ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Έλεγχος Ταυτότητας Πρόσβασης σε ασύρματα και ενσύρματα δίκτυα με χρήση του 802.1X

Χρήστος Κάλλος

Επιβλέπων καθηγητής: Γιάννης Τζήμας

Αντίρριο – Μάιος 2018

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Αντίρριο, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ονοματεπώνυμο, Υπογραφή
2. Ονοματεπώνυμο, Υπογραφή
3. Ονοματεπώνυμο, Υπογραφή

Αφιέρωση

Στη μητέρα μου Ανθούλα, την αδερφή μου Αναστασία και τον θείο Βασίλη

Ευχαριστίες

Αρχικά θέλω να ευχαριστήσω τον Διαχειριστή Δικτύου και υπεύθυνο helpdesktου Τ.Ε.Ι στο NOCτου Μεσολογγίου,κ. Παναγιώτη Ιλαρίδη για όλη την βοήθεια που μου παρείχε να κατανοήσω την αρχιτεκτονική σχεδιασμού και διαχείρισης Δικτύων, ώστε να μπορέσω να εκπληρώσω την πτυχιακή μου εργασία.

Για τις συμβουλές του και την καθοδήγηση του καθ' όλη την διάρκεια των σπουδών μου οφείλω να ευχαριστήσωτον καθηγητή μου κ.Γιάννη Τζήμα.

Επίσης θέλω να ευχαριστήσωξανά τον καθηγητή μου κ. Γιάννη Τζήμα για την επίβλεψη της παρούσας πτυχιακής εργασίας.

Τέλος, θέλω να ευχαριστήσω την οικογένεια μου για την στήριξη τους όλα αυτά τα χρόνια.

Περιεχόμενα

Πρόλογος

Σε ένα σύστημα ελέγχου ταυτότητας πρόσβασης χρηστών, είναι απαραίτητο ειδικά όταν μιλάμε για εταιρικό περιβάλλον να υπάρχει μια σταθερή και οργανωμένη δικτυακή υποδομή η οποία να βασίζεται αρχικά στις ανάγκες του σήμερα αλλά και του αύριο. Πρέπει να λαμβάνονται υπόψιν κατά το σχεδιασμό αλλά και την υλοποίηση ενός δικτύου όλες οι πιθανές παράμετροι από το αν μιλάμε π.χ. για το κομμάτι του πως θα έχουν πρόσβαση οι χρήστες του αλλά και το πόσο αυστηροί θα είναι οι κανόνες πιστοποίησης για έναν νέο χρήστη του δικτύου ο οποίος θέλει να αποκτήσει πρόσβαση σε αυτό.

Περίληψη

Στην παρούσα πτυχιακή εργασία γίνεται μια μελέτη πάνω στο πως μπορούμε να ορίσουμε και να εφαρμόσουμε το 802.1X ως μια λύση για να έχουμε ένα ασφαλές σύστημα ελέγχου ταυτότητας χρηστών. Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή σε ορισμένα από τα βασικά στοιχεία που αποτελούν ένα δίκτυο. Στη συνέχεια παρουσιάζονται ορισμένες βασικές έννοιες port-basedαυθεντικοποίησης και έπειτα γίνεται μια αναφορά στα πρωτόκολλα RADIUS, EAPOL, EAP-Methods τα οποία συμβάλλουν στη δημιουργία ενός συστήματος port-based αυθεντικοποίησης με βάσει το 802.1X. Στο τέλος της εργασίας προτείνεται και παρουσιάζεται το εργαλείο openNACγια τον έλεγχο ταυτότητας πρόσβασης ενός χρήστη με τη χρήση του 802.1X καθώς και δίνονται οι απαραίτητες οδηγίες για την παραμετροποίηση του δικτυακού εξοπλισμού που χρησιμοποιήθηκεαπό την εταιρεία Cisco.

Λέξειςκλειδί:Μηχανισμόςαυθεντικοποίησης,port-based authentication,RADIUSserver, openNAC, 802.1X, Supplicant, Cisco

1 Βασικά στοιχεία που αποτελούν την αρχιτεκτονική ενός Δικτύου

Σε αυτό το κεφάλαιο ορίζουμε τα βασικά στοιχεία που αποτελούν ένα Δίκτυο. Θα γίνει μια σύντομη αναφορά στις συσκευέςχρηστών οι οποίες μπορούν να αποκτήσουν πρόσβαση σε ένα ενσύρματο ή ασύρματο Δίκτυο (Clients). Στη συνέχεια θαμιλήσουμε για τις συσκευές οι οποίες υλοποιούν ένα Δίκτυο (NetworkHardware και Servers). Τέλος θα γίνει μια επισκόπηση ως προς τα Μέσα που χρησιμοποιούνται στα Δίκτυα για τη σύνδεση όλων τωνδικτυακών συσκευών (Clients, Servers, NetworkHardware) μεταξύ τους.

1.1 Συσκευές χρηστών σε ένα Δίκτυο

Για να κάνει χρήση κάποιος των δυνατοτήτων ενός δικτύου, θα πρέπει να έχει αποκτήσει πρόσβαση σε αυτό μέσα από κάποια συσκευή. Ορισμένες συσκευές παρουσιάζονται ενδεικτικά παρακάτω (Εικόνα 1.1):

- Σταθερός Προσωπικός Ηλεκτρονικός Υπολογιστής (PC)
- Φορητός Προσωπικός Ηλεκτρονικός Υπολογιστής (Laptop)
- PDA ή Smartphone
- Εκτυπωτής (Printer)
- Tablet
- IP Τηλέφωνο

Εικόνα1.1

Οι περισσότεροι χρήστες είναι εξοικειωμένοι στο να χρησιμοποιούν τις παραπάνω συσκευές σε ένα δίκτυο. Με τη χρήση του πρωτοκόλλου 802.1X εστιάζουμε στην αυθεντικοποίηση χρηστών σε επίπεδο θυρών, επιτρέποντας ή απαγορεύοντας την πρόσβαση τους στο δίκτυο.

1.2 Συσκευές που υλοποιούν ένα Δίκτυο

Στην ενότητα αυτή θα αναφερθούμε στις συσκευές οι οποίες υλοποιούν ένα δίκτυο και εξυπηρετούν την ανάγκη των χρηστών για πρόσβαση στο δίκτυο.

Servers:

- Οι Serversσε ένα δίκτυο φιλοξενούν εφαρμογές και βάσεις δεδομένων ούτως ώστε οι χρήστες μέσα στο δίκτυο να μπορούν να έχουν πρόσβαση.Επιπροσθέτως, όπως θα δούμε και στο 2^{o} Κεφάλαιο, ένας Server για τηναυθεντικοποίηση συσκευών χρηστών ‘τρέχει’ το πρωτόκολλο RADIUSστο επίπεδο εφαρμογής.

Switches

- Τα Switch είναι συσκευές οι οποίες παρέχουν σημεία ενσύρματης σύνδεσης σε όλο το μήκος της δικτυακής υποδομής για τις συσκευές χρηστών. Τα switch διαθέτουν πολλαπλές θύρες και υλοποιούν το IEEE 802.3 standard (Ethernet) καθώς και τα IEEE 802.1 bridgeprotocols. Κάθε θύρα διαθέτει υποδοχή για καλώδια τύπου Ethernetτα οποία συνδέονται σε συσκευές χρηστών ή άλλο δικτυακό υλικό. Τα τελευταία χρόνια, καθώς οι απαιτήσεις για υψηλότερες ταχύτητες αυξάνουν, πολλές εταιρείες χρησιμοποιούν switchesτα οποία διαθέτουν θύρες με SFPδιεπαφή. Συνήθως οι SFPθύρες χρησιμοποιούνται για σύνδεση με οπτική ίνα (πολύτροπη ή μονότροπη) κυρίως στον πυρήνα (backbone)του δικτύου.

Routers

- Οι δρομολογητές (Routers) είναι συσκευές οι οποίες δρομολογούν πακέτα ανάμεσα σε δίκτυα ανάλογα με τον προορισμό του κάθε πακέτου. Λειτουργούν σε υψηλότερο επίπεδο σε σχέση με τα switches καθώς σκοπός των routerseίναι να ενώνουν διαφορετικά δίκτυα κάνοντας τα να επικοινωνούν μεταξύ τους. Για παράδειγμα, σε ένα εταιρικό δίκτυο η υποδομή του συνήθως αποτελείται από routersτα οποία συνδέονται με switchesόπου ανήκουν σε διαφορετικά υποδίκτυα, και τα switches με τη σειρά τους συνδέουν στο δίκτυο τις συσκευές των χρηστών.

Access Points

- Στα ασύρματα δίκτυα γίνεται χρήση των accesspoints με σκοπό οι χρήστες ασύρματων συσκευών (π.χ. laptop, κινητό, tablet) να αποκτήσουν πρόσβαση στο δίκτυο. Τα accesspointsδημιουργούν μια ραδιοκυψέλη στην οποία οι ασύρματοι clientsμπορούν να συνδεθούν και να λαμβάνουν ή να στέλνουν δεδομένα στο δίκτυο.Εταιρείες οι οποίες παρέχουν και ασύρματη πρόσβαση στο δίκτυο για λόγους ευχρηστίας και κινητικότητας, συνήθως έχουν εγκατεστημένα accesspointsσε σημεία τέτοια ώστε να είναι εφικτή η περιαγωγή χρηστών. Όπως και στα ενσύρματα δίκτυα, έτσι και στα accesspoints εφαρμόζονται τα IEEE 802.1 bridgeprotocols και IEEE 802.11 πρωτόκολλα ασύρματης πρόσβασης. Με το IEEE 802.11 πρωτόκολλο, πολλές συσκευές χρηστών μπορούν να έχουν πρόσβαση και να επικοινωνούν ταυτόχρονα από το ίδιο accesspoint. Τα accesspointsμπορούν να συνδεθούν σε κάποια Ethernet πόρτα ενόςswitch δημιουργώντας έτσι μια υποδομή ασύρματου δικτύου. Επίσης ορισμένα accesspointsσυμπεριλαμβάνουν μηχανισμούς δρομολόγησης και ονομάζονται ασύρματα routers. Ένα ασύρματο routereίναι ιδανικό για οικιακή χρήση ή χρήση σε μικρές εταιρείες όπου είναι καλό να υπάρχει ένα ασύρματο τοπικό δίκτυο (WLAN) το οποίο παρέχεται από μια συσκευή που συνδέεται στο Internetμέσω μιας γραμμής ψηφιακού συνδρομητή (DSL) ή καλωδιακού modem. Το ασύρματο routerεκτελεί τις λειτουργίες ενός accesspointαλλά επίσης συμπεριλαμβανομένων και των λειτουργιών τουDynamicHostConfigurationProtocol(DHCP) πρωτοκόλλου καιNetworkAccessTranslation(NAT). Έτσι παρέχεται η δυνατότητα στο ασύρματο δίκτυο να χρησιμοποιεί μια επίσημη IPδιεύθυνση η οποία παρέχεται από τον πάροχο Internet υπηρεσιών για πολλαπλές συσκευές χρηστών.

1.3 Μέσα

Τα μέσα σε ένα δίκτυο συνδέουν όλες τις εμπλεκόμενες συσκευές σε αυτό. Στα δίκτυα γίνεται χρήση των παρακάτω κατηγοριών μέσων:

- Καλώδιο
- Οπτική Ίνα
- Αέρας

Καλώδιο

- Η χρήση μεταλλικών καλωδίων είναι η πιοδιαδεδομένη μέθοδος σύνδεσης. Όταν ξεκίνησε η ανάπτυξη των πρώτων δικτύων Η/Υ, η σύνδεση πραγματοποιούταν μέσω ομοαξονικού καλωδίου. Πλέον για τη σύνδεση μέσω καλωδίου γίνεται χρήση καλωδίων σύστροφου ζεύγους Κατηγοριών: CAT5e, CAT6 ή CAT7. Τα δεδομένα περνούν από το μέσο υπό μορφή ηλεκτρικής τάσης, υποστηρίζοντας ροή δεδομένων της τάξης των Gigabitανά δευτερόλεπτο (Gbps). Το πρότυπο IEEE 802.3 (Ethernet) τυποποιεί τη χρήση καλωδίων σύστροφου ζεύγους.

Οπτική Ίνα

- Το καλώδιο οπτικής ίνας αποτελείται από κλωστές από γυαλί οι οποίες άγουν το φως αποτελεσματικά από τη μια άκρη στην άλλη. Βασικό πλεονέκτημα της οπτικής ίνας είναι πως σε σχέση με τα μεταλλικά καλώδια υποστηρίζει πολύ υψηλές ταχύτητες μετάδοσης της τάξεως των Terabitανά δευτερόλεπτο (Tbps) για μεγαλύτερη απόσταση κάλυψης από εκείνη των μεταλλικών καλωδίων. Επίσης υπάρχει μεγαλύτερη ασφάλεια και δεν υπάρχουν εκπομπές ηλεκτρομαγνητικής ακτινοβολίας. Ένα μειονέκτημα θα μπορούσε να είναι το υψηλό κόστος εγκατάστασης της οπτικής ίνας. Βέβαια σε περιπτώσεις όπου για παράδειγμα μία μεγάλη εταιρεία θα πρέπει να παρέχει σύνδεση σε υπαλλήλους της που εργάζονται σε διαφορετικά κτίρια, τότε η χρήση οπτικής ίνας στον πυρήνα (backbone) του δικτύου της αποτελεί μονόδρομο.

Αέρας

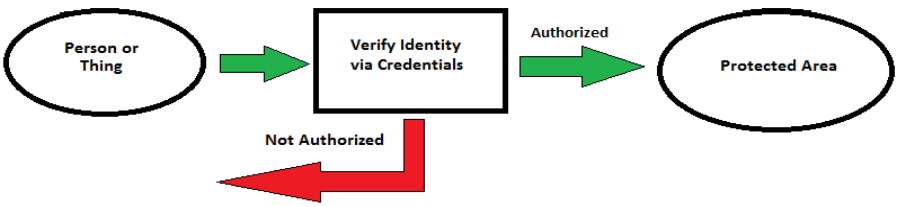
- Ο αέρας αποτελεί μέσο μετάδοσης πληροφορίας σε ένα δίκτυο για ασύρματα συστήματα και χρησιμοποιεί ραδιοκύματα για μεταφορά δεδομένων. Τα ραδιοκύματα συχνοτήτων από 2,4 GHzκαι άνω είναι ο πιο συνηθισμένος τρόπος μετάδοσης σήματος στα ασύρματα δίκτυα. Τα περισσότερα IEEE 802 πρότυπα (όπως τα 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ad, 802.11ah, 802.15 και 802.16) χρησιμοποιούν ραδιοκύματα. Ένα θέμα το οποίο προκύπτει από τη χρήση του αέρα ως μέσο είναι τα εμπόδια τα οποία παρεμβάλλονται μεταξύ συσκευής χρήστη και accesspoint. Εμπόδια όπως ένας τοίχος ή μια συσκευή η οποία εκπέμπει ηλεκτρομαγνητική ακτινοβολία (π.χ. ένας φούρνος μικροκυμάτων) μπορούν να οδηγήσουν σε απώλεια σήματος και σε ορισμένες περιπτώσεις απώλεια σύνδεσης με το δίκτυο. Τα φαινόμενα αυτά μπορούμε να τα αποφύγουμε με σωστό σχεδιασμό του δικτύου και τοποθέτηση των accesspointsσε κατάλληλα σημεία.

2 802.1XPort-Based Έννοιες Αυθεντικοποίησης

Σε αυτό το κεφάλαιο θα εστιάσουμε σε έννοιες οι οποίες αφορούν συγκεκριμένα το 802.1Xπρωτόκολλο και τηνPort-Basedαυθεντικοποίηση. Γίνεται μια εισαγωγή στην ορολογία καιστα πρωτόκολλα τα οποία αποτελούν ένα port-basedσύστημα αυθεντικοποίησης: EAPOL, EAP, EAP-Methods, RADIUS. Τα επόμενα κεφάλαια καλύπτουν τα παραπάνω πρωτόκολλα με μεγαλύτερη λεπτομέρεια. Προς το παρόν θα δούμε σε αυτό το κεφάλαιο το πώς λειτουργούν μεταξύ τους και πώς επιτρέπουν σε ένα σύστημα 802.1Xport-basedαυθεντικοποίησης να λειτουργεί.

2.1 Ορολογία 802.1XPort-Basedαυθεντικοποίησης

Η αυθεντικοποίηση είναι η διαδικασία ταυτοποίησης ενός ατόμου ή αντικειμένου (Εικόνα 2.1). Για παράδειγμα, Η Έλλη φτάνει στο αεροδρόμιο και προσπαθεί να κάνει check-inγια την πτήση της για Παρίσι. Η υπάλληλος της αεροπορικής εταιρείας ζητά από την Έλλη να της δείξει την αστυνομική της ταυτότητα ώστε να επιβεβαιωθεί ότι το άτομο που ισχυρίζεται ότι είναι η Έλλη είναι όντως η Έλλη. Η υπάλληλος ελέγχει την ταυτότητα της Έλλης και επιβεβαιώνει ότι η Έλλη είναι το πρόσωπο που απεικονίζεται και στην ταυτότητα. Οι πληροφορίες της ταυτότητας αποτελούν τα στοιχεία της Έλλης τα οποία είναι αποδεκτά σε διάφορες περιπτώσεις, μια εξ αυτών είναι και αυτή του check-inσε μια αεροπορική πτήση. Η διαδικασία που μόλις περιγράψαμε και γνωρίζουμε όλοι μας, είναι αυτή της αυθεντικοποίησης. Η υπάλληλος της αεροπορικής εταιρείας ταυτοποίησε την Έλλη μέσα από τα στοιχεία της καθώς η διαδικασία της αυθεντικοποίησης ολοκληρώθηκε. Βάσει των στοιχείων, η υπάλληλος της αεροπορικής εταιρείας μπορεί είτε να επιτρέψει ή να απαγορεύσει στην Έλλη να προχωρήσει στο check-intης πτήσης.



Εικόνα2.1

Με βάσει το παράδειγμα του αεροδρομίου, η αυθεντικοποίηση δείχνει να είναι μια απλή διαδικασία.Απλά διαπιστώνουμε πως κάποιος ή κάτι είναι αυτό που ισχυρίζεται πως είναι, με την προϋπόθεση πως το άτομο ή το αντικείμενο έχει τα κατάλληλα διαπιστευτήρια. Πρακτικά αυτή είναι η βασική ιδέα της αυθεντικοποίησης.

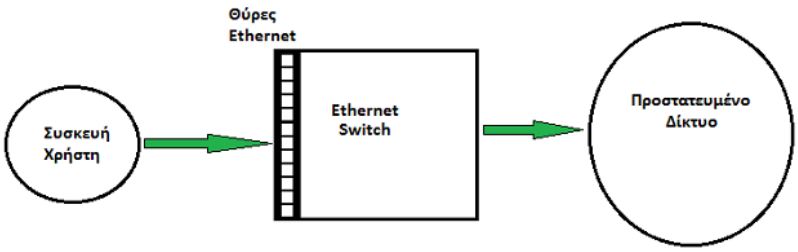
Ένα σύστημα αυθεντικοποίησης χρηστών σε ένα δίκτυο υπολογιστών μπορεί να είναι πιο περίπλοκο. Συσκευές (όπως Ethernetswitchesκαι κάρτες δικτύου) πρέπει να γνωρίζουν με ακρίβεια το τι να κάνουν, πράγμα το οποίο δεν αφήνει περιθώρια λάθους καθώς πρέπει όλες οι συσκευές να λειτουργούν με βάσει τις ανάγκες που καλύπτουν. Μη συμβατά πρωτόκολλα και ακόμα και μικρές απώλειες στην επικοινωνία με τις συσκευές συνήθως οδηγούν σε κακή λειτουργία του συστήματος, υποβαθμίζοντας έτσι την αξιοπιστία και αξία του. Οι άνθρωποι παρόλα αυτά, μπορούμε με βάσει λογικής να προσαρμοστούμε κατά τη διάρκεια επικοινωνίας. Για παράδειγμα, ας υποθέσουμε πως η Έλλη κάνει check-inσε μια πτήση εξωτερικού και ξέρει να μιλάει μόνο Αγγλικά ενώ η υπάλληλος της αεροπορικής εταιρείας μιλάει μόνο Ιταλικά. Η υπάλληλος μπορεί να ρωτήσει στα Ιταλικά την Έλλη να της δείξει το διαβατήριο της, η Έλλη με τη σειρά της να μην καταλάβει την υπάλληλο και αντί του διαβατηρίου της να της δείξει την αστυνομική της ταυτότητα. Η υπάλληλος δεν δέχεται την ταυτότητα αλλά παρά τις δυσκολίες στην επικοινωνία, η υπάλληλος με τη βοήθεια χειρονομιών και της γλώσσας του σώματος δείχνει στην Έλλη πως πρέπει να δει το διαβατήριο της. Μπορεί να είναι ασήμαντο αυτό σαν παράδειγμα αλλά η ουσία είναι πως ο άνθρωπος μπορεί να προσαρμοστεί εύκολα σε μια κατάσταση. Οι συσκευές μπορούν να προσαρμοστούν μέχρι ενός σημείου, απλά θα πρέπει να προγραμματιστούν από κάποιον και να τροποποιηθούν ούτως ώστε να προσαρμόζονται σε συγκεκριμένες καταστάσεις.

Τα πρότυπα και οι προδιαγραφές οι οποίες σχηματίζουν ένα πλήρες 802.1Xport-basedσύστημα αυθεντικοποίησης ορίζονται από διαφορετικούς οργανισμούς: το InstituteofElectricalandElectronicEngineers (IEEE)και το InternetEngineeringTaskForce (IETF). Το IEEEπρότυπο το οποίο εφαρμόζεται στην port-basedαυθεντικοποίησηείναι το 802.1X, που απευθύνεται στο EAPOL (ExtensibleAuthenticationProtocoloverLAN), και ο IETFπαρέχει RFCsγια EAP, EAP-Methods, καιRADIUS. Όλα αυτά τα πρότυπα και προδιαγραφές είναι απαραίτητα. Έτσι, κανένα πρότυπο από μόνο του μπορεί να προσδιορίσει όλα τα συστατικά που

χρειάζονται για να υλοποιήσουν ένα πλήρες σύστημα port-basedαυθεντικοποίησης. Αυτό μας οδηγεί σε μια πολυπλοκότητα η οποία ορισμένες φορές μας οδηγεί σε προβλήματα διαλειτουργικότητας.

Στην πραγματικότητα, τα πρότυπα που αποτελούν ένα port-based σύστημα αυθεντικοποίησης είναι αυτά που κάνουν την κατανόηση του 802.1Xκαι των σχετικών προδιαγραφών σχετικά δύσκολη. Τα πρότυπα και οι προδιαγραφές επίσης αλλάζουν ορισμένες φορές, οπότε πρέπει να είμαστε ιδιαίτερα προσεκτικοί για να έχουμε εξασφαλίσει πως αυτό που υλοποιούμε είναι αντιστρόφως συμβατό με εκδόσεις που έχουμε επιλέξει για μέρη του συστήματος.

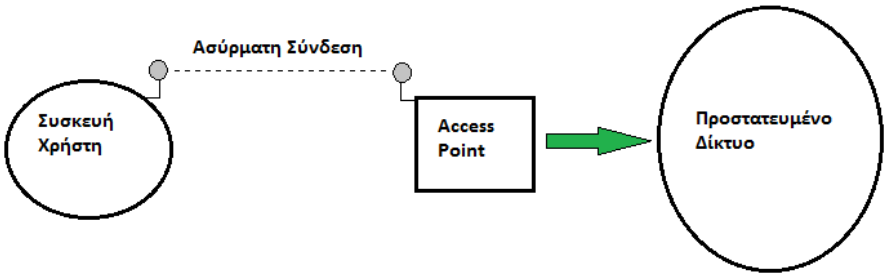
Άλλος ένας όρος που θα πρέπει να κατανοηθεί στην σφαίρα της port-basedαυθεντικοποίησης είναι η λέξη "port" (θύρα/πόρτα), σε ένα δίκτυο υπολογιστών είναι μια σύνδεση στο επίπεδο συνδέσμου μεταφοράς (Layer 2 DataLinkconnection) του μοντέλου OSI. Για τα ενσύρματα δίκτυα, η λέξη "port" (πόρτα) στην port-basedαυθεντικοποίηση απευθύνεται σε μία θύρα ενός Ethernetswitch όπως φαίνεται και παρακάτω (Εικόνα 2.2). Το καλώδιο Ethernetπαρέχει τη σύνδεση ανάμεσα σε συσκευή και δίκτυο και απευθύνεται στο φυσικό επίπεδο (Layer 1 PhysicalLayer). Με την port-basedαυθεντικοποίηση προσπαθούμε να πιστοποιήσουμε την ταυτότητα των συσκευών που συνδέονται στην θύρα Ethernetμέσω καλωδίου, και η αυθεντικοποίηση πραγματοποιείται στοεπίπεδο συνδέσμου μεταφοράς (DataLinkLayer 2).



Εικόνα2.2

Οι πόρτες "ports" διακρίνονται και στα ασύρματα δίκτυα (wirelessLANs). Βέβαια στον ασύρματο κόσμο, η πόρτα συσχετίζεται με κάποιο accesspoint (σημείο πρόσβασης). Όμοια με την ενσύρματη σύνδεση, μια ασύρματη συσκευή χρήστη π.χ. ένα laptopμε Wi-Fiπρόσβαση,

ακολουθεί μια διαδικασία σύνδεσης με ένα accesspoint. Όλα τα accesspointsσε ένα ασύρματο τοπικό δίκτυο εκπέμπουν περιοδικά ένα 802.11 beaconframe προς τις συσκευές το οποίο παρέχει πληροφορίες σχετικά με το δίκτυο. Όταν μία συσκευή χρήστη με δυνατότητα 802.11 ασύρματης πρόσβασης ξεκινά να λειτουργεί, σαρώνει όλα τα κανάλια και εντοπίζει τα accesspointsπου βρίσκονται στην ακτίνα της συσκευής. Στη συνέχεια ο χρήστης προσπαθεί να συνδεθεί με το accesspointπου έχει το δυνατότερο σήμα. Η διαδικασία σύνδεσης περιλαμβάνει μια σειρά από μεταδόσεις 802.11 πλαισίων "frames" ανάμεσα σε συσκευή χρήστη και accesspoint, κάτι το οποίο φαίνεται και στην παρακάτω εικόνα (Εικόνα 2.3). Μια επιτυχής σύνδεση με το accesspoint, επιτρέπει στον ασύρματο χρήστη με βάσει τη MACaddress, να επικοινωνήσει μέσω του accesspointμε άλλες συσκευές στο δίκτυο.Όπως και με την Ethernetενσύρματη σύνδεση, έτσι και στην ασύρματη παρέχεται μια σύνδεση δια της οποίας μια συσκευή μπορεί να αυθεντικοποιηθεί προτού αποκτήσει πρόσβαση στο δίκτυο.



Εικόνα2.1

Να σημειωθεί επίσηςότι η αυθεντικοποίηση (Authentication) είναι κάτι διαφορετικό από την εξουσιοδότηση (Authorization). Συχνά όμως αντιμετωπίζονται από κοινού. Χρησιμοποιώντας το προηγούμενο παράδειγμα, όταν η Έλλη έδωσε στην υπάλληλο της αεροπορικής εταιρείας τα στοιχεία της κατά τη διάρκεια του check-in της πτήσης της, έγινε η αυθεντικοποίηση και αμέσως μετά της δόθηκε η εξουσιοδότηση για να συνεχίσει στο επόμενο βήμα. Η εξουσιοδότηση (Authorization)είναι μια διαδικασία εκχώρησης δικαιωμάτων σε έναν άνθρωπο ή μια συσκευή βάσει του αποτελέσματος της αυθεντικοποίησης. Ας υποθέσουμε ότι ο Γιάννης από το τμήμα της οικονομικής διαχείρισης προσπαθεί να συνδεθεί σε ένα δίκτυο και καλείται να εισάγει το όνομα χρήστη και τον κωδικό του. Αφού εισάγει τα στοιχεία του, το σύστημα επιβεβαιώνει ότι

το όνομα χρήστη και ο κωδικός του Γιάννη ταιριάζουν με εκείνα που υπάρχουν στη βάση δεδομένων. Μέχρι στιγμής βρισκόμαστε στο κομμάτι της αυθεντικοποίησης. Με βάσει το όνομα χρήστη του Γιάννη, το σύστημα δίνει πρόσβαση στον Γιάννη μόνο στις υπηρεσίες των serverπου αφορούν το τμήμα της οικονομικής διαχείρισης και όχι στις υπηρεσίες και εφαρμογές του τμήματος ανθρωπίνου δυναμικού της εταιρείας. Το βήμα αυτό της αποδοχής του Γιάννη μέσα στο δίκτυο αφορά το κομμάτι της εξουσιοδότησης. Το κομμάτι της εξουσιοδότησης (Authorization) σε ένα δίκτυο είναι σίγουρα σημαντικό αλλά προς το παρόν θα πρέπει να εστιάσουμε περισσότερο σε εκείνο της αυθεντικοποίησης.

2.2 Πλεονεκτήματα Αυθεντικοποίησης

Η port-basedαυθεντικοποίησηκρατά μακριά τους μη εξουσιοδοτημένους χρήστες και συσκευές χρηστών από προστατευόμενους πόρους ενός δικτύου όπως είναι οι servers, εταιρικές εφαρμογές και βάσεις δεδομένων. Χωρίς την αυθεντικοποίηση ένας χάκερ θα μπορούσε να αποκτήσει πολύ εύκολα πρόσβαση στο δίκτυο μιας εταιρείας με το να συνδέσει ένα λάπτοπ σε μια θύρα Ethernetεντός του χώρου ή να συνδεθεί ασύρματα μέσω κάποιου accesspointτης εταιρείας. Εάν επιτραπεί σε κάποιο χάκερ η πρόσβαση στο δίκτυο, θα προσπαθήσει με κάθε τρόπο να εκμεταλλευτεί κενά ασφαλείας έχοντας ένα εύρος από εργαλεία και μεθόδους για να λάβει στην κατοχή του υλικό της εταιρείας.

Με την υλοποίηση ενόςport-based συστήματοςελέγχου ταυτότητας πρόσβασης κάνουμε ένα σημαντικό βήμα στο να ασφαλίσουμε ένα ενσύρματο ή ασύρματο δίκτυο. Βέβαια αυτό δεν είναι η τέλεια λύση στο πρόβλημα της ασφάλειας σε ένα δίκτυο. Επιπροσθέτως θα πρέπει να επιστρατευθούν και άλλες μέθοδοι σε συνδυασμό όπως η κρυπτογράφηση των πακέτων πληροφορίας, η ανίχνευση εισβολής, η αποφυγή επιθέσεων άρνησης εξυπηρέτησης,και ο έλεγχος πρόσβασης στους χώρους του κτιρίου ούτως ώστε να καλυφθούν όλες οι πιθανές ευπάθειες ασφαλείας.

Επιπλέον, με το να μένουν τα μη εξουσιοδοτημένα άτομα εκτός δικτύου, ένα port-basedσύστημα αυθεντικοποίησης μπορεί υποστηρίξει επίσης και τις παρακάτω δυνατότητες:

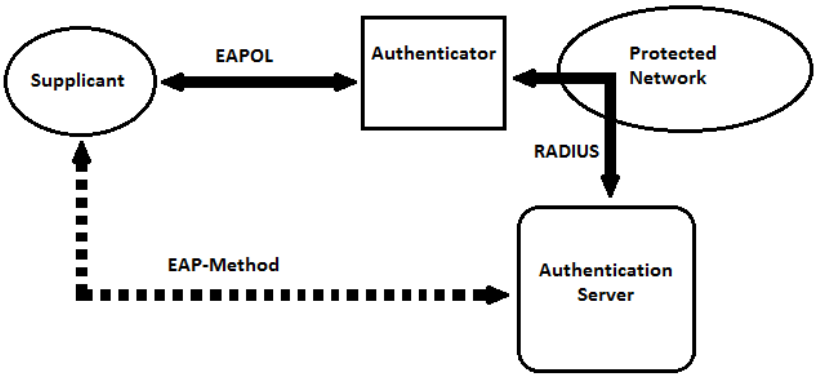
- **Πληροφορίες τοποθεσίας χρήστη:** Μια εφαρμογή μπορεί εύκολα να εντοπίσει την τοποθεσία χρηστών, π.χ. με βάσει το switchή το accesspointαπό το οποίο η εκάστοτε συσκευή αυθεντικοποιήθηκε. Για παράδειγμα ένα νοσοκομείο μπορεί να

χρησιμοποιήσει τέτοιου είδους πληροφορία για να εντοπίσει την τοποθεσία των ιατρών και νοσηλευτών μέσα από ασύρματες συσκευές.

- **Μηχανισμοί χρέωσης:** Η port-basedαυθεντικοποίηση σε συνδυασμό με μηχανισμούς χρέωσης, επιτρέπει στους διαχειριστές και παρόχους πρόσβασης στο δίκτυο να υλοποιούν συστήματα στα οποία οι χρήστες θα πρέπει να πληρώσουν κάποιο αντίτιμο έτσι ώστε να αποκτήσουν πρόσβαση στο δίκτυο. Για παράδειγμα σε μία καφετέρια, υλοποιείται ένα σύστημα πρόσβασης στο ίντερνετ με μορφή ticketing όπου ο κάθε χρήστης θα πρέπει να παραγγείλει κάτι έτσι ώστε μαζί με την απόδειξη να λάβει και ένα όνομα χρήστη με κωδικό. Τα στοιχεία αυτά του δίνουν πρόσβαση στο τοπικό δίκτυο της καφετέριας για ένα ορισμένο χρονικό διάστημα της τάξεως των 2 ωρών. Μετά τις 2 αυτές ώρες, το όνομα χρήστη και ο κωδικός παύουν να είναι ενεργά.
- **Προσωποποιημένη πρόσβαση στο δίκτυο:** Με βάσει τα στοιχεία που δόθηκαν κατά την αυθεντικοποίηση, το σύστημα μπορεί να εξουσιοδοτήσει πρόσβαση στον χρήστη σε συγκεκριμένες εφαρμογές.

2.3 Βασικά στοιχεία ενός port-basedσυστήματος αυθεντικοποίησης

Μέχρι στιγμής έχουμε προσεγγίσει την port-based αυθεντκοποίηση από μια γενική σκοπιά, σε αυτό το σημείο πρόκειται να εμβαθύνουμε σε πιο συγκεκριμένες έννοιες και πρωτόκολλα τα οποία συμβαδίζουν μαζί με τα πρότυπα και προδιαγραφές του 802.1X. Όπως φαίνεται και παρακάτω (Εικόνα 2.4), τα βασικά στοιχεία σε ένα port-based σύστημα αυθεντικοποίησης περιλαμβάνουν τους χρήστες που απαιτούν πρόσβαση στο δίκτυο (supplicants), τον μηχανισμό αυθεντικοποίησης (authenticator), καθώς και τον server αυθεντικοποίησης (authenticationserver).



