Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Υπηρεσίες Δικτύων σε Πλωτά Μέσα: Εγκατάσταση και Παραμετροποίηση Υπηρεσιών Δικτύου σε Πλωτό Σκάφος** **Networking in maritime transport: Installation and configuration of network services in a yacht**
Ονοματεπώνυμο Φοιτητή	**Ιωάννης Κυριαζής**
Πατρώνυμο	**Κανάρης**
Αριθμός Μητρώου	**ΜΠΠΛ 14039**
Επιβλέπων	**Παναγιώτης Κοτζανικολάου, Επίκουρος Καθηγητής**

Ημερομηνία Παράδοσης **24 Οκτωβρίου 2019**

Τριμελής Εξεταστική Επιτροπή

Αποστόλου Δημήτριος, Αναπληρωτής Καθηγητής	Κοτζανικολάου Παναγιώτης, Επίκουρος Καθηγητής	Ψαράκης Μιχαήλ, Επίκουρος Καθηγητής

ΠΕΡΙΛΗΨΗ

Η δικτύωση πλωτών μέσων μεταφοράς απαιτεί ειδικό εξοπλισμό και τη χρήση ασύρματων τεχνολογιών δικτύωσης, με αυξημένο κόστος σε σχέση με άλλα περιβάλλοντα εφαρμογής. Παρόλα αυτά, η εξέλιξη της τεχνολογίας δικτύων, δίνει σήμερα τη δυνατότητα εγκατάστασης υπηρεσιών δικτύου όχι μόνο σε μεγάλης κλίμακας πλωτά μέσα, αλλά και μικρής κλίμακας, όπως είναι τα σκάφη αναψυχής. Στην εργασία αυτή θα γίνει μελέτη υποδομών και υπηρεσιών δικτύου για πλωτά μέσα μικρής κλίμακας. Μέσα από το παράδειγμα χρήσης ενός σκάφους αναψυχής. Θα εξετάσουμε την μεθοδολογία και τα εργαλεία που χρησιμοποιούνται για την δημιουργία τους και θα αναπαραστήσουμε εικονικά την λειτουργία αυτών των υποδομών.

ABSTRACT

Networking in the maritime environment requires specialized infrastructures and wireless networking technologies with increased cost. However, the relative technological advances, allow for the efficient use of networking services even in small scale maritime transport means. In this thesis we will study, through simulation tools the methodologies and tools that may be applied in order to install and configure network infrastructures and services in small scale vessels like maritime yachts.

Περιεχόμενα

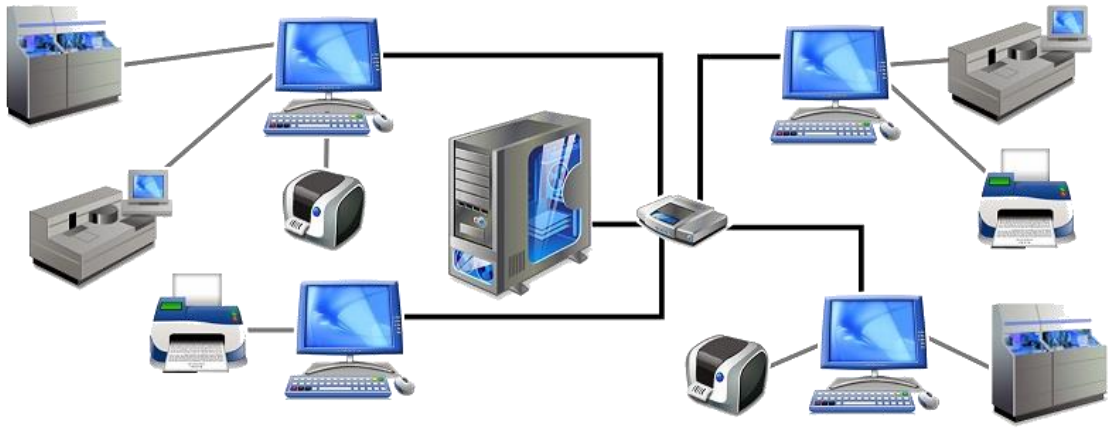
Πίνακας Εικόνων

Πίνακας Πινάκων

Κεφάλαιο 1: Εισαγωγή

Η ανάγκη για υποδομές δικτύων μεγαλώνει καθώς η τεχνολογία εξελίσσεται. Πλέον στα οικιακά δίκτυα έχουμε πολλαπλές τελικές συσκευές (end devices) οι οποίες είναι διασυνδεδεμένες ενώ συνδέονται και με το διαδίκτυο.

Η δυνατότητα διασύνδεσης των συσκευών μεταξύ τους και με το διαδίκτυο επεκτείνει τις προσφερόμενες υπηρεσίες αυξάνοντας παράλληλα τους κινδύνους ασφάλειας.



Εικόνα 1: απεικόνιση τοπικού δικτύου σε γραφείο
(πηγή **https://rainestech.com/services/home-office-network)**

Τα οφέλη από την χρήση εσωτερικών δικτύων σε μια επιχείρηση είναι πολλαπλά καθώς προσφέρει μια πληθώρα υπηρεσιών όπως:

Κοινή χρήση αρχείων: Με την κοινή χρήση των αρχείων μπορούμε να αποκτήσουμε πρόσβαση σε αρχεία τα οποία δεν βρίσκονται στον υπολογιστή μας Ένα δίκτυο καθιστά εύκολο για όλους να έχουν πρόσβαση στο ίδιο αρχείο και να αποτρέπουν τους ανθρώπους από τυχαία δημιουργία διαφορετικών εκδόσεων.

Κοινή χρήση εκτυπωτή: Σε περιβάλλον εργασίας η χρήση εκτυπωτή είναι απαραίτητη. Οι εκτυπωτές που χρησιμοποιούνται σε επιχειρήσεις είναι ακριβοί τόσο για την αγορά τους όσο και για τα αναλώσιμα .Έχοντας στον νου μας ότι δεν μπορούμε να παρέχεται ένας εκτυπωτής ανά υπάλληλο καθώς δημιουργεί τεράστιο κόστος στην εταιρεία, επιλέγεται η χρήση δικτυακού εκτυπωτή αφού επιτρέπει σε ολόκληρα τμήματα να χρησιμοποιούν ένα εκτυπωτή

Επικοινωνία και συνεργασία: Είναι δύσκολο για τους ανθρώπους να συνεργαστούν εάν κανείς δεν ξέρει τι κάνει κάποιος άλλος. Ένα δίκτυο επιτρέπει στους εργαζόμενους να μοιράζονται αρχεία, να βλέπουν το έργο των άλλων και να ανταλλάσσουν ιδέες πιο αποτελεσματικά. Σε μια μεγαλύτερη εταιρία, χρησιμοποιούνται εργαλεία ηλεκτρονικού ταχυδρομείου και άμεσων μηνυμάτων για να επιτυγχάνεται γρήγορη επικοινωνία και αποθήκευση μηνυμάτων για μελλοντική αναφορά.

Οργάνωση: Η οργάνωση των προγραμμάτων των εργαζομένων στα πλαίσια μιας επιχείρησης μπορεί να αποδειχθεί δύσκολο καθήκον. Με την χρήση εσωτερικού δικτύου και κατάλληλου λογισμικού γίνεται κατορθωτή η οργάνωση και ο συντονισμός με σχεδόν αυτόματο τρόπο. Το

λογισμικό μπορεί να περιλαμβάνει και άλλες χρήσιμες λειτουργίες, όπως τα κοινόχρηστα βιβλία διευθύνσεων και τις λίστες υποχρεώσεων.

Απομακρυσμένη πρόσβαση: Η κατοχή του δικού μας δικτύου επιτρέπει μεγαλύτερη κινητικότητα διατηρώντας παράλληλα το ίδιο επίπεδο παραγωγικότητας. Με την απομακρυσμένη πρόσβαση στη θέση τους, οι χρήστες μπορούν να έχουν πρόσβαση στα ίδια αρχεία, δεδομένα και μηνύματα ακόμα και όταν δεν βρίσκονται στο γραφείο. Αυτή η πρόσβαση μπορεί ακόμη να παραχωρηθεί σε φορητές συσκευές κινητής τηλεφωνίας.

Προστασία δεδομένων: Η δημιουργία τακτικών αντιγράφων ασφαλείας των δεδομένων του υπολογιστή μας είναι απαραίτητη σε κάθε επίπεδο χρήσης από το οικιακό σύστημα έως αυτό μιας μεγάλης επιχείρησης. Ένα δίκτυο διευκολύνει τη δημιουργία αντιγράφων ασφαλείας όλων των δεδομένων σε έναν εξωτερικό διακομιστή , ένα σύνολο κασέτας, CD ή άλλα συστήματα δημιουργίας αντιγράφων ασφαλείας. (Φυσικά, μια άλλη πτυχή της προστασίας των δεδομένων είναι η ασφάλεια των δεδομένων.)[15]

Όλα τα παραπάνω αναφέρονται σε κτήρια, γραφεία και σπίτια .Αν και θεωρητικά τα ίδια ισχύουν και για ένα πλωτό σκάφος, θα πρέπει να ληφθεί υπόψιν για το συγκεκριμένο σενάριο χρήσης που εξετάζουμε ,αφενός ότι θα είναι μια κινουμένη εγκατάσταση αφετέρου ότι προκύπτουν παράγοντες στην εγκατάσταση που δεν υπάρχουν σε γραφεία, όπως:

- Επιρροή από καιρικές συνθήκες(καταιγίδες)
- Ο εξοπλισμός μας έχει μεγάλες πιθανότητες να δεχτεί μετακίνηση λόγο κύματος
- Υγρασία
- Λόγο κατασκευής η δυσκολία αλλαγής η αφαίρεση της δομημένης καλωδιακής

Τέλος ένα εξίσου σημαντικό ζήτημα είναι ότι η εγκατάσταση χρειάζεται να εξυπηρετεί και τον υπόλοιπο εξοπλισμό που βρίσκεται μέσα στο σκάφος και που είναι εξοπλισμός τρίτου μέρους δηλαδή εξοπλισμός που έχει εγκατασταθεί από άλλο πάροχο. Τέτοιος εξοπλισμός μπορεί να περιλαμβάνει:

- Συστήματα ήχου και εικόνας
- Συστήματα πλοήγησης
- Μηχανογράφηση
- Συστήματα ασφάλειας (συναγερμός και συστήματα ειδοποίησης)

1.1 Στόχος Διπλωματικής εργασίας

Ο στόχος αυτής της διπλωματικής εργασίας είναι η ανάλυση της εγκατάστασης από την πλευρά του εγκαταστάτη. Να παρουσιάσουμε την διαδικασία του σχεδιασμού ,την επιλογή των υλικών για την εγκατάσταση και τις δυσκολίες που προκύπτουν από αυτά .Επιπρόσθετα θα γίνει ανάλυση στις διαδικασίες ασφάλειας και καλή λειτουργίας του έργου. Μαζί με όλες τις παραμετροποιήσεις που θα γίνουν στον δικτυακό μας εξοπλισμό. Τέλος θα υπάρξει και εικονική απεικόνιση του έργου σε περιβάλλον GNS3 και VMware δημιουργώντας έτσι ένα οδηγό για οποίον θα ήθελε να πραγματοποίηση μια τέτοια διαδικασία.

1.2 Δομή της εργασίας

Στο 2ο κεφάλαιο θα ασχοληθούμε με την σχεδίαση και υλοποίηση της εγκατάστασης, θα αναλύσουμε την διαδικασία σχεδιασμού τι πρέπει να λάβουμε υπόψιν μας όταν σχεδιάζουμε τέτοια εγκατάσταση, τις δυσκολίες που προκύπτουν σε ένα τέτοιο έργο και πως πρέπει να τις αντιμετωπίζουμε. Ύστερα θα ασχοληθούμε με την επιλογή των υλικών αλλά και τον εξοπλισμό που θα χρειαστούμε και γιατί. Τέλος θα δείξουμε στα υπόλοιπα κεφαλαία πως έγινε η υλοποίηση και θα αναφέρουμε τι κίνδυνους έχουμε να αντιμετωπίσουμε σε μια και εγκατάσταση και τι μπορούμε να κάνουμε να την προστατέψουμε.

Στο 3ο κεφάλαιο θα παρουσιάσουμε τον εργαλεία που θα χρησιμοποιήσουμε για την εικονική αναπαράσταση του δικτύου Θα δείξουμε πως έγινε η εγκατάσταση και παραμετροποίηση των εργαλείων GNS3 και VMware. Τέλος θα δείξουμε πως έγινε το στήσιμο του εικονικού radius Server.

Στο 4ο κεφάλαιο θα ασχοληθούμε με την δρομολόγηση και μεταγωγή (Routing and Switching) του δικτύου. Θα αναλύσουμε ποια μορφή σχεδιασμού δίκτυο διαλέξαμε και γιατί, θα αναλύσουμε την παραμετροποίηση που θα κάνουμε στον εξοπλισμό μας και σε τι θα χρησιμεύει στην εγκατάσταση μας. Τέλος θα δείξουμε πως είναι στημένος φυσικά ο εξοπλισμός στον χώρο μας και γιατί επιλέξαμε αυτόν τον τρόπο.

Στο 5ο κεφάλαιο αναλύσουμε την ασφάλεια της εγκατάσταση μας θα δούμε γενικά ποιες απειλές έχουμε να αντιμετωπίσουμε στην εγκατάσταση μας. Τι εξοπλισμό πρέπει να χρησιμοποιήσουμε για να διασφαλίσουμε την σωστή λειτουργία της εγκατάστασης μας και τέλος θα δούμε τα Εικονικά ιδιωτικά δίκτυα(VPN) Πως χρησιμεύουν στην ασφάλεια του δικτύου μας ποια είναι τα είδη και η λειτουργία τους και πως στήνονται και σε επίπεδο router και σε επίπεδο Firewall Cisco ASA .

Επίσης θα δούμε τα Συστήματα ελέγχου πρόσβασης, θα αναλύσουμε τι είναι, σε τι είναι χρήσιμα, ποια είδη υπάρχουν καθώς και τα πλεονεκτήματά και μειονεκτήματά τους .Τέλος θα δείξουμε ποιο διαλέξαμε και πως δουλεύει στην εγκατάσταση μας .

Τέλος στο 6ο κεφάλαιο έχουμε συγκεντρωμένα όλα τα αρχεία παραμετροποιήσεων και τα συμπεράσματα μας από την όλη εγκατάσταση

Κεφάλαιο 2: Σχεδίαση της Εγκατάστασης

2.1 Γενική προσέγγιση εγκατάσταση υποδομής δικτύου

Το πρώτο βήμα για την ανάπτυξη ενός σχεδίου είναι η αξιολόγηση των λειτουργικών απαιτήσεων του δικτύου καθώς και η εξέταση του τρόπου με τον οποίο η επιχείρησή ενδέχεται να αλλάξει με την πάροδο του χρόνου. Στη συνέχεια θα αναφερθούμε στους τρόπους που θα χρησιμοποιηθούν για να επιτευχθεί το επιδιωκόμενο αποτέλεσμα. Οι τρείς γενικές φάσεις αφορούν τις απαιτήσεις χρήσης, την συλλογή στοιχείων και το σχεδιασμό για το μέλλον.

Εξέταση των απαιτήσεων χρήσης: Προσδιορισμός του αριθμό των ατόμων που θα χρησιμοποιήσουν το δίκτυο ώστε να αποκτήσουμε μια γενική ιδέα για τους υπολογιστές και τα περιφερειακά που θα χρειαστεί να υποστηρίξει. Λαμβάνουμε υπόψη πώς οι χρήστες θα αλληλεπιδρούν με το σύστημα για τον καθορισμό των λειτουργιών που θα χρειαστούν. Για παράδειγμα, ποιο είδος πρόσβασης απαιτείται στο δίκτυο (π.χ. ο κάθε χρήστης θα έχει δικό του υπολογιστή, ή πολλοί χρήστες θα μοιράζονται τον ίδιο υπολογιστή;), Θα χρειαστεί κάποιος από τους χρήστες να αποκτήσει πρόσβαση στο δίκτυο από απόσταση; (π.χ. από το σπίτι ή άλλους δικτυακούς τόπους).

Συλλογή στοιχείων: Καταγραφή των αναγκών των διαφόρων ομάδων και τμημάτων του υπο εξέταση οργανισμού στο σχέδιο δικτύου. Αρχικά καθορίζονται οι απαιτήσεις κάθε ομάδας και το σχετικό κόστος ενσωμάτωσης των διαφορετικών απαιτήσεων στο σχέδιο δικτύου. Το μέτρο υπολογισμού αφορά συνήθως το κόστος ή τον χρόνο που εξοικονομείται.

Σχέδιο για το μέλλον: Στην 3η γενική φάση προσπαθούμε να υπολογίσουμε και να ενσωματώσουμε, όσο αυτό είναι εφικτό, τα σχέδια επεκτασιμότητας. Με απλά λόγια να πάρουμε υπόψη την κατεύθυνση που θα αναλάβει η οργάνωση μας στο εγγύς μέλλον (3-5 χρόνια). Για να γίνει κάτι τέτοιο κατορθωτό προσδιορίζουμε τυχόν σχέδια που ενδέχεται να επηρεάσουν τις ανάγκες του δικτύου μας (π.χ. νέο προσωπικό ή εθελοντές, επέκταση γραφείου, απομακρυσμένη εργασία ή εγκατάσταση νέων πακέτων λογισμικού). Προβλέποντας κατά την σχεδίαση τις πιθανές επεκτάσεις έχει σαν αποτέλεσμα η αντικατάσταση ενός ανεπαρκούς δικτύου αργότερα να είναι λιγότερο δαπανηρή και χρονοβόρα.

Σχεδίαση

- Πόσα άτομα θα χρησιμοποιήσουν το δίκτυο;
- Πόσοι χρήστες είναι τοπικοί;
- Πόσοι χρήστες είναι απομακρυσμένοι ή εκτός χώρου και απαιτούν πρόσβαση στο δίκτυο;
- Πόσοι υπολογιστές θα συνδεθούν στο δίκτυο;
- Πόσες συσκευές (υπολογιστές, διακομιστές, σαρωτές, εκτυπωτές κ.λπ.) απαιτούν κάρτα δικτύου;
- Πώς σκοπεύουμε να έχουν πρόσβαση οι απομακρυσμένοι χρήστες στο δίκτυο;
- Ποιες εφαρμογές βασίζονται σε διακομιστές (π.χ. βάσεις δεδομένων, ηλεκτρονικό ταχυδρομείο) σκοπεύετε να εκτελέσετε στο δίκτυο; Ποιες είναι οι ελάχιστες απαιτήσεις υλικού για αυτές τις εφαρμογές που βασίζονται σε διακομιστές;

- Ποιες είναι οι προδιαγραφές των διακομιστών που σκοπεύετε να εγκαταστήσετε στο δίκτυο (π.χ. ποσότητα μνήμης, ταχύτητα επεξεργαστή κ.λπ.);
- Έχουμε αγοράσει επαρκείς άδειες χρήσης για την εκτέλεση όλου του λογισμικού σε διακομιστές και υπολογιστές-πελάτες;

Απαιτήσεις υλικού δικτύου

- Ποιες άλλες συσκευές θα υποστηρίξει το δίκτυό μας (π.χ. εφεδρικές συσκευές, αδιάλειπτα τροφοδοτικά, εκτυπωτές δικτύου κ.λπ.);
- Έχουμε αρκετά σημεία δικτύου για αυτές τις συσκευές δικτύου;
- Έχουν οι κόμβοι ή οι διακόπτες αρκετές θύρες για τον αριθμό των συνδέσεων που θα χρειαστούν; Υπάρχει χώρος για ανάπτυξη;

Σχεδιασμός δικτύου

- Ποια τοπολογία δικτύου θα χρησιμοποιηθεί;
- Έχουν όλοι οι σταθμοί εργασίας τις σωστές κάρτες διασύνδεσης δικτύου (NICs) για να υποστηρίξουν αυτήν την τεχνολογία
- Ποιο είδος καλωδίωσης θα χρησιμοποιήσουμε (π.χ. CAT 6, οπτική ίνα) ή θα είναι κατάλληλο ένα ασύρματο δίκτυο;
- Πού θα βρίσκονται τα καλώδια δικτύου;
- Πού θα εντοπίζονται οι ακόλουθες συσκευές, διακομιστές, κόμβους ή διακόπτες, εκτυπωτές, τείχη προστασίας και δρομολογητές, μόντεμ κ.λπ .;

2.2 Μοντέλο αναφοράς OSI

Για να μπορέσουμε να καταλάβουμε πως λειτουργεί ένα τηλεπικοινωνιακό δίκτυο και να μπορούμε να σχεδιάσουμε πάνω σε αυτό θα πρέπει σε πρώτη φάση να γνωρίζουμε τι είναι το μοντέλο OSI και πώς μπορούν να αξιοποιηθούν οι πληροφορίες που μας παρέχει.

Το μοντέλο OSI είναι μια ιεραρχική δομή επτά επιπέδων που καθορίζει τις προδιαγραφές επικοινωνίας μεταξύ δύο υπολογιστών, ορίζοντας επακριβώς τον σκοπό κάθε επιπέδου αλλά και τα χρησιμοποιούμενα πρωτόκολλα που τυποποιήθηκε πλέον ως πρότυπο ISO 7498-1. Θεωρήθηκε ότι θα επέτρεπε τη λειτουργική συνεργασία μεταξύ ποικίλων ψηφιακών συσκευών που ήταν διαθέσιμες στην αγορά. Το μοντέλο επιτρέπει σε όλα τα στοιχεία ενός δικτύου να συλλειτουργούν, με κάθε στοιχείο να υλοποιεί ένα ή περισσότερα πρωτόκολλα δικτύωσης, ανεξάρτητα από το ποιος είναι ο κατασκευαστής τους. Περί τα τέλη της δεκαετίας του 1980 ο οργανισμός ISO συνιστούσε την εφαρμογή του μοντέλου OSI ως κοινώς αποδεκτού υποδείγματος σχεδιασμού δικτύων.

Ωστόσο εκείνη την εποχή η στοίβα πρωτοκόλλων TCP/IP, η οποία βασιζόταν σε ελαφρώς διαφορετική διαστρωμάτωση επιπέδων, ήταν ήδη επί πολύ καιρό σε ευρεία χρήση. Το TCP/IP ήταν θεμελιώδες για το δίκτυο ARPANET και τα άλλα δίκτυα που εξελίχθηκαν στο σημερινό Διαδίκτυο[1]. Ως αποτέλεσμα το μοντέλο OSI παραμερίστηκε και σήμερα μόνο ένα υποσύνολό

του χρησιμοποιείται ακόμη. Η επικρατούσα αντίληψη είναι ότι οι περισσότερες προδιαγραφές του είναι περίπλοκες και η πλήρης λειτουργικότητά του θα χρειαζόταν μεγάλο χρόνο κατασκευής, αν και συνεχίζουν να υπάρχουν σθεναροί υποστηρικτές του.

Μοντέλο OSI			
	Μονάδα δεδομένων	**Επίπεδο**	**Λειτουργία**
Λογισμικό	Δεδομένα	7. Εφαρμογών	Παρέχεται στις εφαρμογές πρόσβαση στο δίκτυο
		6. Παρουσίασης	Αναπαράσταση δεδομένων και κρυπτογράφηση
		5. Συνόδου	Έλεγχος του διαλόγου μεταξύ των άκρων της επικοινωνίας
	Τμήμα	4. Μεταφοράς	Αξιόπιστη επικοινωνία από άκρο σε άκρο
Υλικό	Πακέτο	3. Δικτύου	Καθορισμός διαδρομών και λογικών διευθύνσεων των κόμβων στα πλαίσια ενός διαδικτύου
	Πλαίσιο	2. Ζεύξης δεδομένων	Φυσική διευθυνσιοδότηση (MAC & LLC)
	Bit	1. Φυσικό	Δυαδική μετάδοση σήματος μέσω του φυσικού μέσου

Πίνακας 1: Το μοντέλο OSI πηγη www.wikipedia.com

Το μοντέλο OSI υποδιαιρεί τις λειτουργίες ενός τηλεπικοινωνιακού δικτύου σε μια «κατακόρυφη» στοίβα από επίπεδα, για το καθένα από τα οποία μπορεί να οριστεί κάποιο πρωτόκολλο σε μία συγκεκριμένη υλοποίηση. Κάθε επίπεδο αξιοποιεί τις λειτουργίες του κατώτερού του στη στοίβα επιπέδου, ενώ στόχος του είναι να παρέχει λειτουργικότητα στο αμέσως ανώτερο επίπεδό του. Μία συγκεκριμένη υλοποίηση του μοντέλου, με καθορισμένα πρωτόκολλα για κάθε επίπεδο, ονομάζεται στοίβα πρωτοκόλλων ή απλά στοίβα. Το κάθε πρωτόκολλο υλοποιείται είτε σε υλικό είτε σε λογισμικό. Συνήθως τα κατώτερα επίπεδα υλοποιούνται στο υλικό ενώ τα ανώτερα σε λογισμικό.

Το μοντέλο OSI είναι στενά συσχετισμένο με τον κλάδο της επιστήμης υπολογιστών και τη δικτύωση υπολογιστών. Το βασικό χαρακτηριστικό του είναι η διασύνδεση μεταξύ των επιπέδων, η οποία υπαγορεύει τις προδιαγραφές της αλληλεπίδρασής τους. Αυτό σημαίνει ότι ένα επίπεδο υλοποιημένο με κάποιο συγκεκριμένο πρωτόκολλο μπορεί να συνεργαστεί με το γειτονικό του στη στοίβα επίπεδο, το οποίο υλοποιείται με κάποιο άλλο πρωτόκολλο, υπό την προϋπόθεση ότι οι προδιαγραφές του καθενός έχουν δημοσιευθεί και έχουν γίνει αντιληπτές σωστά. Αυτές οι προδιαγραφές είναι τυπικά γνωστές ως RFC (Requests for Comments) και αποτελούν πρότυπα του Διεθνούς Οργανισμού Τυποποίησης ISO.

Συνήθως τα επίπεδα είναι αυστηρά διαχωρισμένα μεταξύ τους: αξιοποιούν τις υπηρεσίες του κατώτερου επιπέδου τους και προσφέρουν υπηρεσίες στο ανώτερο τους, αλλά το καθένα δεν παρεμβαίνει στις λειτουργίες του άλλου· πιθανόν να μη γνωρίζει καν γι' αυτές. Αυτός ο λογικός διαχωρισμός των επιπέδων διευκολύνει πολύ τη μελέτη της συμπεριφοράς των πρωτοκόλλων και επιτρέπει τη σχεδίαση πολύπλοκων και αξιόπιστων στοιβών πρωτοκόλλων. Ορισμένες φορές όμως αυτή η αρχή ανεξαρτησίας των επιπέδων παραβιάζεται, για λόγους βελτιστοποίησης της απόδοσης ή αύξησης της λειτουργικότητας, με πρωτόκολλα διαφορετικών επιπέδων να συγχωνεύονται ή να παρεμβαίνουν το ένα στη λειτουργία του άλλου.

Στην εγκατάσταση μας θα επικεντρωθούμε στα εξής επίπεδα του μοντέλου OSI:

Επίπεδο 1: Φυσικό

Το φυσικό επίπεδο (αγγλ. physical layer) ορίζει όλες τις ηλεκτρικές και φυσικές προδιαγραφές της επικοινωνίας. Σ’ αυτές περιλαμβάνονται οι σχηματισμοί των ακίδων, οι επιτρεπτές τάσεις, οι προδιαγραφές των καλωδίων κλπ. Συσκευές φυσικού επιπέδου είναι οι διανεμητές, οι επαναλήπτες (αγγλ. repeaters), οι κάρτες δικτύου, οι προσαρμοστές διαύλου (αγγλ. bus adapters). Οι κυριότερες λειτουργίες και υπηρεσίες του φυσικού επιπέδου είναι:

- Έναρξη και τερματισμός της ηλεκτρικής σύνδεσης μιας επικοινωνιακής συσκευής.
- Συμμετοχή σε διαδικασίες όπου οι επικοινωνιακές συσκευές εξυπηρετούν αποτελεσματικά πολλούς χρήστες (πολυπλεξία). Επιλύονται προβλήματα προτεραιότητας πρόσβασης και ελέγχου ροής δεδομένων.
- Διαμόρφωση και αποδιαμόρφωση των ψηφιακών δεδομένων κατά τη μετάδοση από συσκευή σε συσκευή. Για παράδειγμα, τα ψηφιακά ηλεκτρικά σήματα μπορεί να ταξιδέψουν ως αναλογικά σε χάλκινο καλώδιο, μετά σε οπτική ίνα, μετά να μεταδοθούν από ραδιοζεύξη ή δορυφορικά, να φθάσουν πάλι αναλογικά σε χάλκινο καλώδιο και να γίνουν ψηφιακά στον παραλήπτη.[9]

Επίπεδο 2: Ζεύξης Δεδομένων

Το επίπεδο ζεύξης (αγγλ. data link layer) δεδομένων παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά δεδομένων από μια συσκευή ενός τοπικού δικτύου σε άλλη, αλλά και για την ανίχνευση και διόρθωση σφαλμάτων που συμβαίνουν στο φυσικό επίπεδο. Οι μη ιεραρχημένες διευθύνσεις των συσκευών εδώ είναι οι φυσικές (π.χ. MAC διευθύνσεις), δηλαδή είναι προκαθορισμένες και αποθηκευμένες στις κάρτες δικτύου των επικοινωνούντων κόμβων από το εργοστάσιο.

Το πιο γνωστό πρότυπο αυτού του επιπέδου είναι το Ethernet, για τοπικά δίκτυα. Άλλα παραδείγματα πρωτοκόλλων ζεύξης δεδομένων αποτελούν τα:

- HDLC και ADCCP, για συνδέσεις από-σημείο-σε-σημείο (αγγλ. point-to-point).
- 802.11, για ασύρματα τοπικά δίκτυα.

Στα τοπικά δίκτυα της οικογένειας πρωτοκόλλων IEEE 802, και σε κάποια άλλα όπως το FDDI, αυτό το επίπεδο μπορεί να διαιρεθεί σε δύο μικρότερα:

- Ένα επίπεδο ελέγχου πρόσβασης στο κοινό μέσο, το υποεπίπεδο MAC (αγγλ. Media Access Control, Έλεγχος Πρόσβασης Μέσου)
- Ένα ανώτερο επίπεδο ελέγχου λογικών συνδέσεων, το υποεπίπεδο LLC (αγγλ. Logical Link Control, Έλεγχος Λογικών Ζεύξεων), όπου επικρατεί καθολικά το πρωτόκολλο IEEE 802.2 ανεξάρτητα από το υποκείμενο πρωτόκολλο MAC ή φυσικού επιπέδου.

Στο επίπεδο αυτό λειτουργούν οι δικτυακές γέφυρες (αγγλ. bridge) και οι δικτυακοί διακόπτες (αγγλ. switch). Η συνδεσιμότητα παρέχεται μόνο για κόμβους που συνδέονται στο ίδιο κοινό μέσο (τοπικό δίκτυο ή σύνδεση από-σημείο-σε-σημείο).

