηρεσίας είναι παροχή ασύρματης πρόσβασης στα σχολεία του ΠΣΔ για χρήση από φορητό υπολογιστή (Laptop) ή έξυπνο κινητό τηλέφωνο. Η επίτευξη αυτού του στόχου απαιτεί υλική υποδομή και υλοποίηση μηχανισμών πρόσβασης. Για την αποτύπωση των απαραίτητων συστατικών του υλικού και του λογισμικού θα παρουσιαστούν τα σενάρια χρήσης. Η ανάλυση αυτών των απαιτήσεων θα καθορίσει τα χαρακτηριστικά της υποδομής από τα οποία θα προκύψουν και οι απαιτήσεις υλικού και λογισμικού.

2. ΣΕΝΑΡΙΑ ΧΡΗΣΗΣ

Στην συνέχεια θα παρουσιαστούν μερικά σενάρια τα οποία θα χρησιμοποιηθούν για την παραγωγή τεχνικών προδιαγραφών.

2.1 ΑΣΥΡΜΑΤΗ ΠΡΟΣΒΑΣΗ ΣΕ ΑΝΟΙΚΤΟΥΣ ΔΗΜΟΣΙΟΥΣ ΧΩΡΟΥΣ ΤΟΥ ΣΧΟΛΕΙΟΥ

Σε αυτό το σενάριο χρήσης οι μαθητές (οι οποίοι έχουν προηγούμενα καταχωρηθεί και έχουν προμηθευτεί ένα συνδυασμό κωδικού/συνθηματικού) μπορούν να αποκτήσουν πρόσβαση:

- σε ένα ανοικτό δίκτυο (open SSID) χωρίς κλειδί με περαιτέρω πιστοποίηση μέσω ενός "κλειστού" περιβάλλοντος (captive portal) με χρήση του browser. (ΑΠ_ΔΜ1)
- σε ένα κλειστό δίκτυο (SSID με δυναμικό κωδικό ή κλειδί) με περαιτέρω πιστοποίηση με χρήση συνθηματικών. (ΑΠ_ΔΜ2)

Ο χρήστης του δικτύου έχει πρόσβαση στο διαδίκτυο με τους περιορισμούς της υπηρεσίας πρόσβασης περιεχόμενου. Δεν επιτρέπεται η πρόσβαση στο δίκτυο του μαθητικού εργαστηρίου ή στην υποδομή του σχολείου.

2.1.1 Ασύρματη πρόσβαση δικτύου σε ανοικτούς δημόσιους χώρους από καθηγητές

Σε αυτό το σενάριο χρήσης οι καθηγητές (οι οποίοι έχουν προηγούμενα καταχωρηθεί και έχουν ένα συνδυασμό κωδικού/συνθηματικού) μπορούν να αποκτήσουν πρόσβαση:

- σε ένα ανοικτό δίκτυο (open SSID) χωρίς κλειδί με περαιτέρω πιστοποίηση μέσω ενός "κλειστού" περιβάλλοντος (captive portal) με χρήση του browser. Προτείνεται η χρήση https και χρήση Single Sign On (SSO). (ΑΣΔΚ1)
- σε ένα κλειστό δίκτυο (SSID με κρυπτογράφηση) με περαιτέρω πιστοποίηση με χρήση συνθηματικών. (ΑΣΔΚ2)

Ο χρήστης του δικτύου προορίζεται μόνο για πρόσβαση στο διαδίκτυο **ΧΩΡΙΣ** τους περιορισμούς της υπηρεσίας πρόσβασης περιεχομένου. Δεν επιτρέπεται η πρόσβαση στο δίκτυο του μαθητικού εργαστηρίου ή στην υποδομή του σχολείου.

2.1.2 Ασύρματη πρόσβαση δικτύου σε χώρους μαθητικού εργαστηρίου

Σε αυτό το σενάριο χρήσης οι μαθητές ή και οι καθηγητές (οι οποίοι έχουν προηγούμενα καταχωρηθεί και έχουν ένα συνδυασμό κωδικού/συνθηματικού) μπορούν να αποκτήσουν πρόσβαση:

- σε ένα ανοικτό δίκτυο (open SSID) με WPA/WPA2-PSK με περαιτέρω πιστοποίηση μέσω ενός "κλειστού" περιβάλλοντος με χρήση του browser. (ΑΣΔΜ)
- σε ένα κλειστό δίκτυο (SSID με κρυπτογράφηση) με περαιτέρω πιστοποίηση με χρήση συνθηματικών. (ΑΣΔΜ2)

Σε αυτό το σενάριο χρήσης οι μαθητές/καθηγητές αποκτούν πρόσβαση στο χώρο του μαθητικού εργαστηρίου. Η βασική διαφορά από το προηγούμενο σενάριο χρήσης των μαθητών είναι η χρήση διαφορετικής πολιτικής πρόσβασης με στόχο την απρόσκοπτη πρόσβαση στα αγαθά του σχολικού εργαστηρίου.

2.2 ΧΡΗΣΗ UAM (UNIVERSAL ACCESS METHOD) / CAPTIVE PORTAL ΣΤΗΝ ΑΣΥΡΜΑΤΗ ΠΡΟΣΒΑΣΗ

Σε αρκετές περιπτώσεις των παραπάνω σεναρίων χρήσης προτείνεται η χρήση Captive portal. Με τον όρο αυτό εννοούμε μια περιφραγμένη ιστοσελίδα (εκ του οποίου και ο όρος captive portal) από την οποία δεν μπορεί να φύγει και να πλοηγηθεί στο διαδίκτυο χωρίς επιτυχημένη ταυτοποίηση. Η χρήση captive portal ή αλλιώς UAM (Universal Access Method) με χρήση διαπροσωπίας Web είναι εξαιρετικά διαδεδομένη (π.χ. αεροδρόμια, δημοτικά ασύρματα δίκτυα κλπ) στην πρόσβαση ασύρματων τερματικών σταθμών (π.χ. παλαιών κινητών τηλεφώνων ή Η/Υ με λειτουργικό σύστημα παλιότερο του XP SP3).

Η τυπική διαδικασία ελέγχου πρόσβασης γίνεται μια φορά για κάθε νέο εισερχόμενο χρήστη από την στιγμή που εμφανίζεται σαν νέος σταθμός στο AP. Η διαδικασία έχει ως εξής:

1. Ο χρήστης προσπαθεί να επισκεφθεί με χρήση του browser ένα ιστότοπο.

2. Ο χρήστης ανακατευθύνεται σε μια περιφραγμένη ιστοσελίδα (εξού και ο όρος captive portal) από την οποία δεν μπορεί να ξεφύγει παρά μόνο εάν ταυτοποιηθεί επιτυχώς.

3. Η περιφραγμένη ιστοσελίδα αποδέχεται το συνδυασμό κωδικού/συνθηματικού του κάθε χρήστη

4. Τα διαπιστευτήρια κωδικοποιούνται με κάποια μυστική λέξη και προωθούνται με χρήση διαφόρων μεθόδων π.χ. Radius [Radius] κλπ στην υποδομή ταυτοποίησης για περαιτέρω επιβεβαίωση.

5. Με βάση την απάντηση (δλδ. απόρριψη ή αποδοχή) ο χρήστης είτε ανακατευθύνεται στην αρχική σελίδα που ήθελε να επισκεφθεί είτε του παρουσιάζεται διαγνωστικό μήνυμα λάθους ταυτοποίησης και επιστρέφει για νέα δοκιμή ταυτοποίησης.

Η χρήση του UAM μπορεί να ενσωματωθεί είτε σε κάθε Access Point -AP μέσω του Firmware είτε να υλοποιηθεί για ομάδες AP σε ξεχωριστή μονάδα/server που ονομάζεται με τον γενικό όρο wireless Controller.

2.2.1 Ταυτοποίηση με χρήση κεντρικού captive portal

Η υλοποίηση ενός κεντρικού captive portal για όλα τα σχολεία αποτελεί μια πρόκληση με σημαντικό βαθμό δυσκολίας. Η δυσκολία από την μια αφορά το φορτίο της κίνησης που θα πρέπει να φιλτράρει αυτό το portal και απο την άλλη την δυσκολία να συγκεντρωθεί η κίνηση απο όλα τα ασύρματα δίκτυα και μόνο αυτά, και να οδηγηθεί στο portal.

Παρόλαυτά, θεωρούμε ότι είναι τεχνικά εφικτό να γίνει κάτι τέτοιο και μάλιστα με την υπάρχουσα δικτυακή υποδομή του ΠΣΔ και ότι η λύση αυτή έχει πολλά και σημαντικά πλεονεκτήματα που δεν περνάνε εύκολα απαρατήρητα.

Το πρώτο στάδιο για την υλοποίηση ενός κεντρικού portal είναι η συγκέντρωση της κίνησης όλων των ασυρμάτων δικτύων και η δρομολόγηση αυτής της κίνησης προς το captive portal. Σε αυτό το στάδιο θα χρειαστούν σημαντικές αλλαγές στο δίκτυο διανομής του ΠΣΔ. Η κατάσταση διευκολύνεται απο το γεγονός ότι το μεγάλο πλήθος των δρομολογητών των σχολείων συγκεντρώνεται στους LNS. Οι βασικές αρχές της μεθόδου είναι οι εξης:

- Επιλογή της κίνησης των ασύρματων δικτύων κοντά στο σημείο παραγωγής της (access δίκτυο). Αυτό μπορεί να γίνει με μαρκάρισμα της κίνησης με κάποια DSCP τιμή, στον σχολικό δρομολογητή, είτε στον LNS στον οποιο συνδέεται ο ADSL δρομολογητής. Εναλλακτικά μπορούμε σε κάποιο κεντρικό σημείο του δικτύου, από όπου περνάει όλη η κίνηση των σχολείων, να γίνεται η επιλογή μέσω μιας ip access list, εφόσον τα ασύρματα δίκτυα έχουν ανατεθεί απο εννιαία address blocks και μπορεί να δημιουργηθεί μια access list λογικού μεγέθους.
- Η επιλεγμένη αυτή κίνηση μέσω policy routing μπορεί να δρομολογηθεί προς ένα διαφορετικό next hop, στο οποίο βρίσκεται το portal.

Εφόσον η κίνηση οδηγηθεί στο captive portal, μπορούν όλες οι κλήσεις προς το web να ανακατευθυνθούν προς τον web server του portal, στο οποίο θα ταυτοποιούνται οι χρήστες. Η τεχνολογία αυτή είναι γενικά γνωστή και δεν θα επεκταθούμε παραπάνω.