Εικόνα2.3

Χρήστηςπου απαιτεί πρόσβαση στο δίκτυο (Supplicant)

Μία συσκευή χρήστη που απαιτεί πρόσβαση στο δίκτυο(supplicant) προτού του επιτραπεί η πρόσβαση στο δίκτυο, πρέπει αρχικά να αυθεντικοποιηθεί. Ας υποθέσουμε ότι ο supplicantείναι ένας άγνωστος χρήστης και η ταυτότητα του είναι υπό αμφισβήτηση μέχρι να δώσουν τα σωστά στοιχεία στον serverαυθεντικοποίησης.

Για να θεωρηθεί ένας supplicant έγκυρος χρησιμοποιώντας για παράδειγμα ένα laptop ή ένα IPτηλέφωνο, θα πρέπει να χρησιμοποιεί το 802.1Xκαι κάποιαμέθοδο EAP-Method. Για παράδειγμα το λειτουργικό των Windows υποστηρίζει το 802.1X μαζί με μια ποικιλία από EAP-Methods, όπως για παράδειγμα το EAP-TLS.O supplicantεπικοινωνεί με τον serverαυθεντικοποίησης χρησιμοποιώντας το EAPπρωτόκολλο για τη μεταφορά και κάποια EAP-Methodη οποία παρέχει τον μηχανισμό αυθεντικοποίησης. Όπως θα δούμε και παρακάτω, η πραγματική επικοινωνία μεταξύ supplicantκαι μηχανισμού αυθεντικοποίησης επιτυγχάνεται μέσω του EAPOL πρωτοκόλλου το οποίο ορίζεται από το 802.1X. Το EAPOL μεταφέρει και ενθυλακώνει τα πλαίσια EAP καιEAP-Method ως πληροφορία.

Μηχανισμός αυθεντικοποίησης (Authenticator)

Ένας μηχανισμός αυθεντικοποίησης είναι μια δικτυακή συσκευή επιπέδου 2 (Layer 2), όπως ένα Ethernetswitchή ένα accesspointασύρματουLAN. Σε ένα εταιρικό δίκτυο, όλες οι θύρες των

switchπρέπει να εφαρμόζουν το 802.1X ούτως ώστε να υποστηρίζεται η 802.1X port-basedαυθεντικοποίηση σε όλο το εύρος της εταιρείας. Ο μηχανισμός αυθεντικοποίησης (Authenticator)λειτουργεί ως πύλη ασφαλείας ανάμεσα στον χρήστη ο οποίος απαιτεί πρόσβαση στο δίκτυο (supplicant)και το προστατευμένο δίκτυο. Η θύρα (port)παραμένει κλειστή μέχρι το σύστημα αυθεντικοποίησης να ταυτοποιήσει τα στοιχεία του χρήστη που απαιτεί πρόσβαση στο δίκτυο (supplicant) και θεωρείότι ο supplicantέχει το δικαίωμα να αποκτήσει πρόσβαση στο δίκτυο. Μόλις το σύστημα πιστοποιήσει την ταυτότητα του χρήστη, ο μηχανισμός αυθεντικοποίησης θα ανοίξει μια θύρα (port) για να έχει πρόσβαση στο προστατευμένο δίκτυο ο χρήστης.

Επιπλέον, ο μηχανισμός αυθεντικοποίησης είναι ένας μεταφραστής μεταξύ του χρήστη που απαιτεί πρόσβαση στο δίκτυο (supplicant)και του serverαυθεντικοποίησης. Κατά την επικοινωνία ανάμεσα σε supplicant και serverαυθεντικοποίησης, όλη η ροή επικοινωνίας περνά από τον μηχανισμό αυθεντικοποίησης. Για παράδειγμα, ο supplicant θα στείλει τα στοιχεία του στον serverαυθεντικοποίησης με το να ενθυλακώνει τα στοιχεία του (με βάσει την μέθοδο EAP-Methodπου έχει επιλεχθεί) σε ένα πλαίσιο EAP, το οποίο ενθυλακώνεται με τη σειρά του σε ένα EAPOLπλαίσιο. Το EAPOLπλαίσιο αποστέλλεται στον μηχανισμό αυθεντικοποίησης, όπου εκεί αφαιρεί την EAP-Methodπληροφορία από το EAPOLπλαίσιο. Ο μηχανισμός αυθεντικοποίησης στέλνει την EAP-Methodπληροφορία ενθυλακωμένη σε ένα RADIUSπλαίσιο απευθείας στον serverαυθεντικοποίησης. Έτσι η επικοινωνία ανάμεσα σε supplicantκαι serverαυθεντικοποίησης είναι βασισμένη σε μια κοινή γλώσσα.

ServerΑυθεντικοποίησης (AuthenticationServer)

Όπως αναφέραμε και παραπάνω, ο μηχανισμός αυθεντικοποίησης (authenticator) και ο χρήστης που απαιτεί πρόσβαση στο δίκτυο (supplicant)έχουν μια επικοινωνία σχετικά με την αυθεντικοποίηση.Ο serverαυθεντικοποίησης για παράδειγμα, κάποια στιγμή θα ζητήσει τα στοιχεία του χρήστη που απαιτεί πρόσβαση στο δίκτυο (supplicant). Ο supplicantθα δώσει τότε τα στοιχεία του στον serverαυθεντικοποίησης. Τα πρότυπα και οι προδιαγραφές της port-basedαυθεντικοποίησης δεν καθιστούν υποχρεωτική την ύπαρξη κάποιου συγκεκριμένου τύπου serverαυθεντικοποίησης, αλλά σχεδόν όλες οι υλοποιήσεις στηρίζονται πάνω στο RADIUS. Αυτό έχει ως αποτέλεσμα το RADIUSνα είναι το defacto πρότυπο που αναγνωρίζεται από τη βιομηχανία δικτύων.

Σε ένα εταιρικό σύστημα, ο serverαυθεντκοποίησης είναι πιθανότατα μια ξεχωριστή συνιστώσα που είναι ενσωματωμένη στο δίκτυο. Πιθανότατα θα υπάρχουν αρκετοί serverαυθεντικοποίησης με στόχο την καλύτερη απόδοση και μεγαλύτερη διαθεσιμότητα. Ο κάθε μηχανισμός αυθεντικοποίησης δείχνει προς έναν βασικό serverαυθεντικοποίησης, με πιθανότατα και άλλουςserversοι οποίοι να κατατάσσονται ως δευτερεύοντες serversοι οποίοι να καλούνται εάν ο βασικός serverαυθεντικοποίησης δεν αποκρίνεται.

Σε ορισμένες περιπτώσεις, ο serverαυθεντικοποίησης μπορεί να είναι ενσωματωμένος στους μηχανισμούς αυθεντικοποίησης. Αυτό το μοντέλο κατανεμημένου serverαυθεντικοποίησης ελαττώνει σημαντικά την κίνηση λόγω αυθεντικοποίησης μέσα στο δίκτυο, κάτι το οποίο είναι επιθυμητό στα ασύρματα δίκτυα όπου συχνά συναντάμε το φαινόμενο της περιαγωγής. Έτσι μπορούμε να έχουμε βελτιωμένη απόδοση για όλους τους χρήστες. Επιπροσθέτως, μικρά σε έκταση δίκτυα μπορεί να ωφεληθούν σε μεγάλο βαθμό με το να χρησιμοποιούν ένα switchή ένα accesspointτο οποίο παρέχει λειτουργίες serverαυθεντικοποίησης. Σε μικρά δίκτυα γίνεται εξοικονόμηση χρημάτων καθώς μειώνεται το κόστος σε υλικό (hardware).

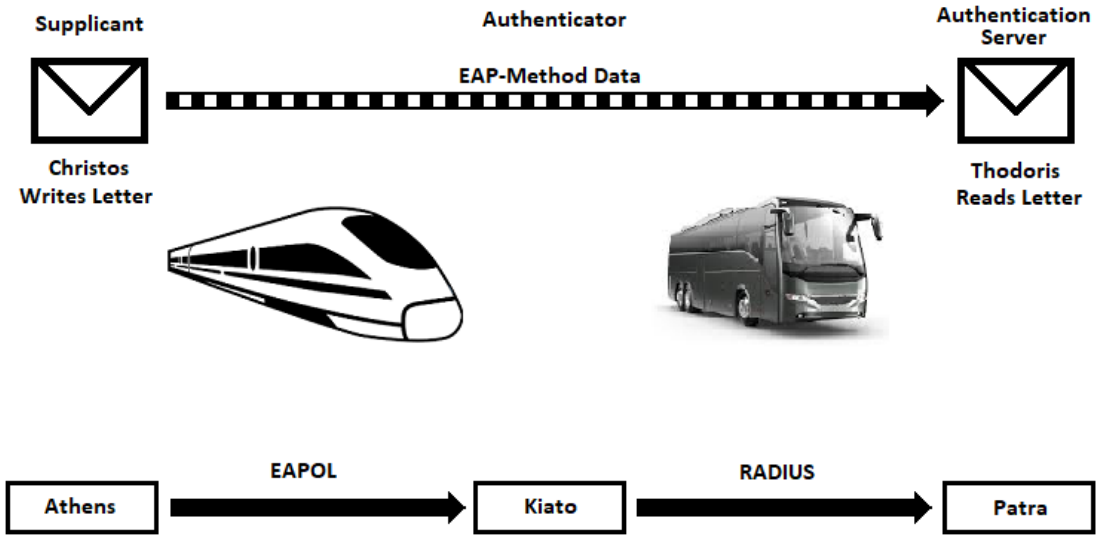
2.4 Εξερευνώντας τα πρωτόκολλα με μια απλή αναλογία

Όπως βλέπουμε, η 802.1X port-basedαυθεντικοποίηση περιλαμβάνει αρκετά διαφορετικά πρωτόκολλα, και συγκεκριμένα τα: EAPOL, EAP, EAP-Methodsκαι RADIUS. Επιπλέον, πραγματοποιείται με αυτά και αρκετή διαστρωμάτωση (layering). Παρακάτω μπορούμε να δούμε ένα παράδειγμα με αναλογία η οποία θα φανεί χρήσιμη για να κατανοήσουμε το πώς η μεταφορά δεδομένων πραγματοποιείται αλλά και το που τα πρωτόκολλα εφαρμόζονται.

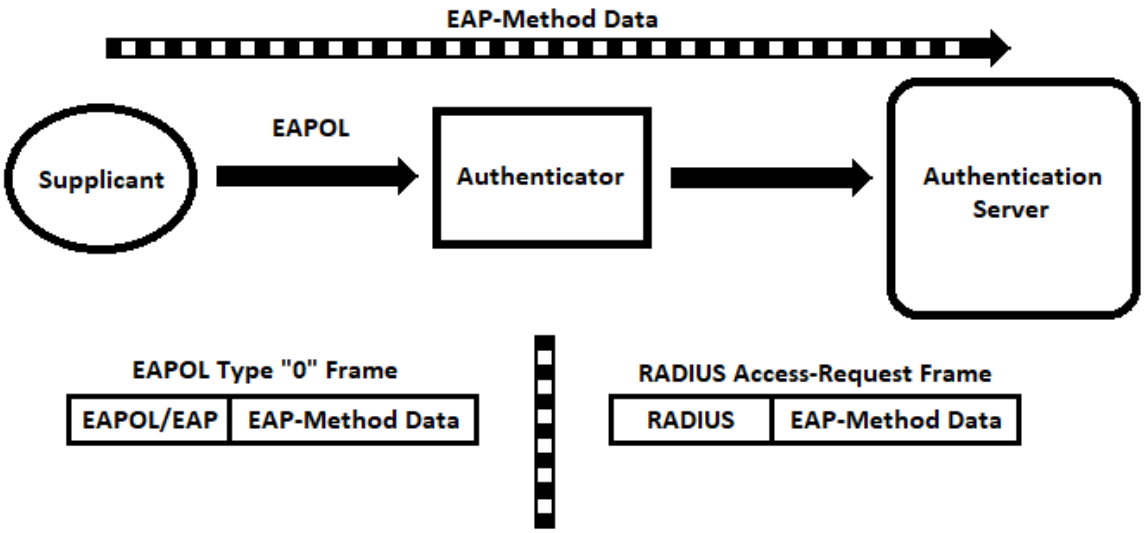
Ας υποθέσουμε ότι ο Χρήστος (χρήστης που απαιτεί πρόσβαση στο δίκτυο) που βρίσκεται στην Αθήνα γράφει και στέλνει ένα γράμμα (EAP-Methoddata) στον φίλο του Θοδωρή (serverαυθεντικοποίησης), ο οποίος ζει στην Πάτρα. Ο Χρήστος στέλνει το γράμμα μέσω ειδικής courier αποστολής η οποία θα στείλει το γράμμα με τραίνο (EAPOL/EAP)στο Κιάτο (μηχανισμός αυθεντικοποίησης), όπου είναι σχεδόν στα μισά της διαδρομής μεταξύ Αθήνας και Πάτρας. Στο Κιάτο, ο couriersυνεχίζει την αποστολή μέσω λεωφορείου (RADIUS). Ο Θοδωρής λαμβάνει και διαβάζει επιτυχώς το γράμμα. Η Εικόνα 2.5 απεικονίζει τη διαδικασία.

Η διαδικασία αποστολής είναι παρόμοια με τη διαδικασία διαστρωμάτωσης που λαμβάνει χώρα σε ένα 802.1X σύστημα port-basedαυθεντικοποίησης. Ο γενικός σκοπός του συστήματος είναι

να επιτρέψει στον χρήστη που απαιτεί πρόσβαση στο δίκτυο (Χρήστος) να επικοινωνήσει με τον serverαυθεντκοποίησης (Θοδωρής) μέσω μιας συγκεκριμένης μεθόδου EAP-Method, η οποία περιλαμβάνει την αμφίδρομη αποστολή δεδομένων EAP-Methodμεταξύ τουχρήστη που απαιτεί πρόσβαση στο δίκτυο (Χρήστος) και του serverαυθεντικοποίησης (Θοδωρή). Για να διεισδύσουν τα EAP-Methodδεδομέναμέσα από το σύστημα, το EAPOL (τραίνο) μεταφέρει το γράμμα στον μηχανισμό αυθεντικοποίησης (Κιάτο), και το RADIUS(λεωφορείο) μεταφέρει τα EAP-Methodδεδομένα (γράμμα) στον serverαυθεντικοποίησης (Θοδωρής). Η Εικόνα 2.6 απεικονίζει τη διαδικασία διαστρωμάτωσης (layeringprocess) στο 802.1X. Επιπροσθέτως, ακόμη ένα επίπεδο το οποίο δεν απεικονίζεται στην εικόνα, θα περιλάμβανε και τα πρωτόκολλα LANανά περίπτωση, δηλαδή τα 802.3 ή 802.11.



Εικόνα2.4



Εικόνα2.4

Η διαστρωμάτωση (layering)πραγματοποιείται για να επιτρέψει διαφορετικά πρωτόκολλα ανάμεσα σε supplicant(χρήστη που απαιτεί πρόσβαση) και μηχανισμό αυθεντικοποίησης (EAPOL), και ανάμεσα σε μηχανισμό αυθεντικοποίησης και serverαυθεντικοποίησης (EAP-Method). Έτσι μπορούν τα πρωτόκολλα να αντιμετωπίσουν τις διάφορες ανάγκες της εκάστοτε σύνδεσης μέσα στο σύστημα και ταυτόχρονα να επιτρέπουν την ύπαρξη μιας συνομιλίας μεταξύ supplicantκαι serverαυθεντικοποίησης (EAP-Method).

2.5 Κατανοώντας το σύστημα συνολικά με μια απλή αναλογία

Στην αρχή του κεφαλαίου αυτού, με το παράδειγμα της Έλλης η οποία έκανε check-inγια μια πτήση της στο αεροδρόμιο ορίσαμε την αυθεντικοποίηση. Το συγκεκριμένο παράδειγμα ήταν πολύ απλό και δεν περιλάμβανε όλα τα επιμέρους στοιχεία ενός port-basedσυστήματος αυθεντικοποίησης. Καθώς θα προχωρήσουμε παρακάτω στο παράδειγμα μας, περισσότεροι όροι και φράσεις θα χαρτογραφήσουν μια αναλογία η οποία αντιστοιχεί σε ένα πραγματικό 802.1X σύστημα port-basedαυθεντικοποίησης.

Ας υποθέσουμε ότιο Δημήτρης (χρήστης που απαιτεί πρόσβαση στο δίκτυο) φτάνει στη Βουλή (προστατευμένο δίκτυο) ούτως ώστε να συναντηθεί με τον πρωθυπουργό (Εικόνα 2.7). Καθώς ο Δημήτρης μπαίνει στο πάρκινγκ (θύρα switch), ένας φύλακας εισόδου (μηχανισμός αυθεντικοποίησης) δίνει εντολή στον Δημήτρη να σταματήσει το αυτοκίνητο του. Ο φύλακας

ρωτάει τον Δημήτρη για ποιο λόγο βρίσκεται εκεί και ο Δημήτρης απαντάει λέγοντας του πως ήρθε για να συναντήσει τον πρωθυπουργό. Ο φύλακας τότε καλεί την Εύα (serverαυθεντικοποίησης) καθώς είναι το κεντρικό σημείο επικοινωνίας με το τμήμα ασφαλείας του πρωθυπουργού, και επιτρέπει στον Δημήτρη να μιλήσει απευθείας στην Εύα η οποία βρίσκεται εντός της Βουλής. Η Εύα μπορεί να δει τον Δημήτρη μέσα από κάμερα ασφαλείας και ζητά από εκείνον να βγάλει την ταυτότητα του και να τη δείξει μπροστά από την κάμερα έτσι ώστε να μπορεί ξεκάθαρα να δει το όνομα,τη φωτογραφία και τον αριθμό ταυτότητας του (EAP-Methoddata). Αφού επιβεβαιωθεί ότι ο Δημήτρης είναι το πρόσωπο που ισχυρίζεται (διαδικασία αυθεντικοποίησης), η Εύα βρίσκει το όνομα του Δημήτρη και τα στοιχεία του στη λίστα με τα πρόσωπα που πρόκειται να συναντηθούν με τον πρωθυπουργό και στη συνέχεια η Εύα λέει στον φύλακα της εισόδου να εκδώσει στον Δημήτρη ένα πάσο για την αίθουσα συναντήσεων (επιτρεπόμενες λειτουργίες). Ο φύλακας τότε αφήνει τον Δημήτρη να προχωρήσει και να φτάσει μέχρι την αίθουσα συναντήσεων.

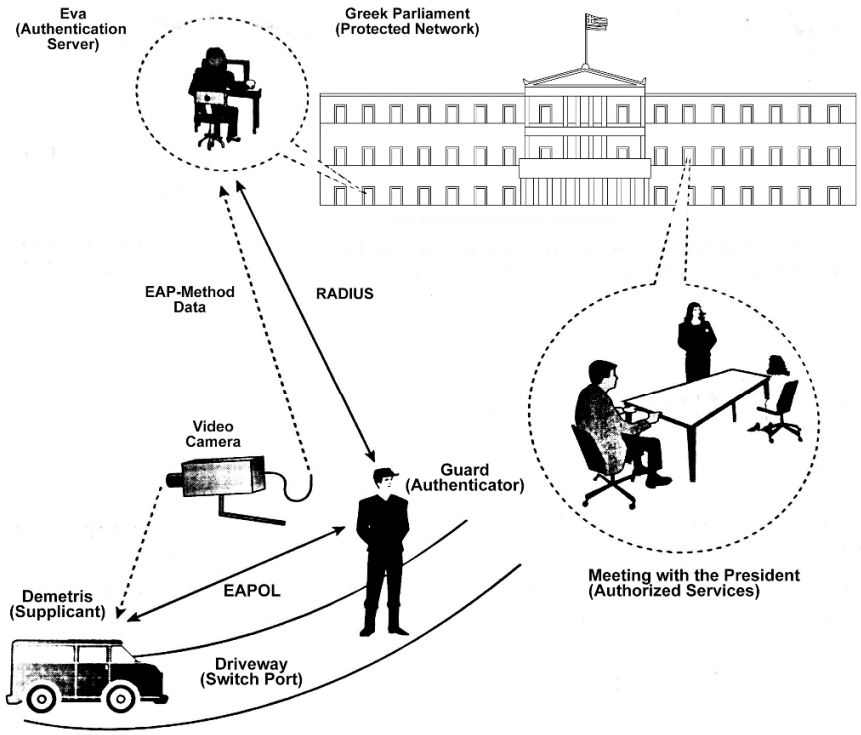
Πολλές "παραλλαγές" αυτού του παραδείγματος συχνά προκύπτουν σε πραγματικά συστήματα port-basedαυθεντικοποίησης. Εάν για παράδειγμα η Εύα δεν έβρισκε τα στοιχεία του Δημήτρη στη σχετική λίστα με τις συναντήσεις, τότε θα έλεγε στον φύλακα να μην αφήσει τον Δημήτρη να προχωρήσει (μη επιτρεπτή πρόσβαση). Ο φύλακας της εισόδου θα έπρεπε αν χρειαζόταν να χρησιμοποιήσει κάθε μέσο έτσι ώστε να μην αποκτήσει πρόσβαση ο Δημήτρης στον χώρο της Βουλής. Αν ο Δημήτρης ήταν τουρίστας (επισκέπτης), ο φύλακας θα έλεγε στον Δημήτρη να αφήσει το όχημα του λίγο πιο έξω από τον χώρο και να προγραμματίσει κάποια ξενάγηση στον χώρο (πρόσβαση επισκέπτη "guest").

Καθώς η Εύα ζητάει από τον Δημήτρη να της δείξει την ταυτότητα του, εκείνος μπορεί να μην την έχει πάνω του. Ο Δημήτρης θα μπορούσε να διαπραγματευτεί με την Εύα την πιθανότητα να χρησιμοποιήσει το δίπλωμα οδήγησης του αντί της ταυτότητας. Κάτι ανάλογο συμβαίνει και με τις μεθόδους port-basedαυθεντικοποίησης όταν ο χρήστης που απαιτεί πρόσβαση στο δίκτυο δεν υποστηρίζει την βασική μέθοδο EAP-Method. Όταν συμβαίνει κάτι τέτοιο, ο χρήστης και ο serverαυθεντικοποίησης μπορούν να διαπραγματευτούν τη χρήση μιας διαφορετικής μεθόδου EAP-Method. Υπάρχει και μια πιθανότητα παρόλα αυτά όπου η Εύα να μην δεχτεί το δίπλωμα οδήγησης ως έγκυρη μέθοδο ταυτοποίησης. Σε αυτή την περίπτωση, θα ενημερώσει τον φύλακα της πύλης να μην αφήσει τον Δημήτρη να περάσει και ο φύλακας πιθανότατα να του προτείνει

να εισέλθει στον χώρο της Βουλής ως επισκέπτης (πρόσβαση επισκέπτη “guest”) μέσω κάποιας προγραμματισμένης ξενάγησης.

Εάν η Εύα δεν απαντήσει στο τηλεφώνημα του φύλακα, τότε ο φύλακας θα μπορούσε να καλέσει κάποιο άλλο άτομο από το τμήμα ασφαλείας. Εν τέλει, ο φύλακας μπορεί να επικοινωνήσει με κάποιο άλλο άτομο από το τμήμα ασφαλείας και το άτομο με τη σειρά του να επικοινωνήσει απευθείας με τον Δημήτρη και να αναλάβει τη διαδικασία ταυτοποίησης (αυθεντικοποίησης). Ο φύλακας μπορεί παρόλα αυτά επίσης να μη καταφέρει να έρθει σε επαφή με κάποιο άτομο του τμήματος ασφαλείας καθώς μπορεί οι γραμμές να μη λειτουργούν είτε το τμήμα ασφαλείας να είναι πολύ απασχολημένο και να μην μπορεί να εξυπηρετήσει άλλα νέα αιτήματα. Σε αυτή την περίπτωση ο Δημήτρης θα πρέπει να περιμένει μέχρι να μπορέσει ο φύλακας να τον φέρει σε επικοινωνία με κάποιον υπάλληλο από το τμήμα ασφαλείας.

Μια ακόμα περίπτωση είναι και εκείνη στην οποία ο Δημήτρης μπορεί να φτάσει στον χώρο της εισόδου και ο φύλακας να μην παρατηρήσει την παρουσία του. Τότε ο Δημήτρης θα προσπαθήσει με κάποιο τρόπο να αποκτήσει την προσοχή του φύλακα της εισόδου λέγοντας του για παράδειγμα: “Με συγχωρείτε!”. Κατά πάσα πιθανότητα ο φύλακας θα εστιάσει την προσοχή του στον Δημήτρη και με τη σειρά του εκείνος θα τον ρωτήσει για ποιο λόγο βρίσκεται στον χώρο. Η συνέχεια έπειτα της συνομιλίας συνεχίζεται όπως την περιγράψαμε παραπάνω.



Εικόνα2.5

2.6 Από τον χρήστη που απαιτεί πρόσβαση στο δίκτυο έως τον Serverαυθεντικοποίησης: Μέθοδοι EAP-Methods

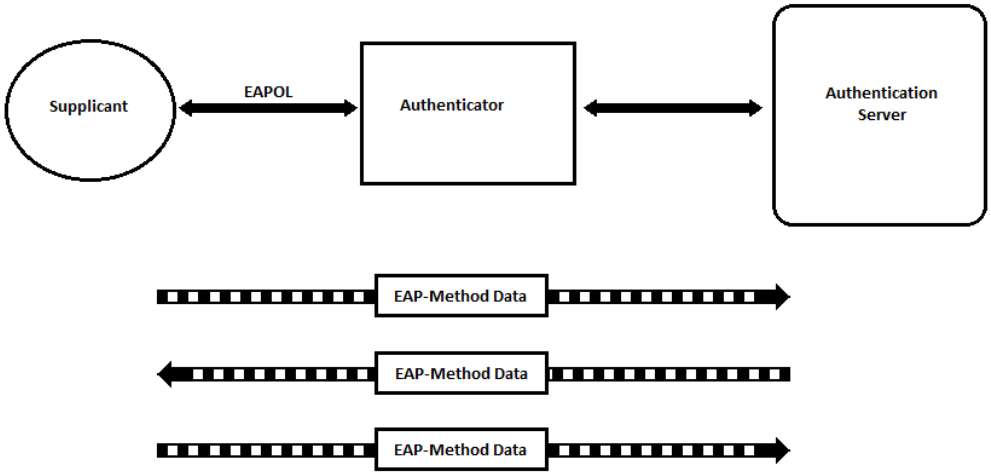
Η πραγματική επικοινωνία σχετικά με την αυθεντικοποίηση γίνεται μεταξύ του χρήστη που απαιτεί πρόσβαση στο δίκτυο (supplicant)και του serverαυθεντικοποίησης.Ομοίως και στο παραπάνω παράδειγμα της συνομιλίας του Δημήτρη και της Εύας, όπου ο Δημήτρης έχει τον ρόλο του supplicantκαι η Εύα τον ρόλο του server αυθεντικοποίησης. Σε ένα σύστημα port-based αυθεντικοποίησης, μια ειδική μέθοδος EAP-Method ορίζει το πως θα πραγματοποιηθεί η αυθεντκοποίηση μεταξύ του supplicantκαι του serverαυθεντικοποίησης. Η συνομιλία ανάμεσα σε supplicantκαι serverαυθεντικοποίησης περιλαμβάνει EAP-Methodδεδομένα, τα οποία αντικατοπτρίζουν διάφορες πληροφορίες όπως είναι για παράδειγμα τα στοιχεία πρόσβασης του supplicant. Η Εικόνα 2.8 απεικονίζει την επικοινωνία μεταξύ του supplicantκαι του serverαυθεντικοποίησης. Η επικοινωνία αυτή ανάμεσα σε supplicantκαι serverαυθεντικοποίησης περιλαμβάνει την ανταλλαγή EAPδεδομένων με βάσει τον τύπο της μεθόδου EAP-Method.

Η υλοποίηση και το αποτέλεσμα μιας μεθόδου EAP-Method είναι ο στόχος ενός συστήματος port-basedαυθεντικοποίησης. Η διαδικασία την οποία ο Δημήτρης και η Εύα ολοκλήρωσαν κατά την ταυτοποίηση των στοιχείων του Δημήτρη με βάσει τις πληροφορίες που υπήρχαν στην αστυνομική ταυτότητα του είναι κάτι το οποίο μία μέθοδος EAP-Methodπαρέχει. Στην πράξη, σε 802.1X συστήματα port-basedαυθεντικοποίησης, οι μέθοδοι EAP-Methodχρησιμοποιούν διαφόρων ειδών στοιχεία, όπως είναι το όνομα χρήστη / κωδικοί, κλειδιά κρυπτογράφησης και ψηφιακά πιστοποιητικά.

Τα πρότυπα χρειάζεται να υλοποιήσουν τις παρακάτω μεθόδους EAP-Methods:

- MD5 challenge
- One-Time Passwords (OTP)
- Generic token card

Επιπροσθέτως, υπάρχουν και άλλες μέθοδοι EAP-Methodsόπως για παράδειγμα οι παρακάτω: EAP-TLS, EAP-TTLS, EAP-FASTκαι EAP-LEAP. Σε επόμενο κεφάλαιο θα σταθούμε σε μεγαλύτερη λεπτομέρεια στις μεθόδους EAP-Methods αναλύοντας περισσότερο τα στοιχεία τους.



Εικόνα2.6

2.7 Από τον χρήστη που απαιτεί πρόσβαση έως τον μηχανισμό αυθεντικοποίησης: 802.1X / EAPOL

Το 802.1X εφαρμόζεται μόνο ανάμεσα στον χρήστη που απαιτεί πρόσβαση στο δίκτυο (supplicant) και τον μηχανισμό αυθεντικοποίησης. Αυτό αντιστοιχίζεται στο προηγούμενο παράδειγμα μας στην επικοινωνία που είχε ο Δημήτρης με τον φύλακα της εισόδου στη Βουλή. Ένα πλήρες 802.1X σύστημα port-basedαυθεντικοποίησης χρησιμοποιεί και άλλα πρωτόκολλα, όπως για παράδειγμα το RADIUS. Το 802.1X αποτελεί ένα μέρος του συνολικού συστήματος.

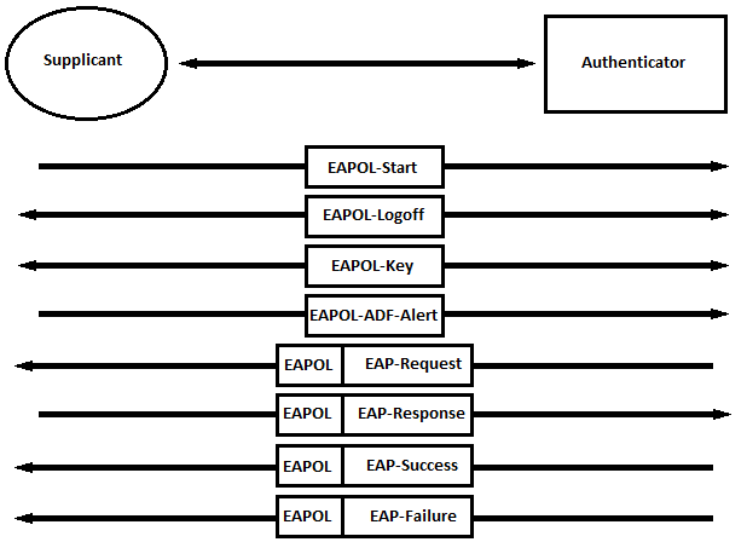
Η Εικόνα 2.9 απεικονίζει την επικοινωνία ανάμεσα σε ένα χρήστη που απαιτεί πρόσβαση στο δίκτυο (supplicant)και έναν μηχανισμό αυθεντικοποίησης.

Το EAPσχεδιάστηκε ως ένα point-to-point (από άκρη σε άκρη) πρωτόκολλο (PPP)για επικοινωνίες πάνω σε σειριακή σύνδεση. Το EAPOLορίζεται στο 802.1X πρότυπο έτσι ώστε να προσαρμοστεί το EAPγια χρήση σε LANs (τοπικά δίκτυα περιοχής).

Για να γίνει κάτι τέτοιο, το EAPOLπροσθέτει τρία επιπλέον πεδία στο EAP:

- Version (Έκδοση)
- Type (Τύπος)
- Length (Μήκος)

Ως αποτέλεσμα, το EAPOLενθυλακώνει EAPπλαίσια ως δεδομένα. Στο επόμενο κεφάλαιο θα αναλύσουμε περαιτέρω τα πεδία αυτά. Προς το παρόν σε αυτό το κεφάλαιο είναι σημαντικό να δούμε τους διάφορους τύπους EAPOLπλαισίων έτσι ώστε να κατανοήσουμε τη βάση στη λειτουργία του 802.1X.



Εικόνα2.7

Ένα Τύπου "0"EAPOLπλαίσιο δείχνει πως το πλαίσιο μεταφέρει ένα EAPπλαίσιο.Παρόλα αυτά είτε μιλάμε για τον supplicantείτε για τον μηχανισμό αυθεντικοποίησης, θα πρέπει να γνωρίζουμε ποιος είναι ο προορισμός έτσι ώστε να βγει η EAPOLκεφαλίδα και να φτάσουμε στο EAPπλαίσιο. Έτσι, τα τύπου "0" EAPOLπλαίσια απλά περνούν EAPπλαίσια τα οποία συνήθως μεταφέρουν δεδομένα EAP-Methodμεθόδων.

Εκτός από τη μεταφορά EAP-Methodδεδομένων, άλλα EAPπλαίσια διαχειρίζονται την πληροφορία αυθεντικοποίησης. Για παράδειγμα, το πρωτόκολλο EAPπαρέχει ένα μηχανισμό για τον supplicantκαι τον serverαυθεντικοποίησης ώστε να διαπραγματευτούν το ποια μέθοδο EAP-Methodθα χρησιμοποιήσουν. Όπως και στο προηγούμενο παράδειγμα μας αντίστοιχα η λογική είναι ίδια ως προς το εάν ο Δημήτρης θα μπορούσε να χρησιμοποιήσει στη συνομιλία του με την Εύα το δίπλωμα οδήγησης του ως στοιχείο ταυτοποίησης αντί να χρησιμοποιηθεί η αστυνομική του ταυτότητα. Επιπροσθέτως, άλλα EAPπλαίσια παρέχουν τα μέσα για την ανταλλαγή στοιχείων ταυτοποίησης και τον καθορισμό μιας επιτυχημένης και μιας αποτυχημένης αυθεντικοποίησης. Η ανταλλαγή τέτοιων στοιχείων μπορεί να φανεί στο παράδειγμα μας στο σημείο το οποίο ο φύλακας της εισόδου λέει στον Δημήτρη το εάν μπορεί ή όχι να περάσει στον χώρο της Βουλής.