Επίπεδο 3: Δικτύου

Το επίπεδο δικτύου (αγγλ. network layer) παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά στοιχειοσειρών δεδομένων μεταβλητού μήκους από μια προέλευση σε έναν προορισμό, μέσα από ένα ή περισσότερα ενδιάμεσα δίκτυα, ενώ διατηρεί την ποιότητα εξυπηρέτησης που απαιτεί το επίπεδο μεταφοράς. Το επίπεδο δικτύου εκτελεί λειτουργίες δρομολόγησης, με πιθανές κατατμήσεις / αποτμηματοποιήσεις, και αναφέρει σφάλματα σχετικά με την παράδοση των πακέτων. Οι δρομολογητές (αγγλ. routers) λειτουργούν στο επίπεδο αυτό· διακινώντας δεδομένα σε διασυνδεδεμένα δίκτυα έκαναν το Διαδίκτυο πραγματικότητα. Υπάρχουν και δικτυακοί διακόπτες που σχετίζονται με τις διευθύνσεις (IP). Εδώ υπάρχει μια λογική οργάνωση και τις τιμές των διευθύνσεων τις καθορίζει ιεραρχικά ο τεχνικός των επικοινωνιών. Το πλέον αναγνωρίσιμο παράδειγμα πρωτοκόλλου δικτύου είναι το Πρωτόκολλο Διαδικτύου (αγγλ. Internet Protocol, IP).[9]

Επίπεδο 4: Μεταφοράς

Το επίπεδο μεταφοράς (αγγλ. transport layer) διεκπεραιώνει τη μεταφορά των δεδομένων από χρήστη σε χρήστη, απαλλάσσοντας έτσι τα ανώτερα επίπεδα από κάθε φροντίδα να προσφέρουν αξιόπιστη μεταφορά δεδομένων από το ένα άκρο της επικοινωνίας στο άλλο. Το επίπεδο μεταφοράς ελέγχει την αξιοπιστία ενός χρησιμοποιούμενου καναλιού με έλεγχο ροής (αγγλ. flow control), κατάτμηση και αποτμηματοποίηση (αγγλ. segmentation / desegmentation), καθώς και έλεγχο σφαλμάτων (αγγλ. error control). Ορισμένα πρωτόκολλα καταγράφουν καταστάσεις και συνδέσεις, οπότε κρατούν λογαριασμό των πακέτων και επανεκπέμπουν αυτά που δεν παρελήφθησαν σωστά. Τα διάφορα πρωτόκολλα μορφοποιούν διαφορετικά τα εκπεμπόμενα πακέτα πληροφοριών, αλλά τα προς αποστολή δεδομένα παραλαμβάνονται αρχικά από τα ανώτερα επίπεδα.[9]

Το συνηθέστερο παράδειγμα πρωτοκόλλου μεταφοράς είναι το TCP (αγγλ. Transmission Control Protocol, πρωτόκολλο ελέγχου μετάδοσης). Άλλα πρωτόκολλα μεταφοράς είναι τα UDP (αγγλ. User Datagram Protocol, πρωτόκολλο για ασυνδεσμική αποστολή δεδομένων, SCTP (αγγλ. Stream Control Transmission Protocol, πρωτόκολλο ελέγχου της ροής μετάδοσης), κλπ.

2.3 Ανάγκες Έργου - Έλεγχος πριν την Εγκατάσταση

2.3.1 Περιγραφη του Εργου

Το σενάριο χρήσης αφορά ένα σκάφος αναψυχής το οποίο ενοικιάζεται σε εταιρείες, ιδιώτες και οργανισμούς. Το σκάφος έχει κατασκευαστεί πριν από 25 χρονιά και η εγκατάσταση των δικτυών έγινε πριν από 12 χρονιά.

Οι απαιτήσεις του έργου είναι οι εξής:

- Αξιολόγηση της ήδη υπάρχουσας δικτυακής εγκατάστασης
- Έλεγχος και πιστοποίησης των καλωδίων της δομημένης καλωδίωσης
- Έλεγχος λειτουργίας και εμβέλειας του ασυρμάτου δικτύου
- Επέκταση και αναβάθμιση του ασυρμάτου δικτύου
- Εφαρμογή συσκευών ασφάλισης δικτυών(firewall)
- Διαχωρισμός πρόσβασης στο ασύρματο δίκτυο
- Δια λειτουργικότητα της δικτυακής εγκατάστασης με την νέα οπτικό ακουστική εγκατάσταση

Πριν ξεκινήσει οποιοδήποτε διαδικασία η τεχνική εταιρεία πρέπει να λάβει γραπτή τεκμηρίωση της υπάρχουσας εγκατάστασης εφόσον υπάρχει είτε από τον ιδιοκτήτη είτε από την προηγουμένη τεχνική εταιρεία.

Έχοντας συμφωνήσει στις απαιτήσεις του έργου και έχοντας λάβει όλη την σχετική τεκμηρίωση του έργου, η τεχνική εταιρεία είναι έτοιμη να ξεκινήσει την διαδικασία του έργου

2.3.2 Ελεγχος πριν την εγκατασταση (Site Survey- Wireless Site Survey)

Μια εγκατάσταση πρέπει πάντα να ξεκινάει με την διαδικασία του **Site Survey** το οποίο αφορά την επιθεώρηση της περιοχής όπου προτείνεται η εργασία καθώς και την συλλογή πληροφοριών για ένα σχέδιο ή εκτίμηση για την ολοκλήρωση των αρχικών απαιτήσεων. Στην περίπτωση του σεναρίου χρήσης που παρουσιάζεται στην εργασία αυτή η τοποθεσία είναι ένα πλωτό σκάφος .Οι περιοχές πρέπει να ελεγχθούν είναι τα επίπεδα του σκάφους.

Από το **Site Survey** προέκυψαν τα εξής:

- Τέσσερα επίπεδα (Crew Deck Lower Deck, Upper Deck ,Sun Deck)
- Lower Deck Upper Deck και Crew Deck, είναι τοποθεσίες κλειστές και δεν υπάρχει κίνδυνος υγρασίας. Το Lower Deck έχει 13 καμπίνες καλεσμένων η κάθε μια με δικιά της θύρα ethernet Crew Deck έχει 10 καμπίνες για το προσωπικό αλλά δεν διαθέτει θύρα ethernet Τέλος το Upper deck φιλοξενεί τις

καμπίνες του ιδιοκτήτη και των στελεχών του σκάφους και κάθε δωμάτιο διαθέτει δικιά του θύρα ethernet

- Sun Deck είναι ανοιχτός χώρος χωρίς προστασία
- Υπάρχουν δυο αίθουσες από καταλήγει η δομημένη καλωδίωση του σκάφους
- Μια αίθουσα οπού βρίσκεται όλη η πληροφοριακή υποδομή του σκάφους (Servers ,Backup)
- 10 Ασύρματες κεραίες
- Γέφυρα οπού φιλοξενεί όλο τον εξοπλισμό πλοήγησης

Έχοντας ολοκληρώσει το Site Survey του χώρου προχωράμε στο στο **Wireless Site Survey** καθώς μια από τις απαιτήσεις του πελάτη είναι ο έλεγχος του υπάρχοντος ασυρμάτου δικτύου και η αναβάθμιση του.

Τα **Wireless Site Survey** συνήθως διεξάγονται χρησιμοποιώντας λογισμικό υπολογιστή που συλλέγει και αναλύει μετρήσεις WLAN και χαρακτηριστικά φάσματος ραδιοσυχνοτήτων. Πριν από μια έρευνα, ένα σχέδιο ορόφου ή χάρτης τοποθεσίας εισάγεται σε μια εφαρμογή έρευνας ιστότοπου και βαθμονομείται για να οριστεί η κλίμακα. Κατά τη διάρκεια μιας έρευνας, ένας επιθεωρητής περπατά την εγκατάσταση με ένα φορητό υπολογιστή που καταγράφει συνεχώς τα δεδομένα. Ο επιθεωρητής είτε επισημάνει τη σημερινή θέση στο χάρτη με το χέρι, κάνοντας κλικ στο σχεδιάγραμμα, είτε χρησιμοποιεί ένα δέκτη GPS που σηματοδοτεί αυτόματα την τρέχουσα θέση αν η έρευνα διεξάγεται σε εξωτερικούς χώρους. Μετά από μια έρευνα, πραγματοποιείται ανάλυση δεδομένων και τα αποτελέσματα των ερευνών τεκμηριώνονται στις αναφορές επιτόπιων ερευνών που δημιουργούνται από την εφαρμογή.

Όλες αυτές οι εργασίες συλλογής, ανάλυσης και οπτικοποίησης δεδομένων είναι ιδιαίτερα αυτοματοποιημένες στο σύγχρονο λογισμικό. Στο παρελθόν, όμως, αυτά τα καθήκοντα απαιτούσαν χειροκίνητη καταγραφή και επεξεργασία δεδομένων. Επίσης σημειώνονται οι διευθύνσεις MAC για να μπορούν να καταγράφουν και να εντοπιστούν στον υπόλοιπο δικτυακό εξοπλισμό[7]

2.4 Επιλογή του εξοπλισμού

Έχοντας ολοκληρώσει το Site Survey και το Wireless Site Survey, το επόμενο βήμα είναι η επιλογή του εξοπλισμού. Σύμφωνα με τα δυο Survey η τεχνική εταιρεία αποφάσισε να αλλάξει όλο το υπάρχον δικτυακό εξοπλισμό και να προχωρήσει στην αναβάθμιση και επέκταση του ασυρμάτου δικτύου της.

Για το κομμάτι του routing επιλέχθηκε η συσκευή Cisco 880 Series Integrated Services Routers. Επιπλέον λόγω της συμβατότητας που έχουν με τον Satellite ISP Switching επιλέχθηκαν 3 Cisco Switch 2960-X Stack Switch.

Το **Stack switch** είναι switch δικτύου το οποίο λειτουργεί πλήρως αυτόνομο αλλά μπορεί επίσης να ρυθμιστεί για να λειτουργεί μαζί με έναν ή περισσότερα switch δικτύου. Αυτή η ομάδα switch παρουσιάζει τα χαρακτηριστικά ενός μόνο switch αλλά να έχει την χωρητικότητα θύρας των συνδυασμένων switch .

Ο όρος "stack" “στοιβα” αναφέρεται στην ομάδα των switch που έχουν ρυθμιστεί με αυτόν τον τρόπο. Το κοινό χαρακτηριστικό μιας στοίβας που λειτουργεί ως ένα απλό switch είναι ότι υπάρχει μια ενιαία διεύθυνση IP για απομακρυσμένη διαχείριση της στοίβας στο σύνολό της, όχι μια διεύθυνση IP για τη διαχείριση κάθε μονάδας στη στοίβα.

Τα πλεονεκτήματα των stack switches είναι:

- **Απλοποιημένη διαχείριση δικτύου:** Εάν ένα stackable switch λειτουργεί μόνο του ή "στοιβάζεται" με άλλες μονάδες, υπάρχει πάντα μόνο μία διεπαφή διαχείρισης για να αντιμετωπίσει ο διαχειριστής του δικτύου. Αυτό απλοποιεί τη ρύθμιση και τη λειτουργία του δικτύου.
- **Επεκτασιμότητα:** Ένα μικρό δίκτυο μπορεί να διαμορφωθεί γύρω από μια ενιαία μονάδα στοιβας και στη συνέχεια το δίκτυο μπορεί να αναπτυχθεί με πρόσθετες μονάδες με την πάροδο του χρόνου εάν και όταν χρειάζεται, με μικρή προστιθέμενη πολυπλοκότητα διαχείρισης.
- **Ευελιξία ανάπτυξης:** Τα stack switches μπορούν να λειτουργούν μαζί με άλλους μετασχηματιστές που μπορούν να στοιβαχθούν ή μπορούν να λειτουργούν ανεξάρτητα. Οι μονάδες μιας ημέρας μπορούν να συνδυαστούν ως στοίβα σε μια τοποθεσία και αργότερα μπορούν να λειτουργούν σε διαφορετικές τοποθεσίες ως ανεξάρτητα switch.

Τα μειονεκτήματα των stack switches είναι:

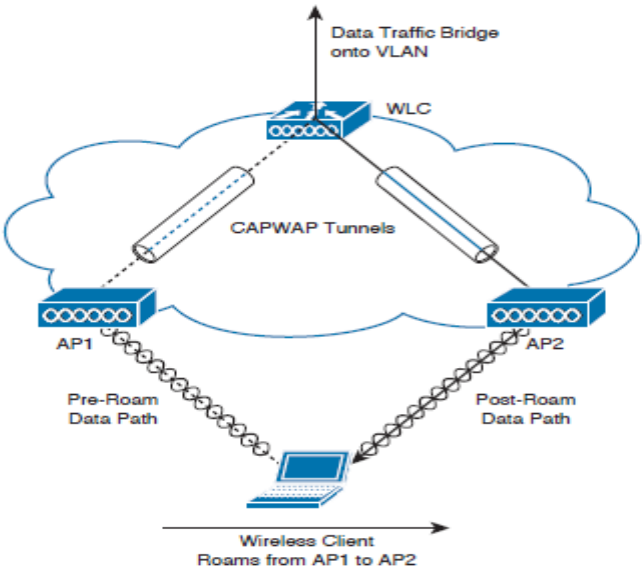
- Για τοποθεσίες που χρειάζονται πολλές θύρες, ένα σπονδυλωτό πλαίσιο μπορεί να κοστίσει λιγότερο. Με στοιβαζόμενη μεταγωγή, κάθε μονάδα σε μια στοίβα έχει το δικό της περίβλημα και τουλάχιστον ένα μόνο τροφοδοτικό. Με αρθρωτή μεταγωγή, υπάρχει ένα περίβλημα και ένα σύνολο τροφοδοτικών.
- Οι αρθρωτοί διακόπτες υψηλού επιπέδου διαθέτουν χαρακτηριστικά υψηλής ευκαμψίας / υψηλής απόδοσης που δεν είναι διαθέσιμα σε όλες τις στοιχειοθετημένες αρχιτεκτονικές.
- Πρόσθετη επιβάρυνση κατά την αποστολή δεδομένων στοίβαξης μεταξύ των switch. Ορισμένα πρωτόκολλα στοίβαξης προσθέτουν επιπλέον κεφαλίδες σε καρέ, αυξάνοντας περαιτέρω τα γενικά έξοδα.

Για ασφάλεια δικτύου η εταιρεία αποφάσισε για dedicated συσκευή τοίχος προστασίας (Firewall). Η συσκευή που επιλέχθηκε είναι Cisco ASA 5505 Adaptive Security Appliance ωφελεί και παραμετροποίηση θα αναφερθούν σε παρακάτω κεφάλαια.

Τέλος και ίσως το πιο σημαντικό σημείο όλης της εγκατάστασης είναι το κομμάτι του ασυρμάτου δικτύου. Μετα από Wireless Site survey αποφασίστηκε να εγκατασταθεί Wireless LAN Controller 3504 και 25 Air AP 1815 και 6 Aironet AP 1532 για εξωτερικό χώρο .Ο λόγος που επιλέχθηκαν οι συγκεκριμένες συσκευές είναι να πέτυχουμε πρώτον τον έλεγχο όλων των κεραιών από μια συσκευή και επίσης να δημιουργήσουμε Ομάδες παραγωγής και κινητικότητας

Ο κύριος λόγος για την ύπαρξη ασύρματων δικτύων είναι η περιαγωγή: η δυνατότητα πρόσβασης σε δικτυακούς πόρους από κοινόχρηστους χώρους και σε περιοχές όπου είναι δύσκολο να εκτελεστεί καλωδίωση. Τερματίστε τους πελάτες μπορεί να θέλετε να μετακινηθείτε από τη μία θέση στην άλλη. Η κινητικότητα επιτρέπει στους χρήστες να έχουν πρόσβαση στο δίκτυο από διάφορες τοποθεσίες. Η περιαγωγή συμβαίνει όταν ο ασύρματος πελάτης αλλάξει συσχέτιση από

ένα AP σε άλλο. Η πρόκληση είναι να κλιμακωθεί το ασύρματο δίκτυο για να επιτραπεί η περιαγωγή των πελατών που είναι απρόσκοπτη και ασφαλής. Η περιαγωγή μπορεί να είναι intracontroller η intercontroller.Στην συγκεκριμένη εγκατάσταση χρησιμοποιούμε intracontroller.



Εικόνα 2: Intracontroller roaming

Η περιηγηση του Intracontroller εμφανίζεται όταν ο πελάτης μετακινεί τη συσχέτιση από ένα AP σε ένα άλλο AP που συνδέεται με το ίδιο WLC. Το WLC ενημερώνει τη βάση δεδομένων πελατών με το νέο συνδεδεμένο AP και δεν αλλάζει τη διεύθυνση IP του πελάτη. Εαν είναι απαραίτητο,οι πελάτες επιβεβαιώνονται εκ νέου και δημιουργείται μια νέα ένωση ασφαλείας. Η βάση δεδομένων του πελάτη παραμένει στο ίδιο WLC.[7]

Κεφάλαιο 3: Παρουσίαση Λογισμικού και Οδηγός Εγκατάστασης

3.1 Απαιτήσεις λογισμικού και υλικού

Για την πραγματοποίηση της προσομοίωσης αυτής της εργασίας θα χρειαστούμε τα εξής υλικά και λογισμικά:

Υλικά

1. Έναν υπολογιστή ο οποίος θα έχει τον ρολό του διακομιστή και θα φιλοξενεί τον λογισμικό εικονικοποιησης και τους εικονικούς υπολογιστές που θα χρειαστούμε για την εργασία .Ο διακομιστής αυτός θα πρέπει να έχει ισχυρά τεχνικά χαρακτηριστικά (Μνήμη, Επεξεργαστή) ώστε να μπορεί να αντέξει το φορτίο τον εικονικών μηχανήματων που θα δημιουργήσουμε .Για την συγκεκριμένη εργασία ο διακομιστής μας έχει 42 GB RAM και επεξεργαστή με 8 πυρηνες
2. Έναν υπολογιστή που θα φιλοξενεί το λογισμικό GNS3 οπού θα πραγματοποιήσουμε την προσομοίωση του δικτυακού εξοπλισμού. Εδώ τα χαρακτηριστικά δεν μας ενδιαφέρουν καθώς ο διακομιστής θα χειριστεί στο μεγαλύτερο μέρος της επεξεργασίας

Λογισμικά

1. **GNS3:**Χρησιμοποιειται για αντιμετώπιση δικτύων σε πραγματικό χρόνο για δοκιμές πριν από την ανάπτυξη χωρίς την ανάγκη υλικού δικτύου: Εκτελούμε το λειτουργικό σύστημα που εξομοιώνει την πραγματική συμπεριφορά του υλικού δίκτυο Μπορούμε να δοκιμάσουμε γρήγορα πολλούς προμηθευτές υλικού χωρίς την ανάγκη υλικό και να δημιουργήσουμε δυναμικούς χάρτες δικτύου για δοκιμές αντιμετώπισης προβλημάτων και απόδειξης ιδεών (POC). Δοκιμάζουμε τα δίκτυά μας πριν τα χρειαστούμε για να μειώσουμε το χρόνο που απαιτείται για να ξεκινήσουμε ένα δίκτυο παραγωγής. Τέλος μπορούμε να συνδέσουμε το GNS3 σε οποιοδήποτε πραγματικό δίκτυο χρησιμοποιώντας το υπάρχον υλικό μας και επεκτείνουμε το τρέχον μας εργαστήριο συνδέοντας απευθείας τις τοπολογίες GNS3 σε αυτό. Το λογισμικό αποτελείται από δυο μέρη το GNS3-all-in-one software το οποίο θα εγκατασταθεί στον υπολογιστή με μας και το GNS3 virtual machine το οποίο θα εγκατασταθεί στο διακομιστή μας και θα φιλοξενεί και θα χειριστεί όλες τις εικονικές “εικόνες” το συσκευών που θα χρησιμοποιήσουμε

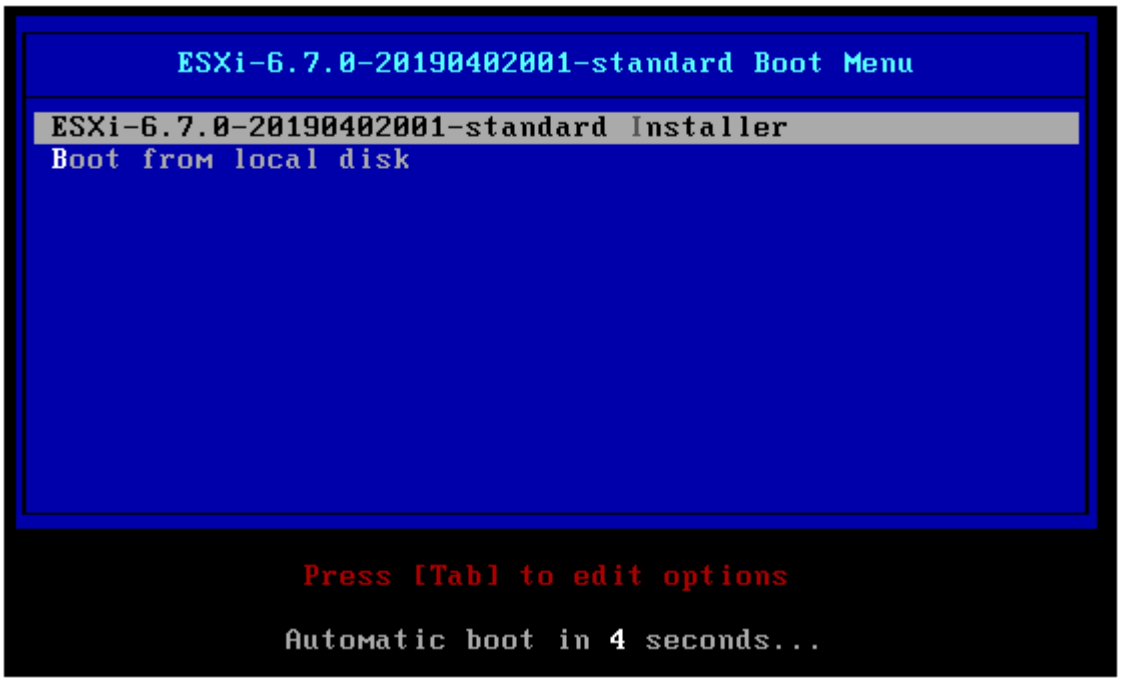
2. **VMware ESXi:** Είναι λειτουργικό εικονικοποιησης που παρέχει ένα πλήρως εικονικοποιημένο hardware στο φιλοξενούμενο λειτουργικό σύστημα, με εικονική κάρτα γραφικών, εικονικό σκληρό δίσκο, εικονικούς οδηγούς για τις θύρες USB, τις παράλληλες και τις σειριακές θύρες. Έτσι τα εικονικά μηχανήματα μπορούν να μεταφερθούν από υπολογιστή σε υπολογιστή και να μην έχουν προβλήματα συμβατότητας. Στην πράξη ένας διαχειριστής μπορεί να κάνει παύση των λειτουργιών ενός εικονικού συστήματος, να το αντιγράψει ή απλώς να το μεταφέρει σε έναν άλλο τοπικό υπολογιστή και να συνεχιστούν εκεί οι προηγούμενες λειτουργίες στο σημείο ακριβώς που είχαν σταματήσει.

Στην παρούσα εργασία ο ESXi θα φιλοξενήσει τον GNS3 virtual machine όπως και τον Radius Server το οποίο θα στηθεί σε περιβάλλον Ubuntu-Linux[13]

3.2 Εγκατάσταση λογισμικού περιβάλλοντος ESXi και δημιουργία εικονικών μηχανήματων

Βήμα 1ο : Λήψη και Εκκίνηση οδηγού εγκατάστασης

Το πρώτο βήμα θα πρέπει να ακολουθήσει η λήψη του ESXi 6.7 ISO και η δημιουργία ενός bootable CD ή DVD. Στη συνέχεια, ο χρήστης μπορεί να χρησιμοποιήσει απευθείας την εικονική τοποθέτηση από μια εικονική εικόνα. Στο επόμενο βήμα ο χρήστης πρέπει να τοποθετήσει το ESXi ISO απευθείας στο διακομιστή. Τώρα ξεκινάμε το διακομιστή και κάνουμε εκκίνηση από το CD / DVD. Θα εμφανιστεί μια οθόνη κατά την εκκίνηση και ο χρήστης πρέπει να πατήσει την επιλογή Enter στο ESXi 6.7. Η παρακάτω εικόνα θα δώσει το παραπάνω βήμα πιο ξεκάθαρο και εύκολο.



Εικόνα 3: Οδηγός εγκατάστασης ESXi

Βήμα 2ο : Συμφωνία με τους όρους χρήσης

Στο επόμενο βήμα ο χρήστης κατευθύνεται να πατήσει το πλήκτρο enter για να συνεχίσει την όλη διαδικασία. Μόλις πιέσετε το enter, ο χρήστης θα παρατηρήσει τις αλλαγές βήμα προς βήμα.

Στην οθόνη θα εμφανιστεί μια συμφωνία άδειας και ο χρήστης θα κατευθυνθεί για να πατήσει το F11 για να αποδεχθεί τη συμφωνία άδειας χρήσης και να συνεχίσει τη διαδικασία με κανονικό τρόπο. Εάν απαιτείται, ο χρήστης πρέπει επίσης να ακολουθήσει και να διαβάσει τους όρους και

τις προϋποθέσεις που εμφανίζονται στην οθόνη. Αυτό γίνεται κυρίως για την ασφάλεια του χρήστη και είναι καλύτερα να διαβάσουμε τη συμφωνία πριν κάνουμε κλικ.

Βήμα 3ο : Επιλογή δίσκου για εγκατάσταση

Στο επόμενο βήμα ο χρήστης πρέπει να επιλέξει το δίσκο στον οποίο θέλει να εγκαταστήσει το ESXi 6.7. Την στιγμή της επιλογής του δίσκου ο χρήστης θα πρέπει να πατήσει το πλήκτρο enter και να συνεχίσει την όλη διαδικασία με ασφάλεια. Η επιλογή του δίσκου θα εμφανιστεί επίσης στην οθόνη και έτσι θα βοηθήσει και τον χρήστη σαφώς σε αυτή την περίπτωση

Βήμα 4ο : Επιλογή διάταξης πληκτρολογίου

Στην επόμενη διαδικασία, υπάρχουν διάφοροι τύποι διάταξης πληκτρολογίου που θα εμφανίζονται στην οθόνη. Ο χρήστης μπορεί να το επιλέξει σύμφωνα με την απαίτηση και να πατήσει το κουμπί Enter. Η επιλογή της διάταξης πληκτρολογίου εξαρτάται πλήρως από τον χρήστη.

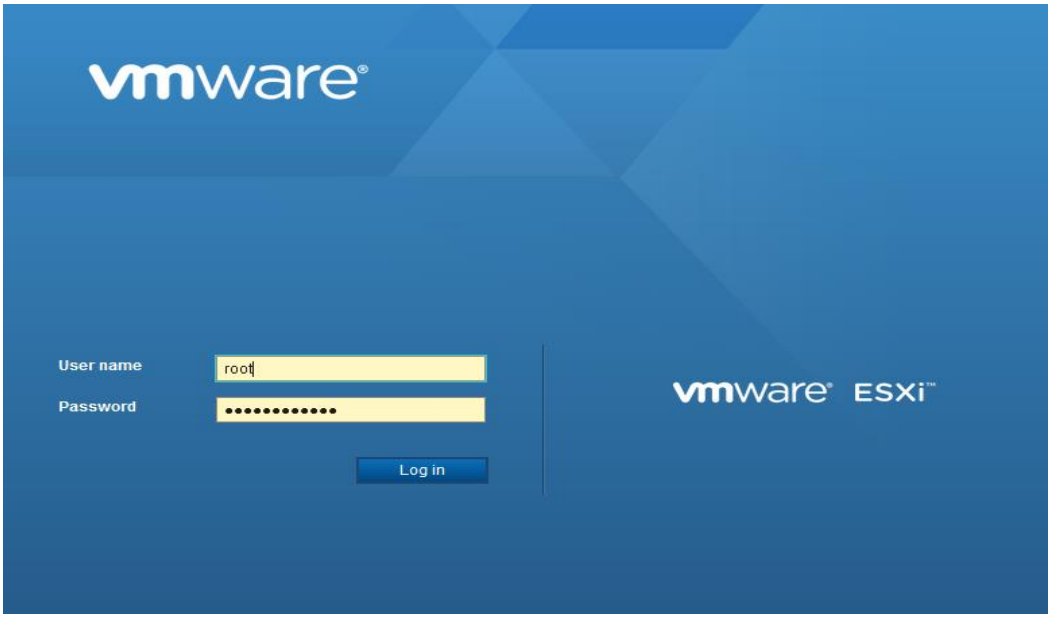
Βήμα 5ο : Επιλογή κωδικού πρόσβασης

Ο χρήστης σε αυτό το βήμα θα πρέπει να ορίσει τον κωδικό πρόσβασης root και να πατήσει enter για να συνεχίσει την όλη διαδικασία. Εάν εμφανιστεί κάτι στην οθόνη, τότε ο χρήστης θα πρέπει να το περάσει σωστά και στη συνέχεια να το επιλέξει.

Βήμα 6ο : Εγκατάσταση

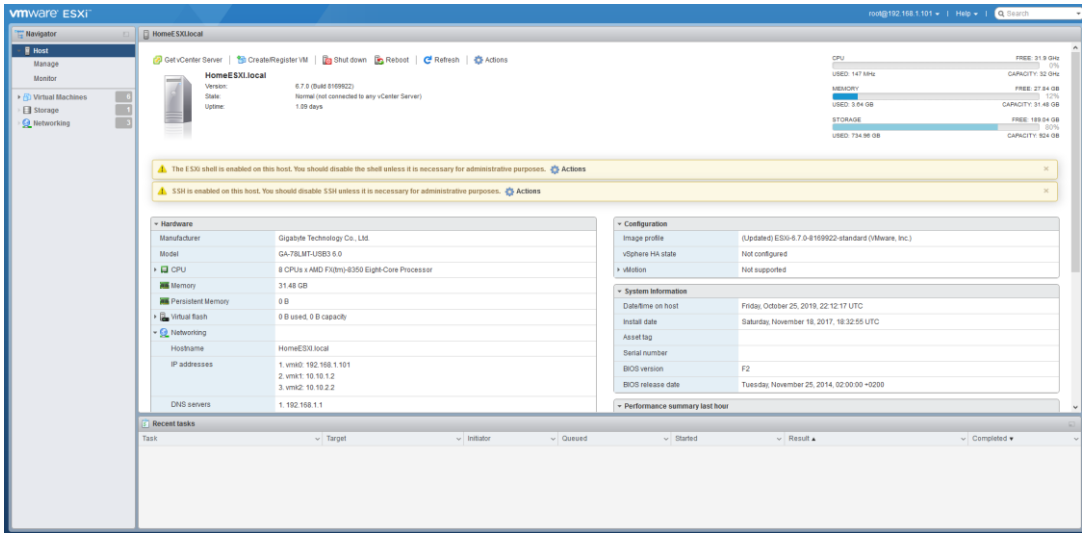
Τέλος, πρέπει να πατηθεί το πλήκτρο F11 για εγκατάσταση. Μόλις τελειώσει η διαδικασία εγκατάστασης, ο χρήστης θα πρέπει να πατήσει Enter για να επανεκκινήσει το διακομιστή. Εάν ο διακομιστής επανεκκινήσει με επιτυχία, τότε ο χρήστης μπορεί να δει καθαρά το ESXi6.7 εγκατεστημένο στον υπολογιστή μαζί με τα στοιχεία μνήμης και CPU.

Μόλις ολοκληρωθεί η εγκατάσταση με επιτυχία το διαχειριστικό του προγράμματος είναι πλέον προσβάσιμο με την χρήση οποιουδήποτε web browser πληκτρολογώντας στην μπάρα διευθύνσεων την διεύθυνση του διακομιστή με την μορφή: https://192.168.1.101/ui/



Εικόνα 4: Login VMware Host

Δίνοντας τα διαπιστευτήρια που ορίσαμε κατά την εγκατάσταση οδηγούμαστε στην παρακάτω εικόνα:



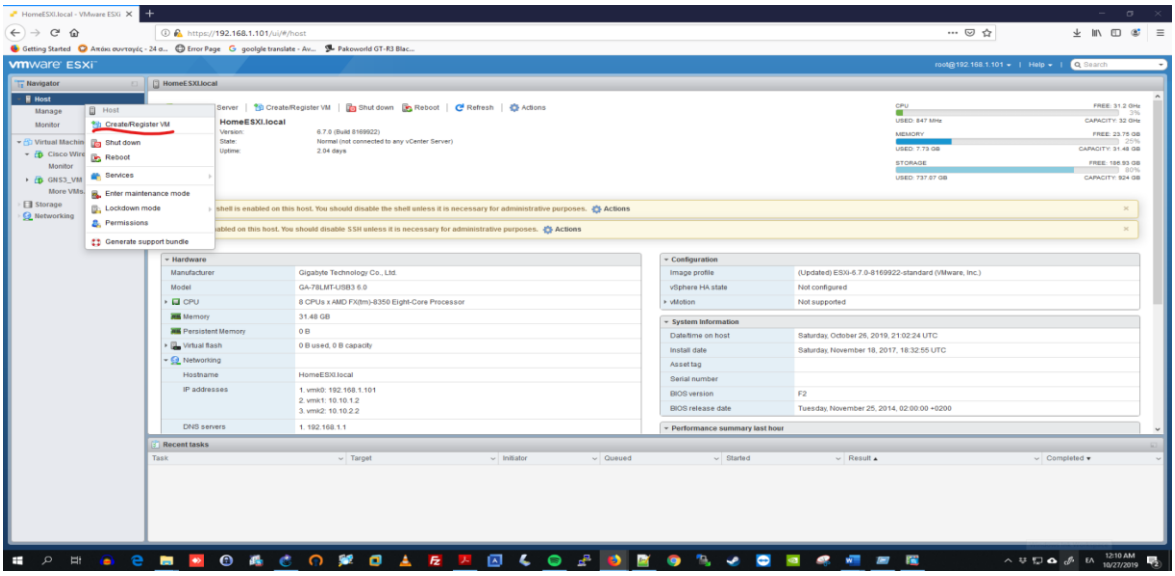
Εικόνα 5: Φόρμα εισαγωγής εικονικών μηχανημάτων

Αυτό είναι το περιβάλλον όπου θα δημιουργήσουμε τα δυο μας εικονικά μηχανήματα.

