ΤΕΙ ΚΗΡΗΤΗΣ
Σχολή Εφαρμοσμένων Επιστημών
Τμήμα Ηλεκτρονικών Μηχανικών Τ.Ε

Ανάπτυξη και διαχείριση ασύρματου συστήματος επικοινωνιών με μηχανισμούς ασφάλειας και περιαγωγής

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Τσαϊρίδης Μιχάλης

Επιβλέπων : Δρ. Μπαρμπουνάκης Ιωάννης

Χανιά 2014

Ευχαριστίες

Θα ήθελα κατ' αρχήν να ευχαριστήσω, τον επιβλέποντα Καθηγητή Εφαρμογών του τμήματος Ηλεκτρονικής της Σχολής Εφαρμοσμένων Επιστήμων του Τ.Ε.Ι Κρήτης, κ. Μπαρμπουνάκη Ιωάννη, για τις πολύτιμες συμβουλές και κατευθύνσεις που μου παρείχε, για την ολοκλήρωση αυτής της πτυχιακής εργασίας.
Επίσης θα ήθελα να ευχαριστήσω τους φίλους μου Βαγγέλη Μαραντίδη, Αλέξανδρο Μελάκη για την πολύτιμη βοήθειά τους.
Τέλος θα ήθελα να ευχαριστήσω την οικογένειά μου για την ηθική στήριξη και την υπομονή τους.

Περίληψη

Η παρούσα πτυχιακή εργασία παρουσιάζει τη σχεδίαση, ανάπτυξη και παραμετροποίηση ενός συστήματος ασύρματων επικοινωνιών, με μηχανισμούς ασφάλειας και περιαγωγής για διασύνδεση στο διαδίκτυο.

Προηγείται η παρουσίαση της προϋπάρχουσας εγκατάστασης και ακολουθεί η περιγραφή της νέας υπηρεσίας ασύρματου δικτύου και συγκεκριμένα των προαπαιτούμενων εφαρμογών (Iptables, FreeRadius, Dhcpd).
Στη συνέχεια παρουσιάζονται σταδιακά οι φάσεις της εγκατάστασης και παραμετροποίησης, ώστε να προσαρμόσουμε την υποδομή στις προδιαγραφές που θέτει το eduroam.

Τέλος, καλύπτεται η παραμετροποίηση της υποδομής των Access Points, με τη νέα υλοποίηση όπως και η τοποθέτησή τους στην τελική θέση ώστε να επεκταθεί η ασύρματη κάλυψη για τη Σχολή Εφαρμοσμένων Επιστημών, του Τεχνολογικού Εκπαιδευτικού Ιδρύματος Κρήτης στα Χανιά.

Abstract

This thesis presents the design, development and configuration of a wireless communication system with security and roaming mechanisms for internet interconnection.

At first we present the prior installed wireless service and then we described the new eduroam compatible wireless service, primarily the prerequisite applications (Iptables, FreeRadius, Dhcpd).

Then gradually presented the phases of installation and configuration to adapt the infrastructure to the standards of the eduroam.

Finally, it covers the configuration of the infrastructure of Access Points with the new implementation as well as their placement in the final position to extend the wireless coverage to the Faculty of Applied Sciences in Chania, Technological Educational Institute of Crete.

Πίνακας περιεχομένων

1 Εισαγωγή

1.1Σκοπός Εργασίας

Η παρούσα πτυχιακή έχει ως σκοπό την ανάλυση του υφιστάμενου ασύρματου δικτύου της Σχολής Εφαρμοσμένων Επιστημών του ΤΕΙ Κρήτης και παράλληλα την ανάπτυξη της υποδομής σε υλικό και λογισμικό, αφενός για να ακολουθεί πιο σύγχρονα πρότυπα ασφαλούς διασύνδεσης και αφετέρου να γίνει συμβατό με τις προδιαγραφές που θέτει το διαπανεπιστημιακό δίκτυο eduroam.

Στο πλαίσιο της παρούσας πτυχιακής εργασίας, μελετήθηκε η αναδιοργάνωση του εγκατεστημένου ασύρματου δικτύου. Μέσα σε αυτό συμπεριλαμβάνονται η υποδομή, η τοπολογία, η παραμετροποίηση των Σημείων Ασύρματης Πρόσβασης, οι περιοχές κάλυψης, ο τρόπος χρήσης και η σύνδεση των χρηστών σε αυτό. Κατά την πορεία της πτυχιακής εργασίας ανατέθηκε η αρμοδιότητα της διαχείρισης, συντήρησης και επίβλεψης του προυπάρχοντος συστήματος.

Για μια πλήρη γεωγραφική κάλυψη, ελήφθησαν μετρήσεις ανά τακτά χρονικά διαστήματα και με κριτήριο την καλύτερη εξυπηρέτηση του ασύρματου χρήστη χρησιμοποιήθηκαν προσωπικές συσκευές ασύρματης δικτύωσης, με το ανάλογο λογισμικό μετρήσεων.

Επίσης κατά την αναδιοργάνωση του ασύρματου δικτύου, διαπιστώθηκε η ανάγκη ενός πιο εξελιγμένου και πιο ασφαλούς συστήματος πιστοποίησης χρηστών, το οποίο υλοποιήθηκε ώστε να αξιοποιείται, για την εξυπηρέτηση των χρηστών του ασύρματου δικτύου της Σχολής Εφαρμοσμένων επιστήμων του ΤΕΙ Κρήτης .

Το νέο σύστημα υποστηρίζει επιπλέον τη δυνατότητα περιαγωγής σε εκπαιδευτικά ιδρύματα σε όλη την Ευρώπη, εφόσον είναι και αυτά μέλη της παγκόσμιας υπηρεσίας eduroam.

1.2Γενικά για το Wi-Fi

Ένα ασύρματο δίκτυο είναι ένα τηλεπικοινωνιακό δίκτυο, συνήθως τηλεφωνικό ή υπολογιστικό, το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς πληροφορίας. Τα δεδομένα λοιπόν μεταφέρονται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα που εξαρτάται κάθε φορά από το ρυθμό μετάδοσης δεδομένων, που απαιτείται να υποστηρίζει το δίκτυο. Η ασύρματη επικοινωνία έχει ως μέσο μετάδοσης τη γήινη ατμόσφαιρα ή το διάστημα, σε αντίθεση με την ενσύρματη επικοινωνία, όπου το μέσο μετάδοσης είναι κάποιος τύπος καλωδίου. Σε παλαιότερες εποχές τα τηλεφωνικά δίκτυα ήταν αναλογικά, αλλά σήμερα όλα τα ασύρματα δίκτυα βασίζονται σε ψηφιακή τεχνολογία και επομένως, κατά μία έννοια, αποτελούν ουσιαστικά δίκτυα υπολογιστών.

Η εξέλιξη των ασύρματων επικοινωνιών τα τελευταία χρόνια έχει δείξει, ότι είναι πολύ δύσκολο ένα σύστημα να μπορέσει να ικανοποιήσει όλες τις ανάγκες του χρήστη και να προσαρμοστεί στις ιδιαιτερότητες κάθε περιβάλλοντος. Για το λόγο αυτό, τα ασύρματα δίκτυα των ερχόμενων γενεών θα αποτελούνται από την

ενοποίηση ενός συνόλου τεχνολογιών, κάθε μια από τις οποίες θα εξειδικεύεται σε ένα συγκεκριμένο περιβάλλον.

Η ασύρματη τεχνολογία εκμεταλλεύεται τις δωρεάν και μη αδειοδοτούμενες ραδιοσυχνότητες στις περιοχές των 2.4GHz και 5GHz.Ενώ τα πρωτόκολλα 802.11b και 802.11g, χρησιμοποιούν τη συχνότητα 2.4MHz, το 802.11a χρησιμοποιεί τη συχνότητα 5GHz και το πρωτόκολλο 802.11n χρησιμοποιεί και τις 2 περιοχές ραδιοσυχνοτήτων .

Η αρχιτεκτονική του συστήματος καλύπτει τόσο δομημένες τοπολογίες (κυψελωτές) όσο και αδόμητες . Βασικό της στοιχείο είναι ο σταθμός (Station - STA), δηλαδή οποιαδήποτε συσκευή που διαθέτει μια διεπαφή συμβατή με το πρότυπο IEEE 802.11 και επιθυμεί να συνδεθεί και να μεταδώσει στο σύστημα. Στις δομημένες τοπολογίες, η μετάδοση γίνεται μόνο από/προς το Σημείο Πρόσβασης (Access Point - AP), δηλαδή του σταθμού εκείνου που διαθέτει και διεπαφή με σταθερό δίκτυο (π.χ., Ethernet), ενώ στις αδόμητες απευθείας, σε οποιοδήποτε άλλο σταθμό, στην περιοχή κάλυψης. Το σύνολο των σταθμών και σημείων πρόσβασης που αποτελούν ένα ασύρματο δίκτυο WiFi ονομάζεται Basic Service Set (BSS) στις δομημένες τοπολογίες και Independent Basic Service Set (IBSS) στις αδόμητες.
Η εξέλιξη του προτύπου ακολούθησε μια βήμα-προς-βήμα προσέγγιση, σύμφωνα με την οποία, στην αρχή σχεδιάστηκε ένα απλό σύστημα περιορισμένης σχετικά λειτουργικότητας και στη συνέχεια επεκτάθηκε, και συνεχίζει να επεκτείνεται με προσθήκες, οι οποίες στόχο έχουν να βελτιώσουν αρχικές αδυναμίες και παραλήψεις. Παρακάτω αναφερόμαστε συνοπτικά στις βασικές εξελίξεις.

- 802.11:Η πρώτη έκδοση του προτύπου, η οποία υποστήριζε ταχύτητα 1 και 2Mbps στη ζώνη των 2,4GHz, με χρήση τεχνικών frequency hopping και direct sequence.
- 802.11a: Επέκταση φυσικού επιπέδου για ασύρματα τοπικά δίκτυα στη ζώνη των 5 GHz, το οποίο χρησιμοποιεί διαμόρφωση Orthogonal Frequency Division Multiplexing (OFDM). Αποτελείται από οκτώ διαθέσιμα μη επικαλυπτόμενα ασύρματα κανάλια, τα οποία έχουν ρυθμό μετάδοσης έως 54 Mbps το καθένα.
- 802.11b: Επέκταση φυσικού επιπέδου για ασύρματα τοπικά δίκτυα στη ζώνη των 2,4 GHz. Είναι υπεύθυνο για την αναβάθμιση του αρχικού φυσικού επιπέδου του 802.11 προσθέτοντας τους ρυθμούς 5.5 Mbps και 11 Mbps μέσω πυκνότερης διαμόρφωσης. Αποτελείται από τρία διαθέσιμα μη επικαλυπτόμενα ασύρματα κανάλια, τα οποία έχουν ρυθμό μετάδοσης έως 11 Mbps το καθένα.
- 802.11e: Είναι ένα συμπληρωματικό πρωτόκολλο για το επίπεδο πολλαπλής πρόσβασης του 802.11 το οποίο παρέχει βελτιωμένη ποιότητα υπηρεσίας. Στοχεύει σε μια από τις βασικές αδυναμίες του κλασσικού 802.11 πρωτοκόλλου, δηλαδή στην έλλειψη δυνατότητας παροχής διαφοροποιημένης μεταχείρισης σε διαφορετικές κατηγορίες κίνησης.
- 802.11g: Πρότυπο φυσικού επιπέδου για ασύρματα τοπικά δίκτυα στη ζώνη των 2,4 GHz. Αποτελείται από τρία διαθέσιμα μη επικαλυπτόμενα ασύρματα κανάλια, τα οποία έχουν ρυθμό μετάδοσης έως 54 Mbps το καθένα με χρήση OFDM. Είναι το πιο διαδεδομένο πρότυπο φυσικού επιπέδου σήμερα.

- 802.11i: Είναι ένα συμπληρωματικό πρότυπο για βελτίωση της ασφάλειας του συστήματος. Παρέχει έναν εναλλακτικό μηχανισμό του κλασσικού Wired Equivalent Privacy - WEP με καινούριες μεθόδους κρυπτογράφησης και πιστοποίησης.
- 802.11n, το οποίο με χρήση πολλαπλών κεραιών (μέθοδος γνωστή ως MIMO, εκ του Multiple Inputs Multiple Outputs) παρέχει ονομαστικό ρυθμό μετάδοσης μέχρι και 150Mbps.
- 802.11ac αναπτύχθηκε στο πλαίσιο των προτύπων της διαδικασίας της IEEE παρέχοντας ασύρματα δίκτυα υψηλής απόδοσης, ρυθμό μετάδοσης μέχρι και 866.7Mbps, στη ζώνη συχνοτήτων 5 GHz . Το πρότυπο αναπτύχθηκε από το 2011 μέχρι το 2013 και εγκρίθηκε τον Ιανουάριο του 2014. Σύμφωνα με μια μελέτη, οι συσκευές με τις προδιαγραφές 802.11ac αναμένεται να είναι διαθέσιμες από το δεύτερο εξάμηνο 2014, με ραγδαίο ρυθμό εξάπλωσης .

1.3 Σημερινή Εγκατάσταση

Η παρούσα εγκατάσταση του Ασύρματου Δικτύου αποτελείται από 10 Access Points τα οποία καλύπτουν τις κτιριακές υποδομές της Σχολής Εφαρμοσμένων Επιστημών και συγκεκριμένα την κτιριακή υποδομή στα Χανιά. Για τις ανάγκες μιας πιο εξελιγμένης και ασφαλούς υπηρεσίας, αναπτύχτηκε το eduroam.
Το eduroam είναι ένα διεθνές δίκτυο περιαγωγής (roaming) συστημάτων ασύρματης πρόσβασης μέσω διαδικτύου, το οποίο αναπτύχθηκε για τη διεθνή ακαδημαϊκή και ερευνητική κοινότητα

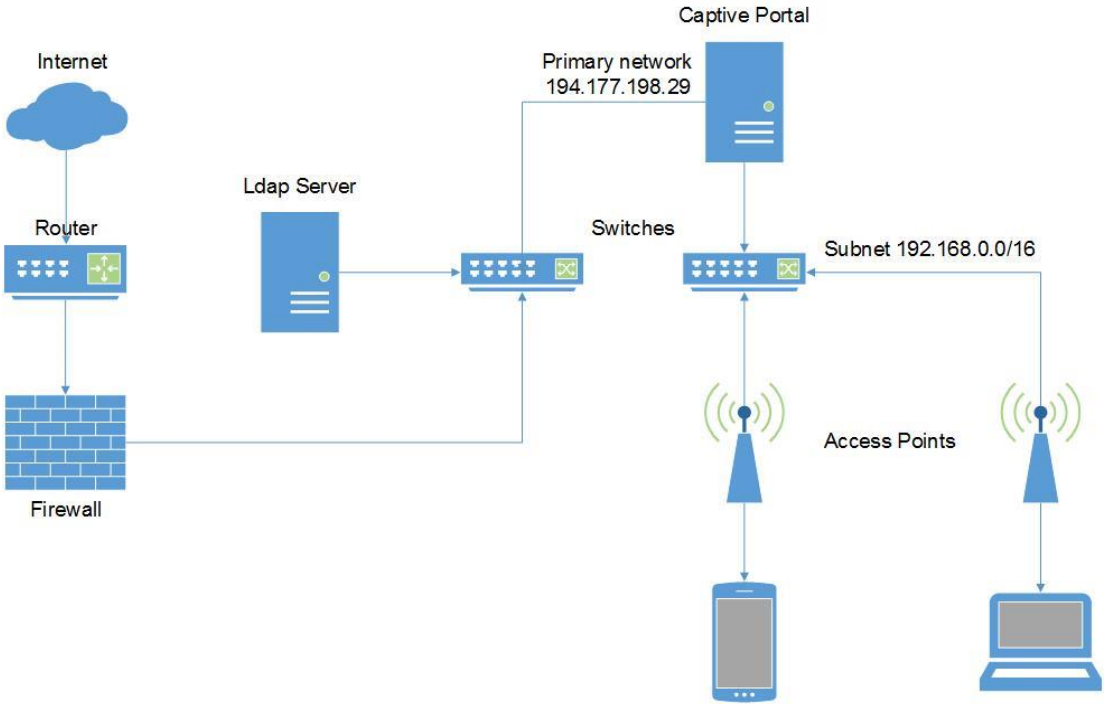
Διασυνδέει ένα πλήθος από ακαδημαϊκά ιδρύματα και προσφέρει δωρεάν πρόσβαση στο διαδίκτυο. Χρήστες από όλη την Ευρώπη έχουν τη δυνατότητα να χρησιμοποιούν τις υπηρεσίες που προσφέρουν τα ιδρύματα, μέσω της υποδομής του eduroam. Έτσι χρήστες που επισκέπτονται άλλα ιδρύματα στην Ελλάδα ή στο εξωτερικό, τα οποία είναι μέλη της υπηρεσίας eduroam, μπορούν να χρησιμοποιούν δωρεάν την πρόσβαση στο διαδίκτυο, κάνοντας χρήση των κωδικών, που τους διαθέτει το ίδρυμά τους.

Το eduroam μέσω της πολιτικής του, εξασφαλίζει την ασφαλή μετάδοση των δεδομένων του χρήστη και προσδιορίζει ένα πλαίσιο συνεργασίας μεταξύ των ιδρυμάτων, που ευνοεί την ανταλλαγή υπηρεσιών και διευκολύνει τους χρήστες, όταν αυτοί βρίσκονται σε ξένα ιδρύματα.

2 Προηγούμενη Εγκατάσταση

2.1 Προηγούμενη Εγκατάσταση Ασύρματης Πρόσβασης

Στην προηγούμενη εγκατάσταση παροχής ασύρματης πρόσβασης στην ακαδημαϊκή κοινότητα της Σχολής Εφαρμοσμένων Επιστημών, κεντρικό ρόλο έπαιζε ένας διακομιστής με την ονομασία Captive Portal. Βασικός του ρόλος ήταν η διαχείριση των ασύρματων συνδέσεων και η ενσύρματη διασύνδεση των σημείων πρόσβασης (AP) στο δίκτυο κορμού της Σχολής. Με την ιδιότητα του firewall, απομόνωνε την κυκλοφορία των ασύρματων δεδομένων και τα διοχέτευε μέσω του μοναδικού σημείου διασύνδεσης, όπου μπορούσαν να εφαρμοστούν τα πρόσθετα επίπεδα ασφαλείας, μέσω της χρήσης ενός ιδιωτικού δικτύου, όπως φαίνεται παρακάτω:



Εικόνα 1 Captive Portal

Η διαχείριση του ασύρματου δικτύου της Σχολής γινόταν από μια υπηρεσία γνωστή ως captive portal. Η τεχνική του Captive Portal δεν κάνει χρήση των κοινών πρωτοκόλλων κρυπτογράφησης σε επίπεδο καναλιού (WPA, WEP, κλπ), αλλά χρησιμοποιεί λύσεις λογισμικού, που κρυπτογραφούν τα στοιχεία της σύνδεσης σε υψηλότερο δικτυακό επίπεδο. Παρεμβάλλεται μεταξύ του διαδικτύου (Internet) και του δικτύου που θέλουμε να παρέχουμε ελεγχόμενη πρόσβαση και ανακατευθύνει τον κάθε χρήστη που συνδέεται σε μία ειδική σελίδα πιστοποίησης μέσω του περιηγητή ιστού (web browser), χωρίς να του επιτρέπει πλήρη πρόσβαση στους πόρους του δικτύου, μέχρι να πιστοποιηθεί. Ένα captive portal, διαμορφώνει τον περιηγητή ιστού σε μια εφαρμογή πιστοποίησης. Αυτό γίνεται με το να παρεμποδίζει όλα τα πακέτα δεδομένων από τη χρονική στιγμή που ο χρήστης συνδέεται και

αποκτά IP διεύθυνση, μέχρι να ανοίξει τον περιηγητή ιστού και ολοκληρώσει την διαδικασία πιστοποίησης. Σε αυτό το σημείο ο περιηγητής ιστού ανακατευθύνεται από το captive portal σε μια ιστοσελίδα όπου του ζητείται η εισαγωγή ονόματος χρήστη και συνθηματικού (password), προκειμένου για πιστοποίηση ή απλά να του εμφανίζεται η πολιτική χρήσης και να απαιτείται από τον χρήστη να συμφωνήσει με αυτή. Σε ορισμένες περιπτώσεις, ενδέχεται μαζί με την πιστοποίηση, να εφαρμόζεται και πολιτική χρήσης με πληρωμή της παρεχόμενης υπηρεσίας. Η τεχνική captive portal χρησιμοποιείται κατά κόρον στα Wi-Fi hotspots. Ωστόσο, μπορεί να υλοποιηθεί το ίδιο επιτυχημένα και για τον έλεγχο της ενσύρματης δικτύωσης (πχ. σε ενοικιαζόμενα διαμερίσματα, δωμάτια ξενοδοχείων, επαγγελματικούς χώρους) αλλά ταυτόχρονα και για τους δύο παραπάνω τρόπους διασύνδεσης.