Στο δεύτερο στάδιο θα πρέπει οι ταυτοποιημένοι χρήστες να βγαίνουν ελεύθερα (με τους όρους του ΠΣΔ) στο internet. Αυτό σημαίνει ότι πρέπει πλέον να επιλέξουμε τους ταυτοποιημένους χρήστες (δηλαδή την IP του κάθε χρήστη) και να τους επιτρέψουμε να βγουν στο internet. Δεδομένου ότι γίνεται ένας σχεδιασμός για χιλιάδες χρήστες, δεν είναι λογικό η κίνηση τους να περνάει μέσα απο το portal. Συνεπώς προτείνεται μια λύση που θεωρούμε ότι μπορεί να αντεπεξέλθει στο φορτίο της κίνησης και στην λογική της διαρκούς εισόδου/εξόδου χρηστών στο ασύρματο δίκτυο. Οι βασικές αρχές της λύσης αυτής είναι οι εξης:

- Ενας software BGP daemon (server) διαφημίζει σε ένα δρομολογητή, όλους τους χρήστες που έχουν ταυτοποιηθεί επιτυχημένα (/32 routes με τις IPs των χρηστών). Ο BGP daemon συνεργάζεται με το captive portal για να μαθαίνει τις IP των ταυτοποιημένων χρηστών. Θα μπορούσε ο BGP daemon αυτός να τρέχει στο ίδιο μηχάνημα με το captive portal. Η διαφήμιση μέσω BGP, χιλιάδων routes, είναι κάτι συνηθισμένο και δεν δημιουργεί πρόβλημα στο δρομολογητή.
- Ο δρομολογητής που λαμβάνει αυτά τα /32 routes των ταυτοποιημένων χρηστών, έχει στο interface εισόδου της κίνησης, ενεργοποιημένο ένα χαρακτηριστικό που στην cisco λέγεται QPPB (QoS Policy Propagation via BGP). Με το QPPB, ο

δρομολογητής μπορεί να ελέγχει την source IP διεύθυνση του κάθε πακέτου που μπαίνει στο interface και εφόσον αυτή είναι μέσα στα /32 routes, μαρκάρει το πακέτο με μια IP Precedence τιμή. Στον επόμενο στάδιο, στο ίδιο interface, μπορεί μέσω policy routing, να αλλάξει το nexthop του πακέτου έτσι ώστε να δρομολογηθεί προς το internet χωρίς να περάσει απο το portal.

Με τον παραπάνω τρόπο, μπορούμε για χιλιάδες χρήστες να οδηγούμε τα IP πακέτα των μην ταυτοποιημένων χρηστών, προς το portal, ενω των ταυτοποιημένων χρηστών να μην περνάνε μέσα απο το portal.

2.2.2 Συγκριση λύσεων captive portal στην ασύρματη συσκευή και κεντρικού captive portal

Η υλοποίηση ενός κεντρικού captive portal σε σ΄χεση με την λειτουργία του captive portal πάνω στην ασύερματη συσκευή, διαφέρει πολύ και ως προς την υλοποίηση, αλλά και ως προς το user experience. Τα βασικά πλεονεκτήματα και μειονεκτήματα της κάθε λύσης φαίνονται παρακάτω:

- Το κεντρικό portal, παρέχει μια εννιαία εμπειρία σε όλους τους χρήστες του ΠΣΔ. Η χρήση captive portal πάνω στο AP, ενδέχεται να διαφοροποιεί την εμπειρία του χρήστη, επειδή μπορεί να διαφέρουν οι συσκευές, αλλά και να παρέχουν λιγότερες δυνατότητες.
- Το κεντρικό captive portal, έχει πλήρεις δυνατότητες και καλύτερο έλεγχο των χρηστών. Δεδομένου ότι θα τρέχει πάνω σε κάποιο πλήρες λειτουργικό σύστημα, θα μπορεί να ενσωματωθεί σε αυτό, οποιαδήποτε τεχνολογία προκύψει τώρα και στο μέλλον (SSO κ.α.).
- Στην υλοποίηση του κεντρικού captive portal, ενδέχεται να είναι δύσκολο να περιοριστεί η επικοινωνία των μη-ταυτοποιημένων χρηστών, μεταξύ τους και μεταξύ διαφορετικών σχολείων. Δηλαδή, ένας μη-ταυτοποιημένος χρήστης του σχολείου Α, θα μπορεί να επικοινωνήσει με έναν άλλο χρήστη στο ΠΣΔ, εκτός και αν περιοριστεί η πρόσβαση με ACL για όλους του χρήστες (ταυτοποιημένους και μη). Αυτό δεν

ισχύει για captive portal πάνω στο AP, όπου η σχεδίαση δεν επιτρέπει τέτοια επικοινωνία.

- Το captive portal πάνω στο AP, είναι μια λύση που εφόσον πληρεί τις προδιαγραφές, υλοποιείται πιο εύκολα και δεν χρειάζεται μεγάλες αλλαγές στο δίκτυο κορμού του ΠΣΔ. Παρόλαυτά, η λύση αυτή εξαρτάται από το μοντέλο του AP και την προσέγγιση του κατασκευαστή του AP, στο θέμα portal. Για να είναι επιτυχής μια μαζική εγκατάσταση, θα πρέπει να βασίζεται σε έναν το πολύ δύο κατασκευαστές.
- Η υλοποίηση ενός κεντρικού captive portal, μπορεί να σημαίνει σημαντικές αλλαγές στην λειτουργία του δικτύου κορμού. Η αύξηση της πολυπλοκότητας του δικτύου κορμού, μπορεί να σημαίνει με την σειρά της, δυσκολότερη υλοποίηση άλλων χαρακτηριστικών και υπηρεσιών στο δίκτυο του ΠΣΔ (πχ ipv6).

2.2.3 Ταυτοποίηση με χρήση τεχνικών WEB-XML σε captive portal

Μια εναλλακτική μέθοδος για την πιστοποίηση χρήση σε περιβάλλον UAM/captive portal είναι η χρήση σε γλώσσα XML του πρωτόκολλου ταυτοποίησης SAML[1] [SAML] σε περιβάλλον www. Το εν λόγω πρωτόκολλο υλοποιείται από το λογισμικό shibboleth του Internet2. Το σημαντικό χαρακτηριστικό του shibboleth είναι οτι επιτρέπει Single Sign On (SSO) την ανάθεση του συστήματος ταυτοποίησης ενός web server (εν προκειμένω του UAM) το οποίο στην ορολογία του SAML/Shibboleth ονομάζεται Service Provider), σε έναν άλλο web server το οποίο δρά ως ένα μοναδικό σημείο ταυτοποίησης (IDP- IDentity Provider).

Με δεδομένο οτι στο ΠΣΔ λειτουργεί η υπηρεσία SSO τίθεται το ερώτημα κατά πόσο μπορεί να χρησιμοποιηθεί σε συστήματα captive portal. Εν γένη δεν υπάρχουν πολλά συστήματα που να υλοποιούν shibboleth identity federation. Τα γνωστά σε μας είναι:

- CoovaChilli

[1] http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

- Kanet, [αναφορά]
- NoCatAuth
- PepperSpot , με patch, [αναφορά]
- Ucopia, [αναφορά]

Το Kanet μπορεί να ρυθμιστεί να λειτουργεί με χρήση CAS/Shibboleth/Radius. Το PepperSpot μπορεί να ρυθμιστεί να παρέχει και IPv6 διευθύνσεις εκτός από IPv4. Το CoovaChilli και το noCatAuth μπορούν να παραμετροποιηθούν με τις κατάλληλες αλλαγές όπως αναφέρεται στην σελίδα του shibboleth.

2.2.4 Χρήση της τεχνολογίας Radius για ταυτοποίηση σε captive portal

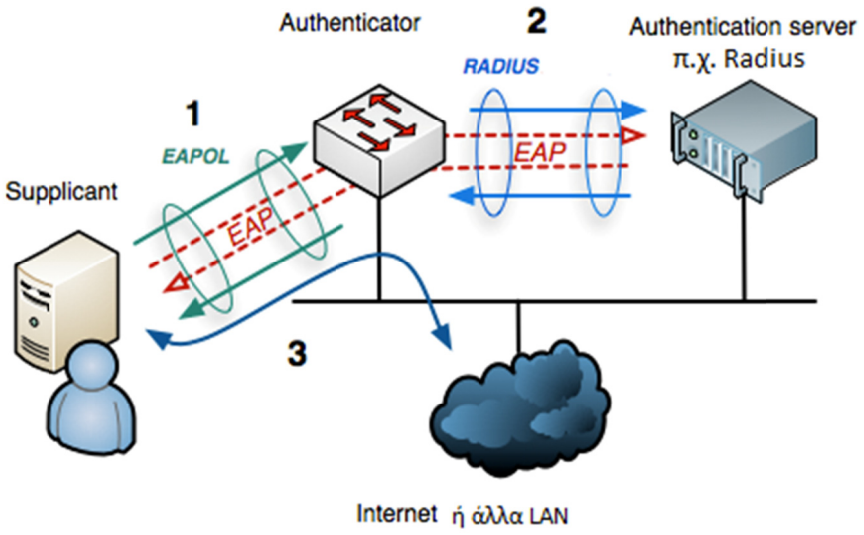
Η τεχνολογία Radius [Radius] μπορεί να χρησιμοποιηθεί ως βασικός μηχανισμός ταυτοποίησης των χρηστών δεδομένου ότι υποστηρίζεται πλήρως από την υποδομή του ΠΣΔ. Εν τούτοις χρειάζεται προσοχή στη ρύθμιση του συνθηματικού του radius (secret) αφού οι radius client είναι αρκετοί στο πλήθος και διαμοιρασμένοι εν δυνάμει σε όλα τα σχολεία, γεγονός που καθιστά την υποδομή AAA οιονεί ευάλωτη. Αυτό το θέμα ξεφεύγει από τα όρια της παρούσης μελέτης και αποτελεί αντικείμενο της μελέτης AAA.

3. ΧΡΗΣΗ ΤΟΥ 802.1X[2] ΓΙΑ ΤΑΥΤΟΠΟΙΗΣΗ ΣΤΟ ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΟ

Όπως φάνηκε σε προηγούμενη ενότητα η ταυτοποίηση χρηστών σε ένα ασύρματο δίκτυο προϋποθέτει από τον χρήστη εργαλείων όπως ο browser. Η IEEE με την σύσταση 802.1x [8021X] πρότεινε ένα νέο μηχανισμό ο οποίος θα ενσωματώνεται στην ασύρματη τεχνολογία πρόσβασης. Το πρωτόκολλο 802.1x ανήκει στην σουίτα των πρωτοκόλλων 802 της IEEE και προδιαγράφει την δυνατότητα ταυτοποιημένης χρήσης ενός τοπικού δικτύου ανεξαρτήτων του φυσικού μέσου (ενσύρματου ή ασύρματου). Ως εκ τούτου στην περίπτωση των ασύρματων δικτύων 802.1 b/g/n η χρήση του πρωτοκόλλου 802.1x εφαρμόζεται χωρίς καμιά τροποποίηση.

