ΠΑΝΕΠΙΣΤΗΜΙΟ
ΙΩΑΝΝΙΝΩΝ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΣΕ ΕΝΑ ΕΤΑΙΡΙΚΟ ΔΙΚΤΥΟ : ΠΕΡΙΠΤΩΣΗ ΜΕΛΕΤΗΣ ΜΕ ΣΥΣΚΕΥΕΣ MIKROTIK

Δάφνη Πάσχου

Επιβλέποντες:

Στεργίου Ελευθέριος Αναπληρωτής καθηγητής,

Σπυριδούλα Μαργαρίτη ΕΔΙΠ,Α

Άρτα, Σεπτέμβριος, 2022

NETWORK SECURITY MANAGEMENT: A CASE USING MIKROTIK EQUIPMENT

Εγκρίθηκε από τριμελή εξεταστική επιτροπή

Τόπος, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Επιβλέπων καθηγητής

   Όνομα Επίθετο,

2. Μέλος επιτροπής

   Όνομα Επίθετο,

3. Μέλος επιτροπής

   Όνομα Επίθετο,

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα μεταπτυχιακή εργασία είναι εξ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

Πάσχου Δάφνη

Υπογραφή

ΕΥΧΑΡΙΣΤΙΕΣ

Η πτυχιακή αυτή εργασία υλοποιήθηκε με την υποστήριξη ορισμένων ανθρώπων στους οποίους θα ήθελα να εκφράσω τις θερμότερες ευχαριστίες μου διότι μου έδωσαν την δυνατότητα να κατανοήσω τις βαθύτατες έννοιες των δικτύων καθώς και να αποκτήσω πολύ έντονη επαφή με το αντικείμενο. Ενδεικτικά, θα ήθελα να ευχαριστήσω την κυρία Σπυριδούλα Μαργαρίτη που χάρη σε αυτή μου κινήθηκε το ενδιαφέρον για τον τομέα των δικτύων καθώς και τον κύριο Ελευθέριο Στεργίου ο οποίος μου έδωσε την ευκαιρία να εργαστώ σε δρομολογητές και να φτιάξω το πρώτο μου δίκτυο μόλις στο 7^{ο} εξάμηνο των ακαδημαϊκών σπουδών μου. Ολοκληρώνοντας, ιδιαίτερες ευχαριστίες θα ήθελα να αποδώσω στον κύριο Γρηγόριο Πολύζο, ο οποίος ήταν ο εργοδότης μου στην υποχρεωτική πρακτική άσκηση που πραγματοποίησα για την σχολή μου διότι μου έδωσε την ευκαιρία να δουλέψω ως τεχνικός δικτύων και να συνδυάσω το θεωρητικό υπόβαθρο που είχα με την πρακτική εφαρμογή.

ΠΕΡΙΛΗΨΗ

Στην συγκεκριμένη πτυχιακή εργασία με θέμα *«Διαχείριση Ασφάλειας σε ένα Εταιρικό δίκτυο, Περίπτωση μελέτης με συσκευές Mikrotik»*, θα αναπτυχθούν και θα μελετηθούν βασικές έννοιες των Δικτύων και της Ασφάλειας τόσο γενικότερα στον τομέα της Πληροφορικής όσο και ειδικότερα στον τομέα των Δικτύων. Πιο συγκεκριμένα θα γίνει αναφορά σε ορισμούς που είναι απαραίτητοι τόσο στα Δίκτυα όσο και για όποιον διαβάσει και μελετήσει την παρακάτω πτυχιακή εργασία. Ωστόσο αφού πραγματοποιηθούν οι προαναφερόμενες έννοιες θα διεξαχθεί η μελέτη, η δημιουργία αλλά και η προσομοίωση μέσω ειδικών προγραμμάτων προσομοίωσης, ενός εταιρικού δικτύου το οποίο θα αποτελείται από ένα κεντρικό κατάστημα σε μια μεγάλη πόλη της Ελλάδας. Το βασικό πρόγραμμα που θα χρησιμοποιηθεί για την παραμετροποίηση των συσκευών που θα χρειαστούν είναι ένα εκτελέσιμο αρχείο που αποτελεί δημιούργημα της εταιρείας *Mikrotik*, την εταιρεία δηλαδή από την οποία θα χρησιμοποιηθούν και οι απαραίτητες συσκευές για την διεξαγωγή της προαναφερόμενης μελέτης που θα πραγματοποιηθεί στα πλαίσια της πτυχιακή αυτής εργασίας. Κλείνοντας, αξίζει να σημειωθεί πως ιδιαίτερη βάση θα δοθεί στους τρόπους με τους οποίους μπορεί κανείς να προστατέψει είτε ένα εταιρικό δίκτυο είτε σε οποιοδήποτε άλλο δίκτυο.

Λέξεις-κλειδιά: Network, Security, Mikrotik, Firewall .

ABSTRACT

In this specific thesis on, *«Mikrotik Security management of an enterprise network»*, will be developed basic concepts of Networks and Security both in general field of Information Technology and particular in the field of Networks. Specifically, reference will be made to definitions that are necessary both in Networks and for anyone who reads and studies the following thesis. However, once the aforementioned concepts are realized, the study, creation and simulation will be carried out though special simulation programs, of a corporate network which will consist of a central store and two branches. The basic program that will be used to configure the devices that will be needed is an executable file that is creation of the company Mikrotik, that is the company from which the necessary devices will be used to carry out the already mentioned study that will be carried out in th context of this thesis. In closing, it is worth noting that a special basis will be given to the ways in which one can protect either a corporate network or any other network.

Keywords: Network, Security, Mikrotik, Firewall

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

LAN – Local Area Network

WAN- Wide Area Network

Winbox- Mikrotik Winbox

IP Address- Internet Protocol Address

MAC Address- Media Access Control Address

Src adr- Sourse address

Dst adr – Destination address

Router – routerboard

VLAN- Virtual Local Area Network

Η/Υ – Ηλεκτρονικός Υπολογιστής

ΑΠΟΔΟΣΗ ΟΡΩΝ / ΓΛΩΣΣΑΡΙΟ

Network – δίκτυο

Security – Ασφάλεια

LAN- MAN- WAN(Τοπικό – Μητροπολιτικό Αστικό Δίκτυο)

MAC Address

TCP - UDP

IP Address

IP δικτύων

Src – search address

Dst – destination address

Gateway

Πακέτο δεδομένων - Packet

Firewall

Safe traffic

Routerboard – router – δρομολογητής

hosts

1 Εισαγωγή

Πλέον η ανάγκη για ανταλλαγή δεδομένων και πληροφοριών είναι ζήτημα καθημερινό στη ζωή των ανθρώπων καθώς αποτελεί το μέσο για πρόσβαση στην πληροφορία, διαπροσωπική επικοινωνία, διασκέδαση και ψυχαγωγία, ηλεκτρονικό εμπόριο και online επιχειρηματική δραστηριότητα, πανταχού παρουσία υπολογισμού χάρη στο διαδίκτυο των πραγμάτων. Αξίζει να επισημανθεί η σημασία που έχει το δίκτυο για τον τομέα των επιχειρήσεων καθώς αποτελεί το μέσο για τη άμεση μετάδοση και διάθεση της πληροφορίας, και τον βασικό παράγοντα για βελτίωση της αποτελεσματικότητας και της ανταγωνιστικότητας ενώ επιτυγχάνεται η μείωση του κόστους και του χρόνου που απαιτείται για την επικοινωνία.

Στη σημερινή εποχή, κάθε επιχείρηση διαθέτει το δίκτυό της το οποίο θα πρέπει να έχει αναπτυχθεί ορθά για να είναι αξιόπιστο αλλά και ασφαλές. Το δίκτυο δεδομένων της επιχείρησης θα πρέπει να καλύπτει τις ανάγκες των χρηστών της, να είναι αποτελεσματικό, ανθεκτικό με πανταχού παρούσα και σωστή ισορροπία ποιότητας, ταχύτητας, ασφάλειας, ελέγχου και κόστους. Επιπλέον, θα πρέπει να ληφθεί μέριμνα για συνεχή υποστήριξη των υποδομών του. Η διαδικασία αυτή ονομάζεται διαχείριση δικτύου και είναι απαραίτητη για κάθε εταιρικό δίκτυο. Με βάση τις παραπάνω ανάγκες έχει αναπτυχθεί η παρακάτω πτυχιακή και έχει ως στόχο την ανάπτυξη ενός εταιρικού δικτύου καθώς και την διαχείριση του εστιάζοντας κυρίως στην ασφάλειά του.

1.1 Κίνητρο

Η αφορμή που οδήγησε στην μελέτη του συγκεκριμένου θέματος ήταν μία εργασία που πραγματοποιήθηκε στα πλαίσια του μαθήματος «Ανάλυση και Προσομοίωση Δικτύων» του 7^{ου} εξαμήνου της σχολής Πληροφορικής και Τηλεπικοινωνιών με θέμα «Υλοποίηση δικτύου με συσκευές Mikrotik». Στην συγκεκριμένη εργασία αναπτύχθηκε η υλοποίηση: «Ρύθμιση Mikrotik ως Router με χρήση DHCP Server και με χρήση Bridge». Χάρη σε αυτή δημιουργήθηκε η ανάγκη και η επιθυμία για προσωπική ανάπτυξη και εξέλιξη στον χώρο των Δικτύων. Επιπλέον, καθώς η επιστήμη της Πληροφορικής εξελίσσεται, δημιουργούνται όλο και περισσότεροι κίνδυνοι έτσι γεννήθηκε η ανάγκη προστασίας των δεδομένων. Η συγκεκριμένη έννοια ονομάζεται Ασφάλεια Πληροφοριακών Συστημάτων και στα Δίκτυα ορίζεται ως Ασφάλεια Επικοινωνιών. Έτσι, σε συνδυασμό με τους κινδύνους που διατρέχει ένα δίκτυο στην σημερινή εποχή αλλά και γενικότερα τα Πληροφοριακά Συστήματα δημιουργήθηκε η ιδέα για μελέτη του παραπάνω θέματος και με τον τρόπο αυτό προέκυψε η ανάπτυξη της συγκεκριμένης εργασίας.