3.2.1 Δημιουργια εικονικου μηχανηματος GNS3 VM

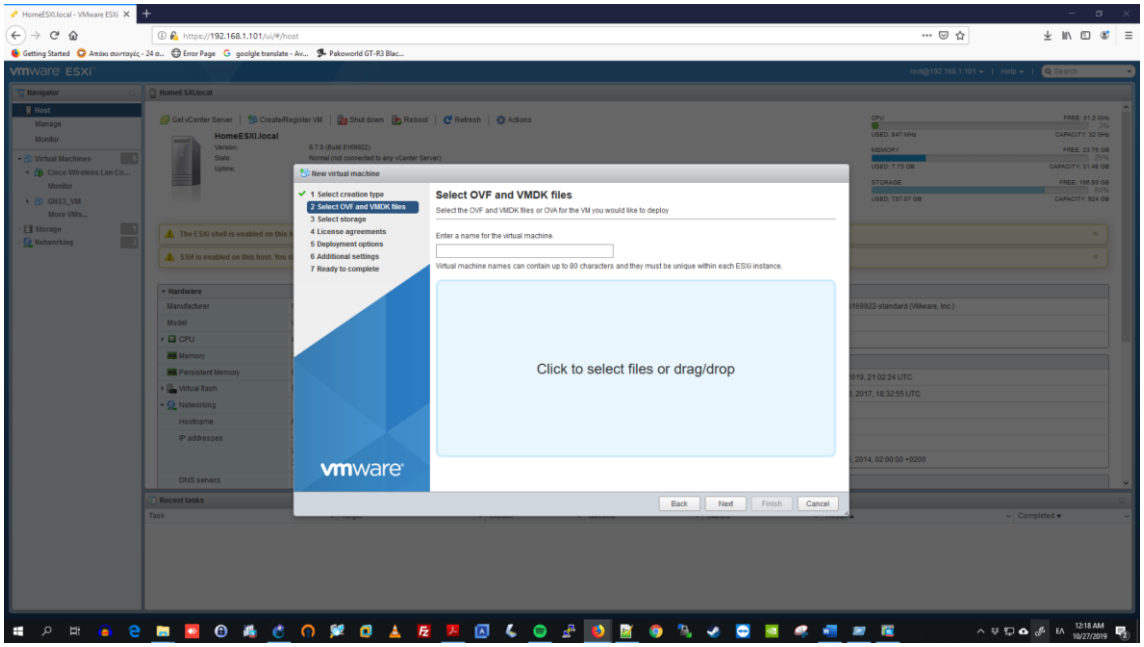
Έχοντας κατεβάσει το απαραίτητο αρχείο από την σελίδα της GNS3,παμε στο ESXi περιβάλλον και πραγματοποιούμε τις εξής ενέργειες:

1. Κάνουμε δεξί κλικ στον host θα μας εμφανιστεί η επιλογή Create/Register VM



Εικόνα 6: Create & register VM

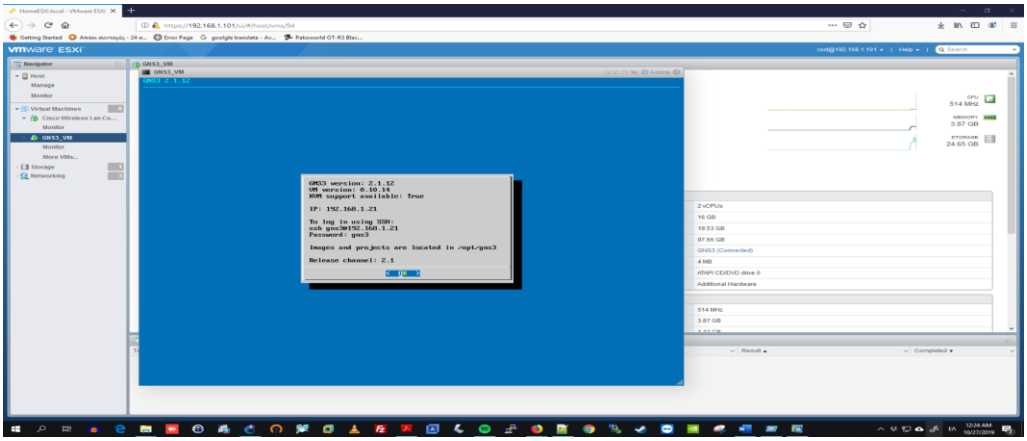
2. Μόλις το επιλέξουμε θα μας εμφανιστεί ένα νέο Wizard που θα μας καθοδηγήσει στην δημιουργία του νέου μας εικονικού μηχανήματος .Στην πρώτη οθόνη επιλέγουμε: ***"Deploy a virtual machine from a OVA or OVF File"*** καθώς η εταιρεία έχει ήδη δημιουργήσει ένα πακέτο OVF το οποίο έχει ήδη εγκατεστημένο το λειτουργικό περιβάλλον. Οι ενέργειες αυτές φαίνονται στην εικόνα που ακολουθεί:



Εικόνα 7: Deploy a virtual machine from a OVA or OVF File

3. Αφού επιλέξουμε το αρχείο που κατεβάσαμε και του δώσουμε την επιθυμητή ονομασία πατώντας next Επιλέγουμε σε ποιον δίσκο θέλουμε να εγκατασταθεί και ολοκληρώνουμε την διαδικασία του Wizard Μόλις ολοκληρώσουμε την διαδικασία και ενεργοποιήσουμε

το νέο μας εικονικό μηχάνημα θα μας εμφανιστεί μια οθόνη με τα δικτυακά στοιχεία του μηχανήματος.



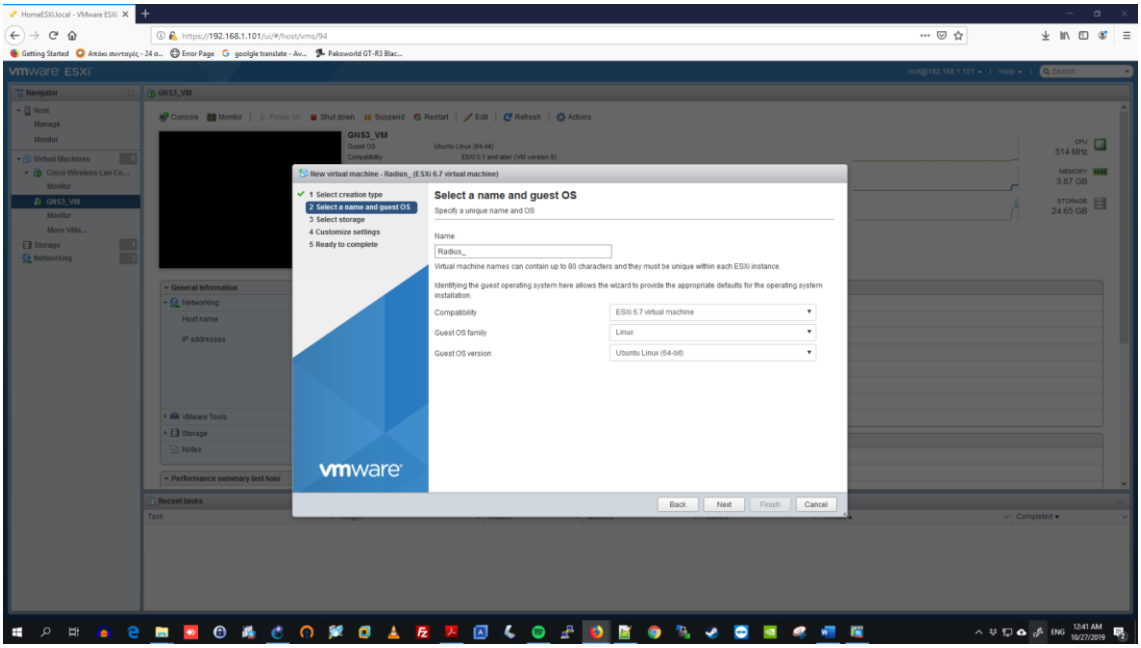
Εικόνα 8: Δικτυακά στοιχεία του εικονικού μηχανήματος

Καλό θα ήταν ολοκληρώνοντας τις παραπάνω ενέργειες να καταγράψουμε την δικτυακή διεύθυνση διότι θα την χρειαστούμε την παραμετροποίηση του GNS3 GUI.

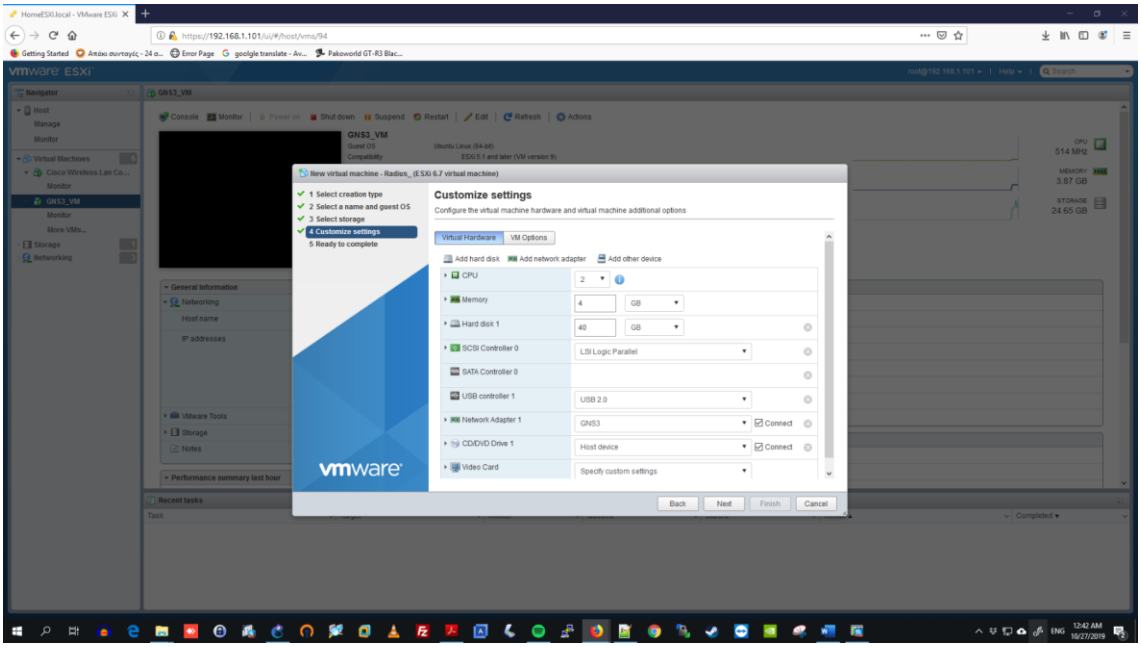
3.2.2 Δημιουργία εικονικού μηχανήματος Radius(Ubuntu)

Για το συγκεκριμένο μηχάνημα καθώς δεν υπάρχει έτοιμο appliance, γι' αυτό θα πρέπει να δημιουργήσουμε ένα νέο εικονικό μηχάνημα. Για τον σκοπό αυτό επιλέγουμε να εγκαταστήσουμε λειτουργικό περιβάλλον Linux και συγκεκριμένα την διανομή Ubuntu 18.04.3.

Αρχικά κατεβάζουμε την διανομή για τα λειτουργικά συστήματα Linux που μας ενδιαφέρουν τα οποία ανήκουν στην γενική κατηγορία Ανοιχτού Κώδικα (Open Source) που σημαίνει ότι είναι δωρεάν. Αφού κατεβάσουμε την διανομή από την ιστοσελίδα www.ubuntu.com μεταφερόμαστε πάλι στον περιβάλλον ESXi και επαναλαμβάνουμε την διαδικασία που κάναμε στο GNS3 μόνο που αντί για ***"Deploy a virtual machine from a OVA or OVF File"*** επιλέγουμε ***"Create a new virtual machine"*** επειδή πλέον είναι σαν να δημιουργούμε ένα νέο υπολογιστή καθώς δεν υπάρχει το OVF το οποίο περιέχει πληροφορίες όπως πόση μνήμη θα χρειαστουμε και πόσοι πυρήνες από τον επεξεργαστή μας θα χρησιμοποιηθούν. Τα στοιχεία αυτά θα πρέπει να δοθούν από μας. [14]

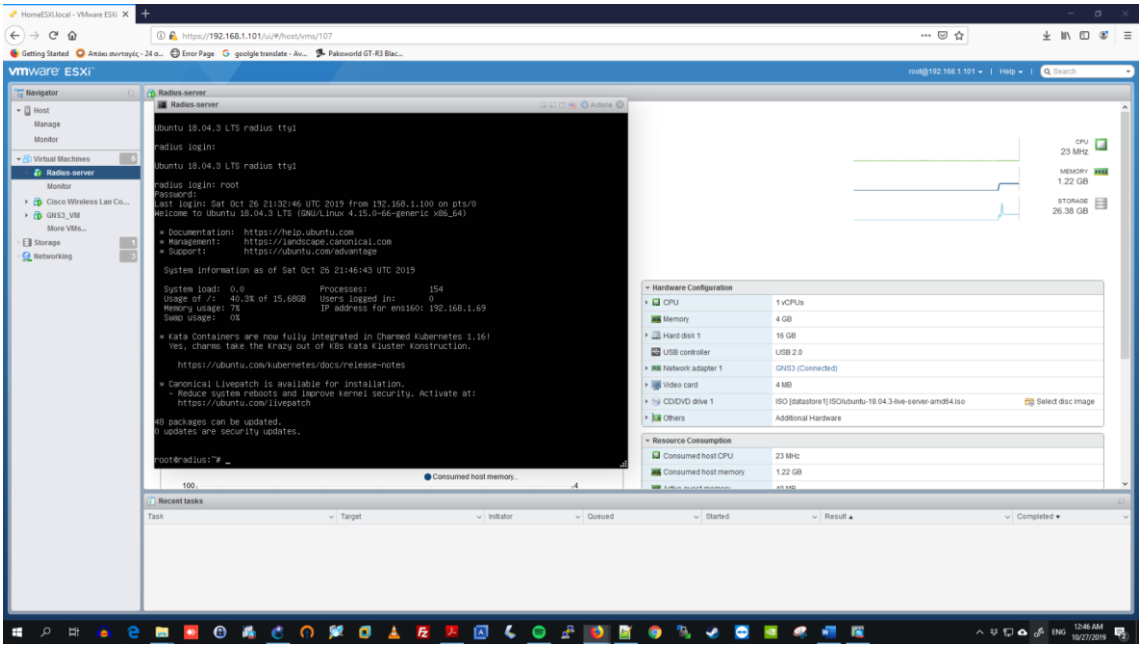


Εικόνα 9: Installing guest OS



Εικόνα 10: Settings customization

Μόλις ολοκληρώσουμε την διαδικασία και ενεργοποιήσουμε το νέο μας εικονικό μηχάνημα προχωράμε στην εγκατάσταση του λειτουργικού Ubuntu σύμφωνα με της οδηγίες του κατασκευαστή. Δίνουμε την IP διεύθυνση της επιλογής μας και την σημειώνουμε για χρήση στα επόμενα βήματα.



Εικόνα 11: Ολοκλήρωση διαδικασίας εγκατάστασης guest OS

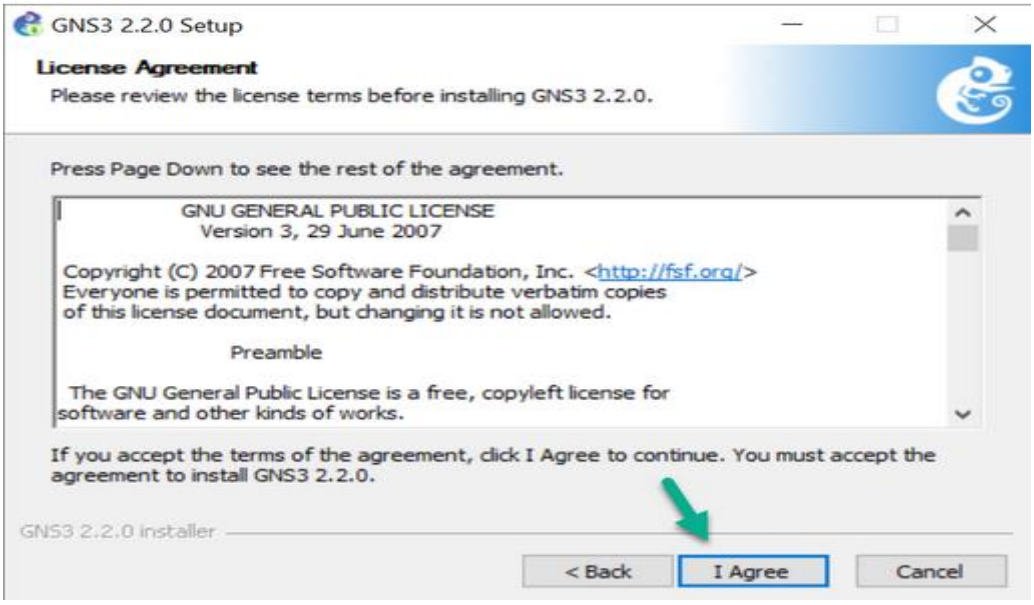
3.3 Εγκατάσταση Λογισμικού GNS3

Εδώ θα δούμε την διαδικασία εγκατάστασης του λογισμικού GNS3. Το λογισμικό αυτό θα εγκατασταθεί σε περιβάλλον Windows 10.

Ξεκινάμε την διαδικασία κατεβάζοντας τον λογισμικό από το ισότοπο www.gns3.com αφού ολοκληρώσουμε την διαδικασία εγγραφής. Στη συνέχεια αφού έχουμε κατεβάσει το λογισμικό μας κάνουμε κλικ πάνω στον εικονίδιο ανοίγει ο οδηγός εγκατάστασης όπως φαίνεται στην παρακάτω εικόνα:

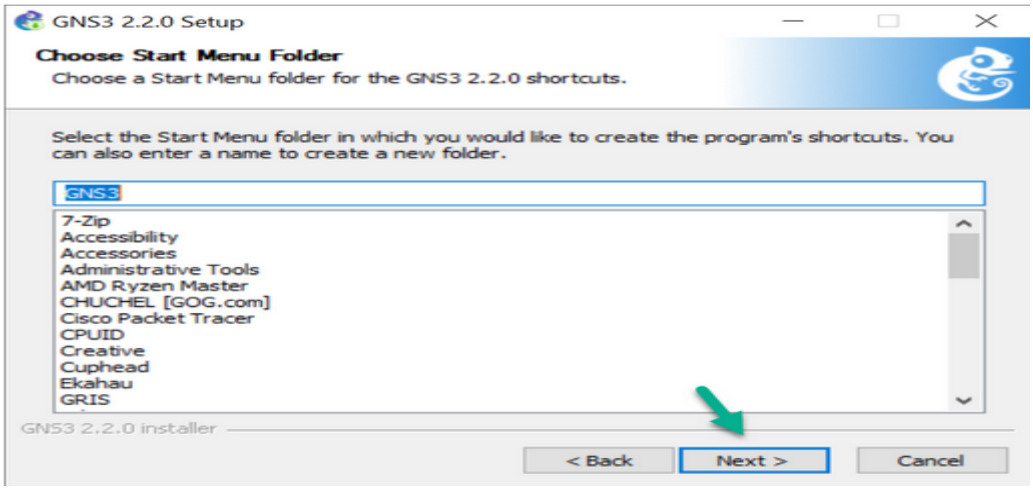
Εικόνα 12: Εκκίνηση οδηγού εγκατάστασης GNS3

Πατώντας next προχωράμε στο επόμενο βήμα που είναι η αποδοχή των όρων χρήσης όπως φαίνεται παρακάτω:



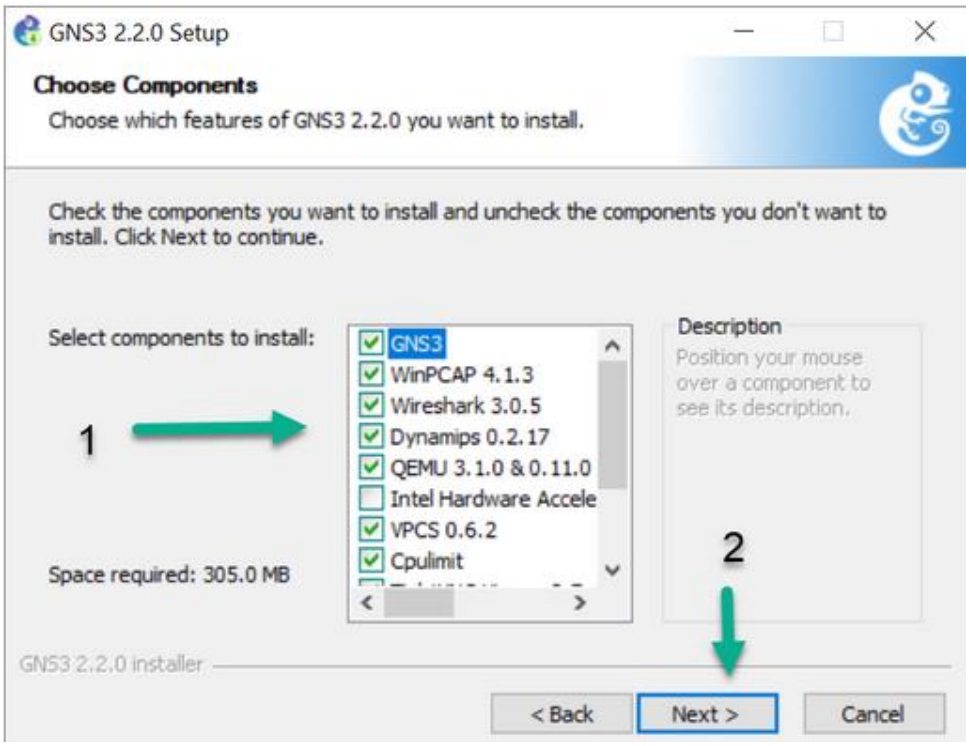
Εικόνα 13: Αποδοχή όρων χρήσης

Πατώντας **Agree** προχωράμε στην συνέχιση της εγκατάστασης επιλέγοντας τον φάκελο εγκατάστασης (κατά προτίμηση επιλέγουμε την προκαθορισμένη τοποθεσία):



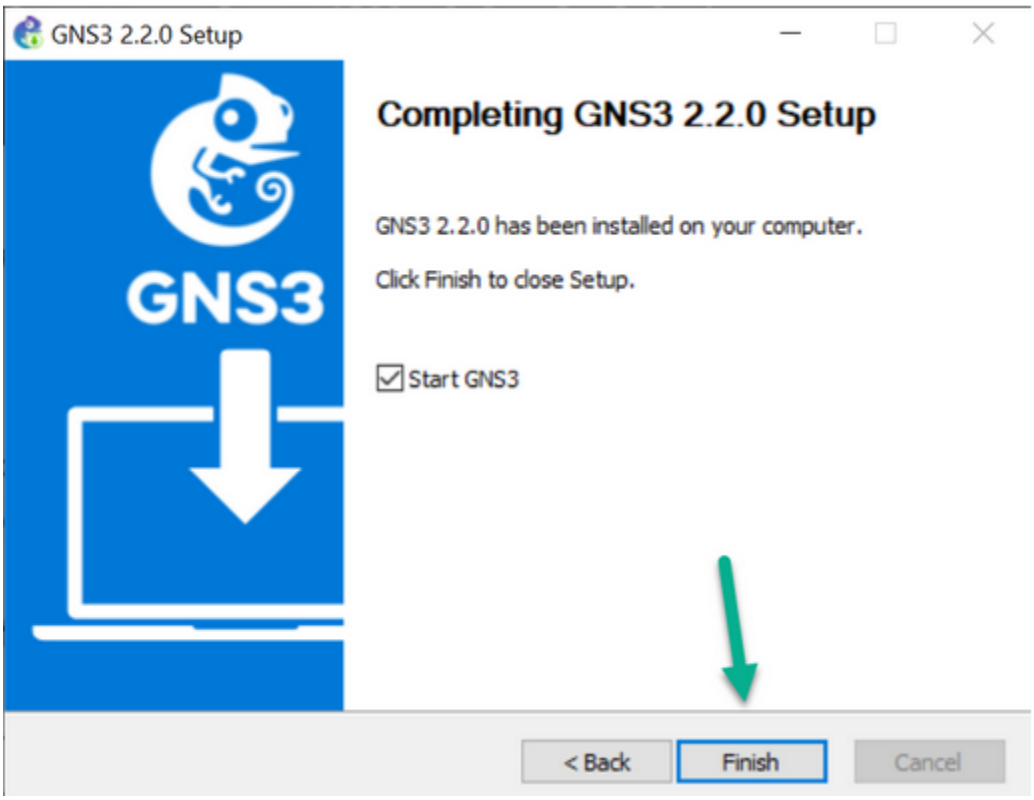
Εικόνα 14: Προορισμός εγκατάστασης

Το GNS3 συνοδεύεται από διάφορα προ απαιτούμενα και προαιρετικά λογισμικά. Από προεπιλογή, το μεγαλύτερο μέρος του λογισμικού έχει επιλεγεί για εγκατάσταση, αλλά μπορείτε να αποφασίσετε να εγκαταστήσετε μόνο κάποια από τα προσφερόμενα λογισμικά όπως φαίνεται στην εικόνα που ακολουθεί:



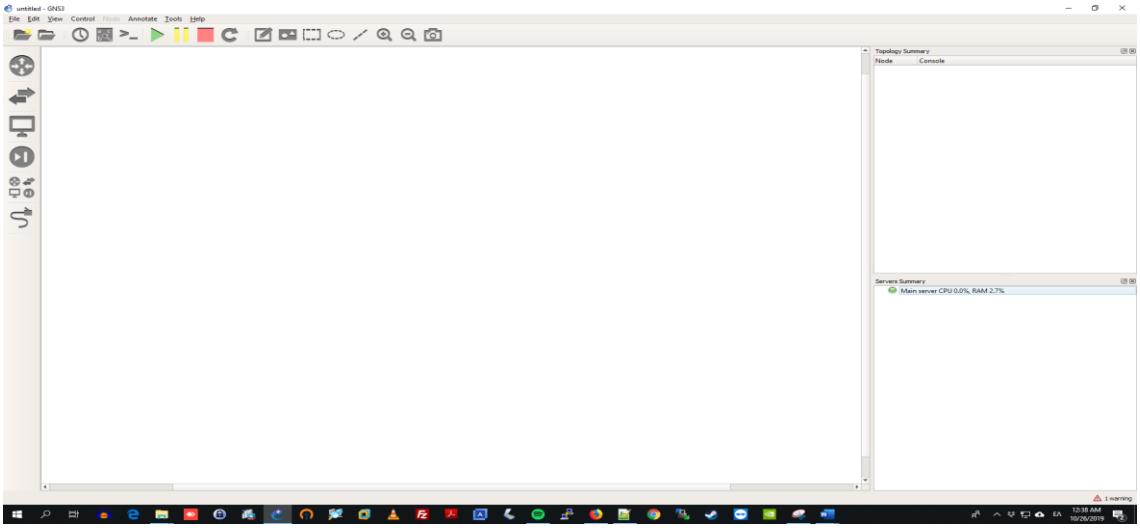
Εικόνα 15: Επιλογή πρόσθετων

Τέλος μόλις τελειώσει η διαδικασία της εγκατάστασης επιλέγουμε **Finish** και προχωράμε στην εκκίνηση του προγράμματος.



Εικόνα 16: Ολοκλήρωση εγκατάστασης

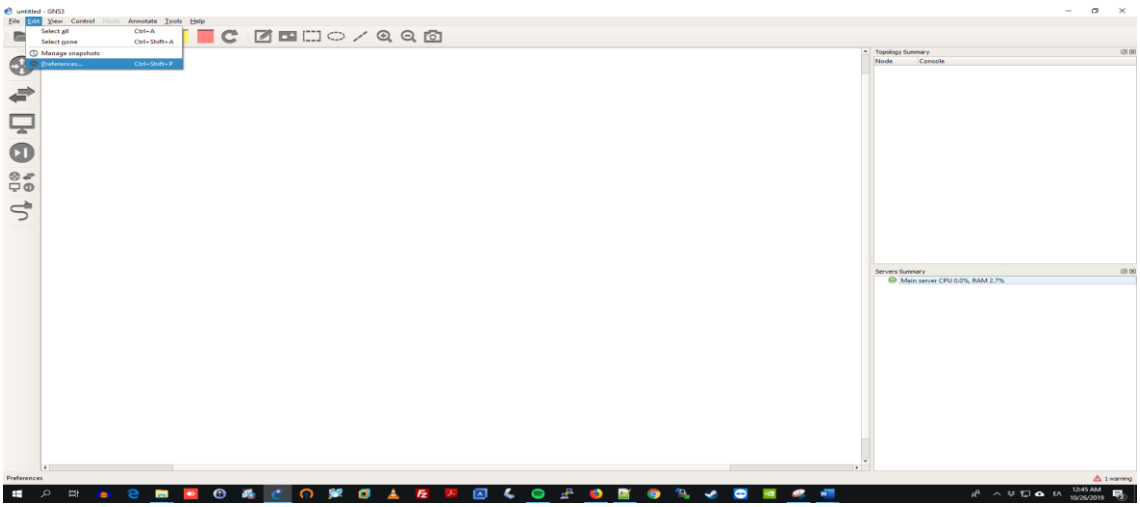
Με την ολοκλήρωση της εγκατάστασης μεταφερόμαστε στην παρακάτω οθόνη:



Εικόνα 17: Οθόνη εκκίνησης GNS3

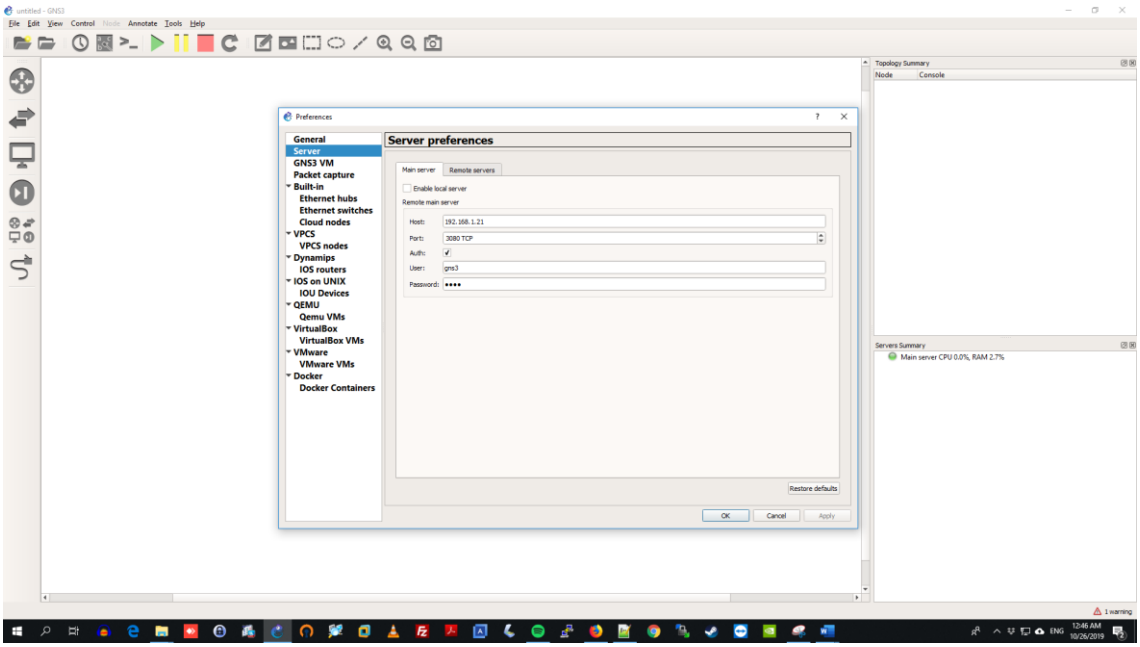
Έχοντας ολοκληρώσει την εγκατάσταση του εικονικού μηχανήματος στο περιβάλλον ESXi θα προχωρήσουμε στην παραμετροποίηση του GNS3 ώστε να επικοινωνήσει με το GNS3 VM.