Το Captive Portal παρεμβάλλεται μεταξύ του κεντρικού δρομολογητή (router) και του υποδικτύου στο οποίο θέλουμε να παρέχουμε ελεγχόμενη πρόσβαση, λειτουργώντας σαν κεντρική πύλη για το υποδίκτυο, αναλαμβάνοντας να διανέμει δυναμικά IP διευθύνσεις στους χρήστες. Για να περιορίσει την πρόσβαση στο υποδίκτυο, μπλοκάρει όλα τα εξερχόμενα πακέτα από την IP του χρήστη. Μόνο όταν ο χρήστης υποβάλλει ένα αίτημα https στην προκαθορισμένη θύρα 443, ανακατευθύνεται στην ιστοσελίδα μιας web εφαρμογής (στην προκειμένη περίπτωση την αποκαλούμε Authentication Server), προβάλλοντας στο χρήστη μια σελίδα πιστοποίησης και επιτρέποντάς του να εισάγει τα πιστοποιητικά του. Αν ο χρήστης εισάγει τα σωστά πιστοποιητικά τότε το Captive Portal προωθεί τα εξερχόμενα πακέτα IP έξω από το προστατευόμενο υποδίκτυο. Όλες οι αλληλεπιδράσεις μεταξύ του περιηγητή ιστού του χρήστη και του Authentication Server, είναι κρυπτογραφημένες για να αποφευχθεί η υποκλοπή τους στο ασύρματο δίκτυο.

2.2 Υλικό (hardware)

Για την υλοποίηση του Captive Portal, χρησιμοποιήθηκε ένας υπολογιστής ως διακομιστής. Στον υπολογιστή εγκαταστάθηκαν δύο κάρτες δικτύου. Η μία συνδέει τον διακομιστή με το υποδίκτυο ασύρματης υποδομής και η άλλη με το πρωτεύον δίκτυο του ΤΕΙ για πρόσβαση στην υπηρεσία του ldap και στο διαδίκτυο.

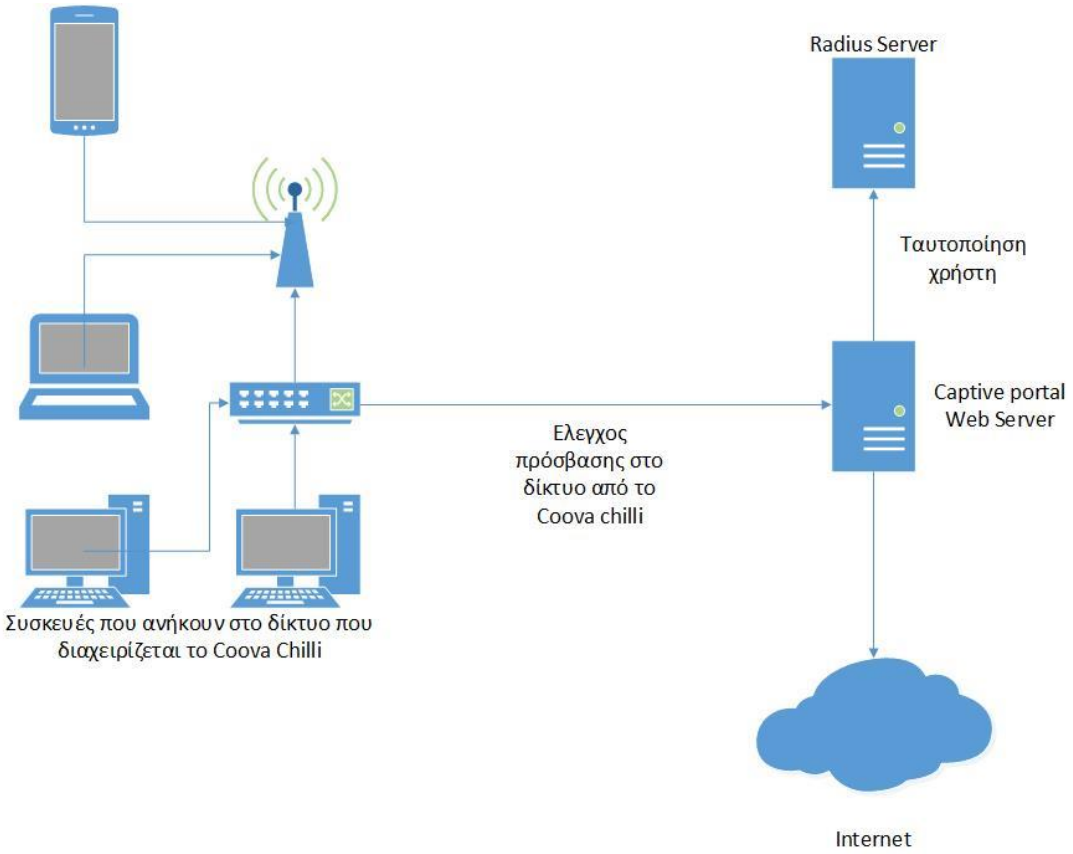
2.3 Λογισμικό

Στο διακομιστή ήταν εγκατεστημένο το λειτουργικό σύστημα Linux Ubuntu Server **8.04**, LTS. Το Coova-chilli αποτελούσε το κυρίως κομμάτι της υλοποίησης. Παρείχε DHCP Server για τη δυναμική διάθεση των IP διευθύνσεων στους χρήστες, τον

Freeradius που αναλάμβανε την πιστοποίηση (Authentication), την εξουσιοδότηση (Authorization), καθώς και την καταγραφή της χρήσης του δικτύου ανά λογαριασμό χρήστη (Accounting). Επίσης, ενσωμάτωνε εγκατεστημένο τον Apache web server, που ήταν υπεύθυνος για την επικοινωνία με τον τελικό χρήστη, καθώς και τον MySql Server, για την καταγραφή του ιστορικού πρόσβασης σε μια βάση δεδομένων. Για τη διαχείριση της βάσης του ιστορικού χρήσης(logs), εγκαταστάθηκε η εφαρμογή web Daloradius, που αποτελεί ένα σύνολο από php scripts και επιτρέπει την διαχείριση της βάσης με γραφικό τρόπο μέσα από τον περιηγητή ιστού.

2.4 Περιγραφή του Coova-Chilli

Το Coova-chilli είναι ένα λογισμικό ελέγχου πρόσβασης ανοικτού κώδικα, που χρησιμοποιείται ευρέως στις υλοποιήσεις ασύρματων σημείων πρόσβασης. Προσφέρει πολλές δυνατότητες και χρησιμοποιεί το δικτυακό πρωτόκολλο Radius για την παροχή πρόσβασης και παρακολούθησης. Σαν εφαρμογή αποτελείται από τρία βασικά υποσυστήματα, ένα υποσύστημα για τη διασύνδεση των χρηστών και την ανάθεση IP διευθύνσεων μέσω DHCP, ένα για την πιστοποίηση χρηστών μέσω Radius Server και ένα τρίτο για τη σύνδεση με το κοινόχρηστο δίκτυο και την προώθηση της κίνησης από και προς τα άλλα δίκτυα (firewall).

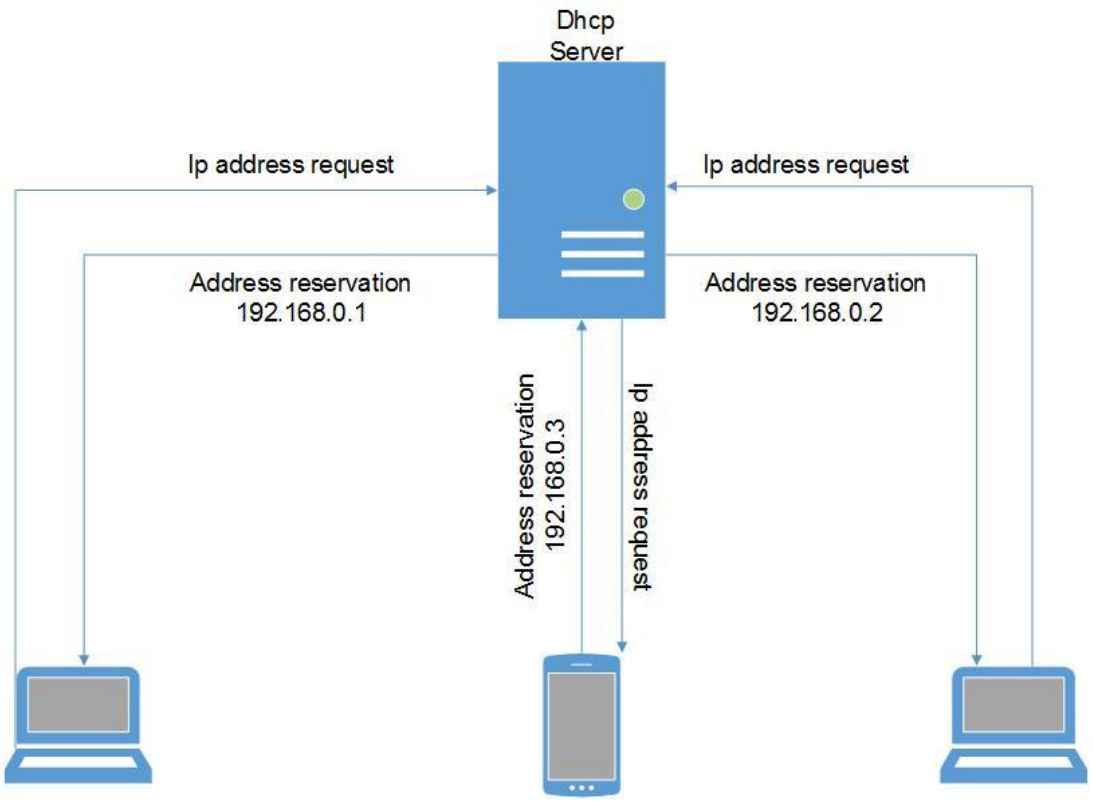


Εικόνα 2 Τρόπος λειτουργιάς Coova Chilli

Όλες οι παράμετροι λειτουργίας του Coova-Chilli, μπορούν, είτε να διαμορφωθούν από τη γραμμή εντολών του συστήματος Linux, είτε από το βασικό αρχείο διαμόρφωσης, καθώς εκεί αποθηκεύονται οι ρυθμίσεις που φορτώνονται κατά την εκκίνηση του προγράμματος.

2.5 Ανάθεση IP διευθύνσεων μέσω DHCP Server

Με τον όρο DHCP (Dynamic Host Configuration Protocol), αναφερόμαστε σε ένα μηχανισμό διαχείρισης των IP παραμέτρων δικτυακών συσκευών. Το πρωτόκολλο αυτό είναι ουσιαστικά ένα λογισμικό που τρέχει σε ένα διακομιστή και ρυθμίζει τις απαραίτητες δικτυακές παραμέτρους, για όλες τις συσκευές των χρηστών, που χρησιμοποιούν το ίδιο πρωτόκολλο.



Εικόνα 3 Dhcp Leasing

Για να λειτουργήσει το πρωτόκολλο DHCP σε όλες τις συσκευές, υπάρχει η ανάγκη να ρυθμίζονται οι κατάλληλες επιλογές του δικτύου, για να παίρνουν τιμές αυτόματα. Η αρχικοποίηση μπορεί να γίνεται κατά τη διάρκεια της εκκίνησης (αν το πρωτόκολλο είναι ενσωματωμένο στο λειτουργικό σύστημα), ή με την έμμεση κλήση του πρωτοκόλλου από κάποια δικτυακή εφαρμογή.

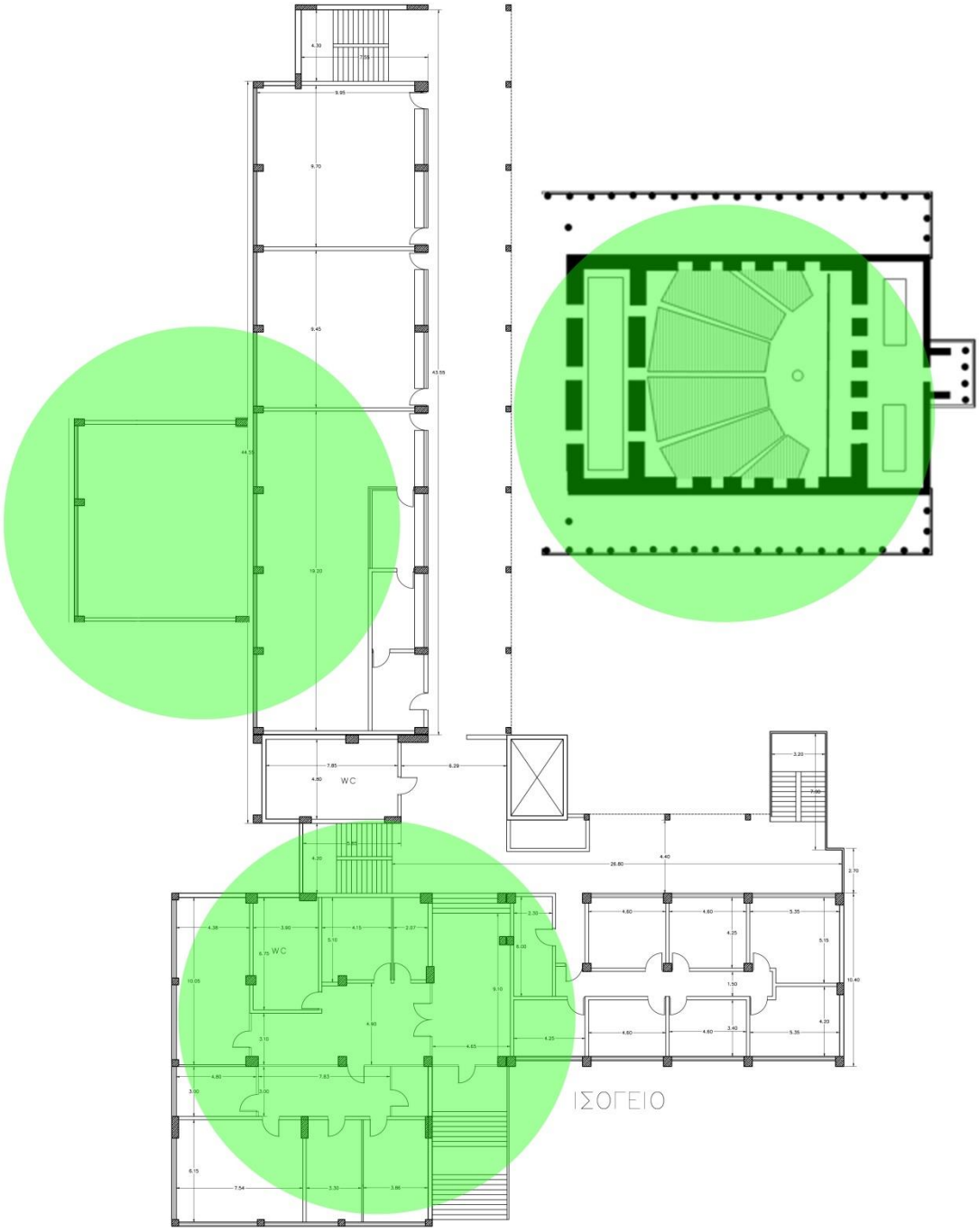
Οι παράμετροι αυτές μπορούν να ορίζονται και χειροκίνητα για κάθε συσκευή, αλλά κάτι τέτοιο δημιουργεί προβλήματα. Κατ' αρχάς, απαιτείται πάρα πολλή εργασία από το διαχειριστή του δικτύου, η οποία είναι χρονοβόρα και επιρρεπής σε λάθη. Το να διατηρούνται ενημερωμένες οι παράμετροι, χρειάζεται συνεχής ενασχόληση, η οποία

αυξάνεται γεωμετρικά με τις αλλαγές που συμβαίνουν στο δίκτυο, ειδικά αν υπάρχουν υπολογιστές που αλλάζουν συνεχώς χώρο χρήσης (πχ φορητοί Η/Υ). Για παράδειγμα, η αλλαγή μιας κοινής παραμέτρου για τους υπολογιστές σε ένα υποδίκτυο (π.χ τοπική διεύθυνση ενός δρομολογητή), απαιτεί αλλαγές σε κάθε υπολογιστή-χρήστη. Μερικά μηχανήματα μπορούν να λειτουργούν ως τερματικά γεγονός που σημαίνει ότι δεν έχουν αποθηκευτικό χώρο για να κρατήσουν τις ρυθμίσεις τους. Σε περιπτώσεις έλλειψης διαθέσιμων διευθύνσεων ή ενός δικτύου που αλλάζει συνέχεια, θα ήταν σπατάλη πόρων να διαθέταμε σε έναν περιστασιακά λειτουργικό υπολογιστή στατική διεύθυνση. Μια καλύτερη προσέγγιση θα ήταν να χρησιμοποιούνται ομάδες διευθύνσεων από ομάδες υπολογιστών. Γενικά, η χειροκίνητη ρύθμιση δεν παρέχει εύκολο τρόπο για να γίνει κάτι τέτοιο. Όλοι αυτοί οι λόγοι οδήγησαν στην ανάγκη για έναν αυτόματο μηχανισμό διαχείρισης των IP διευθύνσεων. Ο DHCP είναι σήμερα ο πιο προηγμένος μηχανισμός για αυτή τη λειτουργία. Έτσι, για να είναι η σύνδεση όσο το δυνατόν περισσότερο αυτοματοποιημένη και να μη γίνονται πολλές ρυθμίσεις από την πλευρά του χρήστη, ενεργοποιήθηκε και παραμετροποιήθηκε ο DHCP Server του Coova-Chilli.

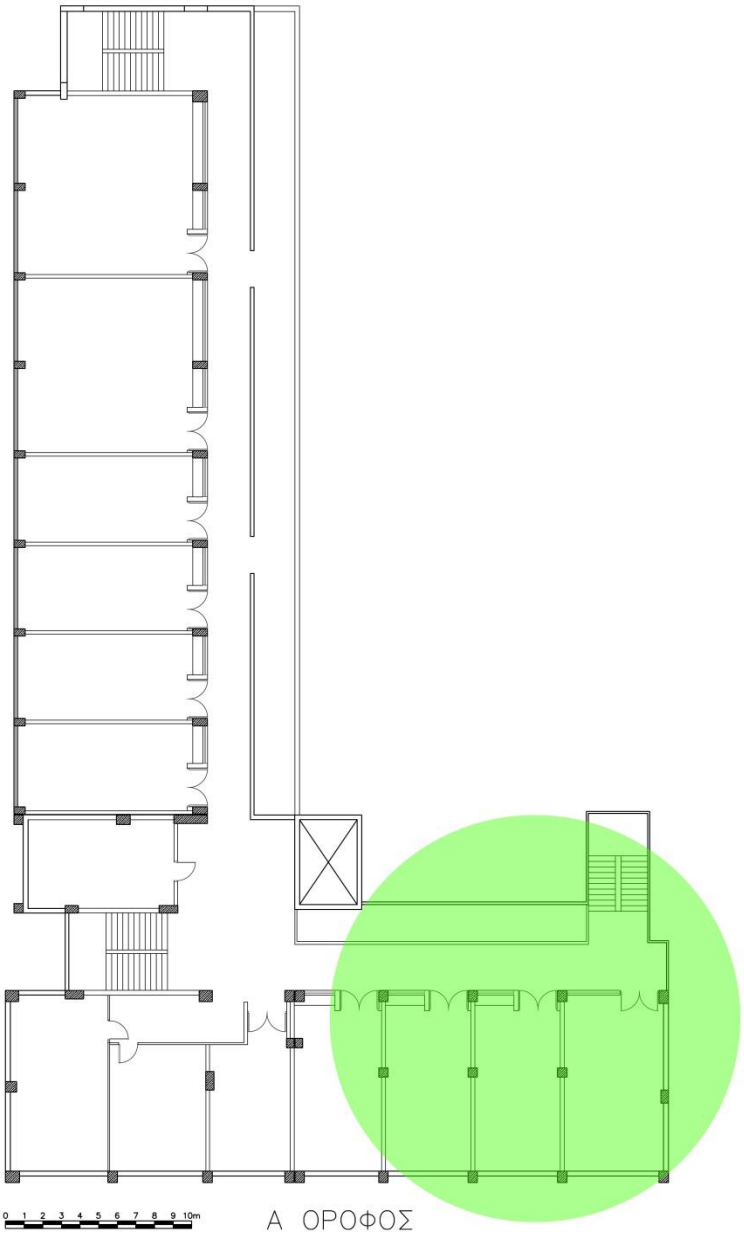
2.6 Σημεία Ασύρματης Πρόσβασης – Access Point

Στους χώρους της Σχολής υπήρχαν συνολικά 5 σημεία ασύρματης πρόσβασης (APs), από τα οποία τα 4 ήταν τύπου Cisco Aironet 1300 series και το 5^{ο} ήταν τύπου Compex-Wpe54g. Τα σημεία ασύρματης πρόσβασης λειτουργούσαν ως γέφυρες με την υπόλοιπη δικτυακή υποδομή, έτσι ώστε με τη σύνδεσή μας στο ασύρματο δίκτυο μας έφερναν σε επικοινωνία με το Captive portal, προκειμένου να ολοκληρωθεί η πιστοποίησή μας και να μας δοθεί πρόσβαση.