1.2 Αντικείμενο και στόχος της πτυχιακής εργασίας

Όπως έχει ήδη αναφερθεί το αντικείμενο που θα αναπτυχθεί στην πτυχιακή αυτή εργασία είναι η Διαχείριση της Ασφάλειας ενός εταιρικού δικτύου. Πιο αναλυτικά, θα σχεδιαστεί, αναπτυχθεί και υλοποιηθεί ένα δίκτυο καταστήματος το οποίο θα απαρτίζεται από ένα κεντρικό κατάστημα και θα βρίσκεται σε μία μεγάλη πόλη της Ελλάδας. Αφού ολοκληρωθεί το δίκτυο αλλά και αναπτυχθεί μεταξύ των συσκευών ο απαραίτητος τρόπος επικοινωνίας θα δοθεί ιδιαίτερη βάση στην δημιουργία της Ασφάλειας του δικτύου αυτού. Ωστόσο η υλοποίηση θα πραγματοποιηθεί σε ένα εικονικό περιβάλλον εργασίας μέσω ειδικών προγραμμάτων που απαιτούνται για την διεξαγωγή της μελέτης του θέματος της εργασίας. Στόχος της πτυχιακής αυτής είναι ο αναγνώστης να γνωρίσει αλλά και να ξεκαθαρίσει ορισμένες βασικές έννοιες για τον τομέα των Δικτύων καθώς και να κατανοήσει την σημαντικότητα της Ασφάλειας των δεδομένων.

1.3 Δομή πτυχιακής εργασίας

Η συγκεκριμένη εργασία αποτελείται από έξι(6) επιμέρους κεφάλαια. Στο πρώτο (1ο) κεφάλαιο γίνεται αναφορά στο κίνητρο που οδήγησε στην ανάπτυξη της πτυχιακής αυτής αλλά και στο αντικείμενο με το οποίο θα αναπτυχθεί καθώς και ο στόχος της. Στο δεύτερο (2ο) κεφάλαιο γίνεται παράθεση ορισμένων βασικών εννοιών για τον τομέα των δικτύων αλλά και γενικότερα παρουσιάζεται το βασικό θεωρητικό υπόβαθρο που καλό είναι να έχει όποιος επιθυμεί να ασχοληθεί με το συγκεκριμένο αντικείμενο που μελετάτε. Στο τρίτο (3ο) κεφάλαιο παρουσιάζεται ο ορισμός αλλά και οι βασικές αρχές της Ασφάλειας τόσο στον τομέα των Πληροφοριακών Συστημάτων όσο και στον χώρο των Επικοινωνιών. Επίσης εστιάζουμε στα Μέσα Προστασίας που υπάρχουν έτσι ώστε να παρέχετε η ασφάλεια των δεδομένων στο δίκτυο αλλά και για την αποφυγή οποιασδήποτε κακόβουλης ενέργειας. Στο τέταρτο (4ο) κεφάλαιο γίνεται λεπτομερής αναφορά στο Firewall το οποίο αποτελεί το βασικότερο Μέσο Προστασίας και περιγράφεται αναλυτικά το πως δημιουργούνται οι κανόνες του Τείχους Προστασίας. Στο πέμπτο (5ο) κεφάλαιο γίνεται ανάπτυξη του Πρακτικού μέρους της εργασίας, πιο συγκεκριμένα σχεδιάζεται , αναπτύσσεται αλλά και παραμετροποιείται το εταιρικό δίκτυο που μελετάτε στην πτυχιακή αυτή. Στο έκτο (6ο)

κεφάλαιο αναπτύσσονται τα συμπεράσματα που προέκυψαν από την μελέτη της συγκεκριμένης πτυχιακής. Ολοκληρώνοντας, γίνεται αναφορά στην Βιβλιογραφία που χρησιμοποιήθηκε για την ανάπτυξη του θεωρητικού μέρους της πτυχιακής αυτής εργασίας.

2 Θεωρητικό υπόβαθρο

Στο συγκεκριμένο κεφάλαιο θα αναλυθούν ορισμένες βασικές έννοιες που χρησιμοποιούνται στον τομέα των δικτύων και οι οποίες αποτελούν τις βασικές θεωρητικές γνώσεις που είναι απαραίτητες έτσι ώστε να είναι σε θέση κανείς να κατανοήσει την λειτουργία τους, τις δυνατότητες που προσφέρουν αλλά και να μπορεί να τις χρησιμοποιήσει για την ανάπτυξη και διαχείριση των δικτύων σε επαγγελματικό επίπεδο. Πιο συγκεκριμένα θα αναπτυχθούν έννοιες όπως: Ορισμός δικτύου υπολογιστών, Δίκτυα και Διαδίκτυο, Μοντέλο Αναφοράς OSI, Virtual Area Networks – VLAN, αλλά και Ασφάλεια Πληροφοριακών Συστημάτων και Επικοινωνιών.

2.1 Βασικές έννοιες

2.1.1 Ορισμός δικτύου υπολογιστών

Δίκτυο υπολογιστών είναι ένα σύνολο από υπολογιστές και συσκευές οι οποίες συνδέονται μεταξύ τους μέσω διαύλων επικοινωνίας οι οποίοι χρησιμοποιούνται για να διευκολύνουν την επικοινωνία μεταξύ των χρηστών. Ωστόσο το δίκτυο επιτρέπει στους χρήστες να ανταλλάσσουν δεδομένα και πόρους με άλλους χρήστες [1]. Κάθε δίκτυο έχει κανόνες με τους οποίους λειτουργεί. Οι κανόνες αυτοί ονομάζονται πρωτόκολλα επικοινωνίας δικτύων και αποτελούν τον κοινό κώδικα με τον οποίο επιτυγχάνεται η επικοινωνία μεταξύ των δικτύων [2].

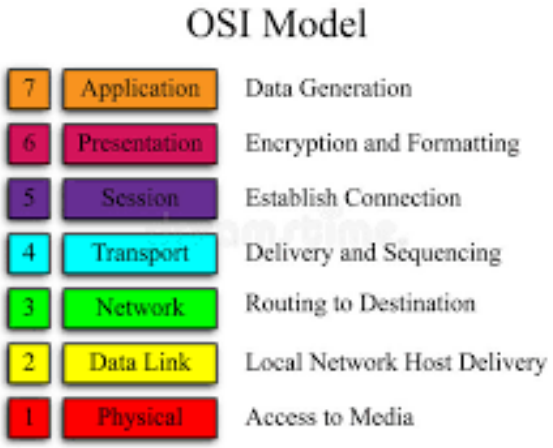
2.1.2 Δίκτυα και Διαδίκτυο

Τα δίκτυα διαχωρίζονται σε κατηγορίες με κριτήριο την διασπορά των συστημάτων στον χώρο αλλά και τον ρόλο που θα έχει το κάθε δίκτυο. Οι κατηγορίες λοιπόν που υπάρχουν είναι οι εξής [4] :

1) Δίκτυα Τοπικής Περιοχής ή Local Area Networks (LAN): η συγκεκριμένη κατηγορία αποτελεί την πιο βασική μορφή δικτύου που μπορεί να συναντήσει κανείς και αποτελείται από ξεχωριστά δίκτυα υπολογιστών που υπάρχουν σε έναν ενιαίο χώρο. Παράδειγμα ενός τέτοιου δικτύου αποτελεί το δίκτυο μιας μικρής επιχείρησης ή ένα οικιακό δίκτυο.
2) Δίκτυα Ευρείας Περιοχής ή Wide Area Networks (WAN): σε αυτή την κατηγορία δικτύων διακρίνονται τα δίκτυα τα οποία αποτελούνται από δύο ή και περισσότερα τοπικά δίκτυα που βρίσκονται σε διαφορετικές περιοχές και συνήθως καλύπτουν μία γεωγραφική περιοχή μεγάλου εύρους.
3) Μητροπολιτικά Δίκτυα ή Metropolitan Area Networks (MAN): τα συγκεκριμένα δίκτυα αποτελούνται από ένα σύνολο τοπικών δικτύων τα οποία βρίσκονται σε ένα μικρό γεωγραφικό τμήμα . Παράδειγμα της κατηγορίας αυτής αποτελούν τα δίκτυα ενός δήμου ή τα δίκτυα των Πανεπιστημιακών Campus.
4) Δίκτυα Προσωπικής Περιοχής ή Personal Area Networks (PAN): η κατηγορία αυτή είναι πιο σύγχρονη μορφή δικτύου η οποία έχει αναπτυχθεί τα τελευταία χρόνια και είναι η μορφή του δικτύου που δημιουργείται από κάποια φορητή συσκευή όπως για παράδειγμα ένας φορητός υπολογιστής ή ένα smartphone.

2.2 Μοντέλο αναφοράς OSI

Το μοντέλο αναφοράς OSI (Open Systems Interconnection), δημιουργήθηκε από έναν παγκόσμιο οργανισμό γνωστό ως ISO (International Standards Organization) το 1977. Σκοπός ήταν η δημιουργία κανόνων έτσι ώστε οι κατασκευαστικές εταιρίες να τηρούν ορισμένες προδιαγραφές κατά την κατασκευή προϊόντων που χρησιμοποιούνται για την ανάπτυξη δικτύων[2]. Το μοντέλο OSI αποτελείται από επτά επίπεδα ή αλλιώς layers και εφαρμόζεται τόσο σε τοπικά δίκτυα όσο και σε δίκτυα ευρείας περιοχής. Κάθε επίπεδο είναι αρμόδιο για ένα διαφορετικό σύνολο λειτουργιών.



Εικόνα 1 Μοντέλο OSI[4].

2.2.1 Επίπεδα μοντέλου αναφοράς OSI

Τα επίπεδα του μοντέλου OSI είναι τα εξής [4]:

1) Φυσικό επίπεδο (Physical layer) : είναι το επίπεδο στο οποίο πραγματοποιείται η μετάδοση των δεδομένων . Η διαδικασία αυτή πραγματοποιείται με την χρήση ορισμένων μέσων μετάδοσης όπως για παράδειγμα ένα κανάλι επικοινωνίας, μέσω του οποίου επιτυγχάνεται η εκπομπή και η λήψη των bits δεδομένων. Αξίζει να σημειωθεί πως στο συγκεκριμένο επίπεδο καθορίζεται ο διαχωρισμός των bit σε “1” και “0” .