Ξεκινάμε επιλέγοντας ***Edit → Preferences***



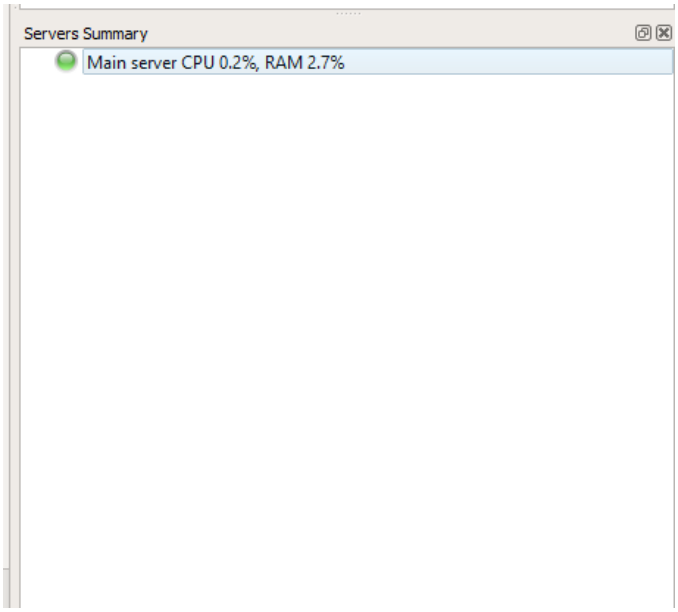
Εικόνα 18: Επιλογή παραμέτρων

Στη συνέχεια επιλέγουμε ***Servers → Main*** για να δώσουμε παραμέτρους που αφορούν τον διακομιστή:



Εικόνα 19: Ρυθμίσεις παραμέτρων διακομιστή

Δίνοντας την διεύθυνση IP που πηρέ το μηχάνημα και ορίστηκε κατά την διάρκεια του στησίματος στο ESXi, μπορούμε να επαληθεύσουμε ότι έχει γίνει η επικοινωνία με το εικονικό μηχάνημα βλέποντας την παρακάτω εικόνα η οποία μας δείχνει αφενός ότι έχουμε επικοινωνία αλλά και τι ποσοστό μνήμης και επεξεργαστή χρησιμοποιεί το εικονικό μας μηχάνημα.

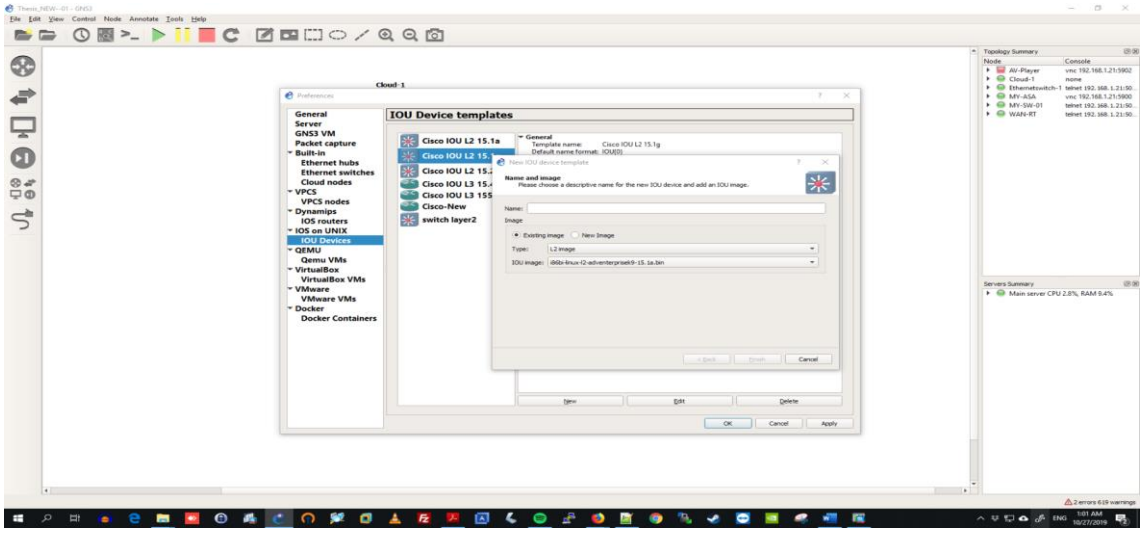


Εικόνα 20: Επαλήθευση επικοινωνίας και παρακολούθηση καταναλισκόμενης μνήμης

Το GNS3 σαν λογισμικό δεν περιέχει από μόνο του τις εικόνες των δικτυακών μηχανήματων και θα πρέπει να προστεθούν από μας. Τις εικόνες τις βρίσκουμε στην επίσημη ιστοσελίδα της Cisco όμως χρειάζονται διαπιστευτήρια.

Αφού κατεβάσουμε τις εικόνες θα πρέπει στη συνέχεια να τις φορτώσουμε στο λογισμικό μας. Για να γίνει αυτό πάμε στις ρυθμίσεις του GNS3 και επιλέγουμε:

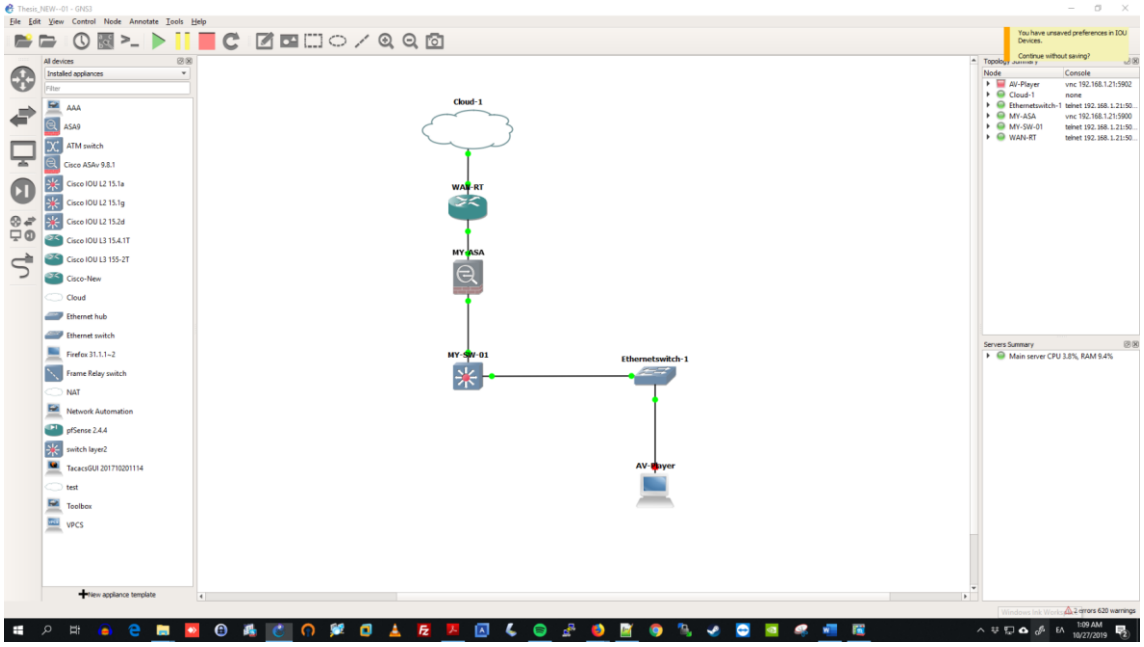
Edit→Preferences→IOU Devices



Εικόνα 21: Φόρτωση εικόνων δικτυακών μηχανημάτων στο GNS3

Θα δώσουμε την τοποθεσία της εικόνας και θα ονομάσουμε το νέο δικτυακό μας μηχάνημα. Την διαδικασία αυτή θα τη επαναλάβουμε για όλες μας τις δικτυακές συσκευές δίνοντας προσοχή στην επιλογή **Type** καθώς για switch θα πρέπει να επιλέξουμε L2 καθώς είναι Layer 2 συσκευή και για router θα πρέπει να επιλέξουμε L3 καθώς είναι Layer3 συσκευή. Την διαφορά Layer 2 και 3 θα την δούμε αναλυτικά στο κεφάλαιο 4.

Μόλις ολοκληρώσουμε την εισαγωγή των μηχανήματων αυτά θα εμφανιστούν σαν συσκευές έτοιμες προς χρήση στο μενού των συσκευών στο πλάι της εφαρμογής, όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 22: Εμφάνιση συσκευών έτοιμων προς χρήση στο GNS3

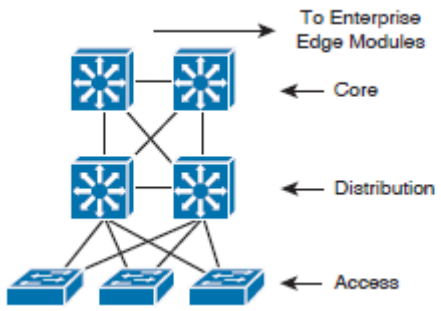
Κεφάλαιο 4: Ανάλυση Εγκατάστασης

4.1 Μέθοδος επιλογής τοπολογίας

Τα ιεραρχικά μοντέλα επιτρέπουν την σχεδίαση εσωτερικών δικτύων που χρησιμοποιούν την εξειδίκευση της λειτουργίας σε συνδυασμό με μια ιεραρχική οργάνωση. Ένας τέτοιος σχεδιασμός απλοποιεί τα απαιτούμενα καθήκοντα για την οικοδόμηση ενός δικτύου που ανταποκρίνεται στις τρέχουσες απαιτήσεις και μπορεί να αναπτυχθεί για να ανταποκριθεί και στις μελλοντικές απαιτήσεις. Τα ιεραρχικά μοντέλα χρησιμοποιούν στρώματα για να απλοποιήσουν τις εργασίες για την εσωτερική δικτύωση. Κάθε στρώμα μπορεί εστιάσει σε συγκεκριμένες λειτουργίες, επιτρέποντάς την επιλογή των σωστών συστημάτων και λειτουργίες για κάθε ένα από αυτά τα στρώματα. Τα ιεραρχικά μοντέλα ισχύουν και για το σχεδιασμό LAN και WAN.

Πλεονεκτήματα του Ιεραρχικού μοντέλου

- Εξοικονόμηση κόστους
- Ευκολία κατανόησης
- Αρθρωτή ανάπτυξη δικτύου
- Βελτιωμένη απομόνωση σφαλμάτων

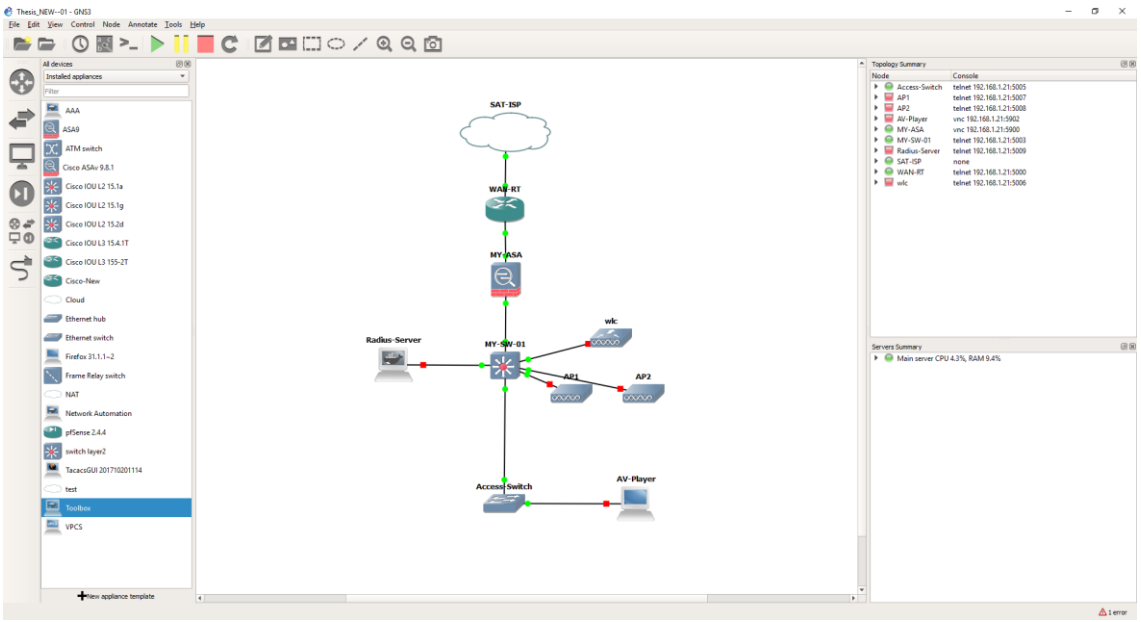


Εικόνα 23: Τα στρώματα του ιεραρχικού μοντέλου

Κάθε ένα από τα στρώματα που βλέπουμε στην παραπάνω εικόνα, παρέχει την απαραίτητη λειτουργικότητα στο δίκτυο. Μπορεί να εφαρμοστεί κάθε στρώμα σε μία ή περισσότερες συσκευές ή ως συνεργαζόμενα στοιχεία διασύνδεσης που μοιράζονται ένα κοινό πλαίσιο. Τα μικρότερα δίκτυα μπορούν να "συρρικνώσουν" τα πολλαπλά στρώματα σε μία μόνο συσκευή.[7]

4.2 Τοπολογία

Στην παρακάτω εικόνα βλέπουμε την τοπολογία όπως αυτή διαμορφώθηκε με την εφαρμογή GNS3:



Εικόνα 24: Τοπολογία στο GNS3

Ξεκινώντας από πάνω προς τα κάτω οι συσκευές SAT-ISP και WAN-RT εκπροσωπούν το επίπεδο Edge στο ιεραρχικό μοντέλο σχεδίασης. Οι συσκευές WAN-RT και MY-ASA εκπροσωπούν το Core στρώμα και οι συσκευές MY-ASA και MY-SW-01 το distribution στρώμα. Τέλος οι MY-SW-01 και Access Switch εκπροσωπούν το access στρώμα.

4.2.1 WAN-RT

Ο WAN-RT είναι ο δρομολογητής (router) ο ρόλος στην τοπολογία αυτή είναι να εξασφαλίσει την δρομολόγηση από και προς τον SAT-IP και το Firewall MY-ASA ουσιαστικά εξασφαλίζοντας την επικοινωνία του έξω κόσμο προς την τοπολογία μας

Στην παρακάτω εικόνα το interface ethernet0/3 όπως φαίνεται στην εντολή ***ip address dhcp*** έχει ρυθμιστεί να πάρει μια αυτόματη IP διεύθυνση από τον πάροχο καθώς το άλλο του ακρο καταλήγει στον εξοπλισμό του παρόχου. Στο interface έχει ρυθμιστεί να γίνει NAT (Network Address Translation) προς το διαδίκτυο. Το NAT είναι η διαδικασία όπου μια συσκευή δικτύου, συνήθως ένα τείχος προστασίας, εκχωρεί μια δημόσια διεύθυνση σε έναν υπολογιστή (ή μια ομάδα υπολογιστών) μέσα σε ένα ιδιωτικό δίκτυο. Η κύρια χρήση του NAT είναι να περιορίσει τον αριθμό των δημόσιων διευθύνσεων IP που πρέπει να χρησιμοποιεί ένας οργανισμός ή εταιρεία, τόσο για λόγους οικονομίας όσο και για λόγους ασφάλειας.

```
interface Ethernet0/0
 description ### Con to ASA ###
 ip address 192.168.254.254 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/1
 no ip address
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 description ### Con to SAT ISP ###
 ip address dhcp
 ip nat outside
 ip virtual-reassembly in
!
```

Εικόνα 25: Αποτελέσματα εκτέλεσης της εντολής ip address dhcp

Το interface ethernet 0/0 έχει συνδεθεί φυσικά στην θύρα Gigabit Ethernet 0/6 της συσκευής MY-ASA στο interface ethernet 0/0 έχουμε δώσει στατικά μια διεύθυνση 192.168.254.254 με σκοπό στην συσκευή MY-ASA να δώσουμε διεύθυνση στο ίδιο subnet 192.168.254.0.Επιπλεον για την ρύθμιση του firewall θα χρησιμοποιήσουμε την εφαρμογή ASDM η οποία θα μας δώσει γραφικό περιβάλλον στο firewall πρέπει να δώσουμε την παρακάτω εντολή:

```
ip nat inside source list NAT interface Ethernet0/3 overload
ip nat inside source static tcp 192.168.254.253 443 interface Ethernet0/3 9443
```

Εικόνα 26: Αποτελέσματα εκτέλεσης της εντολής sh run | I nat

Με την εκτέλεση της εντολής γίνεται προώθηση στην πόρτα 443 της IP διεύθυνσης του MY-ASA 192.168.254.253 για τους χρήστες που είναι εκτός του τοπικού δικτύου.

4.2.2 MY-ASA

Η συσκευή MY-ASA έχει τον ρολό του firewall στην τοπολογία Η παραμετροποίηση του θα γίνει με την χρήση της εφαρμογής ASDM.Πριν επιτραπεί η πρόσβαση στην εφαρμογή πρέπει να διασφαλιστεί η σύνδεση του με τον router .Το router είναι φυσικά συνδεδεμένο με το firewall μέσω του interface gigabitthernet 0/6 ASA→Interface ethernet 0/0 WAN-RT.

Στο firewall θα δώσουμε την στατική διεύθυνση IP 192.168.254.253 και θα ορίσουμε το security-level 0 οπού είναι η χαμηλότερη τιμή που μπορεί να πάρει και διασφαλίζει ότι θα περαστούν όλα τα πακέτα προς αυτή την θύρα. Τέλος θα δημιουργήσουμε έναν χρήστη unipi με κωδικό 123 και μέγιστο priviledge 15 και θα ενεργοποιήσουμε την υπηρεσία HTTP. Γιατί κατά την εκκίνηση της εφαρμογής ASDM θα ζητηθεί IP Username Password.

```
interface GigabitEthernet0/6
 description ### Con to WAN ###
 nameif WAN
 security-level 0
 ip address 192.168.254.253 255.255.255.252
!
```

```
MY-ASA# sh run | i username
username unipi password $sha512$5000$/BKWle9lXEM7S3Yk0/aEUg==$tSx8DOuBCX/jQDTs7X
3TJQ== pbkdf2 privilege 15
MY-ASA#
```

```
http server enable
http 192.168.0.0 255.255.255.0 MGMT
```

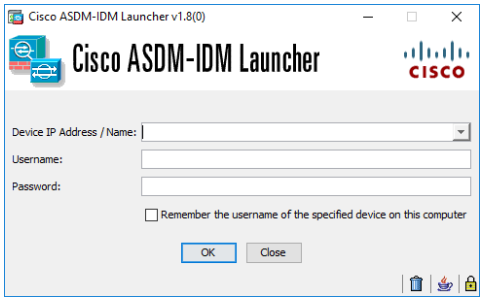
Εικόνα 27: Αποτελέσματα εκτέλεσης της εντολής sh run

Μόλις επιβεβαιώσουμε την επικοινωνία από WAN-RT προς το MY-ASA κάνοντας ping την IP του firewall από το WAN-RT

```
WAN-RT# ping 192.168.254.253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.253, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
WAN-RT#
```

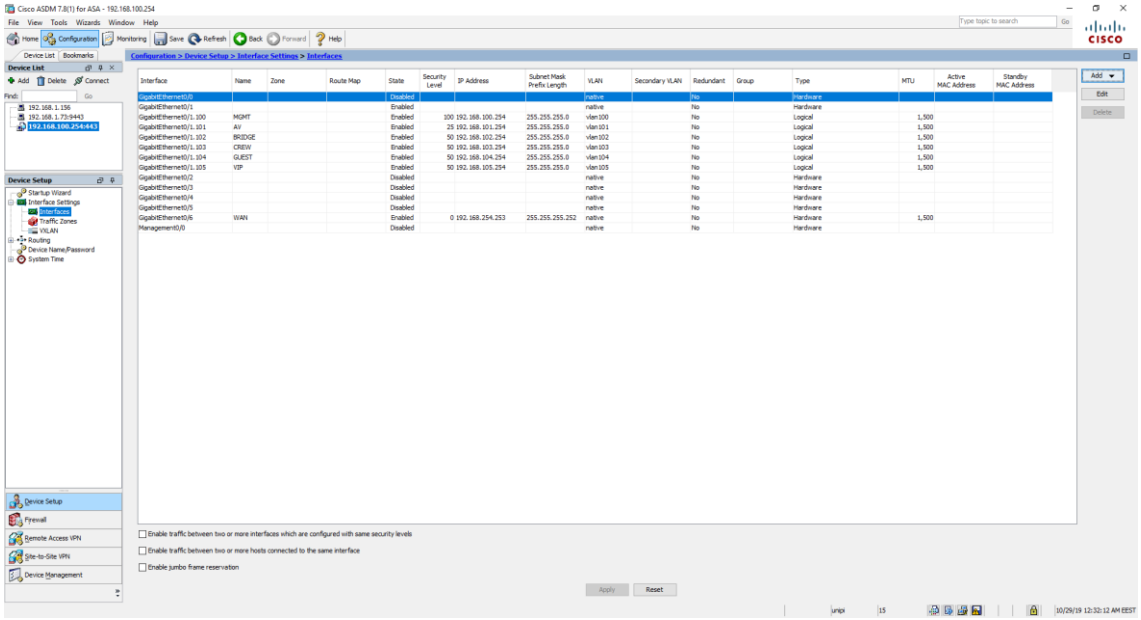
Εικόνα 28: Αποτελέσματα εκτέλεσης της εντολής ping

Ανοίγουμε την εφαρμογη ADSM



Εικόνα 29: Άνοιγμα εφαρμογής ADSM

Δίνουμε την IP διεύθυνση και τα διαπιστευτήρια που ορίστηκαν στο προηγούμενο βήμα και κάνουμε είσοδο στον ASDM



Εικόνα 30:GUI ASDM Menu Interfaces

Μετά την είσοδο στον ASDM στο Device Setup→Interfaces θα δημιουργήσουμε SubInterfaces και Vlan .Το έργο απαιτεί να δημιουργηθούν πέντε διαφορετικά δίκτυα ένα για κάθε ομάδα που δουλεύει στο σκάφος και 1 για όλα τα οπτικό ακουστικά συστήματα που χρησιμοποιούν δίκτυο. Ορίζουμε τα δίκτυα ως εξής:

- AV 192.168.101.254
- BRIDGE 192.168.102.254
- CREW 192.168.103.254
- GUEST 192.168.104.254
- VIP 192.168.105.254
- MGMT 192.168.100.254

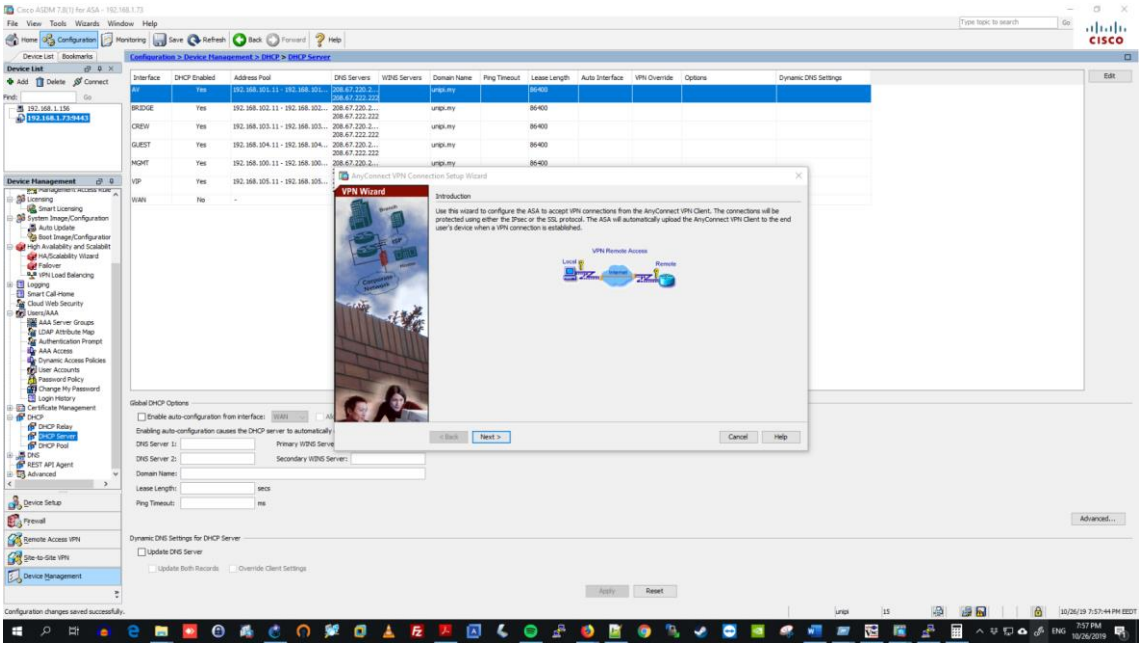
Επειδή υπάρχει μόνο μια φυσική σύνδεση από το interface gi0/1 του MY-ASA προς το MY-SW-01 θα πρέπει να δημιουργηθούν subinterfaces .Τα sub interfaces είναι εικονικά interfaces που μπορούν να περάσουν πολλαπλά δίκτυα πάνω από μια φυσική σύνδεση με την χρήση Vlan (Virtual Lan).Στα subinterfaces που δημιουργήθηκαν BRIDGE,CREW,GUEST,VIP έχουν επίπεδο ασφάλειας 50 ενώ AV έχει 25 ,αυτό σημαίνει ότι και τα τέσσερα μπορούν να δουν το δίκτυο του AV και να χρησιμοποιήσουν τις υπηρεσίες AV. Αλλά το ένα δεν έχει πρόσβαση στο άλλο έτσι επιτυγχάνουμε τον διαχωρισμό και διασφαλίζουμε την μεταξύ τους ασφάλεια.[6][7]

4.2.2.1 MY-ASA SSL VPN

Το Cisco IOS SSL VPN παρέχει συνδεσιμότητα απομακρυσμένης πρόσβασης SSL VPN από σχεδόν οποιαδήποτε τοποθεσία με δυνατότητα Internet χρησιμοποιώντας μόνο ένα web browser που υποστηρίζει τοπικά την κρυπτογράφηση SSL. Αυτή η δυνατότητα επιτρέπει στην εταιρεία να επεκτείνει την πρόσβαση σε οποιονδήποτε εξουσιοδοτημένο χρήστη / εταιρικό πόρο στο ασφαλές

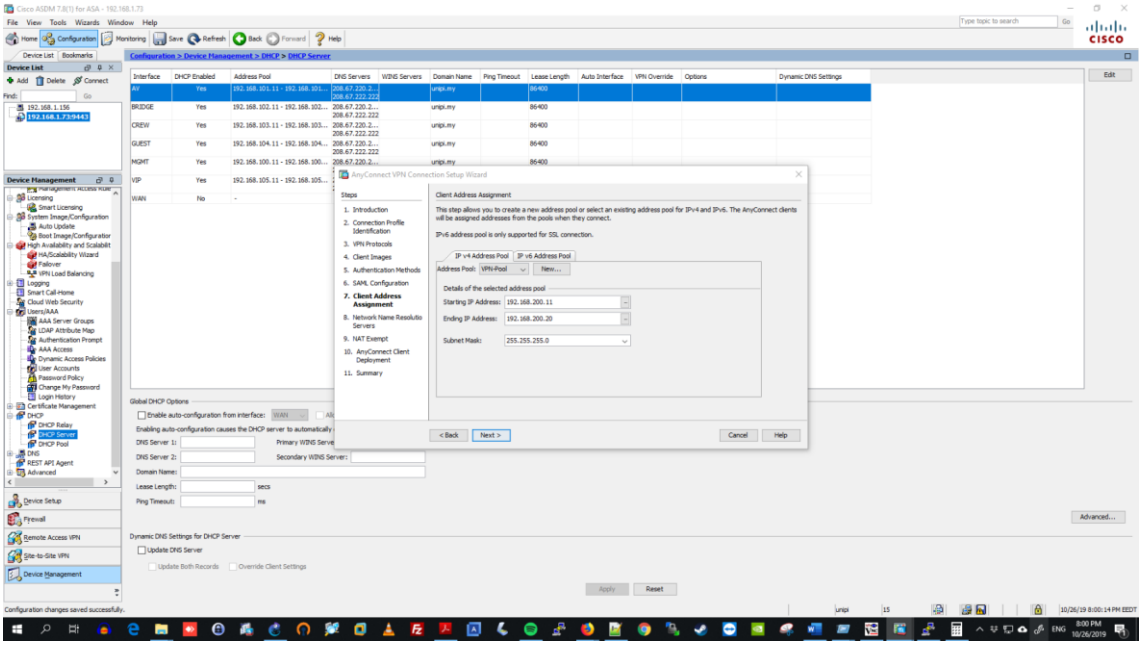
επιχειρησιακό δίκτυο της, παρέχοντας δυνατότητα σύνδεσης από απόσταση από οποιαδήποτε τοποθεσία με δυνατότητα Internet.