2.6.1 Περιοχές Κάλυψης



Εικόνα 4 Κάλυψη Ασύρματου δικτύου στο ισόγειο



Εικόνα 5 Κάλυψη Ασύρματου δικτύου στον Α' όροφο

3 Eduroam

3.1 Το eduroam.

Το **eduroam** (**edu**cation **roam**ing) είναι η ασφαλής, παγκόσμια υπηρεσία ασύρματης, ή ενσύρματης πρόσβασης στο διαδίκτυο, που αναπτύχθηκε για τη διεθνή ερευνητική και εκπαιδευτική κοινότητα και υποστηρίζει περιαγωγή.Το eduroam επιτρέπει στους φοιτητές, ερευνητές και διοικητικό προσωπικό, από τα συμμετέχοντα ιδρύματα, να αποκτούν σύνδεση στο διαδίκτυο, ανοίγοντας απλά το φορητό υπολογιστή τους, είτε όταν βρίσκονται στο δικό τους εκπαιδευτικό ίδρυμα, είτε όταν επισκέπτονται άλλα συμμετέχοντα ιδρύματα

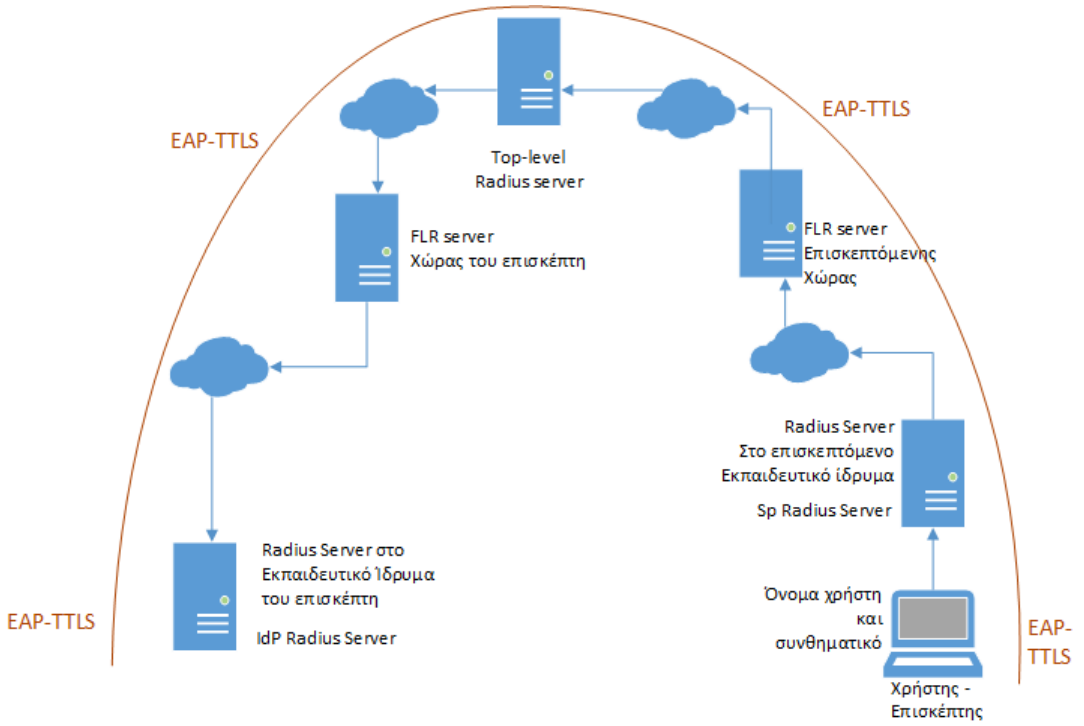
Το eduroam υποστηρίζει την έρευνα και την εκπαίδευση παρέχοντας:

- Υψηλής ταχύτητας, ευρυζωνικές υπηρεσίες περιαγωγής σε 54 χώρες(06/2014)
- Πρόσβαση από χιλιάδες σημεία παρουσίας, με κοινές ρυθμίσεις
- Τεχνολογία που διασφαλίζει τη διαφύλαξη της ιδιωτικότητας
- Αμοιβαία υπηρεσία που παρέχεται χωρίς χρέωση στους χρήστες
- Πρωτοποριακές υπηρεσίες περιαγωγής σε διεθνές επίπεδο.

Η πρωτοβουλία eduroam ξεκίνησε το 2003 μέσα από την ομάδα εργασίας του οργανισμού TERENA για την κινητικότητα (Task Force on mobility). Η ομάδα εργασίας δημιούργησε μια δοκιμαστική υποδομή, για να αποδειχθεί η σκοπιμότητα λειτουργίας του συνδυασμού των τεχνολογιών RADIUS και 802.1X, για την παροχή πρόσβασης στους δικτυακούς πόρους των συνεργαζόμενων ιδρυμάτων έρευνας και εκπαίδευσης, μέσω περιαγωγής. Η αρχική δοκιμή διεξήχθη μεταξύ πέντε ιδρυμάτων που βρίσκονται στην Ολλανδία, τη Φινλανδία, την Πορτογαλία, την Κροατία και το Ηνωμένο Βασίλειο. Αργότερα, άλλα εθνικά ερευνητικά και εκπαιδευτικά δίκτυα στην Ευρώπη αγκάλιασαν την ιδέα με αποτέλεσμα να αρχίσει σταδιακά να αναπτύσσεται μια μεγάλης κλίμακας υποδομή, η οποία έγινε γνωστή με το όνομα eduroam.

Το eduroam επιτρέπει σε κάθε εξουσιοδοτημένο χρήστη να έχει πρόσβαση στο δίκτυο κάθε ιδρύματος που ικανοποιεί τις προδιαγραφές eduroam. Ανάλογα με τις τοπικές πολιτικές χρήσης στα επισκεπτόμενα ιδρύματα, μπορούν να παρέχονται επιπλέον πόροι (π.χ. εκτυπωτές), στη διάθεση των χρηστών.

3.2 Η υποδομή-τρόπος λειτουργίας eduroam.



Εικόνα 6 Τρόπος λειτουργίας Eduroam

Η τεχνολογία eduroam βασίζεται στο πρότυπο 802.1X και στην ιεράρχηση των RADIUS proxy servers. Ο ρόλος της ιεραρχίας των RADIUS είναι να διαβιβάζουν τα «διαπιστευτήρια των χρηστών στο ίδρυμα προέλευσης, όπου μπορούν να επαληθεύονται και να επικυρώνονται.

Ο μηχανισμός με τον οποίο εκτελείται ο έλεγχος ταυτότητας χρηστών αποτελεί το θεμελιώδη λίθο του eduroam.

Ο έλεγχος ταυτότητας ενός χρήστη πραγματοποιείται στον πάροχο ταυτοποίησης Identity Provider (IdP), χρησιμοποιώντας συγκεκριμένη μέθοδο αναγνώρισης της ταυτότητάς τους (πχ EAP-TTLS).

Η έγκριση που επιτρέπει την πρόσβαση στους πόρους του δικτύου μετά τη σωστή επικύρωση, γίνεται από τον πάροχο υπηρεσιών (Service Provider - SP), μέσω ενός ασύρματου σημείου πρόσβασης.

Προκειμένου να μεταφερθεί το αίτημα ταυτότητας ενός χρήστη από τον πάροχο υπηρεσιών, στον πάροχο ταυτότητας και να επιστρέψει η σχετική απάντηση ταυτότητας, έχει δημιουργηθεί ένα παγκόσμιο σύστημα RADIUS servers. Τυπικά κάθε πάροχος ταυτότητας αναπτύσσει ένα διακομιστή RADIUS, ο οποίος είναι συνδεδεμένος με μια τοπική βάση δεδομένων χρηστών. Αυτός ο διακομιστής RADIUS είναι συνδεδεμένος σε έναν κεντρικό εθνικό διακομιστή RADIUS, ο οποίος με τη σειρά του συνδέεται είτε στον ευρωπαϊκό, ή στον αντίστοιχο παγκοσμίου επιπέδου διακομιστή RADIUS, είτε μπορεί να συνδέεται δυναμικά με άλλους διακομιστές RADIUS, (χρησιμοποιώντας το πρωτόκολλο RADIUS / TLS).

Για να μεταφέρονται οι πληροφορίες ελέγχου ταυτότητας του χρήστη με ασφάλεια σε όλη την υποδομή RADIUS(IdP) και να εμποδίζονται άλλοι χρήστες να έχουν

πρόσβαση στα στοιχεία της σύνδεσης, χρησιμοποιείται στα σημεία πρόσβασης το πρότυπο IEEE 802.1X. Το πρότυπο αυτό περιλαμβάνει τη χρήση του Extensible Authentication Protocol (EAP), που επιτρέπει τη χρήση διαφορετικών πρωτοκόλλων πιστοποίησης, δημιουργώντας ένα ασφαλές κανάλι επικοινωνίας . Μερικά από αυτά είναι τα παρακάτω :

- EAP-TLS ("Transport Layer Security") - ένα πρωτόκολλο της IETF που πιστοποιεί τους χρήστες με το IdP με δύο πιστοποιητικά X.509
- EAP-TTLS ("Tunneled TLS") - ένα πρωτόκολλο της IETF που δημιουργεί μια σήραγγα TLS, και στέλνει τους κωδικούς χρηστών και τα συνθηματικά πρόσβασης σε πολλαπλές μορφές στο εσωτερικό της (inner-tunnel).
- FAST (Flexible Authentication via Secure Tunneling) - ένα πρωτόκολλο της Cisco που καθιερώνει μια σήραγγα TLS, και στέλνει τους κωδικούς χρηστών και τα συνθηματικά πρόσβασης, σε μια προσαρμοσμένη διαδρομή στο εσωτερικό της.)
- PEAP (Protected EAP)- ένα πρωτόκολλο της Microsoft που δημιουργεί μια σήραγγα TLS, και στέλνει τους κωδικούς χρηστών και τα συνθηματικά πρόσβασης, μέσα σε αυτή χρησιμοποιώντας MS-CHAPv2 hashes

Το eduroam προϋποθέτει ότι η επιλεγείσα μέθοδος EAP επιτρέπει αμοιβαίο έλεγχο ταυτότητας (δηλαδή ο χρήστης μπορεί να επαληθεύει ότι συνδέεται με τον πάροχο ταυτοποίησής του, όπου και αν βρίσκεται.

Η κρυπτογράφηση των μηνυμάτων που ανταλλάσσονται μεταξύ του χρήστη και του παρόχου ταυτότητας (IdP) για την ανταλλαγή διαπιστευτηρίων, παραμένει αόρατη στον πάροχο υπηρεσιών(SP) και όλα τα ενδιάμεσα proxies

Όταν ένας χρήστης ζητά έλεγχο ταυτότητας, το realm του χρήστη καθορίζει την δρομολόγηση του αιτήματος. Το realm είναι συνήθως η κατάληξη του κωδικού χρήστη, η οποία βρίσκεται μετά το σύμβολο "@", και ταυτίζεται με το domain name του κάθε οργανισμού.

Κάθε εκπαιδευτικό ίδρυμα που θέλει να συμμετάσχει στο eduroam συνδέει τον ιδρυματικό του RADIUS-server στον ανώτατο server εθνικού επιπέδου RADIUS (FLR Server) της χώρας .

Ο κάθε FLR server λειτουργεί υπό την αιγίδα του Εθνικού Δικτύου Έρευνας και Τεχνολογίας (ΕΔΕΤ) της κάθε χώρας. Τέτοιοι διακομιστές λειτουργούν σε επίπεδο χώρας και έχουν μια πλήρη λίστα των ιδρυμάτων που συμμετέχουν στην υποδομή του eduroam. Αυτό είναι αρκετό για να εγγυηθούν την εθνική περιαγωγή.

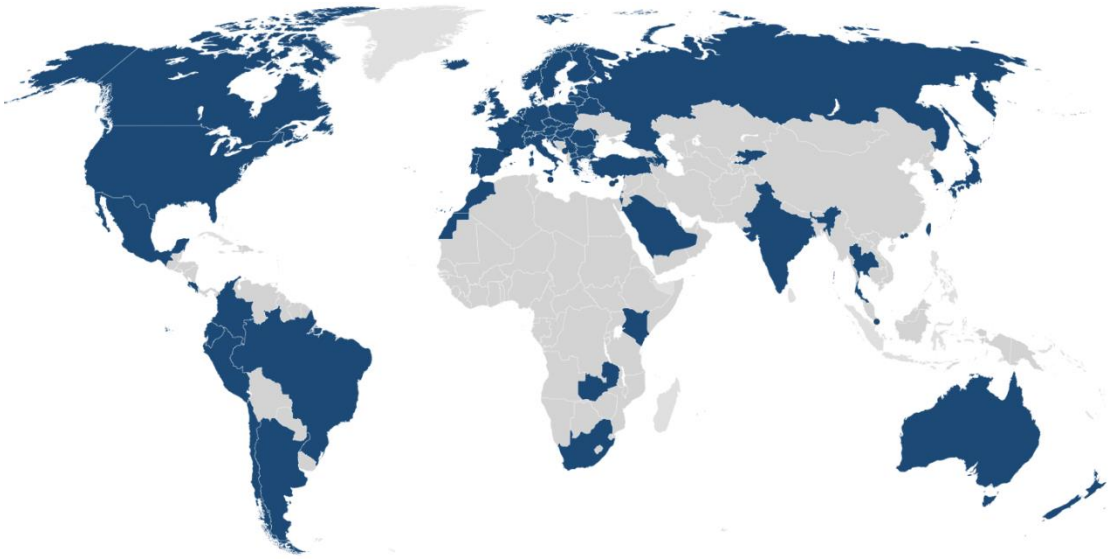
Για τη διεθνή περιαγωγή λειτουργεί μια περιφερειακή υποδομή, με διακομιστή RADIUS σε υψηλότερο επίπεδο, προκειμένου να περιάγει το αίτημα των χρηστών στη χώρα προορισμού. Επί του παρόντος, έχουν αναπτυχθεί διακομιστές διεθνούς περιαγωγής, στις περιοχές Ευρώπης και Ασίας-Ειρηνικού.

Στην περίπτωση της Ευρώπης, ο top-level διακομιστής RADIUS (ETLR) διαχειρίζεται από τον Ολλανδικό ΕΔΕΤ (SURFnet), σε συνεργασια με το ΕΔΕΤ της Δανίας (UNI-C).

Στην περίπτωση της Ασίας-Ειρηνικού, ο top-level διακομιστής RADIUS (APTLR) διαχειρίζεται από το αυστραλιανό ΕΔΕΤ (AARNet) και από το Πανεπιστήμιο του Χονγκ Κονγκ.

3.3Κάλυψη eduroam.

Ξεκινώντας από την Ευρώπη, το eduroam έχει αποκτήσει δυναμική στην παγκόσμια ερευνητική και εκπαιδευτική κοινότητα και είναι διαθέσιμο σε συμμετέχοντα πανεπιστήμια, ερευνητικά κέντρα και βιβλιοθήκες σε περίπου 60 χώρες σε όλο τον κόσμο. Η υπηρεσία eduroam, σε όλη την Ευρώπη συντονίζεται από μια ομάδα του προγράμματος GÉANT, το οποίο χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή.

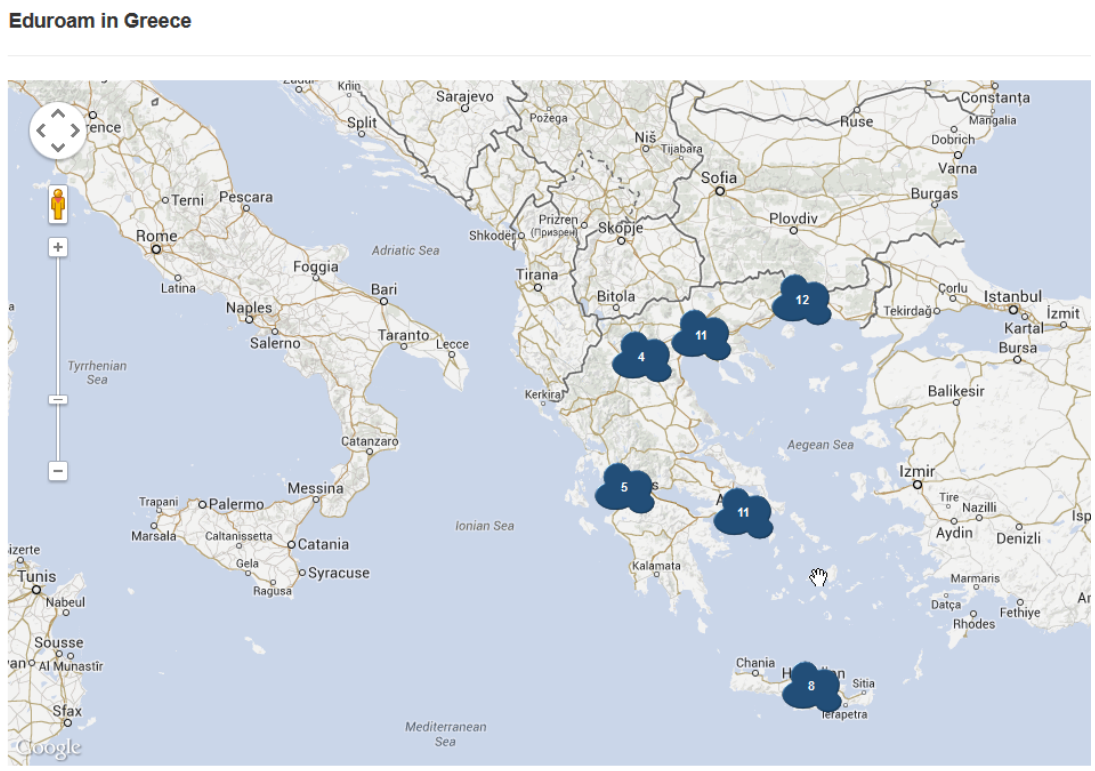


Εικόνα 7 Παγκόσμιος χάρτης παροχής eduroam

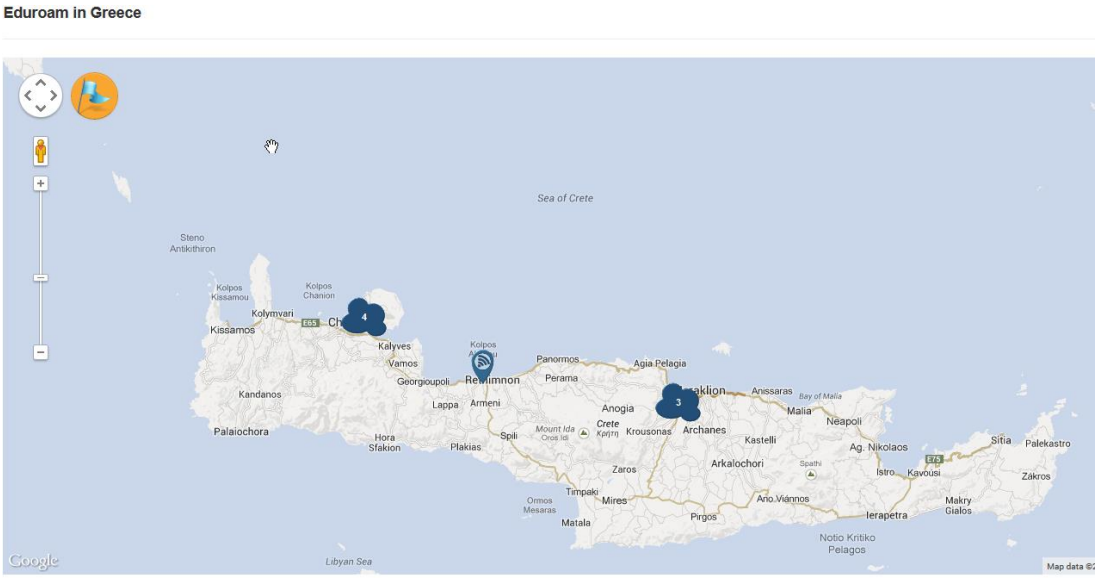
Andorra, Argentina, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Ecuador, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Ireland, Israel, Italy, Japan, Kazakhstan, Kenya, Korea, Kyrgyzstan, Latvia, Lithuania, Luxembourg, Macau, Macedonia, Malta, Mexico, Moldova, Montenegro, Morocco, The Netherlands, New Zealand, Norway, Peru, Poland, Portugal, Romania, Russia, Saudi Arabia, Serbia, Singapore, Slovenia, Slovakia, South Africa, Spain, Sweden, Switzerland, Republic of China, Thailand, Turkey, United Kingdom, United States of America and Zambia