Το EAPδεν παρέχει κάποιο χαρακτηριστικό ασφαλείας όπως η κρυπτογράφηση των δεδομένων τα οποία βρίσκονται στα σώματα των EAPπλαισίων. Έτσι χρειάζεται οι σχεδιαστές του δικτύου

να υλοποιήσουν μηχανισμούς ασφαλείας σε άλλα επίπεδα. Για παράδειγμα, εάν η σύνδεση μεταξύ του supplicantκαι του μηχανισμού αυθεντικοποίησης είναι ασύρματη, τότε θα ήταν βέλτιστο να υλοποιηθεί κάποιου είδους κρυπτογράφηση συνδέσμου όπως για παράδειγμα το 802.11ac. Σε αυτή την περίπτωση, το 802.11acθα κρυπτογραφούσε το κομμάτι των δεδομένων του 802.11 πλαισίου, το οποίο περιέχει τα 802.1X πρωτόκολλα.

Υπάρχουν τέσσερα είδη EAPπλαισίων:

- Request (Αίτημα)
- Response (Απάντηση)
- Success (Επιτυχία)
- Failure (Αποτυχία)

Όπως αναφέρθηκε προηγουμένως, το EAPOLπάντα μεταφέρει EAPπλαίσια σε EAPOLπλαίσια τύπου "0".

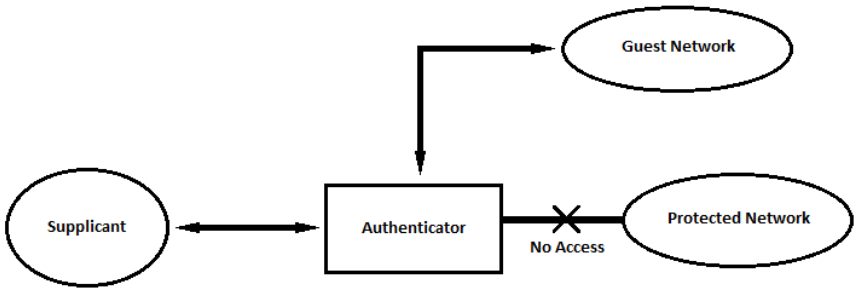
Ο χρήστης που απαιτεί πρόσβαση στο δίκτυο (supplicant) μπορεί να εκδώσει μόνο EAPResponseπλαίσια και ο μηχανισμός αυθεντικοποίησης μπορεί να πραγματοποιήσει EAPRequest, EAPSuccessκαι EAPFailureπλαίσια. Ο μηχανισμός αυθεντικοποίησης εκδίδει EAPRequestπλαίσια για να μεταφέρει EAP-Methodδεδομένα τα οποία ταξιδεύουν από τον supplicantπρος τον serverαυθεντικοποίησης. Ένας μηχανισμός αυθεντικοποίησης θα στείλει ένα EAPSuccessπλαίσιο προς τον supplicantεφόσον ο serverαυθεντικοποίησης ενημερώσει τον μηχανισμό αυθεντικοποίησης ότι ο χρήστης ο οποίος απαιτεί πρόσβαση στο δίκτυο (supplicant) μπορεί να έχει πρόσβαση στο προστατευόμενο δίκτυο. Ο μηχανισμός αυθεντικοποίησης θα στείλει ένα EAPFailureπλαίσιο στον supplicantεάν το αποτέλεσμα της διαδικασίας αυθεντικοποίησης έδειχνε ότι δεν επιτρεπόταν στον supplicantη πρόσβαση στο προστατευμένο δίκτυο. Τα EAPSuccessκαι EAPFailureπλαίσια αποστέλλονται ως απάντηση για το αποτέλεσμα της EAP-Methodμεθόδου. Σε ορισμένες περιπτώσεις ένας μηχανισμός αυθεντικοποίησης μπορεί να εκδώσει EAPFailureπλαίσια προς τον supplicantούτως ώστε να ξεκινήσει η διαδικασία αυθεντικοποίησης καθώς το EAPFailureπλαίσιο προκαλεί επαναφορά στη σύνδεση του supplicant.

Το EAPπαρέχει σωστή διάταξη των EAPπλαισίων μέσω ενός μηχανισμού ο οποίος "κλειδώνει κάθε βήμα"(lock-step). Αυτή είναι μια απλή διαδικασία δια της οποίας ο μηχανισμός

αυθεντικοποίησης για παράδειγμα ορίζει μια τιμή στο πεδίο Αναγνωριστικού του EAPπλαισίου όταν αποστέλλει ένα EAPRequestπλαίσιο στον supplicant. Ο supplicantορίζει την ίδια τιμή στο πεδίο Αναγνωριστικού του EAPResponseπλαισίου. Έτσι ενημερώνεται ο μηχανισμός αυθεντικοποίησης πως ο supplicantέχει λάβει το EAPRequestπλαίσιο και έχει προχωρήσει στο επόμενο πλαίσιο.

Έπειτα αφού ενεργοποιηθεί η σύνδεση μεταξύ του supplicantκαι του μηχανισμού αυθεντικοποίησης, ο μηχανισμός αυθεντικοποίησης στέλνει ένα EAPRequestπλαίσιο (ξανά, ενθυλακωμένο σε ένα πλαίσιο EAPOLτύπου "0")για να ζητήσει την ταυτότητα του supplicant. Ο μηχανισμός αυθεντικοποίησης από αυτό το σημείο, θα κόψει την πρόσβαση σε κάθε μηEAP-Methodκίνηση ως προς το να περάσει στην προστατευμένη πλευρά του δικτύου. Με βάσει τη διαδικασία η οποία έχει οριστεί στην μέθοδο EAP-Method, ο supplicantκαι ο serverαυθεντικοποίησης θα συζητήσουν τη χρήση της EAP-Methodμεθόδου. Η επικοινωνία ανάμεσα σε supplicantκαι μηχανισμό αυθεντικοποίησης περιλαμβάνουν ανταλλαγές EAPOLπλαισίων τύπου "0" τα οποία μεταφέρουν EAPκαι EAP-Methodδεδομένα. Ο μηχανισμός αυθεντικοποίησης απλώς λειτουργεί ως μεταφραστής και διατηρεί τη ροή από EAP-Methodδεδομένα ανάμεσα σε supplicantκαι serverαυθεντικοποίησης μέχρι ο serverαυθεντικοποίησης αποφασίσει να επιτρέψει ή να απαγορεύσει την πρόσβαση στον supplicant.

Εν τέλει, ο μηχανισμός αυθεντικοποίησης μπορεί να κατευθύνει τον χρήστη που απαιτεί πρόσβαση στο δίκτυο (supplicant)σε ένα εξουσιοδοτημένο (authorized) VLAN. Εάν ο supplicantδεν καταφέρει να πιστοποιηθεί, τότε ο μηχανισμός αυθεντικοποίησης θα τον δρομολογήσει σε κάποια πόρτα η οποία φιλοξενεί τους μη-εξουσιοδοτημένους χρήστες (π.χ. guestVLAN), και εκεί θα μπορεί ο εκάστοτε χρήστης να έχει μόνο πρόσβαση στο διαδίκτυο, αν για παράδειγμα του επιτρέπεται (Εικόνα 2.10). Σε ορισμένες περιπτώσεις, οι πόρτες των switchμπορεί να υποστηρίζουν δυναμική εκχώρηση VLANέτσι ώστε ο supplicantνα συνδέεται στο κατάλληλο VLANμε βάσει τα στοιχεία τα οποία έδωσε προς επεξεργασία στον serverαυθεντικοποίησης.



Εικόνα2.7

Αφού ο μηχανισμός αυθεντικοποίησης στείλει το αρχικό EAPRequestπλαίσιο προς τον supplicant,μπορεί να μην υπάρχει ανταπόκριση από τον supplicant. Πηγαίνοντας πίσω στο προηγούμενο παράδειγμα μας, ο Δημήτρης μπορεί να άκουγε πολύ δυνατά μουσική στο αυτοκίνητο του την ώρα που είχε φτάσει στην πύλη της Βουλής με αποτέλεσμα να μην άκουγε τα όσα του έλεγε ο φύλακας. Σε ένα πραγματικό δίκτυο, η κάρτα δικτύου όπως για παράδειγμα η Ethernetκάρτα ή ένας 802.11 αντάπτορας θα μπορούσαν να είναι ελαττωματικές ή να μην υποστηρίζουν το 802.1X. Μετά από κάποια αναμονή ορισμένου χρόνου, ο μηχανισμός αυθεντικοποίησης θα ξαναπροσπαθήσει να στείλει το EAPRequestπλαίσιο. Εάν ο μηχανισμός αυθεντικοποίησης δεν λάβει κάποια απάντηση από τον supplicantμετά από κάποιο αριθμό επαναλαμβανομένων αποστολών EAPRequestπλαισίων, τότε ο μηχανισμός αυθεντικοποίησης μπορεί να τερματίσει τη σύνδεση είτε να συνδέσει τον χρήστη σε ένα guestVLAN, αναλόγως τις ρυθμίσεις του δικτύου. Σε ένα ασύρματο τοπικό δίκτυο WLAN, ο μηχανισμός αυθεντικοποίησης αποσυνδέεται από τον ασύρματο χρήστη (supplicant)καθώς τερματίζει τη σύνδεση.

Μέχρι στιγμής έχουμε αναλύσει τα EAPOLτύπου “0” πλαίσια για τη μεταφορά EAPκαι EAP-Methodδεδομένων. Άλλοι τύποι EAPOL πλαισίων περιλαμβάνουν τα παρακάτω:

- EAPOL-Start
- EAPOL-Logoff
- EAPOL-Key

- EAPOL-Encapsulated_ADF-Alert

Αυτά τα πλαίσια βρίσκονται εκτός του πεδίου EAPκαι δεν μεταφέρουν EAPή EAP-Methodπληροφορίες. Ποιος είναι ο λόγος που τα χρησιμοποιούμε λοιπόν; Η απάντηση βρίσκεται στο ότι παρέχουν επιπλέον λειτουργικότητα η οποία είναι χρήσιμη στο να κάνει το EAPνα λειτουργεί σε ένα τοπικό δίκτυο LAN. Το EAPδεν ήταν αρχικά σχεδιασμένο γιανα λειτουργεί σε LANs, παρόλα αυτά στο 802.1X επινοήθηκε το EAPOLούτως ώστε να ενθυλακώνει μέσα του το EAP(μέσω EAPOLτύπου "0" πλαισίων) και να παρέχει μια επιπλέον LANλειτουργικότητα.

Για παράδειγμα, ένας supplicantμπορεί να στείλει ένα EAPOLStartπλαίσιο. Έτσι 'τραβάει' το ενδιαφέρον του μηχανισμού αυθεντικοποίησης ο οποίος απαντάει αμέσως με ένα EAPRequestπλαίσιο με το οποίο ζητά να μάθει την ταυτότητα του χρήστη (supplicant). Στο παράδειγμα μας προηγουμένως αυτό αντιστοιχίζεται στο σημείο όπου ο Δημήτρης πλησιάζει τον φύλακα της πύλης και εκείνος είναι απασχολημένος καθώς μιλάει με κάποιον. Ο Δημήτρης πρέπει να τραβήξει την προσοχή του φύλακα έτσι ώστε να ξεκινήσει η διαδικασία εισόδου προς τον χώρο της Βουλής. Κάτι παρόμοιο μπορεί να συμβεί και στα πραγματικά δίκτυα διότι ο supplicantμπορεί να δέχεται δεδομένα από άλλες συσκευές όπως για παράδειγμα ένα switch το οποίο είναι ήδη πιστοποιημένο, και η σύνδεση είναι ήδη ενεργή. Ο μηχανισμός αυθεντικοποίησης δεν μπορεί να γνωρίζει εάν ο χρήστης είναι συνδεδεμένος, παρόλα αυτά ο supplicantπρέπει να δώσει σήμα στον μηχανισμό αυθεντικοποίησης με ένα EAPOLStartπλαίσιο.

Το 802.1X (π.χ. EAPOL)εφαρμόζεται στο 2^{ο} Επίπεδο (Layer 2) με σκοπό το να μην επιτρέψει σε έναν χρήστη να συνδεθεί σε ένα δίκτυο εάν δεν έχει πρώτα περάσει από τη διαδικασία της αυθεντικοποίησης. Εάν υποθέσουμε για παράδειγμα πως η διαδικασία της αυθεντικοποίησης γινόταν στο 4^{ο} Επίπεδο (Layer 4), τότε μια σύνδεση στο δίκτυο θα είχε ήδη γίνει προτού ξεκινήσει η διαδικασία της ταυτοποίησης χρήστη. Κάτι τέτοιο θα έκανε το δίκτυο ευάλωτο απέναντι σε κάποιον κακόβουλο χρήστη.

Προκειμένου να επιτευχθεί η υλοποίηση στο 2^{ο} Επίπεδο, το 802.1X εκμεταλλεύεται τον έλεγχο πρόσβασης ο οποίος προσφέρεται από το 802.1Dπρωτόκολλο το οποίο ορίζει τις MACγέφυρες (bridges). Το 802.1Dείναι απαιτείται από όλα τα 802 LANs, συμπεριλαμβανομένων και των 802.3 (Ethernet)και 802.11 (Wi-Fi). Ως αποτέλεσμα, το 802.1X λειτουργεί σε κάθε τύπου

LAN.Η υλοποίηση γίνεται με τρόπο ο οποίος κάνει την κίνηση 802.1X πακέτων να μην παρεμβάλλει τη λειτουργία άλλων LAN πρωτοκόλλωνκαι επιτρέπει στα 802.1X πλαίσια να είναι τα πρώτα τα οποία αποστέλλονται στη σύνδεση.

Το 802.1X χρησιμοποιεί την διευθυνσιοδότηση η οποία είναι αποκλειστικά για το 802.1DSpanning-Treeπρωτόκολλο. Το 802.1Dδιαθέτει αρκετές δεσμευμένες διευθύνσεις ομάδας. Με τις διευθύνσεις ομάδας, κάθε μέλος της ομάδας επεξεργάζεται το πλαίσιο. Στο 802.1X έχει ανατεθεί μια από τις μη χρησιμοποιημένες 802.1DSpanning-Treeδιευθύνσεις ομάδας η οποία και είναι η 01:80:C2:00:00:03.Η διεύθυνση αυτή αρκετές φορές ονομάζεται και 802.1X PortAccessEntry(PAE)διεύθυνση. Όλες οι 802-based συσκευές (κάρτες δικτύου χρηστών, switches, accesspoints κλπ.) έχουν σχεδιαστεί για να λαμβάνουν και να επεξεργάζονται πλαίσια τα οποία έχουν αυτή την διεύθυνση ομάδας.

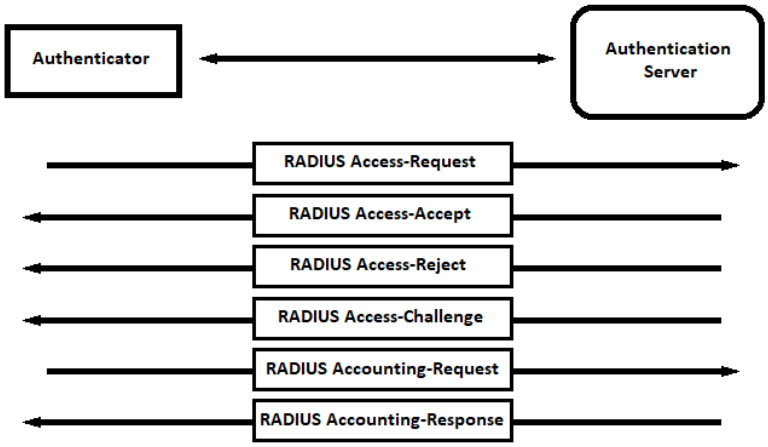
2.8 Από τον μηχανισμό αυθεντικοποίησης έως τον Serverαυθεντικοποίησης: RADIUS

Στην Εικόνα 2.11 απεικονίζεται η επικοινωνία ανάμεσα σε μηχανισμό αυθεντικοποίησης και server αυθεντικοποίησης με τη χρήση του RADIUS. Όμοια με το EAP, τα RADIUS πλαίσια αποστέλλονται με τη χρήση μιας διαδικασίας η οποία ‘κλειδώνει κάθε βήμα’ (lock-step). Οι τύποι πλαισίων RADIUS περιλαμβάνουν και τα παρακάτω:

- Access-Request
- Access-Accept
- Access-Reject
- Access-Challenge
- Accounting-Request
- Accounting-Response

Ένα μεγάλο μέρος της επικοινωνίας μεταξύ του μηχανισμού αυθεντικοποίησης και του serverαυθεντικοποίησης περιλαμβάνουν RADIUSAccess-Requestκαι RADIUSAccess-Challengeπλαίσια. Ο μηχανισμός αυθετικοποίησης στέλνει δεδομένα μεθόδων EAP-Methodπρος τον serverαυθεντικοποίησης μέσω RADIUSAccess-Requestπλαισίων. Ο μηχανισμός αυθεντικοποίησης θα έχει αφαιρέσει τα δεδομένα EAP-Methodαπό τα EAPOL/EAPπλαίσια που έχει λάβει από τον χρήστη (supplicant). Εάν ο serverαυθετικοποίησης λάβει ένα

RADIUSAccess-Request, την IPδιεύθυνση του μηχανισμού αυθεντικοποίησης καθώς και μία κοινή κρυφή πληροφορία που παρέχεται από τον μηχανισμό αυθεντικοποίησης και η οποία ταιριάζει με αυτό που περιμένει να λάβει ο serverαυθεντικοποίησης, τότε ο serverαυθεντικοποίησης θα προχωρήσει στην επεξεργασία του αιτήματος. Εάν τα στοιχεία αυτά δεν ταιριάζουν, τότε ο serverαυθεντικοποίησης παραμένει στάσιμος και δεν απαντάει στα αιτήματα αυτά. Ο μηχανισμός αυθεντικοποίησης κατά πάσα πιθανότητα θα επαναλάβει την αποστολή του RADIUSAccess-Requestπλαισίου μερικές ακόμα φορές. Παρόλα αυτά, εάν γίνει η κατάλληλη παραμετροποίηση, ο μηχανισμός αυθεντικοποίησης από ένα σημείο και μετά θα σταματήσει και θα προσπαθήσει να επικοινωνήσει με έναν άλλο RADIUSserverμέσω μιας άλλης σύνδεσης. Ο serverαυθεντικοποίησης στέλνει EAP-Methodδεδομένα προς τον μηχανισμό αυθεντικοποίησης (και δεσμεύεται για τον supplicant)μέσω RADIUSAccess-Challenge πλαισίων. Βέβαια, ο χρήστης (supplicant) θα εξάγει την πληροφορίαEAP-Methodαπό το RADIUSπλαίσιο και θα στείλει την EAP-Methodπληροφορία προς τον supplicantμέσω EAPOL/EAP.



Εικόνα2.8

Μόλις ληφθεί μια εκτίμηση με βάσει την EAP-Method πληροφορία για το εάν ο supplicantέχει πιστοποιηθεί ή δεν έχει πιστοποιηθεί, ο serverαυθεντικοποίησης στέλνει αντίστοιχα ένα RADIUSAccess-Acceptή ένα RADIUSAccess-Rejectπλαίσιο προς τον μηχανισμό αυθεντικοποίησης. Ο μηχανισμός αυθεντικοποίησης τότε εκδίδει το σχετικό EAPOLSuccessή EAPOLFailureπλαίσιο προς τον supplicant. Σε αυτό το σημείο, εάν το αίτημα ολοκληρώθηκε

επιτυχώς, τότε ο μηχανισμός αυθεντικοποίησης ανοίγει την ‘πόρτα’ (port) για τον χρήστη (supplicant) δίνοντας του πρόσβαση στο προστατευόμενο δίκτυο.

2.9 Μια ιστορική όψη

Τα πρώτα 802 προτύπου LANπαρουσιάστηκαν στις αρχές του 1980. Καθώς αυτά τα δίκτυα άρχισαν ναπληθύνονται και να αντικαθιστούν τα παλαιού τύπου mainframeσυστήματα, οι κατασκευαστές δικτυακού εξοπλισμού και οργανισμοί προτύπων κινητοποιήθηκαν με σκοπό να δημιουργήσουν μια πύλη ασφαλείας. Στις αρχές, δεν ήταν τόσο σημαντικό για τα ενσύρματα εταιρικά δίκτυα διότι οι τοίχοι στα κτίρια πρόσφεραν φυσικό έλεγχο πρόσβασης. Εάν κάποιος κακόβουλος χρήστης δεν μπορούσε να έχει πρόσβαση στον χώρο, τότε ήταν σχεδόν αδύνατο να συνδεθεί στο δίκτυο. Η ώθηση προς την εφαρμογή συστημάτων port-basedαυθεντικοποίησης ξεκίνησε όταν οι υπάλληλοι άρχισαν να έχουν πρόσβαση στα εταιρικά δίκτυα από απομακρυσμένες τοποθεσίες όπως είναι το σπίτι ή ένα δωμάτιο ξενοδοχείου. Το ‘άνοιγμα’ αυτό των εταιρικών δικτύωνπρος το διαδίκτυο και η βελτίωση των ταχυτήτων του internet έχει ως συνέπεια να απαιτεί πιο αυστηρούς κανόνες κατά τον έλεγχο πρόσβασης.Έτσι η port-basedαυθεντικοποίηση αποτέλεσε ένα πολύ σημαντικό εργαλείο, κάτι το οποίο οδήγησε στη δημιουργία σχετικών IEEEπροτύπων και IETFπροδιαγραφών.

Στις μέρες μας, σχεδόν όλα τα εταιρικά δίκτυα συνδέονται με το internetκαι παρά τη χρήση τοίχων προστασίας, υπάρχει πάντα η ανησυχία πως κάποιος κακόβουλος χρήστης μπορεί να μπει στο δίκτυο. Επιπλέον, αρκετές εταιρίες έχουν ασύρματα δίκτυα (WLANs) είτε ως βασική δικτυακή υποδομή είτε ως επέκταση της υπάρχουσας ενσύρματης υποδομής. Τα ασύρματα δίκτυα είναι πολύ πιο εύκολο να δώσουν πρόσβαση σε κάποιον κακόβουλο χρήστη λόγω της φύσης τους, μιας και τα ασύρματα δίκτυα μπορούν να έχουν εμβέλεια και έξω από τους τοίχους μιας εταιρίας. Θα μπορούσε δηλαδή κάποιος κακόβουλος χρήστης να βρίσκεται δίπλα από τον χώρο της εταιρίας στην οποία θέλει να διεισδύσει σε σημείο το οποίο μπορεί να λάβει σήμα από κάποιο ασύρματο σημείο πρόσβασης (accesspoint).

Το πρώτο βήμα για τη δημιουργία προδιαγραφών port-basedαυθεντικοποίησης ήταν με την δημιουργία του ExtensibleAuthenticationProtocol (EAP), το οποίο και εγκρίθηκε το 1998 ως IETFRFC 2284 με τίτλο “PPPExtensibleAuthenticationProtocol”. Το EAPπαρέχει επικοινωνία μεταξύ μιας συσκευής χρήστη η οποία βρίσκεται στη διαδικασία αυθεντικοποίησης και ενός serverαυθεντικοποίησης. Το EAPείναι ένα point-to-pointπρωτόκολλο το οποίο μεταφέρει

στοιχεία αυθεντικοποίησης. Συγκεκριμένες μέθοδοι EAP-Methodsπαρέχουν τον μηχανισμό αυθεντικοποίησης, όπως για παράδειγμα τον καθορισμό των στοιχείων ταυτοποίησης. Υπάρχουν κάποιες μέθοδοι EAP-Methodsοι οποίες πρέπει να υποστηρίζονται απαραίτητα από το EAP και άλλες προαιρετικές μέθοδοι EAP-Methods.

Ακόμη ένα σημαντικό βήμα έγινε το 2001 όταν η IEEEεπικύρωσε το 802.1X πρότυπο. Η πρώτη αυτή έκδοση του 802.1X-2001 προτύπου είχε βασιστεί κυρίως στο EAP. Στην πραγματικότητα το 802.1X αποτέλεσε μια επέκταση του EAPη οποία λειτουργεί σε τοπικά δίκτυα (LANs). Το 802.1X ορίζει το EAPπάνω σε LANs (EAPOL)πρωτόκολλο για να πετύχει αυτό. Το 802.1X (και το EAPOL)εφαρμόζει μόνο κατά τη διεπαφή ανάμεσα σε συσκευή χρήστη η οποία ταυτοποιείται και ένα Ethernetswitchή ένα WLAN access-point στο οποίο η συσκευή του χρήστη συνδέεται. Το 2004 το EAPκαι το 802.1X ανανεώθηκαν σημαντικά, οδηγώντας στη δημιουργία του RFC 3748 για το EAPκαι το 802.1X-2004.Στη συνέχεια έχουμε ακόμα μια βελτιωμένη έκδοση του πρωτοκόλλου μετην ονομασία IEEE 802.1X-2010. Επίσης το RADIUSαποτελεί ακόμα ένα σημαντικό στοιχείο ενός συστήματος port-basedαυθεντικοποίησης. Το RADIUSεισήχθη πιο επίσημα στα έγγραφα port-basedαυθεντικοποίησης το 2003.

Στις μέρες μας το 802.1X, το RADIUS, το EAPκαι οι μέθοδοι EAP-Methodsείναι αρκετά καλά συνδεδεμένα μέσω προτύπων και προδιαγραφών. Αυτό οδηγεί στην ανάπτυξη ασφαλών συστημάτων port-basedαυθεντικοποίησης τα οποία παρέχουν βελτιωμένη διαλειτουργικότητα σε σχέση με τις πρώτες υλοποιήσεις και εφαρμογές.

3 Το πρωτόκολλο EAPOL

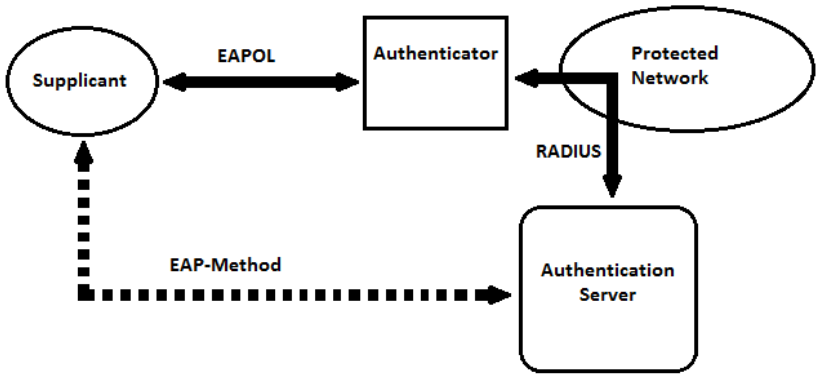
Στο κεφάλαιο αυτό θα μελετήσουμε με μεγαλύτερη λεπτομέρεια τη δομή πακέτων του EAPOLπρωτοκόλλου (ExtensibleAuthenticationProtocoloverWirelessLAN). Αυτό σε συνδυασμό με τα όσα είδαμε και στο προηγούμενο κεφάλαιο θα μας δώσουν μια καλή εικόνα σχετικά με το πως το EAPOLλειτουργεί. Έτσι θα έχουμε μια βάση ως προς την υλοποίηση και την αντιμετώπιση προβλημάτων σε port-basedσυστήματα αυθεντικοποίησης.

3.1 ΑνακεφαλαίωσηEAPOL

Το EAPOLορίζεται στο 802.1X πρότυπο έτσι ώστε να προσαρμόσει την EAPεπικοινωνία για να λειτουργεί πάνω σε τοπικά δίκτυα (LANs).Για να συμβεί αυτό, το EAPOLπαρέχει επιπλέον πεδία κεφαλίδας σε EAPπακέτα και δημιουργεί μερικούς εξειδικευμένους τύπους πακέτων EAP.

Επιπλέον, το EAPOLμεταφέρει EAPπακέτα ως δεδομένα μέσα στο σώμα EAPOLπακέτων. Όπως φαίνεται και στην Εικόνα 3.1, το EAPOLείναι ο βασικός σύνδεσμος επικοινωνίας ανάμεσα σε χρήστη που απαιτεί πρόσβαση στο δίκτυο (supplicant) και μηχανισμό αυθεντικοποίησης μέσα σε ένα σύστημα port-basedαυθεντικοποίησης.

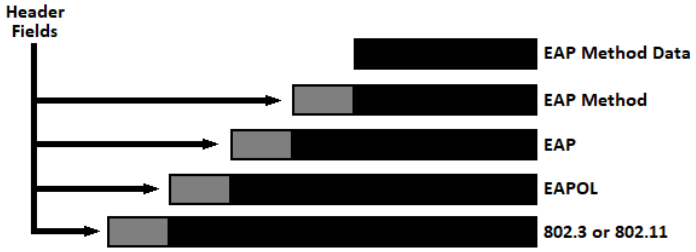
Το EAPOLπρωτόκολλο λειτουργεί στο 2^{ο} Επίπεδο (Layer 2)για να αποτρέψει τη σύνδεση ενός supplicantμε το δίκτυο πριν την αυθεντικοποίηση. Αυτό επιτυγχάνεται με την εκμετάλλευση του ελέγχου πρόσβασης που προσφέρεται από το IEEE 802.1D, το οποίο ορίζει τις MACγέφυρες και είναι απαραίτητο σε όλα τα 802τύπου τοπικά δίκτυα (LANs). Το πρωτόκολλο εξασφαλίζει ότι τα EAPOLπακέτα είναι τα πρώτα που αποστέλλονται στη σύνδεση.



Εικόνα3.1

3.2 ΕνθυλάκωσηEAPOL

Είναι σημαντικό να έχουμε στο μυαλό μας ότι η ενθυλάκωση η οποία συμβαίνει, γίνεται για να στηρίξει την επικοινωνία ανάμεσα σε supplicantκαι μηχανισμό αυθεντικοποίησης. Αυτό είναι ιδιαίτερα σημαντικό όταν μαθαίνουμε για πρώτη φορά τον τρόπο με τον οποίο η port-basedαυθεντικοποίηση λειτουργεί και πότε γίνεται αντιμετώπιση προβλημάτων. Η διαδικασία διαστρωμάτωσης είναι όμοια με άλλες δικτυακές αρχιτεκτονικές. Η Εικόνα 3.2 απεικονίζει την ενθυλάκωση που λαμβάνει χώρα μεταξύ του supplicantκαι του μηχανισμού αυθεντικοποίησης. Η συλλογή αυτών των πρωτοκόλλων περιλαμβάνει ένα σύστημα 802.1X port-basedαυθεντικοποίησης. Το EAPOLείναι η συνολική οντότητα port-basedαυθεντικοποίησης η οποία χρειάζεται μεταφορά μέσω ενός πρωτοκόλλου ζεύξης.

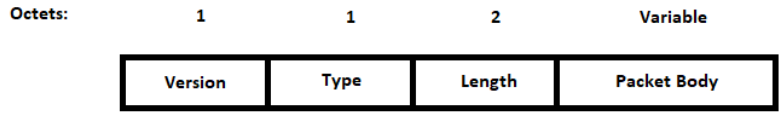


Εικόνα3.2

Ο βασικός στόχος της επικοινωνίας κατά την port-basedαυθεντικοποίηση είναι η μεταφορά δεδομένων EAP-Methodμεθόδων, τα οποία υλοποιούν την διαδικασία αυθεντικοποίησης. Η κάθε μέθοδος EAP-Methodπου είναι σε χρήση ορίζει τα EAPδεδομένα. Τα EAPπακέτα (EAP-Requestκαι EAP-Responseπακέτα) μεταφέρουν τις κεφαλίδες πρωτοκόλλωντων EAP-Method μαζί με δεδομένα. Τα EAPOLπακέτα μεταφέρουν τα EAPπακέτα μαζί με 802.3 (ή 802.11) δεδομένα πλαισίων μεταφέρονται στα EAPOLπακέτα.Εκτός από τη μεταφορά των πρωτοκόλλων υψηλότερου επιπέδου ως δεδομένα, καθώς θα προχωράμε στις επόμενες υποενότητες, καθένα από τα πρωτόκολλα (EAPOL, EAPκλπ.) έχει τη δική του λειτουργία και ορίζει πακέτα τα οποία μπορεί να μην μεταφέρουν κάποιο από τα υψηλότερου επιπέδου πρωτόκολλα. Ένα απλό παράδειγμα που θα μπορούσε να περιγράψει την διαδικασία της ενθυλάκωσης είναι εκείνο μιας εταιρείας μεταφορών η οποία μεταφέρει αγαθά από την Αθήνα (supplicant)στην Πάτρα (μηχανισμός αυθεντικοποίησης). Το αντικείμενο το οποίο μεταφέρεται είναι ένα ποδήλατο (δεδομένα μεθόδων EAPMethod)το οποίο βρίσκεται μέσα σε ένα κουτί (EAP)το οποίο κουτί με τη σειρά του είναι τυλιγμένο με ειδικό υλικό που το προστατεύει από χτυπήματα (EAPOL).

3.3 Δομή πακέτωνEAPOL

Το EAPOL προσθέτει τρία επιπλέον πεδία σε EAPπακέτα, όπως φαίνεται και στην Εικόνα 3.3. Τα πεδία αυτά προσθέτουν επιπλέον λειτουργίες οι οποίες είναι απαραίτητες για την ενσωμάτωση με τα LANsκαθώς και για την αποτελεσματική μεταφορά EAPπακέτων (και δεδομένα μεθόδωνEAP-method). Στις παρακάτω ενότητες θα αναλύσουμε κάθε πεδίο ξεχωριστά.



Εικόνα3.3

3.3.1 Πεδίο Version

Το πεδίο Versionενός EAPOLπακέτου προσδιορίζει την έκδοση του EAPOLπρωτοκόλλου την οποία ο αποστολέας του EAPOLπακέτου υποστηρίζει. Η τιμή η οποία βρίσκεται σε αυτό το πεδίο έχει μήκος μιας οκτάδας (1 byte). Το πεδίο Versionσε όλες τις 802.1X υλοποιήσεις περιέχει την τιμή "0000 0002". Όπως και σε άλλα πρωτόκολλα επικοινωνίας, η υλοποίηση του πεδίου Versionεπιτρέπει την ανάπτυξη εξαρτημάτων και συστημάτων τα οποία έχουν συμβατότητα προς τα πίσω.