Το Cisco IOS SSL VPN θα ενεργοποιηθεί μέσω του ASA με την χρήση Wizard Setup

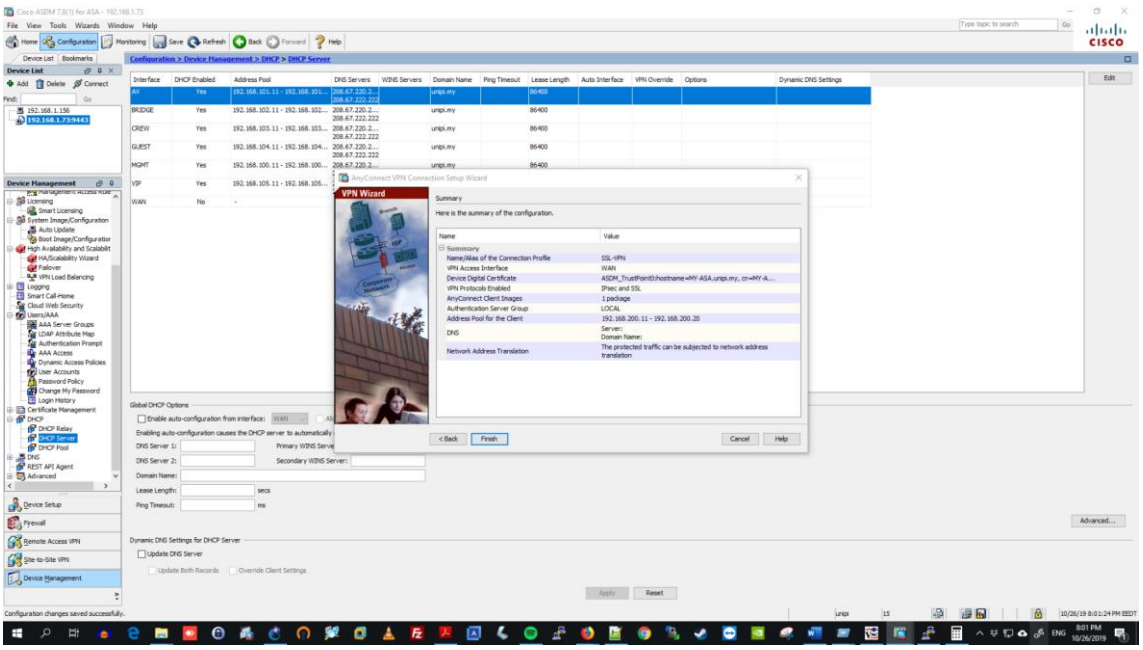


Εικόνα 31:Εναρξη Wizard SSL-VPN

Οι χρήστες που θα συνδεθούν στο SSL-VPN θα πάρουν διεύθυνση IP από το δίκτυο 192.168.200.0/24

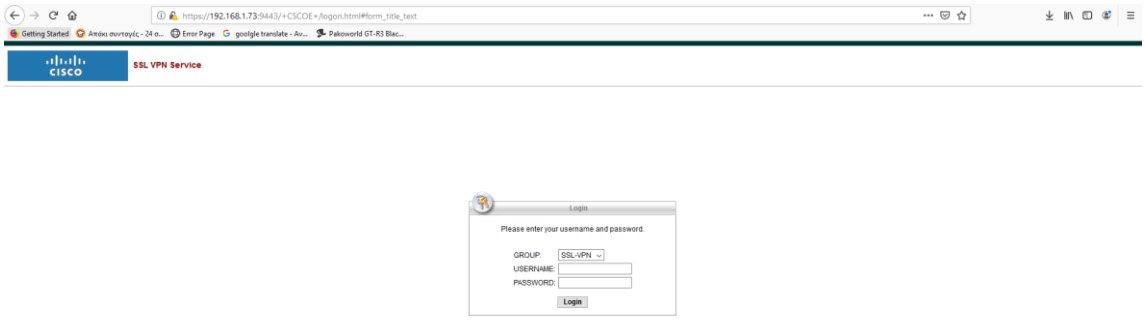


Εικόνα 32:Wizard SSL IP Range χρηστων

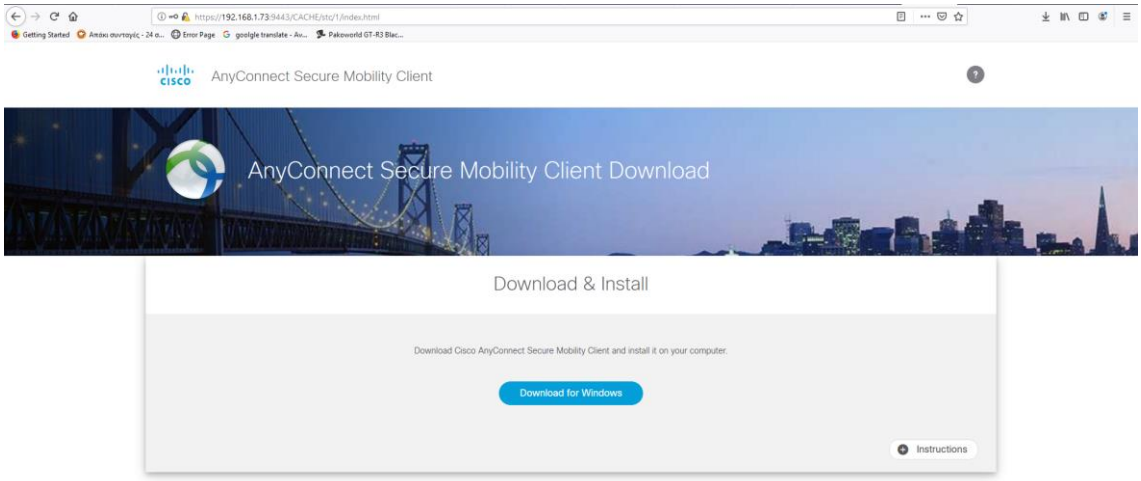


Εικόνα 33:Ολοκληρωση διαδικασίας SSL-VPN

Μόλις ολοκληρωθεί η διαδικασία του Wizard ο χρήστης μπορεί μέσω οποιοδήποτε browser να πάει στο public url του ASA οπου θα του δοθούν οδηγίες εγκατάστασης του Cisco Anyconnect Client



Εικόνα 34:URL Cisco Any Connect



Εικόνα 35:Σελιδα Download Anyconnect Client

4.2.3 MY-SW-01

Τέλος αφού έχει ολοκληρωθεί η παραμετροποιήσεις του ASA μας μένει το Switch MY-SW-01

Εδώ θα συνδεθούν όλες οι υπόλοιπες συσκευές όπως ο WLC(Wireless Lan Controller) ο RADIUS Server και όλα τα Access Points .Οι ρυθμίσεις που πρέπει να γίνουν στο switch είναι πιο απλές καθώς το μεγαλύτερο μέρος το έχει αναλάβει ο ASA.

Πρώτα πρέπει να διασφαλίσουμε επικοινωνία με τον ASA το φυσικό interface του ASA είναι το gigabit Ethernet 0/1 και αυτό συνδέετε στο switch στο interface 3/3

```
interface Ethernet3/3
 description ### Con to ASA ###
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Εικόνα 36:My-Sw-01 Interface σύνδεσης με ASA

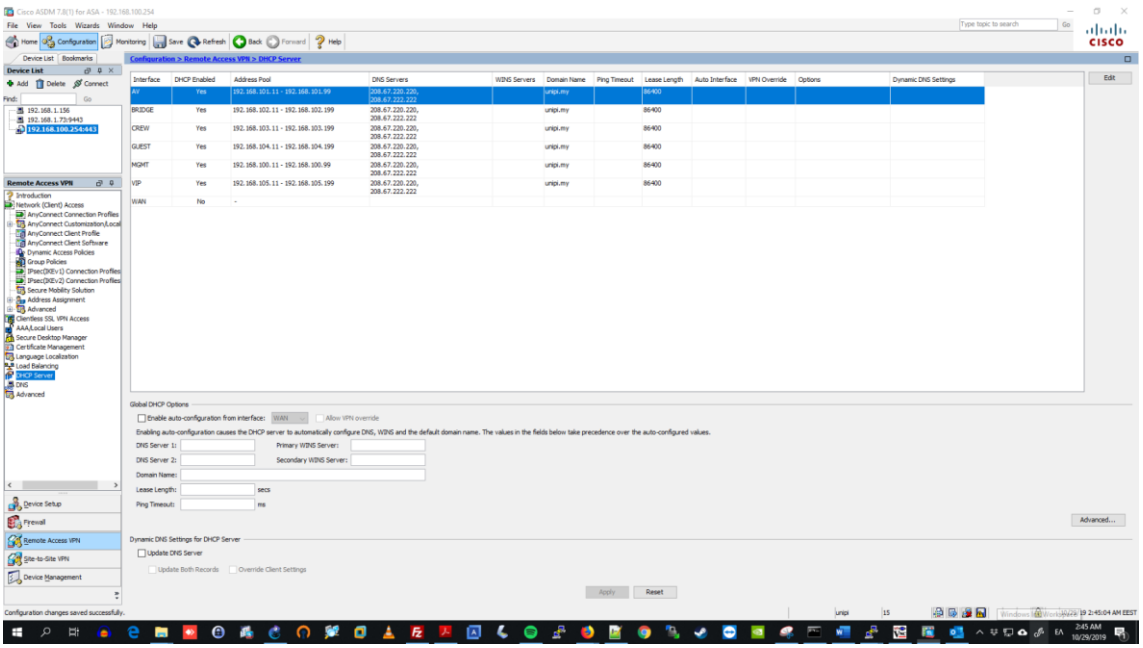
Βάζοντας την θύρα σε mode trunk διασφαλίζουμε ότι θα έχουμε επικοινωνία με όλα τα VLAN που δημιουργήσαμε στον ASA .Στην συνέχεια πρέπει να πάμε στα υπόλοιπα interfaces και ουσιαστικά να ορίσουμε σε ποια Vlan θα εχει πρόσβαση το καθένα. Για μεγαλύτερη ασφάλεια μπορεί να εφαρμοστεί port security δεσμεύοντας έτσι και την MAC Address ενός μηχανήματος η οποία είναι μοναδική και αν προσπαθεί κάποιος να βάλει άλλο διακομιστή η συσκευή πάνω στην θύρα αυτή θα κλείσει .Αυτό γίνεται σε περίπτωση AAA Server η Exchange Server

```
interface Ethernet0/0
 description ### APs ###
 switchport access vlan 100
 switchport mode access
!
interface Ethernet0/1
 description ### APs ###
 switchport access vlan 100
 switchport mode access
!
interface Ethernet0/2
 description ### APs ###
 switchport access vlan 100
 switchport mode access
!
interface Ethernet0/3
 description ### APs ###
 switchport access vlan 100
 switchport mode access
!
interface Ethernet1/0
 description ### TRUNK DECK L0 ###
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```

Εικόνα 37:Εμφανιση όλων των Interface

Όπως δείχνει η προηγουμένη εικόνα τα interfaces Ethernet 0/0-2 είναι ρυθμισμένα να βλέπουμε μόνο το Vlan 100 που θα χρησιμοποιηθεί για τα Access points interface Ethernet 1/0 είναι σε mode trunk ,από την περιγραφή δείχνει ότι πάει στο Lower Deck επίπεδο όπου θα συνδεθεί ένα Access Switch εκεί για εξυπηρετήσει τον όροφο

Το DHCP το οποίο θα αναλάβει να δώσει αυτόματα IP σε οποία συσκευή συνδεθεί επάνω σε κάποιο access switch την έχει αναλάβει ο ASA όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 38:Gui ASDM Menu DHCP POOLS

Σε κάθε interface εχει δημιουργηθεί ένα DHCP pool με ένα συγκεκριμένο ευρως διευθύνσεων που μπορεί να δώσει για κάθε VLAN

Κεφάλαιο 5: Ασφάλεια δικτύου

5.1 Γενικά

Σημαντικός πλέον παράγοντας σε κάθε εγκατάσταση πληροφοριακού συστήματος και δικτύου είναι η ασφάλεια, καθώς μεγαλώνει ο όγκος δεδομένων και η αξία τους Εταιρείες και πάροχοι σπαταλούν εκατομμύρια στο να θωρακίσουν τα συστήματα τους αλλά και να εκπαιδεύσουν το προσωπικό τους σε θέματα ασφάλειας .

Σε αυτό το κεφάλαιο θα αναφέρουμε γενικά τρόπους πως να προστατεύσουμε την εγκατάστασης μας και θα αναλύσουμε συγκεκριμένα τους τρόπους και ποια συστήματα χρησιμοποιήσαμε για να προστατεύσουμε την δική μας εγκατάσταση

Οι τρόποι να εξασφαλίσουμε το πεδίο διαχείρισης μας είναι οι εξής:

Οφείλουμε έχουμε αλλά και να τηρούμε την γραπτή πολιτική που έχει ορίσει ο υπεύθυνος ασφαλείας μας η οποία θα αναφέρει ποιοι έχουν πρόσβαση στον δικτυακό μας εξοπλισμό και σε τι επίπεδο ασφάλειας ο καθένας. Συγκεκριμένα:

1. Εξασφάλιση και θωράκιση της φυσικής πρόσβασης στο χώρο τον οποίο θα φιλοξενείται ο εξοπλισμός μας και τηρούνται οι παρακάτω συνθήκες:

α) Να υπάρχει σύστημα πυρόσβεσης

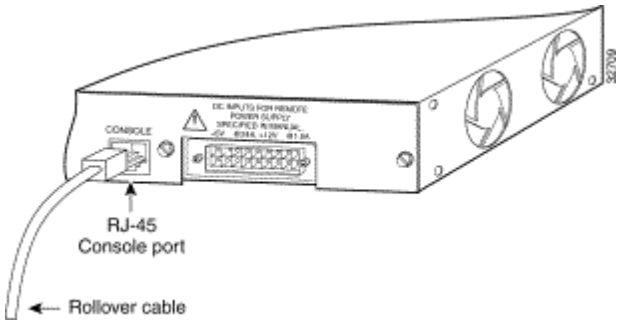
β) Εναλλακτικός τρόπος τροφοδοσίας και περίπτωση απώλειας ρεύματος όπως η χρήση και συντήρηση (UPS)

γ) Έλεγχος επιπέδου θερμοκρασίας αλλά και υγρασίας

δ) Ένας σημαντικός αριθμός ανταλλακτικών στον χώρο

2. Η χρήση κωδίκων αυξημένης πολυπλοκότητας και κρυπτογράφησης ,σε απλές εγκατάστασης με την εφαρμογή πολιτικής ελάχιστων χαρακτήρων .Σε ποιο μεγάλες εγκατάστασης ειδικά με μεγάλο αριθμό χρηστών συνίσταται η χρήση διακομιστή «AAA»*

3. Ο τακτικός έλεγχος των θυρών πρόσβασης του δικτυακού μας εξοπλισμού συγκείμενα οι θύρες διαχείρισης όπως η θύρα κονσόλας (console port ,auxiliary port) αλλά και η θωράκιση και τον πρωτοκόλλων πρόσβασης sash ,telnet τα οποία και αυτά θα πρέπει να έχουν ενσωματωμένο δικού τους κωδικό πρόσβαση.



Εικόνα 39:Γραφικη αναπαρασταση RJ-45 connection

4. Έλεγχος του επιπέδου πρόσβασης στον εξοπλισμό μας . Ο διαχειριστής του συστήματος μας θα πρέπει να ορίσει σε συνεννόηση με τον πελάτη το επίπεδο ασφάλειας που θα έχει ο κάθε χρήστης που θα έχει πρόσβαση στον δικτυακό μας εξοπλισμό . Κάποιες χρήστες θα έχουν πλήρες πρόσβαση σε όλο το επίπεδο του λειτουργικού του εξοπλισμού δηλαδή να μπορεί να τροποποίηση η και να σβήσει το αρχείο ρυθμίσεων του εξοπλισμού , άλλοι θα μπορούν απλά να το διαβάσουν σε περίπτωση που χρειάζονται να έχουν κάποια στοιχεία (αυτό συνήθως γίνεται σε εξωτερικούς συνεργάτες που υστέρα να κάνουν αίτηση στον διαχειριστή για οποία επιλογή επιθυμούν).

5. Η χρήση ασφαλών πρωτοκόλλων διαχείρισης του εξοπλισμού . Οι τρόποι με τους οποίους δίνεται η δυνατότητα εισόδου στον εξοπλισμού μας απομακρυσμένα είναι η με το πρωτόκολλο ssh , telnet η Http συνήθως αντί του πρωτοκόλλου telnet προτιμάμε το ssh και σε περίπτωση που θα χρησιμοποιήσουμε το πρωτόκολλο HTTP προτιμούμε την αυξημένης ασφάλειας έκδοση του HTTPS .

Αν για κάποιο λόγο δεν μας δίνεται η ευκαιρία να χρησιμοποιήσουμε αυτά τα πρωτοκολλά και αναγκαζόμαστε για κάποια λόγο να χρησιμοποιήσουμε τα λιγότερα ασφαλή τότε θα προβούμε στην χρήση του πρωτοκόλλου ‘’εικονικού προσωπικού δίκτυο’’ η VPN ώστε να εξασφαλίσουμε την κρυπτογράφηση όλης της δικτυακής μας κίνησης. Για το πρωτόκολλο VPN θα μιλήσουμε αναλυτικά στην συνέχεια του κεφαλαίου.

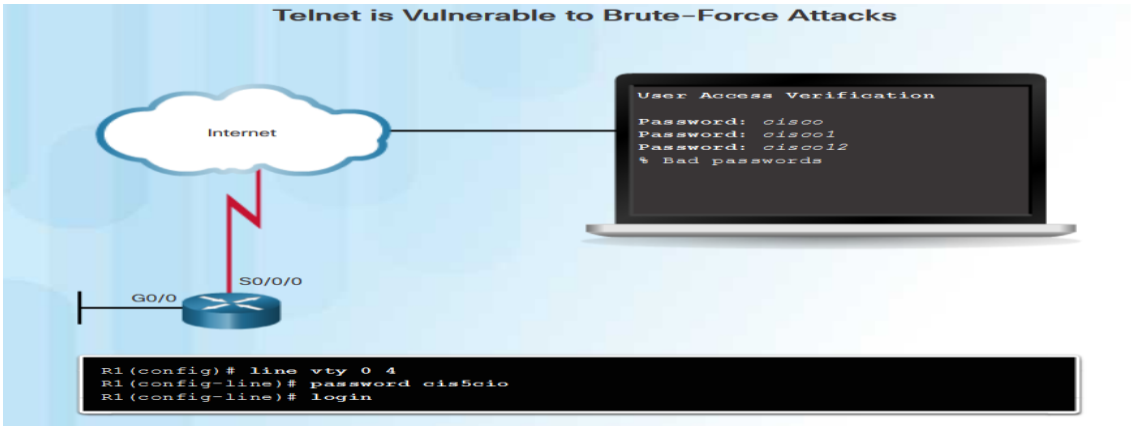
6. Η εφαρμογή λογισμικού καταγραφής συστήματος (syslog). Με την εφαρμογή του συστήματος αυτού μπορούμε να έχουμε ιστορικό δικτυακής κίνησης αλλά και με την οποία θα μπορούμε να παρακολουθούμε όποια κίνηση γίνεται στο δίκτυο αλλά και ποιος πραγματοποιεί αυτή την κίνηση . Με αυτό θα μπορέσουμε να εντοπίσουμε ασυνήθιστη και ύποπτη κίνηση στον δίκτυο μας και με αυτό το τρόπο ουσιαστικά να αποφύγουμε τυχόν επίθεσης η και σφάλματα.

7. Τέλος η συχνή λήψη αντιγράφων ασφάλειας και η δημιουργία αρχείου με όλες της διαδικασίες που έχουμε ακολουθήσει στην εγκατάσταση μας αλλά και την τοποθεσία που αποθηκεύονται τα αντίγραφα ασφάλειας μας επίσης να περιέχει και την διαδικασία αποκατάστασή του συστήματος σε περίπτωση καταστροφής . Όσον αφορά τα αντίγραφα θα πρέπει εκτός από την τοποθεσία του έργου να υπάρχουν και σε χώρο εκτός αρχικής τοποθεσίας.[6]

5.2 Έλεγχος ταυτότητας χωρίς AAA

Οι χάκερ των δικτύων μπορούν να αποκτήσουν πρόσβαση σε ευαίσθητο εξοπλισμό και υπηρεσίες δικτύου. Ο έλεγχος πρόσβασης περιορίζει ποιος ή τι μπορεί να χρησιμοποιήσει συγκεκριμένους πόρους. Περιορίζει επίσης τις υπηρεσίες ή τις επιλογές που είναι διαθέσιμες μετά τη χορήγηση της πρόσβασης. Πολλοί τύποι ελέγχου ταυτότητας μπορούν να εκτελεστούν σε μια συσκευή Cisco και κάθε μέθοδος προσφέρει διαφορετικά επίπεδα ασφάλειας.

Η απλούστερη μέθοδος επαλήθευσης απομακρυσμένης πρόσβασης είναι να διαμορφώσετε έναν συνδυασμό σύνδεσης και κωδικού πρόσβασης στις κονσόλες, τις γραμμές vty και τις θύρες aux, όπως φαίνεται στην παρακάτω εικόνα:

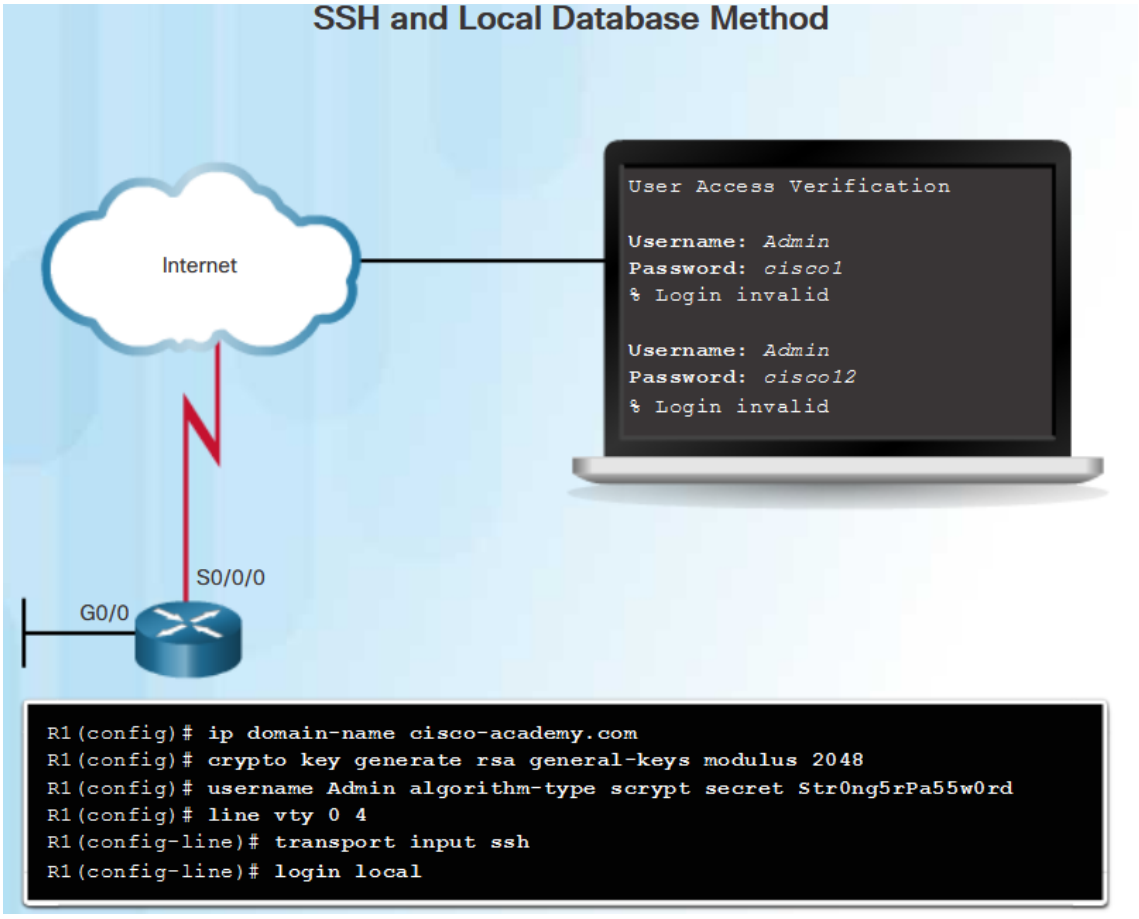


Εικόνα 40:Telnet Vulnerability πηγη www.netacad.com

Αυτή η μέθοδος είναι η πιο εύκολη στην εφαρμογή, αλλά είναι και η πιο αδύνατη και λιγότερο ασφαλής. Αυτή η μέθοδος δεν παρέχει λογοδοσία. Όποιος έχει τον κωδικό πρόσβασης μπορεί να εισέλθει στη συσκευή και να αλλάξει τη διαμόρφωση.

Το SSH είναι μια ασφαλέστερη μορφή απομακρυσμένης πρόσβασης. Απαιτεί τόσο όνομα χρήστη όσο και κωδικό πρόσβασης, και τα δύο κρυπτογραφούνται κατά τη διάρκεια των μεταδόσεων. Η μέθοδος της τοπικής βάσης δεδομένων παρέχει πρόσθετη ασφάλεια, επειδή ένας εισβολέας πρέπει να γνωρίζει ένα όνομα χρήστη και έναν κωδικό πρόσβασης. Παρέχει επίσης μεγαλύτερη υπευθυνότητα, επειδή το όνομα χρήστη καταγράφεται όταν κάποιος χρήστης συνδεθεί. Παρόλο που το Telnet μπορεί να ρυθμιστεί χρησιμοποιώντας ένα όνομα χρήστη και έναν κωδικό πρόσβασης, και οι δύο αποστέλλονται σε απλό κείμενο, το οποίο τον καθιστά ευάλωτο σε καταγραφή και εκμετάλλευση.

Η μέθοδος της τοπικής βάσης δεδομένων έχει ορισμένους περιορισμούς. Οι λογαριασμοί χρηστών πρέπει να διαμορφώνονται τοπικά σε κάθε συσκευή, όπως φαίνεται για τη διαμόρφωση του SSH στην παρακάτω εικόνα:



Εικόνα 41:Προσβαση σε router μεσω ssh πηγη www.netacad.com

Σε ένα μεγάλο περιβάλλον επιχείρησης που έχει πολλούς δρομολογητές και διακόπτες για διαχείριση, μπορεί να χρειαστεί χρόνος για την υλοποίηση και την αλλαγή τοπικών βάσεων δεδομένων σε κάθε συσκευή. Επιπλέον, η ρύθμιση παραμέτρων της τοπικής βάσης δεδομένων δεν παρέχει μέθοδο εναλλαγής ταυτότητας. Για παράδειγμα, τι γίνεται αν ο διαχειριστής ξεχάσει το όνομα χρήστη και τον κωδικό πρόσβασης για αυτήν τη συσκευή; Αν δεν υπάρχει διαθέσιμη μέθοδος δημιουργίας αντιγράφων ασφαλείας για έλεγχο ταυτότητας, η επαναφορά κωδικού πρόσβασης γίνεται η μόνη επιλογή.

Μια καλύτερη λύση είναι να έχετε όλες τις συσκευές να ανατρέχουν στην ίδια βάση δεδομένων με ονόματα χρήστη και κωδικούς πρόσβασης από κεντρικό διακομιστή. Αυτό το κεφάλαιο εξετάζει τις διάφορες μεθόδους εξασφάλισης της πρόσβασης στο δίκτυο με χρήση του ελέγχου ταυτότητας, της εξουσιοδότησης και της λογιστικής (AAA) για τη διασφάλιση δρομολογητών Cisco.

5.3 Συστατικά AAA

Οι υπηρεσίες ασφάλειας δικτύου AAA παρέχουν το πρωτεύον πλαίσιο για τη ρύθμιση του ελέγχου πρόσβασης σε μια συσκευή δικτύου. Το AAA είναι ένας τρόπος για τον έλεγχο του ποιος μπορεί να έχει πρόσβαση σε ένα δίκτυο (έλεγχος ταυτότητας), τι μπορούν να κάνουν ενώ βρίσκονται εκεί (εξουσιοδοτεί) και να ελέγχει ποιες ενέργειες πραγματοποίησαν κατά την πρόσβαση στο δίκτυο (λογιστική).

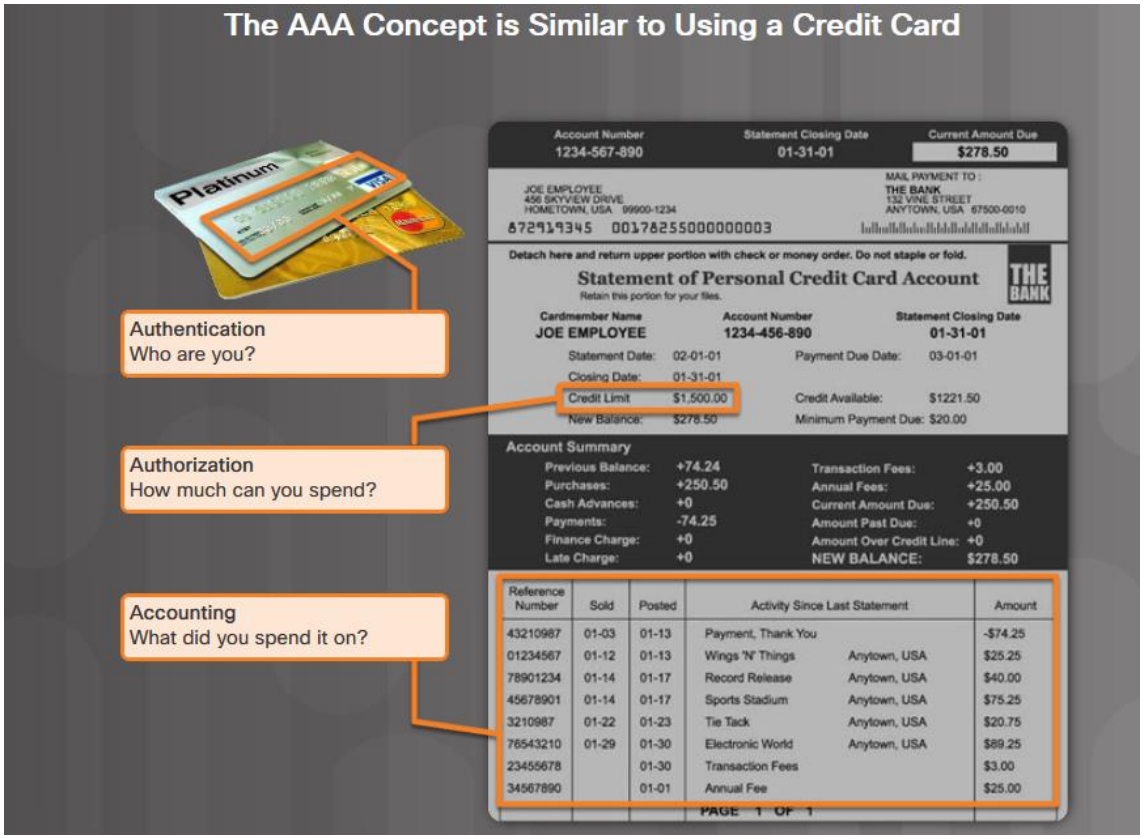
Η δικτυακή και διοικητική ασφάλεια AAA στο περιβάλλον της Cisco έχει τρία λειτουργικά στοιχεία:

Έλεγχος ταυτότητας - Οι χρήστες και οι διαχειριστές πρέπει να αποδείξουν ότι είναι αυτοί που λένε ότι είναι. Ο έλεγχος ταυτότητας μπορεί να δημιουργηθεί χρησιμοποιώντας συνδυασμούς ονόματος χρήστη και κωδικού πρόσβασης, ερωτήσεις πρόκλησης και απάντησης, καρτέλες συμβόλων και άλλες μεθόδους. Για παράδειγμα: "Είμαι φοιτητής χρήστης και γνωρίζω τον κωδικό πρόσβασης για να το αποδείξω".

Εξουσιοδότηση - Μετά την επαλήθευση του χρήστη, οι υπηρεσίες εξουσιοδότησης καθορίζουν ποιοι πόροι μπορεί να έχει πρόσβαση ο χρήστης και ποιες λειτουργίες του επιτρέπει ο χρήστης. Ένα παράδειγμα είναι ότι "ο φοιτητής χρήστης" μπορεί να έχει πρόσβαση στον κεντρικό διακομιστήXYZ χρησιμοποιώντας μόνο SSH. "

Λογιστική και έλεγχος - Η λογιστική καταγράφει τι κάνει ο χρήστης, συμπεριλαμβανομένου του προσπελάσιμου, του χρονικού διαστήματος στο οποίο έχει πρόσβαση ο πόρος και των τυχόν αλλαγών που έγιναν. Η λογιστική παρακολουθεί τον τρόπο με τον οποίο χρησιμοποιούνται οι πόροι δικτύου. Ένα παράδειγμα είναι ο "εξυπηρετητής" χρήστης που έχει πρόσβαση στον κεντρικό διακομιστήXYZ χρησιμοποιώντας SSH για 15 λεπτά. "

Αυτή η έννοια είναι παρόμοια με τη χρήση πιστωτικής κάρτας, όπως υποδεικνύεται από το σχήμα. Η πιστωτική κάρτα προσδιορίζει ποιος μπορεί να το χρησιμοποιήσει, πόσο μπορεί να ξοδέψει ο χρήστης και διατηρεί λογαριασμό για τα στοιχεία ή τις υπηρεσίες που αγόρασε ο χρήστης.