Εικόνα 8 Ιδρύματα και οργανισμοί που προσφέρουν eduroam

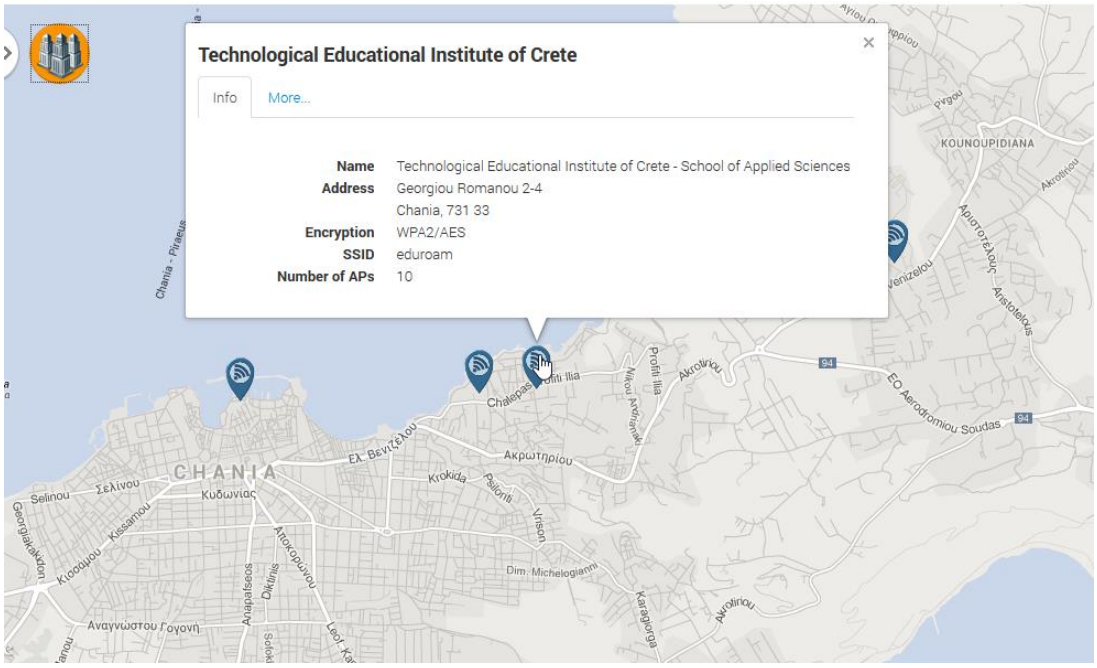
Μέχρι και τον Ιούνιο του 2014, στην Ελλάδα υπήρχαν 51 εκπαιδευτικά ιδρύματα και ερευνητικοί οργανισμοί που προσφέρουν πρόσβαση στο eduroam. Ειδικότερα, στην Κρήτη υπάρχουν συνολικά 8. Πιο συγκεκριμένα, στα Χανιά υπάρχουν 4 ανεξάρτητες γεωγραφικές περιοχές ιδρυμάτων που υποστηρίζονται από 95 Access points για πρόσβαση στο διαδίκτυο μέσω eduroam, τα 10 εκ των οποίων ανήκουν στο ΤΕΙ Κρήτης και συγκεκριμένα στη Σχολή Εφαρμοσμένων Επιστημών.



Εικόνα 9 Περιοχές κάλυψης ανά Νομούς στην Ελλάδα



Εικόνα 10 Περιοχές κάλυψης στην Κρήτη



Εικόνα 11 Λεπτομέρειες για την πρόσφορα eduroam στη Σχολή Εφαρμοσμένων Επιστημών

4 Το πρωτόκολλο Radius

4.1Εισαγωγή

Remote Authentication Dial In User Service (RADIUS) είναι ένα πρωτόκολλο παροχής κεντρικού ελέγχου ταυτότητας, εξουσιοδότησης και καταγραφής κίνησης χρηστών (authentication, authorization, accounting-AAA), για τη διαχείριση των χρηστών που συνδέονται και χρησιμοποιούν υπηρεσίες του δικτύου. Το πρωτόκολλο RADIUS αναπτύχθηκε από την εταιρία Livingston Enterprises Inc το 1991 ως διακομιστής ελέγχου ταυτότητας πρόσβασης και πρωτόκολλο καταγραφής κίνησης λογαριασμών, ενώ στη συνέχεια προτυποποιήθηκε από τον οργανισμό Internet Engineering Task Force (IETF).

Λόγω της ευρείας υποστήριξης και της πανταχού παρουσίας του, το RADIUS χρησιμοποιείται συχνά από τους ISPs και τις επιχειρήσεις για να διαχειρίζονται την πρόσβαση στο διαδίκτυο ή σε εσωτερικά ασύρματα – ενσύρματα δίκτυα καθώς και σε ολοκληρωμένες υπηρεσίες όπως το e-mail. Όσο αφορά τα δίκτυα, το radius χρησιμοποιείται σε μόντεμ, DSL, ασύρματα σημεία πρόσβασης, VPNs, θύρες δικτύου σε μεταγωγείς , web servers, κλπ.

Το RADIUS πρωτόκολλο είναι τύπου χρήστη/ διακομιστή που εκτελείται στο επίπεδο εφαρμογών, χρησιμοποιώντας UDP ως πρωτόκολλο μεταφοράς. Ο διακομιστής απομακρυσμένης πρόσβασης, ο διακομιστής VPN, το Network switch με έλεγχο ταυτότητας βάσει θύρας(802.1x), και ο Network Access Server (NAS), είναι οι βασικές πύλες που ελέγχουν την πρόσβαση στο δίκτυο, και όλες τους είναι εφοδιασμένες με την εφαρμογή χρήστη RADIUS που επικοινωνεί με το διακομιστή RADIUS. Το RADIUS αποτελεί συχνά το backend της επιλογής για έλεγχο ταυτότητας 802.1x. Επιπλέον, η εφαρμογή διακομιστή RADIUS εκτελείται σε ένα διακομιστή Linux ή Microsoft Windows Server και τρέχει συνήθως στο παρασκήνιο.

4.2 Authentication, Authorization, Accounting-AAA

Οι RADIUS servers χρησιμοποιούν την αρχή AAA για τη διαχείριση της πρόσβασης στο δίκτυο με την ακόλουθη διαδικασία τριών σταδίων, γνωστή και ως "AAA transaction". Τα αρχικά AAA σημαίνουν ταυτοποίηση (**A**uthentication), εξουσιοδότηση(**A**uthorization) και καταγραφή κίνησης χρηστών(**A**ccounting). Ο έλεγχος Πιστοποίησης και Εξουσιοδότησης του RADIUS περιγράφεται στο πρωτόκολλο RFC 2865, ενώ η καταγραφή κίνησης χρηστών περιγράφεται στο RFC 2866.

4.2.1 Επαλήθευση ταυτότητας και αδειοδότηση

Κατά τη διάρκεια της επαλήθευσης, ο χρήστης ή το μηχάνημα στέλνει μια αίτηση σε ένα διακομιστή απομακρυσμένης πρόσβασης, για να αποκτήσει πρόσβαση σε ένα συγκεκριμένο πόρο δικτύου, χρησιμοποιώντας τα διαπιστευτήριά του. Τα διαπιστευτήρια πρέπει να περάσουν στο διακομιστή απομακρυσμένης πρόσβασης, μέσω του πρωτοκόλλου επιπέδου σύνδεσης, π.χ., Point-to-Point Protocol (PPP) στην περίπτωση dialup ή DSL παρόχων.

Με τη σειρά του, ο διακομιστής απομακρυσμένης πρόσβασης στέλνει ένα μήνυμα «Αίτηση RADIUS πρόσβαση» στο διακομιστή RADIUS, ζητώντας του άδεια να επιτρέψει την πρόσβαση μέσω του πρωτοκόλλου RADIUS στον αρχικό χρήστη.

Η εν λόγω αίτηση περιλαμβάνει τα διαπιστευτήρια πρόσβασης, συνήθως με τη μορφή του ονόματος χρήστη και του κωδικού πρόσβασης ή το πιστοποιητικό ασφαλείας που παρέχεται από το χρήστη. Επιπλέον, η αίτηση μπορεί να περιέχει και άλλες πληροφορίες σχετικά με τη φυσική πλευρά του χρήστη της σύνδεσης, τα οποία γνωρίζει ο διακομιστής απομακρυσμένης πρόσβασης, όπως η διεύθυνση του δικτύου(IP), ο αριθμός τηλεφώνου ή ακόμη και η διεύθυνση ηλεκτρονικής αλληλογραφίας.

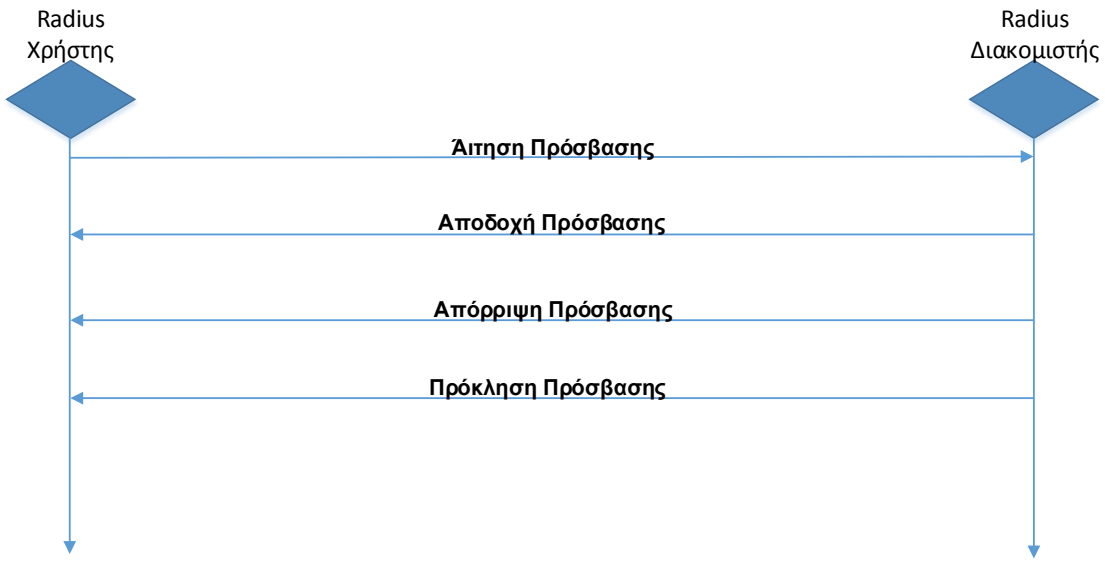
Ο RADIUS ελέγχει ότι οι πληροφορίες είναι σωστές , χρησιμοποιώντας συστήματα ελέγχου ταυτότητας, όπως PAP , CHAP ή EAP. Για να αποδειχτεί ότι ο χρήστης πιστοποιείται με τα στοιχεία λογαριασμού του, προαιρετικά αποστέλλονται και άλλες πληροφορίες που συνδέονται με την αίτηση, όπως η κατάσταση του λογαριασμού του (enabled/disabled/paused) και συγκεκριμένα προνόμια πρόσβασης (permission level) υπηρεσιών δικτύου. Ιστορικά, οι RADIUS servers ελέγχουν τις πληροφορίες για τον χρήστη σε μια βάση δεδομένων σε τοπικό επίπεδο. Οι σύγχρονοι Radius servers μπορούν να συνδέονται και σε εξωτερικές πηγές, συνήθως SQL, Kerberos, LDAP, ή διακομιστές Active Directory για την επαλήθευση των διαπιστευτηρίων των χρηστών.

Ο διακομιστής πρόσβασης επιστρέφει στη συνέχεια μία από τις τρεις απαντήσεις του Radius

1) Απόρριψη Πρόσβασης,

2) Πρόκληση Πρόσβασης,

3) Αποδοχή Πρόσβασης



Εικόνα 12 Διαδικασία πρόσβασης με Radius

Απόρριψη Πρόσβασης σημαίνει ότι στο χρήστη απαγορεύεται η πρόσβαση σε όλους τους ζητούμενους πόρους του δικτύου. Οι λόγοι μπορούν να περιλαμβάνουν είτε αδυναμία παροχής απόδειξης της ταυτότητάς του ή άγνωστο/ανενεργό λογαριασμό χρήστη.

Πρόκληση Πρόσβασης σημαίνει αίτημα για πρόσθετες πληροφορίες από το χρήστη, όπως δευτερεύων κωδικός πρόσβασης, PIN, κουπόνι πρόσβασης. Το κουπόνι πρόσβασης χρησιμοποιείται επίσης σε πιο σύνθετους διαλόγους ταυτοποίησης όπου είναι εγκατεστημένο ένα ασφαλές κανάλι επικοινωνίας μεταξύ του χρήστη και του διακομιστή Radius, κατά τέτοιο τρόπο, ώστε τα πιστοποιητικά πρόσβασης να μην είναι αντιληπτά στο διακομιστή απομακρυσμένης πρόσβασης.

Αποδοχή Πρόσβασης Ο χρήστης αποκτά πρόσβαση μόλις πιστοποιηθούν τα στοιχεία του. Ο διακομιστής RADIUS ελέγχει συχνά εάν ο χρήστης είναι εξουσιοδοτημένος να χρησιμοποιεί την υπηρεσία δικτύου που έχει ζητήσει.

Σε έναν τυπικό χρήστη μπορεί να επιτραπεί να χρησιμοποιεί το ασύρματο δίκτυο μιας εταιρείας, αλλά όχι την υπηρεσία VPN, για παράδειγμα. Οι πληροφορίες ταυτοποίησης μπορούν να αποθηκεύονται τοπικά στο διακομιστή RADIUS, ή να αναζητούνται σε μια εξωτερική πηγή, όπως LDAP, Active Directory, Βάση Δεδομένων.

Κάθε μία από αυτές τις τρεις παραπάνω απαντήσεις μπορεί να περιλαμβάνει ένα χαρακτηριστικό μήνυμα που να περιέχει ένα λόγο για την απόρριψη, προτροπή για πρόσθετη πληροφορία πιστοποίησης, ή κείμενο καλωσορίσματος για την αποδοχή. Το κείμενο του μηνύματος μπορεί να μετακυλίεται στο χρήστη μέσω ιστοσελίδας. Τα στοιχεία της εξουσιοδότησης μεταφέρονται στο διακομιστή απομακρυσμένης πρόσβασης, ορίζοντας τους όρους της πρόσβασης που χορηγείται. Για παράδειγμα , τα ακόλουθα στοιχεία της εξουσιοδότησης μπορούν να συμπεριλαμβάνονται σε ένα μήνυμα Αποδοχής Πρόσβασης:

- Η συγκεκριμένη διεύθυνση IP που διατίθεται για το χρήστη
- Το εύρος των διευθύνσεων από τα οποία επιλέγεται η IP του χρήστη.
- Το μέγιστο χρονικό διάστημα που ο χρήστης μπορεί να παραμένει συνδεδεμένος
- Οι παράμετροι L2TP και VLAN καθώς και η ποιότητα της παρεχόμενης υπηρεσίας (QoS)

4.3 Λογαριασμοί χρηστών

Όταν η πρόσβαση στο δίκτυο δίδεται στο χρήστη από το NAS (Network access server), ένα αίτημα τύπου έναρξης καταγραφής κίνησης του συγκεκριμένου χρήστη στέλνεται από τον NAS στον RADIUS, για να σηματοδοτήσει την έναρξη πρόσβασης του χρήστη στο δίκτυο.

Το αίτημα έναρξης τυπικά περιέχει την ταυτότητα του χρήστη, τη διεύθυνση του δικτύου, το σημείο προσάρτησης και ένα μοναδικό αναγνωριστικό της συνεδρίας.

Περιοδικά, για λόγους προσωρινής ενημέρωσης, ως προς την κατάσταση της ενεργής συνεδρίας, στέλνεται από το NAS στο διακομιστή RADIUS ένα πακέτο με την αίτηση λογαριασμού RADIUS, το οποίο είναι τύπου "προσωρινής ενημέρωσης". Τα πακέτα radius τυπικά μεταφέρουν πληροφορίες για τη διάρκεια της τωρινής συνεδρίας και την τρέχουσα χρήση δεδομένων.

Τέλος, όταν ολοκληρωθεί η πρόσβαση του χρήστη στο δίκτυο, το NAS εκδίδει μια τελευταία αίτηση για την αποσύνδεση του χρήστη στο διακομιστή RADIUS με ένα πακέτο τύπου "αποσύνδεσης-τερματισμού", που παρέχει πληροφορίες για την συνολική χρήση σε σχέση με το χρόνο, τα πακέτα και τα δεδομένα που μεταφέρθηκαν, το λόγο διακοπής σύνδεσης και άλλες πληροφορίες σχετικές με την πρόσβαση του χρήστη στο δίκτυο.

Τυπικά ο χρήστης (radius client) στέλνει πακέτα καταγραφής κίνησης λογαριασμού ανά τακτά χρονικά διαστήματα, μέχρι να λάβει επιβεβαίωση.

Ο κύριος σκοπός αυτών των δεδομένων είναι η ανάλογη χρέωση του χρήστη. Επίσης τα δεδομένα χρησιμοποιούνται για στατιστικές αναλύσεις και γενικότερη παρακολούθηση της χρήσης των δικτύων.

4.4 Περιαγωγή (roaming)

Το RADIUS χρησιμοποιείται για να διευκολύνει την περιαγωγή μεταξύ ISPs όπως εταιριών που παρέχουν ένα ενιαίο σύνολο παγκόσμιων διαπιστευτηρίων για χρήση σε πολλά δημόσια δίκτυα και·ανεξάρτητων, αλλά συνεργαζόμενων φορέων που εκδίδουν τα δικά τους διαπιστευτήρια για τους δικούς τους χρήστες, που επιτρέπουν σε ένα χρήστη-επισκέπτη τους να πιστοποιείται από το δικό του φορέα, όπως συμβαίνει με το eduroam.

Το RADIUS διευκολύνει την περιαγωγή με τη βοήθεια των realms, τα οποία ρυθμίζουν που πρέπει να προωθήσει ο διακομιστής RADIUS τα αιτήματα AAA για επεξεργασία.

4.5 Realms

Το realm είναι αυτό που συνήθως προσαρτάται στο όνομα του χρήστη και οριοθετείται με το σύμβολο '@', θυμίζοντας έτσι διεύθυνση ηλεκτρονικού ταχυδρομείου.

Αυτό είναι γνωστό ως κατάληξη (postfix) για το realm. Μια ακόμη κοινή χρήση του realm είναι σαν πρόθεμα (prefix), στο όνομα χρήστη, χρησιμοποιώντας το σύμβολο '/' ως οριοθέτη.

Οι μοντέρνοι διακομιστές Radius επιτρέπουν σε κάθε χαρακτήρα να χρησιμοποιείται ως οριοθέτης για το realm , αν και πρακτικά χρησιμοποιούνται συνήθως το '@' και το '/'.

Τα realm μπορούν να αναμιχθούν χρησιμοποιώντας και το prefix και το postfix, για να καταστούν δυνατά πιο περίπλοκα σενάρια περιαγωγής. Για παράδειγμα το όνομα χρήστη somedomain.com\username@anotherdomain.com θα μπορούσε να είναι ένα έγκυρο για δύο realm.

Παρόλο που τα realms μοιάζουν με τα domains, είναι σημαντικό να σημειωθεί ότι τα realms είναι στην πραγματικότητα αυθαίρετα κείμενα και δεν χρειάζεται να περιέχουν πραγματικά ονόματα domain. Η δομή των realm είναι τυποποιημένη σε ένα Network Access Identifier (NAI), στη μορφή 'χρήστης@realm'.

Ωστόσο, στηΝ προδιαγραφή του Network Access Identifier (NAI), το τμήμα «realm» πρέπει να είναι ένα όνομα domain, αν και η πρακτική αυτή δεν ακολουθείται πάντα.