3.3.2 Πεδίο Type

Το πεδίο Typeενός EAPOLπακέτου αναπαρίσταται από μια τιμή με μήκος μιας οκτάδας (1 byte), και αντιστοιχίζει τον τύπο πακέτου που αποστέλλεται. Ο παρακάτω Πίνακας 3.1 απεικονίζει τους τύπους των EAPOLπακέτων με βάσει την τιμή που έχει το πεδίο Type.

Πίνακας3.3

PACKET TYPE	TYPE FIELD VALUE
EAP-Packet	0000 0000 (Hex "00")
EAPOL-Start	0000 0001 (Hex "01")
EAPOL-Logoff	0000 0010 (Hex "02")
EAPOL-Key	0000 0011 (Hex "03")
EAPOL-Encapsulated-ASF-Alert	0000 0100 (Hex "04")

3.3.3 Πεδίο Length

ΤοπεδίοLengthσεέναEAPOLπακέτοέχειμήκοςδυοοκτάδων (2 bytes)καιορίζειτομέγεθοςτουπεδίουPacketBody. Η τιμή που υπάρχει στο πεδίο Length

απεικονίζει το μήκος ως μέγεθος σε οκτάδες (bytes). Για παράδειγμα, ένα EAPOLLengthπεδίο με τιμή “0000 0000 0001 1011” δείχνει πως το πεδίο PacketBodyενός EAPOLπακέτου περιέχει 27 οκτάδες (bytes) με δεδομένα. Στο πεδίο Lengthμια τιμή της μορφής “0000 0000 0000 0000” σημαίνει πως το EAPOLπακέτο δεν έχει το πεδίοPacketBody, κάτι τέτοιο συμβαίνει με τις περιπτώσεις των EAPOL-Startκαι EAPOL-Logoffπακέτων.

3.3.4 Πεδίο Packet Body

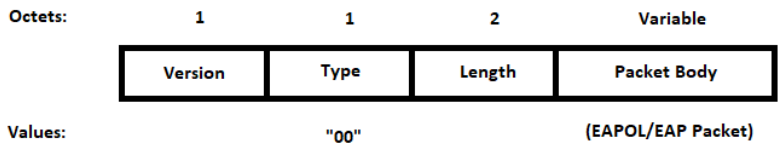
Το πεδίο PacketBodyαποτελεί το ωφέλιμο τμήμα ενός EAPOLπακέτου και είναι παρόν στα EAP-Packet, EAPOL-Keyκαι EAPOL-Encapsulated-ASF-Alertτύπους πακέτων, το PacketBodyπεριλαμβάνει ακριβώς ένα ASF-Alertπακέτο.

3.4 Τύποιπακέτων EAPOL

Οι παρακάτω ενότητες περιγράφουν κάθε τύπο πακέτων EAPOL.

3.4.1 EAP-Packet

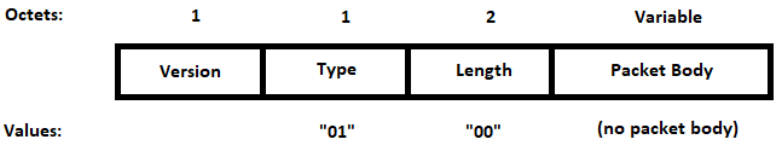
ΣτηνΕικόνα 3.4 απεικονίζεταιέναEAP-Packet. Ένα EAP-Packetμερικές φορές αποκαλείται και ως ένα Type “0” EAPOLπακέτο ή EAPOLπακέτο δεδομένων το οποίο μεταφέρει ένα EAPπακέτο. Αυτό απαιτεί να γνωρίζει τον προορισμό, είτε εκείνος είναι ο supplicantείτε ο μηχανισμός αυθεντικοποίησης έτσι ώστε να αφαιρεθεί η EAPOLκεφαλίδα και να γίνει η επεξεργασία του EAPπακέτου. Έτσι, τα Type “0” EAPOLπακέτα απλώς περνούν EAPπακέτα τα οποία με τη σειρά τους συνήθως μεταφέρουν EAP-Methodδεδομένα. Μετά την έναρξη της σύνδεσης, τα πιο συνήθη EAPOLπακέτα είναι οι EAP-Packetοντότητες.



Εικόνα3.4

3.4.2 EAPOL-Start

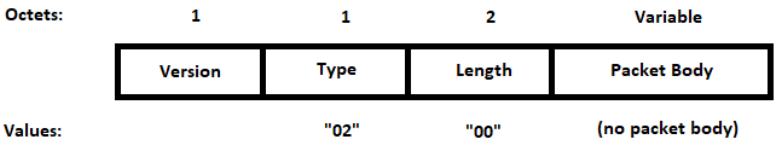
Η διαδικασία αυθεντικοποίησης ξεκινά συνήθως όταν η κατάσταση σύνδεσης μεταβάλλεται από ανενεργή σε ενεργή. Ο μηχανισμός αυθεντικοποίησηςσυνήθως ξεκινά την διαδικασία ταυτοποίησης χρήστη μόλις η κατάσταση σύνδεσης γίνει από ανενεργή σε ενεργή, για παράδειγμα όταν ένας χρήστης σε ένα ενσύρματο Ethernetδίκτυο ανοίξει τον υπολογιστή του. Εάν η σύνδεση είναι ήδη ενεργή, και ο χρήστης που ζητά πρόσβαση (supplicant)πρέπει να αυθεντικοποιηθεί, τότε ο supplicantπρέπει να ξεκινήσει την διαδικασία αυθεντικοποίησης με το να στείλει ένα EAPOL-Startπακέτο με σκοπό να τραβήξει την προσοχή του μηχανισμού αυθεντικοποίησης. Ο μηχανισμός αυθεντικοποίησης τότε θα ξέρει πως πρέπει να ξεκινήσει η διαδικασία αυθεντικοποίησης. Η Εικόνα 3.5 απεικονίζει ένα EAPOL-Start πακέτο.



Εικόνα3.4

3.4.3 EAPOL-Logoff

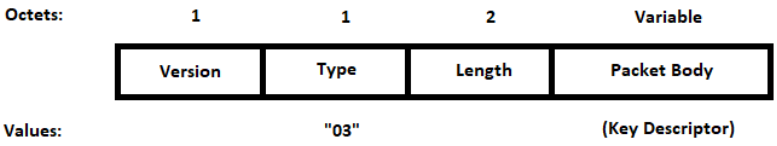
ΣτηνΕικόνα 3.6 απεικονίζεταιέναEAPOL-Logoffπακέτο. OsupplicantστέλνειέναEAPOL-Logoffπακέτο προς τον μηχανισμό αυθεντικοποίησης με σκοπό να επιστρέψει η θύρα που έχει ταυτοποιηθεί σε κατάσταση μη εξουσιοδοτημένη. Κάτι τέτοιο μπορεί να συμβεί όταν ο χρήστης αποφασίσει να αποσυνδεθεί από ένα σύστημα το οποίο βρίσκεται από την προστατευόμενη πλευρά του δικτύου. Η χρήση EAPOL-Logoffπακέτων είναι ιδανική καθώς κάνει πιο αποτελεσματική τη χρήση πόρων του μηχανισμού αυθεντικοποίησης.



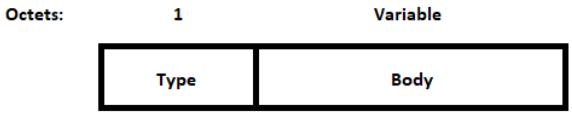
Εικόνα3.4

3.4.4 EAPOL-Key

ΣτηνΕικόνα 3.7 απεικονίζεταιέναEAPOL-Keyπακέτοτοοποίομπορείναναποσταλείείτεαπότονχρήστηπουεπιθυμείπρόσβασηστοδίκτυο (supplicant) είτεαπότονμηχανισμόαυθεντικοποίησης. ΤοEAPOL-Key πακέτο είναι προαιρετικό. Εάν η 802.1X εφαρμογή προϋποθέτει τη μεταφορά κλειδιών ανάμεσα σε supplicantκαι μηχανισμό αυθεντικοποίησης, το PacketBodyενός EAPOL-Keyπακέτου περιέχει και ένα KeyDescriptor πεδίο με τη μορφή που δείχνει η Εικόνα 3.8



Εικόνα3.4



Εικόνα3.4

DescriptorTypeπεδίο

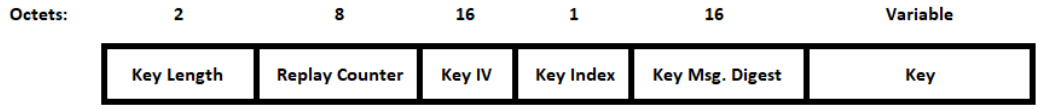
ToDescriptorTypeπεδίοενόςEAPOL-Keyπακέτουέχειμήκοςμιαςοκτάδας (1 byte) καιαντιπροσωπεύειτοντύποτουKeyDescriptorπουμεταφέρεται από το EAPOL-Keyπακέτο. Η τιμή του DescriptorTypeεπιτρέπει στην πλευρά που λαμβάνει το πακέτο να ερμηνεύσει σωστά τον KeyDescriptor. Στον Πίνακα 3.2 βλέπουμε τις τιμές για τα EAPOLDescriptorTypes.

Πίνακας3.4

DESCRIPTOR TYPE	VALUE
RC4 Key Descriptor	1
IEEE 802.11 Key Descriptor	2

Descriptor Body πεδίογιαRC4

Η Εικόνα 3.9 μας δείχνει την μορφή ενός RC4 DescriptorBodyσε ένα EAPOL-Keyπακέτο. Αυτού του τύπου descriptorμπορούμε να συναντήσουμε σε προηγούμενες υλοποιήσεις του 802.1X. Η ερμηνεία του κάθε πεδίου φαίνεται παρακάτω στον Πίνακα 3.3



Εικόνα3.4

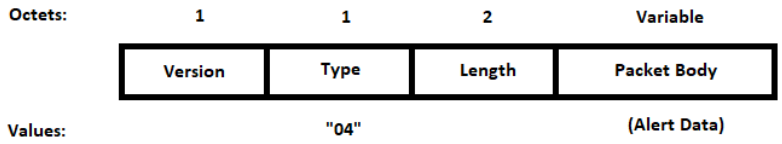
Πίνακας3.4

EAPOL-KEY FIELDS	SIZE	VALUE
Key Length	2 bytes	Είναιίσομετοναριθμόbytesστοκλειδί. Π.χ. ένα κλειδί με μήκος 40 bitsέχει τιμή πεδίου KeyLengthίση με 5.
Replay Counter	8 bytes	Μια τιμή μετρητή η οποία εντοπίζει και αποτρέπει την επανάληψη μηνυμάτων κλειδιών
Key IV (Initialization Vector)	16 bytes	Ένας 128-bitτυχαίος αριθμός που απεικονίζει την IVτιμή που χρησιμοποιείται για να δημιουργήσει το RC4 κλειδί κρυπτογράφησης
Key Index	1 byte	Η τιμή δημιουργείται από τον μηχανισμό αυθεντικοποίησης και χρησιμοποιείται για να διαχωρίσει πολλαπλά κλειδιά τα οποία είναι σε χρήση. 7 bitsστο πεδίο αντιπροσωπεύουν έναν ακέραιο 0-127, ο οποίος είναι το KeyIndex. Μια σημαία ενός bit απεικονίζει τα παρακάτω: flag = 1 σημαίνει πως το κλειδί είναι ένα unicastκλειδί, flag = 0 σημαίνει πως το κλειδί είναι ένα broadcastκλειδί.
Key Message Digest	16 bytes	Αφομοιώνει όλα τα πεδία ενός

	EAPOLπακέτου
Key	Το πραγματικό κλειδί

3.4.5 EAPOL-Encapsulated-ASF-Alert

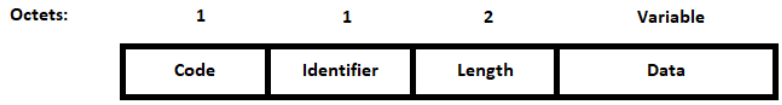
Η Εικόνα 3.10 μας δείχνει το πως είναι ένα EAPOL-Encapsulated-ASF-Alertπακέτο. Το πακέτο αυτό είναι χρήσιμο όταν ο supplicantπρέπει να στείλει πληροφορία προς την προστατευμένη πλευρά του δικτύου προτού ολοκληρωθεί η αυθεντικοποίηση. Για παράδειγμα, ο supplicantμπορεί να χρειαστεί να στείλει ένα μήνυμα κατάστασης προς τον server. Το περιεχόμενο των πακέτων EAPOL-Encapsulated-ASF-Alertπακέτων είναι γενικά αυτόνομο.



Εικόνα3.4

3.5 ΔομήπακέτωνEAP

Ένα EAPπακέτο περιλαμβάνει τα πεδία που απεικονίζονται στην Εικόνα 3.11. Οι παρακάτω ενότητες περιγράφουν αναλυτικά κάθε ένα από τα πεδία του EAPπακέτου.



Εικόνα3.5

3.5.1 Πεδίο EAP Code

ΌμοιαμετοTypeπεδίοσταEAPOLπακέτα, τοEAPCodeπεδίοαναγνωρίζειτοντύποτουEAPπακέτου. Το πεδίο αυτό έχει μέγεθος 1 byte. Στον Πίνακα 3.4 βλέπουμε τους διάφορους τύπους EAPπακέτων με βάσει την τιμή του πεδίου Code.

Πίνακας3.5

PACKET TYPE	CODE FIELD VALUE
EAP-Request	0000 0001 (Hex “01”)
EAP-Response	0000 0010 (Hex “02”)
EAP-Success	0000 0011 (Hex “03”)
EAP-Failure	0000 0100 (Hex “04”)

3.5.2 ΠεδίοEAP Identifier

ΤοπεδίοEAPIdentifierέχειμέγεθος 1 byte και δίνειτηνδυνατότηταναναντιστοιχίσειEAP-ResponseπακέταμεταισχύονταEAP-Requestπακέτα. Εάν το πεδίο Identifierσε ένα EAP-Requestπακέτο που έχει σταλεί από τον serverαυθεντικοποίησης προς τον supplicantκαι έχει για παράδειγμα την τιμή “0000 0101”, τότε ο supplicantθα απαντήσει με ένα EAP-Responseπακέτο στο οποίο το EAP-Identifier πεδίο θα έχει τιμή “0000 0101”. Επιπροσθέτως, ο μηχανισμός αυθεντικοποίησης χρησιμοποιεί τις ίδιες τιμές με εκείνες του Identifierόταν επανεκπέμπει EAPπακέτα. Για παράδειγμα ο μηχανισμός αυθεντικοποίησης μπορεί αρχικά να στείλει ένα EAP-Requestπακέτο προς τον supplicantμε τιμή στο πεδίο Identifierνα έχει οριστεί σε “0000 1100”. Εάν δεν υπάρξει απάντηση από τον supplicantτότε ο μηχανισμός αυθεντικοποίησης θα κάνει επανεκπομπή του EAP-Requestπακέτου με την τιμή στο πεδίο Identifierορισμένη σε

“0000 1100”.Έτσι ο supplicantγνωρίζει πως ένα συγκεκριμένο πακέτο αποτελεί επανεκπομπή και αποφεύγεται η επεξεργασία διπλότυπων πακέτων. Μια τυπική 802.1X εφαρμογή έχει ως μέγιστο αριθμό αναμεταδόσεων από τρεις έως πέντε.

3.5.3 ΠεδίοEAP Length

Το EAPLengthπεδίο έχει μέγεθος 2 bytesκαι προσδιορίζει τον αριθμό των bytesπου περιλαμβάνει το EAP πακέτο. Η τιμή στο EAPLength πεδίο συμπεριλαμβάνει τα πεδία Code, Identifier, Lengthκαι Data, πεδία τα οποία αποτελούν ολόκληρο το EAPπακέτο. Επίσης η τιμή του EAPLengthπεδίου είναι ίδια με την τιμή του EAPOLLengthπεδίου. Για παράδειγμα η τιμή “0000 0100 1001 1110” για ένα EAPLengthπεδίο μας δείχνει ότι το EAPπακέτο είναι συνολικού μεγέθους 1182 bytes. Σε αυτή την περίπτωση το EAPDataπεδίο περιέχει 1178 bytesτα οποία είναι τα συνολικά 1182 bytes μείον 4 byteskεφαλίδας.Εάν μια οντότητα όπως ένας supplicantή μηχανισμός αυθεντικοποίησης λάβει ένα EAPπακέτο με το μέγεθος λήψης να είναι μικρότερο από την τιμή του πεδίου Length, τότε η εκάστοτε οντότητα θα πρέπει να απορρίψει το πακέτο. Για παράδειγμα ένα πακέτο EAPπου λήφθηκε έχει συνολικά 1179 bytes, θα απορριφθεί εάν το EAPLengthπεδίο ήταν 1182 bytes.

3.5.4 ΠεδίοEAPData

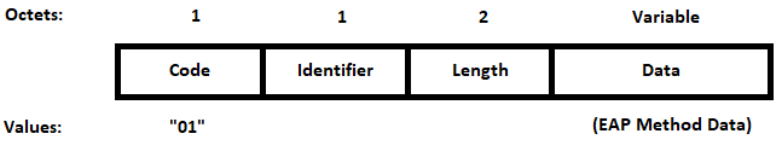
Το περιεχόμενο του Dataπεδίου ενός EAPπακέτου εξαρτάται από τον τύπο πακέτου. Για παράδειγμα, τα EAP-Requestπακέτα έχουν πεδία Data. Σε ορισμένες περιπτώσεις το EAPDataπεδίο μπορεί να μην περιέχει δεδομένα.

3.6 ΤύποιπακέτωνEAP

Οι επόμενες υποενότητες περιγράφουν κάθε έναν από τους τύπους πακέτων EAP.

3.6.1 EAP-Request

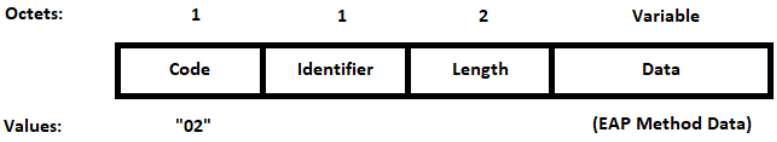
ΗΕικόνα 3.12 απεικονίζειέναEAP-Requestπακέτο. Ο μηχανισμός αυθεντικοποίησης επικοινωνεί με τον supplicant χρησιμοποιώντας EAP-Requestπακέτα για να παραδώσει EAP-Methodδεδομένα τα οποία ταξιδεύουν από τον serverαυθεντικοποίησης προς τον supplicant. Είτε ο supplicantμπορεί να στείλει ένα EAP-Requestπακέτο για να ζητήσει την ταυτότητα του μηχανισμού αυθεντικοποίησης για αμοιβαία αυθεντικοποίηση ανάλογα με την μέθοδο EAP-Methodπου είναι σε χρήση.



Εικόνα3.6

3.6.2 EAP-Response

Στην Εικόνα 3.13 απεικονίζεται ένα EAP-Responseπακέτο. Ο μηχανισμός αυθεντικοποίησης εκδίδει ένα EAP-Responseπακέτο για να επικοινωνεί με τον supplicant, όπως για παράδειγμα όταν αποστέλλονται δεδομένα μεθόδων EAP-Methodή στοιχεία εισόδου που έχουν ζητηθεί από τον supplicant να δώσει.



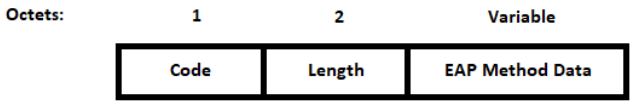
Εικόνα3.6

3.6.3 EAP-Request/Response Τύποι

Η EAPπροδιαγραφή καθορίζει ένα αρχικό σύνολο από EAPτύπους οι οποίοι καθορίζουν τη δομή των EAP-Requestκαι EAP-Responseπακέτων. Ο τύπος EAPελέγχει το τι μεταφέρει το EAPπακέτο. Ο Πίνακας 3.5 μας δείχνει τους βασισμένους σε πρότυπα EAPτύπους. Οι τύποι 1,2 και 3 είναι τύποι ειδικών περιπτώσεων, και οι υπόλοιποι τύποι είναι για ανταλλαγές αυθεντικοποίησης. Όλες οι EAPυλοποιήσεις θα πρέπει να υποστηρίζουν τους τύπους 1,2,3 και 4. Ο τύπος EAPφαίνεται στο πεδίο Codeενός EAP-Methodπακέτου ως μια τιμήμε μέγεθος ενός byte (Εικόνα 3.14). Σε επόμενο κεφάλαιο θα αναλύσουμε πιο λεπτομερώς αυτούς τους τύπους EAPκαθώς και άλλους οι οποίοι αναπτύχθηκαν μετά την επικυροποίηση των 802.1X καιEAPπροτύπων.

Πίνακας3.6

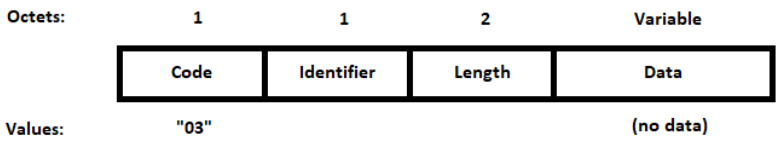
VALUE (DECIMAL AND BINARY)	EAP TYPE
1 (0000 0001)	Identity
2 (0000 0010)	Notification
3 (0000 0011)	NAK
4 (0000 0100)	MD5-Challenge
5 (0000 0101)	One-Time Password (OTP)
6 (0000 0110)	Generic Token Card (GTC)
254 (1111 1110)	Expanded Types
255 (1111 1111)	Experimental Use



Εικόνα3.6

3.6.4 EAP-Success

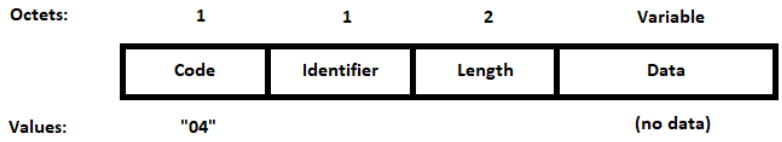
Με βάσει το αποτέλεσμα των EAP-Methodδιαδικασιών, ο μηχανισμός αυθεντικοποίησης αποστέλλει ένα EAP-Successπακέτο προς τον supplicantεάν ο serverαυθεντικοποίησης πληροφορήσει τον μηχανισμό αυθεντικοποίησης πως ο supplicantμπορεί να έχει πρόσβαση στο προστατευόμενο δίκτυο. Η Εικόνα 3.15 μας δείχνει ένα EAP-Successπακέτο. Το πακέτο αυτό δεν διαθέτει EAPDataπεδίο.



Εικόνα3.6

3.6.5 EAP-Failure

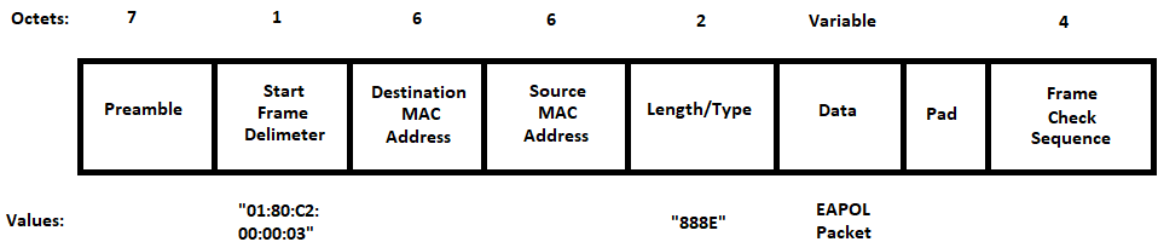
Ο μηχανισμός αυθεντικοποίησης στέλνει πακέτο EAP-Failureπρος τον supplicantεάν το αποτέλεσμα της διαδικασίας υποδείξει πως στον supplicantδεν επιτρέπεται η πρόσβαση στο προστατευμένο δίκτυο. Η Εικόνα 3.16 απεικονίζει ένα EAP-Failureπακέτο. Το πακέτο αυτό δεν διαθέτει EAP-Dataπεδίο.



Εικόνα3.6

3.7 Δομήπλαισίων 802.3

Το IEEE 802.3 (Ethernet) πρότυπο ορίζει ένα ενσύρματο τοπικό δίκτυο (LAN). Εάν οι χρήστες είναι σταθεροί, το 802.3 κατά πάσα πιθανότητα θα παρέχει PhysicalLayerκαι DataLinkLayerσυνδεσιμότητα ανάμεσα σε supplicantsκαι μηχανισμό αυθεντικοποίησης. Σε αυτή την περίπτωση, οι υπολογιστές των χρηστών (supplicants)θα είναι εξοπλισμένες με Ethernetκάρτες δικτύου οι οποίες επικοινωνούν χρησιμοποιώντας το 802.3 πρωτόκολλο με κάποιο Ethernetswitch (μηχανισμός αυθεντικοποίησης). Ένα σημαντικό πλεονέκτημα του Ethernetείναι πως προσφέρει πολύ αξιόπιστη σύνδεση ανάμεσα σε supplicantκαι μηχανισμό αυθεντκοποίησης. Το Dataπεδίο μέσα στο 802.3 Dataπλαίσιο όπως φαίνεται και στην Εικόνα 3.17, μεταφέρει τα EAPOL/EAPπακέτα. Ο Πίνακας 3.6 περιγράφει κάθε ένα από τα πεδία του 802.3 Data πλαισίου.



Εικόνα3.7

Πίνακας3.7

FIELD	SIZE	VALUE
Preamble	7 Bytes	Used by the receiving station to synchronize on the incoming data
Start Frame Delimiter	1 Byte	A value of "1010 1011", which indicates the start of the frame
Destination MAC Address	6 Bytes	For 802.1X, the value is always 01:80:C2:00:00:03 (hex format).
Source MAC Address	6 Bytes	MAC address of the sending station
Length/Type	2 Bytes	For 802.1X frames, this value is 888e (hex format) and indicates the nature of the protocol (i.e., Data field contains an EAPOL/EAP packet).
Data	Variable packets	Encapsulated EAPOL/EAP and EAP-Method
Pad	Variable	Variable number of bytes based on 802.3 specifications
Frame Check Sequence	4 Bytes	Value generated prior to transmitting the frame for the destination station to determine whether errors occurred during transmission over the medium

Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, το 802.1X χρησιμοποιεί την MACδιευθυνσιοδότηση η οποία υπάρχει στο 802.1DSpanning-Treeπρωτόκολλο. Στο 802.1X έχει ανατεθεί μια από τις αχρησιμοποίητες 802.1Dομάδα διευθύνσεων η οποία είναι η 01:80:C2:00:00:03. Όλες οι 802-basedσυσκευές λαμβάνουν και επεξεργάζονται πλαίσια τα οποία έχουν αυτή την ομάδα διευθύνσεων.

Πριν την αποστολή ενός 802.3 πλαισίου, ένας σταθμός ο οποίος θα μπορούσε να είναι μια κάρτα Ethernetστον supplicantή τον μηχανισμό αυθεντικοποίησης, πρέπει πρώτα να "ακούσει"το ενσύρματο μέσο(π.χ. το Ethernetκαλώδιο το οποίο ενώνει τον supplicantκαι τον μηχανισμό αυθεντικοποίησης) για να προσδιορίσει εάν κάποιος από τους σταθμούς εκπέμπει κάποιο

πλαίσιο. Τα πλαίσια μεταδίδονται στα Ethernetδίκτυα με τη χρήση ψηφιακών σημάτων, τα οποία είναι σε μορφή ηλεκτρικών παλμών τα οποία αναπαριστούν τα ψηφία 1 και 0 (δεδομένα σε δυαδική μορφή) στα πακέτα EAPOL, EAP καιEAP-Method. Όταν κανένας σταθμός δεν εκπέμπει πακέτα, τότε ο σταθμός που θέλει να στείλει δεδομένα μπορεί να κάνει εκπομπή πακέτων. Εάν κάποιος άλλος σταθμός ήδη εκπέμπει πακέτα, τότε όλοι οι υπόλοιποι σταθμοί που θέλουν να στείλουν πακέτα θα πρέπει να "κρατηθούν" και να μην προχωρήσουν σε εκπομπή. Το πρωτόκολλο το οποίο ευθύνεται για αυτή την διαδικασία είναι το carriersensemultipleaccess(CSMA) ή πιο απλά, πρωτόκολλο στο οποίο "ακούς προτού μιλήσεις". Το αποτέλεσμα που προκύπτει από την χρήση του ίδιου μέσου μπορεί να οδηγήσει σε καθυστερήσεις εάν υπάρχει πολύ αυξημένη κίνηση στο δίκτυο. Όμως το Ethernetείναι πολύ αποτελεσματικό και τέτοιου είδους καθυστερήσεις σπάνια έχουν αντίκτυπο στην λειτουργία του 802.1X σε σημαντικό επίπεδο.

3.8 Δομήπλαισίων 802.11

Το IEEE 802.11 (Wi-Fi) πρότυπο ορίζει ένα ασύρματο LANτο οποίο προσφέρει μια αποτελεσματική, χωρίς καλώδια διεπαφή ανάμεσα σε supplicantsκαι μηχανισμούς αυθεντικοποίησης. Ένα πλεονέκτημα του Wi-Fiείναι ότι προσφέρει κινητικότητα, παρόλα αυτά έχει ως αποτέλεσμα οι ασύρματες συνδέσεις μεταξύ supplicant και μηχανισμού αυθεντικοποίησης να είναι αναξιόπιστες ορισμένες φορές. Ηλεκτρομαγνητικές παρεμβολές από φούρνους μικροκυμάτων, ασύρματα τηλέφωνα και άλλα ασύρματα συστήματα μπορεί να παρέμβουν στην κανονική λειτουργία των Wi-Fiδικτύων. Η Εικόνα 3.18 απεικονίζει το Dataπεδίο μέσα στο 802.11 Dataπλαίσιο. Όπως και στο 802.3, τα 802.11 Dataπεδία μεταφέρουν τα EAPOL/EAPπακέτα μέσα στο FrameBodyπεδίο.

Octets:	2	2	6	6	6	2	6	Variable	4
	Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	Frame Check Sequence

Εικόνα3.8

Όμοια με το 802.3, τα 802.11 δίκτυα επίσης χρησιμοποιούν το CSMAγια έλεγχο πρόσβασης στο ασύρματο μέσο. Με τα ασύρματα δίκτυα παρόλα αυτά, ραδιοκύματα παρέχουν έναν μηχανισμό για ανταλλαγή δεδομένων. Τα ραδιοκύματα γενικά αναπαριστούν τα δυαδικά 1 και 0 των EAPOL,EAPκαι EAP-Methodπακέτων με τη χρήση διαφορετικών συχνοτήτων ή διαμορφώσεις φάσεων. Το αποτέλεσμα με τη χρήση ενός ασύρματου μέσου από πολλούς χρήστες μπορεί να οδηγήσει σε μεγαλύτερες καθυστερήσεις από εκείνες στο 802.3 διότι το 802.11 δεν είναι τόσο αποτελεσματικό.

Ο συνδυασμός της ηλεκτρομαγνητικής παρεμβολής (RFinterference) και η μειωμένη χωρητικότητα μπορεί μερικές φορές να έχει αντίκτυπο στη λειτουργία του 802.1X και των port-basedσυστημάτων αυθεντικοποίησης, εκτός εάν δοθεί ιδιαίτερη έμφαση στον σχεδιασμό του ασύρματου δικτύου. Για παράδειγμα, όσοι είναι υπεύθυνοι για την εγκατάσταση πρέπει να έχουν εξασφαλίσει πως υπάρχει επαρκής κάλυψη σήματος σε όλες τις περιοχές όπου οι χρήστες θα θέλουν να έχουν πρόσβαση στο δίκτυο. Επιπλέον, προληπτικά μέτρα θα πρέπει να ληφθούν υπ' όψιν όπως οι ρυθμίσεις των ηλεκτρομαγνητικών καναλιών (RFchannelsettings)έτσι ώστε να μειωθεί η έκθεση του συστήματος σε ηλεκτρομαγνητικές παρεμβολές (RFinterference).

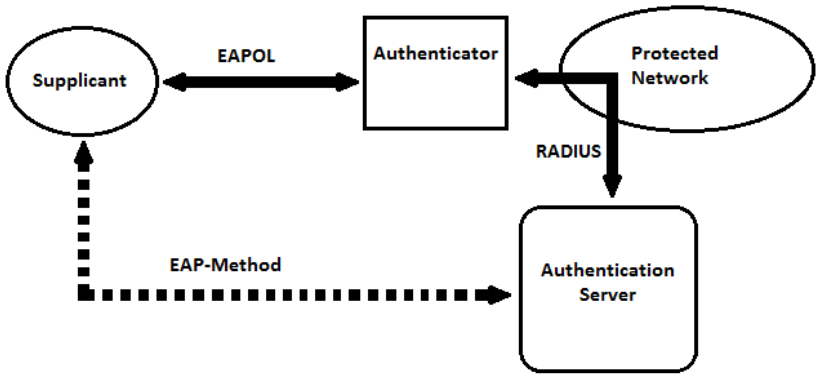
4 Πρωτόκολλα RADIUS

Σε αυτό το κεφάλαιο συνεχίζουμε την ανάλυση των 802.1X πρωτοκόλλων port-basedαυθεντικοποίησης η οποία ξεκίνησε στα κεφάλαια 2 και 3 και εστιάζουμε σε αυτό το σημείο πάνω στο RADIUS, ένα πρωτόκολλο το οποίο είναι το πιο σύνηθες πρωτόκολλο για serverαυθεντικοποίησης. Όπως θα δούμε, το RADIUSπρωτόκολλο είναι αρκετά απλό. Βέβαια υπάρχουν αρκετά στοιχεία σε αυτό τα οποία είναι χρήσιμο να γνωρίζουμε καθώς είναι κοινά σε 802.1Xσυστήματα. Στόχος του κεφαλαίου είναι να κατανοήσουμε καλύτερα το RADIUSκαι τις λειτουργίες του έτσι ώστε να αποκτήσουμε μια καλή βάση για να μπορούμε να παραμετροποιούμε και να αντιμετωπίζουμε προβλήματα σε συστήματα port-basedαυθεντικοποίησης.

4.1 Το RADIUS με λίγα λόγια

Όπως είδαμε και στο 2^{ο} κεφάλαιο, το RADIUSαποτελεί τον βασικό μηχανισμό επικοινωνίας ανάμεσα σε μηχανισμό αυθεντικοποίησης και serverαυθεντικοποίησης μέσα σε ένα port-basedσύστημα αυθεντικοποίησης (βλέπε Εικόνα 4.1). Ορισμένες φορές ο serverαυθεντικοποίησης ο οποίος εφαρμόζει το RADIUSσυνήθως αποκαλείται ως "RADIUSserver". Το RADIUSπρωτόκολλο ανάμεσα στον μηχανισμό αυθεντικοποίησης και τον serverαυθεντικοποίησης μεταφέρει τα EAP-Methodδεδομένα σε κρυπτογραφημένη μορφή. Το

802.1X πρότυπο και οι EAPπροδιαγραφές, δεν απαιτούν απαραίτητα το RADIUSως serverαυθεντικοποίησης, παρόλα αυτά το RADIUSείναι το πιο κοινώς χρησιμοποιούμενο πρωτόκολλο. Στην προκειμένη όμως περίπτωση, σε αυτή την πτυχιακή εργασία θα γίνει χρήση του RADIUS πάνω σε ένα σύστημα port-basedαυθεντικοποίησης.