2) Επίπεδο ζεύξης δεδομένων (Data link layer) : είναι το επίπεδο στο οποίο εκτελείται μία πολύ σημαντική διεργασία. Πιο συγκεκριμένα μέσω του επιπέδου ζεύξης δεδομένων πραγματοποιείται η μεταφορά των πακέτων (δεδομένων) από το φυσικό επίπεδο στο “ανώτερο “ επίπεδο, δηλαδή στο επίπεδο δικτύου. Η διαδικασία αυτή επιτυγχάνεται μόνο αφού γίνει πρώτα ο έλεγχος των δεδομένων για τυχόν σφάλματα. Επιπλέον, στο επίπεδο αυτό είναι δυνατόν να γίνει και η αντίστροφη διαδικασία. Καταληκτικά στο επίπεδο αυτό τα bit ομαδοποιούνται σε τέσσερα πλαίσια τα οποία αναφέρονται ονομαστικά παρακάτω :

- Πεδίο διεύθυνσης (address)
- Πεδίο ελέγχου (Flow Control)
- Πεδίο δεδομένων (Data)
- Πεδίο ελέγχου λαθών .

3) Επίπεδο Δικτύου (Network layer) : είναι το επίπεδο που είναι υπεύθυνο για την δρομολόγηση των μηνυμάτων και την οργάνωση τους σε πακέτα. Γενικά έχει όλα τα στοιχεία έτσι ώστε να επιτυγχάνεται η δημιουργία, η υποστήριξη αλλά και ο τερματισμός συνδέσεων ανάμεσα στους συνδρομητές ενός δικτύου .

4) Επίπεδο Μεταφοράς (Transport layer) : είναι το επίπεδο το οποίο παρέχει την αξιόπιστη μεταφορά και παράδοση δεδομένων και αυτό συμβαίνει διότι έχει ως βάση του τους μηχανισμούς ελέγχου λαθών για τα χαμηλότερα επίπεδα έτσι ώστε να εξασφαλίζεται η ακεραιότητα των δεδομένων.

5) Επίπεδο Συνόδου (Session layer) : είναι το επίπεδο το οποίο χρησιμοποιεί το επίπεδο Μεταφοράς έτσι ώστε να παρέχει βελτιωμένες υπηρεσίες όπως για παράδειγμα η διαχείριση και ο έλεγχος προσπέλασης της κάθε συνόδου. Ωστόσο μέσω του επιπέδου αυτού επιτρέπεται και η αμφίδρομη επικοινωνία μεταξύ των άκρων μιας σύνδεσης.

6) Επίπεδο Παρουσίασης (Presentation layer) : είναι το επίπεδο στο οποίο πραγματοποιείται η κρυπτογράφηση των δεδομένων. Πιο συγκεκριμένα γίνεται η συμπίεση αλλά και η αποσυμπίεση των δεδομένων έτσι ώστε να μεταφέρονται με ασφάλεια στον τελικό χρήστη.

7) Επίπεδο Εφαρμογών (Application layer) : είναι το επίπεδο που είναι πιο κοντά στο επίπεδο του χρήστη. Μέχρι σήμερα αποτελεί το πιο υψηλό επίπεδο στο πρότυπο του OSI . Αποτελεί το interface μεταξύ της εφαρμογής και των υπόλοιπων επιπέδων. Κατά κύριο λόγο οι λειτουργίες του συγκεκριμένου επιπέδου καθορίζονται από τον χρήστη του δικτύου.

2.3 Δικτυακός εξοπλισμός

2.3.1 Switch

Switch ονομάζεται η συσκευή η οποία ανήκει στο δεύτερο layer του επιπέδου OSI (ωστόσο υπάρχουν και ορισμένες συσκευές Switch οι οποίες ανήκουν στο τρίτο επίπεδο)και έχει την δυνατότητα να μεταφέρει την κίνηση και τα δεδομένα από το ένα interface στο άλλο. Η μεταφορά των δεδομένων από port εισόδου σε port εξόδου αποφασίζεται με βάση τους πίνακες προώθησης που διαθέτει το κάθε switch. Οι δρομολογητές καθορίζουν το περιεχόμενο αυτών των πινάκων. Ωστόσο ο τρόπος με τον οποίο θα γίνεται η μεταφορά

ορίζεται από μία άλλη συσκευή που χρησιμοποιείται και εκεί πραγματοποιούνται όλες οι ρυθμίσεις του δικτύου. Η συσκευή αυτή ονομάζεται δρομολογητής ή αλλιώς routerboard και παρακάτω αναφέρεται αναλυτικά το πως λειτουργεί[5].

Εικόνα 2 Mikrotik Cloud Smart Switch

2.3.2 Δρομολογητές -Routerboard

Routerboard (router) ή αλλιώς δρομολογητής είναι η συσκευή η οποία έχει την δυνατότητα να συνδέει δύο η περισσότερα τοπικά δίκτυα μεταξύ τους και από αυτά να δημιουργεί ένα άλλο δίκτυο ευρείας ζώνης[5]. Όλα τα δίκτυα που συνδέονται μέσω των δρομολογητών θα πρέπει να υποστηρίζουν το ίδιο πρωτόκολλο στο επίπεδο δικτύου. Μία από τις βασικές διεργασίες που εκτελεί ένας δρομολογητής είναι η μεταφορά και η μεταγωγή πακέτων. Είναι μία συσκευή η οποία λειτουργεί στο επίπεδο δικτύου και είναι ανεξάρτητη από το φυσικό επίπεδο και το επίπεδο ζεύξης δεδομένων. Ωστόσο μια συσκευή δρομολόγησης μπορεί να χρησιμοποιηθεί και ως switch με την μέθοδο της γεφύρωσης. Γενικά οι δρομολογητές έχουν πολλές δυνατότητες αλλά και ιδιότητες οι οποίες τους επιτρέπουν να υποστηρίζουν διάφορες τεχνικές ώστε να λειτουργούν σε περισσότερα επίπεδα[2].

Οι δρομολογητές έχουν δύο βασικές χρήσεις :

- Διασυνδέουν δίκτυα Ευρείας ζώνης (WAN)
- Χρησιμοποιούνται στην σύνδεση διαφορετικών Τοπικών δικτύων (LAN)

Εικόνα 3 Mikrotik Routerboard(RB5009UPr+S+IN)

2.4 Δικτυακές τεχνολογίες

2.4.1Virtual Local Area Network -VLAN

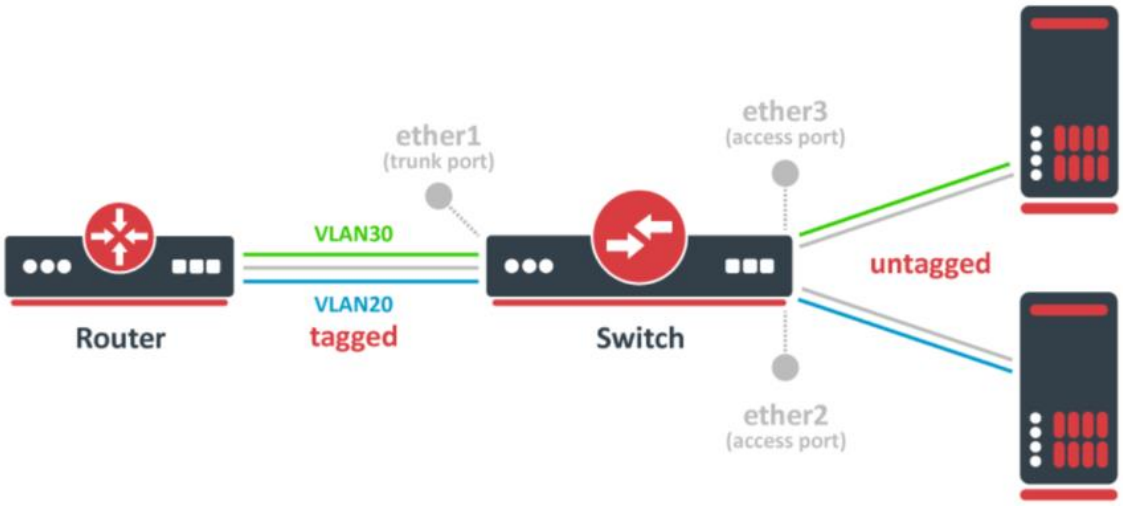
Τα Virtual Local Area Network(VLAN) ή αλλιώς εικονικό τοπικό δίκτυο, είναι μία μέθοδος που επιτρέπει σε πολλές εικονικές συνδέσεις να υπάρχουν σε μια φυσική διεπαφή (ethernet). Ανήκει στο δεύτερο επίπεδο του μοντέλου αναφοράς OSI και έχει την δυνατότητα να διαχωρίζει αποτελεσματικά τα τοπικά δίκτυα LAN. Είναι γνωστό ότι ένα δίκτυο LAN αν δεν έχει προστασία μπορεί πολύ εύκολα κάποιος να συνδεθεί χωρίς να έχει γενικά πρόσβαση σε αυτό. Με την μέθοδο των VLAN, δηλαδή τον διαχωρισμό του δικτύου σε μικρότερα εικονικά δίκτυα, η πρόσβαση στο δίκτυο από κάποιον εξωτερικό χρήστη δεν μπορεί να επιτευχθεί. Αυτό συμβαίνει γιατί η μεταφορά δεδομένων μέσα στο εικονικό δίκτυο πραγματοποιείται μέσω ενός Switch ενώ αντιθέτως η έξοδος των δεδομένων από το εικονικό δίκτυο γίνεται μέσω Δρομολογητή. Ωστόσο υπάρχουν δύο βασικοί όροι στα εικονικά δίκτυα και είναι οι εξής [8]:

Α) **Tagged** είναι η θύρα που μπορεί να μεταφέρει δεδομένα από ένα ή και περισσότερα εικονικά δίκτυα τα οποία είναι διαμορφωμένα σε αυτή, ενώ

Β) **Untagged** είναι η θύρα η οποία έχει διαμορφωμένο μόνο ένα VLAN και μεταφέρει την κίνηση μόνο από αυτό.

Σε αυτό το σημείο αξίζει να σημειωθεί πως οι δύο παραπάνω όροι χρησιμοποιούνται από την εταιρία Mikrotik δηλαδή την εταιρία παραγωγής υλικών για δικτυακές συσκευές που θα χρησιμοποιηθεί στην συγκεκριμένη πτυχιακή εργασία στα πλαίσια ανάπτυξης του πρακτικού μέρους της. Ωστόσο σε άλλες εταιρίες παραγωγής υλικού μπορεί κανείς να

συναντήσει τους όρους αυτούς ως «trunk» και «access». Όπως και αν τις γνωρίζει κανείς, η χρήση τους και οι ιδιότητες τους είναι η ίδια στον τομέα των δικτύων.