Το πρωτόκολλο ταυτοποίησης 802.1x περιλαμβάνει τρείς συντελεστές: τον τελικό χρήστη της τερματικής συσκευής ή λογισμικού ο οποίος στην ορολογία του προτύπου ονομάζεται supplicant (επειδή τροφοδοτεί τα απαραίτητα διαπιστευτήρια π.χ. ζεύγος κωδικού/συνθηματικού, ψηφιακό πιστοποιητικό), τον ταυτοποιητή (authenticator) ο οποίος είναι στην γενική περίπτωση ένας ασύρματος ή ενσύρματος μεταγωγέας πρόσβασης, και τον εξυπηρετητή ταυτοποίησης (authentication server), οποίος στην δική μας περίπτωση είναι η υποδομής ΑΑΑ του ΠΣΔ η οποία βασίζεται στην τεχνολογία Radius.

[2] http://en.wikipedia.org/wiki/802.1X



Σχήμα 1 Σχηματική παράστασης ταυτοποίησης σε ασύρματο δίκτυο

Ο ταυτοποιητής λειτουργεί σαν φύλακας και δεν επιτρέπει την πρόσβαση στο δίκτυο για τον τελικό χρήστη εάν δεν λάβει μήνυμα από το σύστημα ταυτοποίησης οτι ο χρήστης έχει παρέχει τα σωστά διαπιστευτήρια.

Το πρωτόκολλο 802.1x χρησιμοποιεί την τεχνολογία EAP (Extensible Authentication Protocol) [EAP] η οποία επιτρέπει μεταξύ άλλων: α) την ειδοποίηση του τελικού χρήστη για την ανάγκη ταυτοποίησης β) την μεταφορά των διαπιστευτηρίων σε ένα εξυπηρετητή ταυτοποίησης και γ) την επιλογή της μεθόδου ταυτοποίησης ως αντικείμενο διαπραγμάτευσης μεταξύ συσκευής/λογισμικού χρήστη και του εξυπηρετητή ταυτοποίησης. Όταν η επικοινωνία γίνεται μεταξύ τελικού χρήστη και ταυτοποιητή η πληροφορία ενθυλακώνεται σε ειδικού τύπου πακέτα Ethernet (EAPoL - EAP over LAN), ενώ στην περίπτωση προώθησης των διαπιστευτηρίων στον τελικό εξυπηρετητή η επικοινωνία γίνεται μέσω ειδικού τύπου πακέτα Radius.

Το συνολικό σενάριο εξελίσσεται ως εξής:

1. Αρχικά ο χρήστης επιλέγει μέσω της τερματικής συσκευής του (supplicant) την συσχέτιση με ένα ασύρματο δίκτυο.

2. Ο ταυτοποιητής τον ειδοποιεί οτι χρειάζεται να παρέχει διαπιστευτήρια (μέσω ενός ειδικού πακέτου EAP).

3. Ο τελικός χρήστης ενθυλακώνει τα διαπιστευτήρια και τα στέλνει στον φύλακα ταυτοποίησης με πακέτα EAPoL.

4. Ο φύλακας τα παραλαμβάνει, τα ενθυλακώνει σε πακέτα ειδικού τύπου πακέτα Radius και τα προωθεί στην υποδομή AAA για έλεγχο.

5. Ο ταυτοποιητής παραλαμβάνει την απάντηση και αναλόγως επιτρέπει ή αρνείται την πρόσβαση.

4. ΕΠΙΛΟΓΗ ΤΗΣ ΜΕΘΟΔΟΥ ΤΑΥΤΟΠΟΙΗΣΗΣ ΓΙΑ 802.1Χ

Η χρήση του EAP στην επιλογή ταυτοποίησης επιτρέπει στον σχεδιαστή της υπηρεσίας WiFi να επικεντρώσει στις δυνατότητες του λογισμικού των τερματικών σταθμών αφού ο ταυτοποιητής δεν εμπλέκεται στην επιλογή της μεθόδου ταυτοποίησης παρά μόνο στην υλοποίησης της ασφάλειας επικοινωνίας (π.χ. κρυπτογράφηση) της ασύρματης επικοινωνίας. Με δεδομένο οτι η υποδομή ΑΑΑ του ΠΣΔ υποστηρίζει τις παρακάτω μεθόδους

- EAP-MD5: χρησιμοποιεί τον αλγόριθμο MD-5 για κρυπτογράφηση του συνθηματικού (password). Αυτή η μέθοδος δεν προτείνεται εξαιτίας προβλημάτων ασφάλειας του αλγορίθμου MD5
- EAP-TLS (Transport Layer Security) δημιουργεί ένα προστατευμένο κανάλι επικοινωνίας με χρήση της τεχνολογίας TLS με ταυτοποίηση με certificates τόσο από τον server όσο και από τον client. Αυτό σημαίνει οτι πρέπει να αποδοθούν πιστοποιητικά σε κάθε χρήστη γεγονός που μπορεί να εισάγει μεγάλο διαχειριστικό φορτίο.
- EAP-PEAP (Protected EAP) δημιουργεί επίσης ένα κανάλι ασφαλούς επικοινωνίας τεχνολογίας TLS για την μεταφορά των μηνυμάτων EAP. Η ταυτοποίηση του καναλιού απαιτεί μόνο την ταυτοποίηση του server (όπως συμβαίνει με την επίσκεψη ενός browser σε web site με μέθοδο https). Η μέθοδος EAP-PEAP χρησιμοποιεί ως μέθοδος μεταφοράς κρυπτογράφησης των διαπιστευτηρίων (Password) το MS-CHAPv2 το οποίο χρησιμοποιείται κατά βάση από Directory servers της Microsoft. Η μέθοδος αυτή είναι προεγκατεστημένη στους χρήστες με λειτουργικό σύστημα XP SP3 και πάνω. Επιπλέον βάση της χρήσης MS-CHAPv2 παρέχεται η δυνατότητα άσκησης πολιτικής χρόνου γήρανσης στα ήδη χρησιμοποιούμενα password.
- EAP-TTLS (Tunneled TLS) παρέχει τα ίδια χαρακτηριστικά ασφαλείας με τις προηγούμενες δύο μεθόδους. Το πλεονέκτημα αυτής της μεθόδου είναι οτι παρέχει ελευθερία στην μέθοδος ταυτοποίησης ανάλογα με τα μηνύματα radius. Με αυτό τον τρόπο υπάρχει δυνατότητα χρήσης passwords αποθηκευμένα με PAP.

Μέθοδος	Πρόβλημα	Επιπτώσεις	Πιθανό όφελος
EAP-MD5	Δεν υπάρχει επαρκής ασφάλεια	μπορεί να διαφύγουν τα passwords	Δεν υπάρχει
EAP-TLS	Απαιτείται παροχή πιστοποιητικών σε όλους τους τελικούς χρήστες	Μεγάλο διαχειριστικό φορτίο στην υπηρεσία PKI	Οι χρήστες αποκτούν και certificate για άλλες υπηρεσίες
EAP-PEAP	Χρειάζεται αποθήκευση των passwords σε μορφή NTLM	Δεν υπάρχει, δεδομένου οτι τα passwords αποθηκεύονται σε δύο μορφές στην υπηρεσία καταλόγου.	Δεν χρειάζεται πρόσθετο λογισμικό στους τελικούς χρήστες με λειτουργικό σύστημα MS.
EAP-TTLS	Δεν υπάρχει εγγενής υποστήριξη σε περιβάλλον MS windows	Χρήση ξεχωριστού client σε υπολογιστές με λειτουργικό σύστημα από Windows XP SP3 και πάνω.	Χρήση roaming

Στην επιλογή της μεθόδου ταυτοποίησης χρήσιμα είναι και τα δεδομένα που αφορούν την ωριμότητα των λύσεων και τα προβλήματα τους καθώς θα επηρεάσουν αφενός την ευκολία εφαρμογής της λύσης και αφετέρου την φορτίο που θα δεχθεί το Helpdesk για την αντιμετώπιση των προβλημάτων. Ενδεικτικά:

- Τα Windows XP, Windows Vista, Windows 7 υποστηρίζουν 802.1X για όλες τις συνδέσεις δικτύου εξορισμού. Τα Windows 2000 έχουν υποστήριξη από την

τελευταία έκδοση service pack (SP4) ενώ τα Windows Mobile 2003 και πάνω έχουν εγγενή υποστήριξη 802.1X.

- Υπάρχει ένα open source project με όνομα Open1X το οποίο έχει δημιουργήσει μια υλοποίηση πελάτη με το όνομα Xsupplicant ο οποίος είναι διαθέσιμος για Windows Linux.
- Mac OS X έχει ενγενή υποστήριξη από την έκδοση 10.3. Τα iPhone και iPod Touch υποστηρίζουν 802.1X από την έκδοση iOS 2.0.

Αναφορικά με την ωριμότητα των λύσεων ενδεικτικά αναφέρονται τα παρακάτω προβλήματα και οι λύσεις που έχουν προταθεί.

4.1 Προβληματα υλοποιησης 802.1X στις διαφορες εκδοσεις των Windows

4.1.1 Windows

Οι γενικές ρυθμίσεις των Windows έχουν καταχωρήσει την τιμή των 20 λεπτών για κάθε νέα δοκιμή μετά από μια αποτυχημένη δοκιμή. Αυτό επιφέρει σημαντικές δυσκολίες στον τρόπο λειτουργίας της υπηρεσίας. Ευτυχώς αυτός ο χρόνος μπορεί να ρυθμιστεί με αλλάζοντας την τιμή της μεταβλητής BlockTime στην registry. Χρειάζεται όμως hotfix για να αλλάξει αυτή η τιμή από σταθερή σε προγραμματιζόμενη στα Windows XP SP3 και Windows Vista SP2[3].

Δεν υποστηρίζονται πιστοποιητικά server τύπου Wildcard server από το υποσύστημα EAPHost που υλοποιεί το EAP στο λειτουργικό σύστημα, ως αποτέλεσμα χρειάζονται εξατομικευμένα πιστοποιητικά για κάθε server.