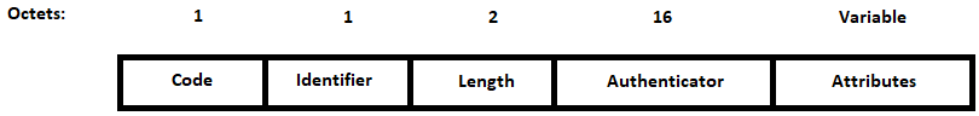


Εικόνα4.1

Ο serverαυθεντικοποίησης πραγματοποιεί μια "συνομιλία" προς δυο κατευθύνσεις, μια με τον μηχανισμό αυθεντικοποίησης μέσω RADIUSπρωτοκόλλων και μια με τον supplicantμέσω των μεθόδων EAP-Methods. Η χρήση των RADIUSπρωτοκόλλων είναι κατά κάποιο τρόπο μια φυσιολογική διαδικασία, ενώ η επικοινωνία μέσω των μεθόθων EAP-Methodsείναι σε λογικό επίπεδο. Τα πρωτόκολλα RADIUSπραγματοποιούν την φυσική "μεταφορά" των μεθόδων EAP-Methods ανάμεσα σε μηχανισμό αυθεντικοποίησης και serverαυθεντικοποίησης. Οι μέθοδοι EAP-Methodsαπό την άλλη κάνουν πιο "έξυπνη" την επικοινωνία. Όπως είδαμε και στο 2^{ο} Κεφάλαιο το μεγαλύτερο μέρος της επικοινωνίας ανάμεσα σε μηχανισμό αυθεντικοποίησης και serverαυθεντικοποίησης περιέχουν RADIUSAccess-Requestκαι Access-Challengeπακέτα. Ο μηχανισμός αυθεντικοποίησης στέλνει δεδομένα EAP-Methodπρος τον serverαυθεντικοποίησης μέσω RADIUSAccess-Request πλαισίων και ο serverαυθεντικοποίησης στέλνει EAP-Methodδεδομένα προς τον μηχανισμό αυθεντικοποίησης μέσω Access-Challengeπακέτων.

4.2 Δομή πακέτων RADIUS

Όλα τα RADIUSπακέτα έχουν την ίδια βασική δομή, αυτή περιέχει τα πεδία Code, Identifier, Length, Authenticatorκαι Attributes (βλέπε Εικόνα 4.2). Το πακέτο EAP-Methodβρίσκεται στο Dataπεδίο ενός EAPπακέτου. Στις παρακάτω υποενότητες γίνεται ανάλυση των πεδίων ενός EAP-Methodπακέτου.



Εικόνα4.2

4.2.1 Πεδίο Code

Το RADIUSCodeπεδίο έχει μέγεθος 1 bytekαι καθορίζει τον τύπο του RADIUSπακέτου. Ο Πίνακας 4.1 μας δείχνει τις τιμές του πεδίου Codekαι τους σχετικούς τύπους πακέτων. Για παράδειγμα εάν το πεδίο Codeέχει την τιμή "1", τότε το πακέτο είναι τύπου RADIUSAccess-Request.

Πίνακας4.2

CODE	PACKET TYPE
1	RADIUS Access-Request
2	RADIUS Access-Accept
3	RADIUS Access-Reject
4	RADIUS Accounting-Request
5	RADIUS Accounting-Response
11	RADIUS Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

4.2.2 Πεδίο Identifier

ToRADIUSIdentifierπεδίοέχειμέγεθος 1byte. Όμοια με το αντίστοιχο σε όνομα πεδίο στο EAPπρωτόκολλο, το πεδίο Identifierενός RADIUSπακέτου δίνει τη δυνατότητα να γίνει αντιστοίχιση των RADIUSAccess-Challengeπακέτων με Access-Requestπακέτα. Το πεδίο

Identifierσε ένα RADIUSAccess-Requestπακέτο το οποίο αποστέλλεται από τον μηχανισμό αυθεντικοποίησης, για παράδειγμα μπορεί να περιέχει την τιμή “0000 1101”. Ο serverαυθεντικοποίησης θα απαντήσει με ένα RADIUSAccess-Challengeπακέτο με το πεδίο Identifierνα έχει τιμή “0000 1101”. Επίσης, ο μηχανισμός αυθεντικοποίησης θα χρησιμοποιήσει την ίδια τιμή στο πεδίο Identifiereάν κάνει αναμετάδοση του ίδιου σχετικού RADIUSAccess-Requestπακέτου.

Για παράδειγμα, ένας μηχανισμός αυθεντικοποίησης μπορεί αρχικά να στείλει ένα RADIUSAccess-Requestπακέτο προς τον serverαυθεντικοποίησης με το Identifierπεδίο να έχει οριστεί στην τιμή “0001 1100”. Εάν δεν υπάρξει απάντηση από τον server, τότε ο μηχανισμός αυθεντικοποίησης θα αναμεταδόσει το πακέτο RADIUSAccess-Requestμε την τιμή του Identifierπεδίου ορισμένη σε “0001 1100”. Αυτό μας εξασφαλίζει πως ο serverαυθεντικοποίησης γνωρίζει πότε ένα πακέτο αποτελεί αναμετάδοση και έτσι αποφεύγεται η επεξεργασία διπλότυπων πακέτων.

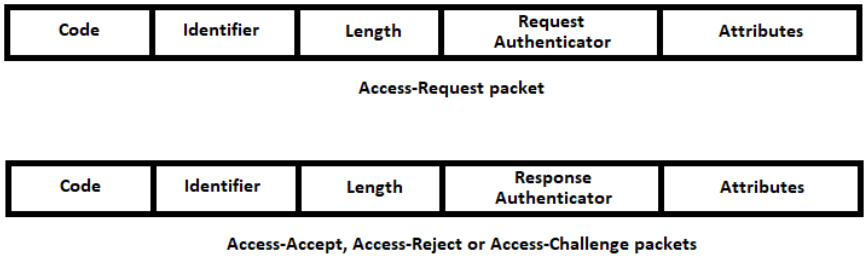
4.2.3 Πεδίο Length

Το RADIUSLengthπεδίο έχει μέγεθος 2 bytes και μας υποδεικνύει τον αριθμό των bytesτα οποία αποτελούν το RADIUSπακέτο. Το μέγιστο μέγεθος των RADIUSπακέτων είναι 4.096 bytes. ΗτιμήτουRADIUSLengthπεδίουπεριλαμβάνειταπεδίαEAPCode, Identifier, Length, Authenticator, καιAttributes. Για παράδειγμα, μια τιμή για το πεδίο RADIUSLength “0000 0100 1001 1110” υποδεικνύει πως το EAPπακέτο περιέχει 1.182 συνολικά bytes.Σε αυτή την περίπτωση το RADIUSAttributesπεδίο το οποίο έχει μεταβλητό μέγεθος, περιέχει 1.162 bytesμε δεδομένα, που είναι τα 1.182 συνολικά bytesμείον 20 byteskεφαλίδας. Όπως και με τα EAPπακέτα, εάν μια οντότητα όπως ένας μηχανισμός αυθεντικοποίησης ή ένας serverαυθεντικοποίησης λάβει ένα RADIUSπακέτο το οποίο έχει πραγματικό μέγεθος λήψης μικρότερο από την τιμή του πεδίου Length, τότε η οντότητα αυτή θα πρέπει να απορρίψει το πακέτο αυτό.

Για παράδειγμα ένα RADIUSπακέτο το οποίο έχει ληφθεί και έχει συνολικό μέγεθος 1.179 bytes θα απορριφθεί εάν το πεδίο EAPLengtheίχε 1.182 bytes. Εάν το πακέτο RADIUSπου έχει ληφθεί έχει μέγεθος το οποίο είναι μεγαλύτερο από εκείνο που έχει εντοπιστεί στο Lengthπεδίο, τότε η οντότητα που λαμβάνει το πακέτο θα πρέπει να απορρίψει τα επιπλέον bytes. Για παράδειγμα ένας serverαυθεντικοποίησης ο οποίος λαμβάνει ένα RADIUSπακέτο με συνολικό μέγεθος 1.029 byteskαι το Lengthπεδίο να υποδεικνύει ένα πακέτο μεγέθους 1.022 bytes, θα γίνει η επεξεργασία του πακέτου αλλά τα 7 τελευταία bytestου πακέτου θα απορριφθούν.

4.2.4 Πεδίο Authenticator

Το πεδίο Authenticatorέχει μέγεθος 16 bytesκαι περιέχει μια τιμή η οποία σχετίζεται με τον τύπο του RADIUSπακέτου που αποστέλλεται. Η Εικόνα 4.3 απεικονίζει το περιεχόμενο του Authenticatorπεδίου για διάφορους τύπους πακέτων.



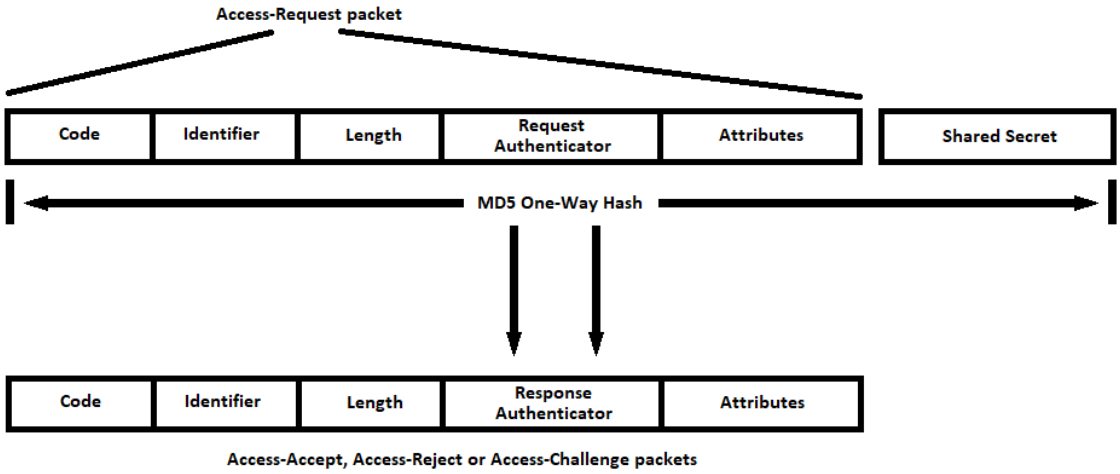
Εικόνα4.2

4.2.4.1 Request Authenticator

ΣταRADIUSAccess-Requestπακέτα, τοπεριεχόμενοτουπεδίουAuthenticatorείναιτοRequest Authenticator. Η τιμή αυτή είναι ένας τυχαίος αριθμός και θα πρέπει να είναι μοναδικός και μη προβλέψιμος. Το sharedsecretπου έχει παραμετροποιηθεί στον μηχανισμό αυθεντικοποίησης και τον serverαυθεντικοποίησης έχει συνδυαστεί με το RequestAuthenticatorκαι έχει περαστεί μέσα από ένα μονόδρομο MD5 hashγια να δημιουργήσει την digest τιμή (μεγέθους 16 bytes) η οποία γίνεται XORedμαζί με τον κωδικό του χρήστη. Το RADIUSAccess-Requestπακέτο μεταφέρει το αποτέλεσμα αυτό μέσα στην User-Password ιδιότητα. Η τιμή του RequestAuthenticatorαλλάζει κάθε φορά που αλλάζει και η τιμή του πεδίου Identifier.

4.2.4.2 Response Authenticator

ToResponse Authenticator βρίσκεταιστοAuthenticator πεδίοτωνRADIUS Access-Accept, Access-Reject καιAccess-Challenge πακέτων. Το ResponseAuthenticatorείναι ένα μονόδρομο MD5 hashτο οποίο υπολογίζεται πάνω από το συνολικό μέγεθος του σχετικού RADIUSAccess-Requestπακέτου και του sharedsecret. Στην Εικόνα 4.4 βλέπουμε τον τρόπο λειτουργίας.



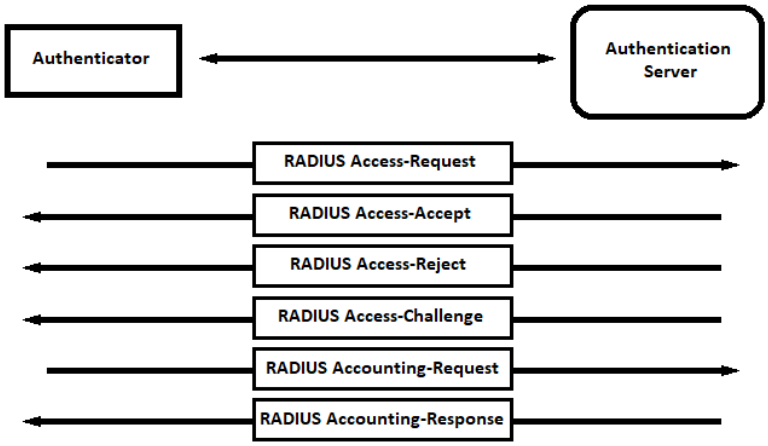
Εικόνα4.2

4.2.5 Πεδίο Attributes

Το Attributesπεδίο ενός RADIUSπακέτου είναι μεταβαλλόμενο σε μέγεθος και περιέχει συγκεκριμένα στοιχεία δεδομένων τα οποία επικοινωνούν με τον μηχανισμό αυθεντικοποίησης και τον serverαυθεντικοποίησης. Η ενότητα "RADIUSAttributes" αναλύει πολλά από τα κοινά στοιχεία που χρησιμοποιεί το RADIUS.

4.3 Τύποι πακέτων RADIUS

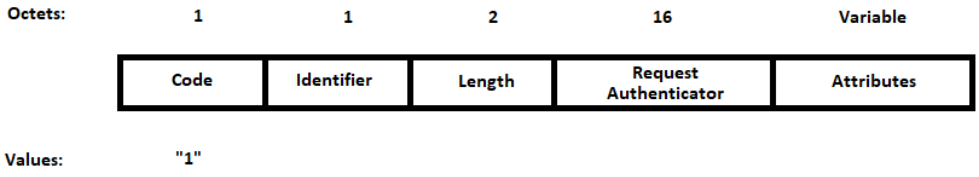
Η Εικόνα 4.5 απεικονίζει την επικοινωνία ανάμεσα σε μηχανισμό αυθεντικοποίησης και τον serverαυθεντικοποίησης με τη χρήση του RADIUS. Όμοια με το EAP, τα RADIUSπλαίσια αποστέλλονται μέσα από μια lock-stepδιαδικασία.



Εικόνα4.3

4.3.1 RADIUS Access-Request

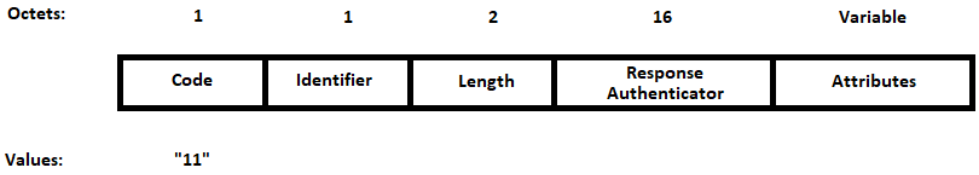
Στην Εικόνα 4.6 βλέπουμε ένα RADIUSAccess-Requestπακέτο το οποίο αποστέλλεται από τον μηχανισμό αυθεντικοποίησης προς τον RADIUSserver για να μεταφέρει δεδομένα σχετικά με την μέθοδο EAP-Methodπου χρησιμοποιείται. Για παράδειγμα το Access-Requestπακέτο θα μπορούσε να περιλαμβάνει τα στοιχεία πρόσβασης του supplicant. Όλες οι υλοποιήσεις ταυτοποίησης χρηστών πρέπει να εκδίδουν ένα Access-Requestπακέτο κατά τη διάρκεια αυθεντικοποίησης του supplicant. Το Access-Requestγενικά περιέχει την User-Nameιδιότητα και την NAS-IP-Addressιδιότητα (ή διαφορετικά NAS-Identifierιδιότητα). Όταν περιέχεται η User-Passwordιδιότητα, το passwordείναι κρυφό με τη χρήση μιας μεθόδου βασισμένη στο RSAMD5.



Εικόνα4.3

4.3.2 RADIUS Access-Challenge

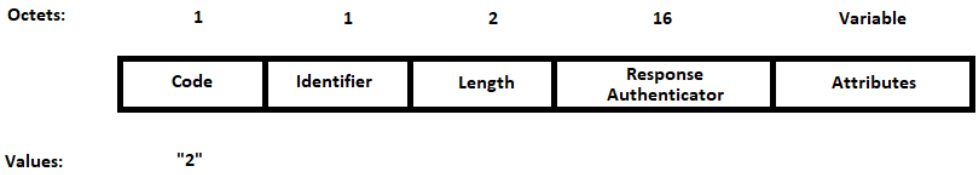
Στην Εικόνα 4.7 απεικονίζεται ένα RADIUSAccess-Challengeπακέτο το οποίο αποστέλλεται από τον RADIUSserverπρος τον μηχανισμό αυθεντικοποίησης ως απάντηση σε ένα RADIUSAccess-Requestπακέτο. Η τιμή του πεδίου Identifier του Access-Challengeθα πρέπει να ταιριάζει με την τιμή του πεδίου Identifierστο σχετικό Access-Requestπακέτο. Το πεδίο Attributesενός Access-Challengeπακέτου μπορεί να περιέχει μια ή περισσότερες από τις παρακάτω ιδιότητες: State, Reply-Message, Vendor-Specific, Idle-Timeout, Session-Timeoutκαι Proxy-State.



Εικόνα4.3

4.3.3 RADIUS Access-Accept

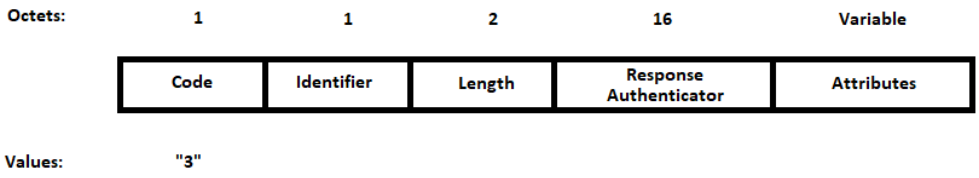
Η Εικόνα 4.8 μας δείχνει ένα RADIUSAccess-Acceptπακέτο το οποίο αποστέλλεται από τον RADIUSserverπρος τον μηχανισμό αυθεντικοποίησης ως απάντηση προς κάποιο RADIUSAccess-Request. Για παράδειγμα το Access-Acceptπακέτο μπορεί να περιέχει πληροφορίες σχετικές με την αποδοχή του χρήστη ή πληροφορίες ρυθμίσεων για τον εκάστοτε χρήστη. Η τιμή του πεδίου Identifierστο Access-Acceptπακέτο θα πρέπει να ταιριάζουν με την τιμή του πεδίου Identifierστο αντίστοιχο σχετικό Access-Requestπακέτο. Το πεδίο Attributesενός Access-Acceptπακέτου μπορεί να έχει ένα ή περισσότερα κοινά στοιχεία με εκείνα που εντοπίζονται στο RADIUSAccess-Challengeπακέτο.



Εικόνα4.3

4.3.4 RADIUS Access-Reject

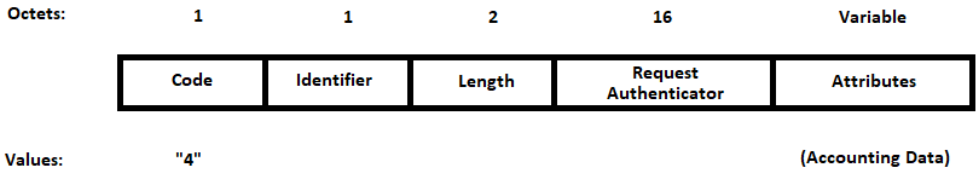
Στην Εικόνα 4.9 βλέπουμε ένα RADIUSAccess-Rejectπακέτο το οποίο αποστέλλεται από τον RADIUSserverπρος τον μηχανισμό αυθεντικοποίησης ως απάντηση σε κάποιο RADIUSAccess-Request. Το Access-Rejectπακέτο αποστέλλεται όταν οποιαδήποτε από τις ιδιότητες μέσα στο Access-Requestπακέτο κριθεί ως μη αποδεκτή. Η τιμή του πεδίου Identifier σε ένα Access-Acceptπακέτο πρέπει να ταιριάζει με την τιμή του πεδίου Identifierστο αντίστοιχο Access-Requestπακέτο. Το πεδίο Attributesσε ένα Access-Rejectπακέτο μπορεί να περιλαμβάνει ένα ή περισσότερα Reply-Messageστοιχεία σε μορφή μηνύματος, τα οποία στη συνέχεια μπορεί ο μηχανισμός αυθεντικοποίησης να εμφανίσει στον χρήστη.



Εικόνα4.3

4.3.5 RADIUS Accounting-Request

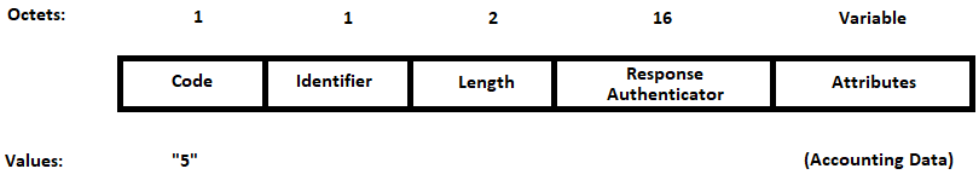
Στην Εικόνα 4.10 βλέπουμε ένα RADIUSAccounting-Requestπακέτο το οποίο αποστέλλεται από τον μηχανισμό αυθεντικοποίησης προς τον RADIUSserverμε σκοπό να λάβει πληροφορίες.



Εικόνα4.3

4.3.6 RADIUS Accounting-Response

Παρακάτω στην Εικόνα 4.11 , μπορούμε να δούμε ένα RADIUSAccounting-Responseπακέτο το οποίο αποστέλλεται από τον RADIUSserverπρος τον μηχανισμό αυθεντικοποίησης ως απάντηση στο RADIUSAccounting-Requestπακέτο. Στο Accounting-Responseπακέτο θα πρέπει η τιμή του Identifierπεδίου να ταιριάζει με εκείνη στο σχετικό Accounting-Requestπακέτο.



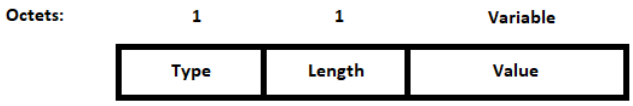
Εικόνα4.3

4.4 Ιδιότητες RADIUS

Οι RADIUSιδιότητες που περιέχονται μέσα σε ένα RADIUSπακέτο είναι στοιχεία από δεδομένα τα οποία μεταφέρονται ανάμεσα σε μηχανισμό αυθεντικοποίησης και RADIUSserver.

4.4.1 Μορφή ιδιοτήτων RADIUS

Κάθε ιδιότητα που περιέχεται στο πεδίο Attributesενός πακέτου RADIUSέχει τη μορφή που μας δείχνει η Εικόνα 4.12. Ορισμένα πακέτα RADIUSμεταφέρουν διάφορες ιδιότητες. Ως αποτέλεσμα, η μορφή που βλέπουμε στην Εικόνα 4.12 επαναλαμβάνεται μέσα στο πεδίο Attributesενός πακέτου RADIUS.



Εικόνα4.4

4.4.1.1 Πεδίο Type

Η τιμή του πεδίου Typeσε μια RADIUS ιδιότητα έχει μέγεθος 1 bytekαι απεικονίζει μια συγκεκριμένη ιδιότητα. Οι Typeτιμές 192-223 είναι για πειραματική χρήση, οι τιμές 224-240 είναι για εφαρμογές και συγκεκριμένη χρήση και οι τιμές 241-255 είναι δεσμευμένες και δεν θα πρέπει να χρησιμοποιούνται. Οι RADIUSserverséχουν σχεδιαστεί για να αγνοούν ιδιότητες με άγνωστη τιμή στο πεδίο Typetou RADIUSπακέτου. Το RFC 2865 ορίζει ένα αρχικό σετ από ιδιότητες οι οποίες φαίνονται στον Πίνακα 4.2.

Πίνακας4.4

ATTRIBUTE NUMBER	ATTRIBUTE NAME
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port

6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
9	Framed-IP-Netmask
10	Framed-Routing
11	Filter-Id
12	Framed-MTU
13	Framed-Compression
14	Login-IP-Host
15	Login-Service
16	Login-TCP-Port
17	(unassigned)
18	Reply-Message
19	Callback-Number
20	Callback-Id
21	(unassigned)
22	Framed-Route
23	Framed-IPX-Network
24	State
25	Class
26	Vendor-Specific
27	Session-Timeout
28	Idle-Timeout
29	Termination-Action
30	Called-Station-Id
31	Calling-Station-Id
32	NAS-Identifier
33	Proxy-State
34	Login-LAT-Service
35	Login-LAT-Node
36	Login-LAT-Group
37	Framed-AppleTalk-Link
38	Framed-AppleTalk-Network
39	Framed-AppleTalk-Zone
40-59	(reserved for accounting)
60	CHAP-Challenge
61	NAS-Port-Type
62	Port-Limit
63	Login-LAT-Port

4.4.1.2 Πεδίο Length

Το πεδίο Length σε μια ιδιότητα RADIUSέχει μέγεθος 1 byte και καθορίζει το μέγεθος της ιδιότητας αυτής. Το μέγεθος περιλαμβάνει τα πεδία Type, Length και Value. Εάν ο

RADIUSserverλάβει μια ιδιότητα σε ένα RADIUSAccess-Requestπακέτο με μη έγκυρο μέγεθος, τότε ο RADIUSserver θα απαντήσει με ένα RADIUSAccess-Rejectπακέτο. Εάν ο μηχανισμός αυθεντικοποίησης λάβει μια ιδιότητα σε ένα RADIUSAccess-Accept, Access-Rejectή Access-Challengeπακέτο με μη έγκυρο μέγεθος, τότε ο μηχανισμός αυθεντικοποίησης είτε θα θεωρήσει το πακέτο που έλαβε ως ένα Access-Rejectείτε απλά θα απορρίψει το πακέτο.

4.4.1.3 Πεδίο Value

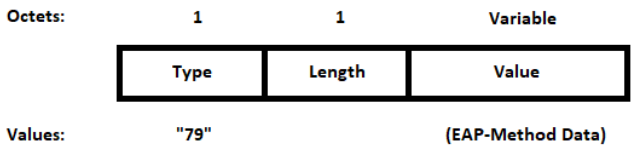
Το Valueπεδίο σε μια RADIUSιδιότητα έχει μεταβλητό μέγεθος σε bytesτο οποίο ξεκινά από την τιμή "0" και περιλαμβάνει σχετικά με την ιδιότητα δεδομένα. Το πεδίο Valueμπορεί να περιλαμβάνει τους παρακάτω τύπους δεδομένων:

- **Text:** 1-253 bytesτα οποία περιέχουν χαρακτήρες σε UTF-8 encoding. Εάν δεν αποστέλλεται κείμενο, τότε ολόκληρη η ιδιότητα απορρίπτεται από τους περισσότερους RADIUSservers και μηχανισμούς αυθεντικοποίησης.
- **String:** 1-253 bytesτα οποία περιέχουν δεδομένα σε δυαδική μορφή. Εάν δεν αποστέλλονται καθόλου δεδομένα, τότε ολόκληρη η ιδιότητα απορρίπτεται από τους περισσότερους RADIUSserversκαι μηχανισμούς αυθεντικοποίησης.
- **Address:**Μια τιμή μεγέθους 32-bit
- **Integer:**Μια άγνωστη τιμή μεγέθους 32-bit
- **Time:** Μια τιμή μεγέθους 32-bit μη καθορισμένη η οποία απεικονίζει τον αριθμό δευτερολέπτων από την ημερομηνία: 00:00:00 UTC, 1 Ιανουαρίου, 1970. Οι κλασσικές ιδιότητες δεν χρησιμοποιούν αυτόν τον τύπο δεδομένων, αλλά άλλοι τύποι ιδιοτήτων μπορεί να τον χρησιμοποιούν.

Οι παρακάτω ενότητες συνοψίζουν ορισμένες από τις κλασσικές RADIUSιδιότητες που χρησιμοποιούνται μαζί με συστήματα 802.1X port-basedαυθεντικοποίησης.

4.4.2 Ιδιότητα EAP-Message

HEAP-MessageRADIUSιδιότητα (πεδίοType = "79") σε ένα RADIUSπακέτο είναι η βασική ιδιότητα για το 802.1X καθώς ενθυλακώνει δεδομένα μεθόδων EAP-Methodανάμεσα σε μηχανισμό αυθεντικοποίησης και serverαυθεντικοποίησης (βλέπε Εικόνα 4.13). Οι μέθοδοι EAP-Methodsαποτελούν την επικοινωνία ανάμεσα σε supplicantκαι server αυθεντικοποίησης. Η ιδιότητα EAP-Messageστην ουσία περιέχει το πακέτο EAP-Method. Όλες οι άλλες RADIUSιδιότητες σε 802.1Xport-basedauthenticationυλοποιήσεις είναι περιφερειακές ως προς την EAP-Messageιδιότητα.



Εικόνα4.4

Οι EAP-Messageιδιότητες αποστέλλονται από τον μηχανισμό αυθεντικοποίησης προς τον RADIUSserverμέσα σε RADIUSAccess-Requestπακέτα. Οι EAP-Messageιδιότητα αποστέλλονται από τον RADIUSserverπρος τον μηχανισμό αυθεντικοποίησης μέσα σε RADIUSAccess-Challengeπακέτα. ΈναRADIUSAccess-RequestήAccess-Challengeπακέτομπορείναπεριέχει διάφορα EAPπακέτα. Σε αυτή την περίπτωση θα πρέπει να είναι ταξινομημένα σε συνεχή ροή από EAP-Messageιδιότητες. Τα RADIUSAccess-Acceptκαι Access-Rejectπακέτα συνήθως μεταφέρουν μόνο μια EAP-Messageιδιότητα. Για παράδειγμα, το Access-Acceptπακέτο θα περιέχει ένα EAP-Successπακέτο και το Access-Rejectπακέτο θα περιέχει ένα EAP-Failureπακέτο. Εάν ένας RADIUSserverλάβει ένα EAPπακέτο το οποίο δεν καταλαβαίνει, τότε λογικά θα απαντήσει με ένα RADIUSAccess-Rejectπακέτο.

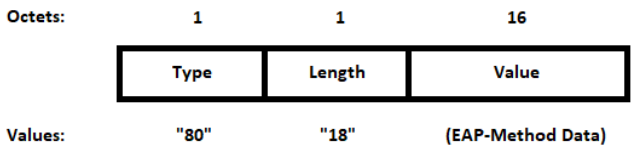
ΚαθώςυλοποιείταιηEAP-Messageιδιότητα, ηMessage-AuthenticatorιδιότηταπροστατεύειόλαταAccess-Request, Access-Challenge, Access-AcceptκαιAccess-Rejectπακέτα τα οποία περιέχουν δεδομένα μεθόδων EAP-Method. Στην πραγματικότητα, ένας RADIUSservero οποίος λαμβάνει ένα RADIUSAccess-Requestπακέτο και περιλαμβάνει μια EAP-Messageιδιότητα χωρίς να έχει ένα έγκυρο Message-Authenticator, ο serverμε τη σειρά του θα απορρίψει το πακέτο αυτό. Επιπρόσθετα, οι RADIUSserversπου δεν υποστηρίζουν την EAP-Messageιδιότητα επίσης θα απορρίψουν τα σχετικά RADIUSAccess-Requestπακέτα που περιέχουν EAP-Messageιδιότητες.

4.4.3 Ιδιότητα Message-Authenticator

Γενικά, ηRADIUSMessage-Authenticatorιδιότητα (πεδίοType= “80”) μπορεί να χρησιμοποιηθεί από τον RADIUSserverσε οποιοδήποτε RADIUSAccess-Request πακέτο για να πιστοποιήσει RADIUSAccess-Requests. Επιπλέον, η Message-Authenticatorιδιότητα μπορεί να ελέγχει την

ακεραιότητα των Access-Requestπακέτων για να αποτρέψει τυχόν πλαστογράφηση. ΌτανυποστηρίζονταιοιEAP-Messageιδιότητες, τότεόλαταAccess-Request, Access-Accept, Access-RejectκαιAccess-Challengeπακέταπρέπει να περιλαμβάνουν την Message-Authenticatorιδιότητα.

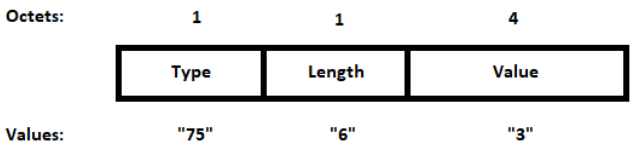
Η Εικόνα 4.14 απεικονίζει την μορφή της Message-Authenticatorιδιότητας. Το μέγεθος της ιδιότητας αυτής είναι πάντα 18 bytes. Για τα Access-Requestπακέτα, η τιμή της ιδιότητας Message-Authenticatorείναι ένα HMAC-MD5 hashαπό το Access-Requestπακέτο, με χρήση ενός sharedsecretως κλειδί.



Εικόνα4.4

4.4.4 Ιδιότητα Password-Retry

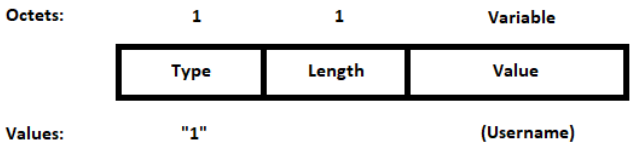
Η ιδιότητα Password-Retry (πεδίο Type= "75") μπορεί να συμπεριληφθεί σε ένα RADIUSAccess-Rejectπακέτο για να προσδιορίσει τον αριθμό των προσπαθειών αυθεντικοποίησης που μπορεί να πραγματοποιήσει ένας χρήστης προτού αποσυνδεθεί. Η Εικόνα 4.15 μας δείχνει την μορφή που έχει η Password-Retryιδιότητα. Η ιδιότητα αυτή έχει πάντα μέγεθος 6 bytes. Το πεδίο Valueέχει μέγεθος 4 byteskαι περιλαμβάνει έναν ακέραιο ο οποίος προσδιορίζει τον αριθμό των προσπαθειών εισαγωγής κωδικού πρόσβασης για έναν χρήστη. Στο παράδειγμα που φαίνεται στην Εικόνα 4.15, ο χρήστης έχει τρεις προσπάθειες για να ταυτοποιηθεί. Εάν και στην τρίτη προσπάθεια αποτύχει, τότε ο supplicantαποσυνδέεται από το δίκτυο.