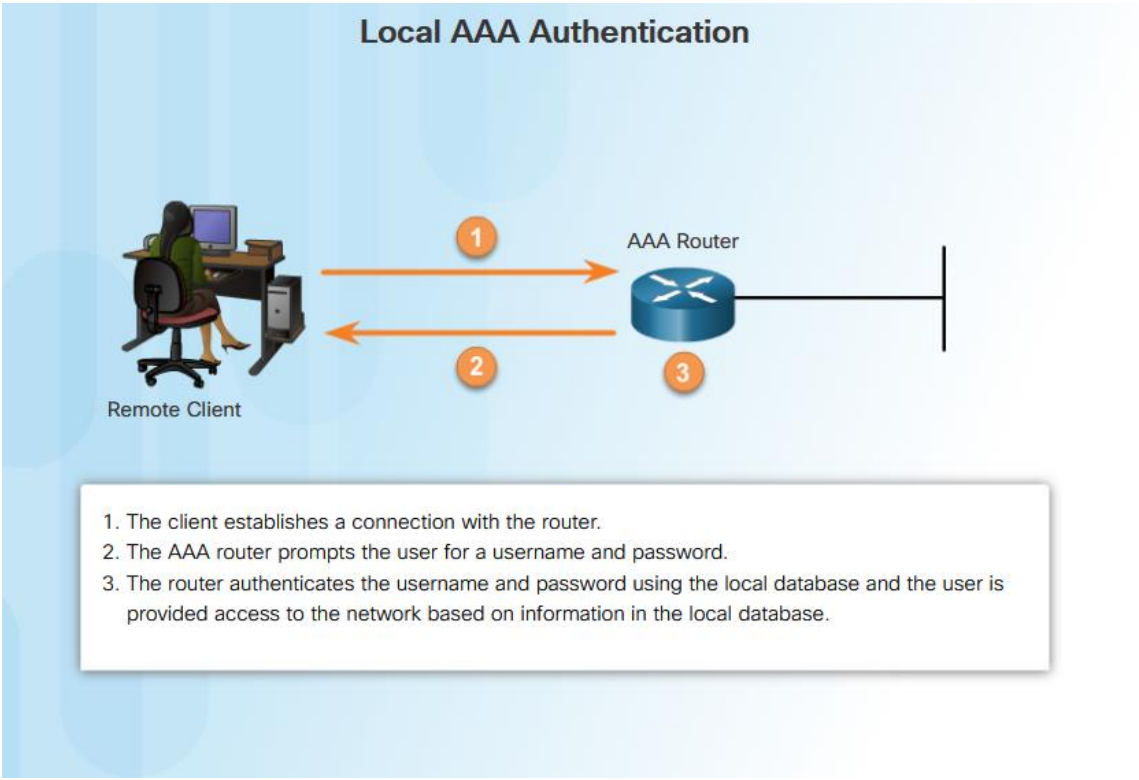


Εικόνα 42:Λειτουργια AAA με παραδειγμα "αγορα με πιστωτικη καρτα"πηγη www.netacad .com

5.3.1 Τρόποι ελέγχου ταυτότητας

Ο έλεγχος ταυτότητας AAA μπορεί να χρησιμοποιηθεί για τον έλεγχο ταυτότητας χρηστών για πρόσβαση διαχειριστή ή μπορεί να χρησιμοποιηθεί για τον έλεγχο ταυτότητας χρηστών για απομακρυσμένη πρόσβαση στο δίκτυο. Η Cisco παρέχει δύο κοινές μεθόδους εφαρμογής των υπηρεσιών AAA:

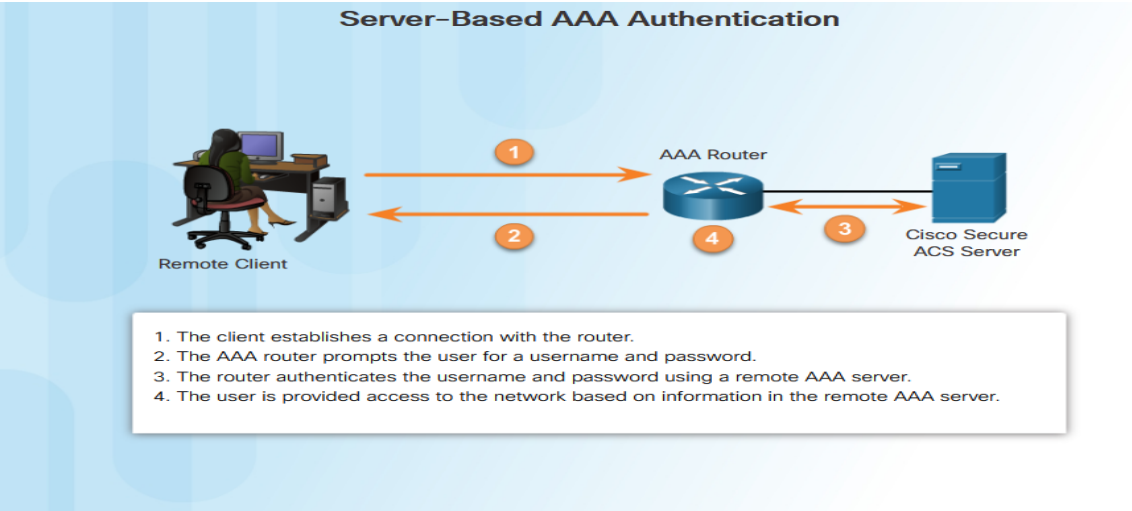
Τοπικός έλεγχος ταυτότητας AAA - Το τοπικό AAA χρησιμοποιεί μια τοπική βάση δεδομένων για έλεγχο ταυτότητας. Αυτή η μέθοδος είναι μερικές φορές γνωστή ως αυτοτελής έλεγχος ταυτότητας. Σε αυτήν την πορεία, θα αναφέρεται ως τοπικός έλεγχος ταυτότητας AAA. Αυτή η μέθοδος αποθηκεύει τα ονόματα χρηστών και τους κωδικούς πρόσβασης τοπικά στο δρομολογητή Cisco και οι χρήστες εξακριβώνουν την ταυτότητά τους έναντι της τοπικής βάσης δεδομένων, όπως φαίνεται στο σχήμα . Αυτή η βάση δεδομένων είναι η ίδια που απαιτείται για τον καθορισμό του CLI με βάση το ρόλο. Το τοπικό AAA είναι ιδανικό για μικρά δίκτυα.[8][6]



Εικόνα 43: Τοπικός έλεγχος ταυτότητας AAA πηγη www.netacad.com

Έλεγχος ταυτότητας AAA βάσει διακομιστή - Με τη μέθοδο που βασίζεται σε διακομιστές, ο δρομολογητής αποκτά πρόσβαση σε έναν κεντρικό διακομιστή AAA, όπως το Cisco Secure Access Control System (ACS) για τα Windows, που παρουσιάζεται στο Σχήμα . Ο κεντρικός διακομιστής AAA περιέχει τα ονόματα χρηστών και τον κωδικό πρόσβασης για όλους χρήστες. Ο δρομολογητής χρησιμοποιεί είτε τα πρωτόκολλα του Remote Authentication Dial-In User Service (RADIUS) είτε το πρωτόκολλα TACACS + για την επικοινωνία με το Terminal Access Controller

(TACACS +) για επικοινωνία με τον διακομιστή AAA. Όταν υπάρχουν πολλοί δρομολογητές και διακόπτες, το διακομιστή AAA είναι πιο κατάλληλη



Εικόνα 44: Έλεγχος ταυτότητας AAA βάσει διακομιστή πηγη www.netacad.com

Εξουσιοδότηση

Μετά την επιτυχή πιστοποίηση των χρηστών με βάση την επιλεγμένη πηγή δεδομένων AAA, είτε τοπική είτε βασισμένη σε διακομιστή, τότε εξουσιοδοτούνται για συγκεκριμένους πόρους δικτύου, όπως φαίνεται στο σχήμα. Η εξουσιοδότηση είναι βασικά αυτό που οι χρήστες μπορούν και δεν μπορούν να κάνουν στο δίκτυο μετά την πιστοποίησή τους. Αυτό είναι παρόμοιο με το πώς τα επίπεδα προνομίων και το CLI που βασίζονται σε ρόλους παρέχουν στους χρήστες συγκεκριμένα δικαιώματα και προνόμια σε ορισμένες εντολές του δρομολογητή.

Η εξουσιοδότηση υλοποιείται συνήθως χρησιμοποιώντας μια λύση που βασίζεται σε διακομιστές AAA. Η εξουσιοδότηση χρησιμοποιεί ένα δημιουργημένο σύνολο χαρακτηριστικών που περιγράφει την πρόσβαση του χρήστη στο δίκτυο. Αυτά τα χαρακτηριστικά συγκρίνονται με τις πληροφορίες που περιέχονται στη βάση δεδομένων AAA και ο προσδιορισμός των περιορισμών για αυτόν τον χρήστη γίνεται και παραδίδεται στον τοπικό δρομολογητή όπου είναι συνδεδεμένος ο χρήστης.

Η εξουσιοδότηση είναι αυτόματη και δεν απαιτεί από τους χρήστες να εκτελούν πρόσθετα βήματα μετά τον έλεγχο ταυτότητας. Η εξουσιοδότηση υλοποιείται αμέσως μετά την επικύρωση του χρήστη.

Λογιστική

Η υπηρεσία AAA Accounting συλλέγει και αναφέρει δεδομένα χρήσης. Αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν για σκοπούς όπως ο έλεγχος ή η τιμολόγηση. Τα δεδομένα που συλλέχθηκαν ενδέχεται να περιλαμβάνουν τους χρόνους σύνδεσης και εκκίνησης, τις εντολές που εκτελούνται, τον αριθμό των πακέτων και τον αριθμό των byte.

Η λογιστική υλοποιείται χρησιμοποιώντας μια λύση βασισμένη σε διακομιστές AAA. Αυτή η υπηρεσία αναφέρει τα στατιστικά χρήσης πίσω στον εξυπηρετητή ACS. Αυτά τα στατιστικά στοιχεία μπορούν να εξαχθούν για να δημιουργηθούν λεπτομερείς αναφορές σχετικά με τη διαμόρφωση του δικτύου.

Μια ευρέως χρησιμοποιούμενη χρήση της λογιστικής είναι να συνδυαστεί με την αυθεντικότητα AAA. Αυτό βοηθά στη διαχείριση της πρόσβασης σε συσκευές δια δικτύωσης από το προσωπικό διαχείρισης του δικτύου. Η λογιστική παρέχει περισσότερη ασφάλεια από τον έλεγχο ταυτότητας. Οι διακομιστές AAA διατηρούν ένα λεπτομερές αρχείο καταγραφής ακριβώς του τι κάνει ο πιστοποιημένος χρήστης στη συσκευή, όπως φαίνεται στο σχήμα 1. Περιλαμβάνει όλες τις εντολές EXEC και διαμόρφωσης που εκδόθηκαν από το χρήστη. Το αρχείο καταγραφής περιέχει πολλά πεδία δεδομένων, συμπεριλαμβανομένου του ονόματος χρήστη, της ημερομηνίας και της ώρας και της πραγματικής εντολής που εισήχθη από το χρήστη. Αυτές οι πληροφορίες είναι χρήσιμες κατά την αντιμετώπιση προβλημάτων συσκευών. Παρέχει επίσης μοχλεύσει έναντι ατόμων που εκτελούν κακόβουλες ενέργειες.[6]

Επαλήθευση της πρόσβασης διαχειριστή

Ο τοπικός έλεγχος ταυτότητας AAA πρέπει να διαμορφωθεί για μικρότερα δίκτυα. Τα μικρότερα δίκτυα είναι εκείνα τα δίκτυα που διαθέτουν έναν ή δύο δρομολογητές που παρέχουν πρόσβαση σε περιορισμένο αριθμό χρηστών. Αυτή η μέθοδος χρησιμοποιεί τα τοπικά ονόματα χρήστη και τους κωδικούς πρόσβασης που είναι αποθηκευμένοι σε δρομολογητή. Ο διαχειριστής συστήματος πρέπει να συμπληρώσει την τοπική βάση δεδομένων ασφαλείας καθορίζοντας τα προφίλ χρήστη και κωδικού πρόσβασης για κάθε χρήστη που μπορεί να συνδεθεί.

Η μέθοδος Local Authentication AAA είναι παρόμοια με τη χρήση της τοπικής εντολής σύνδεσης με μία εξαίρεση. Το AAA παρέχει επίσης έναν τρόπο ρύθμισης των μεθόδων δημιουργίας αντιγράφων ασφαλείας των στοιχείων ταυτότητας.

Η διαμόρφωση τοπικών υπηρεσιών AAA για την επαλήθευση της πρόσβασης διαχειριστή απαιτεί μερικά βασικά βήματα:

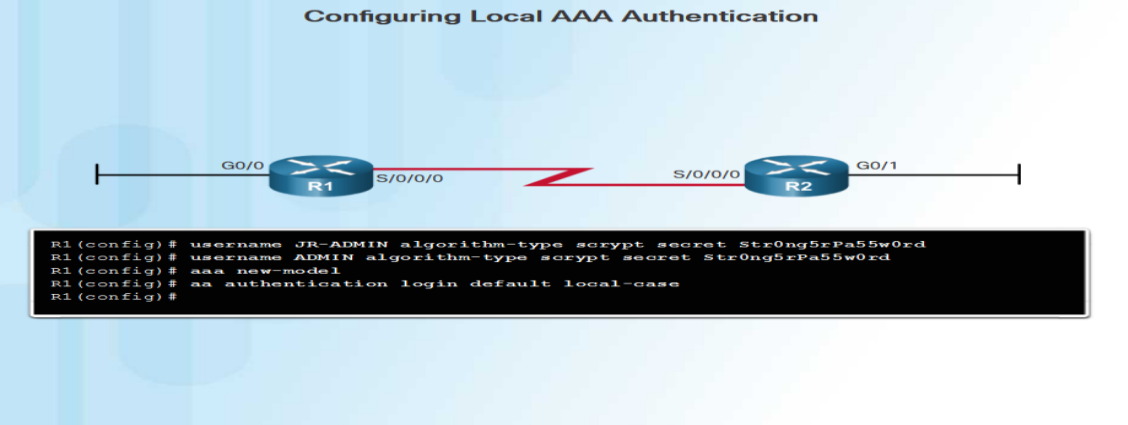
Βήμα 1. Προσθέστε ονόματα χρήστη και κωδικούς πρόσβασης στη βάση δεδομένων τοπικού δρομολογητή για χρήστες που χρειάζονται πρόσβαση διαχειριστή στο δρομολογητή.

Βήμα 2. Ενεργοποιήστε AAA σε όλο τον δρομολογητή.

Βήμα 3. Διαμορφώστε τις παραμέτρους AAA στον δρομολογητή.

Βήμα 4. Επιβεβαιώστε και αντιμετωπίσετε τη διαμόρφωση AAA.

Η εντολή σύνδεσης aaa για την επαλήθευση ταυτότητας στο σχήμα επιτρέπει στους χρήστες ADMIN και JR-ADMIN να συνδεθούν στο δρομολογητή μέσω των γραμμών τερματικών κονσόλας ή vty. Η προεπιλεγμένη λέξη-κλειδί σημαίνει ότι η μέθοδος ελέγχου ταυτότητας ισχύει για όλες τις γραμμές, εκτός από εκείνες για τις οποίες μια συγκεκριμένη ρύθμιση γραμμής υπερισχύει της προεπιλεγμένης. Ο έλεγχος ταυτότητας γίνεται διάκριση πεζών - κεφαλαίων, που υποδεικνύεται από τη λέξη-κλειδί τοπικής περίπτωσης Αυτό σημαίνει ότι τόσο ο κωδικός πρόσβασης όσο και το όνομα χρήστη κάνουν διάκριση πεζών-κεφαλαίων.



Εικόνα 45:Εντολες παραμετροποιησεις τοπικου ελεγχου AAA

Μέθοδοι ελέγχου ταυτότητας

Για να ενεργοποιήσετε το AAA, πρέπει πρώτα να ρυθμιστεί η εντολή global aaa global model configuration. Για να απενεργοποιήσετε το AAA, χρησιμοποιήστε τη μηδενική μορφή αυτής της εντολής.

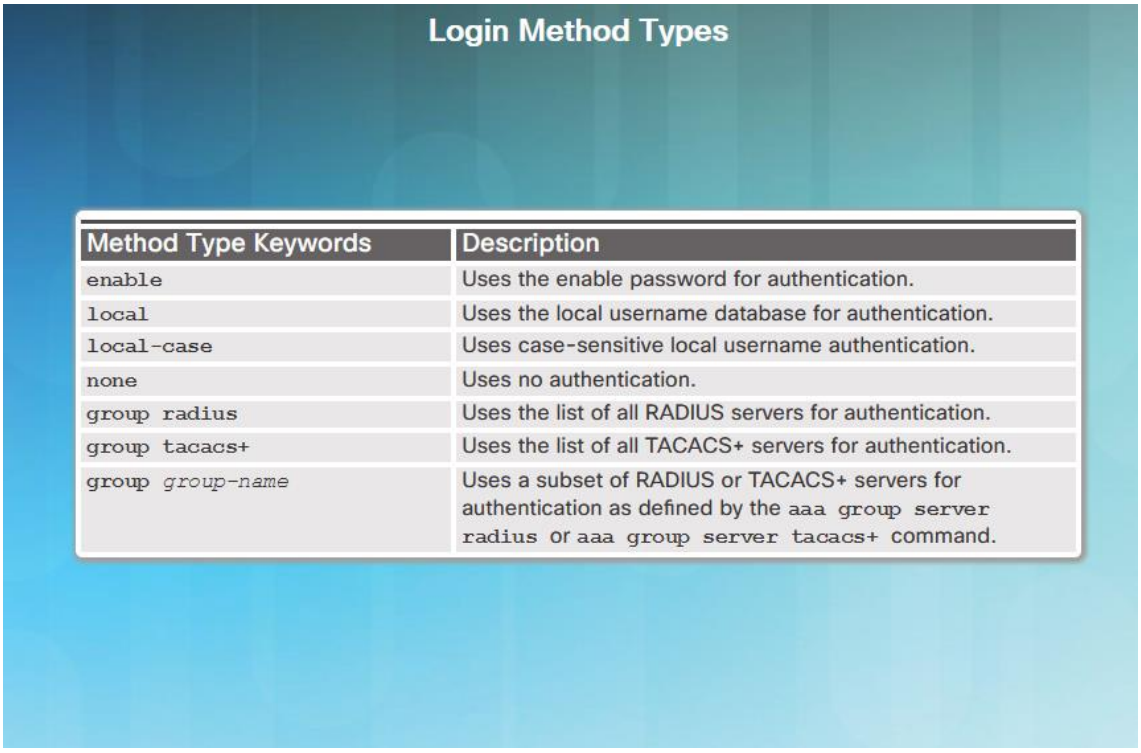
Σημείωση 1: Δεν υπάρχουν άλλες εντολές AAA μέχρι να εισαχθεί αυτή η εντολή.

Σημείωση 2: Είναι σημαντικό να γνωρίζετε ότι όταν εισάγεται αρχικά η εντολή aaa new-model, ένας μη αναγνωσμένος "προεπιλεγμένος" έλεγχος ταυτότητας που χρησιμοποιεί την τοπική βάση δεδομένων εφαρμόζεται αυτόματα σε όλες τις γραμμές εκτός από την κονσόλα. Για το λόγο αυτό, ρυθμίστε πάντα μια καταχώρηση τοπικής βάσης δεδομένων πριν ενεργοποιήσετε το AAA.

Χρησιμοποιήστε την εντολή σύνδεσης aaa authentication που φαίνεται στο σχήμα για να ενεργοποιήσετε τον έλεγχο ταυτότητας των γραμμών κονσόλας, aux και vty. Η προεπιλεγμένη λέξη-κλειδί εφαρμόζει τον έλεγχο ταυτότητας σε όλες τις γραμμές. Εναλλακτικά, μια προσαρμοσμένη μέθοδος ελέγχου ταυτότητας μπορεί να ρυθμιστεί χρησιμοποιώντας ένα όνομα-λίστας.[8]

Εικόνα 46:Συνταξη εντολης σε router για την ενεργοποιηση AAA

Το τελικό τμήμα της εντολής προσδιορίζει τον τύπο των μεθόδων που θα ερωτηθούν για τον έλεγχο ταυτότητας των χρηστών. Μπορούν να καθοριστούν έως και τέσσερις μέθοδοι, παρέχοντας εναλλακτικές μεθόδους εάν δεν είναι διαθέσιμη μια μέθοδος. Το σχήμα δείχνει κοινές μεθόδους που μπορούν να καθοριστούν. Όταν ένας χρήστης επιχειρεί να συνδεθεί, χρησιμοποιείται η πρώτη μέθοδος που αναφέρεται. Το λογισμικό Cisco IOS επιχειρεί τον έλεγχο ταυτότητας με την επόμενη εγκεκριμένη μέθοδο επαλήθευσης μόνο όταν δεν υπάρχει απόκριση ή υπάρχει λάθος από την προηγούμενη μέθοδο. Εάν η μέθοδος ελέγχου ταυτότητας αποκλείει την πρόσβαση του χρήστη, η διαδικασία ελέγχου ταυτότητας σταματά και δεν επιτρέπονται άλλες μέθοδοι επαλήθευσης ταυτότητας.



Εικόνα 47:Μεθοδοι απομακρυσμένης πρόσβασης σε δικτυακό εξοπλισμό

Για να ενεργοποιήσετε τον τοπικό έλεγχο ταυτότητας χρησιμοποιώντας μια προκαθορισμένη τοπική βάση δεδομένων, χρησιμοποιήστε τη λέξη-κλειδί τοπική ή τοπική περίπτωση. Η διαφορά μεταξύ των δύο επιλογών είναι ότι ο τοπικός χρήστης δέχεται ένα όνομα χρήστη ανεξάρτητα από την περίπτωση, ενώ στην τοπική περίπτωση γίνεται διάκριση πεζών-κεφαλαίων. Για παράδειγμα, εάν μια τοπική καταχώρηση βάσης δεδομένων με το όνομα χρήστη ADMIN έχει ρυθμιστεί, η τοπική μέθοδος θα δέχεται ADMIN, Admin ή ακόμα και admin. Εάν η μέθοδος τοπικής περίπτωσης διαμορφώθηκε, τότε θα ήταν αποδεκτή μόνο το ADMIN.

Για να καθορίσετε ότι ένας χρήστης μπορεί να πιστοποιήσει τον έλεγχο ταυτότητας χρησιμοποιώντας τον κωδικό ενεργοποίησης, χρησιμοποιήστε τη λέξη-κλειδί ενεργοποίησης. Για να εξασφαλιστεί ότι ο έλεγχος ταυτότητας είναι επιτυχής, ακόμη και αν όλες οι μέθοδοι επιστρέψουν ένα σφάλμα, δεν καθορίστε κανένα ως την τελική μέθοδο

5.4 Χρήση Συστημάτων Αναγνώρισης και Πιστοποίησης Χρηστών(Radius)

5.4.1 Radius

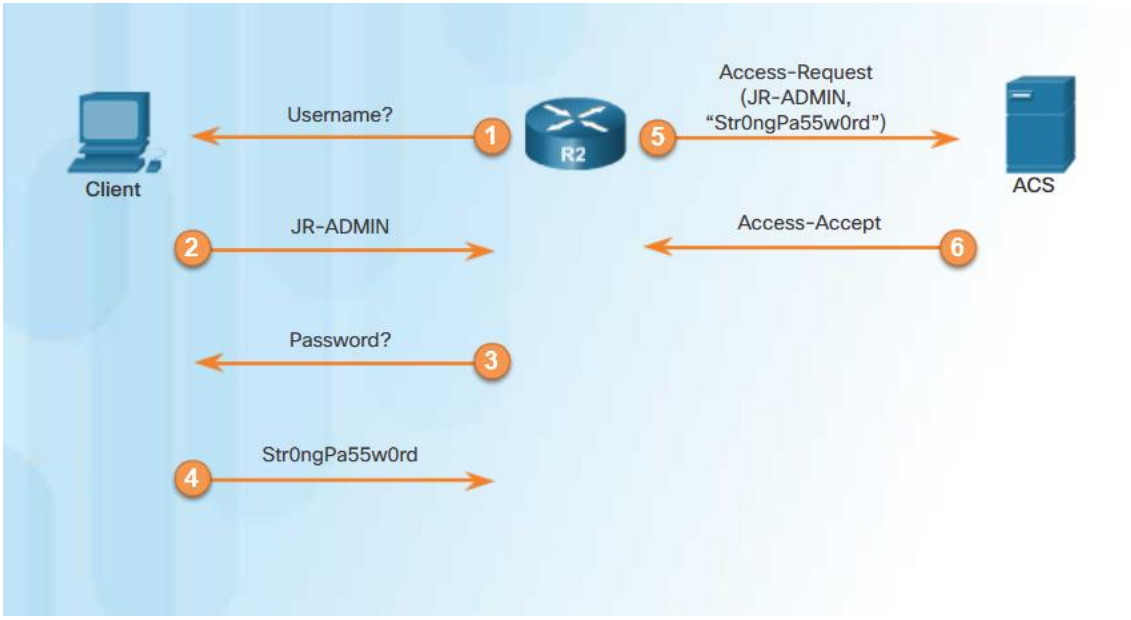
Το RADIUS, το οποίο αναπτύχθηκε από την Livingston Enterprises, είναι ένα ανοικτό πρότυπο πρωτόκολλο AAA IETF για εφαρμογές όπως η πρόσβαση στο δίκτυο ή η κινητικότητα IP. Το RADIUS λειτουργεί τόσο σε τοπικές όσο και σε περιαγωτικές καταστάσεις και χρησιμοποιείται συνήθως για λογιστικούς σκοπούς. Το RADIUS ορίζεται σήμερα από τα RFC 2865, 2866, 2867, 2868, 3162 και 6911.

Το πρωτόκολλο RADIUS αποκρύπτει κωδικούς πρόσβασης κατά τη διάρκεια της μετάδοσης, ακόμη και με το πρωτόκολλο ελέγχου ταυτότητας με κωδικό πρόσβασης (PAP), χρησιμοποιώντας μια μάλλον πολύπλοκη λειτουργία που περιλαμβάνει το hashing και ένα κοινό μυστικό του Message Digest 5 (MD5). Ωστόσο, το υπόλοιπο του πακέτου αποστέλλεται σε απλό κείμενο.

Το RADIUS συνδυάζει τον έλεγχο ταυτότητας και την εξουσιοδότηση ως μία διαδικασία. Όταν ένας χρήστης έχει πιστοποιηθεί, αυτός ο χρήστης είναι επίσης εξουσιοδοτημένος. Το RADIUS χρησιμοποιεί θύρα UDP 1645 ή 1812 για έλεγχο ταυτότητας και θύρα UDP 1646 ή 1813 για λογιστική.

Το RADIUS χρησιμοποιείται ευρέως από τους παρόχους υπηρεσιών VoIP. Παρέχει τα διαπιστευτήρια σύνδεσης ενός τελικού σημείου SIP, όπως ένα ευρυζωνικό τηλέφωνο, σε έναν καταχωρητή SIP χρησιμοποιώντας έλεγχο ταυτότητας digest, και έπειτα σε ένα διακομιστή RADIUS που χρησιμοποιεί το RADIUS. Το RADIUS είναι επίσης ένα κοινό πρωτόκολλο ελέγχου ταυτότητας που χρησιμοποιείται από το πρότυπο ασφαλείας 802.1X.

Μια εναλλακτική λύση πρωτοκόλλου AAA επόμενης γενιάς για το RADIUS είναι το πρωτόκολλο AAA DIAMETER. Το DIAMETER είναι ένα πρότυπο IETF που χρησιμοποιεί ένα νέο πρωτόκολλο μεταφοράς που ονομάζεται πρωτόκολλο μετάδοσης πρωτεύοντος ελέγχου (SCTP) και TCP αντί UDP.[8]

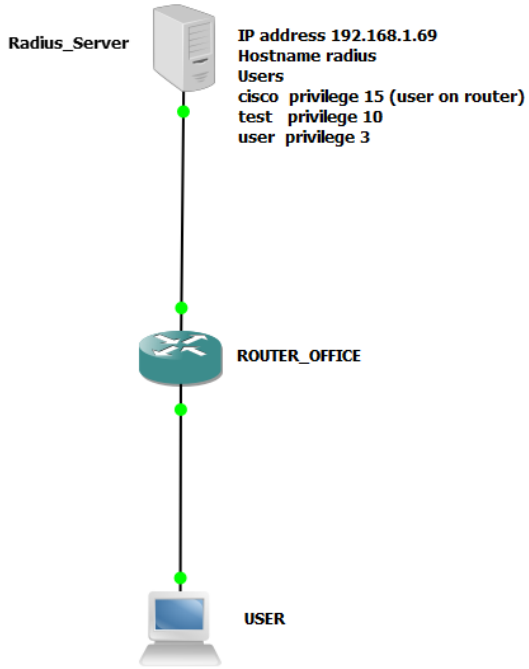


Εικόνα 48: Διαδικασία Επαλήθευσης Ταυτότητας από Radius
(πηγή https://static-course-assets.s3.amazonaws.com/CCNAS2/en/index.html#3.3.2.3)

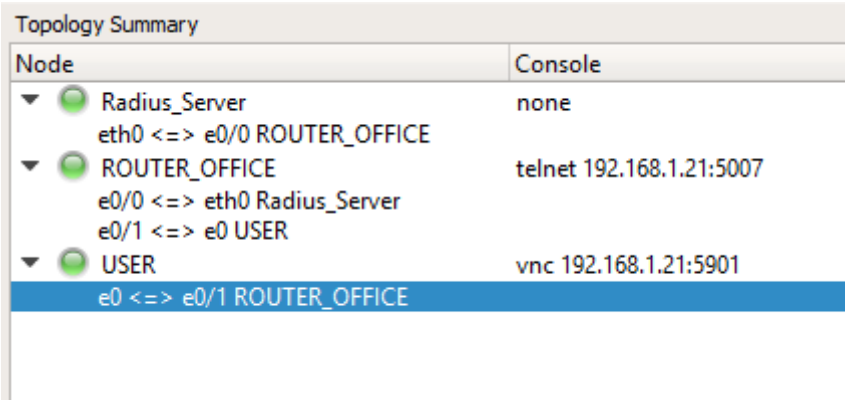
5.4.2 Παράδειγμα Εγκατάστασης και Παραμετροποίησης Radius Server με GNS3

Για το παράδειγμα αυτό θα χρησιμοποιήσουμε το εικονικό μηχάνημα Radius Server που δημιουργήσαμε στο ESXi περιβάλλον μας. Στην συνέχεια θα το εισάγουμε στο GNS3 με την χρήση της συσκευής cloud η οποία μας δίνει την δυνατότητα να συνδεθούμε με συσκευές που βρίσκονται στο δίκτυο μας .

Οι υπόλοιπες συσκευές που θα χρησιμοποιήσουμε είναι ένα δρομολογητή Cisco και ένα μηχάνημα χρήστη που θα κάνει την διαδικασία σύνδεσης στον δρομολογητή με την χρήση του πρωτοκόλλου telnet το οποίο όπως αναφέραμε σε προηγουμένη ενότητα δεν είναι το πιο ασφαλές αλλά λόγο περιορισμού του GNS3 θα προχωρήσουμε με αυτό



Εικόνα 49: Τοπολογια radius σε GNS3



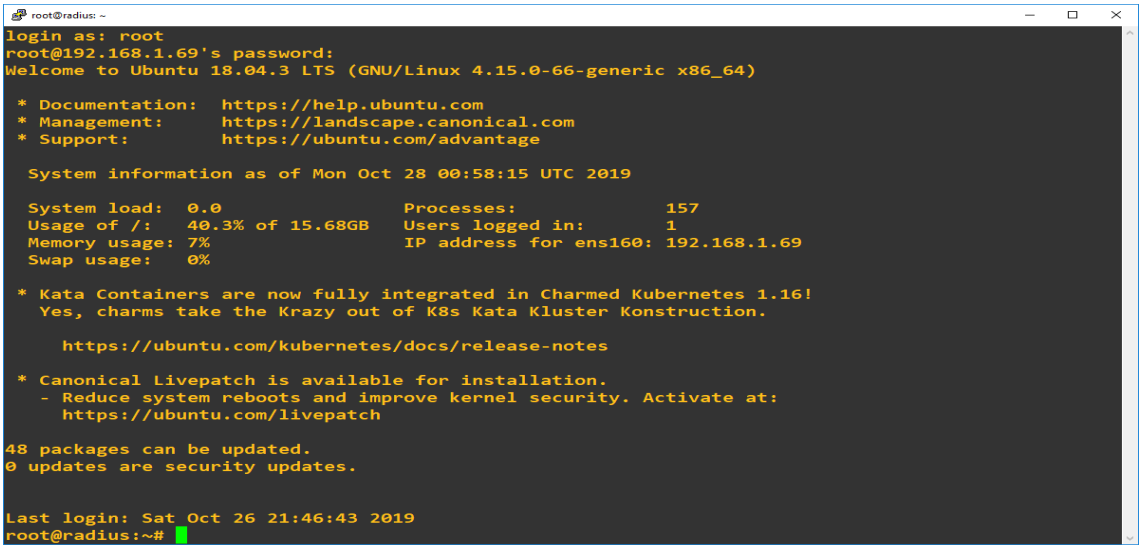
Εικόνα 50:Περιληψη τοπολογιας

Η παραπάνω εικόνες μας δείχνουν την τοπολογία του παραδείγματος μας και πως συνδέονται μεταξύ τους

5.4.2.1 Εγκατάσταση FreeRadius Σε Περιβάλλον Ubuntu 18.0.4

Για το Radius Server μας θα κάνουμε χρήση του δωρεάν λογισμικού Freeradius.Το Freeradius ανήκει στην κατηγορία λογισμικών Open Source ,το οποίο σημαίνει ότι δεν απαιτείται η αγορά άδεια χρήσης του λογισμικού και η χρήση του είναι δωρεάν.