4.1.2 Windows XP

Τα Windows XP μερικές φορές παρουσιάζουν προβλήματα όταν χρειάζεται να συνδεθούν (winlogon) σε DC μετά την αλλαγή διευθύνσεων IP κατά την οποία αλλάζει και το VLAN και άρα το subnet. Αυτό το πρόβλημα εντοπίζεται στους χρήστες με roaming profiles και μπορεί

[3] http://support.microsoft.com/kb/957931

να διορθωθεί με hotfix. Ένα συμπληρωματικό πρόβλημα εντοπίζεται σε χρήστες με χρήση του PEAP και PEAP-MSCHAPv2 όταν έχουν mandatory user profiles και συνδέονται σε NPS (network policy server είναι το προϊόν Radius) της Microsoft. Παρόμοια έχει εκδοθεί hotfix για την επίλυση αυτού του προβλήματος.

4.1.3 Windows Vista & 7

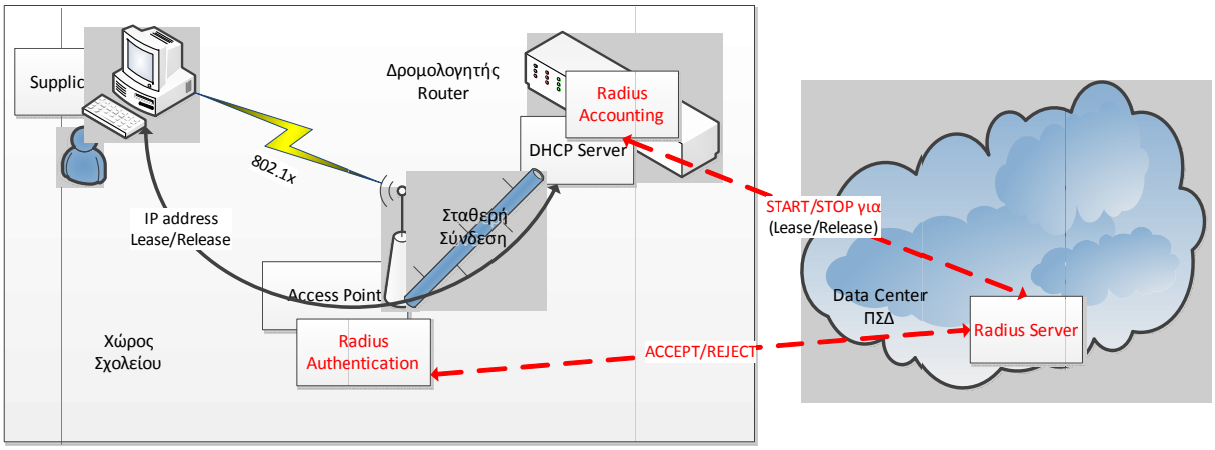
Η/Υ με λειτουργικά Windows Vista οι οποίοι συνδέονται μέσω ενσύρματων μεταγωγέων 802.1X σε ένα δίκτυο μπορεί να μην καταφέρουν να επανασυνδεθούν μετά από hybernate ή sleep. Υπάρχει hotfix για αυτό το πρόβλημα[4].

[4] http://support.microsoft.com/kb/976373

5. Το 802.1x για το ΠΣΔ με SSID edusch

Η χρήση της τεχνολογία 802.1x στο ΠΣΔ σε συνδυασμό με την ταυτοποίηση με χρήση Radius επιτρέπει δυνητικά την πρόσβαση κάθε μαθητή σε οποιοδήποτε ασύρματο δίκτυο με την τεχνολογία 802.1x και WPA/WPA2 Enterprise σε οποιοδήποτε σχολείο στην Ελλάδα. Αυτό είναι πολύ σημαντικό επειδή δεν περιορίζει την πρόσβαση τοπικά για τους μαθητές αλλά εντάσει στο μαθητή την έννοια μιας ομάδας χρηστών σε ολόκληρη την γεωγραφική επικράτεια. Ειδικότερα στα πλαίσια του ΠΣΔ προτείνουμε την χρήση ενός SSID π.χ. **edusch** το οποίο θα είναι ενιαίο σε όλα τα σχολεία. Αυτό το SSID θα έχει ενιαία πολιτική χρήσης π.χ. θα επιτρέπει την χρήση αρκετών αλλά όχι όλων των πρωτοκόλλων (π.χ. IMAPS(tcp_995), POPS(tcp_993), HTTP(tcp_80), HTTPS(tcp_443), SMTPS, ssh(tcp:22), sftp κλπ)

Καθώς η χρήση του ασύρματου δικτύου εκτιμάται να είναι μαζική θα απαιτηθεί καταγραφή του διευθύνσεων των χρηστών. Εφόσον οι διευθύνσεις δεν είναι εξατομικευμένες για κάθε χρήστη (όπως είναι π.χ. για την περίπτωση των δρομολογητών των σχολείων) αλλά χρησιμοποιείται κάποια λίστα διευθύνσεων, θα χρειαστεί να υπάρχει εγγραφή για κάθε νέα δέσμευση και απόλυση διεύθυνσης. Η δέσμευση και η απόλυση των διευθύνσεων για τους ασύρματους σταθμούς δεν γίνεται όμως μέσω του πρωτοκόλλου radius (όπως είναι π.χ. για την περίπτωση των δρομολογητών των σχολείων) αλλά μέσω του πρωτοκόλλου DHCP (Dynamic Host Configuration Protocol)). Στην περίπτωση των ασύρματων σημείων ο radius client είναι το AP το οποίο δεν συμμετέχει στην διαδικασία απόδοσης διευθύνσεων στα τερματικά σημεία (supplicants), επειδή δρά ως συσκευή επιπέδου 2. Οι δρομολογητές των σχολείων χρησιμοποιούνται ως DHCP (Dynamic Host Configuration Protocol) servers με πελάτες τα ασύρματα τερματικά σημεία.



Σχήμα 2 Καταγραφή Διευθύνσεων από DHCP μέσω Radius

Για κάθε απόδοση και απόλυση διεύθυνσης οι δρομολογητές θα πρέπει να ενημερώνουν την κεντρική υποδομή AAA/ΠΕΚ. Απαιτείται ως εκ τούτου να ρυθμιστούν οι δρομολογητές των σχολείων (Cisco) με εντολές που θα επιτρέπουν την καταγραφή. Ενδεικτικά για λειτουργικό IOS 12.2(15)T και νεώτερα:

```
Router(config)# configure terminal
Router(config)# aaa new-model
Router(config)#radius-server host <ip_address> acct-port 1646 key lab
Router(config)#radius-server key lab
!
Router(config)#aaa accounting network default start-stop group radius
Router(config)#aaa accounting update periodic 1
Router(config)#interface ethernet 1/0/1
Router(int ethernet1/0/1)#accounting dhcp source-ip aaa list default
end
```

ή

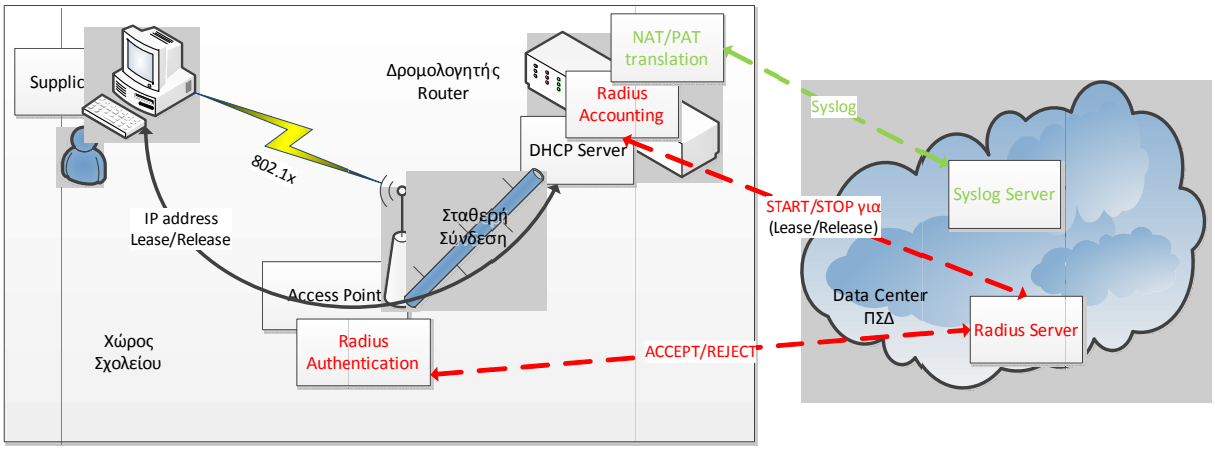
```
aaa new-model
aaa group server radius RGROUP-1
```

```
 server <ip_address> auth-port 1645 acct-port 1646
 exit
aaa accounting network RADIUS-GROUP1 start-stop group RGROUP-1
aaa session-id common
ip radius source-interface Ethernet0
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
exit
```

6. ΔΙΑΣΥΝΔΕΣΗ ΜΕ ΤΟ EDUROAM ΣΤΗΝ ΕΛΛΑΔΑ ΚΑΙ ΣΤΟ ΕΞΩΤΕΡΙΚΟ

Η χρήση της τεχνολογίας 802.1x, και radius επιτρέπει την διασύνδεση οργανισμών σε ένα χαλαρό συσχετισμό τύπου συνομοσπονδίας (confederation) κάνοντας χρήση περιαγωγής των στοιχείων ταυτοποίησης κατά τον οποίο οποιοδήποτε μέλος της συνομοσπονδίας μπορεί να αποκτά πρόσβαση σε ασύρματο δίκτυο υπό την προϋπόθεση ότι ο οργανισμός που ανήκει δέχεται όρους και πολιτική καλής χρήσης του δικτύου και επιπλέον πολιτικές προώθησης στοιχείων ταυτοποίησης (π.χ. username) σε περίπτωση κακόβουλης χρήσης. Η συνομοσπονδία έχει αποδειχθεί εξαιρετικά δημοφιλής σε ολόκληρη την Ευρώπη και σε μεγάλο μέρος του κόσμου. Η ύπαρξη δυνατότητας roaming στους χρήστες Wifi εμφανίζεται με την ύπαρξη ενός ασύρματου δικτύου με SSID: **eduroam**.