Εικόνα4.4

4.4.5 Ιδιότητα User-Name

HUser-Nameιδιότητα (TypeField= “1”) αντιστοιχίζει το όνομα του χρήστη ο οποίος προσπαθεί να ταυτοποιηθεί και αποστέλλεται από τον μηχανισμό αυθεντικοποίησης προς τον RADIUSserver μέσα σε ένα RADIUSAccess-Acceptπακέτο. Το usernameέχει μέγεθος από ένα ή περισσότερα bytes. Η Εικόνα 4.16 μας δείχνει την μορφή μιας User-Nameιδιότητας.



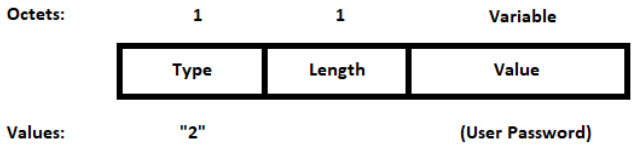
Εικόνα4.4

Το usernameγενικά έχει μια από τις παρακάτω μορφές:

- **Text:** UTF-8 encodedμε 10646 διαφορετικούς χαρακτήρες
- **Network access identifier:**Identifier οοποίοςέχειοριστεί στο RFC 2486
- **Distinguishedname:**ΟνομασεμορφήASN.1 που χρησιμοποιείται σε συστήματα PublicKeyauthentication

4.4.6 Ιδιότητα User-Password

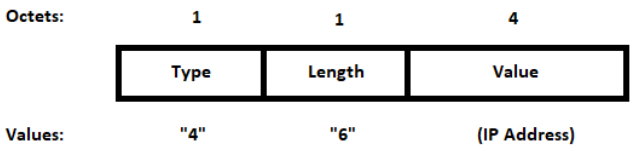
ΗιδιότηταUser-Password (TypeField= “2”) ορίζει τον κωδικό πρόσβασης ενός χρήστη κατά την διαδικασία της ταυτοποίησης και αποστέλλεται από τον μηχανισμό αυθεντικοποίησης προς τον RADIUSserverσε ένα RADIUSAccess-Requestπακέτο. Ο κωδικός πρόσβασης χρήστη έχει μέγεθος από ένα ή περισσότερα bytes. Η Εικόνα 4.17 απεικονίζει τη μορφή μιας User-Passwordιδιότητας. Ο κωδικός πρόσβασης είναι κρυμμένος πριν την μετάδοση μέσα στο Access-Requestπακέτο. Ένα μονόδρομο MD5 hashυπολογίζεται πάνω από ένα sharedsecret και ένα RequestAuthenticator. Το αποτέλεσμα του υπολογισμού στη συνέχεια γίνεται XORedμε τα πρώτα 16 bytestου passwordκαι τοποθετείται στην αρχή της User-Passwordιδιότητας του πεδίου Value.



Εικόνα4.4

4.4.7 Ιδιότητα NAS-IP-Address

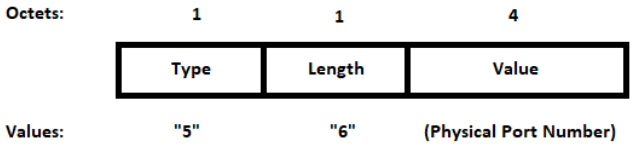
HNAS-IP-Addressιδιότητα (TypeField= “4”) υποδεικνύει την IPδιεύθυνση ενός μηχανισμού αυθεντικοποίησης ο οποίος ζητά να ταυτοποιήσει τον supplicant. Η ιδιότητα NAS-IP-Addressχρησιμοποιείται μόνο στα RADIUSAccess-Requestπακέτα. Είτε η NAS-IP-Addressιδιότητα είτε η NAS-Identifierιδιότητα θα πρέπει να βρίσκεται σε ένα Access-Requestπακέτο. Η Εικόνα 4.18 μας δείχνει το πως είναι η μορφή μιας NAS-IP-Addressιδιότητας. Η ιδιότητα αυτή έχει πάντα 8 bytesμέγεθος και 4 byteskατανέμονται στο πεδίο IPAddress.



Εικόνα4.4

4.4.8 Ιδιότητα NAS-Port

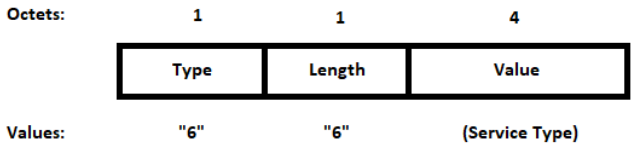
HNAS-Portιδιότητα (Typefield= “5”) περιλαμβάνει τον αριθμό από φυσικές πόρτες (όχι τις TCPή UDP)ενός μηχανισμού αυθεντικοποίησης ο οποίος ζητά να πιστοποιήσει τον supplicant. Η ιδιότητα NAS-Portχρησιμοποιείται μόνο σε RADIUSAccess-Requestπακέτα. Η Εικόνα 4.19 δείχνει τη μορφή μιας NAS-Portιδιότητας. Η ιδιότητα αυτή έχει πάντα 6 bytesμέγεθος και 4 byteskατανέμονται στο πεδίο PortNumber.



Εικόνα4.4

4.4.9 Ιδιότητα Service-Type

ΗιδιότηταService-Type (Typefield= “6”) αντιπροσωπεύει τον τύπο της υπηρεσίας που είτε ο supplicant ζητάει είτε ο RADIUSserverεγκρίνει. Η Service-Typeιδιότητα χρησιμοποιείται και στα Access-Requestπακέτα αλλά και στα Access-Acceptπακέτα. Στην Εικόνα 4.20 βλέπουμε τη μορφή μιας Service-Typeιδιότητας. Η ιδιότητα αυτή έχει πάντα μέγεθος 6 bytesκαι το πεδίο Valueέχει μέγεθος 4 bytes. Ο μηχανισμός αυθεντικοποίησης χειρίζεται όλους τους μη υποστηριζόμενους τύπους υπηρεσιών που παρέχονται από τον RADIUSserverως Access-Rejectπακέτα.



Εικόνα4.4

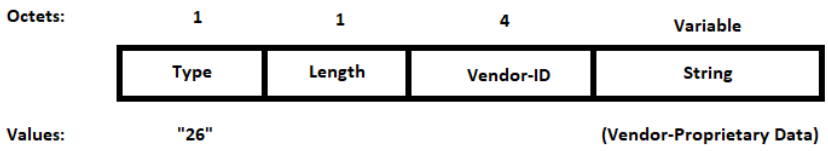
Το πεδίο Valueμιας Service-Type ιδιότητας μπορεί να είναι μια από τις παρακάτω που βρίσκονται στον Πίνακα 4.3.

Πίνακας4.4

VALUE	SERVICE
1	Login
2	Framed
3	Callback Login
4	Callback Framed
5	Outbound
6	Administrative
7	NAS Prompt
8	Authenticate Only
9	Callback NAS Prompt
10	Call Check
11	Callback Administrative

4.4.10 Ιδιότητα Vendor-Specific

HRADIUSVendor-Specificιδιότητα (Typefield= “26”) επιτρέπει σε προμηθευτές να υλοποιήσουν ιδιόκτητες ιδιότητες οι οποίες δεν είναι κατάλληλες για γενική χρήση. Η ένταξη επιπλέον ιδιοτήτων παρόλα αυτά δεν παρεμβάλλει στην λειτουργία του RADIUSπρωτοκόλλου. Εάν ένας RADIUSserver λάβει ένα RADIUSπακέτο το οποίο περιέχει κάποια Vendor-Specificιδιότητα την οποία δεν καταλαβαίνει, τότε ο RADIUSserverθα απορρίψει την ιδιότητα και πιθανότατα θα στείλει ένα μήνυμα στον μηχανισμό αυθεντικοποίησης. Η Εικόνα 4.21 μας δείχνει τη μορφή μιας Vendor-Specificιδιότητας.



Εικόνα4.4

4.4.10.1 Πεδίο Vendor-ID

ToVendor-IDπεδίομιαςVendor-Specificιδιότητας έχει μέγεθος 4 bytes. Τα high-orderbytesαποτελούνται από μόνο μηδενικά και τα low-order3bytesπεριέχουν τον SMINetworkManagementPrivateEnterpriseCodetου προμηθευτή.

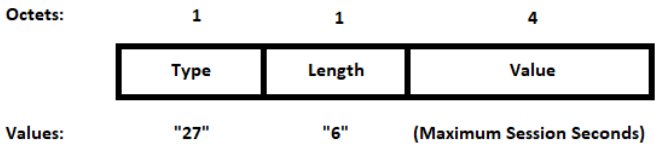
4.4.10.2 Πεδίο String

ToStringπεδίομιαςVendor-Specificιδιότητας έχει μέγεθος από ένα ή περισσότερα bytes.

4.4.11 Ιδιότητα Session-Timeout

HRADIUSSession-Timeoutιδιότητα (Typefield= “27”) καθορίζει τον μέγιστο χρόνο σε δευτερόλεπτα στον οποίο ο supplicantθα εξυπηρετηθεί. Η ιδιότητα αυτή αποστέλλεται μόνο από τον RADIUSserverπρος τον μηχανισμό αυθεντικοποίησης μέσα σε RADIUSAccess-Acceptή Access-Challengeπακέτα. Η Εικόνα 4.22 μας δείχνει τη δομή μιας Session-Timeout ιδιότητας. Το μέγεθος της ιδιότητας αυτής είναι πάντα 6 bytes. Το πεδίο Valueέχει 4 bytesκαι περιέχει έναν

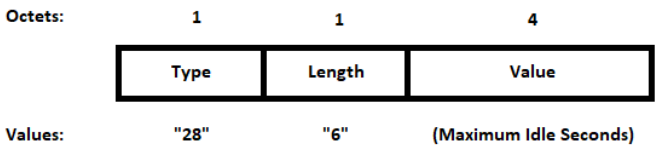
32-bitάγνωστο ακέραιο αριθμό ο οποίος αντιπροσωπεύει τον μέγιστο αριθμό δευτερολέπτων που ο χρήστης μπορεί να εξυπηρετηθεί.



Εικόνα4.4

4.4.12 Ιδιότητα Idle-Timeout

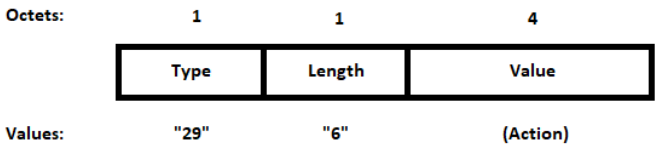
ΗιδιότηταIdle-Timeout (Typefield= “28”) ορίζει τον μέγιστο αριθμό δευτερολέπτων όπου ο supplicantμπορεί να είναι σε κατάσταση idleπροτού αποσυνδεθεί από το δίκτυο. Η ιδιότητα αυτή αποστέλλεται μόνο από τον RADIUSserverπρος τον μηχανισμό αυθεντικοποίησης μέσα σε RADIUSAccess-Acceptή Access-Challengeπακέτα. Η Εικόνα 4.23 απεικονίζει τη μορφή της ιδιότητας Idle-Timeout. Το μέγεθος της ιδιότητας Idle-Timeoutείναι πάντα 6 bytes. Το Valueπεδίο έχει 4 bytesκαι περιέχει έναν 32-bitάγνωστο ακέραιο αριθμό που αντιπροσωπεύει τον μέγιστο αριθμό δευτερολέπτων που ο συγκεκριμένος χρήστης μπορεί να είναι σε idleκατάσταση.



Εικόνα4.4

4.4.13 Ιδιότητα Termination-Action

HRADIUSTermination-Actionιδιότητα (Type-field= “29”) καθορίζειποια ενέργεια θα πρέπει να λάβει ο μηχανισμός αυθεντικοποίησης όταν μια συγκεκριμένη λειτουργία ολοκληρώνεται. Η ιδιότητα Termination-Actionχρησιμοποιείται μόνο στα Access-Acceptπακέτα. Στην Εικόνα 4.24 βλέπουμε τη δομή της ιδιότητας Termination-Action. Το πεδίο Valueέχει 4 bytesμέγεθος και μπορεί να είναι είτε “0” για Defaultείτε “1” για RadiusRequest. Εάν το πεδίο Valueείναι “RadiusRequest”, τότε ο μηχανισμός αυθεντικοποίησης μπορεί να αποστείλει ένα νέο Access-Requestπρος τον RADIUSserver αφού τερματιστεί η υπηρεσία.



Εικόνα4.4

4.5 Σκέψεις για την σωστήεπιλογή AuthenticationServer

Κατά την υλοποίηση συστημάτων 802.1Xport-basedauthentication, πρέπει να γίνει επιλογή ενός συγκεκριμένου serverαυθεντικοποίησης. Σχεδόν σε κάθε περίπτωση, το RADIUSπιθανότατα θα ικανοποιήσει όλες τις απαιτήσεις για ταυτοποίηση.

4.5.1 Attributes

Κατά την επιλογή του RADIUSserver, θα πρέπει σίγουρα να σκεφτούμε το ποιες RADIUSιδιότητες πρέπει να υποστηρίξουμε. Για παράδειγμα εάν ο μηχανισμός αυθεντικοποίησης μπορεί να κάνει χρήση των ιδιόκτητων λειτουργιών, τότε είναι πιθανό να χρειάζεται ο RADIUSserverνα υποστηρίζει τις ιδιόκτητες Vendor-Specificιδιότητες. Προφανώς, ο RADIUSserverθα πρέπει να υποστηρίζει την EAP-Messageιδιότητα ώστε να δουλεύει γενικότερα μαζί με μεθόδους EAP-Methods, βέβαια σχεδόν όλοι οι RADIUSserversσυμπεριλαμβάνουν την EAP-Messageιδιότητα.

4.5.2 EAP-Methods

Ο RADIUSserverπου επιλέγουμε, θα πρέπει επίσης να υποστηρίζει τις μεθόδους EAP-Methodsπου σκοπεύουμε να χρησιμοποιήσουμε. Πολλές από τις καθιερωμένες μεθόδους είναι ενσωματωμένες σε όλους τους RADIUSservers, παρόλα αυτά θα ήταν καλό να προσέξουμε εάν πρόκειται να χρησιμοποιήσουμε μια λιγότερο δημοφιλή μέθοδο EAP-Method.

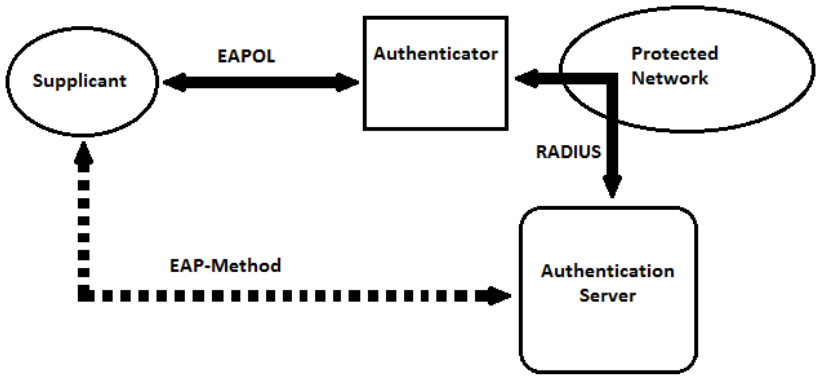
5 Πρωτόκολλο EAP-Methods

Σε αυτό το κεφάλαιο ολοκληρώνουμε την θεωρητική μελέτη των πρωτοκόλλων port-basedαυθεντικοποίησης με το να εξετάσουμε με μεγαλύτερη λεπτομέρεια των τύπων μεθόδωνEAP (ExtensibleAuthenticationProtocol) Method και δομών πακέτων. Τα πρωτόκολλα των EAP-Methodsείναι εκείνα που πραγματοποιούν τις διαδικασίες αυθεντικοποίησης, και υπάρχουν αρκετές επιλογές. Το παρών κεφάλαιο θα δώσει μια καλύτερη εικόνα για το ποια μέθοδος EAP-Methodείναι βέλτιστη ανά υλοποίηση.

5.1 Ανακεφαλαίωση μεθόδων EAP-Methods

Οι μέθοδοι EAP-Methodsείναι ο βασικός μηχανισμός για την end-to-endεπικοινωνία σε λογικό επίπεδο ανάμεσα σε έναν χρήστη και serverαυθεντικοποίησης μέσα σε ένα σύστημα port-basedαυθεντικοποίησης (βλέπε Εικόνα 5.1). Μερικές φορές μια EAP-Methodαποκαλείται και “EAPAuthentiationtype” ή πιο σύντομα “EAPtype”. Μια EAP-Methodστην ουσία υλοποιεί την

διαδικασία ελέγχου ταυτότητας, ενώ άλλα πρωτόκολλα όπως το EAPOLκαι το RADIUS απλώς μεταφέρουν τα EAP-Methodδεδομένα.

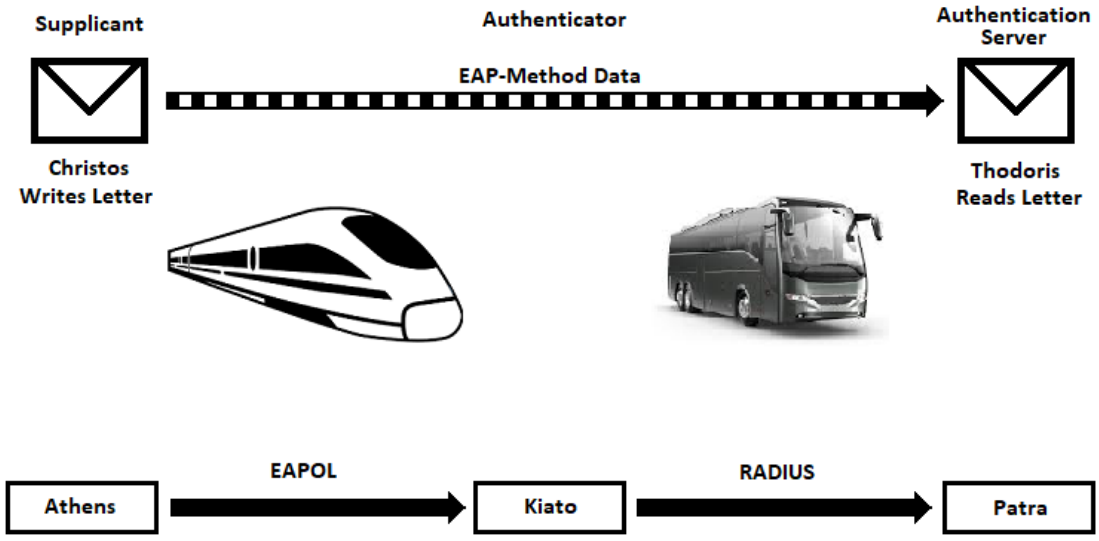


Εικόνα5.1

5.2 Ενθυλάκωση μεθόδων EAP-Methods

Στην Εικόνα 5.2 βλέπουμε το πως εφαρμόζεται η διαδικασία της ενθυλάκωσης μέσα από το παράδειγμα που είχαμε δει και σε προηγούμενο κεφάλαιο με την αποστολή της επιστολής από Αθήνα προς Πάτρα.Δεδομένα μεθόδων EAP-Methodαποστέλλονται ανάμεσα σε χρήστη (Supplicant) και μηχανισμό αυθεντικοποίησης μέσα σε EAPπακέτα. Ο μηχανισμός αυθεντικοποίησης για παράδειγμα θα αποστείλει EAP-Methodδεδομένα μέσω ενός EAPRequestπακέτου. Ένα EAPπακέτο που βλέπουμε στην Εικόνα 5.2, μεταφέρεται ανάμεσα σε supplicantκαι μηχανισμό αυθεντικοποίησης μέσα σε EAPOLπακέτα (EAPDatapackets), και συμβολίζουν το τραίνο που δείχνει η εικόνα. Το EAPOL πρωτόκολλο, είναι εκείνο που στο IEEE802.1Xπρότυπο ενσωματώνει το EAP με σκοπό να μπορεί να λειτουργήσει μέσα σε ένα LAN αντί να λειτουργεί σε κάποιο απλού τύπου point-to-pointσύστημα όπως είχε αρχικά σχεδιαστεί να λειτουργεί το EAP. Τα EAPResponseπακέτα μεταφέρουν δεδομένα EAP-Methodαπό τον supplicantπρος τον μηχανισμό αυθεντικοποίησης όπως βλέπουμε και στο παράδειγμα της παρακάτω εικόνας. EAPRequestπακέτα μεταφέρουν EAP-Methodδεδομένα από τον μηχανισμό αυθεντικοποίησης προς τον supplicant. Κατά τη μεταφορά μεταξύ του μηχανισμού αυθεντικοποίησηςκαι του serverαυθεντικοποίησης, δεδομένα EAP-Methodαποστέλλονται σε πακέτα RADIUSτα οποία απεικονίζονται στο παράδειγμα μας από το λεωφορείο. Τα RADIUSAccess-Requestπακέτα μεταφέρουν δεδομένα μεθόδων EAP-Method

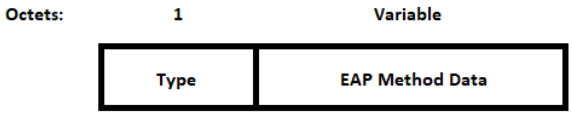
από τον μηχανισμό αυθεντικοποίησης προς τον serverαυθεντικοποίησης, και RADIUSAccess-Acceptπακέτα μεταφέρουν EAP-Methodδεδομένα από τον serverαυθεντικοποίησης προς τον μηχανισμό αυθεντικοποίησης. Τα πακέτα EAPOL καιRADIUS μαζί, μπορούν αποτελεσματικά να μεταφέρουν EAP-Method δεδομένα ανάμεσα σε χρήστη, μηχανισμό αυθεντικοποίησης και serverαυθεντικοποίησης.



Εικόνα5.2

5.3 Δομή πακέτων EAP-Method

Όλα τα EAP-Methodπακέτα έχουν την ίδια βασική δομή η οποία αποτελείται από τα πεδία Typeκαι EAP-MethodData (βλέπε Εικόνα 5.3). Το πακέτο EAP-Methodμεταφέρεται μέσα στο πεδίο Dataενός EAPπακέτου.



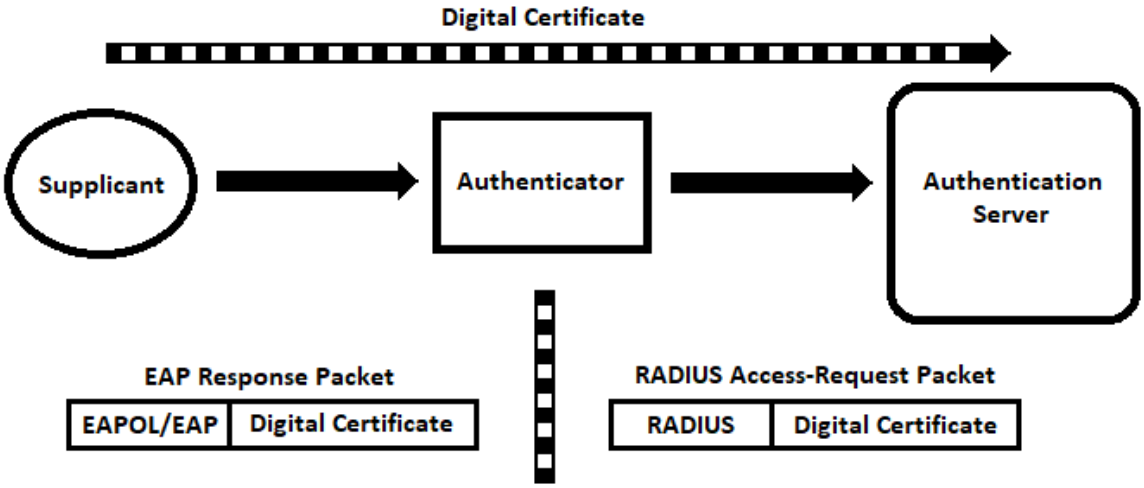
Εικόνα5.3

5.3.1 Πεδίο EAP-Method Type

Το πεδίο EAP-MethodType, με μέγεθος 8 bytes χρησιμοποιείται για να ορίσει την εκάστοτε EAP-Method. Υπάρχουν αρκετές μέθοδοι EAP-Methods, κάποιες από αυτές είχαν οριστεί και στο EAPπρότυπο και αρκετές άλλες είναι προαιρετικές και κατ' επιλογή. Στον Πίνακα 5.1 βρίσκεται μια λίστα με αρκετούς τύπους EAP-Method. Η τιμή του πεδίου EAP-MethodTypeυποδεικνύει το τι μεταφέρει το EAPπακέτο. Για παράδειγμα, μια τιμή πεδίου Type= "13" σημαίνει πως τα δεδομένα EAP-Methodπεριέχουν πληροφορίες σχετικά με την EAP-TLSδιαδικασία αυθεντικοποίησης η οποία είναι και μια από τις πιο κλασσικές. Το δεκαδικού τύπουνούμερο για κάθε μια EAP-Methodαναπαριστά την τιμή η οποία αντιστοιχεί στο Typeπεδίο.Για παράδειγμα, μια τιμή του πεδίου Type= "5" περιλαμβάνεται στη δυαδική μορφή του πεδίου Typeως "0000 0101".

5.3.2 Πεδίο EAP-Method Data

ΤοπεδίοEAP-MethodDataπεριέχει πληροφορίες σχετικές με τον τύπο EAP-Methodκαι τις ανταλλαγές πρωτοκόλλων. Για παράδειγμα, το EAP-MethodDataπεδίο μπορεί να μεταφέρει στοιχεία πρόσβασης, όπως για παράδειγμα ένα ψηφιακό πιστοποιητικό από τον χρήστη προς τον serverαυθεντικοποίησης (βλέπε Εικόνα 5.4).



Εικόνα5.3

Πίνακας5.3

TYPE	EAP-METHOD
1	Identity [RFC 3748]
2	Notification [RFC 3748]
3	NAK [RFC 3748]
4	MD5-Challenge [RFC 3748]
5	One-Time Password (OTP) [RFC 3748]
6	Generic Token Card (GTC) [RFC 3748]
9	RSA Public Key Authentication
10	DSS Unilateral
11	KEA
12	KEA-Validate
13	EAP-TLS
14	Defender Token (AXENT)
15	RSA Security SecureID EAP
16	Arcot Systems EAP

17	EAP-Cisco Wireless
18	GSM Subscriber Identity Modules (EAP-SIM) [RFC 4186]
19	SRP-SHA1
21	EAP-TTLS
22	Remote Access Service
23	EAP-AKA Authentication [RFC 4187]
24	EAP-3Com Wireless
25	PEAP
26	MS-EAP-Authentication
27	Mutual Authentication w/Key Exchange (MAKE)
28	CRYPTOCard
29	EAP-MSCHAP-V2
30	DynamID
31	Rob EAP
32	Protected One-Time Password [RFC 4793]
33	MS-Authentication-TLV
34	SentriNET
35	EAP-Actiontec Wireless
36	Cogent Systems Biometrics Authentication EAP
37	AirFortress EAP
38	EAP-HTTP Digest
39	SecureSuite EAP
40	DeviceConnect EAP
41	EAP-SPEKE
42	EAP-MOBAC
43	EAP-FAST [RFC 4851]

44	ZoneLabs EAP (ZLXEAP)
45	EAP-Link
46	EAP-PAX
47	EAP-PSK [RFC 4764]
48	EAP-SAKE [RFC 4763]
254	Expanded Types [RFC 3748]
255	Experimental use [RFC 3748]

Να σημειωθεί πως λόγω των διάφορων EAP-Methodτύπων, υπάρχει περίπτωση να παρουσιαστούν προβλήματα συμβατότητας κατά την ανάπτυξη συστημάτων 802.1X port-basedαυθεντικοποίησης. Ως αποτέλεσμα, καλό θα ήταν να έχουμε εξασφαλίσει την επιλογή συμβατών EAP-Methodτύπων για όλα τα συστήματα.

5.4 Πρώτοι τύποι EAP-Method πακέτων

Το RFC 3748, το οποίο και είναι και η βάση του αρχικού σετ EAP-Methodτύπων, περιγράφει τις παρακάτω EAP-Methods:

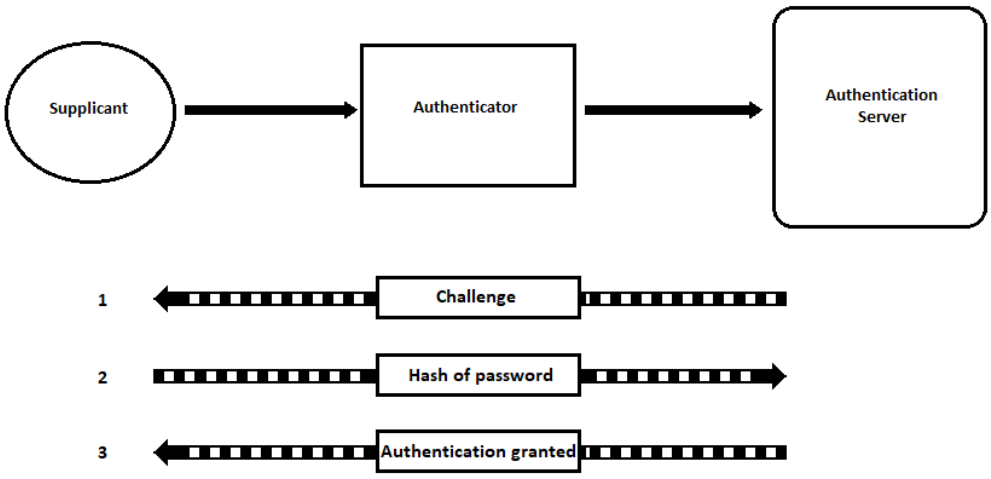
- Identity (Type 1)
- Notification (Type 2)
- Legacy NAK (Type 3)
- MD5-Challenge (Type 4)
- One-Time Password (Type 5)
- Generic Token Card (Type 6)
- Expanded Types (Type 254)
- Experimental Use (Type 255)

ΟιτύποιMD5-Challenge, One-TimePasswordκαιGenericTokenCardυλοποιούντηνδιαδικασία αυθεντικοποίησης. Στις παρακάτω υποενότητες θα κάνουμε μια αναφορά σε αυτούς τους EAP-Methodτύπους. Οι υπόλοιποι τύποι θεωρούνται πως είναι τύποι ειδικών περιπτώσεων.

5.4.1 MD5-Challenge

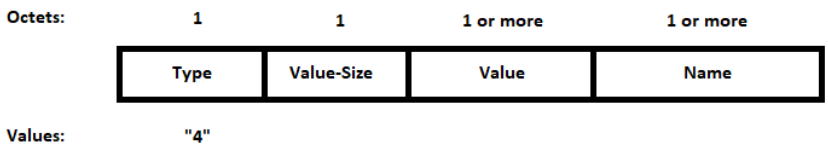
ΟτύποςτηςEAP-MethodMD5-Challengeαναπαρίσταται από τον αριθμό “4” στο πεδίο Typeενός EAP-Methodπακέτου. Το MD5-Challengeείναι μια από τις πρώτες διαδικασίες αυθεντικοποίησης που έχουν οριστεί από το EAP. Το MD5 παρέχει μονόδρομη αυθεντικοποίηση, κάτι το οποίο επιτρέπει στους χρήστες να ταυτοποιηθούν με έναν server αυθεντικοποίησης χρησιμοποιώντας έναν κωδικό χρήστη. Όταν ένας χρήστης αρχικά πληκτρολογεί τον κωδικό πρόσβασης για να δημιουργήσει έναν λογαριασμό στον serverαυθεντικοποίησης, ο serverαρχικά αποθηκεύει το hashτου κωδικού αντί να αποθηκεύσει τον κωδικό πρόσβασης σε μη κρυπτογραφημένη μορφή. Η τιμή hashείναι ένα αποτύπωμα 128-bitτο οποίο συχνά αποκαλείται και messagedigest. Στη συνέχεια, κάθε φορά που ο χρήστης συνδέεται στο σύστημα, ο χρήστης υπολογίζει το hashτου κωδικού πρόσβασης τον οποίο έχει πληκτρολογήσει ο χρήστης κατά την είσοδο του στο σύστημα και στέλνει την τιμή του hash προς τον serverαυθεντικοποίησης για ταυτοποίηση. Ο serverπιστοποιεί τον κωδικό πρόσβασης με το να πραγματοποιεί ένα MD5 hashστον κωδικό πρόσβασης του χρήστη.

Η διαδικασία ταυτοποίησης αποτελείται από μια τριπλή χειραψία ανάμεσα στον χρήστη supplicantκαι τον serverαυθεντικοποίησης (βλέπε Εικόνα 5.5). Ο serverαυθεντκοποίησης θα προκαλέσει τον χρήστη μέσα από την αποστολή ενός RADIUSAccess-Challenge πακέτου. Ο χρήστης με τη σειρά του απαντά με την αποστολή ενός EAPResponseπακέτου το οποίο περιέχει μέσα ένα MD5-Challengeμήνυμα. Εάν η απάντηση είναι ένα MD5-Challenge, τότε το περιεχόμενο του πακέτου θα είναι η τιμή του μονόδρομου hashαπό τον κωδικό πρόσβασης που έχει υποβάλλει ο χρήστης. Ο serverαυθεντικοποίησης με τη σειρά του λαμβάνει το hashαυτό και αποφασίζει εάν η διαδικασία έχει πραγματοποιηθεί επιτυχώς από τον χρήστη. Αν όλα έχουν γίνει σωστά, τότε επιτρέπεται η πρόσβαση στον χρήστη.



Εικόνα5.4

Το MD5 δεν είναι κατάλληλο για ασύρματα δίκτυα και δημόσια δίκτυα καθώς ένας κακόβουλος χρήστης θα μπορούσε εύκολα να κάνει snifftις hashτιμές των κωδικών πρόσβασης. Κάτι τέτοιο κάνει το δίκτυο μη ασφαλές και αναξιόπιστο. Η δομή του MD5-Challengeπακέτου φαίνεται στην Εικόνα 5.6 και στις παρακάτω υποενότητες περιγράφονται τα πεδία Value-Size, Valueκαι Name.



Εικόνα5.4

5.4.1.1 Πεδίο Value-Size

ΤοπεδίοValue-SizeενόςEAP-MethodMD5-Challengeπακέτουέχειμέγεθος από 1ή περισσότερα bytes και απεικονίζει το μέγεθος του πεδίου Value.