4.6 Λειτουργίες μεσολάβησης (Proxy operations)

Όταν ένας διακομιστής RADIUS λαμβάνει μια AAA αίτηση για ένα όνομα χρήστη που περιέχει ένα realm, τότε ο διακομιστής αναφέρεται σε ένα πίνακα από διαμορφωμένα realms. Εάν το realm είναι γνωστό, τότε ο διακομιστής θα προωθήσει το αίτημα στο διακομιστή του φορέα που είναι υπεύθυνος γι΄ αυτό το domain.

Η συμπεριφορά του διακομιστή μεσολάβησης (proxying server) σε ότι αφορά την κατάργηση του realm από το αίτημα («απογύμνωση» stripping), εξαρτάται από τη διαμόρφωση των περισσοτέρων διακομιστών. Επιπλέον ο διακομιστής μεσολάβησης μπορεί να ρυθμίζεται για να προσθέτει, να καταργεί ή να ξαναγράφει αιτήσεις AAA όταν αυτές προωθούνται ξανά και ξανά.

4.7 RADIUS history

Το RADIUS είχε οριστεί αρχικά σαν ένα RFI (Request for information) από τη Merit Network το 1991 για τον έλεγχο της πρόσβασης dial-in στο NSFnet. Οι Livingston Enterprises ανταποκρίθηκαν στο RFI με μια περιγραφή ενός διακομιστή RADIUS. Η Merit Network ανέθεσε τη σύμβαση στην Livingston η οποία εξέδωσε με τη σειρά της PortMaster για Network Access Servers και τον αρχικό διακομιστή RADIUS για τη Merit

Το RADIUS εκδόθηκε αργότερα (1997) σαν Remote Authentication Dial In User Service (RADIUS) και RADIUS Accounting.

Τώρα υπάρχουν αρκετοί εμπορικοί και open-source διακομιστές RADIUS. Τα χαρακτηριστικά μπορεί να ποικίλουν, αλλά στις περισσότερες υλοποιήσεις αναζητούν τα στοιχεία των χρηστών μέσα σε LDAP διακομιστές ή σε διάφορες βάσεις δεδομένων. Τα στοιχεία των λογαριασμών μπορούν να γραφτούν σε αρχεία κειμένου, σε διάφορες βάσεις δεδομένων, ή να διαβιβαστούν σε εξωτερικούς διακομιστές.

Το SNMP (Simple Network Management Protocol) χρησιμοποιείται συχνά για την απομακρυσμένη παρακολούθηση και για συνεχείς ελέγχους ενός διακομιστή RADIUS. Οι διακομιστές μεσολάβησης χρησιμοποιούνται για κεντρική διαχείριση και για να ξαναγράφονται πακέτα όσο πιο γρήγορα γίνεται (για λόγους ασφαλείας).

Το πρωτόκολλο Diameter (Διάμετρος) προοριζόταν ως αντικαταστάτης του RADIUS. Ενώ και τα δύο ακλουθούν την αρχή λειτουργίας Authentication, Authorization, and Accounting (AAA), οι περιπτώσεις χρήσης για τα δύο αυτά πρωτόκολλα έχουν έκτοτε αποκλίνει (αλλάξει πορεία). Το Diameter χρησιμοποιείται σε μεγάλο βαθμό στο χώρο του 3G. Το RADIUS χρησιμοποιείται οπουδήποτε αλλού. Ένα από τα μεγαλύτερα εμπόδια για να αντικαταστήσει το Diameter το RADIUS είναι ότι οι

μεταγωγείς και τα σημεία πρόσβασης συνήθως εφαρμόζουν RADIUS, αλλά όχι Diameter.

Το Diameter χρησιμοποιεί SCTP ή TCP, ενώ το RADIUS τυπικά χρησιμοποιεί UDP ως επίπεδο μεταφοράς. Από το 2012 και μετά, μπορεί και το RADIUS να χρησιμοποιεί το TCP ως επίπεδο μεταφοράς με TLS για την ασφάλεια.

5 Εγκατάσταση παραμετροποίηση CentOS Firewall Radius & DHCP server

5.1 Εγκατάσταση Λειτουργικού CentOS

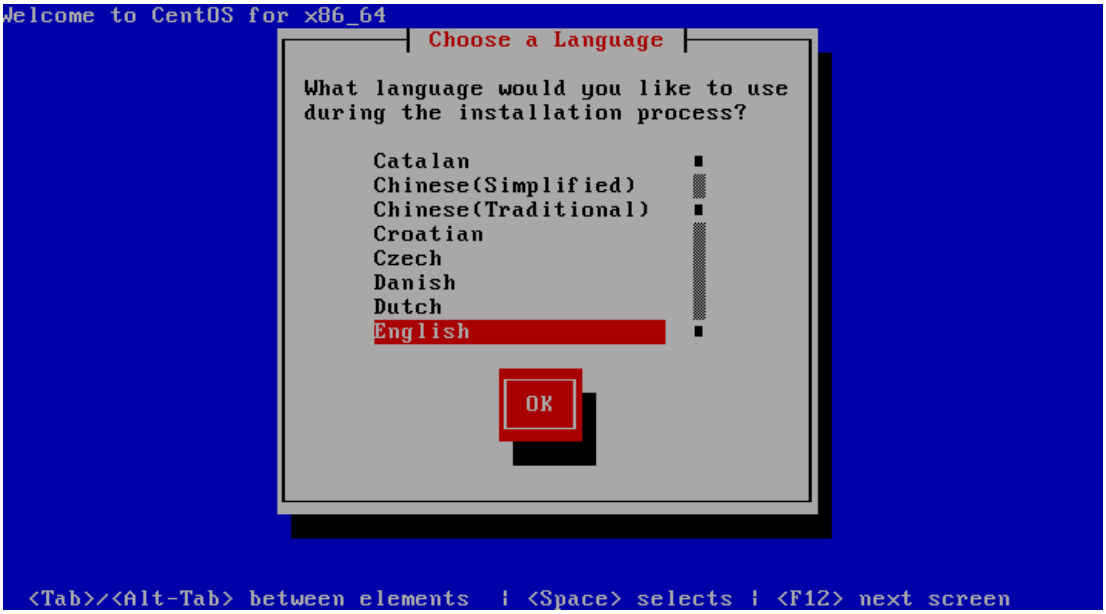
Το λειτουργικό που χρησιμοποιήθηκε είναι το Linux CentOS 6.5, 64-bit αρχιτεκτονικής και πιο συγκεκριμένα η έκδοση "CentOS-6.5-x86_64-netinstall". Η κατάληξη netinstall στην έκδοση που επιλέξαμε, σημαίνει πως το αρχείο που χρησιμοποιήσαμε για την εκκίνηση της εγκατάστασης περιέχει τα απαραίτητα, έτσι ώστε να ξεκινήσει η εγκατάσταση, ενώ τα υπόλοιπα θα μεταφορτωθούν από το διαδίκτυο, σύμφωνα με τις επιλογές μας, κατά τη διάρκεια της εγκατάστασης. Σε πρώτη φάση η εγκατάσταση ξεκίνησε σε φυσικό μηχάνημα, ενώ στη διάρκεια της πτυχιακής εργασίας μεταφέρθηκε σε ένα εικονικό μηχάνημα (Vm) αρχικά με 2 πυρήνες CPU, 2 GB μνήμη RAM και 14GB σκληρού δίσκου, ενώ στη συνέχεια χρειάστηκε να αυξηθεί η μνήμη στα 4GB.

5.1.1 Συνοπτικά βήματα εγκατάστασης του λειτουργικού

1) Η πρώτη οθόνη που συναντάμε ξεκινώντας τον server μας με την εγκατάσταση του CentOS, μας δίνει τις παρακάτω επιλογές από τις οποίες επιλέγουμε την πρώτη.

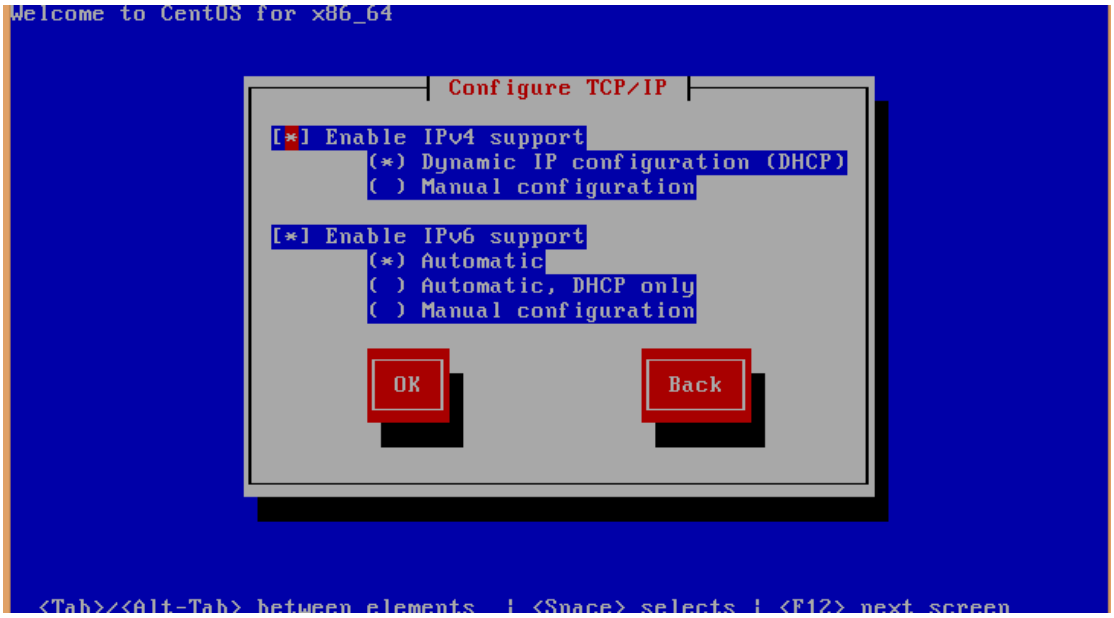
Εικόνα 13 Centos boot loader

Το αμέσως επόμενο βήμα είναι η επιλογή της γλώσσας κατά τη διάρκεια της εγκατάστασης.



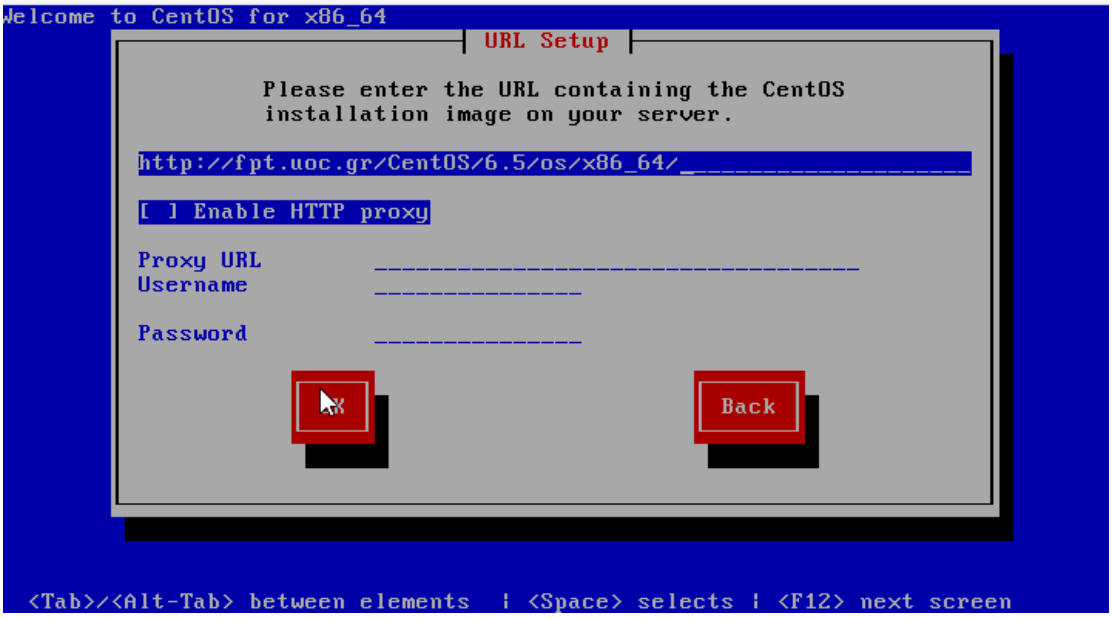
Εικόνα 14 Επιλογή γλώσσας για το λειτουργικό

Παραλείποντας κάποια αυτονόητα βήματα έχουμε φτάσει στις ρυθμίσεις TCP/IP. Συγκεκριμένα, δηλώσαμε χειροκίνητα τις σχετικές IP διευθύνσεις.



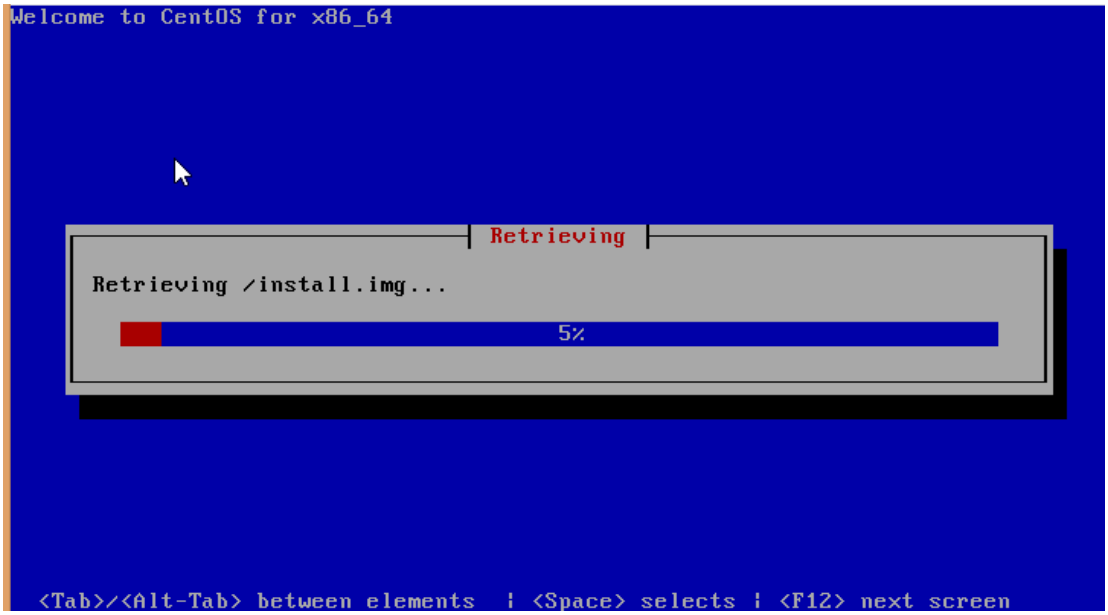
Εικόνα 15 Ρυθμίζοντας τις ip διευθύνσεις

Αφού ρυθμίσαμε επιτυχώς το δίκτυό μας, δηλώνουμε τη διεύθυνση για τη μεταφόρτωση των αρχείων εγκατάστασης.



Εικόνα 16 Δηλώνουμε τη διεύθυνση για την μεταφόρτωση

Η μεταφόρτωση των αρχείων ξεκινά επιτυχώς

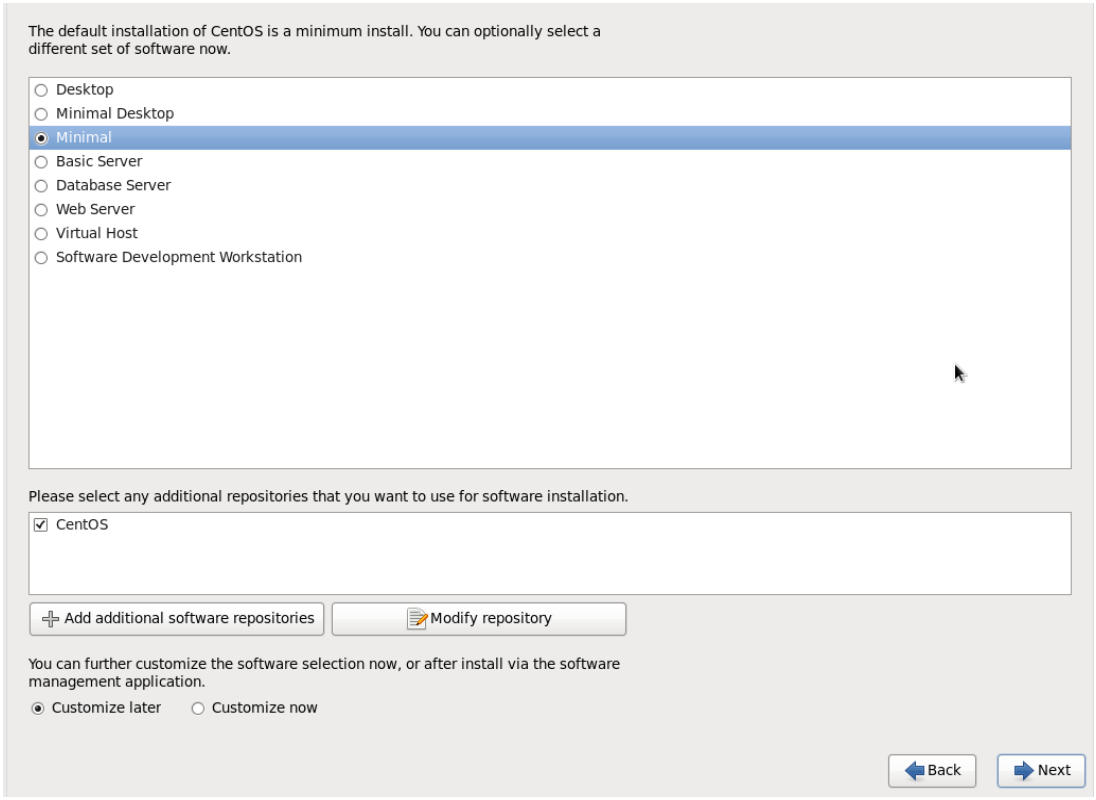


Εικόνα 17 Μεταφορτώνοντας τα αρχεία της εγκατάστασης του CentOS

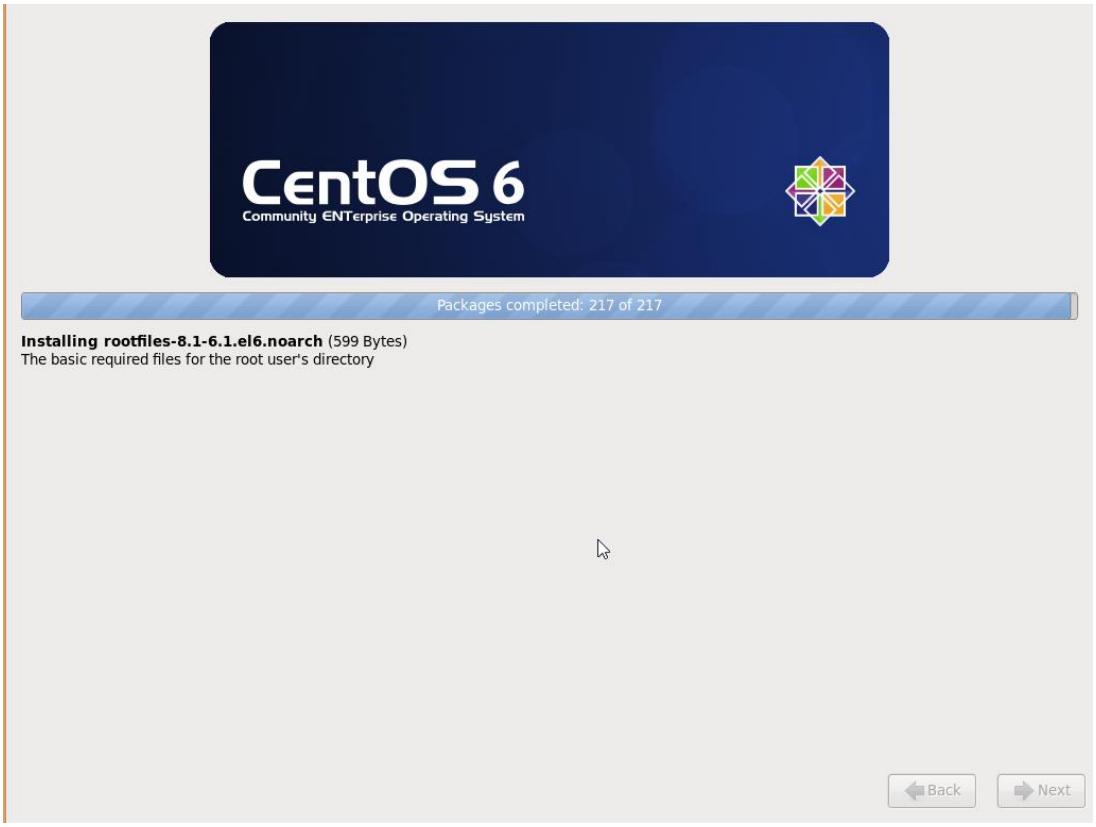
Αφού η μεταφόρτωση έχει τελειώσει, ξεκινά η εγκατάσταση του λειτουργικού μας

Εικόνα 18 Πρώτη εικόνα εγκατάστασης λειτουργικού

Στην οθόνη επιλογής τύπου εγκατάστασης, επιλέγουμε την πιο απλή.
Ο λόγος που επιλέγουμε την minimal έκδοση είναι για να έχουμε μια εγκατάσταση όσο πιο «καθαρή» γίνεται, εγκαθιστώντας και ρυθμίζοντας χειροκίνητα και την παραμικρή εφαρμογή (ακόμα και το wget).