Στην προηγούμενη ενότητα δόθηκαν τα στοιχεία που χρειάζονται για την καταγραφή των ιδιωτικών διευθύνσεων μέσω του πρωτοκόλλου DHCP από την υποδομή AAA μέσω του πρωτοκόλλου Radius. Το ζητούμενο στην υλοποίηση του eduroam (το οποίο άπτεται πολιτικής έγκρισης) είναι οι δυσκολίες εφαρμογής του επικεντρώνονται στην αναζήτηση της αντιστοίχησης από ιδιωτικές σε δημόσιες διευθύνσεις της τεχνολογίας NAT/PAT που χρησιμοποιούνται στους σχολικούς δρομολογητές. Σε αυτή την περίπτωση απαιτείται η καταγραφή της αντιστοίχισης. Αυτό προτείνεται να γίνει μέσω υποδομής syslog. Το syslog είναι μια πληροφοριακού τύπου υπηρεσία η οποία μπορεί να ρυθμιστεί να καταγράφει αυθαίρετο τύπο και είδος συμβάντων σε κάθε συσκευή που το υποστηρίζει. Εν προκειμένω υποστηρίζεται στο λειτουργικό IOS από την έκδοση 12.4(2)



Σχήμα 3 Καταγραφή αντιστοίχηση ιδιωτικής σε δημόσια διεύθυνση μέσω υποδομής Syslog για το ssid eduroam

Στο παραπάνω σχήμα φαίνεται σε επαλληλία οι καταγραφές αντιστοίχησης με κόκκινα και πράσινα στοιχεία. Για την ακριβή ταυτοποίηση της χρήσης μιας δημόσιας διεύθυνσης IP χρειάζεται:

- (προαιρετικά)την καταγραφή των στοιχείων χρήσης του transparent proxy
- την καταγραφή των στοιχείων χρήσης μετάφρασης NAT/PAT
- την καταγραφή των στοιχείων απόδοσης/απόλυσης διευθύνσεων μέσω DHCP

Για την ενεργοποίηση της μετάφρασης χρειάζεται η τροποποίηση του configuration όπως φαίνεται στην συνέχεια.

```
Router(config)# logging on   # ενεργοποίηση logging

Router(config)# service timestamps log localtime msec year #φορμάτ μηνυμάτων logging

Router(config)# no logging console # απενεργοποίηση του logging στην κονσόλα

Router(config)# logging <sys_log_server_IP_address> #ρύθμιση του server

Router(Config)# ip nat log translations syslog # ενεργοποίηση της αποστολής μηνυμάτων τύπου NAT
```

```
12:17:12.503:    %IPNAT-6-NAT_CREATED:    Created    tcp    10.0.0.1:43800
10.17.3.32:1024                 192.168.0.1:80                 10.17.3.2:80
12:18:47.751:    %IPNAT-6-NAT_DELETED:    Deleted    tcp    10.0.0.1:43800
10.17.3.32:1024 192.168.0.1:80 10.17.3.2:80
```

Δεν έχει εκτιμηθεί το φορτίο που θα επιφέρει αυτή η αλλαγή στον δρομολογητή και την γραμμή πρόσβασης του κάθε σχολείου.

Για τους χρήστες του σχολικού δικτύου σημαίνει οτι κάθε φορά που βλέπουν ένα ασύρματο δίκτυο στην Ελλάδα ή στο εξωτερικό με όνομα **eduroam** θα μπορούν με χρήση του κωδικού <user>@sch.gr και του συνθηματικού τους να αποκτούν πρόσβαση στο τοπικό δίκτυο.

7. ΥΠΟΔΟΜΗ

7.1 ΚΟΜΒΟΙ ΠΡΟΣΒΑΣΗΣ – ACCESS POINTS

7.1.1 Χαρακτηριστικά Access Points

Για την ασύρματη πρόσβαση των ασύρματων τερματικών σταθμών απαιτείται η ύπαρξη κόμβων πρόσβασης (Access Points - AP) τα οποία υλοποιούν την λειτουργικότητα δικτύου IEEE 802.11. Στην παρούσα μελέτη ενδιαφερόμαστε κατά βάση για υποστήριξη του IEEE **802.11 b/g/n** με προτεραιότητα στα πιο σύγχρονα **g/n** και λιγότερο στο παλαιότερο **b** το οποίο δεν κάνει καλή χρήση της διαθέσιμης χωρητικότητας. Είναι υποχρεωτικό τα AP να υλοποιούν την λειτουργικότητα των πολλαπλών SSID ή virtual AP για διαφοροποιημένη πρόσβαση με βάση κριτήρια πολιτικής (π.χ. ανάλογα με την ομάδα που ανήκουν οι χρήστες δλδ. καθηγητές/μαθητές) ή για λόγους τεχνικής διαφοροποίησης των μεθόδων πρόσβασης (π.χ. Web σε αντιπαράθεση με ειδικούς clients) ή για λόγους ασφάλειας. Τέλος στην παρούσα φάση κρίνεται απαραίτητη η υποστήριξη ασφάλισης της ασύρματης πρόσβασης με βάση το πρότυπο WPA2 Enterprise και λιγότερο με το WPA για την χρήση εξατομικευμένου κωδικού χρήσης. Η προαιρετική αποδοχή του WPA μπορεί να δείχνει ανούσια δεδομένου της υποχρεωτικής WPA2 αλλά γίνεται για να μπορούν να λειτουργούν τερματικοί σταθμοί με παλιού τύπου λογισμικό.

Συνοπτικά τα παραπάνω χαρακτηριστικά φαίνονται στον ακόλουθο πίνακα.

Υποστήριξη IEEE 802.11g/n	Υποχρεωτικό
Υποστήριξη IEEE 802.11b	Προαιρετικό
Υποστήριξη IEEE WMM	Προαιρετικό
Υποστήριξη WPA-PSK with TKIP/AES, WPA2-PSK με AES	Υποχρεωτικό
Υποστήριξη WPA Enterprise/WPA2 Enterprise	Υποχρεωτικό
Υποστήριξη 802.1x	Υποχρεωτικό
Πολλαπλά SSID ή virtual AP, τουλάχιστον 4	Υποχρεωτικό
Υποστήριξη ξεχωριστής προφίλ ασφαλείας σε κάθε SSID.	Υποχρεωτικό
Υποστήριξη δυνατότητας συσχέτισης SSID με VLAN	Υποχρεωτικό
Υποστήριξη EAP στο 802.1x και διαφανή προώθηση του EAP στο δηλωμένο RADIUS server	Υποχρεωτικό
Υποστήριξη Radius (client). Δυνατότητα δήλωσης περισσότερων απο έναν radius servers.	Υποχρεωτικό
Δυνατότητα ορισμού προφίλ ασφάλειας σε ένα SSID ενός απο τα ακόλουθα: WPA-PSK/TKIP/AES, WPA2-PSK /AES, WPA Enterprise,WPA2 Enteprise,no security	Υποχρεωτικό
Υποστήριξη VLANs. Τουλάχιστον 4.	Υποχρεωτικό

Υποστήριξη 802.1q trunking για σύνδεση του AP σε μια πόρτα του σχολικού δρομολογητή	Υποχρεωτικό
Υποστήριξη Radius accounting για όλες τις περιπτώσεις που χρησιμοποιείται ο Radius	Υποχρεωτικό
Διαχείριση μέσω telnet ή/και ssh	Υποχρεωτικό
Αποθήκευση και ανάκληση ρυθμίσεων μέσω εξωτερικού πρωτοκόλλου (π.χ. ftp, tftp, http κλπ)	Υποχρεωτικό
captive portal (εφόσον αποφασιστεί ότι δεν θα γίνει κεντρικό portal)	Υποχρεωτικό
Χρήση Radius για την ταυτοποίηση χρηστών στο captive portal	Υποχρεωτικό
WDS ή άλλο Mesh protocol	Προεραιτικό

Πίνακας 1 Χαρακτηριστικά AP

7.2 ΔΙΕΥΘΥΝΣΙΟΔΟΤΗΣΗ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΠΣΔ

Το κάθε σχολικό εργαστήριο στο ΠΣΔ, αυτή την στιγμή χρησιμοποιεί ένα μοναδικό /24 ιδιωτικό δίκτυο, για το LAN του. Το δίκτυο αυτό χρησιμοποιείται για όλους τους υπολογιστές και τον/τους server του σχολικού εργαστηρίου. Το δίκτυο αυτό γίνεται τοπικά NAT απο τον δρομολογητή του σχολείου, όταν βγαίνει προς το internet. Το NAT γίνεται με την χρήση ενός μπλοκ τεσσάρων μοναδικών πραγματικών διευθύνσεων (/30), το οποίο ανατίθεται στο σχολείο και ρυθμίζεται στο δρομολογητή.

Δεδομένου ότι είναι δύσκολο να χωριστεί το ιδιωτικό δίκτυο του σχολείου σε δύο μικρότερα /25, προτείνεται να γίνει απόδοση ενός νέου ιδιωτικού δίκτυου /24 απο τον hostmaster του ΠΣΔ, για την κάθε ασύρματη υπηρεσία που δίνει ένα AP, δηλαδή ένα για κάθε SSID. Είναι

σημαντικό τα δίκτυα που θα αποδοθούν απο τον hostmaster να προέρχονται απο εννιαία address blocks, έτσι ώστε να είναι εύκολο με μια λίστα ασφαλείας να επιλέξεις τα δίκτυα αυτά. Τα ασύρματα δίκτυα αναμένεται να διαφοροποιούνται σε σχέση με τα ενσύρματα σε διάφορους τομείς, όπως είναι ο web proxy του ΠΣΔ, το τοίχος προστασίας (firewall), η δρομολόγηση, το logging, οπότε και η απόδοση απο εννιαία address blocks ιδιαίτερα σημαντική.

Το κάθε δίκτυο που θα ανατίθεται σε σχολείο θα πρέπει να ενημερώνεται στην βάση του ΠΣΔ καθώς και στον LDAP του ΠΣΔ, για να μπορεί να λειτουργεί χωρίς πρόβλημα.