Η εγκατάσταση του θα γίνει με την χρήση command line και όχι σε γραφικό περιβάλλον καθώς η οδηγίες που δίνονται επισημά στην ιστοσελίδα του λογισμικού δείχνουν αυτό τον τρόπο. Θα ξεκινήσουμε την εγκατάσταση μας κάνοντας SSH στον Ubuntu εικονικό μηχάνημα μας που του έχομε δώσει την IP 192.168.1.69 τα διαπιστευτήρια μας είναι όνομα χρήστη root και κωδικός πρόσβασης είναι test123. [13][5][8]



Εικόνα 51: Αρχική οθόνη Radius Server (Ubuntu)

Θα ξεκινήσουμε την διαδικασία εγκατάστασης του λογισμικού μας δίνοντας την εντολή **apt-get update** ώστε να γίνει η αναβάθμιση των πακέτων που προσφέρουν η διακομιστές που συνδέεται το περιβάλλον ώστε να κατεβάσει τα απαραίτητα αρχεία εγκατάστασης που χρειαζόμαστε

Υστέρα θα δώσουμε την εντολή **apt-get install freeradius freeradius-mysql freeradius-utils -y** η οποία θα εγκατάσταση τα πακέτα του freeradius . Μόλις τελειώσει η εγκατάσταση προχωράμε στη εγκατάσταση βάσης δεδομένων MySql και PHP δίνοντας της παρακάτω εντολές

```
apt-get install php-common php-gd php-curl php-mysql -y
apt-get install mysql-server mysql-client -y
```

Επόμενο βήμα είναι να ασφαλίσουμε την βάση δεδομένων μας δίνοντας την εντολή:

```
mysql_secure_installation

VALIDATE PASSWORD PLUGIN can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD plugin?

Press y|Y for Yes, any other key for No:
```

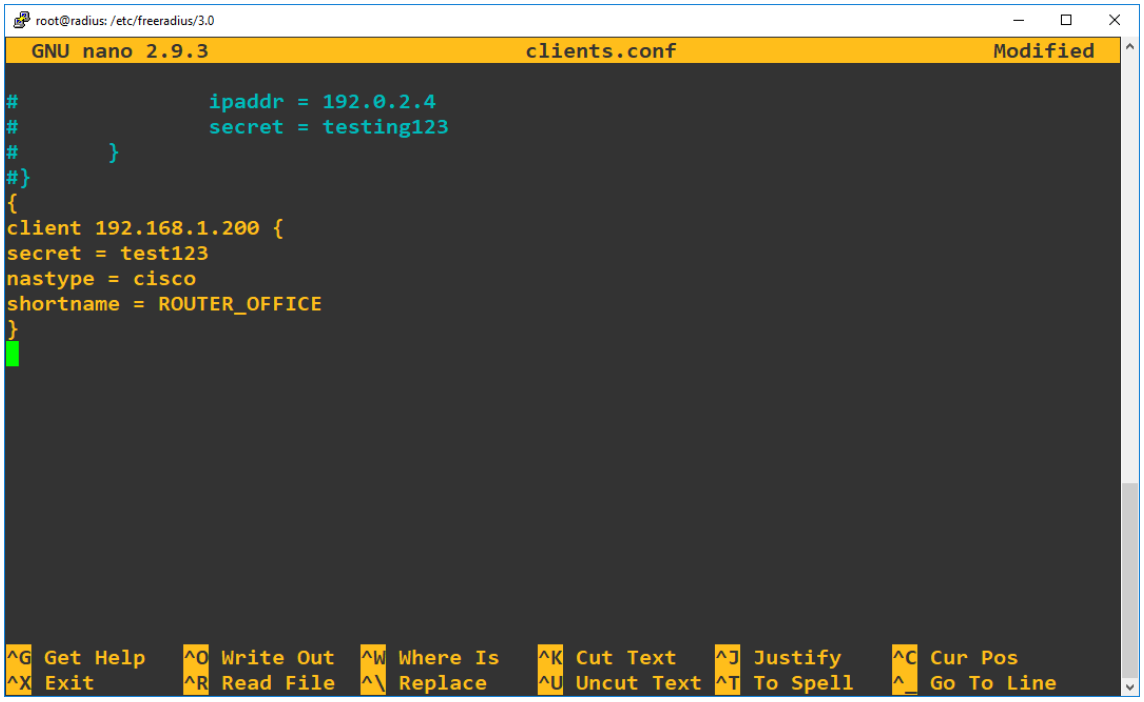
Τέλος θα δημιουργήσουμε μια βάση οπού θα αποθηκεύονται οι χρήστες μας και θα ξεκινήσουμε την υπηρεσία Free radius:

```
mysql -uroot -p test123
CREATE DATABASE radius;
exit

freeradius -X
```

Επιβεβαιώνουμε ότι έχει ξεκινήσει η υπηρεσία όταν εμφανιστεί το παρακάτω:

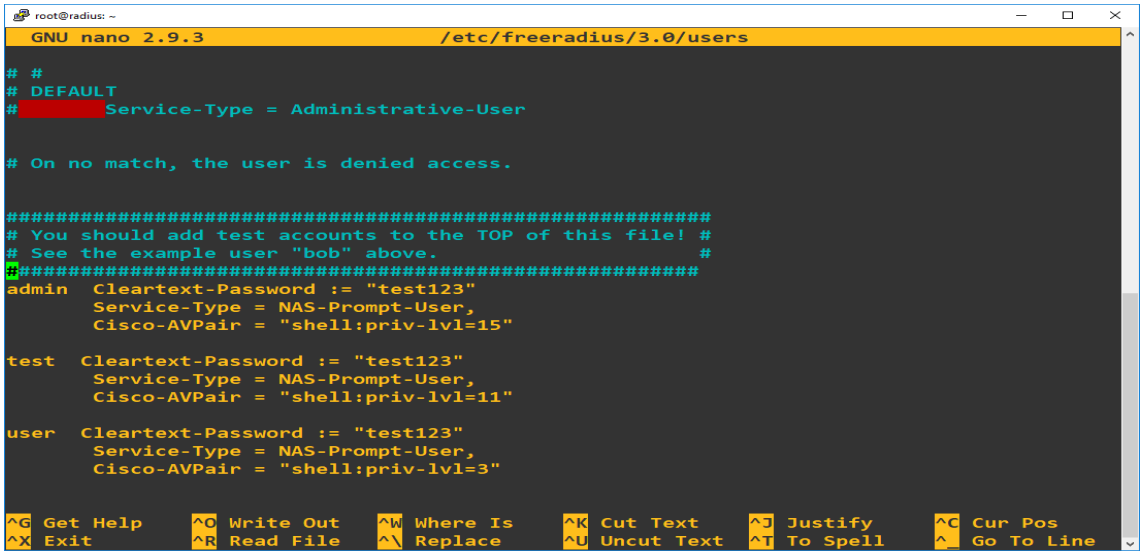
```
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on proxy address * port 59791
Listening on proxy address :: port 36140
Ready to process requests
```

Μόλις έχει ενεργοποιηθεί η υπηρεσία θα πρέπει να παραμετροποιησουμε κάποια αρχεία του freeradius server ώστε να μπορεί να επικοινωνήσει με τον εξοπλισμό Cisco .Το πρώτο αρχείο το οποίο θα παραμετροποιησουμε είναι το αρχείο client.conf στο οποίο θα δηλώσουμε τις συσκευές που θα συνδεθούν στον radius.Στο αρχείο θα δώσουμε την διεύθυνση της συσκευής το κωδικό πρόσβασης ,τον τύπο μηχανήματος και το όνομα της συσκευής.



Εικόνα 52: Περιεχόμενο αρχείου client.conf στον Radius Server

Υστέρα θα πρέπει να παραμετροποιήσουμε το αρχείο users οπού εκεί θα δηλώσουμε ποιοι χρήστες θα έχουν πρόσβαση στις συσκευές Cisco αλλά και τη επίπεδο πρόσβασης θα έχουν



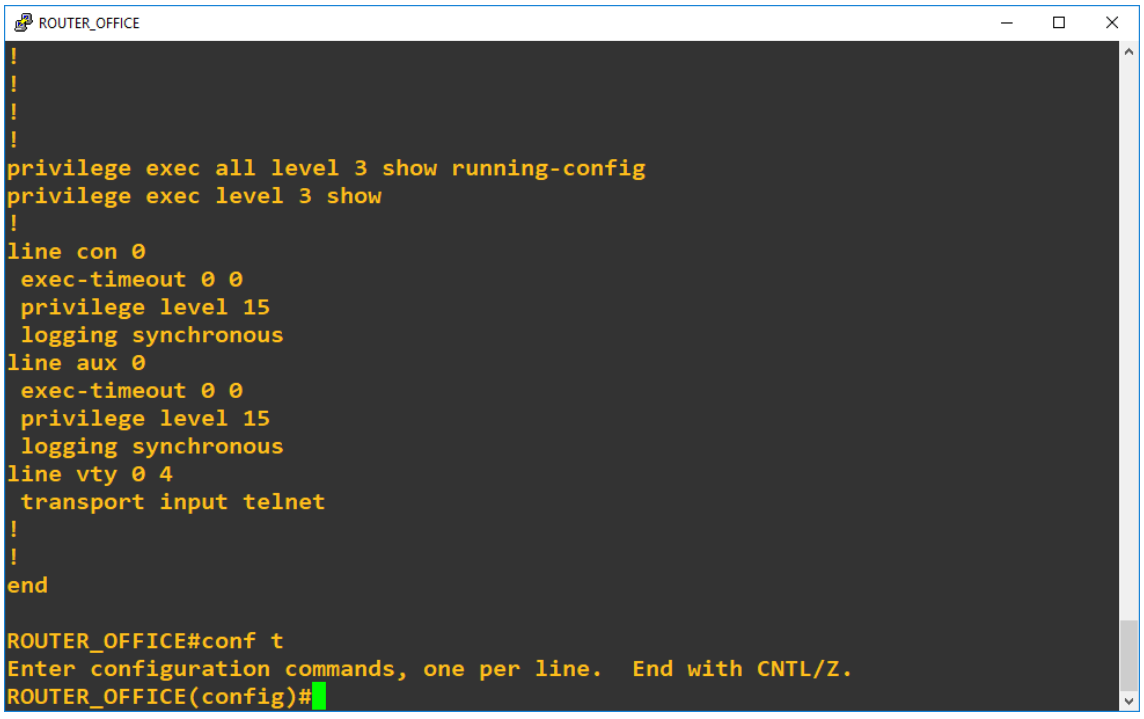
Εικόνα 53: Περιεχόμενο αρχείου users στον Radius Server

Αναλόγως το priv-lvl ο χρηστης θα μπορέσει η να κάνει αλλαγές στις ρυθμίσεις της συσκευής η απλά να μπορεί να δει τις ρυθμίσεις .Στον λειτουργικό περιβάλλον τον Cisco που λέγεται IOS κάθε επίπεδο privilege ορίζεται για συγκεκριμένο τύπο χρήστη. 0-5 Οριζεται για απλούς χρήστες και δίνει την δυνατότητα να μπορούν να πραγματοποιήσουν κάποιες απλές εντολές όπως ping 5-13 μπορούν να δουν κάποια βασικές πληροφορίες όπως την κατάσταση των θυρών.

Τέλος 15-16 ορίζεται για διαχειριστές και δίνει την δυνατότητα αλλαγή ρυθμίσεων και την επιλογή επανεκκίνησης και επαναφορά του εξοπλισμού στις εργοστασιακές ρυθμίσεις.

5.4.2.2 Παραμετροποίηση εξοπλισμού Cisco για Freeradius

Ξεκινάμε πρώτα δίνοντας την εντολή configure terminal βάζοντας την συσκευή σε κατάσταση να μπορεί να δεχτεί εντολές από τον χρήστη. Μόλις μπει η συσκευή μας σε configuration mode



Εικόνα 54:Ενεργοποιηση configuration mode σε συσκευη cisco

Υστέρα θα πρέπει να ενεργοποιήσουμε την υπηρεσία AAA στον δρομολογητή μας δίνοντας την εντολή aaa new-model .Στην συνέχεια θα πρέπει να δηλώσουμε το όνομα του aaa διακομιστή όπως και επίσης να ορίσουμε κωδικό πρόσβασης και δείξουμε στον δρομολογητή μας τις πόρτες επικοινωνίας που θα χρησιμοποιήσει να μιλήσει με τον Radius server μας

```
aaa group server radius RadiusGrp
server-private 192.168.1.200 auth-port 1812 acct-port 1813 key test123
```

Επόμενο βήμα είναι να ενεργοποιήσουμε τον έλεγχο ταυτότητας και την εξουσιοδότηση

```
aaa authentication login default group RadiusGrp
aaa authorization exec default group RadiusGrp
aaa accounting exec default start-stop group RadiusGrp
aaa accounting system default start-stop group RadiusGrp
```

Τέλος θα πρέπει να ενεργοποιήσουμε την απομακρυσμένη πρόσβαση στον δρομολογητή και να του υποδείξουμε ότι την είσοδο θα την κάνει μέσω Radius.

```
line vty 0 4
transport input telnet ssh
login authentication default
```

Επιβεβαιώνουμε ότι έχουμε επικοινωνία με τον Radius Server δίνοντας την εντολή show aaa servers

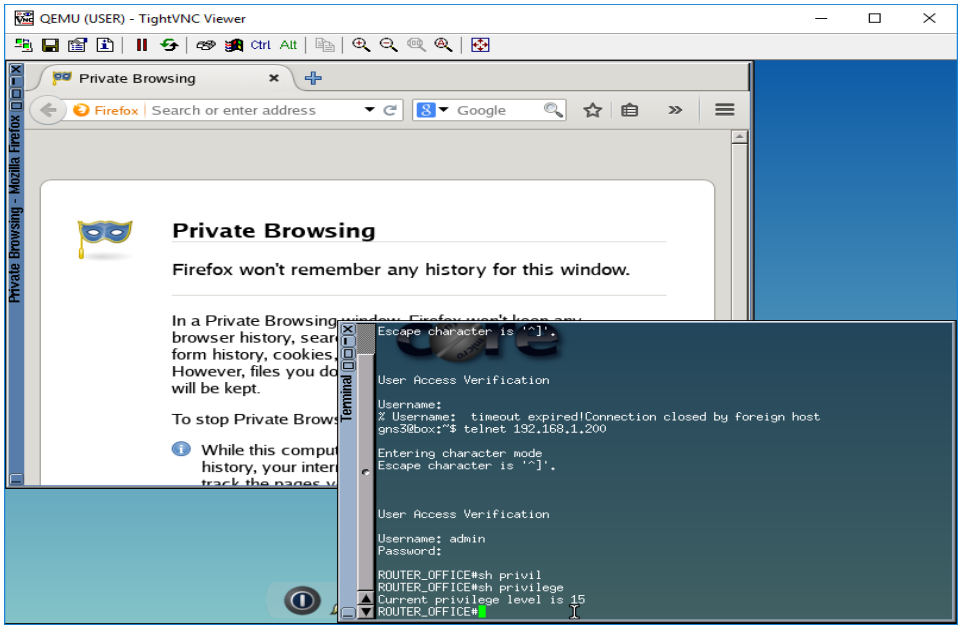
```
ROUTER_OFFICE
ROUTER_OFFICE#show aaa servers

RADIUS: id 1, priority 1, host 192.168.1.69, auth-port 1812, acct-port 1813
     State: current UP, duration 8854s, previous duration 0s
     Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 8, timeouts 8, failover 0, retransmission 6
             Response: accept 0, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 2
             Throttled: transaction 0, timeout 0, failure 0
     Author: request 0, timeouts 0, failover 0, retransmission 0
             Response: accept 0, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Account: request 0, timeouts 0, failover 0, retransmission 0
             Request: start 0, interim 0, stop 0
             Response: start 0, interim 0, stop 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Elapsed time since counters last cleared: 2h27m
     Estimated Outstanding Access Transactions: 0
     Estimated Outstanding Accounting Transactions: 0
     Estimated Throttled Access Transactions: 0
     Estimated Throttled Accounting Transactions: 0
     Maximum Throttled Transactions: access 0, accounting 0
     Requests per minute past 24 hours:
             high - 0 hours, 21 minutes ago: 7
             low  - 2 hours, 27 minutes ago: 0
             average: 0
ROUTER_OFFICE#
```

Εικόνα 55: Αποτέλεσμα εντολής show aaa servers

5.4.2.3 Διαδικασία σύνδεσης χρήστη Radius σε εξοπλισμό Cisco

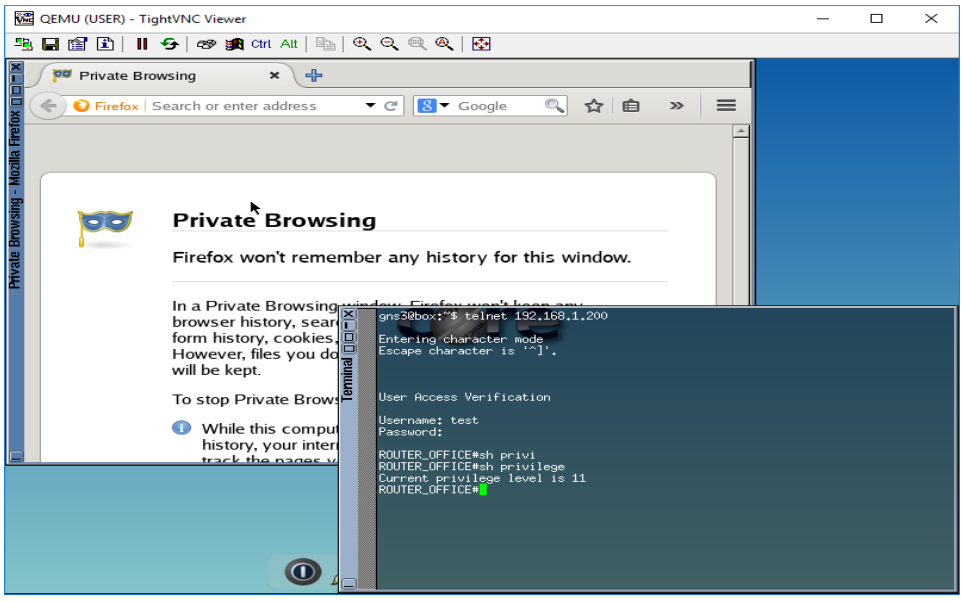
Έχοντας ορίσει τους χρήστες μας στον Radius Server και ενεργοποιήσει την υπηρεσία AAA στον δρομολογητή μας ,το επόμενο βήμα είναι από το υπολογιστή χρήστη που έχουμε δημιουργήσει στο GNS3 να κάνουμε προσπάθεια να συνδεθούμε στον δρομολογητή μας με κάθε χρήστη και να δούμε αν έχει το κατάλληλο επίπεδο πρόσβασης

Η πρώτη προσπάθεια θα γίνει με τον χρήστη admin που έχει privilege level 15



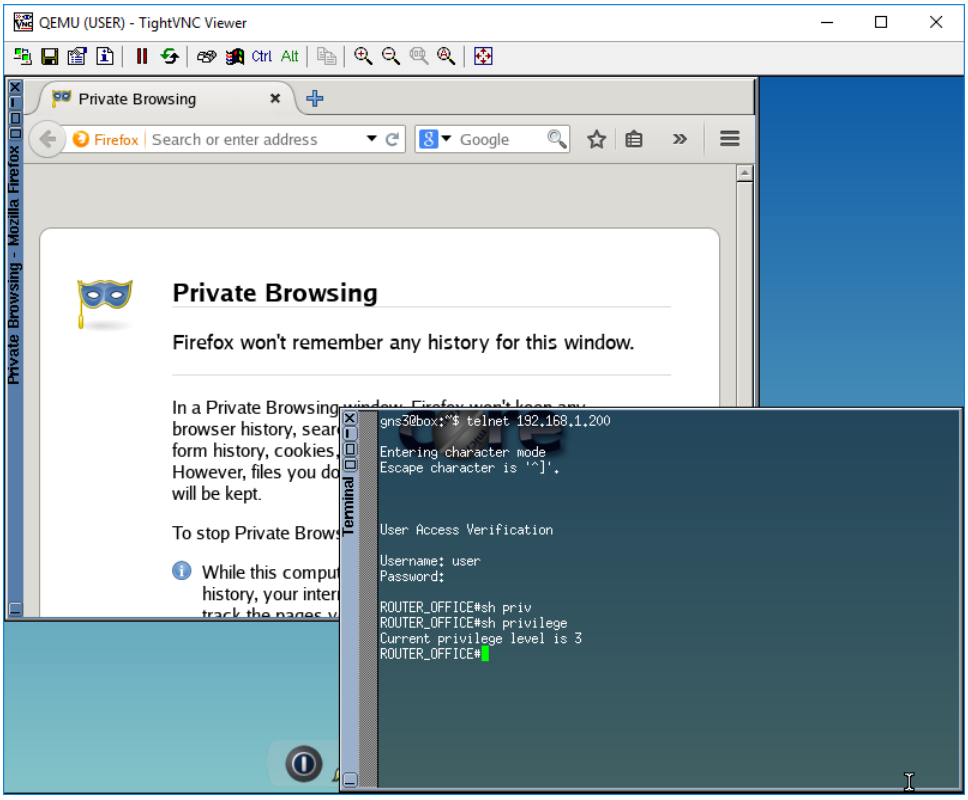
Εικόνα 56: Client PC απομακρυμενη προσβαση σε router με την χρηση telnet και privilege 15 (Full privilege)

Η δεύτερη προσπάθεια θα γίνει με τον χρήστη test που έχει privilege level 11



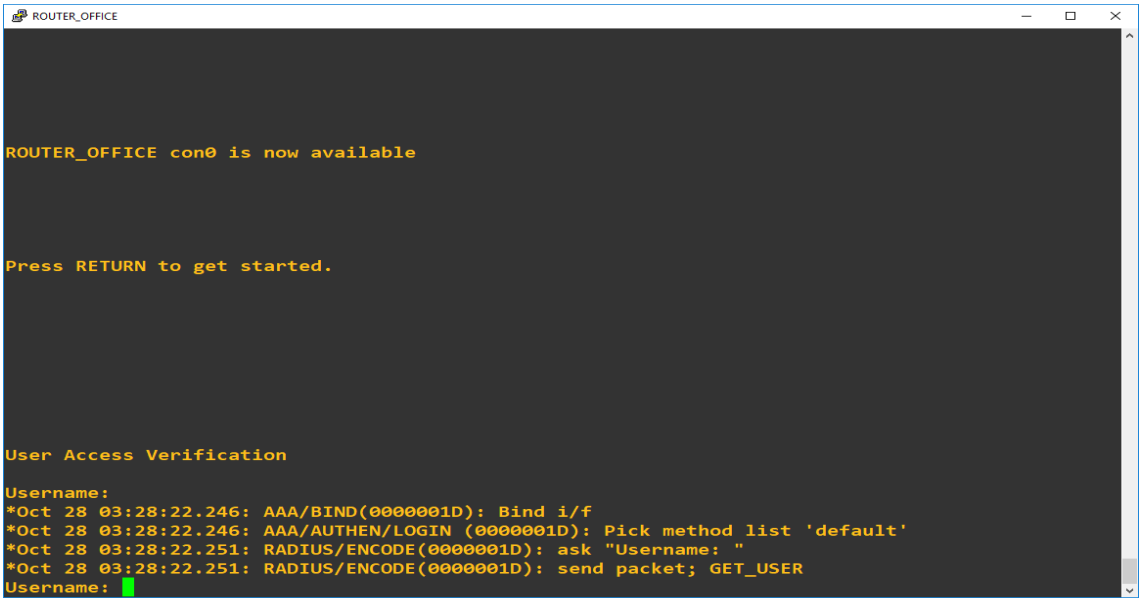
Εικόνα 57: Client PC απομακρυσμένη πρόσβαση σε router με την χρήση telnet και privilege 11

Η τελευταία προσπάθεια θα γίνει με τον χρήστη user που έχει privilege level 3



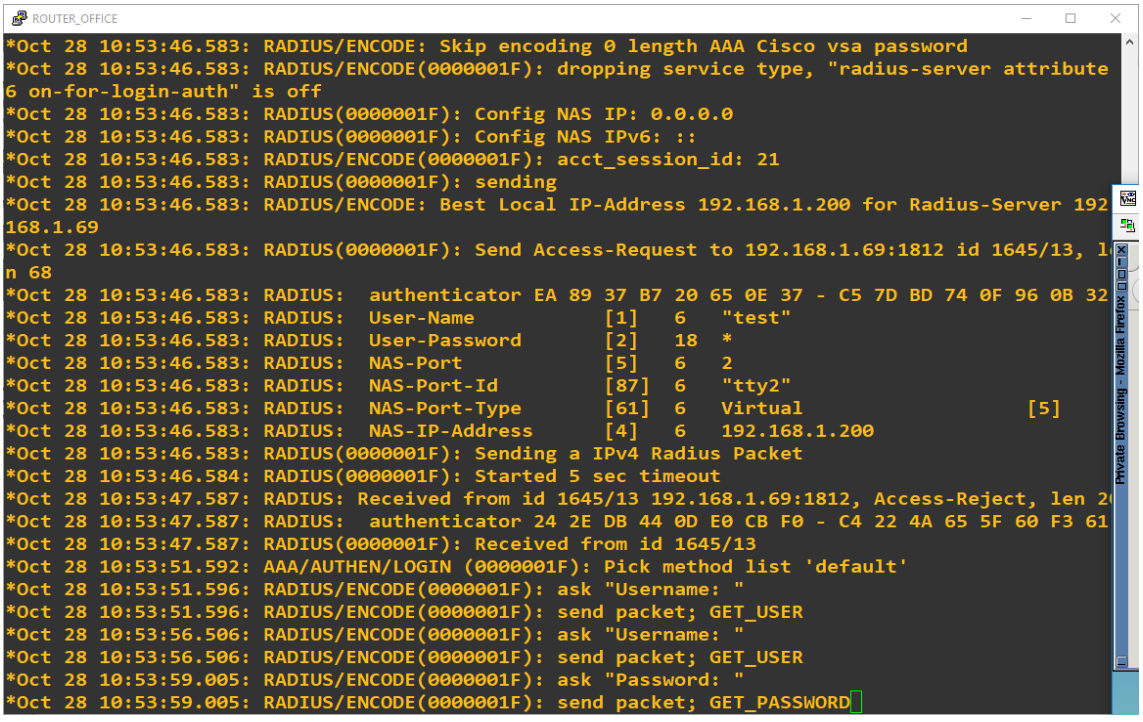
Εικόνα 58: Client PC απομακρυσμένη πρόσβαση σε router με την χρήση telnet και privilege 3 (Lowest privilege)

Για να δούμε πως ακριβώς δουλεύει η διαδικασία AAA θα ενεργοποιήσουμε το debug radius οπού θα δούμε πως ακριβώς δουλεύει το πρωτόκολλο



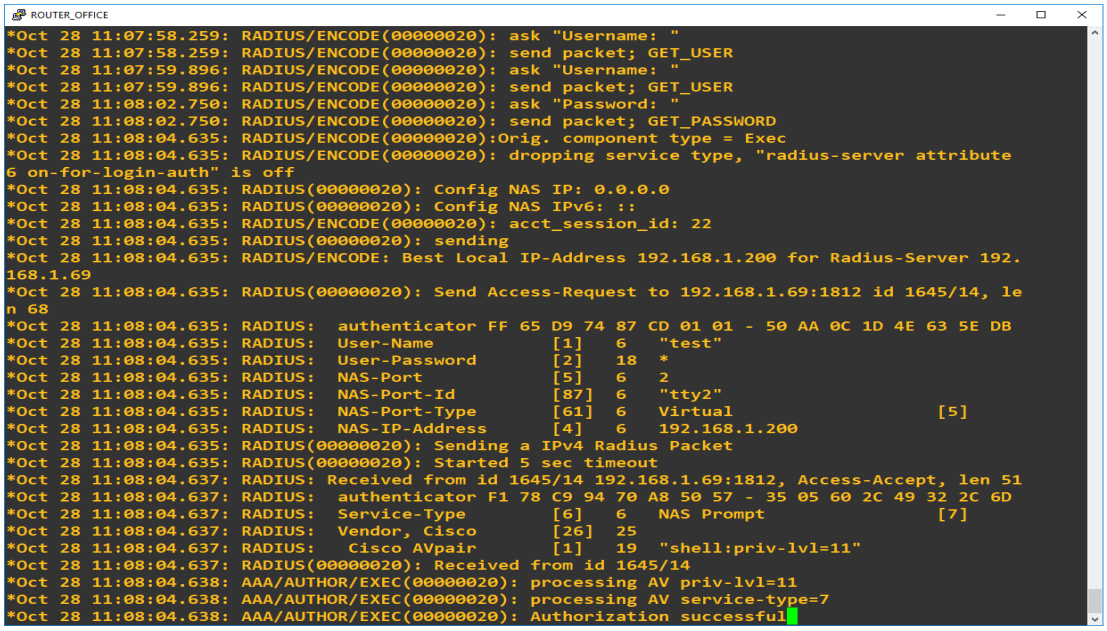
Εικόνα 59:Terminal Monitor AAA Get User

Παρατηρούμε ότι ο δρομολογητής ζητάει από το χρήστη το username του ώστε να στείλει πίσω στο radius το πακέτο GET_USER μόλις δώσει χρήστης το username του ο δρομολογητής μας θα ζητήσει τον κωδικό πρόσβασης



Εικόνα 60: Terminal Monitor AAA Get Password

Μόλις λάβει και τον κωδικό και επιβεβαίωση ότι είναι σωστός θα ελέγξει το επίπεδο πρόσβασης του χρήστη και στην συνέχεια θα του επιτρέψει την είσοδο όπως φαίνεται στο παρακάτω σχήμα:



Εικόνα 61: Terminal Monitor AAA Successful Login

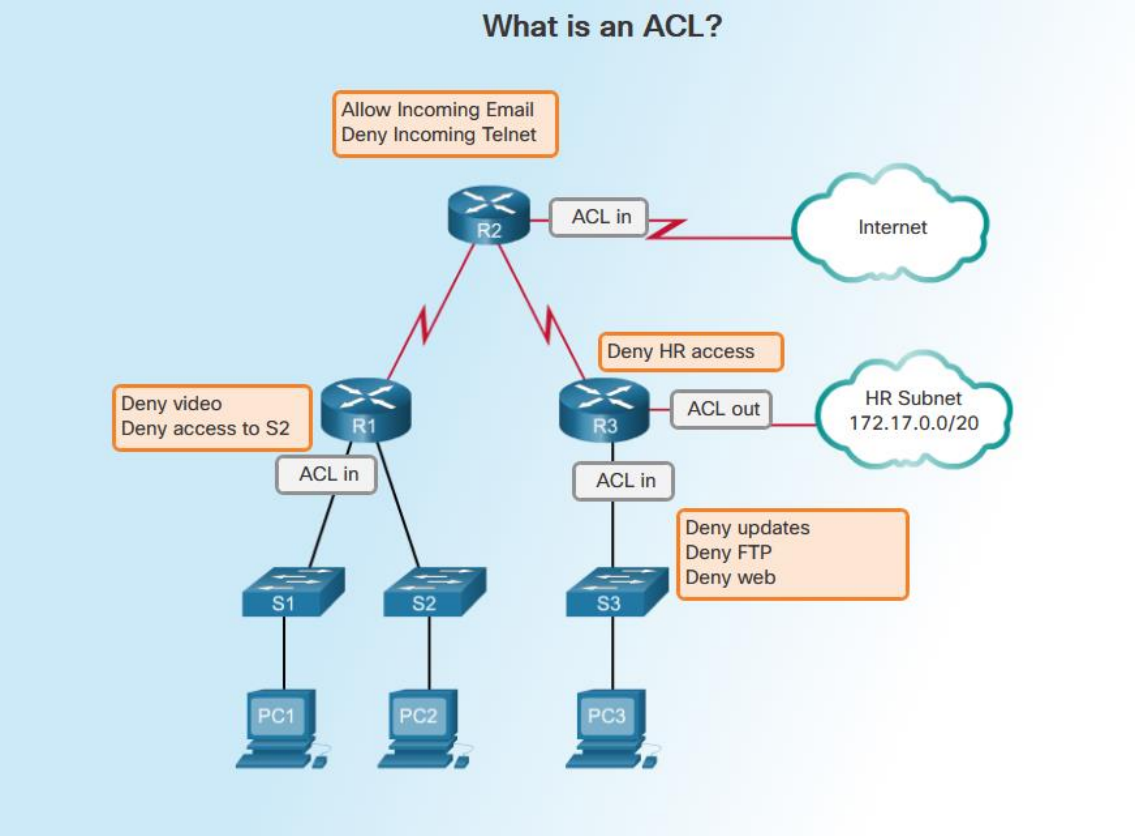
5.5 Τείχος Προστασίας (Firewall)

Καθώς τα δίκτυα συνέχιζαν να αναπτύσσονται με την πάροδο του χρόνου, χρησιμοποιούνταν όλο και περισσότερο για τη μεταφορά και αποθήκευση ευαίσθητων δεδομένων. Αυτό εντείνει την ανάγκη για ισχυρότερες τεχνολογίες ασφάλειας, οι οποίες οδήγησαν στην εφεύρεση του τείχους προστασίας. Ο όρος τείχος προστασίας αναφέρεται αρχικά σε έναν πυρίμαχο τοίχο, συνήθως κατασκευασμένο από πέτρα ή μέταλλο, που εμπόδισε τη διάδοση φλόγας μεταξύ των συνδεδεμένων δομών. Στον κόσμο της δικτύωσης, τα firewalls χωρίζουν τις προστατευόμενες περιοχές από τις μη προστατευόμενες περιοχές. Αυτό εμποδίζει τους μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση σε προστατευμένους πόρους δικτύου.