Εικόνα 4 Virtual Local Area Network – VLAN[8]

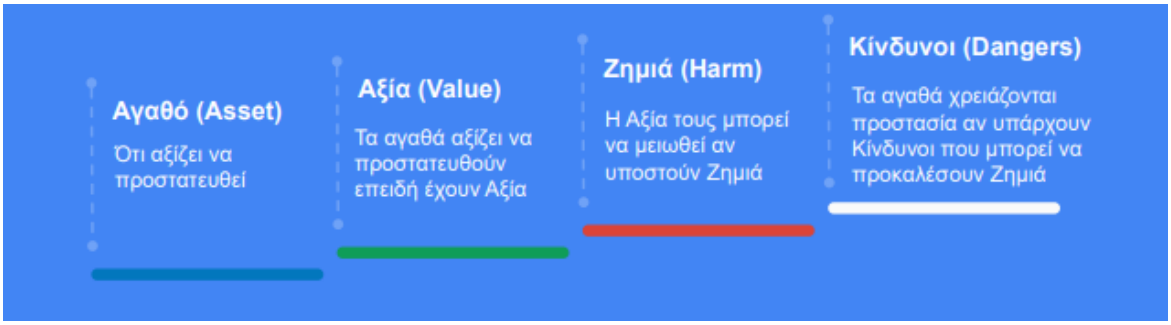
3 Ασφάλεια Δικτύων

3.1 Επισκόπηση

3.1.1 Βασικοί ορισμοί στην Ασφάλεια

Στην Ασφάλεια εκτός από τις Θεμελιώδης Αρχές υπάρχουν και ορισμένοι βασικοί ορισμοί οι οποίοι καλό είναι να τους γνωρίζει όποιος θέλει να ασχοληθεί με το συγκεκριμένο αντικείμενο. Οι έννοιες αυτές αριθμούνται στις τέσσερις (4) και είναι οι εξής[4][6] :

1) Αγαθό (Asset) : είναι οτιδήποτε αξίζει να προστατευτεί στον χώρο της Πληροφορικής μπορεί να είναι είτε κάποιο δεδομένο είτε ένα εταιρικό δίκτυο το οποίο περιέχει σημαντικές πληροφορίες .
2) Αξία (Value) : κάθε αγαθό έχει κάποια αξία για τον λόγο αυτό πρέπει να προστατευτεί
3) Ζημιά (Harm) : κάθε αγαθό έχει μια αξία αν όμως το αγαθό υποστεί κάποια ζημιά αυτόματα θα μειωθεί η αξία αυτή ή ακόμη μπορεί και να χαθεί.
4) Κίνδυνοι (Dangers) : η προστασία των αγαθών είναι πολύ σημαντική διότι υπάρχουν πολλοί κίνδυνοι που μπορεί να του προκαλέσουν Ζημιά.
5) Απειλή(treating) είναι οποιοδήποτε ενέργεια ή δράση με ή χωρίς κακόβουλο κίνητρο και που μπορεί ενδεχομένως να προκαλέσει ζημία σε κάποιο αγαθό



Εικόνα 5 Βασικοί ορισμοί στην Ασφάλεια[4]

3.1.2 Ευρύτερος ορισμός της Ασφάλειας στην Πληροφορική

Ο όρος Ασφάλεια ως ευρύτερη έννοια στον χώρο της Πληροφορικής αφορά την προστασία των δεδομένων και γενικότερα των πληροφοριών που μπορεί να υπάρχουν σε ένα πληροφοριακό σύστημα από τυχόν ζημιές οι οποίες μπορούν να προκαλέσουν μείωση της αξίας τους. Γενικά σκοπός της Ασφάλειας είναι να παρέχει στον χρήστη αξιόπιστες

πληροφορίες και εξουσιοδοτημένες. Υπάρχουν τρία βασικά στάδια στην Ασφάλεια τα οποία αναφέρονται αναλυτικά παρακάτω και είναι τα εξής[4] :

Εικόνα 6 Βασικές Αρχές της Ασφάλειας[4]

1) Πρόληψη : η συγκριμένη έννοια βασίζεται στην διαδικασία λήψης των απαραίτητων μέτρων προστασίας έτσι ώστε να επιτευχθεί η αποφυγή οποιαδήποτε ανεπιθύμητης ενέργειας.
2) Ανίχνευση : με τον όρο ανίχνευση ερμηνεύεται η διαδικασία εντοπισμού ενεργειών και γεγονότων τα οποία προκαλούν κακόβουλες επιθέσεις είτε στο σύστημα είτε στο δίκτυο.
3) Αντίδραση : οι ενέργειες που πραγματοποιούνται για την αποκατάσταση των πόρων οι οποίοι υπέστησαν ζημιά αλλά και η αντιμετώπιση πιθανών εν εξελίξει επιθέσεων.

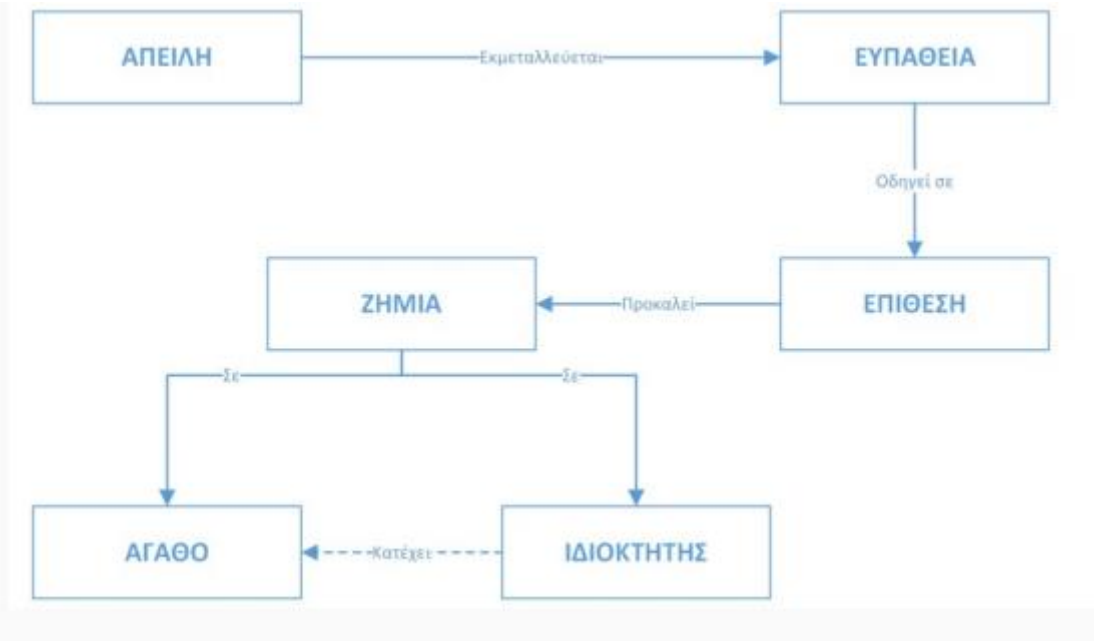
3.1.3 Βασικές Αρχές της Ασφάλειας

Υπάρχουν τρείς (3) βασικές Αρχές της Ασφάλειας με σκοπό την ορθή διαφύλαξη των πόρων αλλά και την προστασία των δεδομένων . Οι Αρχές αυτές ονομάζονται και Θεμελιώδης Αρχές της Ασφάλειας των Πληροφοριών και είναι οι εξής[4]:

1) Εμπιστευτικότητα ή αλλιώς Confidentiality : βασίζεται στην προστασία της πληροφορίας έτσι ώστε να μην αποκαλύπτεται χωρίς εξουσιοδότηση .
2) Ακεραιότητα ή αλλιώς Integrity : η αρχή αυτή βασίζεται στην προστασία της πληροφορίας από οποιαδήποτε μη εξουσιοδοτημένη τροποποίηση της .
3) Διαθεσιμότητα η αλλιώς Availability : η συγκεκριμένη αρχή είναι υπεύθυνη να διαφυλάσσει την εξουσιοδοτημένη πρόσβαση στην πληροφορία με μηδενική καθυστέρηση.

Ωστόσο, στον χώρο των Δικτύων Επικοινωνίας η Ασφάλεια είναι επίσης πολύ σημαντική, για τον λόγο αυτό έχουν αναπτυχθεί ακόμη τέσσερις βασικές Αρχές στην Ασφάλεια από τον χώρο των Τεχνολογιών Πληροφορίας και Επικοινωνιών ή κοινώς ΤΠΕ. Οι αρχές που αναπτύχθηκαν από τον οργανισμό Τεχνολογιών και Πληροφορίας και Επικοινωνιών είναι οι ακόλουθες [4]:

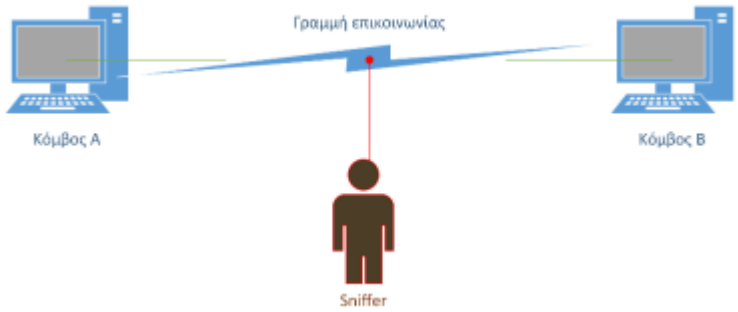
1) Αναγνώριση ή αλλιώς Identification : η διαδικασία κατά την οποία παρουσιάζεται η ταυτότητα μιας οντότητας στον εξυπηρετητή
2) Αυθεντικοποίηση η αλλιώς Authentication : είναι η διαδικασία όπου πραγματοποιείται η επιβεβαίωση της ταυτότητας της οντότητας που έχει παρουσιαστεί στον εξυπηρετητή.
3) Εξουσιοδότηση η αλλιώς Authorization : είναι η διαδικασία κατά την οποία θα επιλεχθεί αν το αίτημα πρόσβασης θα απορριφθεί ή αν θα γίνει αποδεχτό από τον εξυπηρετητή .
4) Αδυναμία αποποίησης η αλλιώς Non-Repudiation : είναι η διαδικασία όπου αποδίδεται η ευθύνη για να πραγματοποιηθεί μια ενέργεια στον εξυπηρετητή.