5.4.1.2 Πεδίο Value

Το πεδίο Valueσε ένα EAP-MethodMD5-Challengeπακέτο έχει μέγεθος από 1 ή περισσότερα bytes. Σε EAPRequestsπου αποστέλλονται από τον μηχανισμό αυθεντικοποίησης προς τον χρήστη, η τιμή του πεδίου Valueπεριέχει την τιμή της πρόκλησης. Η τιμή αυτή κάθε φορά που αποστέλλεται διαφοροποιείται. Στο EAPResponse που αποστέλλεται από τον χρήστη προς τον μηχανισμό αυθεντικοποίησης, η τιμή Valueπεριέχει την μονόδρομη hashτιμή η οποία έχει μέγεθος 16 bytes.

5.4.1.3 Πεδίο Name

Το NameπεδίοενόςEAP-MethodMD5-Challengeπακέτουέχει μέγεθος από 1 ή περισσότερα bytes και φανερώνει το ποιος είναι ο αποστολέας του MD5-Challenge πακέτου.

5.4.2 One-Time Password

ΟτύποςEAP-MethodOne-TimePassword (OTP) απεικονίζεται με την τιμή "5" στο πεδίο TypeενόςEAP-Methodπακέτου. Το OTPείναι μια από τις πρώτες διαδικασίες αυθεντικοποίησης που έχουν οριστεί από το EAP. Το OTPπαρέχει μονόδρομη αυθεντικοποίηση η οποία επιτρέπει στους χρήστες να ταυτοποιηθούν με έναν server αυθεντικοποίησης. Όταν λαμβάνεται ένα πακέτοOTPauthenticationrequest, ο χρήστης απαντά με ένα OTPresponse.

5.4.3 Generic Token Card

ΟτύποςEAP-MethodGenericTokenCard (GTC) απεικονίζεται με την τιμή "6" στο πεδίο Typeενός EAP-Methodπακέτου. Όπως και με το MD5-Challengeκαι το OTP, ο GTCείναι επίσης μέσα στις πρώτες διαδικασίες πιστοποίησης που έχουν οριστεί στο EAP. Το GTCεπίσης παρέχει μονόδορομη αυθεντικοποίηση η οποία επιτρέπει στους χρήστες να ταυτοποιηθούν με έναν serverαυθεντικοποίησης. Με το GTCένα authenticationrequestαπό τον μηχανισμό αυθεντικοποίησης περιέχει ένα αναγνώσιμο μήνυμα και το authenticationresponseαπό τον χρήστη περιλαμβάνει δεδομένα που έχει διαβάσει από την tokencardσυσκευή η οποία χρειάζεται για την ταυτοποίηση. Όταν λαμβάνεται ένα GTCauthenticationrequest, ο χρήστης μπορεί να απαντήσει με ένα LegacyNAKή GTCResponse.

5.5 Επιπλέον τύποι EAP-Method Types

Τα 8-bitπεδίαTypesεEAP-Methodπακέτα επιτρέπουν τη χρήση επιπλέον τύπων EAP-Methodπέρα από τους αρχικούς που αναφέραμε προηγουμένως. Οι επιπλέον αυτές EAP-Methodsπροορίζονται για ευρεία χρήση. Γενικά, οι περισσότεροι από τους επιπλέον EAP-Method τύπους ανταλλάσσουν στοιχεία πρόσβασης με βάσει τους κωδικούς χρηστών ή ψηφιακών πιστοποιητικών. Ορισμένοι από αυτούς εγκαθιστούν ένα ασφαλές τούνελ για να χρησιμοποιηθεί από κάποια άλλη EAP-Method. Στις επόμενες υποενότητες θα δούμε μερικούς γνωστούς τύπους EAP-Method που χρησιμοποιούνται και έχουν οριστεί πέρα από το RFC 3748.

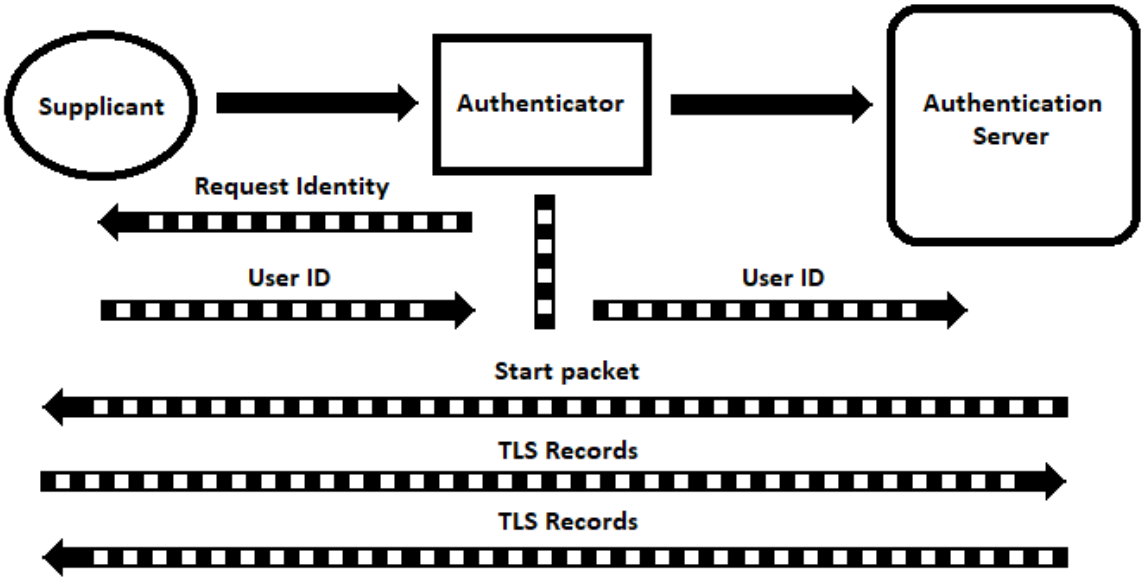
5.5.1 EAP-TLS

ToEAPμεTransportLayerSecurity (EAP-TLS) μετιμήπεδίουEAP-MethodType “13”, παρέχειαμοιβαία αυθεντικοποίηση όπου και ο χρήστης αλλά και ο serverαυθεντικοποίησης πιστοποιούν την ταυτότητα τους ο ένας στον άλλο. Το EAP-TLSκάνει χρήση της κρυπτογράφησης δημοσίου κλειδιού για λόγους αυθεντικοποήσης, κάτι το οποίο θα μπορούσε να συμπεριλάβει και τις έξυπνες κάρτες ή τα ψηφιακά πιστοποιητικά. Το EAP-TLSέχει με διαφορά την μεγαλύτερη υποστήριξη ανάμεσα σε χρήστες και serversαυθεντικοποίησης. Ως παράδειγμα ενδεικτικό, οι εταιρείες και οργανισμοί Cisco, FreeRADIUS, Interlink, Microsoft, παρέχουν RADIUSserverυποστήριξη για το EAP-TLS.

Οι επικοινωνία ανάμεσα σε χρήστη και serverαυθεντικοποίησης επιτυγχάνεται μέσω ενός κρυπτογραφημένου TLStούνελ. Αυτό κάνει το EAP-TLSαρκετά ασφαλές. Το EAP-TLS είναι καλύτερο για τις εταιρείες οι οποίες έχουν ήδη αναπτύξει κάποια ψηφιακά πιστοποιητικά και εξυπηρετούν χρήστες. Παρακάτω, περιγράφεται γενικά η όλη διαδικασία ταυτοποίησης EAP-TLS (βλέπε Εικόνα 5.7):

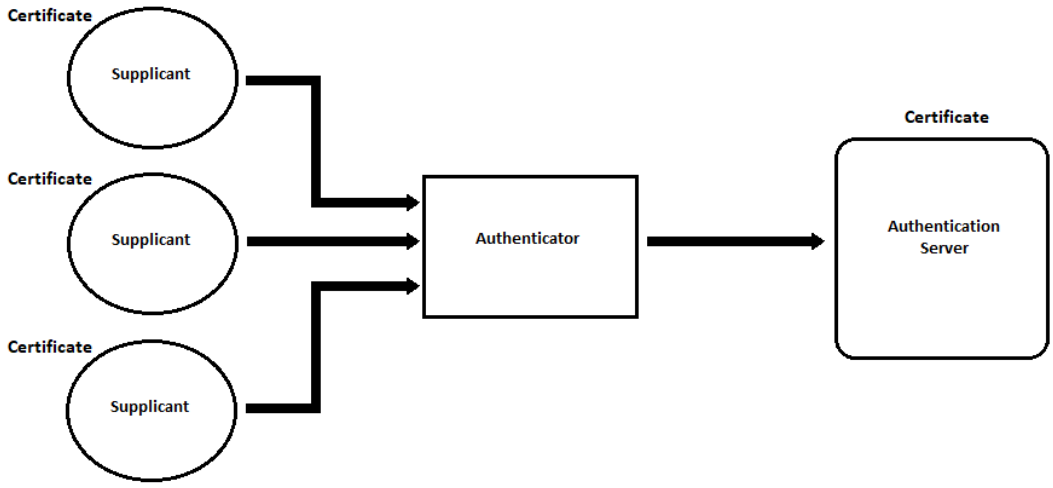
1. Ο μηχανισμός αυθεντικοποίησης στέλνει ένα EAP-Request/Identityπακέτο προς τον χρήστη.
2. Ο χρήστης απαντά αποστέλλοντας προς τον μηχανισμό αυθεντικοποίησης ένα EAP-Response/Identityπακέτο το οποίο περιέχει το userIDτου χρήστη.
3. Ο μηχανισμός αυθεντικοποίησης με τη σειρά του αποστέλλει προς τον serverαυθεντικοποίησης την ταυτότητα του χρήστη.
4. Ο serverαυθεντικοποίησης απαντά στέλνοντας ένα EAP-TLS/ Start πακέτο.

5. Ο χρήστης στέλνει ένα EAP-Responseπακέτο με το πεδίο Type= EAP-TLS, και το πεδίο Datatου πακέτου αυτού να περιέχει μια ή περισσότερες TLSεγγραφές.
6. Ο serverαυθεντικοποίησης τότε απαντά με ένα EAP-Requestπακέτο με πεδίο Type= EAP-TLS, και το πεδίο Data να περιέχει μια ή περισσότερες TLSεγγραφές.



Εικόνα5.5

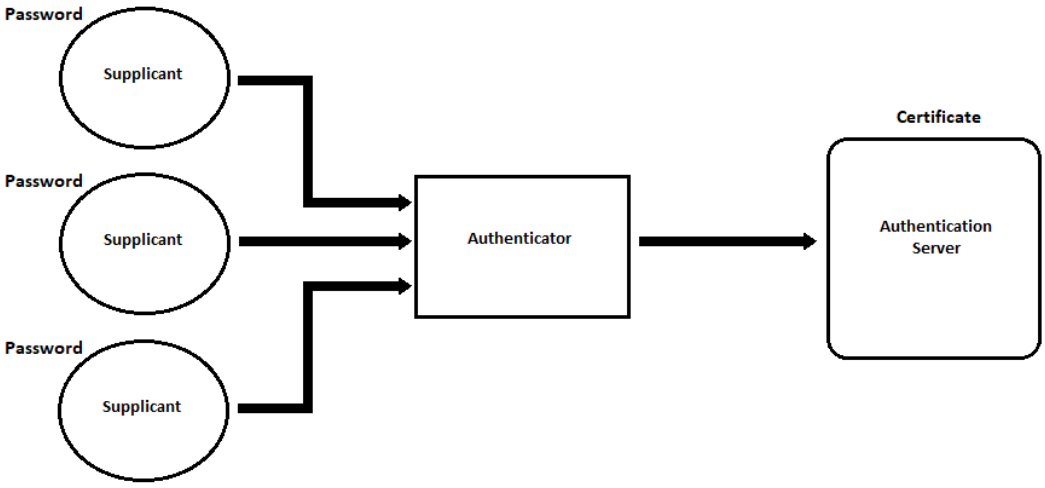
Κατά την ανάπτυξη ψηφιακών πιστοποιητικών, πιστοποιητικά εγκαθίστανται και στους χρήστες αλλά και στον serverαυθεντικοποίησης (βλέπε Εικόνα 5.8). Ως αποτέλεσμα, ένα σημαντικό μειονέκτημα του EAP-TLSείναι ότι υπάρχει δυσκολία στη διαχείριση πιστοποιητικών σε ένα μεγάλο εταιρικό δίκτυο.



Εικόνα5.5

5.5.2 EAP-TTLS

ToEAP-TTLS (TunneledTransportLayerSecurity) μετιμήπεδίουEAP-MethodType “21”, αναπτύχθηκεωςεπέκταση του EAP-TLS. Όμοια με το EAP-TLS, το EAP-TTLS είναι ένα σύστημα αμοιβαίας αυθεντικοποίησηςβασισμένο σε πιστοποιητικά. Παρόλα αυτά, το EAP-TTLSαπαιτεί μόνο server-sideπιστοποιητικά. (βλέπε Εικόνα 5.9). Αυτό επιτυγχάνεται με το να συνδέουμε τον χρήστη με τον server αυθεντικοποίησης μέσω TLSτο οποίο διασχίζει ένα ασφαλές τούνελ. Οι χρήστες τότε μπορούν να ταυτοποιηθούν με τη χρήση ενός κωδικού πρόσβασης αντί να χρησιμοποιούν κάποιο πιστοποιητικό. Με τον τρόπο αυτό απλοποιείται η λειτουργία ενός port-basedauthenticationσυστήματος διότι δεν είναι απαραίτητο να εγκαθιστούμε σε όλες τις συσκευές χρηστών τα αντίστοιχα πιστοποιητικά και να τα διαχειριζόμαστε.



Εικόνα5.5

5.5.3 PEAP

ToPEAP (ProtectedExtensibleAuthenticationProtocol) μετιμήπεδίουEAP-MethodType “25”, είναιόμοιομετοEAP-TTLSκαιαναπτύχθηκε από τις Microsoft, Ciscoκαι RSASecurity. Όπως και με το EAP-TTLS, το PEAP δεν χρειάζεται πιστοποιητικά στις συσκευές χρηστών. Το PEAPπροσφέρει ένα ασφαλές περιβάλλον μεταφοράς για τα δεδομένα αυθεντικοποίησης, τα οποία περιέχουν κωδικούς πρόσβασης. Το PEAPπραγματοποιεί τη διαδικασία αυτή με τη χρήση tunnelingμεταξύ PEAPχρηστών και serverαυθεντικοποίησης.

5.5.4 LEAP

ToLEAP (LightweightExtensibleAuthenticationProtocol) μετιμήπεδίουEAP-MethodType “17”, αναπτύχθηκεαπότηCiscoγιαασύρματα τοπικά δίκτυα LANs. Το LEAPπαρέχει κρυπτογράφηση μέσω δυναμικών WEP(WiredEquivalentPrivacy) κλειδιών χρησιμοποιώντας τους κωδικούς πρόσβασης των χρηστών. Παρόλα αυτά για λόγους ασφαλείας καλό θα ήταν να χρησιμοποιήσομε για νέες εφαρμογές κάποιο άλλο πρωτόκολλο το οποίο είναι λιγότερο ευάλωτο σε επιθέσεις.

5.5.5 EAP-FAST

ToEAP-FAST (FlexibleAuthenticationviaSecureTunneling) μετιμήπεδίουEAP-MethodType “43”, αναπτύχθηκεαπότηνCiscoως αντικαταστάτης του LEAP. Στην ουσία το EAP-FAST παρέχει αμοιβαία αυθεντικοποίηση με τη χρήση ενός ProtectedAccessCredential (PAC) αντί

ψηφιακών πιστοποιητικών. Ένας διαχειριστής μπορεί να μοιράσει τα PACsχειροκίνητα ή αυτοματοποιημένα μέσα από τον serverαυθεντικοποίησης. Το πλεονέκτημα του EAP-FASTείναι πως οι εταιρείες δεν χρειάζεται να αναπτύξουν ψηφιακά πιστοποιητικά.

5.5.6 EAP-SIM

ToEAP-SIM (SubscriberIdentityModule) παρέχειαμοιβαία αυθεντικοποίηση για τις κάρτες SIMπου βρίσκονται στα κινητά τηλέφωνα. Το EAP-SIMεπιτρέπει στην κάρτα να ταυτοποιηθεί με έναν GSMserverαυθεντικοποίησης και αντίστροφα. Τα smartphonesμε EAP-SIMμπορούν να αυθεντικοποιηθούν μέσω κάποιου Wi-Fihotspotκατά την περιαγωγή από το GSMδίκτυο στο hotspot.

5.6 Σκέψεις για Επιλογή EAP-Method

Η επιλογή του σωστού τύπου EAP-Methodπιθανότατα θα είναι μια σημαντική επιλογή κατά το σχεδιασμό ενός συστήματος port-basedαυθεντικοποίησης. Παρακάτω γίνεται μια σύντομη περιγραφή ορισμένων σημείων που θα πρέπει να λάβουμε υπ' όψιν κατά την επιλογή ενός EAP-Method τύπου.

- **Πολιτικές ασφαλείας:** Σε κάθε υλοποίηση θα πρέπει να σκεφτούμε το εάν κάποια πολιτική ασφαλείας της εταιρείας επιβάλλει τη χρήση συγκεκριμένων τύπων EAP-Methods και το πως μπορούμε να πετύχουμε μεγαλύτερη ασφάλεια.
- **Ήδη υπάρχουσες εγκαταστάσεις:** Θα ήταν καλό να εξετάζουμε τις ήδη υπάρχουσες εγκαταστάσεις και εξοπλισμό με σκοπό την καλή λειτουργία, συντήρηση και εξέλιξη του συστήματος χωρίς προβλήματα ασυμβατότητας.
- **Συσκευές χρηστών:** Ανάλογα με τις συσκευές οι οποίες έχουν πρόσβαση στο δίκτυο και με βάσει τις ανάγκες τους, θα πρέπει να γίνεται και η καταλληλότερη επιλογή EAP-Method τύπων.

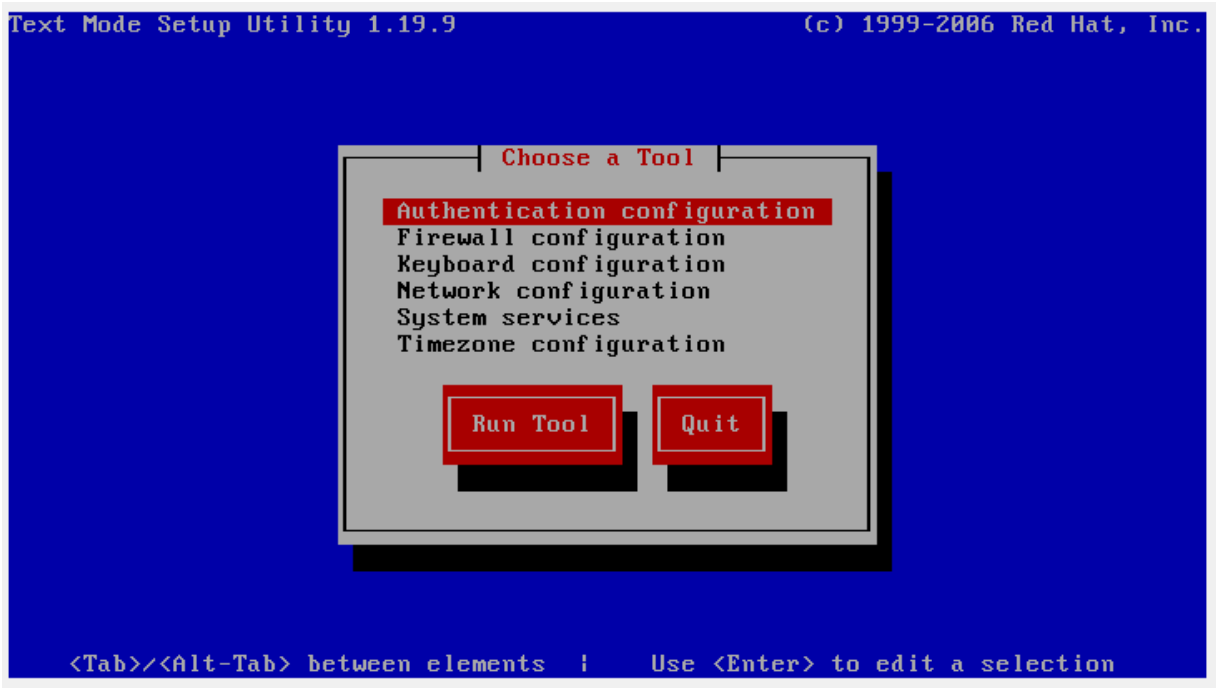
6 Από τη θεωρία στην υλοποίηση

Στο σημείο αυτό αφού έχουμε μιλήσει σε θεωρητικό επίπεδο για τα στοιχεία που αποτελούν ένα σύστημα port-basedαυθεντικοποίησης, θα μεταβούμε σε μια υλοποίηση ενός συστήματος ελέγχου ταυτότητας και πρόσβασης χρηστών σε ένα δίκτυο με τη χρήση του 802.1X.Για να

επιτευχθεί η υλοποίηση θα χρειαστεί να έχουμε στη διάθεση μας κάποιο δικτυακό εξοπλισμό και λογισμικό το οποίο θα στηριχθεί πάνω στο hardware. Από πλευράς hardware χρειάζεται ένα switch και ένα ασύρματο accesspoint. Το switchστην περίπτωση μας είναι ένα CiscoCatalyst 2960 switchγια το ενσύρματο μέρος, και για το ασύρματο κομμάτι θα δοκιμαστεί ένα Level 1 ασύρματο accesspoint. Ο παραπάνω εξοπλισμός μπορεί να υποστηρίξει το 802.1X και τα πρωτόκολλα RADIUS. Από πλευράς λογισμικού θα γίνει εγκατάστασητου openNAC, μια εικονική μηχανή μέσω Virtualboxη οποία είναι ένας networkaccesscontroller.

6.1 Προαπαιτούμενο λογισμικό και ρυθμίσεις

Για να στηθεί το κομμάτι του λογισμικού στον υπολογιστή, χρησιμοποιήθηκε μια Linuxδιανομή λειτουργικού συστήματος, το Ubuntu 18.04 . Έγινε εγκατάσταση του λειτουργικού συστήματος με βάσει τις default ρυθμίσειςγια desktop. Εν συνεχεία έγινε εγκατάσταση του VirtualBoxτης Oracleως πρόγραμμα το οποίο θα φιλοξενήσει το εικονικό μας μηχάνημα. Το εικονικό μηχάνημα που χρησιμοποιήθηκε είναι όπως αναφέραμε το openNAC το οποίο βασίζεται σε επίσης Linux σύστημα διανομής CentOS. Ως ρύθμιση που έγινε για να μπορεί να επικοινωνεί το δίκτυο του openNAC με το υπόλοιπο δίκτυο είναι να κάνουμε bridgeτην κάρτα δικτύου του VirtualBoxμε την κάρτα δικτύου Ethernetστον ηλεκτρονικό μας υπολογιστή που φιλοξενεί το εικονικό μηχάνημα. Παρακάτω ακολουθούν μερικές εικόνες στις οποίες φαίνεται το πως ξεκινάει η εγκατάσταση του NetworkAccessControllerκαθώς και η αρχική του παραμετροποίηση.

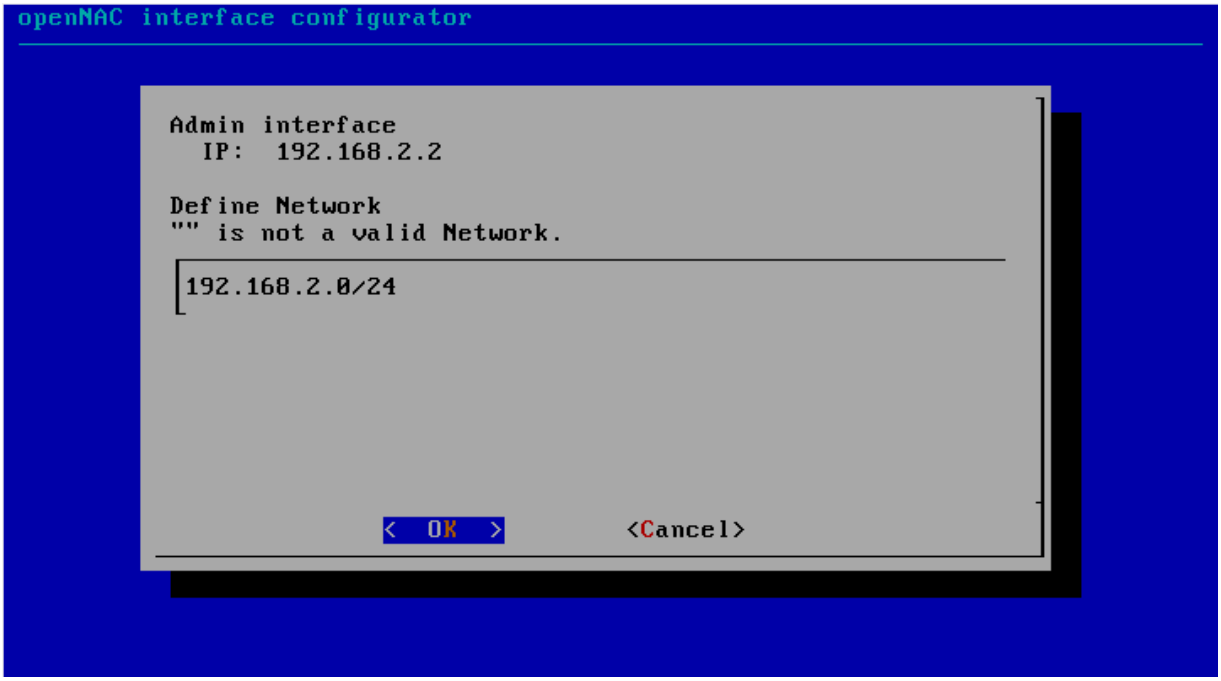


Εικόνα6.1

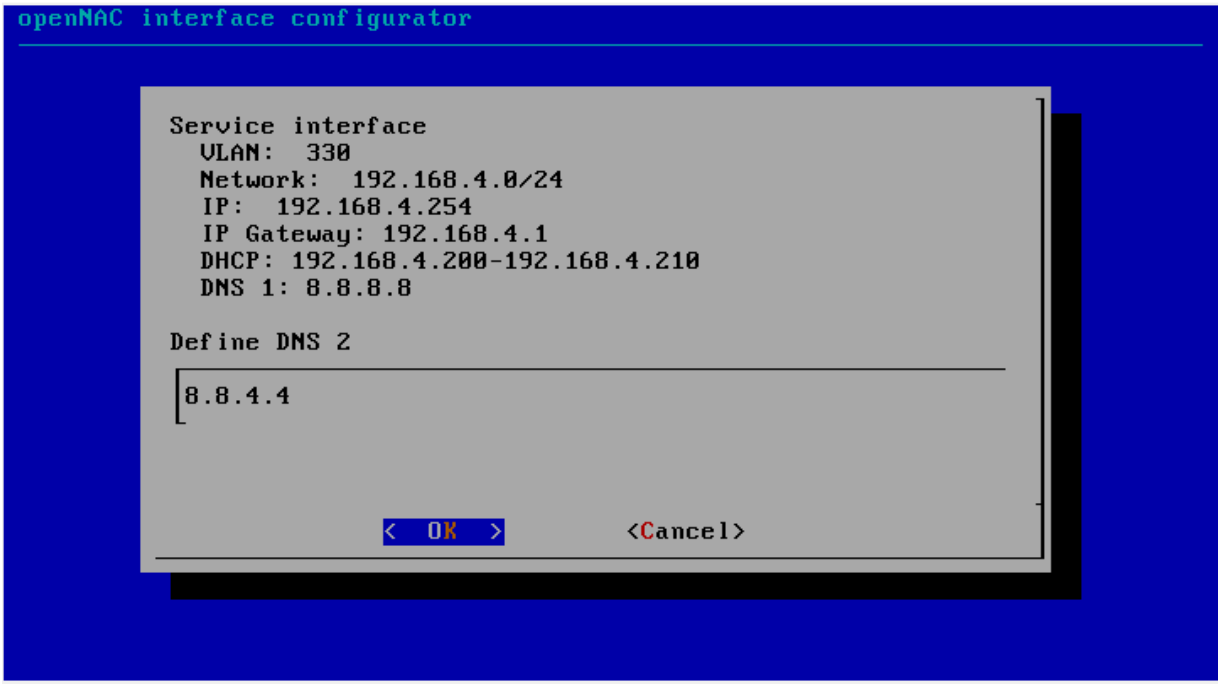
Εικόνα6.1

Στην Εικόνα 1 έγινε ένας έλεγχος όσον αφορά τις ρυθμίσεις πληκτρολογίου ώστε να είναι σε αγγλικά. Στη συνέχεια με βάσει και τα όσα βλέπουμε και στην Εικόνα 2 εκτελέστηκε η εντολή:

/usr/share/opennac/utils/vm-iface-config/opennac-ifaceμε σκοπό την ρύθμιση των δικτυακών παραμέτρων και των vlanπου θα χρησιμοποιηθούν. Στη συνέχεια μετά την εκτέλεση της παραπάνω εντολής μεταφερθήκαμε στο περιβάλλον το οποίο ρυθμίζει τις παραμέτρους αυτές. Ενδεικτικά στις παρακάτω εικόνες θα δούμε λίγο συνοπτικά τις απαραίτητες παραμέτρους που θα πρέπει να οριστούν και στη συνέχεια θα ακολουθήσει μια σύντομη περιγραφή αυτών.

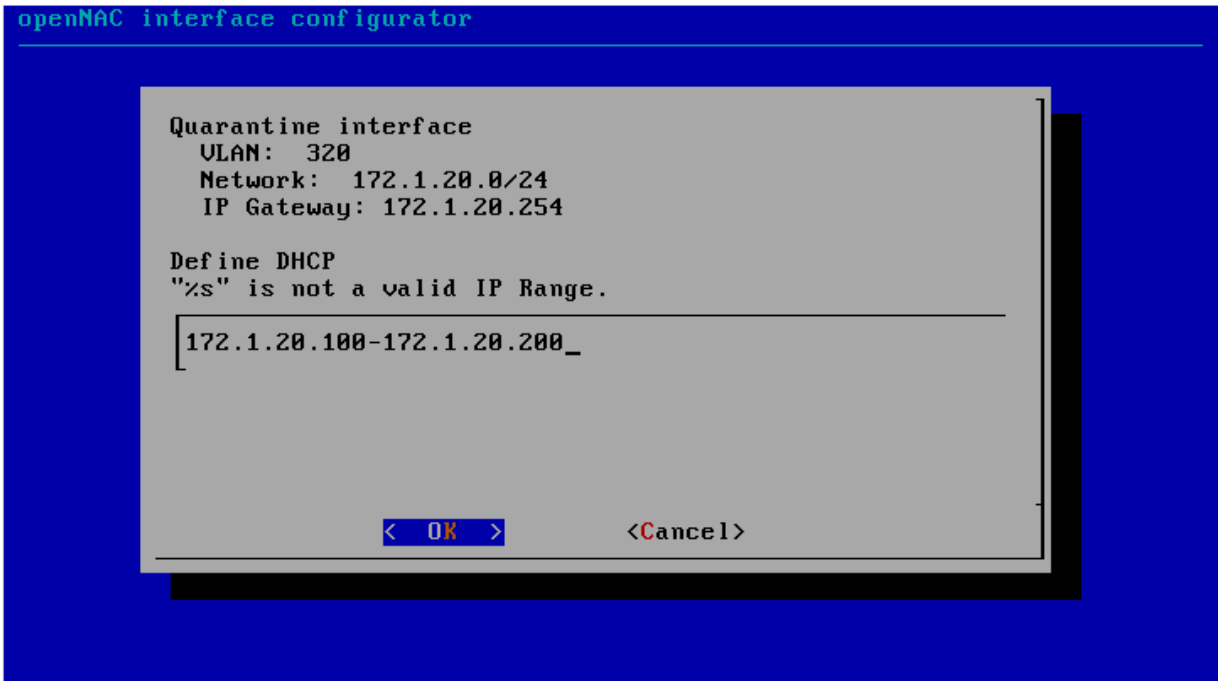


Εικόνα6.1

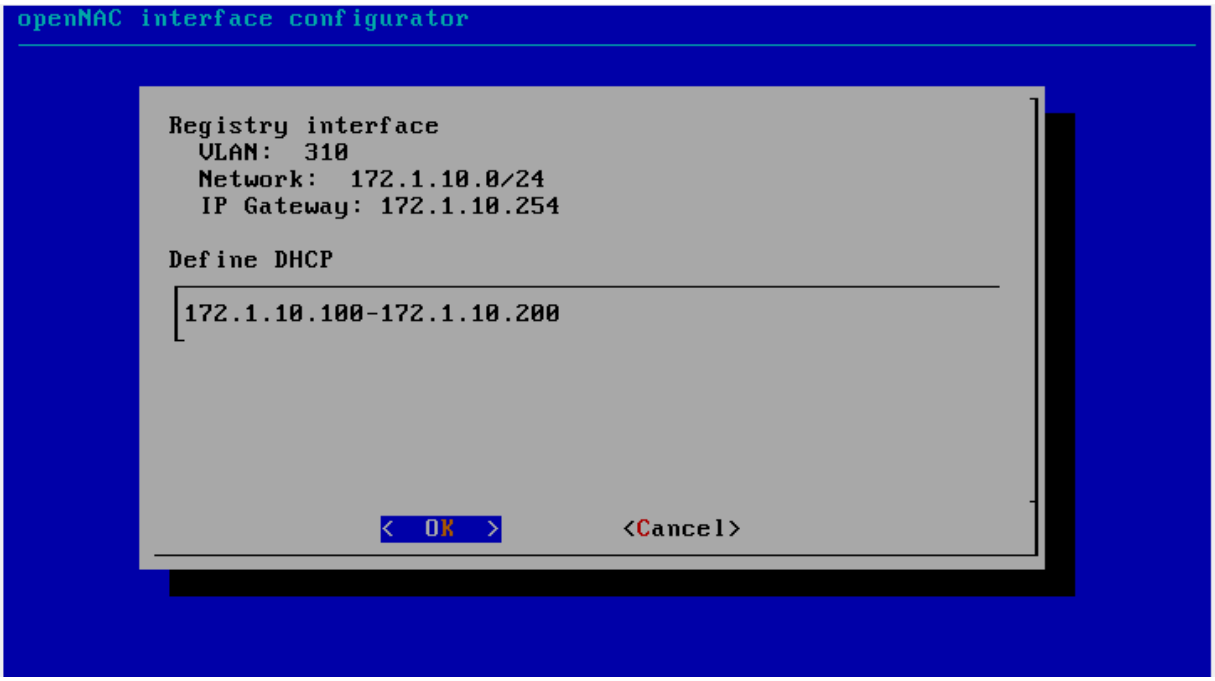


Εικόνα6.1

Στην Εικόνα 6.3 ορίζεται το διαχειριστικό περιβάλλον στο οποίο θα συνδέεται ο διαχειριστής της δικτυακής υποδομής στο εργαλείο του openNACαπό τον υπολογιστή του. Στην περίπτωση μας η IPδιεύθυνση που δόθηκε ήταν η: 192.168.1.103 και το δίκτυο στο οποίο απευθυνόμαστε είναι το 192.168.1.0/24. Στη συνέχεια μεταφερθήκαμε στις ρυθμίσεις των VLANπου θα χρειαστούν για την υλοποίηση μας (βλέπε Εικόνα 6.4) όπου εκεί ορίσαμε το πρώτο μας VLANτο οποίο είναι το VLANService για την παροχή δικτύου. Έπειτα από το VLANαυτό, ορίσαμε το VLANQuarantineστο οποίο και μεταφέρονται οι χρήστες οι οποίοι δεν έχουν πρόσβαση στο δίκτυο για λόγους είτε μη πιστοποίησης είτε για λόγους κακόβουλης χρήσης (Εικόνα 6.5). Στην Εικόνα 6.6 απεικονίζονται οι ρυθμίσεις που έγιναν για τον ορισμό του RegistryVLANστο οποίο μεταβαίνουν οι χρήστες οι οποίοι περνάνε τη διαδικασία ελέγχου ταυτότητας πρόσβασης.