Ένα μεγάλο κομμάτι στην λειτουργία του τείχους προστασίας είναι η Λίστα ελέγχου πρόσβασης ACL – Access control List.

5.5.1 Λίστα ελέγχου πρόσβασης (Access Control List)

Οι ACL χρησιμοποιούνται ευρέως στη δικτύωση υπολογιστών και στην ασφάλεια δικτύων για τον περιορισμό των επιθέσεων δικτύου και τον έλεγχο της κυκλοφορίας δικτύου. Οι διαχειριστές μπορούν να χρησιμοποιήσουν ACL για να καθορίσουν και να ελέγξουν τις κατηγορίες κυκλοφορίας σε συσκευές δικτύωσης για να ικανοποιήσουν ένα συγκεκριμένο σύνολο απαιτήσεων ασφάλειας.[12]



Εικόνα 62:Παραδειγμα λειτουργιας Access List

Η λίστα ελέγχου πρόσβασης (ACL) είναι μια διαδοχική λίστα δηλώσεων αδειών ή αρνήσεων, γνωστών ως καταχωρήσεων ελέγχου πρόσβασης (ACE). Οι ACEs συνήθως ονομάζονται επίσης και ACL. Τα ACE μπορούν να δημιουργηθούν για να φιλτράρουν την επισκεψιμότητα βάσει ορισμένων κριτηρίων όπως: η διεύθυνση προέλευσης, η διεύθυνση προορισμού, το πρωτόκολλο και οι αριθμοί θυρών.

Τα τυπικά πακέτα ACL αντιστοιχούν στα πακέτα εξετάζοντας το πεδίο διεύθυνσης IP προέλευσης στην κεφαλίδα IP αυτού του πακέτου. Αυτά τα ACL χρησιμοποιούνται για να φιλτράρουν τα πακέτα με βάση μόνο τις πληροφορίες προέλευσης του Layer 3.

5.5.2 Οφέλη και Περιορισμοί του Τείχους Προστασίας

Υπάρχουν πολλά οφέλη από τη χρήση ενός τείχους προστασίας σε ένα δίκτυο:

- Αποτροπή της έκθεσης ευαίσθητων κεντρικών υπολογιστών, πόρων και εφαρμογών σε μη αξιόπιστους χρήστες.
- Αποκλεισμός κακόβουλων δεδομένων από διακομιστές και πελάτες.
- Μείωση της πολυπλοκότητας της διαχείρισης της ασφάλειας με την εκφόρτωση του μεγαλύτερου μέρους του ελέγχου πρόσβασης δικτύου σε μερικά τείχη προστασίας στο δίκτυο.

Τα τείχη προστασίας παρουσιάζουν επίσης ορισμένους περιορισμούς:

- Τα δεδομένα από πολλές εφαρμογές δεν μπορούν να μεταφερθούν με ασφάλεια στα τείχη προστασίας.
- Οι χρήστες ενδέχεται να αναζητήσουν δυναμικά τρόπους γύρω από το τείχος προστασίας για να λάβουν υλικό που έχει μπλοκαριστεί, γεγονός που εκθέτει το δίκτυο σε πιθανή επίθεση.
- Η απόδοση του δικτύου μπορεί να επιβραδυνθεί.
- Η μη εξουσιοδοτημένη κυκλοφορία μπορεί να γίνει tunneling ή να κρυφτεί ως νόμιμη κίνηση μέσω του τείχους προστασίας.[6]

5.5.3 Περιγραφή τύπων τείχους προστασίας

Ένα σύστημα τείχους προστασίας μπορεί να αποτελείται από πολλές διαφορετικές συσκευές και εξαρτήματα. Ένα στοιχείο είναι το φιλτράρισμα της κίνησης, το οποίο οι περισσότεροι άνθρωποι καλούν συνήθως ένα τείχος προστασίας. Τα παρακάτω τρία firewalls καλύπτονται σε αυτό το κεφάλαιο:

1. **Τείχος προστασίας φιλτραρίσματος πακέτων** - Συνήθως ένας δρομολογητής με δυνατότητα φιλτραρίσματος κάποιου περιεχομένου πακέτου, όπως το Layer 3 και ενίοτε το Layer 4

2. **Stateful firewall** - Παρακολουθεί την κατάσταση των συνδέσεων, ανεξάρτητα από το εάν η σύνδεση είναι σε κατάσταση έναρξης, μεταφοράς δεδομένων ή τερματισμού).

3. **Τείχος προστασίας πύλης εφαρμογών (τείχος προστασίας proxy)** - Φιλτράρει πληροφορίες στα επίπεδα 3, 4, 5 και 7 του μοντέλου αναφοράς OSI. Το μεγαλύτερο μέρος του ελέγχου και του φιλτραρίσματος του τείχους προστασίας γίνεται στο λογισμικό /Όταν ένας πελάτης χρειάζεται να αποκτήσει πρόσβαση σε έναν απομακρυσμένο διακομιστή, συνδέεται με ένα διακομιστή μεσολάβησης. Ο διακομιστής μεσολάβησης συνδέεται στον απομακρυσμένο διακομιστή για λογαριασμό του πελάτη. Επομένως, ο διακομιστής βλέπει μόνο μια σύνδεση από το διακομιστή μεσολάβησης.

Άλλες μέθοδοι εφαρμογής τείχους προστασίας περιλαμβάνουν:

Τείχος προστασίας που βασίζεται σε κεντρικό υπολογιστή (διακομιστή και προσωπική) - Ένας υπολογιστής ή διακομιστής με λογισμικό τείχους προστασίας που εκτελείται σε αυτό.

Hybrid firewall - Συνδυασμός των διαφόρων τύπων τείχους προστασίας. Για παράδειγμα, ένα τείχος προστασίας επιθεώρησης εφαρμογών συνδυάζει ένα κρατικό τείχος προστασίας με ένα τείχος προστασίας πύλης εφαρμογής

Κεφάλαιο 6: Συμπεράσματα

Στην παρούσα μεταπτυχιακή διατριβή παρουσιάστηκε η εγκατάσταση και η παραμετροποίηση της δικτυακής υποδομής σε πλωτό, μη ιδιωτικό σκάφος αναψυχής. Η εγκατάσταση παρουσιάστηκε με την χρήση λογισμικών εξομοίωσης GNS3 και VMWare. Με την χρήση των λογισμικών αυτών μπορέσαμε να αναπαραστήσουμε ακριβώς τις λειτουργίες του δικτυακού εξοπλισμού που βρίσκεται αυτή την στιγμή στο σκάφος. Αναλύσαμε της διαδικασίες επιλογής εξοπλισμού και τις μεθόδους ελέγχου και ερευνάς πριν την τελική εγκατάσταση. Έχοντας πραγματοποιήσει τις διαδικασίες Site και Wireless Site Survey, μπορέσαμε να καταλήξουμε στην τοπολογία που θα χρησιμοποιήσουμε στην εγκατάσταση, ακολουθώντας τα ιεραρχικά μοντέλα σχεδίασης δικτυών τα οποία μπορούν να εφαρμοστούν σε οποιαδήποτε επαγγελματική δικτυακή εγκατάσταση. Έχοντας καταλήξει στην τοπολογία περάσαμε στον τρόπο διαχείρισης του ασυρμάτου δικτύου με την χρήση Intracontroller roaming, διασφαλίζοντας έτσι τη συνεχόμενη και αδιάκοπη σύνδεση των χρηστών σε όλο το σκάφος.

Στην συνέχεια, περάσαμε στην ανάλυση και εφαρμογή μεθόδων ασφάλειας του δικτύου και αναλύσαμε γενικούς κανόνες ασφάλειας δικτυακών υποδομών που πρέπει να ακολουθήσουν οι χρήστες αλλά και οι εγκαταστάτες αυτών. Δείξαμε ποιες είναι οι αδυναμίες που μπορούν να εμφανιστούν σε οποιαδήποτε εγκατάσταση και ποια είναι τα βήματα να διορθωθούν. Επίσης, δείξαμε μηχανισμούς αναγνώρισης και πιστοποίησης χρηστών με την χρήση Radius server, δίνοντας με αυτόν τον τρόπο τα καταλληλά δικαιώματα πρόσβασης σε χρήστες αλλά και τεχνικούς που αργότερα μπορεί να χρειαστεί να προβούν σε αλλαγές αλλά και επιδιορθώσεις στον εξοπλισμό. Τέλος αναφέρουμε την χρήση συσκευών ασφάλειας firewall με τις οποίες μπορούμε, όχι μόνο να διασφαλίσουμε την ασφάλεια του δικτύου μας και των πληροφοριών που περνάνε πάνω σε αυτό το δίκτυο, αλλά και να αποκτήσουμε μια απομακρυσμένη πρόσβαση στον εξοπλισμό από οποιοδήποτε μέρος του κόσμου με την χρήση VPN. Με την χρήση VPN, δίνεται σε τεχνικούς αλλα και διαχειριστές του σκαφους και της εταιρείας η δυνατότητα εκμετάλλευσης του να μπαίνουν σε συστήματα που βρίσκονται πάνω στο σκάφος και να πραγματοποιούν αλλαγές και επιδιορθώσεις συστημάτων σε οποίο μέρους του κόσμου να βρίσκεται αυτό, χωρίς την φυσική τους παρουσία εκεί. Με την εφαρμογή κρυπτογράφησης οι πληροφορίες που ανταλλάσσονται μεταξύ των τεχνικών που βρίσκονται εκτός σκάφους με τα τοπικά συστήματα δεν διατρεχουν κανένα κίνδυνο υποκλοπής η παραποίησης.

Κεφάλαιο 7 Βιβλιογραφια

- [1] www.cisco.com
- [2] www.ciscopress.com
- [3] www.ietf.org
- [4] www.ieee.org
- [5] www.gns3.com
- [6] CCNA Security 210-260 Official Cert Guide: CCNA Sec 210-260 OCG John Stuppi CCIE NO 11154
- [7] CCDA 200-310 Official Cert Guide ANTHONY BRUNO, CCIE No. 2738
- [8] www.netacad.com
- [9] www.wikipedia.com
- [10] Ccda: Cisco Certified Design Associate Exam Notes Exam 640-441
- [11] SSL VPN : Understanding, evaluating and planning secure, web-based remote access: A comprehensive overview of SSL VPN technologies and design strategies
- [12] VPNs: A Beginner's Guide John Mairs
- [13] VMware vSphere 6.7 Cookbook: Practical recipes to deploy, configure, and manage VMware vSphere 6.7 components, 4th Edition by Abhilash G B
- [14] Mastering Ubuntu Server: Master the art of deploying, configuring, managing, and troubleshooting Ubuntu Server 18.04, 2nd Edition Jay LaCroix
- [15] https://rainestech.com/services/home-office-network

Κεφάλαιο 8 Παράρτημα

(Παράθεση των configuration files)

8.1Τοπολογια εγκαταστασης

8.1.1 Configuration WAN Router

WAN-RT#sh run

Building configuration...

Current configuration : 2920 bytes

!

version 15.5

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname WAN-RT

!

boot-start-marker

boot-end-marker

!

!

!

no aaa new-model

!

!

!

bsd-client server url https://cloudsso.cisco.com/as/token.oauth2

mmi polling-interval 60

```
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
!
!
!
!
!
!
!
!
!
!
ip domain name unipi.my
ip name-server 208.67.220.220
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
```

```
!
!
!
!
!
cts logging verbose
!
!
username unipi privilege 15 secret 5 $1$9CYR$kkUW187IMzAlY4WYXOkHP.
!
redundancy
!
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 description ### Con to ASA ###
 ip address 192.168.254.254 255.255.255.252
 ip nat inside
```

```
 ip virtual-reassembly in
!
interface Ethernet0/1
 no ip address
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 description ### Con to SAT ISP ###
 ip address dhcp
       ip nat outside
       ip virtual-reassembly in
      !
      interface Ethernet1/0
       no ip address
       shutdown
      !
      interface Ethernet1/1
       no ip address
       shutdown
      !
      interface Ethernet1/2
       no ip address
       shutdown
      !
      interface Ethernet1/3
       no ip address
       shutdown
      !
```

```
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
```

```
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list NAT interface Ethernet0/3 overload
ip nat inside source static tcp 192.168.254.253 443 interface Ethernet0/3 9443
ip route 192.168.100.0 255.255.255.0 192.168.254.253
ip route 192.168.101.0 255.255.255.0 192.168.254.253
ip route 192.168.102.0 255.255.255.0 192.168.254.253
ip route 192.168.103.0 255.255.255.0 192.168.254.253
ip route 192.168.104.0 255.255.255.0 192.168.254.253
ip route 192.168.105.0 255.255.255.0 192.168.254.253
ip route 0.0.0.0 0.0.0.0 Ethernet0/3 dhcp
!
ip access-list extended NAT
 permit ip 192.168.254.0 0.0.0.255 any
 permit ip 192.168.100.0 0.0.0.255 any
 permit ip 192.168.101.0 0.0.0.255 any
 permit ip 192.168.102.0 0.0.0.255 any
 permit ip 192.168.103.0 0.0.0.255 any
 permit ip 192.168.104.0 0.0.0.255 any
```

```
 permit ip 192.168.105.0 0.0.0.255 any
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login local
 transport input ssh
!
!
End
```

8.1.2 Configuration Core Switch

MY SW 01

```
MY-SW-01#sh run
Building configuration...


Current configuration : 3048 bytes
!
! Last configuration change at 15:51:08 GR Mon Oct 28 2019
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname MY-SW-01
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username unipi privilege 15 secret 5 $1$8EQV$pqw0Sowu9Tf0bLVAT6yYf.
no aaa new-model
clock timezone GR 3 0
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip domain-name unipi.my
ip name-server 208.67.220.220
```

```
ip cef
no ipv6 cef
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 description ### APs ###
 switchport access vlan 100
 switchport mode access
!
interface Ethernet0/1
 description ### APs ###
 switchport access vlan 100
 switchport mode access
!
interface Ethernet0/2
 description ### APs ###
 switchport access vlan 100
 switchport mode access
```

```
!
interface Ethernet0/3
 description ### APs ###
 switchport access vlan 100
 switchport mode access
!
interface Ethernet1/0
 description ### TRUNK DECK L0 ###
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/1
 description ### TRUNK DECK L0 ###
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/2
 description ### TRUNK DECK L1 ###
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet1/3
 description ### TRUNK DECK L1 ###
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet2/0
 description ### TRUNK DECK L2 ###
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet2/1
 description ### TRUNK DECK L2 ###
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet2/2
 description ### SUN DECK L3 ###
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet2/3
 description ### SUN DECK L3 ###
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet3/0
!
interface Ethernet3/1
 description ### Con to AAA ###
 switchport access vlan 100
 switchport mode access
!
interface Ethernet3/2
 description ### Con to WLC ###
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet3/3
 description ### Con to ASA ###
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100
 description ### MGMT ###
 ip address 192.168.100.240 255.255.255.0
!
ip default-gateway 192.168.100.254
ip forward-protocol nd
!
!
no ip http server
```

```
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.100.254
!
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login local
 transport input all
!
ntp server time.google.com
!
End
```

8.1.3 Configuration ASA Firewall

```
MY ASA
ASA Version 9.8(1)
!
hostname MY-ASA
domain-name unipi.my
enable password
$sha512$5000$5ZIrYRbjkAICzM/YMC6DKw==$8nInWBeFODqAarSHRubK1g==
pbkdf2
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
```

```
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
ip local pool VPN-Pool 192.168.200.11-192.168.200.20 mask 255.255.255.0

!
interface GigabitEthernet0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/1.100
 vlan 100
 nameif MGMT
 security-level 100
 ip address 192.168.100.254 255.255.255.0
!
interface GigabitEthernet0/1.101
 vlan 101
 nameif AV
 security-level 25
 ip address 192.168.101.254 255.255.255.0
!
interface GigabitEthernet0/1.102
 vlan 102
 nameif BRIDGE
 security-level 50
 ip address 192.168.102.254 255.255.255.0
!
interface GigabitEthernet0/1.103
 vlan 103
```

```
 nameif CREW
 security-level 50
 ip address 192.168.103.254 255.255.255.0
!
interface GigabitEthernet0/1.104
 vlan 104
 nameif GUEST
 security-level 50
 ip address 192.168.104.254 255.255.255.0
!
interface GigabitEthernet0/1.105
 vlan 105
 nameif VIP
 security-level 50
 ip address 192.168.105.254 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
```

```
interface GigabitEthernet0/6
 description ### Con to WAN ###
 nameif WAN
 security-level 0
 ip address 192.168.254.253 255.255.255.252
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
clock timezone EEST 2
clock summer-time EEDT recurring last Sun Mar 3:00 last Sun Oct 4:00
dns server-group DefaultDNS
 domain-name unipi.my
access-list MGMT standard permit 192.168.100.0 255.255.255.0
pager lines 23
logging enable
logging asdm informational
mtu MGMT 1500
mtu AV 1500
mtu BRIDGE 1500
mtu CREW 1500
mtu GUEST 1500
mtu VIP 1500
mtu WAN 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
route WAN 0.0.0.0 0.0.0.0 192.168.254.254 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
```

```
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
user-identity default-domain LOCAL
aaa authentication enable console LOCAL
aaa authentication http console LOCAL
aaa authentication serial console LOCAL
aaa authentication ssh console LOCAL
aaa authentication login-history
http server enable
http 192.168.0.0 255.255.255.0 MGMT
http 192.168.1.0 255.255.255.0 WAN
no snmp-server location
no snmp-server contact
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-
proposal AES256 AES192 AES 3DES DES
crypto map WAN_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
crypto map WAN_map interface WAN
crypto ca trustpoint _SmartCallHome_ServerCA
 no validation-usage
```

```
 crl configure
crypto ca trustpoint ASDM_TrustPoint0
 enrollment self
 subject-name CN=MY-ASA
 crl configure
crypto ca trustpool policy
 auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
 certificate ca 18dad19e267de8bb4a2158cdcc6b3b4a
    308204d3 308203bb a0030201 02021018 dad19e26 7de8bb4a 2158cdcc
6b3b4a30
    0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302
55533117
    30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06
0355040b
    13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038
06035504
    0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d
20466f72
    20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504
03133c56
    65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61
72792043
    65727469 66696361 74696f6e 20417574 686f7269 7479202d 20473530
1e170d30
    36313130 38303030 3030305a 170d3336 30373136 32333539 35395a30
81ca310b
    30090603 55040613 02555331 17301506 0355040a 130e5665 72695369
676e2c20
    496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573
74204e65
    74776f72 6b313a30 38060355 040b1331 28632920 32303036 20566572
69536967
    6e2c2049 6e632e20 2d20466f 72206175 74686f72 697a6564 20757365
206f6e6c
    79314530 43060355 0403133c 56657269 5369676e 20436c61 73732033
20507562
    6c696320 5072696d 61727920 43657274 69666963 6174696f 6e204175
74686f72
    69747920 2d204735 30820122 300d0609 2a864886 f70d0101 01050003
82010f00
    3082010a 02820101 00af2408 08297a35 9e600caa e74b3b4e dc7cbc3c
451cbb2b
```

e0fe2902 f95708a3 64851527 f5f1adc8 31895d22 e82aaaa6 42b38ff8 b955b7b1
b74bb3fe 8f7e0757 ecef43db 66621561 cf600da4 d8def8e0 c362083d 5413eb49
ca595485 26e52b8f 1b9febf5 a191c233 49d84363 6a524bd2 8fe87051 4dd18969
7bc770f6 b3dc1274 db7b5d4b 56d396bf 1577a1b0 f4a225f2 af1c9267 18e5f406
04ef90b9 e400e4dd 3ab519ff 02baf43c eee08beb 378becf4 d7acf2f6 f03dafdd
75913319 1d1c40cb 74241921 93d914fe ac2a52c7 8fd50449 e48d6347 883c6983
cbfe47bd 2b7e4fc5 95ae0e9d d4d143c0 6773e314 087ee53f 9f73b833 0acf5d3f
3487968a ee53e825 15020301 0001a381 b23081af 300f0603 551d1301 01ff0405
30030101 ff300e06 03551d0f 0101ff04 04030201 06306d06 082b0601 05050701
0c046130 5fa15da0 5b305930 57305516 09696d61 67652f67 69663021 301f3007
06052b0e 03021a04 148fe5d3 1a86ac8d 8e6bc3cf 806ad448 182c7b19 2e302516
23687474 703a2f2f 6c6f676f 2e766572 69736967 6e2e636f 6d2f7673 6c6f676f
2e676966 301d0603 551d0e04 1604147f d365a7c2 ddecbbf0 3009f343 39fa02af
33313330 0d06092a 864886f7 0d010105 05000382 01010093 244a305f 62cfd81a
982f3dea dc992dbd 77f6a579 2238ecc4 a7a07812 ad620e45 7064c5e7 97662d98
097e5faf d6cc2865 f201aa08 1a47def9 f97c925a 0869200d d93e6d6e 3c0d6ed8
e6069140 18b9f8c1 eddfdb41 aae09620 c9cd6415 3881c994 eea28429 0b136f8e
db0cdd25 02dba48b 1944d241 7a05694a 584f60ca 7e826a0b 02aa2517 39b5db7f
e784652a 958abd86 de5e8116 832d10cc defda882 2a6d281f 0d0bc4e5 e71a2619
e1f4116f 10b595fc e7420532 dbce9d51 5e28b69e 85d35bef a57d4540 728eb70e
6b0e06fb 33354871 b89d278b c4655f0d 86769c44 7af6955c f65d3208 33a454b6
183f685c f2424a85 3854835f d1e82cf2 ac11d6a8 ed636a
quit
crypto ca certificate chain ASDM_TrustPoint0
certificate 0966b45d
308201d9 30820142 a0030201 02020409 66b45d30 0d06092a 864886f7 0d01010b
05003031 310f300d 06035504 0313064d 592d4153 41311e30 1c06092a 864886f7
0d010902 160f4d59 2d415341 2e756e69 70692e6d 79301e17 0d313931 30323631

```
        36353030 305a170d 32393130 32333136 35303030 5a303131 0f300d06
03550403
        13064d59 2d415341 311e301c 06092a86 4886f70d 01090216 0f4d592d
4153412e
        756e6970 692e6d79 30819f30 0d06092a 864886f7 0d010101 05000381
8d003081
        89028181 00bce5ea f6942f56 47688c70 7771e103 f966bf17 6deaf914 0080620e
        b514cfef e7c2bde2 5304281b a67ed649 56d75f6f d2e0d5f2 03f298f7 84bad12a
        33811378 8fe27b14 0f4c5ec1 9a7ac3e9 c41bab8f db3b6277 bda514f9 5cae8a05
        9ad6cefb d42b8c3d 01771894 f33bf196 e4ef8ccd c832c43b 90bd2840 c3c5847e
        8ad7e506 87020301 0001300d 06092a86 4886f70d 01010b05 00038181
0017f369
        0b483e2a e3801f59 bdbe29ae ee890ca0 2c7654b8 ea8c3b37 2da91f00
423e6b7a
        bf99bc6b d9bd0f2f 97447e7e 55a4245f 8826bc6e 0995057b 23e6e417
ec8e6790
        bb75c69c f4fc0ead 36bde6d1 ac1d7940 db8c610f 543f66a5 12cc1c86 480494f9
        b4daa0a3 c91c9bb9 4a270318 f3f52391 5a21e142 fee51682 92b82df1 49
      quit
    crypto ikev2 policy 1
     encryption aes-256
     integrity sha
     group 5 2
     prf sha
     lifetime seconds 86400
    crypto ikev2 policy 10
     encryption aes-192
     integrity sha
     group 5 2
     prf sha
     lifetime seconds 86400
    crypto ikev2 policy 20
     encryption aes
     integrity sha
     group 5 2
     prf sha
     lifetime seconds 86400
    crypto ikev2 policy 30
     encryption 3des
     integrity sha
     group 5 2
```

```
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 40
 encryption des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable WAN client-services port 443
crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.100.0 255.255.255.0 MGMT
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group14-sha1
console timeout 0
dhcpd address 192.168.100.11-192.168.100.99 MGMT
dhcpd dns 208.67.220.220 208.67.222.222 interface MGMT
dhcpd lease 86400 interface MGMT
dhcpd domain unipi.my interface MGMT
dhcpd enable MGMT
!
dhcpd address 192.168.101.11-192.168.101.99 AV
dhcpd dns 208.67.220.220 208.67.222.222 interface AV
dhcpd lease 86400 interface AV
dhcpd domain unipi.my interface AV
dhcpd enable AV
!
dhcpd address 192.168.102.11-192.168.102.199 BRIDGE
dhcpd dns 208.67.220.220 208.67.222.222 interface BRIDGE
dhcpd lease 86400 interface BRIDGE
dhcpd domain unipi.my interface BRIDGE
dhcpd enable BRIDGE
!
dhcpd address 192.168.103.11-192.168.103.199 CREW
dhcpd dns 208.67.220.220 208.67.222.222 interface CREW
dhcpd lease 86400 interface CREW
dhcpd domain unipi.my interface CREW
dhcpd enable CREW
```

```
!
dhcpd address 192.168.104.11-192.168.104.199 GUEST
dhcpd dns 208.67.220.220 208.67.222.222 interface GUEST
dhcpd lease 86400 interface GUEST
dhcpd domain unipi.my interface GUEST
dhcpd enable GUEST
!
dhcpd address 192.168.105.11-192.168.105.199 VIP
dhcpd dns 208.67.220.220 208.67.222.222 interface VIP
dhcpd lease 86400 interface VIP
dhcpd domain unipi.my interface VIP
dhcpd enable VIP
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 216.239.35.0 source WAN prefer
ntp server 216.239.35.4 source WAN
ssl trust-point ASDM_TrustPoint0 MGMT
ssl trust-point ASDM_TrustPoint0 AV
ssl trust-point ASDM_TrustPoint0 BRIDGE
ssl trust-point ASDM_TrustPoint0 CREW
ssl trust-point ASDM_TrustPoint0 GUEST
ssl trust-point ASDM_TrustPoint0 VIP
ssl trust-point ASDM_TrustPoint0 WAN
webvpn
 enable WAN
 anyconnect image disk0:/anyconnect-win-4.6.03049-webdeploy-k9.pkg 1
 anyconnect profiles SSL-VPN_client_profile disk0:/SSL-VPN_client_profile.xml
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
group-policy GroupPolicy_SSL-VPN internal
group-policy GroupPolicy_SSL-VPN attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
```

```
 split-tunnel-network-list value MGMT
 default-domain none
 webvpn
  anyconnect profiles value SSL-VPN_client_profile type user
dynamic-access-policy-record DfltAccessPolicy
username unipi password
$sha512$5000$/BKWle9lXEM7S3Yk0/aEUg==$tSx8DOuBCX/jQDTs7X3TJQ==
pbkdf2 privilege 15
tunnel-group SSL-VPN type remote-access
tunnel-group SSL-VPN general-attributes
 address-pool VPN-Pool
 default-group-policy GroupPolicy_SSL-VPN
tunnel-group SSL-VPN webvpn-attributes
 group-alias SSL-VPN enable
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
```

```
 inspect xdmcp
 inspect icmp
policy-map type inspect dns migrated_dns_map_2
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
 profile License
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination transport-method http
Cryptochecksum:3e897e4f67b4c74cd41c4d5736acbffd
: end
no asdm history enable
```

8.2 Radius Server

8.2.1 Router

```
ROUTER_OFFICE#sh run
Building configuration...

Current configuration : 2563 bytes
!
! Last configuration change at 02:43:20 UTC Mon Oct 28 2019 by cisco
!
```

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ROUTER_OFFICE
!
boot-start-marker
boot-end-marker
!
!
!
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius if-authenticated
!
!
!
!
!
aaa session-id common
!
!
!
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
no ip icmp rate-limit unreachable
!
```

```
!
!
!
!
!
!
!


!
!
ip dhcp pool TEST
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
cts logging verbose
!
!
username cisco privilege 15 secret 5 $1$WEV3$.ebgonwrbhZ3FvM0x9Ku70
!
redundancy
!
!
ip tcp synwait-time 5
```

```
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
 ip address 192.168.1.200 255.255.255.0
!
interface Ethernet0/1
 ip address 192.168.10.1 255.255.255.0
!
interface Ethernet0/1.150
 encapsulation dot1Q 150
 ip address 192.168.150.1 255.255.255.0
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 no ip address
 shutdown
!
interface Ethernet1/1
 no ip address
 shutdown
```

```
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
```

```
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
!
!
!
!
radius server Radius
 address ipv4 192.168.1.69 auth-port 1812 acct-port 1813
 key test123
!
!
control-plane
!
!
!
!
!
!
!
!
privilege exec all level 3 show running-config
privilege exec level 3 show
!
```

```
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 transport input telnet
!
!
End
```

8.2.2 Client Nas Configuration Radius Server

Client.conf

```
#######################################################################
#
#  Per-socket client lists.  The configuration entries are exactly
#  the same as above, but they are nested inside of a section.
#
#  You can have as many per-socket client lists as you have "listen"
#  sections, or you can re-use a list among multiple "listen" sections.
#
#  Un-comment this section, and edit a "listen" section to add:
#  "clients = per_socket_clients".  That IP address/port combination
#  will then accept ONLY the clients listed in this section.
#
#clients per_socket_clients {
#      client socket_client {
#                ipaddr = 192.0.2.4
#                secret = testing123
#      }
#}
{
client 192.168.1.200 {
secret = test123
```

```
nastype = cisco
shortname = ROUTER_OFFICE
}
```

8.2.3 User Configuration Radius Server

User.conf

```
#############################################################
# You should add test accounts to the TOP of this file! #
# See the example user "bob" above.                 #
#############################################################
admin  Cleartext-Password := "test123"
      Service-Type = NAS-Prompt-User,
      Cisco-AVPair = "shell:priv-lvl=15"

test  Cleartext-Password := "test123"
      Service-Type = NAS-Prompt-User,
      Cisco-AVPair = "shell:priv-lvl=11"

user  Cleartext-Password := "test123"
      Service-Type = NAS-Prompt-User,
      Cisco-AVPair = "shell:priv-lvl=3"
```