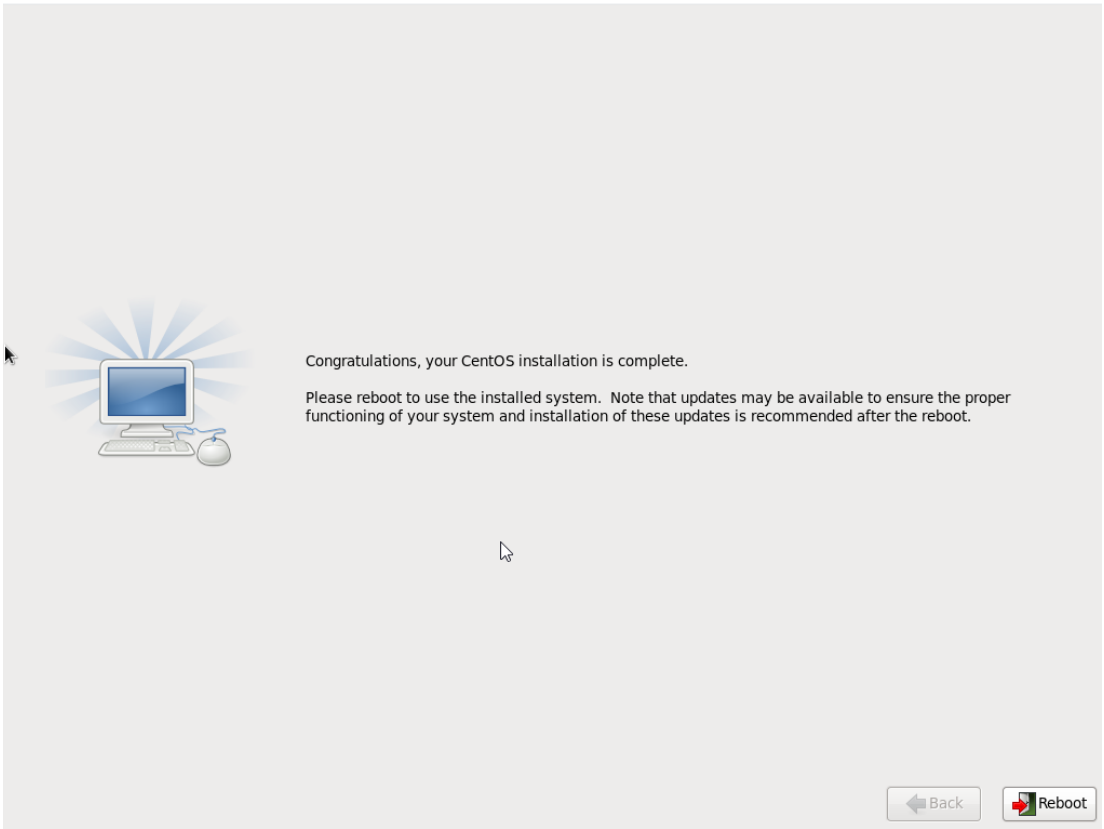


Εικόνα 19 Επιλογή Minimal έκδοσης



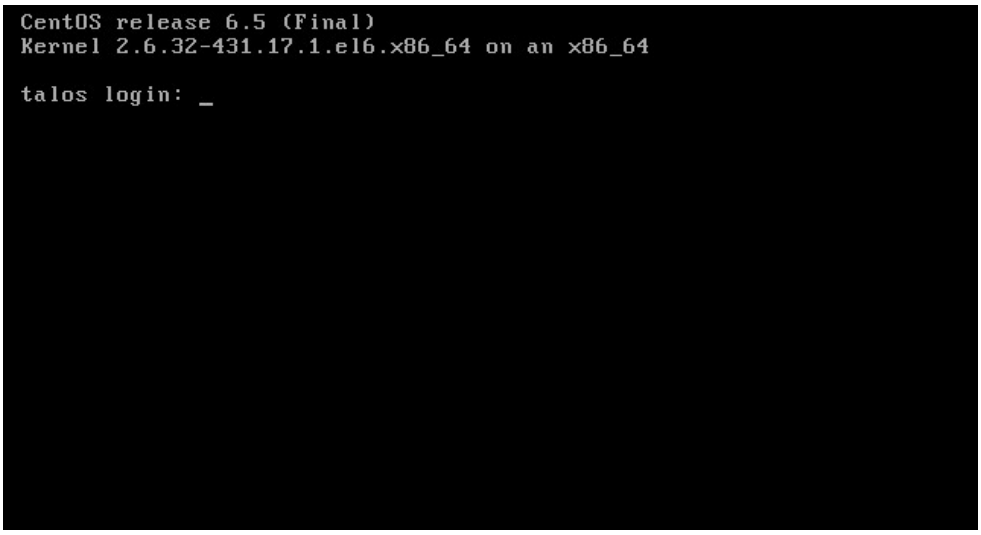
Εικόνα 20 Ολοκλήρωση εγκατάστασης CentOS 6.5

Με την ολοκλήρωση της εγκατάστασης προχωρούμε στην επανεκκίνηση του συστήματος.



Εικόνα 21 Τελευταία εικόνα κατά την εγκατάσταση

Τώρα, είμαστε έτοιμοι να εισέλθουμε στο λειτουργικό σύστημα σύμφωνα με τα συνθηματικά που δώσαμε κατά τη διάρκεια της εγκατάστασης.



Εικόνα 22 Η πρώτη εικόνα μετά την ολοκλήρωση της εγκατάστασης

Εικόνα 23 Εχουμε ησελθει στο συστημα μας για πρωτη φορα

5.1.2 Προετοιμασία λειτουργικού

Η πρώτη ενέργεια είναι να κάνουμε ενημέρωση σε όλα τα πακέτα του λειτουργικού μας με την εντολή

```
yum update
```

Για την παροχή των αναγκαίων πακέτων, εγκαταστήσαμε τα δυο παρακάτω repositories

RPMforge για CentOS 6.x

RHEL EPEL για CentOS 6.x

5.2 Networking

Για τις ανάγκες της υλοποίησης προστέθηκε μια δεύτερη κάρτα δικτύου, η οποία ρυθμίστηκε να λειτουργεί στο ιδιωτικό δίκτυο C class 192.168.200.0, με την ip διεύθυνση 192.168.200.1, στην οποία θα συνδεθεί ο δικτυακός εξοπλισμός, για να παρέχεται η υπηρεσία eduroam.

Η άλλη κάρτα δικτύου συνδέεται στο κυρίως δίκτυο με δημόσια ip διεύθυνση, για να επικοινωνεί ο server μας με την υπόλοιπη δικτυακή υποδομή, αλλά και το διαδίκτυο

5.3 Firewall

Αφού οι δικτυακές μας διεπαφές είναι ρυθμισμένες έτσι όπως ορίσαμε, θα πρέπει να ρυθμίσουμε κατάλληλα και το τοίχος προστασίας του διακομιστή μας, έτσι ώστε από την διεπαφή με το ιδιωτικό δίκτυο, να έχουμε πρόσβαση στο υπόλοιπο δίκτυο και τις υπηρεσίες της σχολής. Αυτό επιτυγχάνεται με τη μέθοδο NAT (Network address translation).

Η μέθοδος NAT (Μεταφραστής Διευθύνσεων Δικτύου), σχεδιάστηκε για απλοποίηση και διατήρηση των IP διευθύνσεων, αφού αυτό που κάνει είναι να επιτρέπει σε ιδιωτικά δίκτυα που χρησιμοποιούν μη εγγεγραμμένες IP διευθύνσεις, να έχουν σύνδεση με το Internet. Το σύστημα NAT λειτουργεί σε κάποιον δρομολογητή ή διακομιστή, ο οποίος συνδέει συνήθως δύο δίκτυα και μεταφράζει τις ιδιωτικές διευθύνσεις του εσωτερικού δικτύου, σε δημόσιες διευθύνσεις, προτού τα πακέτα προωθηθούν σε άλλο δίκτυο. Σαν μέρος αυτής της λειτουργίας, το NAT μπορεί να ρυθμιστεί να κάνει γνωστή μόνο μία διεύθυνση στον έξω κόσμο για ολόκληρο το δίκτυο που συνδέει με αυτόν. Αυτό το χαρακτηριστικό παρέχει επιπλέον ασφάλεια αφού κρύβει ολόκληρο το εσωτερικό δίκτυο πίσω από μία διεύθυνση.

Σε πρώτη φάση καθαρίζουμε το firewall από όλους τους κανόνες

```
iptables –F
iptables -t nat -F
iptables -t mangle -F

iptables -X
iptables -t nat -X
iptables -t mangle -X
```

Αφού έχουμε διαγράψει όλους τους κανόνες του firewall, αποθηκεύουμε τις αλλαγές και κάνουμε επανεκκίνηση της υπηρεσίας firewall.

```
service iptables save
service iptables restart
```

Στη συνέχεια επεξεργαζόμαστε το αρχείο στη διαδρομή/etc/rc.d/rc.και προσθέτουμε την παρακάτω γραμμή

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Με αυτή τη γραμμή ενεργοποιούμε την IP προώθηση

Γνωρίζοντας ότι η διεπαφή με ονομασία eth0 είναι ορισμένη για να επικοινωνεί με το δίκτυο της σχολής, αλλά και το διαδίκτυο, τότε τρέχουμε τις παρακάτω εντολές:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Όπου :

iptables:	Με την εντολή αυτή καλούμε την εφαρμογή iptables
-t nat	Με την επιλογή -t καλούμε τον πινάκα "nat" για να κάνουμε τις κατάλληλες ρυθμίσεις.
-A POSTROUTING	Προσάπτουμε έναν κανόνα στην αλυσίδα POSTROUTING (Η επιλογή -A χρησιμοποιείται για την προσάρτηση).
-o eth0	Η επιλογή -o χρησιμοποιείται για να δηλώσουμε τη δικτυακή διεπαφή που θα χρησιμοποιεί ο κανόνας που θα δηλώσουμε
-j MASQUERADE	Με την επιλογή αυτή δίνουμε την εντολή «μεταμφίεσης» στα πακέτα, δηλαδή την αντικατάσταση διεύθυνσης του αποστολέα από τη διεύθυνση του δρομολογητή.

```
service iptables save
service iptables restart
```

Κάνουμε αποθήκευση και επανεκκίνηση για να εφαρμοστούν οι νέοι κανόνες στο τοίχος προστασίας

Έχουν εφαρμοστεί και άλλοι κανόνες, οι οποίοι δεν αναφέρονται για λόγους ασφαλείας

Σε αυτό το σημείο συνδέσαμε ένα φορητό υπολογιστή στη διεπαφη δικτύου με τις ρυθμίσεις για ιδιωτικό δίκτυο, δίνοντας του στατικές ρυθμίσεις στο φορητό, για να ελέγξουμε αν οι ρυθμίσεις μας έχουν γίνει σωστά.

5.4 DHCP

Με τον όρο DHCP (Dynamic Host Configuration Protocol) αναφερόμαστε σε ένα μηχανισμό δυναμικής διαχείρισης υπολογιστών, αναφορικά με τη σουίτα πρωτοκόλλων TCP/IP .

Το TCP/IP είναι ουσιαστικά ένα λογισμικό που τρέχει σε έναν δρομολογητή ή και σε κάποιο διακομιστή και είναι υπεύθυνο για να διευθετεί όλα τα θέματα επικοινωνίας, με τις υπόλοιπες συσκευές του δικτύου που έχει πρόσβαση. Για να λειτουργήσει το ίδιο λογισμικό σε όλες τις δικτυακές συσκευές, υπάρχει η ανάγκη να το ξεκινήσουμε σε κάθε συσκευή με τις αντίστοιχες παραμέτρους,για αυτήν και για τη θέση της στο δίκτυο. Η αρχικοποίηση (initialization) μπορεί να γίνει κατά τη διάρκεια της εκκίνησης (αν το πρωτόκολλο dhcp είναι ενσωματωμένο στο λειτουργικό σύστημα), ή με την κλήση του πρωτοκόλλου από κάποια εφαρμογή (αν το πρωτόκολλο ενσωματώνεται σε εφαρμογή). Οι παράμετροι αυτές μπορούν να οριστούν τοπικά, και ξεχωριστά, για κάθε δικτυακή συσκευή. Κάτι τέτοιο όμως δημιουργεί αρκετά προβλήματα.

Απαιτείται μεγάλος φόρτος εργασίας από το διαχειριστή του δικτύου, η οποία είναι χρονοβόρα και επιρρεπής σε λάθη.

Το να διατηρούνται οι παράμετροι ενημερωμένες χρειάζεται συνεχής εργασία, η οποία αυξάνεται γεωμετρικά με τις αλλαγές που συμβαίνουν στο δίκτυο, ειδικά αν υπάρχουν υπολογιστές που αλλάζουν συνεχώς θέση. (φορητοί Η/Υ, smartphones).

Για παράδειγμα, η αλλαγή μίας κοινής παραμέτρου για τις δικτυακές συσκευές που ανήκουν στο ίδιο δίκτυο (π.χ. τοπική διεύθυνση ενός router), απαιτεί αλλαγές σε κάθε συσκευή.

Μερικά μηχανήματα μπορεί να μην έχουν αποθηκευτικό χώρο για να κρατήσουν τις ρυθμίσεις.

Σε περιπτώσεις έλλειψης διευθύνσεων, ή ένα δίκτυο με συνεχείς μεταβολές, είναι σπατάλη πόρων, το να δίνουμε μόνιμη διεύθυνση, σε μια συσκευή που δεν λειτουργεί σε σταθερή βάση

Όλοι αυτοί οι λόγοι οδήγησαν στην ανάγκη για έναν αυτόματο μηχανισμό διαχείρισης των TCP/IP πρωτοκόλλων. Ο μηχανισμός DHCP είναι αυτή τη στιγμή ο πιο προηγμένος μηχανισμός.

Το DHCP παρέχει παραμέτρους ρυθμίσεων για ένα μοντέλο δικτύου πελάτη-διακομιστή. Οι DHCP server δεσμεύουν τις διευθύνσεις του δικτύου και στέλνουν τις πληροφορίες για αυτές στους χρήστες. Το DHCP αποτελείται από δύο τμήματα. Το πρώτο είναι το πρωτόκολλο που στέλνει τις παραμέτρους ρυθμίσεων από τον server στο χρήστη και το δεύτερο είναι ο μηχανισμός για να αντιστοιχίζει τις διευθύνσεις στους χρήστες.

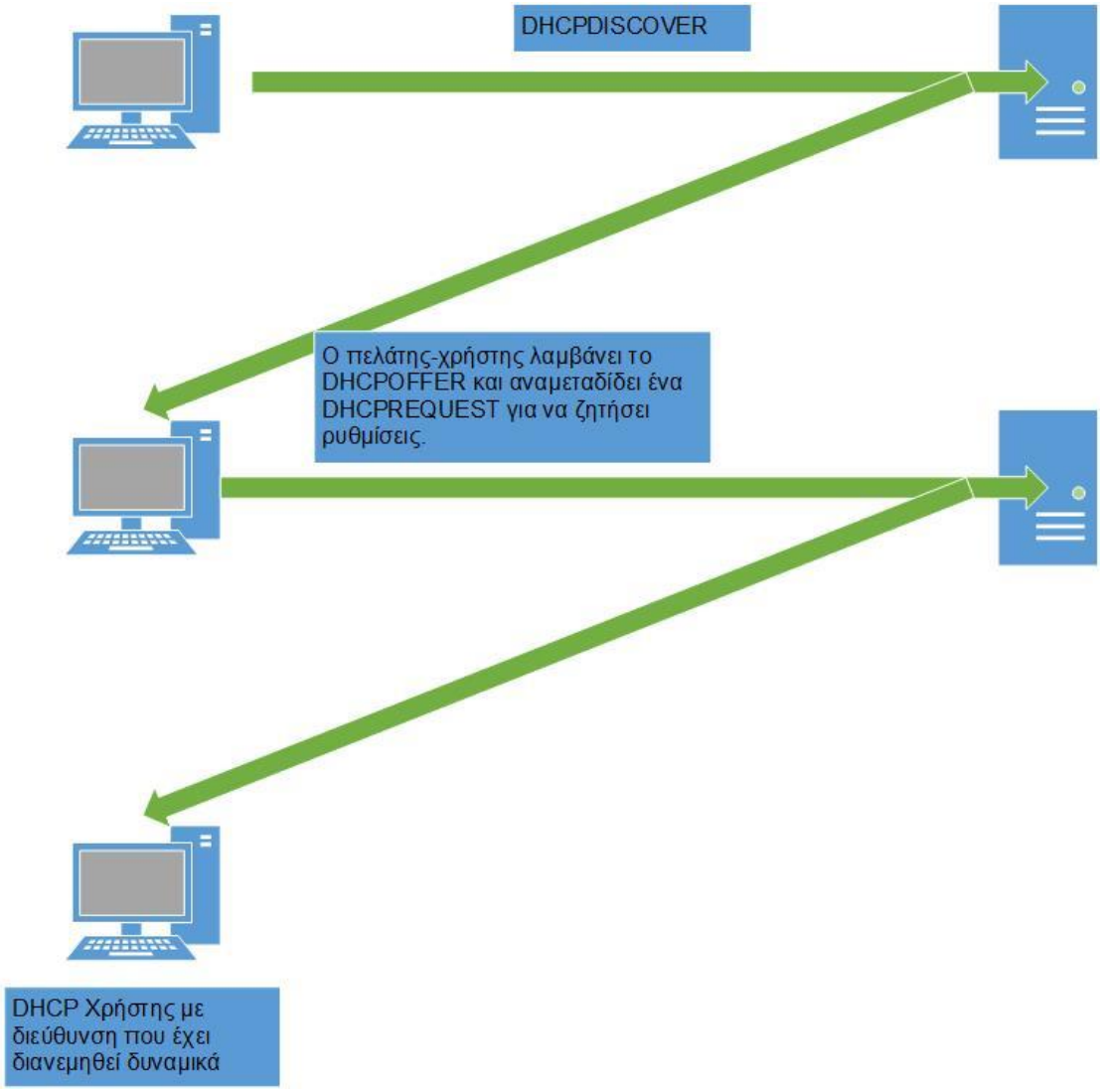
5.4.1 Αντιστοίχηση διευθύνσεων IP

Το DHCP υποστηρίζει 3 μηχανισμούς για να αντιστοιχίζει διευθύνσεις.

Αυτοί είναι:

- Αυτόματη αντιστοίχηση (με αντιστοίχηση μόνιμης διεύθυνσης)
- Δυναμική αντιστοίχηση (με διεύθυνση με ημερομηνία λήξης)
- Χειροκίνητη αντιστοίχηση (ο διαχειριστής κανονίζει ότι θεωρεί καλύτερο)
- Αποστολή παραμέτρων ρύθμισης

Ο χρήστης στέλνει μήνυμα στο server για να του ζητήσει τις παραμέτρους και ο server ανταποκρίνεται με ένα μήνυμα που τις περιέχει.



Εικόνα 24 Μοντέλο Χρήστη-Διακομιστή dhcp

Ο πελάτης (Client) και ο διακομιστής (Server) εμπλέκονται σε μία ανταλλαγή μηνυμάτων ώστε να λάβει ο πελάτης τις ζητούμενες ρυθμίσεις, με την ακόλουθη σειρά:

1. Ο πελάτης μεταδίδει DHCPDISCOVER.
2. Ο διακομιστής απαντά με ένα μήνυμα DHCPOFFER.
3. Ο πελάτης-χρήστης λαμβάνει το DHCPOFFER και αναμεταδίδει ένα DHCPREQUEST για να ζητήσει ρυθμίσεις.

Αν κάποιοι διακομιστές δεν προτιμήθηκαν από τον πελάτη (σε δίκτυα με άνω του ενός διακομιστή), δηλαδή κατανοούν την DHCPREQUEST ως απόρριψή τους, τότε ο διακομιστής που επελέγη με την DHCPREQUEST απαντά με το μήνυμα DHCPACK, που περιέχει τις παραμέτρους για τον πελάτη.