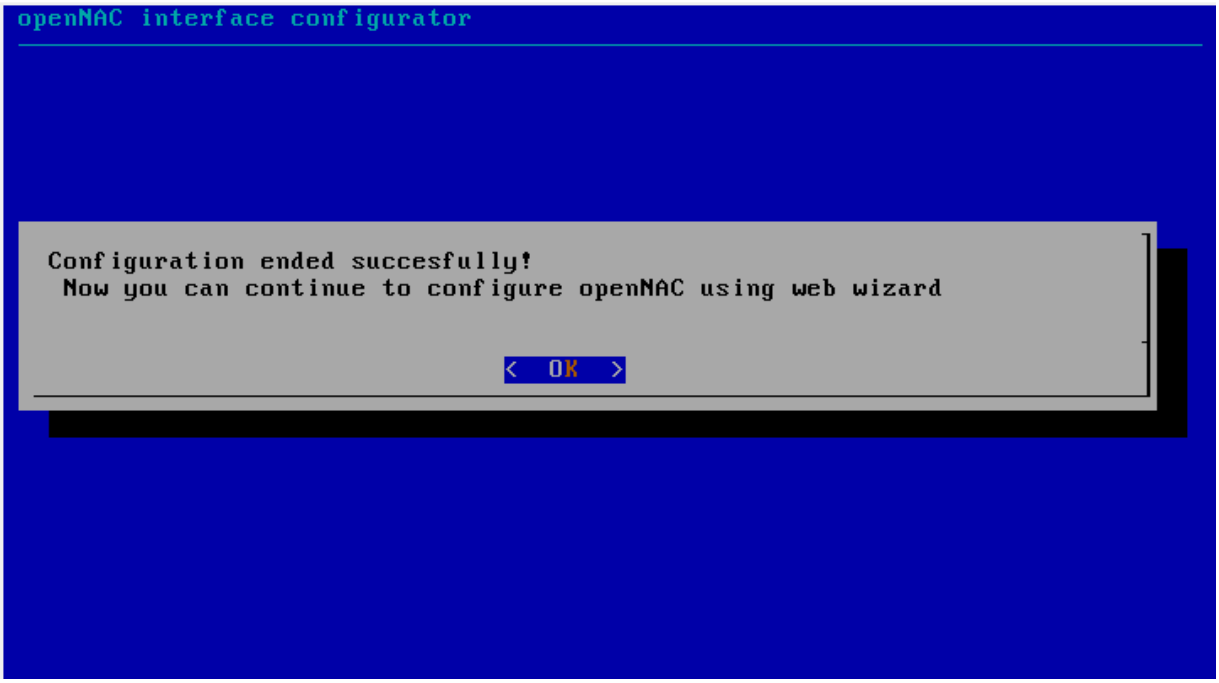


Εικόνα6.1



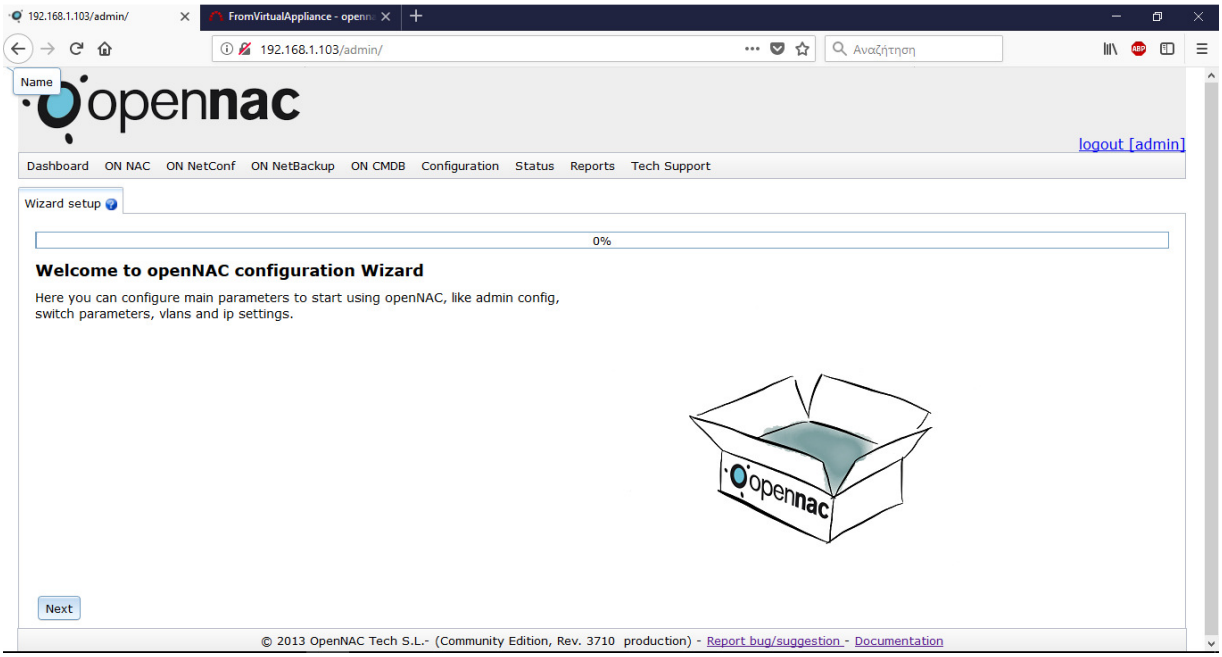
Εικόνα6.1

Μετά και τη ρύθμιση του Registryinterfaceολοκληρώνεται η διαδικασία πρώτης παραμετροποίησης του συστήματος και στη συνέχεια μπορούμε να προχωρήσουμε σε οποιαδήποτε αλλαγή μέσω του διαχειριστικού περιβάλλοντος με τη χρήση κάποιου περιηγητή (Εικόνα 6.7).



Εικόνα6.1

Σε αυτό το σημείο, μεταβήκαμε στο webbased περιβάλλον τουopenNACανοίγοντας έναν browserκαι πληκτρολογώντας την IP διεύθυνση που είχε οριστεί παραπάνω για το διαχειριστικό μας περιβάλλον. **Σημείωση:** η IPπου έχουμε εμείς ορίσει για το σύστημα μας είναι η **http://192.168.1.103/admin**. Στην διεύθυνση αυτή θα χρειαστεί να κάνουμε loginμε τα στοιχεία του διαχειριστή και έπειτα να επιβεβαιώσουμε ή να τροποποιήσουμε τις βασικές μας ρυθμίσεις (Εικόνα 6.8).



Εικόνα6.1

Επιπρόσθετα, το διαχειριστικό περιβάλλον του openNACπροσφέρει τη δυνατότητα παρακολούθησης του δικτύου μέσω γραφημάτων, τον καθορισμό κανόνων rules, τον έλεγχο χρηστών, των συσκευών χρηστών καθώς και του εκάστοτε δικτυακού εξοπλισμού. Στην επόμενη ενότητα θα μιλήσουμε σχετικά με τον δικτυακό εξοπλισμό και τις ρυθμίσεις που έγιναν για το ενσύρματο δικτυακό σκέλος το οποίο βασίζεται σε ένα CiscoCatalyst 2960switch.

6.2 Παραμετροποίηση ενσύρματου εξοπλισμού

Σε αυτή την ενότητα θα εστιάσουμε στην παραμετροποίηση του εξοπλισμού για το ενσύρματο σκέλος του ελέγχου ταυτότητας πρόσβασης χρήστη. Στον Πίνακα 6.1 απεικονίζονται οι ρυθμίσεις που έγιναν πάνω στο switch έτσι ώστε να μπορεί ένας χρήστης ο οποίος συνδέεται να πιστοποιεί την ταυτότητα του.

Πίνακας6.2

SW1#sh run Building configuration... Current configuration : 6049 bytes

```
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$i7X/$f2LoP5qJHJY/4RpcS8UFZ1
!
!
username admin password 7 04541B03012F4D4D
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
!
!
aaa session-id common
system mtu routing 1500
ip subnet-zero
!
!
```

```
no ip domain-lookup
!
!
crypto pki trustpoint TP-self-signed-214843008
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-214843008
 revocation-check none
 rsakeypair TP-self-signed-214843008
!
!
crypto pki certificate chain TP-self-signed-214843008
 certificate self-signed 01
  3082023A 308201A3 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32313438 34333030 38301E17 0D393330 33303130 31333135
  335A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3231 34383433
  30303830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  9DC60690 48CB0138 330252B9 7D56C937 AE73A6DE B4341EDB D98E39D4 5661C525
  538DC2C7 A2E8D039 BB03AFFE 746F9406 B704D3A9 ACACBC22 D565F5DE
9EA37CA3
  FE305248 70510674 21563BA2 9545AF55 44221DEF EE15E224 99E3096E 09DF6F78
  2698C0BA 5FEC2BD6 57FABA9D 249B0A5B 4DA530E7 577B048F 52F0DF93
215BCCDB
  02030100 01A36430 62300F06 03551D13 0101FF04 05300301 01FF300F 0603551D
  11040830 06820453 57312E30 1F060355 1D230418 30168014 A3F04283 A142CFA4
  42A6C478 E6C3E2FF A32B1976 301D0603 551D0E04 160414A3 F04283A1 42CFA442
  A6C478E6 C3E2FFA3 2B197630 0D06092A 864886F7 0D010104 05000381 81005481
  E4FBCADA ED169F67 023FD18A 72B38D01 BDCE2915 E0471AB3 3043B097
ECE6C54C
  4AD2D01D 34E400FB E4DF77B1 9E0642CB 18022CF3 CB8D10EA 1F42B4C2
```

```
E6094B7D
 9967E054 A1F47B80 BDE5ABB2 0E38B337 665CB5DD 5AA7555F C01348AC
C91452AD
 04A07F9E 8143D22A F7BFBD6D 8FAA5027 19CF29C7 75D27959 6676901E E45A
 quit
!
!
dot1x system-auth-control
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
 description externaltrunk
 switchport mode trunk
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 description uploadswitch
 switchport access vlan 330
!
interface FastEthernet0/3
!
interface FastEthernet0/4
```

```
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
 description TaBon
!
interface FastEthernet0/12
 description TaBon
!
interface FastEthernet0/13
 switchport mode access
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 2
!
interface FastEthernet0/14
!
interface FastEthernet0/15
```

```
 switchport mode access
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
!
interface FastEthernet0/16
 description test8021x
 switchport mode access
 authentication event no-response action authorize vlan 310
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
!
interface FastEthernet0/17
 description test8021x
 switchport mode access
 authentication event no-response action authorize vlan 310
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
```

```
interface FastEthernet0/22
!
interface FastEthernet0/23
 description opennactrunk
 switchport mode trunk
 authentication port-control auto
 mab
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/24
 description opennactrunk
 switchport mode trunk
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface FastEthernet0/25
!
interface FastEthernet0/26
!
interface FastEthernet0/27
!
interface FastEthernet0/28
!
interface FastEthernet0/29
!
```

```
interface FastEthernet0/30
!
interface FastEthernet0/31
!
interface FastEthernet0/32
!
interface FastEthernet0/33
!
interface FastEthernet0/34
!
interface FastEthernet0/35
!
interface FastEthernet0/36
!
interface FastEthernet0/37
!
interface FastEthernet0/38
!
interface FastEthernet0/39
!
interface FastEthernet0/40
!
interface FastEthernet0/41
!
interface FastEthernet0/42
!
interface FastEthernet0/43
!
interface FastEthernet0/44
!
interface FastEthernet0/45
```

```
!
interface FastEthernet0/46
!
interface FastEthernet0/47
!
interface FastEthernet0/48
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.254 255.255.255.0
 no ip route-cache
!
ip http server
ip http secure-server
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps mac-notification change move threshold
snmp-server host 192.168.1.103 version 2c public
radius-server host 192.168.1.103 auth-port 1812 acct-port 1813 key 7 0700314940071806
radius-server vsa send accounting
radius-server vsa send authentication
!
control-plane
!
banner motd ^CC
   Switch Node Barcelona.
   Access Restricted and monitored.
```

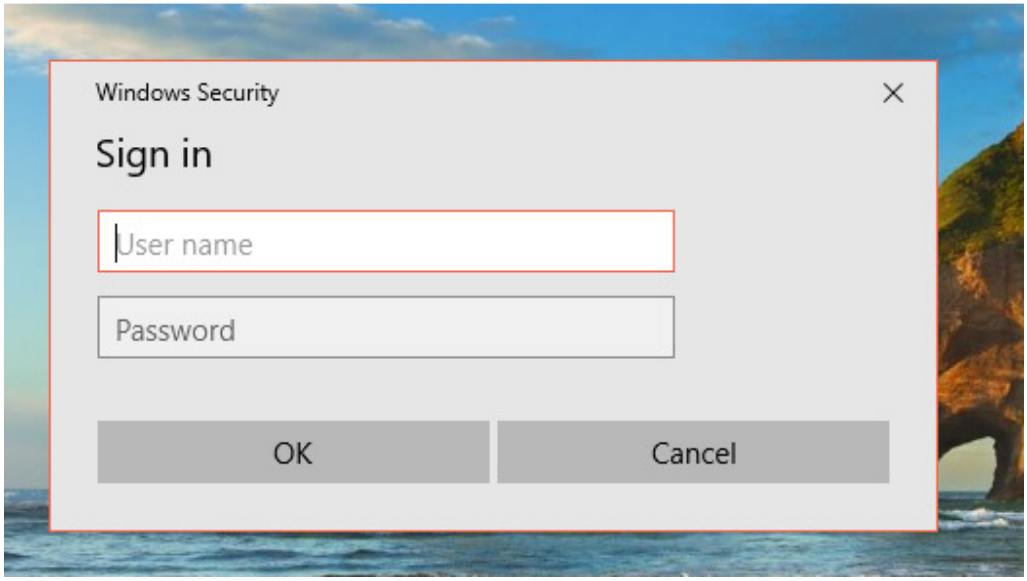
```
   Authorized Access Only.
^C
!
line con 0
 exec-timeout 0 0
 password 7 104D000A0618
 logging synchronous
line vty 0 4
 exec-timeout 0 0
 password 7 0209145E05080E22
 logging synchronous
 transport input telnet ssh
line vty 5 15
 exec-timeout 0 0
 password 7 104D000A0618
 logging synchronous
!
mac address-table notification change
end
```

Στον παραπάνω πίνακα είδαμε το running-configurationτου switchτο οποίο έχει ρυθμιστεί για τις ανάγκες της παρούσας εργασίας. Αρχικά ορίστηκε ένα secretpasswordκαθώς και το usernameadminpassword. Στη συνέχεια έγινε ορισμός του μοντέλου AAA (Authentication, Authorization, Accounting) για πιστοποίηση με βάσει το 802.1X και το RADIUS και επίσης ορίστηκε ένα selfsignedcertificate. Έπειτα δόθηκαν εντολές για να ρυθμιστούν οι θύρες του switch με βάσει τις ανάγκες του openNAC, για παράδειγμα η FastEthernet 0/1θύρα ορίστηκε ως Trunkπόρτα για να συνδεθεί με το openNACκαι να μπορεί να επικοινωνεί με τα υπόλοιπα VLANs. Ως επόμενο βήμα ήταν να ορίσουμε το VLAN 1 στο οποίο θα πατάει η Trunkπόρτα της FastEthernet 0/1. Έπειτα δόθηκαν εντολές για ρύθμιση παραμέτρωνστο switch σχετικά με τον server. Η παραμετροποίηση του εξοπλισμού έγινε μέσω καλωδίου κονσόλας (RS232) το οποίο

συνδέθηκε στον υπολογιστή και με τη χρήση του προγράμματος PuTTYδόθηκαν οι απαραίτητες εντολές.

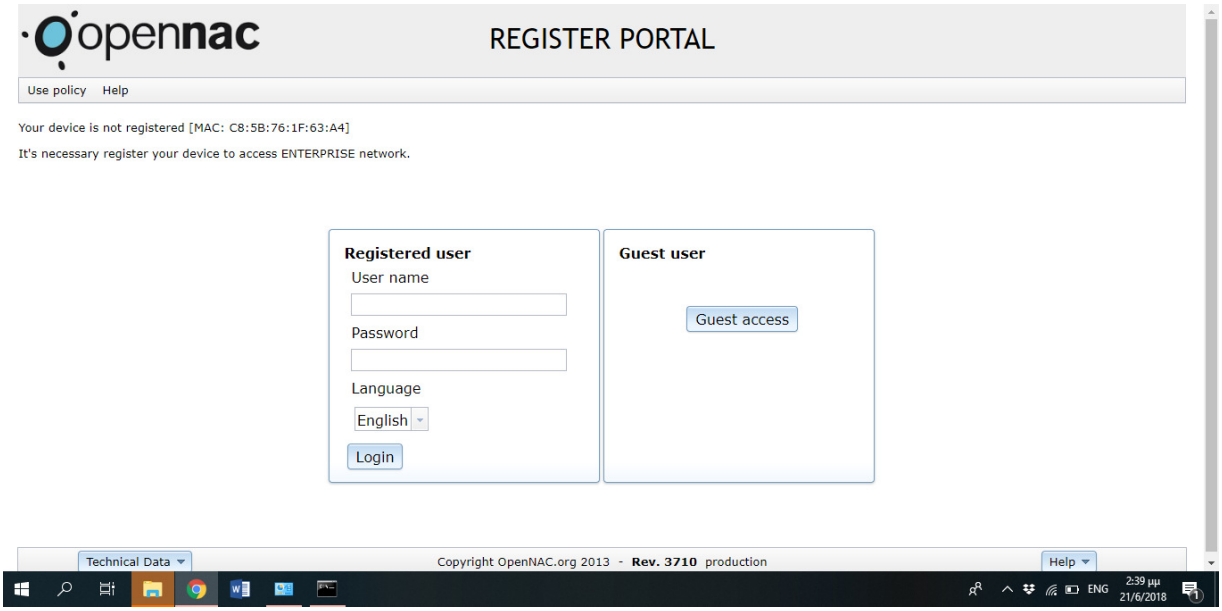
6.3 Διαδικασία πιστοποίησης ταυτότητας χρήστη στο δίκτυο

Μετά από τη διαδικασία που προηγήθηκε, ερχόμαστε στο σημείο το οποίο πρέπει να πιστοποιήσουμε έναν χρήστη μέσα σε ένα δίκτυο με τη χρήση του openNAC. Η διαδικασία που θα χρειαστεί ναακολουθήσει ο χρήστης είναι η εξής ακόλουθη. Αρχικά θα πρέπει ο χρήστης να επιτρέπει αλλά και να κάνει χρήση του 802.1X ως μέθοδο αυθεντικοποίησης σε ένα δίκτυο. Στη συνέχεια εφόσον πληρεί το παραπάνω κριτήριο, μόλις συνδεθεί στο δίκτυο αυτό θα χρειαστεί να πληκτρολογήσει κάποια στοιχεία πρόσβασης τα οποία φαίνονται παρακάτω στην Εικόνα 6.9 κατά το login.



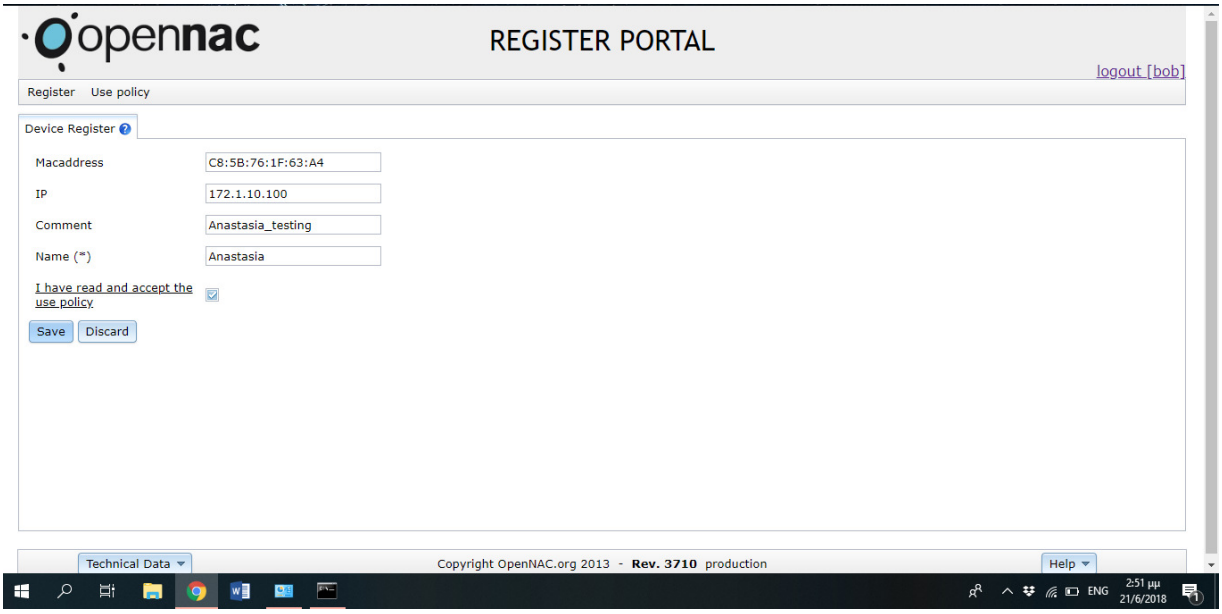
Εικόνα6.3

Στη συνέχεια (βλέπε Εικόνα 6.10) και εφόσον τα στοιχεία είναι εκείνα που ορίζει το openNACτότε ο χρήστης μεταφέρεται στο webbasedπεριβάλλον του openNACόπου και εκεί θα πρέπει να γίνει το registrationτου χρήστη για να προστεθεί στο ασφαλές περιβάλλον του δικτύου του.



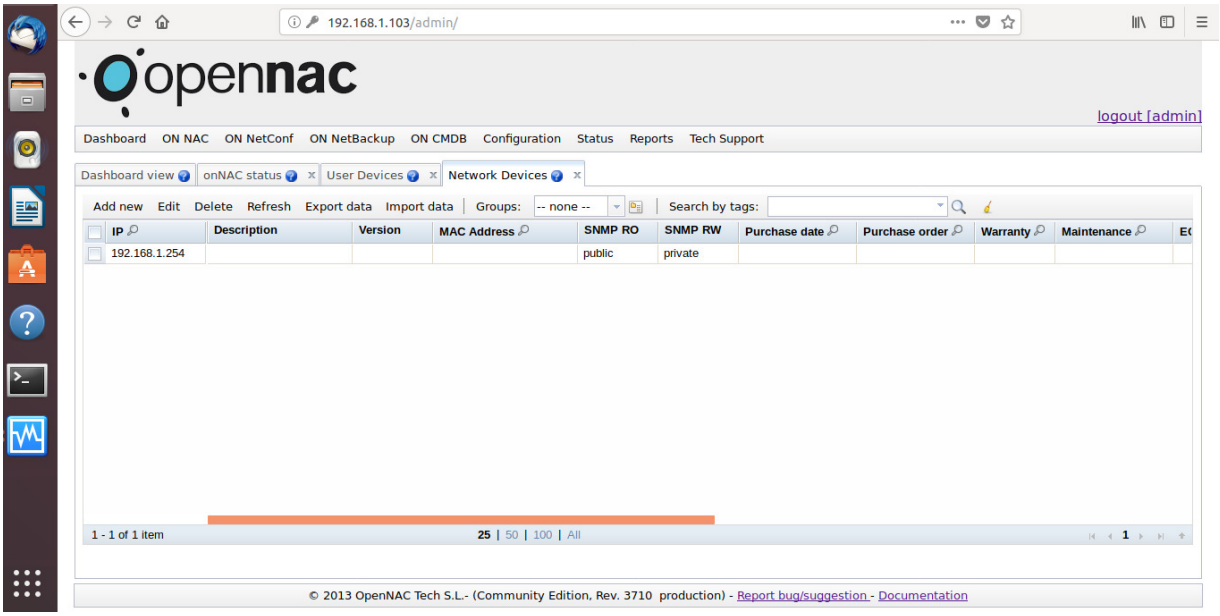
Εικόνα6.3

Στο portalτης Εικόνας 6.10 έχουμε τη δυνατότητα να επιλέξουμε ανάμεσα σε δυο μεθόδους πρόσβασης χρήστη. Εκείνη του πιστοποιημένου χρήστη καθώς και εκείνη του χρήστη guest. Στο παράδειγμα μας εξετάζουμε το σενάριο του πιστοποιημένου χρήστη και κάνουμε loginμε τη χρήση username και password. Κατόπιν στην Εικόνα 6.11 ζητείται από τον χρήστη να πιστοποιήσει και τη συσκευή από την οποία έχει πρόσβαση στο δίκτυο ορίζοντας τη MACAddress, την IPδιεύθυνση του, το όνομα και κάποιο πιθανό σχόλιο. Στη συνέχεια και αφού γίνει αποδοχή της πολιτικής χρήσης, πατάμε save.

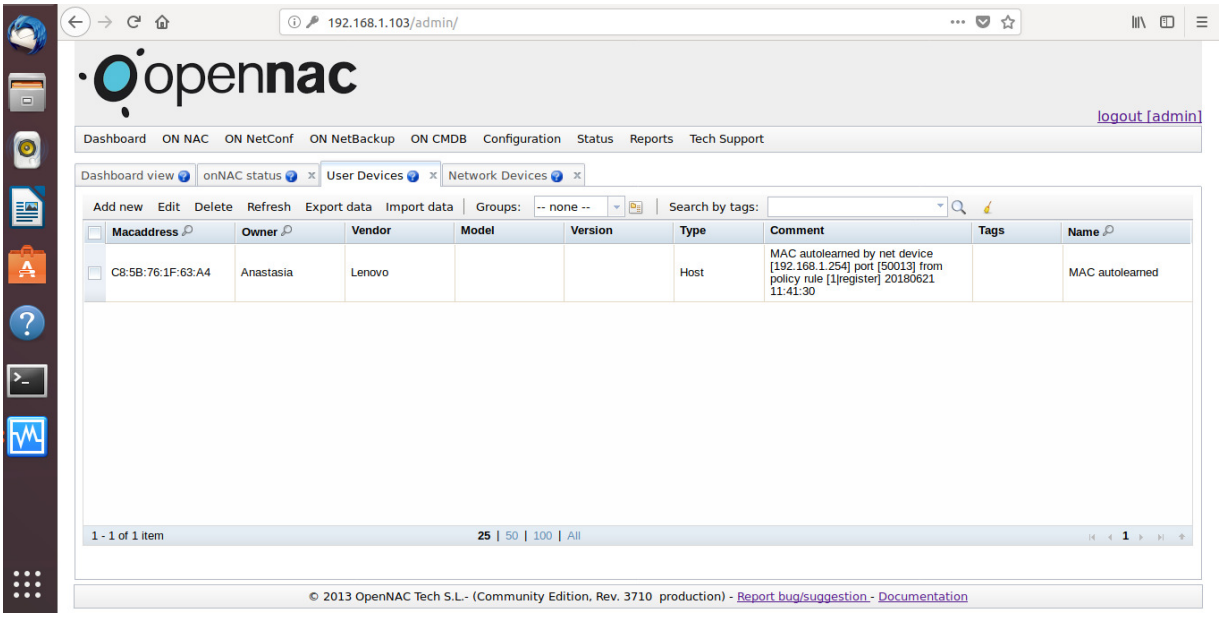


Εικόνα6.3

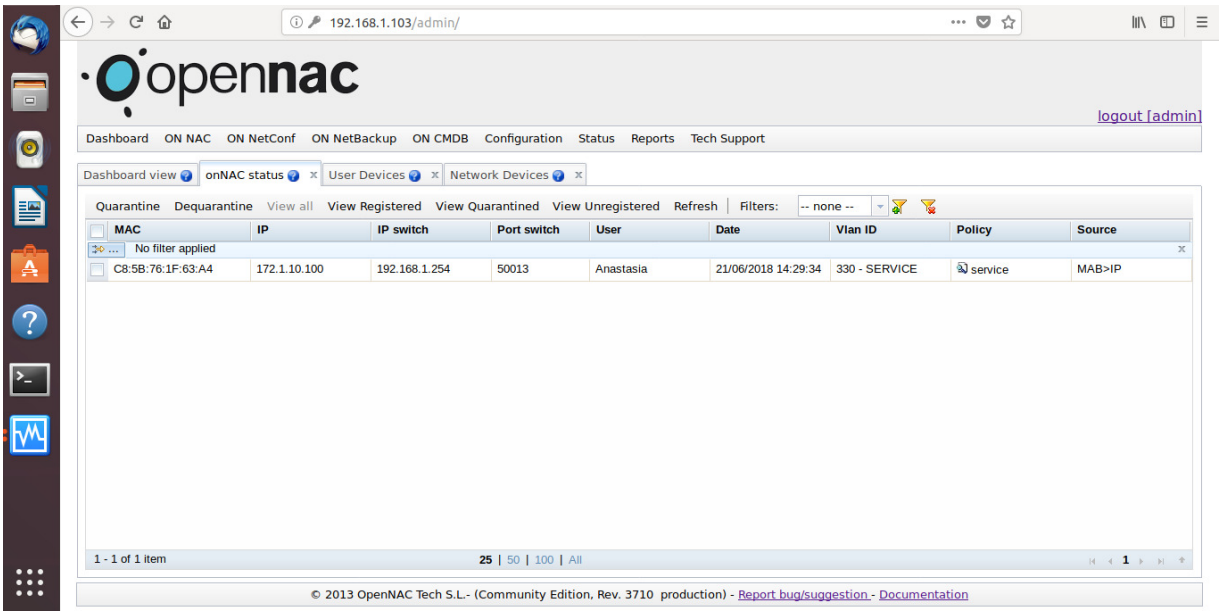
Με το πάτημα του πλήκτρου save, ο χρήστης αφού περάσει ένα μικρό χρονικό διάστημα στη συνέχεια καταχωρείται στο openNAC ως πιστοποιημένος χρήστης. Στις Εικόνες 12, 13 και14 που ακολουθούν έχουμε μια εποπτική εικόνα σχετικά με τις δικτυακές συσκευές που είναι καταχωρημένες στο δίκτυο, τους χρήστες καθώς και την κατάσταση στην οποία βρίσκεται ο εκάστοτε χρήστης είτε είναι registered, unregisteredή σε quarantine.



Εικόνα6.3



Εικόνα6.3



Εικόνα6.3

Επίλογος

Στην παρούσα εργασία παρουσιάστηκε μια μέθοδος ελέγχου ταυτότητας πρόσβασης χρηστών σε ένα δίκτυο με τη χρήση του 802.1X ξεκινώντας από τις βασικές αρχές που καθορίζουν ένα ολοκληρωμένο σύστημα port-basedαυθεντικοποίησης χρηστών μέχρι την τελική υλοποίηση ενός συστήματος ελέγχου ταυτότητας πρόσβασης χρηστών. Για τον σκοπό αυτό, έγινε χρήση τουεργαλείου openNAC, ενός ανοικτού λογισμικού NetworkAccessController.Ως συμπέρασμα βλέπουμε πως για τη δημιουργία ενός ασφαλούς δικτυακού περιβάλλοντος στο οποίο έχουμε ελεγχόμενη πρόσβαση χρηστών μέσω του 802.1X χρειάζεται να λάβουμε υπόψιν αρκετές παραμέτρους και να σχεδιάσουμε το εκάστοτε σύστημα που θα πρέπει να υλοποιηθεί με βάσει τις τρέχουσες αλλά και μελλοντικές ανάγκες των χρηστών.

Φυσικάυπάρχουνκαιάλλοιτρόποι υλοποίησης

7 Λίστα RFCs

- RFC 2284: PPP Extensible Authentication Protocol (EAP). L. Blunk - J. Vollbrecht, March 1998
- RFC 3748: Extensible Authentication Protocol (EAP). Bernard Aboba - L. Blunk - J. Vollbrecht - James Carlson - Henrik Levkowetz, June 2004
- RFC 2865:Remote Authentication Dial In User Service (RADIUS). Carl Rigney - Allan C. Rubens - William Allen Simpson - Steve Willens, June 2000
- RFC 2486:The Network Access Identifier. Bernard Aboba - Mark A. Beadles, January 1999
- RFC 4186:Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM)Subscriber Identity Modules (EAP-SIM). Henry Haverinen - Joseph Salowey, January 2006
- RFC 4187:Extensible Authentication Protocol Method for 3rd GenerationAuthentication and Key Agreement (EAP-AKA). JariArkko - Henry Haverinen, January 2006
- RFC 4793:The EAP Protected One-Time Password Protocol (EAP-POTP). Magnus Nystroem, February 2007
- RFC 4851:The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST). Nancy Cam-Winget - David McGrew - Joseph Salowey - Hao Zhou, May 2007
- RFC 4764:The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method. FlorentBersani - Hannes Tschofenig, January 2007
- RFC 4763:Extensible Authentication Protocol Method for Shared-secret Authentication and Key Establishment (EAP-SAKE). Michaela Vanderveen - HeshamSoliman, November 2006

8 Βιβλιογραφία

[1] Implementing 802.1X Security Solutions for Wired and Wireless Networks. Jim Geier – Wiley Publishing Inc. – ISBN: 978-0-470-16860-8

[2] Catalyst 2960 and2960-S Switch Command Reference – Cisco Press