Εικόνα 7 Βασικοί όροι στην Ασφάλεια[4]

3.2 Κατηγορίες επιθέσεων στο επίπεδο Δικτύου

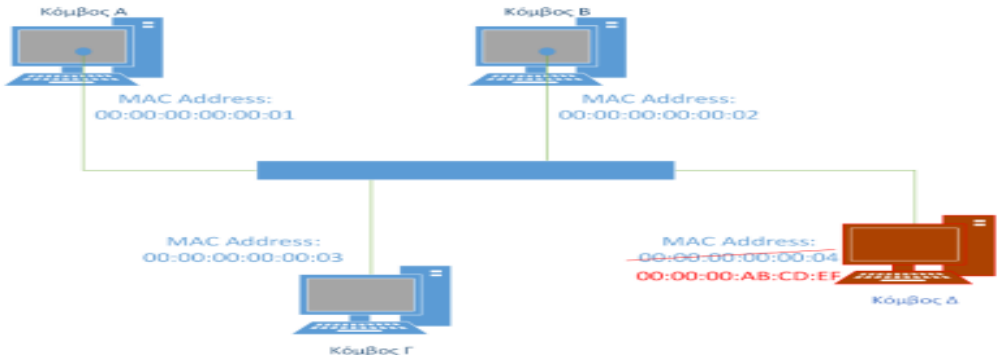
Υπάρχουν δύο μορφές επιθέσεων που μπορεί να πραγματοποιηθούν σε ένα δίκτυο. Στο υποκεφάλαιο αυτό θα δούμε αναλυτικά τα είδη αυτά. Η πρώτη μορφή ονομάζεται Sniffing και ορίζει την προσπάθεια απόσπασης πληροφοριών που πραγματοποιεί μια οντότητα εκτός δικτύου σε ένα δίκτυο. Η ενέργεια αυτή μπορεί να επιτευχθεί μόνο αν η οντότητα εκτός δικτύου αποκτήσει πρόσβαση στο μέσο που μεταφέρονται οι πληροφορίες. Αυτό μπορεί να συμβεί με δύο τρόπους, είτε αν το μέσο ανήκει σε ένα ενιαίο collision domain δηλαδή σε ένα τύπο δικτύου που χρησιμοποιεί κάποιο ασύρματο δίκτυο, είτε αν με κάποιο τρόπο καταφέρει η οντότητα αυτή να αντιγράφει όλες τις πληροφορίες που διακινούνται από μια ορισμένη διεπαφή. Στην περίπτωση της συγκεκριμένης μελέτης σε ένα εταιρικό δηλαδή δίκτυο μία τέτοιας μορφής επίθεση μπορεί να συμβεί από κάποιον ο οποίος θα θέλει να αποσπάσει πολύ σημαντικές πληροφορίες από το δίκτυο της εταιρίας. Αξίζει να σημειωθεί πως μία εταιρία έχει στην κατοχή της πολύ σημαντικά δεδομένα τόσο των πελατών της όσο και των υπαλλήλων της. Αυτά τα δεδομένα μπορεί να είναι οικονομικά αλλά και προσωπικά δεδομένα όπως αριθμοί φορολογικού μητρώου[4].



Εικόνα 8 Κατηγορία επίθεσης με όνομα Sniffer[4]

Η δεύτερη μορφή επίθεσης ονομάζεται MAC Spoofing και αποτελεί την περίπτωση εκείνη όπου η επίθεση γίνεται μέσω του φυσικού επιπέδου πρόσβασης δηλαδή μέσω της MAC Address μιας συσκευής που υπάρχει στο δίκτυο. Η επίθεση αυτή επιτυγχάνεται όταν ο επιτιθέμενος παρεμβληθεί σε κάποια επικοινωνία χρησιμοποιώντας διαφορετική MAC Address η οποία δεν είναι η πραγματική που υπάρχει στο δίκτυο και αυτό το κάνει με σκοπό να υποκλέψει τα πακέτα που προορίζονται για κάποιον εντός του δικτύου. Στην περίπτωση που μελετάτε στην πτυχιακή αυτή η οποία είναι ένα εταιρικό δίκτυο παράδειγμα ενός τέτοιου είδους απειλής είναι όταν για παράδειγμα ένας εργαζόμενος της

επιχείρησης που ανήκει σε έναν τυχαίο τομέα υποθετικά στον τομέα του Marketing προσπαθήσει να υποκλέψει σημαντικά δεδομένα από ένα άλλο τμήμα της εταιρίας όπως είναι το τμήμα του Λογιστηρίου (Accounting). Αυτή η μορφή απειλής είναι ένα πολύ καλό παράδειγμα του MAC Spoofing διότι το τμήμα του Λογιστηρίου έχει πολύ σημαντικά δεδομένα όπως τραπεζικούς λογαριασμούς, αριθμούς φορολογικού μητρώου ακόμη και διευθύνσεις κατοικιών και επιχειρήσεων. Αυτά τα δεδομένα θα πρέπει να προστατευθούν.



Εικόνα 9 Κατηγορία επίθεσης με όνομα MAC Spoofing[4]

3.2 Μηχανισμοί ασφάλειας

Με βάση το μοντέλο OSI καθορίζονται συγκεκριμένοι μηχανισμοί ασφάλειας ανά επίπεδο. Συγκεκριμένα[13]:

- **Ασφάλεια στο επίπεδο εφαρμογών:** Ο κάθε μηχανισμός επιλέγεται σε συνάρτηση με συγκεκριμένη εφαρμογή η οποία διαφέρει για κάθε επίπεδο. Για παράδειγμα το Secure Multipurpose Internet Mail Extensions (S/MIME) χρησιμοποιείται στην κρυπτογράφηση των e-mail, το XMLDSIG και WS security που χρησιμοποιούνται στις ψηφιακές υπογραφές στα web services, ενώ για την πρόσβαση σε έναν ιστότοπο ή σε μια βάση δεδομένων ή σε ένα σύστημα αρχείων εφαρμόζεται ο έλεγχος πρόσβασης με τη χρήση συνθηματικών (identity and password), βάσει ρόλου/διακομιστή/, ή Αυθεντικοποίηση.
- **Ασφάλεια στο επίπεδο μετάδοσης:** Ο μηχανισμός αυτός χρησιμοποιεί μέτρα ασφαλείας για την προστασία των δεδομένων ανάμεσα στους χρήστες. Παράδειγμα αποτελούν τα πρωτόκολλα όπως το HTTP , το Transport Layer Security(TLS) και το Secure Socket Layer(SSL).
- **Ασφάλεια στο επίπεδο δικτύου:** Στο επίπεδο δικτύου χρησιμοποιούνται πρωτόκολλα τα οποία έχουν πολλές εφαρμογές και δεν χρειάζονται τροποποιήσεις. Παράδειγμα του συγκεκριμένου πρωτοκόλλου αποτελεί το πρωτόκολλο Internet Protocol Security (IPSec).
- **Ασφάλεια στο επίπεδο ζεύξης δεδομένων:** Όπως και σε παραπάνω επίπεδα έτσι και στο επίπεδο ζεύξης δεδομένων γίνεται χρήση πρωτοκόλλων για την ασφάλεια των δεδομένων . Πιο συγκεκριμένα χρησιμοποιείται το πρωτόκολλο ARP Spoofing το οποίο έχει την δυνατότητα να χαρτογραφεί τις IP διευθύνσεις που είναι γνωστές στην φυσική διεύθυνση που γνωρίζει η Ethernet σε τοπικό επίπεδο. Μια ακόμη μέθοδο που χρησιμοποιείται στο επίπεδο αυτό είναι η μέθοδος MAC flooding που είναι ένας απλός πίνακας που περιέχει MAC Addresses και όταν κάποιος πραγματοποιήσει κάποια επίθεση μπορεί να λαμβάνει τα δεδομένα από τον πίνακα αυτόν. Η διαδικασία αυτή γίνεται μέσω ενός μεταγωγέα. Ωστόσο στο συγκεκριμένο επίπεδο υπάρχουν και δύο ακόμη μέθοδοι , το Port Stealing και οι Επιθέσεις DHCP.
- **Ασφάλεια σε εικονικά δίκτυα:** Η μέθοδος που χρησιμοποιείται στο συγκεκριμένο επίπεδο είναι η μέθοδος των VLAN. Πιο συγκεκριμένα τα εικονικά δίκτυα δημιουργούν όρια στο δίκτυο στα οποία η μετάδοση δεδομένων μέσω DHCP και

ARP δεν είναι εφικτή. Σε έναν μεταγωγέα μπορούν να υπάρχουν περισσότερα από ένα VLAN.

3.3 Μέσα Προστασίας

Στο συγκεκριμένο κεφάλαιο θα αναπτυχθούν θέματα που αφορούν τα μέσα προστασίας ενός αγαθού, στην περίπτωση της πτυχιακής αυτής εργασίας είναι ένα εταιρικό δίκτυο. Τα Μέσα Προστασίας θα μπορούσε κανείς να πει ότι είναι ένα σχέδιο ασφαλείας που χρησιμοποιεί ο ιδιοκτήτης ή πιο απλά ο χρήστης για να διατηρήσει ασφαλές το αγαθό του. Για κάθε σχέδιο ο χρήστης ακολουθεί μία Στρατηγική(Strategy). Κάθε Στρατηγική ορίζει τον τρόπο με τον οποίο τα Μέτρα Προστασίας θα ικανοποιήσουν τις Απαιτήσεις του χρήστη αλλά και τα μέσα μείωσης των Επιπτώσεων Παραβίασης που θα χρησιμοποιηθούν. Σκοπός είναι να επιτευχθεί η προστασία των δεδομένων[4].

Ωστόσο τα Μέτρα Προστασίας μπορούν να σταματήσουν την Απειλή, δηλαδή την πιθανή κακόβουλη κίνηση, αναπτύσσεται μειώνοντας τις πιθανότητες να πραγματοποιηθεί. Αυτό συμβαίνει διότι παρέχουν μια παθητική αντίσταση στην Απειλή. Γενικότερα μειώνουν την ευπάθεια των πληροφοριών και κατά συνέπεια τις επιπτώσεις στον οργανισμό που ανήκουν οι συγκεκριμένες πληροφορίες .