Ο πελάτης λαμβάνει την DHCPACK και ρυθμίζεται με βάση αυτές. Αν λάβει την εντολή DHCPNAK (απόρριψη), ξαναρχίζει τη διαδικασία.

Ο πελάτης μπορεί να ελευθερώσει τη διεύθυνσή του με το μήνυμα DHCPRELEASE στο διακομιστή.

Ο διακομιστής λαμβάνει την DHCPRELEASE και σημειώνει τις σχετικές ρυθμίσεις ως ελεύθερες.

Στις περισσότερες περιπτώσεις, ο client μπορεί να επαναχρησιμοποιήσει μία διεύθυνση που είχε. Έτσι απλά παρακάμπτει μερικά από τα παραπάνω βήματα.

5.4.2 Ασφάλεια

Το πρωτόκολλο DHCP δεν διαθέτει κάποιο μηχανισμό ασφαλείας.

Η αυτόματη ανάκτηση διεύθυνσης και IP των διακομιστών DNS μπορεί να δημιουργήσει τα εξής προβλήματα.

1. Κάποιος κακόβουλος χρήστης μπορεί να παρεμβάλει ένα διακομιστή DHCP ο οποίος:
2. Θα δίνει κακόβουλες διευθύνσεις διακομιστών DNS, με αποτέλεσμα όσοι τον χρησιμοποιούν να είναι ευάλωτοι σε επιθέσεις.
3. Θα δίνει ψεύτικες διευθύνσεις, με αποτέλεσμα να μη μπορούν οι υπολογιστές-πελάτες να συνδεθούν στο δίκτυο (επίθεση άρνησης εξυπηρέτησης – Denial of Service attack)
4. Μπορεί κάποιος να ζητάει συνεχώς διευθύνσεις από το διακομιστή DHCP (είτε κακόβουλα είτε λόγω αστοχίας υλικού ή λογισμικού), με αποτέλεσμα να τελειώσουν όλες οι διευθύνσεις που μπορεί να παρέχει ο διακομιστής DHCP (επίθεση άρνησης εξυπηρέτησης - Denial of Service attack).

5.4.3 Εγκατάσταση Dhcpd

Εμείς για τις ανάγκες της υλοποίησης θα χρησιμοποιήσουμε το πρόγραμμα DHCPD το οποίο θα αναλάβει τον ρόλο του DHCP server, όπου το εγκαθιστούμε με την παρακάτω εντολή

```
yum install dhcp
```

Οι ρυθμίσεις ανάλογα με τη σχεδίαση του δικτύου έχουν και το ανάλογο επίπεδο δυσκολίας. Επειδή στο δίκτυό μας, οι ασύρματες συσκευές πρόσβασης είναι δέκα και είναι εύκολα διαχειρίσιμο, επιλέξαμε μια απλή σχεδίαση του δικτύου. Το configuration file του dhcpd το βρίσκεται στη διαδρομή **/etc/dhcp/dhcpd.conf** και περιέχει τα εξής στοιχεία:

```
subnet 192.168.200.0 netmask 255.255.255.0 {
          range 192.168.200.10 192.168.200.250;
          default-lease-time 360; max-lease-time 500;
          option subnet-mask 255.255.255.0;
          option broadcast-address 192.168.200.255;
          option routers 192.168.200.1;
          option domain-name-servers 194.177.198.2 , 194.177.198.1;
         }
```

Σύμφωνα με αυτά που έχουμε δηλώσει στο παραπάνω configuration file ο dhcpd μας συμπεριφέρεται ως εξής:

Το δίκτυο που έχει να διαχειριστεί είναι το 192.168.200.0 .

Για λόγους διαχείρισης το εύρος των IP διευθύνσεων που του έχουμε ορίσει να αναθέτει στις δικτυακές συσκευές είναι από την 192.168.200.10 έως και 192.168.200.250

Το lease time ή ο χρόνος μίσθωσης είναι ρυθμισμένος στα 360 δευτερόλεπτα (6 ώρες) και ο μέγιστος στα 500 (8,5 ώρες). Δηλαδή αν κάποιος χρήστης πάει να χρησιμοποιήσει πάνω από 6 ώρες μια διεύθυνση τότε ο server θα πραγματοποιήσει το μέγιστο lease time στις 8.5 ώρες. Αν τυχόν και στις 8.5 ώρες συνεχίσει να το χρησιμοποιεί τότε ο dhcpd θα του αναθέσει την ίδια IP διεύθυνση χωρίς να διακοπεί η χρήση του δικτύου.

Ο dhcpd ανακοινώνει στις συσκευές ότι η προεπιλεγμένη πύλη είναι η 192.168.200.1 και domain name servers είναι οι 194.177.198.2 , 194.177.198.1

Δηλαδή από τη στιγμή που καταφέρουμε να συνδεθούμε στο ασύρματο δίκτυο eduroam ένα σύνολο ρυθμίσεων που θα μας αναθέσει ο dhcpd είναι :

IP address	192.168.200.54
Netmask	255.255.255.0
Gateway	192.168.200.1
Dns	194.177.198.2 , 194.177.198.1

Στη συνέχεια πραγματοποιήθηκε η εγκατάσταση του freeradius

5.5 FreeRadius

Το πακέτο FreeRADIUS περιλαμβάνει ένα διακομιστή RADIUS, μια BSD βιβλιοθήκη-πελάτη, μια βιβλιοθήκη PAM (Pluggable Authentication Modules) και μια συνιστώσα του Apache. Στις περισσότερες περιπτώσεις, η λέξη FreeRADIUS αναφέρεται στο διακομιστή RADIUS.

Όταν οι ρυθμίσεις και οι πολιτικές του FreeRADIUS είναι αποθηκευμένες στη μνήμη RAM, τότε ο διακομιστής είναι σε θέση να εκτελεί 10 από τις 1000 πιστοποιήσεις PAP ανά δευτερόλεπτο. Οι δυνατότητες απόδοσης εξαρτώνται από έναν αριθμό παραγόντων συμπεριλαμβανομένων και των ακόλουθων:

- Τύπος Βάσης δεδομένων (LDAP, SQL).
- RAM, CPU, χωρητικότητα δίσκου, ρυθμός μετάδοσης του δικτύου και λανθάνοντες χρόνοι.
- Χρήση της EAP (το SSL προκαλεί σημαντική επιβάρυνση στη CPU)
- Πολυπλοκότητα των πολιτικών ασφαλείας.

Το πακέτο FreeRADIUS είναι η ευρύτερα διαδεδομένη ανοιχτού κώδικα έκδοση διακομιστή RADIUS στον κόσμο. Αποτελεί τη βάση για πολλές εμπορικές εφαρμογές. Εξυπηρετεί τις ανάγκες Authentication-Authorization-Accounting (AAA) πολλών εταιρειών-και ISPs πρώτου επιπέδου. Επίσης, χρησιμοποιείται ευρέως στην ακαδημαϊκή κοινότητα, συμπεριλαμβανομένου του eduroam. Ο διακομιστής είναι γρήγορος και επεκτάσιμος σε όλα τα χαρακτηριστικά του.

Η εγκατάσταση των σχετικών πακέτων έγινε με την παρακάτω εντολή (Εικόνα 25)

```
yum install  freeradius freeradius-utils
```

Το πακέτο freeradius-utils εγκαταστάθηκε γιατί περιλαμβάνει προγράμματα που θα μας χρειαστούν για δοκιμές στη συνέχεια.

Για να μπορούμε να πιστοποιούμε τους χρήστες του ιδρύματος, χρειαζόμαστε την επέκταση του ldap για τον freeradius. που την εγκαθιστούμε με την παρακάτω εντολή

```
yum install freeradius-ldap.x86_64
```

```
[root@talos ~]# yum install freeradius-ldap.x86_64
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.ntua.gr
 * epel: ftp.ntua.gr
 * extras: ftp.ntua.gr
 * updates: centosp5.centos.org
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package freeradius-ldap.x86_64 0:2.1.12-4.el6_3 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package               Arch          Version                 Repository   Size
================================================================================
Installing:
 freeradius-ldap       x86_64        2.1.12-4.el6_3          base         61 k

Transaction Summary
================================================================================
Install       1 Package(s)

Total download size: 61 k
Installed size: 54 k
Is this ok [y/N]:
```

Εικόνα 25 Εγκατάσταση του πακέτου FreeRadius-ldap

Σε αυτό το σημείο, είμαστε έτοιμοι να ρυθμίσουμε την επέκταση του ldap και να ξεκινήσουμε τις πρώτες δοκιμές

Αρχικά επεξεργαζόμαστε το σχετικό αρχείο του freeradius που είναι διαθέσιμο στην διαδρομή /etc/radbmodules/ldap, με έναν απλό κειμενογράφο, προκειμένου να το προσαρμόσουμε στις απαιτήσεις μας

```
ldap {

      server = "ldap.chania.teicrete.gr"

      port= 636

      identity = "cn=readrightsonly ,ou=Special,dc=chania,dc=teicrete,dc=gr"

      password = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx”

      basedn = "dc=chania,dc=teicrete,dc=gr"

      filter = "(|(mail=%{%{Stripped-User-Name}:-%{User-Name}})(eduPersonPrincipalName=%{%{Stripped-User-Name}:-
%{User-Name}}))"

……

}
```

Το εργαλείο που θα χρησιμοποιηθεί για τις δοκιμές σε τοπικό επίπεδο είναι το radtest.

Η χρήση της εντολής μπορεί να γίνει με τις παρακάτω παραμέτρους :

Usage: radtest [OPTIONS] **user** passwd **radius-server[:port]** nas-port-number **secret** [ppphint] [nasname]

Η σύνταξη της εντολής στις πρώτες δοκιμές ήταν ως εξής (Εικόνα 26)

```
radtest –t pap tl3384 “xxxxx” localhost 1 testing123
```

Εδώ λέμε στον radius server να πιστοποιήσει το χρήστη *tl3384* χωρίς κάποια κρυπτογράφηση, μόνο με απλό κείμενο, πράγμα το οποίο δεν το θέλουμε σε καμία περίπτωση.

```
[root@wifi ~]# radtest -t pap tl3384 "[redacted]" localhost 1 testing123
Sending Access-Request of id 4 to 127.0.0.1 port 1812
        User-Name = "tl3384"
        User-Password = "[redacted]"
        NAS-IP-Address = 194.177.198.8
        NAS-Port = 1
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=4, length=20
[root@wifi ~]# radtest -t chap tl3384 "[redacted]" localhost 1 testing123
Sending Access-Request of id 49 to 127.0.0.1 port 1812
        User-Name = "tl3384"
        CHAP-Password = 0x31d68fdbd496baf674bbee7cf7d609ea26
        NAS-IP-Address = 194.177.198.8
        NAS-Port = 1
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=49, length=20
```

Εικόνα 26 Πρώτη προσπάθεια πιστοποίησης

Στη δεύτερη εντολή

```
radtest –t chap tl3384 “xxxx” localhost 1 testing123
```

του λέμε να χρησιμοποιήσει κρυπτογράφηση chap αλλά διαπιστώνουμε ότι ο Ldap server δεν την υποστηρίζει.

Σε αυτή τη φάση της υλοποίησης έχουμε καταφέρει να εγκαταστήσουμε το λειτουργικό μας, να κάνουμε τις απαραίτητες ρυθμίσεις σε αυτό, να εγκαταστήσουμε και να παραμετροποιήσουμε τον freeradius, να πετύχουμε την πρώτη πιστοποίηση χρήστη έστω και με αποστολή plain text του συνθηματικού (password). Με άλλα λόγια, έχουμε δοκιμάσει επιτυχώς τη σύνδεση, μεταξύ του radius server με τον ldap server του ιδρύματος.

5.6 IdP(Identity Provider) και SP(Service Provider) διακομιστές Radius

Οι eduroam Idp είναι Radius servers που είναι υπεύθυνοι για την πιστοποίηση των τοπικών χρηστών, ελέγχοντας τα στοιχεία τους σε ένα τοπικό σύστημα διαχείρισης ταυτότητας. Στην περίπτωσή μας, υπάρχει ένας Ldap server (**Lightweight Directory Access Protocol)**

Οι eduroam SP Radius servers είναι υπεύθυνοι για να προωθούν τα αιτήματα από τους επισκεπτόμενους χρήστες στον Idp από τον οποίο προέρχονται (οι χρήστες) .

Συνήθως τα Ιδρύματα που υποστηρίζουν το eduroam, τρέχουν IdP και SP ταυτόχρονα όπου ο Radius server εκτελεί και τους 2 ρόλους.

5.6.1 Eduroam IdP

Για την εγκατάσταση και παραμετροποίηση του παρόχου ταυτότητας (IdP), έχουμε να επιλέξουμε ανάμεσα από πολλούς τύπους πιστοποίησης του EAP (Extensible

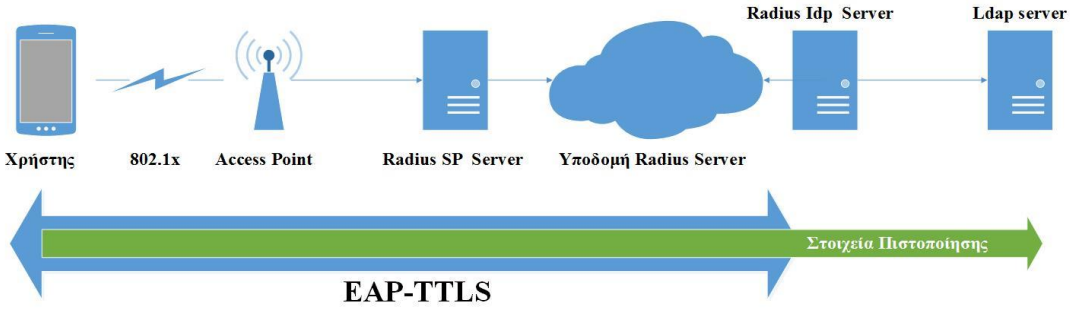
Authentication Protocol). Αυτό που πρέπει να προσέξουμε, είναι η επιλογή μας να είναι συμβατή με την backend εγκατάστασή μας και τις συσκευές που θέλουμε να υποστηρίξουμε (δηλαδή laptops, smartphones κτλ).

Σε πρώτη φάση ο ldap server, που προϋπήρχε, δεν υποστήριζε την αποστολή του συνθηματικού(password) κρυπτογραφημένου (chap), παρά μόνο σε απλό κείμενο (pap). Όπως αναφέραμε και πιο πάνω, κάτι τέτοιο δεν επιτρέπεται να υλοποιηθεί σε κάθε περίπτωση. Για το λόγο αυτό πρέπει να δημιουργηθεί στη βάση του ldap, ένα αλφαριθμητικό πεδίο NT/LM για κάθε χρήστη. Για το λόγο αυτό δημιουργήθηκε ένα php script όπου ο κάθε χρήστης δίνει τα στοιχεία του στον ldap και δημιουργεί το δικό του NT/LM hash. Προκειμένου για την ενεργοποίηση – δημιουργία NT/LM hashes στο λογαριασμό του, ο κάθε χρήστης του Ιδρύματος στα Χανιά, μπορεί να επισκεφτεί την ιστοσελίδα https://www.chania.teicrete.gr/eduroam/

Το επόμενο βήμα είναι να ρυθμίσουμε στο Radius server τους τύπους EAP (Extensible Authentication Protocol) που θέλουμε να χρησιμοποιεί. Έτσι διαμορφώσαμε το αρχείο **eap.conf** όπως φαίνεται παρακάτω:

```
eap {
        default_eap_type = ttls
        timer_expire     = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no
        max_sessions = 4096
        # Supported EAP-types
#Md5
        md5 {
        }
#EAP-TLS
        tls {
                certdir = ${confdir}/certs/
                cadir = ${confdir}/certs/
                private_key_password = xxxxxxxxx
                private_key_file = ${certdir}/server.key
                certificate_file = ${certdir}/server.pem
                CA_file = ${cadir}/ca.pem
                dh_file = ${certdir}/dh
                random_file = ${certdir}/random
                fragment_size = 1024
                include_length = yes
                check_crl = yes
                CA_path = ${cadir}
        #  The TTLS
        ttls {
                default_eap_type = mschapv2
                copy_request_to_tunnel = yes
                use_tunneled_reply = yes
                virtual_server = "eduroam-inner-tunnel"
        }
        peap {
                default_eap_type = mschapv2
                copy_request_to_tunnel = yes
                use_tunneled_reply = yes
                virtual_server = "eduroam-inner-tunnel"
        }
```

Όπως παρατηρούμε στο configuration file υποστηρίζονται αρκετοί τύποι πιστοποίησης, αλλά εμείς έχουμε προεπιλέξει τον EAP-TTLS (Εικόνα 27) που θεωρείται και ο πιο ασφαλής .



Εικόνα 27 Λειτουργία EAP-TTLS

5.6.2 eduroam SP

Η πολιτική του server εφαρμόζεται με την ενεργοποίηση ορισμένων modules σε συγκεκριμένη σειρά. Αυτά τα modules ρυθμίζονται χωριστά και βρίσκονται στον υποκατάλογο στο /etc/raddb/modules/.Το πως θα ενεργοποιηθούν αυτά τα modules ορίζεται στα λεγόμενα virtual servers, που καθορίζονται στο /etc/raddb/sites-available /eduroam. Για τη δημιουργία του δικού μας SP για λογαριασμό του eduroam δημιουργήσαμε τον virtual server eduroam και περιέχει τα παρακάτω :

```
server eduroam {

   authorize {
                        auth_log
                        eap
                        suffix
                        }

   authenticate{
                        eap
                        }

   preacct {
                        suffix
}
            accounting {
                        detail
                        attr_filter.accounting_response
      }
       post-auth {
                    reply_log
                    Post-Auth-Type REJECT {
                    reply_log
                    attr_filter.access_reject
                  }
      }

      pre-proxy {
                    pre_proxy_log
                    if (Packet-Type != Accounting-Request) {
                    attr_filter.pre-proxy
                   }
      }

      post-proxy {
            post_proxy_log
            attr_filter.post-proxy
      }
}
```

Για να υποβληθεί το αίτημα (proxy) σε απομακρυσμένο radius server, υλοποιούνται σε σειρά οι ακόλουθες διαδικασίες :

authorize → authenticate → pre-proxy

Όταν το πακέτο έχει προωθηθεί στον απαιτούμενο server, η απάντηση έρχεται πίσω με την εξής σειρά :

post-proxy → post-auth

Σε κάθε διαδικασία (από αυτές που οριοθετούνται με τα {} σύμβολα όπως {eap }) που εκτελεί ο server σύμφωνα με το αρχείο **eduroam** περιέχονται τα ονόματα των modules που πρέπει να εκτελεστούν. Παρακάτω τα βλέπουμε ένα προς ένα.

- **auth_log**: γίνεται καταγραφή του εισερχόμενου πακέτου στο σύστημά μας. Αυτό χρειάζεται για να εκπληρωθούν οι ανάγκες του eduroam SP.
- **suffix**: επιβλέπει τη δομή του πακέτου για να αναλύσει το realm στον τύπο του eduroam (που διαχωρίζεται από το σύμβολο @)
- **pre_proxy_log**: γίνεται πάλι καταγραφή του πακέτου στο σύστημα. Υπάρχουν πρόσθετα χαρακτηριστικά που προστέθηκαν κατά τη διάρκεια της διαδικασίας ελέγχου , τα οποία έχουν μεγάλη χρησιμότητα κατά τη διάρκεια ελέγχου.
- **attr_filter.pre-proxy**: εδώ αφαιρούνται τα ανεπιθύμητα χαρακτηριστικά από το πακέτο πριν αποσταλούν στον επόμενο server (upstream)
- **post_proxy_log**: γίνεται καταγραφή των reply packets στο σύστημά μας-έτσι όπως έχουν ληφθεί από τον αντίστοιχο server (upstream server)
- **attr_filter.post-proxy**: εδώ αφαιρούνται τα ανεπιθύμητα χαρακτηριστικά από το πακέτο της απάντησης και στέλνονται πίσω στα σημεία πρόσβασης (ασύρματα/ενσύρματα)
- **reply_log**: αφού γίνει φιλτράρισμα των χαρακτηριστικών, καταγράφεται το πακέτο απάντησης στο σύστημά μας

5.6.3 Virtual server eduroam:

Όπως είδαμε στο configuration eduroam IdP, για να κάνουμε χρήση του **ttls** ή του **peap** χρησιμοποιήσαμε την παράμετρο

virtual_server = "eduroam-inner-tunnel”

Έτσι δημιουργούμε ένα configuration file στη διαδρομή /etc/raddb/sites-available/ με την ονομασία “eduroam-inner-tunnel” που έχει την παρακάτω μορφή :

```
server eduroam-inner-tunnel {

authorize {
      auth_log
      eap
      suffix
      mschap
      ldap
      pap
}
authenticate {
       Auth-Type PAP {
            pap
      }
       Auth-Type MS-CHAP {
            mschap
       }
       eap
}
post-auth {
       reply_log
       Post-Auth-Type REJECT {
       reply_log
       }
}
}
```

Παρακάτω δείχνουμε ένα προς ένα τα modules που πρόκειται να εκτελεστούν.