7.3 ΛΟΓΙΣΜΙΚΟ ΔΙΑΧΕΙΡΙΣΗΣ

Η ύπαρξη τόσου μεγάλου αριθμού AP δημιουργεί ανάγκες για την μαζική διαχείριση. Έχουν εμφανιστεί συστήματα λογισμικού που ονομάζονται ελεγκτές (controller) για την μαζική διαχείριση των ασύρματων σταθμών πρόσβασης. Οι απαιτήσεις διαχείρισης είναι :

- αναπαράσταση σε χάρτη
- αναπαράσταση κατάστασης λειτουργίας με ενδεικτικά χρώματα (π.χ. πράσινο, κόκκινο κλπ)
- Λειτουργίες συγκρότησης (π.χ. μαζική αναβάθμιση, τροποποίηση κλπ

7.3.1 Απόδοση κωδικών χρήσης ασύρματου δικτύου

Σε αυτή την ενότητα θα σχεδιαστεί ο μηχανισμός (λογικό διάγραμμα) απόδοσης κωδικών χρήσης στους μαθητές:

- αίτηση με συμπλήρωση φόρμας
- δημιουργία κωδικού χρήσης και μοναδικού αναγνωριστικού (UUID)
- έγκριση από τρίτο πρόσωπο

Επέκταση εφαρμογής διαχείρισης χρηστών (ΠΔΧ) για τους χρήστες/ληξίαρχους ασύρματης υποδομής

7.3.2 Πρόσθετες Απαιτήσεις παρακολούθησης διαχείρισης

Οι πρόσθετες απαιτήσεις προκύπτουν από απαιτήσεις παρακολούθησης από μια κεντρική υπηρεσία εποπτείας. Ενδεικτικά:

- διαχείριση μέσω SNMP (v2c),
- απομακρυσμένη αναβάθμιση
- απομακρυσμένη ανάκτηση και αποθήκευση αρχείου συγκρότησης,
- περιορισμός χρηστών (αριθμητικά ή με βάση δ/νσεις MAC)

7.3.3 Λογισμικό ελέγχου Πρόσβασης (AAA)

Στο ΠΣΔ το λογισμικό ελέγχου πρόσβασης, εξουσιοδότησης καταγραφής (Authentication Authorization Accounting) θα είναι το ανοικτό λογισμικό FreeRadius v2.1.2 [FR]. Το εν λόγω λογισμικό καλύπτει εν γένει τις ανάγκες για τον έλεγχο πρόσβασης. Σε περίπτωση που χρειαστεί να χρησιμοποιηθεί λογισμικό FreeRadius έκδοσης 3.xx υπάρχει δυνατότητα κατασκευής πακέτων από το πηγαίο κώδικα αναλύεται στο σύνδεσμο http://wiki.freeradius.org/Build Από τα περιεχόμενα της σελίδας φαίνεται ότι τα λειτουργικά συστήματα debian και redhat φαίνεται ότι έχουν καλύτερη αυτοματοποίηση της διαδικασίας.

Εν προκειμένω για debian/Ubuntu ακολουθείται η παρακάτω διαδικασία:

```
User%ubuntu>sudo apt-get install dpkg-dev

User%ubuntu>sudo apt-get build-dep freeradius
```

Στην συνέχεια μεταφέρεται ο πηγαίος κώδικας από το αποθετήριο git:

```
git clone git://git.freeradius.org/freeradius-server.git
```

και ακολούθως μεταφράζεται και γίνονται πακέτα…

```
User%ubuntu>cd freeradius-server

freeradius-server> fakeroot dpkg-buildpackage -b -uc
```

```
freeradius-server>sudo dpkg -i ../*freeradius*.deb
```

7.4 ΛΟΓΙΣΜΙΚΟ ΧΡΗΣΤΩΝ

Όπως έχει αναφερθεί και στα προηγούμενα μέρη αυτής της μελέτης το λογισμικό χρήσης των περισσότερων λειτουργικών συστημάτων αναφορικά με την χρήση της τεχνολογίας 802.1x παρουσιάζει δυσκολίες στην ρύθμιση του ασύρματου. Σκοπός αυτής της ενότητας είναι να συνοψίσει όλες τις αλλαγές που χρειάζονται σε ένα συνολικό πακέτο χωρίς να χρειάζονται περίπλοκοι οδηγοί χρήσης. Το εν λόγω λογισμικό κατασκευάστηκε με βάση το SU1X από το πανεπιστήμιο του Swansea. Το λογισμικό επιτρέπει την ρύθμιση των Windows XP [SP3/vista/7/8] με τα SSID και τις απαραίτητες ιδιότητες τους για την χρήση στο σχολικό δίκτυο.

Ο πηγαίος κώδικας βρίσκεται στο https://github.com/GarethAyres/SU1X . Οι βασικές αλλαγές που έγιναν είναι: α) στα εικονίδια που εμφανίζονται στον χρήστη, β) στο ψηφιακό πιστοποιητικό και στα διαθέσιμα SSID που χρειάζεται να εισαχθούν στο τυχαίο Η/Υ του μαθητή.

Με την υπόθεση ότι ο διαχειριστής έχει ένα laptop στο οποίο έχει καταχωρήσει τα απαραίτητα ssid και το ψηφιακό πιστοποιητικό της αρχής πιστοποίησης ένα εκτελέσιμο αρχείο χρήστης ρυθμίζει α)τα ασύρματα δίκτυα για κάθε μαθητή στο περιβάλλον του ασύρματου δικτύου του σχολείου του, επιτρέπει την χρήση roaming με χρήση TTLS και PAP χωρίς να χρειαστεί ο μαθητής να ακολουθήσει μια δύσκολη διαδικασία διαμόρφωσης και εγκατάστασης λογισμικού.

8. ΔΙΑΧΕΙΡΙΣΗ ΥΠΟΔΟΜΗΣ AP ΕΝΤΟΣ ΣΧΟΛΕΙΩΝ

8.1 ΥΦΙΣΤΑΜΕΝΗ ΚΑΤΑΣΤΑΣΗ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥ ΠΣΔ ΕΝΤΟΣ ΤΩΝ ΣΧΟΛΕΙΩΝ

Στην σημερινή κατάσταση του ΠΣΔ η έννοια διαχείρισης της υποδομής πρόσβασης του σχολείου σχετίζεται μόνο με την αρωγή της συγκρότησης (configuration), της καταγραφής (registration) κωδικών πρόσβασης στην υποδομή καταλόγου **χωρίς** την παρακολούθηση (monitoring) της κατάστασης λειτουργίας του δικτύου του σχολείου. Αυτό γίνεται επειδή το ΠΣΔ δεν έχει αντίληψη της κατάσταση λειτουργίας των λειτουργικών υποδομών IT εντός του σχολείου. Η μόνη εικόνα που υπάρχει για την λειτουργία του σχολείου είναι μέσω της υποδομής ΑΑΑ/ΠΕΚ όπου καταγράφονται τα στοιχεία ταυτοποίησης/καταγραφής μέσω των εξυπηρετητών Radius. Απολογιστικά πλέον μπορεί να γίνει έλεγχος καλής λειτουργίας της υποδομής μέσω της συχνότητας καταγραφής. Η έλλειψη καταγραφών μπορεί να οδηγήσει σε προληπτικό έλεγχο, αλλά στην πλειονότητα των περιπτώσεων η παρακολούθηση λειτουργίας γίνεται κατόπιν ανακοίνωσης βλάβης.

Η παραπάνω κατάσταση θέτει τους περιορισμούς στην παρακολούθηση της υποδομής AP στο ΠΣΔ με τον επιπλέον περιορισμό ότι τα AP δεν καταγράφονται στην υποδομή καταλόγου για χρήση ταυτοποίησης.

8.2 ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΕΞΟΠΛΙΣΜΟΥ AP

Είναι σαφές ότι είναι εκτός δικαιοδοσίας των συγγραφέων της παρούσας μελέτης ο καθορισμός της πολιτικής διαχείρισης των AP παρόλα αυτά θα γίνουν μερικές προτάσεις που μπορεί να επιφέρουν αλλαγές: α) στις λειτουργικές απαιτήσεις του εξοπλισμού πρόσβασης και β) στην κεντρική υποδομή παρακολούθησης της υπηρεσίας.

ΠΡΟΤΑΣΗ 1: Καμιά παρακολούθηση λειτουργίας AP.

- Πλεονεκτήματα: Ελάχιστο κόστος συγκρότησης στους δρομολογητές πρόσβασης, Μηδενικό κόστος ανάπτυξης, καμιά επιπλέον απαίτηση στις προδιαγραφές λειτουργίας των AP.
- Μειονεκτήματα: Έλλειψη εικόνας λειτουργίας της υποδομής. Τα στατιστικά χρήσης είναι συνεπαγόμενα από τα στατιστικά χρήσης των διευθύνσεων IP μέσω του DHCP όπως αναφέρθηκε παραπάνω υπό την προϋπόθεση ότι μπορεί να εφαρμοστεί μαζικά.

ΠΡΟΤΑΣΗ 2: Ελάχιστη παρακολούθηση μέσω snmp/http και dyn-dns και script. Θεωρούμε ότι η πρόταση 2, είναι η πιο κατάλληλη για το σχήμα λειτουργίας του ΠΣΔ.

- Πλεονεκτήματα: Ελάχιστο κόστος συγκρότησης στους δρομολογητές πρόσβασης, Μικρό κόστος ανάπτυξης, επιπλέον απαίτηση στις προδιαγραφές λειτουργίας των AP για http. Βελτίωση εικόνας λειτουργίας της υποδομής. Μέσω της λειτουργίας http-dns προκύπτει κατάσταση λειτουργίας σε περιβάλλον λειτουργίας π.χ. nagios
- Μειονεκτήματα: Επιπλέον απαιτήσεις προδιαγραφών AP. Απολογιστική λειτουργία διαχείρισης χωρίς συνολική εικόνα λειτουργίας

ΠΡΟΤΑΣΗ 3: Παρακολούθηση μέσω snmp/http και dyn-dns και script και αποτύπωση σε χάρτη

- Πλεονεκτήματα: Ελάχιστο κόστος συγκρότησης στους δρομολογητές πρόσβασης, Μικρό κόστος ανάπτυξης, επιπλέον απαίτηση στις προδιαγραφές λειτουργίας των AP για http. Βελτίωση εικόνας λειτουργίας της υποδομής. Κόστος παραμετροποίησης λογισμικού συντήρησης εικόνας δικτύου
- Μειονεκτήματα: Επιπλέον απαιτήσεις προδιαγραφών AP. Πιθανή εσφαλμένη εικόνα από αυθαίρετη λειτουργία περιβάλλοντος σχολείου.

8.3 ΔΙΑΔΙΚΑΣΙΕΣ ΛΕΙΤΟΥΡΓΙΑΣ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ ΣΤΟ ΠΣΔ

8.4 ΔΙΑΔΙΚΑΣΙΕΣ ΔΗΜΙΟΥΡΓΙΑΣ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ ΣΕ ΣΧΟΛΕΙΟ

Στην ενότητα αυτή γίνεται αναφορά διαδικασίες που σχετίζονται με την υποστήριξη ασύρματου δικτύου σε ένα σχολείο.