4 Τείχος Προστασίας – Firewall

Firewall είναι ένα σύστημα το οποίο έχει σχεδιαστεί για να αποτρέπει την ανεπιθύμητη πρόσβαση που μπορεί να εισέρθει σε ένα ιδιωτικό δίκτυο από το διαδίκτυο φιλτράροντας τα εισερχόμενα δεδομένα που προέρχονται από αυτό[9]. Γενικότερα αποτρέπει την ανεπιθύμητη κίνηση και επιτρέπει μόνο την επιθυμητή. Ωστόσο σκοπός του είναι να δημιουργεί ένα ασφαλές φράγμα ανάμεσα στο ιδιωτικό δίκτυο και στο ίντερνετ, εκεί δηλαδή όπου οι κακόβουλοι χρήστες θα προσπαθήσουν να παραβιάσουν το ιδιωτικό δίκτυο. Οι κινήσεις αυτές περνάνε είτε στο τοπικό firewall είτε από το τοπικό firewall ή διαμέσων του firewall. Υπάρχουν κατηγορίες στο firewall, το passive(παθητικό) και το bridging firewall (γεφύρωση). Και στις δύο περιπτώσεις κάθε συσκευή εισέρχεται στο δίκτυο μέσω layer2 (επίπεδο ζεύξης δεδομένων) που σημαίνει ότι τα πακέτα δεν είναι δρομολογημένα. Τυπικά έχουν μια διεύθυνση IP αλλά χρησιμοποιείται μόνο από τον διαχειριστή. Αντίθετα σε έναν δρομολογητή όλα τα πακέτα περνάνε από το passive firewall εκτός αν υπάρχουν κανόνες που τα απορρίπτουν. Στην συγκεκριμένη πτυχιακή εργασία στο τμήμα το οποίο θα μελετηθεί το πρακτικό μέρος της θα χρησιμοποιηθεί για την ασφάλεια του εταιρικού δικτύου η μέθοδος του passive firewall στον δρομολογητή διότι είναι πολύ σημαντικό να γνωρίζει ο διαχειριστής τι πακέτα εισέρχονται στο δίκτυο. Ο λόγος που γίνεται αυτό είναι για να αποτρέψει τις απειλές που μπορεί να συμβούν σε ένα δίκτυο. Οι απειλές αυτές έχουν αναπτυχθεί αναλυτικά στο προηγούμενο κεφάλαιο.

Ωστόσο, το firewall χρειάζεται ορισμένους κανόνες έτσι ώστε να περιορίζει την ροή της κίνησης. Οι κανόνες αυτοί οργανώνονται σε αλυσίδες και σκοπός τους είναι να ορίζουν τον τρόπο με τον οποίο το firewall θα δέχεται ή θα απορρίπτει πακέτα. Υπάρχουν τρείς προκαθορισμένοι κανόνες- αλυσίδες στο firewall και είναι οι εξής : 1) input, 2) output, 3) forward. Ωστόσο ανάλογα την χρήση του firewall μπορούν να δημιουργηθούν και άλλοι κανόνες, όλοι όμως ως βάση θα πρέπει να έχουν τους τρεις προκαθορισμένους κανόνες . Επιπρόσθετα, οι επιπλέον κανόνες μπορούν να δημιουργηθούν από τους χρήστες, χωρίς όμως να έχουν την δυνατότητα να βλέπουν την κίνηση ή τα πακέτα που εισέρχονται . Αυτό μπορεί να συμβεί μόνο αν τα πακέτα αυτά στέλνονται με βάση τους τρεις κανόνες που αναφέρθηκαν.

Οι κανόνες του firewall είναι απλοί αντιστοιχιστές πακέτων. Καθορίζουν ορισμένα κριτήρια ώστε να αναγνωρίζουν πακέτα και να εκτελούν κάποιες ενέργειες στα πακέτα αυτά. Οι

κανόνες λειτουργούν σαν ένα loop στον τομέα του προγραμματισμού δηλαδή με “if-then”. Το κριτήριο ελέγχεται από την ακολουθία “if”, “αν “ δηλαδή και ελέγχει αν ταιριάζει με τα κριτήρια των κανόνων(rules) και το “then”, δηλαδή “τότε” εκτελεί την αντίστοιχη διαδικασία για το κάθε πακέτο(είτε αποδοχή είτε απόρριψη πακέτου).

4.1 Input chain

Ο συγκεκριμένος κανόνας είναι σχεδιασμένος να προστατεύει τον δρομολογητή και αποτελεί τον βασικό τύπο firewall σε ένα routerboard αφού βρίσκεται στο Gateway του δηλαδή εκεί που φαίνεται στο public ίντερνετ ο δρομολογητής από το τοπικό δίκτυο[9]. Τα LAN δίκτυα χρησιμοποιούν ιδιωτικές IP διευθύνσεις που δεν είναι γνωστές στο public internet ή το WAN, επίσης βρίσκεται πίσω από τις δημόσιες διευθύνσεις πίσω από το firewall. Τα πακέτα που προέρχονται είτε από το LAN είτε από το WAN προορίζονται για τον δρομολογητή και θα περάσουν το input chain με τον τρόπο αυτό η τοποθεσία είναι αυτή που θα προστατέψει τον δρομολογητή. Αυτό αποτελεί μία σημαντική λεπτομέρεια για την λειτουργία των IP δικτύων όπως αναφέρεται για τον σχηματισμό πακέτων. Τυπικά τα πακέτα που έρχονται σε έναν δρομολογητή είναι είτε τα πακέτα που προέκυψαν από κάποια σύνδεση ή επικοινωνία, είτε τα πακέτα που ξεκίνησαν από τον δρομολογητή αφού προηγήθηκε κάποια διαμόρφωση (configuration) ή διαχείριση. Αυτό στενεύει σε μεγάλο βαθμό την λίστα από τις ασφαλείς συνδέσεις (διευθύνσεις IP) και κάνει τους κανόνες του firewall πιο απλούς. Η πιο απλή τεχνική που χρησιμοποιείται για να δημιουργήσει κανείς κανόνες στο firewall είναι με το να καθορίσει τι θα επιτρέπει ως καλή κίνηση (safe traffic) και τι κίνηση θα θεωρείται κακόβουλη για να απορρίπτεται. Στο κεφάλαιο 4.5 θα παρουσιαστεί αναλυτικά ο τρόπος που δημιουργείται ο συγκεκριμένος κανόνας στο περιβάλλον Winbox και σε συσκευή δρομολόγησης της εταιρίας Mikrotik .

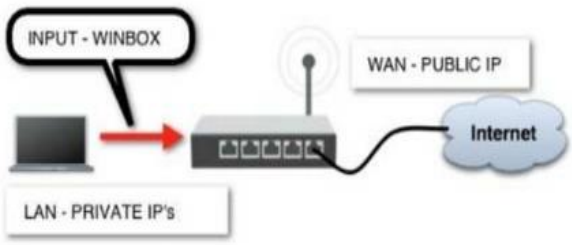


Figure 1 - IP Firewall Input Chain

Εικόνα 10 Firewall - Input chain

4.2 Output Chain

Το output chain έχει ακριβώς τον ίδιο τρόπο λειτουργίας με το input chain, η μόνη διαφορά που έχουν είναι ότι το output chain στέλνει τα πακέτα στα chain που προορίζουν την κίνηση από και προς το εξωτερικό δίκτυο[9]. Καλό είναι να αναφερθεί πως πολύ σπάνια θα δημιουργηθεί κάποιος κανόνας για το συγκεκριμένο chain διότι όλα τα πακέτα για να εισέρθουν στον δρομολογητή θα πρέπει πρώτα να περάσουν από τους κανόνες που έχουν τεθεί για το input chain. Καταληκτικά, αν τα πακέτα ακολουθούν τους κανόνες του input chain και περάσουν στο δίκτυο, η δημιουργία κανόνων για το output chain θα είναι άστοχοι.

4.3 Forward Chain

Ο συγκεκριμένος προκαθορισμένος κανόνας του Firewall έχει την ιδιότητα να προστατεύει τους πελάτες (clients) του ιδιωτικού δικτύου[9]. Η κίνηση μεταφέρεται από τους hosts πίσω από το firewall και περνάει από το forward chain . Οι κανόνες των client τοποθετούνται σε αυτό το σημείο ακριβώς. Για να υλοποιηθεί ο κανόνας αυτός απαραίτητη προϋπόθεση είναι να δημιουργηθούν ορισμένα φίλτρα – κανόνες τα οποία θα καθορίζουν ποια πρωτόκολλα θα επιτρέπεται να περνάνε από το firewall και ποια θα απορρίπτονται. Παρόλα αυτά, αντικειμενικά για να προστατευτούν οι συνδέσεις σε ένα δίκτυο και να προστατευτούν οι clients δεν αρκούν οι απλοί κανόνες. Ο βασικότερος κανόνας στο forward chain είναι να επιτρέψουμε την κίνηση στο LAN για τους πελάτες έτσι ώστε να δημιουργηθούν καινούργιες συνδέσεις στο firewall. Αναλυτικότερα το πως οργανώνεται και δημιουργείται ο συγκεκριμένος κανόνας θα παρουσιαστεί στο κεφάλαιο 4.5.

5 Πρακτικό μέρος

Στο συγκεκριμένο κεφάλαιο αρχικά θα αναφερθεί ο τρόπος με τον οποίο θα οργανωθεί το εταιρικό δίκτυο, τι υλικά είναι απαραίτητα για την δημιουργία του καθώς και πως αυτό το δίκτυο θα είναι ασφαλές. Ωστόσο αξίζει να σημειωθεί πως στο κεφάλαιο αυτό θα πραγματοποιηθεί και το πρακτικό μέρος της πτυχιακής αυτής εργασίας το οποίο αποτελείται από προσομοιώσεις σε συγκεκριμένα περιβάλλοντα προσομοίωσης δικτύων.

5.1 Εργαλεία προσομοίωσης

Στο συγκεκριμένο μέρος της εργασίας που αφορά την πρακτική μελέτη και ανάλυση του δικτύου θα χρησιμοποιηθούν ορισμένα προγράμματα που είναι γνωστά στον τομέα των δικτύων διότι χρησιμοποιούνται για τον σχεδιασμό την υλοποίηση και την προσομοίωση οποιασδήποτε μορφής δικτύου. Πιο συγκεκριμένα θα χρησιμοποιηθούν τα παρακάτω προγράμματα :

1) GNS3 VM για την σχεδίαση του δικτύου [10],
2) VMware WorkStation Player16 για την προσομοίωση και εισαγωγή των συσκευών που απαιτούνται για την συγκεκριμένη πρακτική μελέτη[11],
3) Mikrotik Winbox, για την ρύθμιση, προσομοίωση και εξαγωγή του configuration που θα χρησιμοποιηθεί στο δίκτυο[12].