- **auth_log**: γίνεται καταγραφή του εισερχομένου πακέτου στο σύστημά μας. Αυτό χρειάζεται για να εκπληρωθούν οι ανάγκες του eduroam SP. Να σημειωθεί ότι μπορεί να περιέχονται μέσα σε αυτή την καταγραφή το συνθηματικό του κάθε χρήστη σε καθαρή μορφή κειμένου στην περίπτωση που χρησιμοποιείται η μέθοδος TTLS-PAP.
- **eap**: Αν η EAP πιστοποίηση περιέχει ένα άλλο EAP-instance στο εσωτερικό της τότε το eap-module θα την αποκωδικοποιήσει . Στην περίπτωσή μας έχουμε το TTLS.
- **mschap**: αυτό το module ενεργοποιείται μόνο όταν γίνεται χρήση PEAP-MSCHAPv2 ή TTLS-MSCHAPv2 . Απλά μαρκάρει τα πακέτα ότι θα πιστοποιηθούν αργότερα με τους αλγόριθμους MS-CHAP.
- **Ldap**: χρησιμοποιείται για δηλώσουμε την χρήση του module ldap έτσι ώστε ο έλεγχος για την πιστοποίηση να γίνεται με τα στοιχεία που περιέχει ο κατάλογος του ldap.
- **reply_log**: καταγράφεται το πακέτο απάντησης στο σύστημά μας.

5.6.4 Ορισμός των συσκευών χρηστών του RADIUS server.

Ο FreeRADIUS ορίζει τους συνδεμένους RADIUS clients, δηλαδή τις συσκευές που έχουν τη δυνατότητα να στέλνουν αιτήματα πρόσβασης στον Radius Server. Το αρχείο /etc/raddb/clients.conf είναι υπεύθυνο για τους Radius clients. Αυτό το αρχείο πρέπει να έχει καταχωρημένη οποιαδήποτε συσκευή παρέχει πρόσβαση στο δίκτυο του eduroam, πχ Access Point. Κάθε συσκευή μοιράζεται ένα συνθηματικό με τον server όπως φαίνεται στο χαρακτηριστικό configuration file που ακλουθεί:

```
clients.conf
client apnoc_1stfloor
{
   ipaddr      = 192.168.8.254
   secret       = yoursecret
   shortname     = apnoc_1stfloor
   virtual_server = eduroam
}
client thlep_2ndfloor
{
   ipaddr      = 192.168.8.253
   secret       = yoursecret2
   shortname     = thlep_2ndfloor
   virtual_server = eduroam
}
Clients new_building
{
   ipaddr      = 192.168.10.0/24
   secret       = yoursecret3
   shortname     = new_building
   virtual_server = eduroam
}
```

5.6.5 Proxy.conf

Ο FreeRadius περιέχει αρκετές επιλογές για να καθοριστούν οι προωθήσεις των αιτημάτων στο αρχείο /etc/raddb/proxy.conf. Για ένα και μόνο SP eduroam server όλα αυτά μπορεί να φαίνονται υπερβολικά, παρόλα αυτά, απαιτούνται παραμετροποιήσεις. Η δική μας παραμετροποίηση περιέχει τρεις server, δυο για να προωθούν τα αιτήματα στον FLR server της χώρας και έναν για να προωθεί τα αιτήματα στην υποδομή του ΤΕΙ ΚΡΗΤΗΣ στο Ηράκλειο.

Το αμέσως επόμενο κομμάτι που πρέπει να ρυθμίσουμε είναι τα realms. Στο κάθε realm ορίζουμε το σύνολο των server ή αλλιώς το server pool που θέλουμε να χρησιμοποιεί. Στο παρακάτω configuration file βλέπουμε μια παρόμοια παραμετροποίηση με αυτή που έχουμε στη Σχολή Εφαρμοσμένων Επιστημών.

```
proxy server

……

home_server eduroam.radius1.gr {

        type                = auth+acct

        ipaddr              = 172.20.1.2

        port                = 1812

        secret              = secretstuff

        status_check        = status-server

}

 home_server eduroam.radius2.gr {

        type                = auth+acct

        ipaddr              = 172.25.9.3

        port                = 1812

        secret              = secretstuff

        status_check        = status-server

}

home_server  teicrete.gr {

        type                = auth+acct

        ipaddr              = 147.95.4.2

        port                = 1812

        secret              = secret

       status_check         = status-server

}

home_server_pool EDUROAM {

        type                = fail-over

        home_server         = eduroam.radius1.gr

        home_server         = eduroam.radius2.gr
```

```
}
home_server_pool teicrete.gr_pool {
        type = fail-over
        home_server = teicrete.gr
}
 realm DEFAULT {
        pool                    = EDUROAM
        nostrip
#realms_conf
}
realm chania.teicrete.gr {
                nostrip
}
realm "~.*\\.chania\\.teicrete\\.gr$" {
                virtual_server = auth-reject
                nostrip
}
realm teicrete.gr {
                pool = teicrete.gr_pool
                nostrip
}
realm "~.*\\.teicrete\\.gr$" {
                pool = teicrete.gr_pool
                nostrip
}
realm LOCAL {
   virtual_server = auth-reject
   nostrip
}
realm NULL {
  nostrip
}
realm "~.+$" {
   pool = EDUROAM
   nostrip
}
```

6 Παραμετροποίηση Συσκευών Ασύρματης Κάλυψης

6.1 Πρώτη επαφή με τα Access Points

Για την ασύρματη κάλυψη στους χώρους της Σχολής Εφαρμοσμένων Επιστημών στα Χανιά κατά τη διάρκεια της πτυχιακής εργασίας χρησιμοποιήθηκαν διαφόρων τύπων Access Point.

Σε πρώτη φάση παραμετροποιήθηκαν ξανά τα τέσσερα Access Points τύπου Cisco 1300 air bridge έτσι ώστε να είναι εφικτή η ασύρματη πρόσβαση και από υπολογιστές με λειτουργικό πρόγραμμα Mac osX και θέτοντας ως προτεραιότητα την καλύτερη δυνατή λήψη σήματος και όχι το ρυθμό μετάδοσης πληροφορίας. Επίσης διασφαλίσαμε την ασφάλεια από την πλευρά της διαχείρισης για να μην είναι ευπρόσβλητα σε επιθέσεις. Σε δεύτερη φάση αντικαταστάθηκαν όλες οι κεραίες από τα cisco access points καθώς αυτές που προϋπήρχαν ήταν τύπου yagi (Εικόνα28) ενώ τοποθετήθηκαν τύπου omni (πολύ-κατευθυντικές)(Εικονα 29) και μάλιστα σε ζεύγη ανά access point .

Εικόνα 28 Κεραία τύπου yagi

Εικόνα 29 Κεραία τύπου omni

6.2 Παραμετροποίηση υποδομής των Access Points με την υλοποίηση eduroam.

Αφότου υλοποιήθηκε η υποδομή για το eduroam, η δομή των ρυθμίσεων των access points άλλαξε ριζικά. Έπειτα από πρωτοβουλίες του Γραφείου Τηλεπικοινωνιών & Δικτύων, παραλάβαμε άλλα 7 access points ίδιου τύπου και φτάσαμε συνολικά τα 11 access points. Αφού όλα τα access points γύρισαν σε εργοστασιακές ρυθμίσεις έγινε αναβάθμιση στο λειτουργικό τους διότι παρουσίαζαν διάφορα μικροπροβλήματα. Για παράδειγμα, σε κάποια access points δεν συγχρόνιζαν οι ρυθμίσεις μεταξύ κονσόλας και της πλατφόρμας μέσω περιηγητή ιστού. Επίσης ένα από αυτά δεν λειτουργούσε καθόλου, μέχρι και την αναβάθμιση.

Ξεκίνησε εκ νέου η παραμετροποίηση των access points για χρήση μεταβατικής περιόδου με εκπομπή τριών διαφορετικών ασύρματων δίκτυων (**S**ervice **S**et

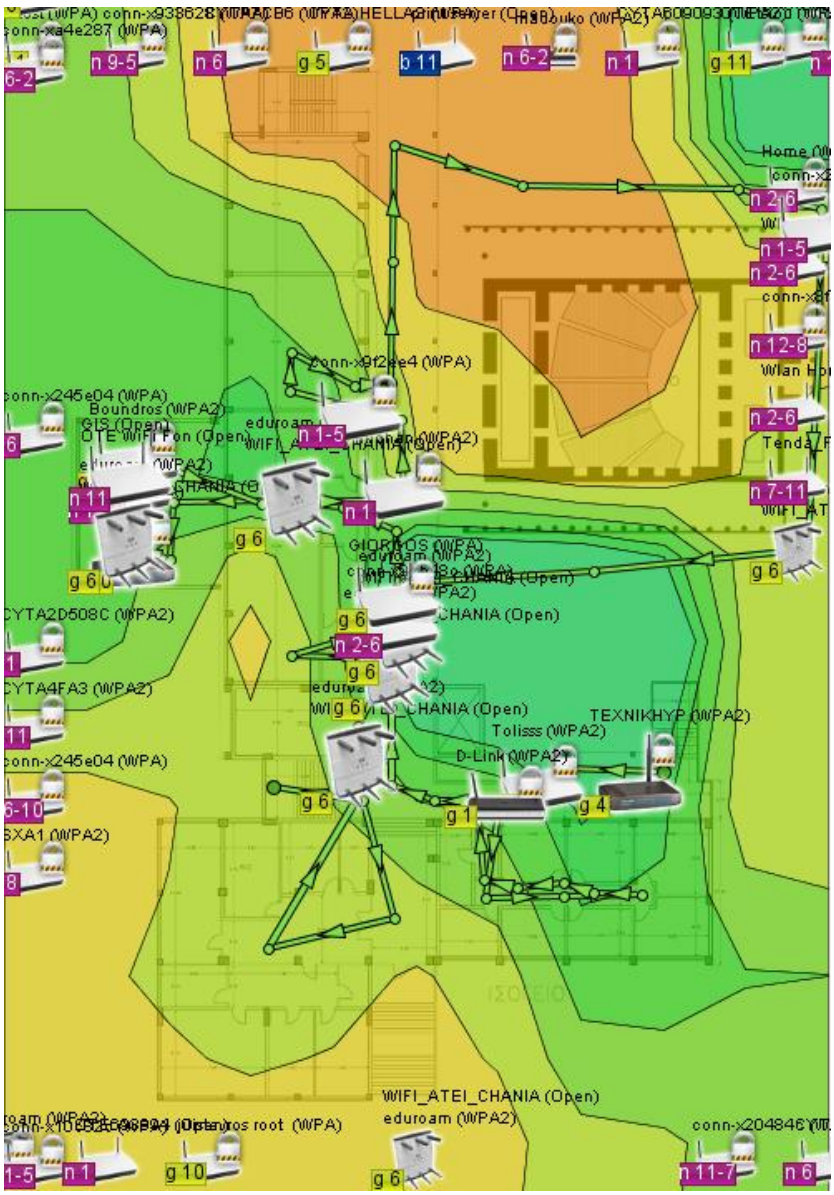
IDentification) τα οποία γεφυρώνουν με την υπόλοιπη δικτυακή υποδομή μέσω τριών διαφορετικών εικονικών δικτύων (VLan)

Το πρώτο από αυτά, με την ονομασία **WIFI ATEI CHANIA**, αφορά την παλαιότερη υποδομή ενώ σήμερα μας παρέχει αποκλειστικά πληροφορίες για τις ενέργειες που πρέπει να ακολουθήσουμε έτσι ώστε να συνδεθούμε στο δεύτερο με την ονομασία **eduroam** το οποίο αφορά την καινούρια υποδομή και είναι το μοναδικό πλέον που μας διασυνδέει στο διαδίκτυο. Ένα τρίτο ασύρματο δίκτυο είναι κρυφό και χρησιμοποιείται αποκλειστικά για λόγους διαχείρισης των access points.

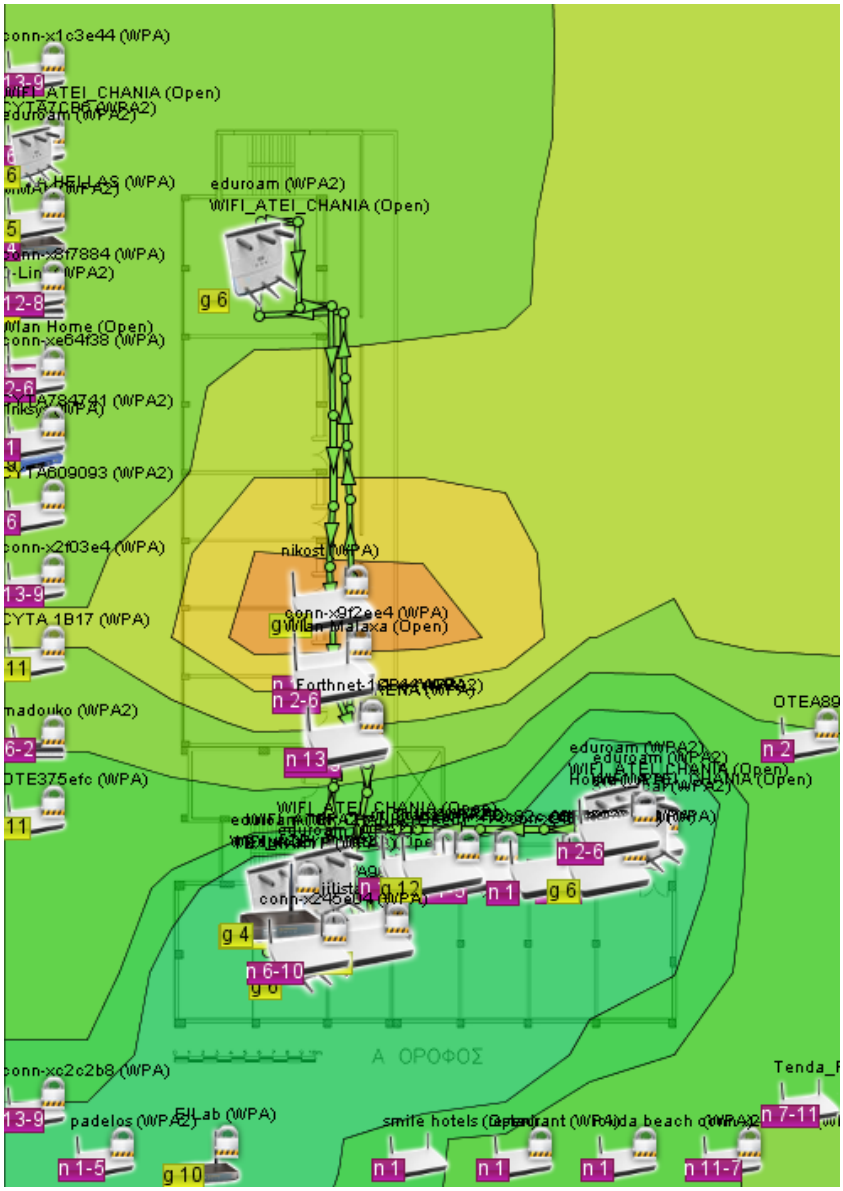
Στο διαχειριστικό περιβάλλον σε μια γέφυρα μεταξύ ενσύρματου και ασύρματου δικτύου έχει δηλωθεί ένα εικονικό δίκτυο το οποίο χρησιμοποιεί ιδιωτικές ip διευθύνσεις για λόγους ασφάλειας.

Στο τελικό μοντέλο εγκατάστασης και παραμετροποίησης των access points θα παραμείνουν 2 SSID, το eduroam και το διαχειριστικό.

Τέλος, μαζί με την νέα παραμετροποίηση, έχει διαμορφωθεί και η τοποθέτησή τους στην τελική τους θέση ώστε να επεκταθεί η ασύρματη κάλυψη όπως φαίνεται και στις κατόψεις, που ακολουθούν.



Εικόνα 30 Κάλυψη Ισόγειου Παλαιού Κτηρίου



Εικόνα 301 Κάλυψη 1ου ορόφου Παλαιού Κτηρίου

Συμπεράσματα

Κατά τη διάρκεια της εκπόνησης της πτυχιακής εργασίας , μου δόθηκε η ευκαιρία να δουλέψω σε πραγματικό περιβάλλον. Χρειάστηκε να διαχειριστώ και να βελτιώσω μια υπηρεσία που ήταν σε λειτουργία πάνω από 7 χρόνια και εξυπηρετούσε τους φοιτητές καθώς και το εκπαιδευτικό και διοικητικό προσωπικό της Σχολής Εφαρμοσμένων Επιστημών στα Χανιά. Επίσης αναπτύχθηκε μια καινούργια υπηρεσία σύμφωνα με τις σύγχρονες ανάγκες για να καλύψει θέματα ασφάλειας και περιαγωγής που δεν μας παρείχε η προηγούμενη εγκατάσταση. Με αυτό τον τρόπο διασφαλίσαμε μέσω κρυπτογράφησης καναλιού την ανταλλαγή δεδομένων των χρηστών και υποστηρίξαμε την περιαγωγή τους στο διαπανεπιστημιακό δίκτυο eduroam.

Δυο περιορισμοί μας δυσκόλεψαν κατά τη διάρκεια της πτυχιακής.

Ο πρώτος είχε να κάνει με την έλλειψη εξοπλισμού που είναι κρίσιμος για δοκιμές με αποτέλεσμα να χρησιμοποιηθεί προσωπικός/ιδιωτικός εξοπλισμός.

Ο δεύτερος και σημαντικότερος είχε να κάνει με την έλλειψη σχετικού πληροφοριακού υλικού για την ανάπτυξη της συγκεκριμένης υπηρεσίας.

Παρά τις δυσκολίες είχα την τύχη να βρω λύσεις και να καταλήξω στην ομαλή λειτουργία της υπηρεσίας.

Θέματα που απορρόφησαν μεγάλο ποσοστό του χρόνου μου είχαν να κάνουν με τον επανασχεδιασμό της παραμετροποίησης των access points καθώς και τον σχεδιασμό της τελικής τοποθέτησής τους, βάσει μελέτης γεωγραφικής κάλυψης χώρου (site survey).

Επεξήγηση Συντομογραφιών

AAA authentication, authorization, accounting

Captive Portal technique forces an HTTP client on a network to see a special web page

CHAP Challenge-Handshake Authentication Protocol

DHCP Dynamic Host Configuration Protocol

EAP Extensible Authentication Protocol

Eduroam education roaming

ETLR top-level radius server

FLR Federation Level Radius

GEANT The pan-European Gigabit Research Network

IEEE Institute of Electrical and Electronics Engineers

IdP Identity Provider

LDAP Lightweight Directory Access Protocol

MS-CHAP Microsoft version of the Challenge-Handshake Authentication Protocol

NAS (Network access server)

NAT Network address translation

PAP Password authentication protocol

RADIUS Remote Authentication Dial In User Service

Realm A realm is commonly appended to a user's user name and delimited with an '@' sign, resembling an email address domain name.

SSID Service Set Identification

SP Service Provider

Πηγές

- http://www.howtoforge.com/
- http://justlinux.com/
- http://www.islab.demokritos.gr/
- http://davidwills.net
- http://freeradius.org/
- http://eduroam.org
- http://www.eduroam.gr
- http://www.terena.org/
- http://www.informit.com/
- http://hermes.di.uoa.gr/RETUDIS/Dhcp/dhcp.html
- http://www.telecom.tuc.gr/courses/net2/winter04-05/exercises/Ethereal_DHCP.pdf
- http://www.windowsecurity.com/articles-tutorials/misc_network_security/DHCP-Security-Part1.html
- http://www.terena.org/
- http://www.geant.net/
- Michael Patrick (January 2001). «RFC 3046 - DHCP Relay Agent Information Option». *Network Working Group*.
- Ralph Droms (March 1997). «RFC 2131 - Dynamic Host Configuration Protocol». *Network Working Group*.
- Hassell, Jonathan (2002). RADIUS - Securing Public Access to Private Resources. O'Reilly & Associates. ISBN 0-596-00322-6
- Νικόλαος Πρέβε (2008) Ασύρματα Δίκτυα Υπολογιστών Ασφάλεια και Απόδοση των Πρωτοκόλλων Εκδόσεις Νέων Τεχνολογιών TCP/IP ISBN 9789606759130