Αρχικά, θα πρέπει να γίνει ένα αίτημα στο helpdesk του ΠΣΔ απο το σχολείο που επιθυμεί να αποκτήσει ασύρματο δίκτυο. Στο αίτημα αυτό θα πρέπει να περιλαμβάνονται τα εξης στοιχεία:

- Ονομα υπευθύνου στο σχολείο
- Δρομολογητής στον οποίο θα συνδεθεί ο εξοπλισμός (εφόσον το σχολείο διαθέτει περισσότερους απο ένα δρομολογητές)
- Μοντέλο δρομολογητή
- Μοντέλο access point, εφόσον έχει γίνει προμήθεια απο το σχολείο
- Ασύρματες υπηρεσίες που θα ενεργοποιηθούν στο σχολείο

1.

Το Helpdesk του ΠΣΔ ως απάντηση του αιτήματος θα πρέπει άμεσα να αποστέλει στο σχολείο τα εξής:

- Τις σχετικές οδηγίες που αφορούν τις προδιαγραφές του εξοπλισμού
- την τοπολογία σύνδεσης του access point στο δρομολογητή
- τις ρυθμίσεις που πρέπει να έχει το access point
- την πολιτική καλής χρήσης (AUP).

Στην συνέχεια θα πρέπει να ανοίγονται στο σχετικό δελτίο οι ακόλουθες ενέργειες προς τους φορείς διαχείρισης του ΠΣΔ:

- Ενέργεια προς τον Hostmaster του ΠΣΔ, με αίτημα την ανάθεση των ιδιωτικών /24 IP δικτύων που απαιτούνται απο τις υπηρεσίες του ασύρματου δίκτυου.
- Ενέργεια προς την ΔΟ-Database του ΠΣΔ, με αίτημα την ανανέωση του νέων δικτύων στην βάση του ΠΣΔ, καθώς και τα λοιπά στοιχεία που αφορούν το ασύρματο δίκτυο.
- Ενέργεια προς το Helpdesk του ΠΣΔ, για την εισαγωγή των κατάλληλων εγγραφών στον LDAP που θα επιτρέψουν στο νέο δίκτυο να δρομολογηθεί. Η εγγραφή αυτή θα είναι της μορφής:

2.

```
3. Cisco-AVPair := "ip:route= X.Y.Z.0 255.255.255.0 A.B.Γ.Δ"
```

4. Όπου το Α.Β.Γ.Δ είναι η loopback του δρομολογητή του σχολείου και X.Y.Z.0 είναι το νέο private δίκτυο που θα αναθέσει ο hostmaster για το ασύρματο δίκτυο του σχολείου.

- Ενέργεια προς το Helpdesk του ΠΣΔ, που θα αιτείται την κατάλληλη ρύθμιση του δρομολογητή για να λειτουργήσει το ασύρματο δίκτυο. Το εργαλείο παραγωγής ρυθμίσεων για τους δρομολογητές, θα πρέπει να μπορεί να παράγει τις σχετικές ρυθμίσεις για το συγκεκριμένο σχολείο. Αν ο δρομολογητής είναι της σειράς Cisco 87x, οι ρυθμίσεις που πρέπει να γίνουν μια ασύρματη υπηρεσία με captive portal είναι ενδεικτικά οι ακόλουθες:

```
5.
6.  ip access-list extended wlan-in
7.    permit tcp any any eq www
8.    permit tcp any any eq 443
9.    permit udp any host 194.63.239.164 eq domain
10.   permit udp any host 194.63.237.4 eq domain
11.   permit udp any host 194.63.238.4 eq domain
12.   permit udp any any eq bootps
13.   permit udp any any eq bootpc
14.   deny   ip any any
15.
16. interface FastEthernet2
```

```
17.  switchport access vlan 10
18.  no shut
19.
20. interface Vlan10
21.  ip address X.Y.Z.1 255.255.255.0
22.  ip access-group wlan-in in
23.  no shut
24.
25. ip dhcp excluded-address X.Y.Z.0 X.Y.Z.10
26.
27. ip dhcp pool wlan
28.    network X.Y.Z.0 255.255.255.0
29.    domain-name att.sch.gr
30.    default-router X.Y.Z.1
31.    netbios-node-type b-node
32.    dns-server 194.63.239.164 194.63.237.4 194.63.238.4
33.    lease 0 3
34. end
35.
36.
```

- Ενέργεια προς το σχολείο, που θα ζητά ενημέρωση για τον τύπο/μάρκα/μοντέλο του εξοπλισμού που έχει αγορασθεί και την πρόοδο των ενεργειών της φυσικής διασύνδεσης και των ρυθμίσεων του εξοπλισμού.

Με την ολοκλήρωση των παραπάνω ενεργειών το ασύρματο δίκτυο θα μπορεί να λειτουργήσει, εφόσον και το σχολείο έχει προχωρήσει στις σχετικές φυσικές συνδέσεις.

8.5 ΔΙΑΧΕΙΡΙΣΗ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ ΜΕ ΤΑ ΕΡΓΑΛΕΙΑ ΤΟΥ ΠΣΔ

Στο τρέχων πλαίσιο διαχείρισης του δικτύου του ΠΣΔ, υπάρχει μια σειρά απο εργαλεία τα οποία συμβάλλουν στην διαχείριση του δικτύου πρόσβασης του ΠΣΔ. Αυτά τα εργαλεία είναι ο radius, η βάση του ΠΣΔ, ο LDAP, το εργαλείο παραγωγής configuration για τους δρομολογητές του δικτύου πρόσβασης και άλλα. Οι λειτουργία των ασύρματων δικτύων επιβάλει την προσαρμογή των εργαλείων αυτών, για να μπορέσουν να καλύψουν τις ανάγκες των ασύρματων δικτύων.

Οσον αφορά το radius και LDAP, δεν χρειάζονται αλλαγές στον τρόπο λειτουργίας των υπηρεσιών, αλλά απλές προσθήκες εγγραφών που περιγράφονται σε άλλο σημείο της μελέτης.

Αντίστοιχα στην βάση του ΠΣΔ, θα πρέπει να δημιουργηθούν τα κατάλληλα πεδία που θα φιλοξενούν τις πληροφορίες των ασύρματων δικτύων. Πιο συγκεκριμένα πρέπει να υπάρχουν οι ακόλουθες πληροφορίες:

- Κωδικός υπηρεσίας -> SSID
- Κωδικός υπηρεσίας -> Ιδωτικό IP δίκτυο
- Κωδικός σχολείου -> IP διαχείρισης access point
- Κωδικός σχολείου -> τύπος/μοντέλο access point

Οσον αφορά το δίκτυο παραγωγής ρυθμίσεων για τους δρομολογητές πρόσβασης, θα πρέπει να γίνουν εκτεταμένες αλλαγές. Οι αλλαγές αυτές περιγράφονται πιο κάτω:

- Παραγωγή ρυθμίσεων όχι μόνο με βάση τον τύπο του δρομολογητή, αλλά και με βάση τον συνδυασμό «τυπος δρομολογητή» και «τύπος access point». Θα πρέπει το εργαλείο να διαβάζει τι υπηρεσίες είναι ενεργοποιημένες στο σχολείο και να παράγει ρυθμίσεις ειδικά για αυτό.
- Το εργαλείο θα πρέπει να παράγει τις ρυθμίσεις που αντιστοιχούν στο access point, κάτι που δεν έχει την δυνατότητα να κάνει αυτή τη στιγμή.

8.6 ΣΥΣΤΗΜΑΤΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΥΡΜΑΤΗΣ ΥΠΟΔΟΜΗΣ

8.6.1 Οφέλη-κόστος

Η ύπαρξη μεγάλου αριθμού AP θέτει εμμέσως πλην σαφώς το θέμα της διαχείρισης τους. Μια τέτοια απόφαση στο υψηλότερο επίπεδο είναι πολιτική και σε χαμηλότερο βαθμό τεχνική με θετικά και αρνητικά στοιχεία και αναμφίβολο κόστος. Η ύπαρξη διαχειριστικής εφαρμογής AP επιφέρει τα πλεονεκτήματα οικονομίας λειτουργικών πόρων (OPEX-operation expenditures) στον έλεγχο και παρακολούθηση της λειτουργίας των AP αλλά επιφέρει κόστος στο αρχικό ποσό κτήσης (Capital expenditure). Η έλλειψη μιας τέτοιας υποδομής δεν σημαίνει την παύση λειτουργίας των AP αλλά δεν επιτρέπει:

- την παρακολούθησης σε ζωντανό χρόνο της υποδομής μέσα στο σχολείο.

- μαζικές λειτουργίες αναβάθμισης και συγκρότησης

Τα προϊόντα μαζικής διαχείρισης AP αναφέρονται ως wireless controllers ενώ στην κοινότητα των δημόσιων ασύρματων δικτύων (community networks) τα ονόματα ποικίλουν αλλά κατά βάση τα συστήματα αποτελούνται από ένα υποσύστημα παρακολούθησης με ονομασία nodewatcher και από ένα απεικονιστικό υποσύστημα σε χάρτη.

8.6.2 Χρήση Wireless Controllers στο ΠΣΔ

Στο εμπόριο υπάρχουν προϊόντα που παρέχονται από εταιρίες (π.χ. Cisco κλπ) και λύσεις ανοικτού λογισμικού π.χ. Coovachili για την διαχείριση μεγάλου αριθμού AP. Στον παρακάτω πίνακα παρουσιάζονται μερικά εμπορικά προϊόντα μαζί με τους περιορισμούς τους και το κόστος υλοποίησης.

Μοντέλο	Cisco 5508	Aruba 6000	Meru Networks MC5000	ZoneDirector 5000
Αριθμός AP	200	200	200	200
Αριθμός Clients	7,000	16,000	10,000	20,000
Για υποστήριξη 1.000 APs	Πολλαπλές μονάδες & άδειες χρήσης	Πολλαπλές μονάδες & άδειες χρήσης	Πολλαπλές μονάδες & άδειες χρήσης	-
Maximum αριθμός APs	500	512/2000**	300/1500**	1000
Τιμή για (200 APs)	$65.000	$75.000	$55.000	$45.000
Τιμή για (1000 APs)	$302.000	$140.000	$150.000	$120.000

Πίνακας 2 Εμπορικά προϊόντα wireless controllers

Η μεγάλη εξάπλωση της ασύρματης τεχνολογίας WiFi εξαιτίας του χαμηλού κόστους και της έλλειψης άδεις χρήσης οδήγησε κοινότητες χρηστών να κτίσουν ασύρματα μητροπολιτικά δίκτυα. Τα ασύρματα μητροπολιτικά δίκτυα είναι κατά βάση point-to-point αλλά έχουν και AP. Πολύ σύντομα φάνηκε η απαίτηση διαχείρισης τους με όρους που έχουν αναφερθεί στα προηγούμενα (καταγραφή, συγκρότηση, παρακολούθηση). Σε ορισμένες περιπτώσεις οι ανοικτές λύσεις λογισμικού ήταν τόσο καλές που οδήγησαν στην αυτονόμηση (και το κλείσιμο των προϊόντων διαχείρισης) μαζί με την διαχείριση τους π.χ. για τα προϊόντα meraki, Fonera, open-mesh. Σε αυτά τα προϊόντα το λογισμικό διαχείρισης παρέχεται μέσω τεχνολογίας σύννεφου (cloud).