5.2 Σχεδίαση και παρουσίαση της δομής του εταιρικού δικτύου.

Στο συγκεκριμένο μέρος της πτυχιακής αυτής εργασίας θα γίνει εκτενής αναφορά στην σχεδίαση και παρουσίαση της δομής που θα έχει το εταιρικό δίκτυο το οποίο μελετάτε. Πιο αναλυτικά,η εταιρία που μελετάτε έχει ένα κύριο κατάστημα σε μία μεγάλη πόλη της Ελλάδος. Η δομή και ο τρόπος οργάνωσης τους δικτύου της εταιρίας που θα μελετηθεί περιγράφεται παρακάτω :

Το κεντρικό κατάστημα της εταιρίας θα αποτελείται από δύο ορόφους, ένα ισόγειο και ένα υπόγειο. Συγκεκριμένα, στο υπόγειο της εταιρίας θα βρίσκεται το Server room το δωμάτιο δηλαδή το οποίο θα φιλοξενεί τους κεντρικούς Server της εταιρίας. Οι Server θα είναι δύο, ένας θα είναι ο FileServer ο οποίος χρησιμοποιείται για την αποθήκευση αλλά και αναζήτηση αρχείων της εταιρίας. Ο Server αυτός θα είναι ένας απλός υπολογιστής ο οποίος

θα έχει ένα ethernet port για την σύνδεση του με τον κεντρικό δρομολογητή. Ο δεύτερος Server θα χρησιμοποιείται για την βάση δεδομένων της εταιρίας. Και οι δύο Server's θα συνδέονται με έναν κεντρικό δρομολογητή ο οποίος στην περίπτωση της προσομοίωσης θα είναι ο chr (cloud hosting router) της Mikrotik. Σε περίπτωση υλοποίησης θα μπορούσε να είναι ένας RB4011. Σε κάθε περίπτωση ο δρομολογητής θα έχει σαν DNS Server τον Server της Google δηλαδή τον : 8.8.8.8 και θα συνδέεται με ένα κεντρικό switch. Η παραπάνω περιγραφή αφορά μόνο το Server room στο υπόγειο .

Όσον αφορά το ισόγειο, στο συγκεκριμένο τμήμα θα φιλοξενούνται δύο βασικά τμήματα της εταιρίας το τμήμα Management και το τμήμα του Λογιστηρίου. Και τα δύο τμήματα θα ανήκουν σε ένα VLAN δίκτυο το οποίο θα ονομάζεται VLanAccounting20. Αξίζει να σημειωθεί πως όλες οι απαραίτητες συσκευές θα συνδέονται σε ένα κεντρικό Switch που θα υπάρχει στον όροφο αυτό. Το switch αυτό θα ονομάζεται Switch_Ground_Floor .

Στον πρώτο όροφο της εταιρίας θα φιλοξενηθεί το τμήμα Marketing. Το συγκεκριμένο τμήμα θα ανήκει στο VLan με όνομα VLanMarketing30. Επίσης θα υπάρχει και σε αυτόν τον όροφο ένα κεντρικό switch στο οποίο θα συνδέονται όλες οι συσκευές που είναι απαραίτητο και θα ονομάζεται Switch_First_Floor.

Τέλος στο δεύτερο όροφο της εταιρίας θα φιλοξενούνται δύο τμήματα, το τμήμα του IT και το τμήμα Διοίκησης, όπου το καθένα θα ανήκει αντίστοιχα σε κάποιο VLan. Πιο συγκεκριμένα το VLanIT40 θα είναι για το τμήμα του IT και στο το τμήμα της διοίκησης θα ανήκει και αυτό στο VLanAccounting20 στο οποίο ανήκουν εξίσου τα τμήματα του Λογιστηρίου και του Management. Αξίζει να σημειωθεί πως όλα τα VLan θα ανήκουν στο VLan του διαχειριστή το οποίο θα ονομάζεται VLanAdmin26. Η σημασία του συγκεκριμένου VLan είναι μεγάλη διότι θα πρέπει ο διαχειριστής να έχει πρόσβαση σε όλα τα υποδίκτυα και οποιαδήποτε αλλαγή χρειαστεί θα έχει το δικαίωμα μόνο αυτός να την πραγματοποιήσει. Σε αυτό το σημείο θα μπορούσε κανείς να πει πως ξεκινάει και η ασφάλεια του δικτύου της εταιρείας αφού για να θεωρηθούν ασφαλής τα δεδομένα της εταιρείας θα πρέπει να διασφαλιστεί ότι δεν θα μπορεί οποιοσδήποτε να έχει πρόσβαση σε αυτά. Τα ξεχωριστά VLan δίκτυα θα δημιουργηθούν για αυτόν τον σκοπό. Ωστόσο μπορεί ορισμένα από αυτά τα τμήματα να μοιράζονται πληροφορίες από τα ίδια αρχεία αυτά τα τμήματα λοιπόν θα ανήκουν στο ίδιο VLan άρα και στο ίδιο υποδίκτυο. Έτσι με αυτόν τον τρόπο διασφαλίζεται ότι κανένας απλός χρήστης δεν μπορεί να αντλήσει πληροφορίες από το εσωτερικό δίκτυο. Ωστόσο για να προστατευτεί ένα εταιρικό δίκτυο δεν φτάνει μόνο ο

διαχωρισμός των εσωτερικών υποδικτύων αλλά απαιτείται για την ασφάλεια των δεδομένων η προστασία ολόκληρου του δικτύου δηλαδή θα πρέπει να περιοριστεί η είσοδος των δεδομένων από το εξωτερικό δίκτυο, το δίκτυο δηλαδή του Internet. Πιο συγκεκριμένα θα πρέπει να γνωρίζει το δίκτυο τα πακέτα δεδομένων που εισέρχονται σε αυτό αλλά και να τα αναγνωρίζει. Όπως έχει αναφερθεί και παραπάνω η μέθοδος αυτή ονομάζεται τοίχος προστασίας ή αλλιώς Firewall. Σε προηγούμενο κεφάλαιο πραγματοποιήθηκε εκτενής αναφορά στον όρο του Firewall, ωστόσο παρακάτω θα παρουσιαστεί αναλυτικά και η διαδικασία η οποία χρειάζεται για να επιτευχθεί η προαναφερόμενη μέθοδος.

Η εικόνα που θα έχει το εταιρικό δίκτυο που μόλις αναφέρθηκε έπειτα από την ανάπτυξη του στο περιβάλλον του GNS3 είναι η παρακάτω(για διευκόλυνση της προσομοίωσης έχει χρησιμοποιηθεί ένα επιπλέον Switch το οποίο είναι συνδεδεμένο στον κεντρικό δρομολογητή και τον πάροχο καθώς και με όλα τα υπάρχοντα Switch . Με τον τρόπο αυτό πραγματοποιήθηκε η σύνδεση των Switch και του κεντρικού δρομολογητή στο περιβάλλον του Winbox και πραγματοποιήθηκε η παραμετροποίηση που δίνεται σε επόμενο υποκεφάλαιο). Ωστόσο για την ανάπτυξη του εταιρικού δικτύου θα χρησιμοποιηθούν τα εξής δικτυακά προϊόντα:

1)Ένας Δρομολογητής Mikrotik chr (cloud hosting router)

2) Ένα απλό virtual switch για να βλέπω τα υπόλοιπα switch που υπάρχουν σε κάθε όροφο

3)Τέσσερις ακόμη chr που με την μέθοδο “Bridge” θα χρησιμοποιηθούν ως switch

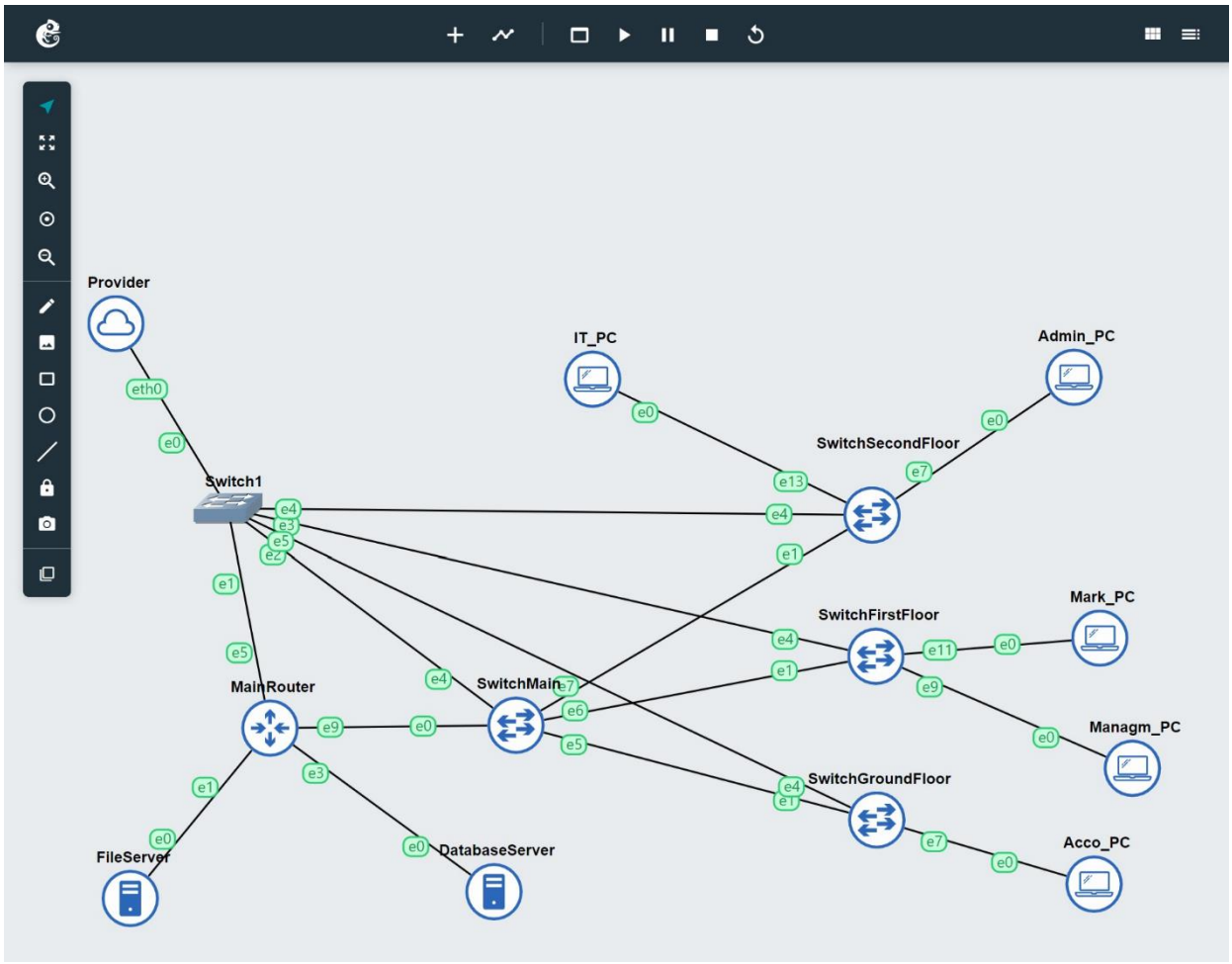
4)Πέντε υπολογιστές , ένας για κάθε τμήμα της εταιρίας