8.6.2.1 **Ανοικτά λογισμικά διαχείρισης**

Coovachili (http://coova.org/CoovaChilli)

CoovaChilli είναι ένα ανοιχτό λογισμικό ελεγκτή το οποίο βασίζεται στο ChilliSpot project το οποίο πλέον από ένα συμμετέχοντα στο ChilliSpot. Το CoovaChilli έχει πολλά χαρακτηριστικά όπως captive portal / walled-garden το οποίο χρησιμοποιεί RADIUS ή HTTP πρωτόκολλο για ενεργοποίηση πρόσβασης και χρέωση. CoovaChilli είναι ένα ενεργό μέρος του CoovaAP ενός firmware που βασίζεται στο OpenWRT ειδικό για hotspots.

Το μειονέκτημα αυτής της λύσης είναι χρειάζεται επαναπρογραμματισμός (flash) των AP.

Packetfense (http://www.packetfence.org/)

PacketFence είναι ένας μηχανισμός ελέγχου δικτύου network access control (NAC) με captive-portal για καταχώρηση επισκεπτών και χρηστών με υποστήριξη, 802.1X. Η λύση αυτή λειτουργεί μόνο για συσκευές που υποστηρίζουν ενδογενώς 802.1x

Nodeshot (https://github.com/ninuxorg/nodeshot)

Nodeshot είναι ένα εργαλείο ιστού για ασύρματα δίκτυα. Επιτρέπει στους χρήστες να προσθέσουν κόμβους και να διαχειριστούν πληροφορίες συγκρότησης (ip διευθύνσεις, ασύρματους παραμέτρους).

WNMap (http://wnmap.sourceforge.net): Wireless network map display

WNMap είναι ένα χάρτης απεικόνισης κόμβων βασισμένος σε Google και Yahoo! χάρτες. Ο χρήστης μπορεί να προσθέτει κόμβους στην Βάση δεδομένων της εφαρμογής οι οποίοι εμφανίζονται στους επισκέπτες. Συνοπτικά η εν λόγω εφαρμογή παρέχει μια συνολική εικόνα του δικτύου.

9. ΕΝΔΕΙΚΤΙΚΟ SETUP ACCESS POINT ΣΤΟ ΠΣΔ

Εχει δημιουργηθεί ένα setup ασύρματου δικτύου σε σχολείο, με βάση την παρούσα μελέτη. Δεδομένου ότι η μελέτη αυτή παρουσιάζει μια πληθώρα επιλογών που μπορούν να γίνουν για την ασύρματη πρόσβαση στο ΠΣΔ, έχουν γίνει συγκεκριμένες επιλογές για να την υλοποίηση αυτού του setup.

Το AP στο οποίο βασίζεται το setup είναι της εταιρείας Mikrotik, μοντέλο 751U-2Hnd, το οποίο τρέχει το λειτουργικό της Mikrotik, RouterOS, με license level 4. Το κόστος της συσκευής αυτής είναι περίπου 50ευρώ χωρίς ΦΠΑ. Άλλες συσκευές μπορεί να έχουν λιγότερο ή και περισσότερο ανάλογα με τις δυνατότητες τους. Θεωρούμε ότι ένα κόστος της τάξης των 50ευρώ είναι ικανοποιητικό για την παροχή ασύρματων υπηρεσιών σε ένα σχολείο.

Η συσκευή διαθέτει 2 routed πόρτες Ethernet RJ45 και ένα Ethernet switch τεσσάρων πορτών. Διαθέτει ακόμα ασύρματη κάρτα δικτύου συμβατή με το 802.11b/g/n.

Εχουν υλοποιηθεί τρία ασύρματα δίκτυα για τρείς διαφορετικές χρήσεις:

- **schoolcafe**

  Η υπηρεσία αυτή παρέχει ένα ανοιχτό ασύρματο δίκτυο, χωρίς κρυπτογράφηση, το οποίο έχει στόχο να εξυπηρετήσει τους μαθητές/καθηγητές που θέλουν να συνδεθούν ασύρματα στο internet για λόγους αναψυχής και όχι στα πλαίσια μιας εργασίας ή ενός εργαστηρίου. Μόλις οι χρήστες συνδέονται στο ανοιχτό ασύρματο δίκτυο και προσπαθήσουν να επισκεφτούν μια web σελίδα, γίνονται redirect σε ένα captive portal που έχει υλοποιηθεί εσωτερικά στο ίδιο το AP. Εκει πρέπει να δώσουν ένα username/password για να τους επιτρέψει το captive portal να βγουν στο internet.

  Οι κωδικοί (username/pass) των χρηστών μπορούν να οριστούν στο AP, αλλά είναι εφικτό να χρησιμοποιηθεί και RADIUS για την είσοδο των χρηστών, που ταιριάζει περισσότερο στο ΠΣΔ. Είναι όμως χρήσιμο, να μπορούν κάποιοι χρήστες να εισέλθουν στο ασύρματο δίκτυο με τα local user/pass, όταν δεν δουλεύει ο RADIUS για κάποιο τεχνικό λόγο.

- **schoolab**

Η υπηρεσία αυτή υλοποιεί ένα ανοιχτό ασύρματο δίκτυο, στο οποίο η ταυτοποίηση βασίζεται στο 802.1x με WPA2-Enterprise. Η ταυτοποίηση του client γίνεται σε layer2 (οπως περιγράφεται σε άλλο σημείο στο κείμενο) πάνω απο ένα κανάλι TLS και γίνεται αποκλειστική χρήση RADIUS για τους κωδικούς.

Αυτή η υπηρεσία εξυπηρετεί, τους μαθητές καθηγητές, που παίρνουν μέρος σε ένα σχολικό εργαστήριο και χρειάζονται πρόσβαση σε κάποιος τοπικούς πόρους, αλλά και πρόσβαση στο internet. Το φιλτράρισμα της πρόσβασης υλοποιείται απο μια λίστα ελέγχου που είναι πάνω στο δρομολογητή του σχολείου.

Οι χρήστες της υπηρεσίας, απολαμβάνουν υψηλότερης ποιότητας υπηρεσία, και έχουν ξεχωριστό κρυπτογραφικό κλειδί ο καθένας. Ετσι, η ασφάλεια του σχολικού εργαστηρίου γίνεται καλύτερη και ο κίνδυνος υποκλοπής user/pass ελαχιστοποιείται.

- **bathtub**

Η υπηρεσία αυτή, αντίστοιχα με το schoolcafe, εξυπηρετεί τους μαθητές/καθηγητές που θέλουν να σερφάρουν στο δίκτυο, μέσω ενός captive portal, το οποίο όμως δεν βρίσκεται τοπικά στο AP, αλλά σε ένα κεντρικό σημείο στο δίκτυο του ΠΣΔ.

Η εμπειρία του χρήστη, είναι γενικά αντίστοιχη με το schoolab, δηλαδή η ταυτοποίηση γίνεται μέσα απο το captive portal, αλλά εδώ μπορούμε να έχουμε περισσότερες δυνατότητες, όπως την λειτουργία SSO, όπου μετά την είσοδο στο captive portal, ο χρήστης μπορεί να προσπελάσει άλλους πόρους εκτός σχολείου χωρις περαιτέρω ταυτοποίηση. Επίσης είναι ευκολότερο να διαφοροποιηθεί η υπηρεσία που δίνεται στους μαθητές απο τους καθηγητές.

Οι υπηρεσίες αυτές, υλοποιουνται στο Mikrotik, μέσω πολλαπλών SSID και την λειτουργία VirtualAP του RouterOS. Το κάθε SSID έχει το δικό του security-profile. Το κάθε SSID αντιστοιχεί σε ένα VLAN που έχει δημιουργηθεί για αυτό το σκοπό στο Mikrotik. Η σύνδεση

του Mikrotik με το σχολικό δρομολογητή γίνεται σε μια συγκεκριμένη πόρτα του δρομολογητή, η οποία ορίζεται σαν trunk port με encapsulation 802.1q. Ετσι ο δρομολογητής τερματίζει τα VLANs αυτά και μπορεί να δώσει layer2 υπηρεσίες, όπως είναι το DHCP, gateway κτλ. Ειδικά το SSID schoolcafe, δεν συνδέεται σε layer-2 με τον δρομολογητή, αλλά δρομολογείται (layer3) απο το AP προς το router.

Το management interface του Mikrotik, είναι σε διαφορετικό VLAN/υποδίκτυο, από τα αντίστοιχα VLAN/υποδίκτυα των υπηρεσιών. Ετσι διασφαλίζεται η ασφάλεια της συσκευής από κακόβουλες ενέργειες και γίνεται ευκολότερη η διαχείριση της.

Η λειτουργία hotspot που διαθέτει το Mikrotik, είναι αρκετά ευέλικτη ώστε να μπορείς να δημιουργήσεις την δικιά σου σελίδα login, χωρίς να στερείται σημαντικά σε δυνατότητες.

Οσον αφορά την διαχείριση του Mikrotik στο πλαίσιο της διαχείρισης χιλιάδων τέτοιων συσκευών, η συσκευή διαθέτει αρκετές ευκολίες. Οι ρυθμίσεις της μπορούν να εξαχθούν ή εισαχθούν σε ένα text αρχείο, που μάλιστα είναι εύκολο να διαβαστεί από ένα script. Διαθέτει SNMP για την εξαγωγή στατιστικών και άλλων πληροφοριών για την κατάσταση της και είναι διαχειρίσιμη από command line.

10. ΑΝΑΦΟΡΕΣ

[Radius] RFC 2865 Remote Authentication Dial In User Service (RADIUS)

[SAML] http://saml.xml.org/

[8021X] 802.1X-2004 - Port Based Network Access Control

[EAP] Extensible Authentication Protocol , RFC 5247

[FR] Free Radius http://freeradius.org