5) Πάροχος δικτύου

6)Δύο Server’s

7)Καλώδια κατηγορίας ethernet για την σύνδεση όλων των απαραίτητων συσκευών στο δίκτυο

Τελικά η εικόνα του δικτύου θα είναι ως εξής:



Εικόνα 11 Εικόνα του εταιρικού δικτύου

5.2.1 Υποδίκτυα του εταιρικού δικτύου.

Στο εταιρικό δίκτυο που θα δημιουργηθεί για τα πλαίσια της συγκεκριμένης πτυχιακής εργασίας θα αναπτυχθούν ορισμένα υποδίκτυα τα οποία όπως αναφέρθηκε στο προηγούμενο υποκεφάλαιο θα ανήκουν στα VLan του κάθε τμήματος της εταιρίας. Πιο συγκεκριμένα τα υποδίκτυα θα είναι τα εξής :

Α) Το υποδίκτυο που θα ανήκει στον διαχειριστή και ανήκει στο VLanAdmin26 έχει διεύθυνση IP :192.168.26.0/24

Β) Το υποδίκτυο που θα ανήκει στα τμήματα που ανήκουν στο VLanAccounting20 έχει διεύθυνση IP :192.168.20.0/24

Γ) Το υποδίκτυο που θα ανήκει στο τμήμα του Marketing και ανήκει στο VLanMarketing30 έχει διεύθυνση IP :192.168.30.0/24

Δ) Το υποδίκτυο που θα ανήκει στο τμήμα του IT και ανήκει στο VLanIT40 έχει διεύθυνση IP :192.168.40.0/24 .

5.2.2 Γιατί επιλέχθηκαν συσκευές Mikrotik;

Στα πλαίσια της συγκεκριμένης πτυχιακής εργασίας επιλέχθηκαν συσκευές της εταιρίας Mikrotik διότι είναι μια εταιρία ανάπτυξης υλικού δικτύων η οποία παρέχει καλούς και λειτουργικούς δρομολογητές αλλά και λοιπές συσκευές που χρησιμοποιούνται στα δίκτυα και όλα αυτά σε τιμές που είναι προσιτές για όλων των τύπων επιχειρήσεις αφού το κόστος σε σχέση με άλλες επώνυμες εταιρίες του χώρου είναι πολύ οικονομικές διότι είναι μια καινούργια εταιρεία στο χώρο του υλικού για την χρήση σε δικτυακά συστήματα. Καταληκτικά, παρόλο το μειωμένο κόστος ανάπτυξης του δικτύου προσφέρουν ασφάλεια τόσο στο υλικό κομμάτι όσο και στο κομμάτι του δικτύου.

5.2.3 Ποιο μοντέλο/ μοντέλα θα χρησιμοποιήσω

Το μοντέλο που θα χρησιμοποιηθεί για την συγκεκριμένη προσομοίωση θα είναι ο δρομολογητής chr ή αλλιώς cloud hosting router ο οποίος είναι σε εικονική μορφή και μπορεί κανείς να τον βρει στην επίσημη σελίδα της Mikrotik []. Αξίζει να σημειωθεί πως ο δρομολογητής αυτός θα χρησιμοποιηθεί μόνο για τα πλαίσια της προσομοίωσης . Ωστόσο αν χρειαστεί το δίκτυο που θα μελετηθεί να υλοποιηθεί σε μια εταιρία θα μπορούσε να χρησιμοποιηθεί ένας άλλος δρομολογητής της ίδιας εταιρίας ο Rb4011 ο οποίος είναι ένας πολύ καλός δρομολογητής και χρησιμοποιείται για επαγγελματικές χρήσεις. Επίσης καλό είναι να αναφερθεί πως έχουν χρησιμοποιηθεί ακόμη τέσσερις (4) δρομολογητές chr οι οποίοι έχουν προγραμματιστεί κατάλληλα έτσι ώστε να χρησιμοποιηθούν σαν switches. Τέλος οι υπολογιστές που χρησιμοποιήθηκαν τόσο για την ανάπτυξη των τμημάτων της εταιρείας όσο και για τους Server’s της είναι ένα απλό Virtual PC που υπάρχει εγκατεστημένο στο περιβάλλον του GNS3.

5.2.4 Ολοκλήρωση των απαραίτητων συνδέσεων για το εταιρικό δίκτυο.

Για να πραγματοποιηθεί οποιαδήποτε παραμετροποίηση τόσο στον δρομολογητή όσο και στο δίκτυο θα πρέπει πρώτα να μπορεί ο δρομολογητής να επικοινωνεί με τις συσκευές

που είναι συνδεδεμένες στο δίκτυο του. Πιο συγκεκριμένα θα πρέπει δηλαδή να υπάρχει επικοινωνία από την μια άκρη του δικτύου μέχρι την άλλη. Αυτό είναι πολύ εύκολο να το ελέγξει κανείς τα βήματα είναι τα εξής :

Α)να δημιουργηθούν οι συνδέσεις των συσκευών στο δίκτυο και

Β) να ελεγχθεί αν ο δρομολογητής «βλέπει» τις συσκευές αυτές.

Όπως φαίνεται στην εικόνα 11 η συνδέσεις έχουν πραγματοποιηθεί οπότε μένει να ελεγχθεί αν ο δρομολογητής «βλέπει» τις συσκευές. Αυτό μπορεί να γίνει απλώς εκτελώντας την εντολή *ping* από τον δρομολογητή προς κάθε διεύθυνση IP που έχουν οι συσκευές. Αν ο δρομολογητής βλέπει όλες τις συσκευές τότε το δίκτυο είναι έτοιμο και μπορεί να γίνει όποια παραμετροποίηση χρειάζεται. Καλό είναι να αναφερθεί πως οι διευθύνσεις που έχουν δωθεί στου υπολογιστές ανήκουν μερικές σε διαφορετικά υποδίκτυα για λόγους ασφαλείας και είναι οι εξής :

Η/Υ τμήματος Λογιστηρίου : 192.168.20.150

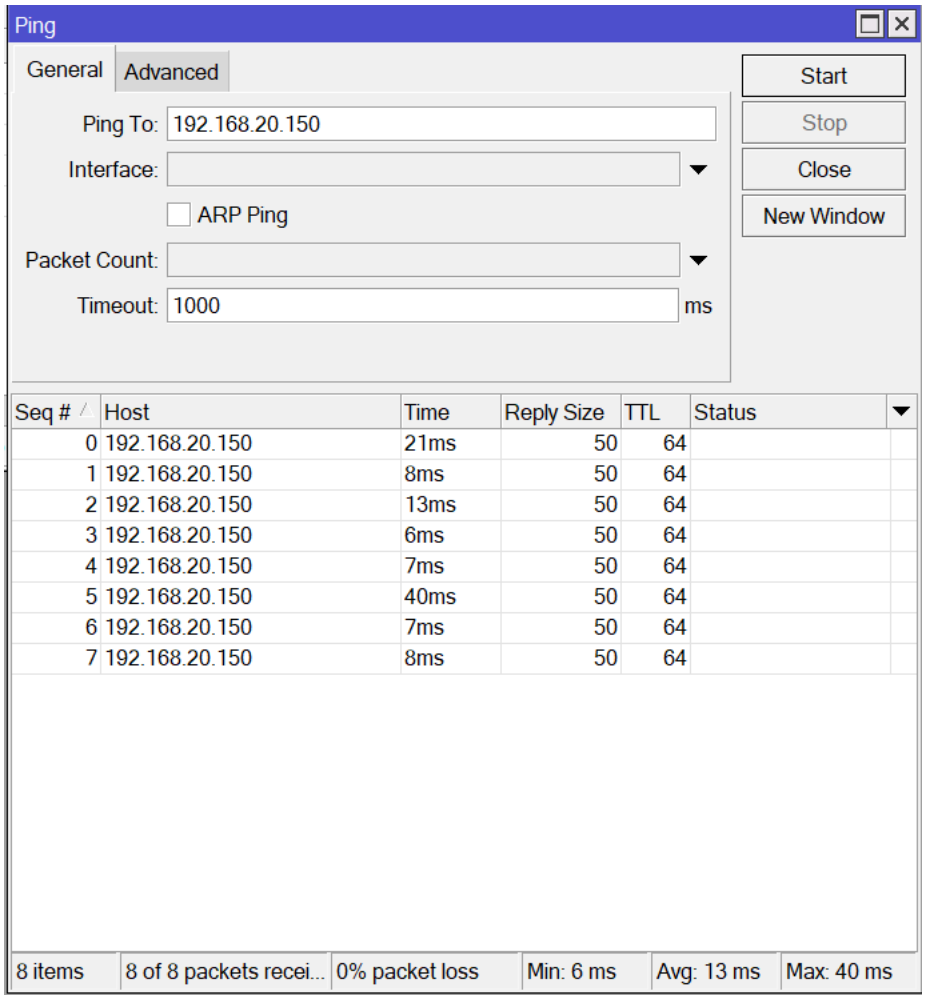
Η/Υ τμήματος Management : 192.168.20.150

Η/Υ τμήματος Administration : 192.168.20.170

Η/Υ τμήματος Marketing : 192.168.30.150

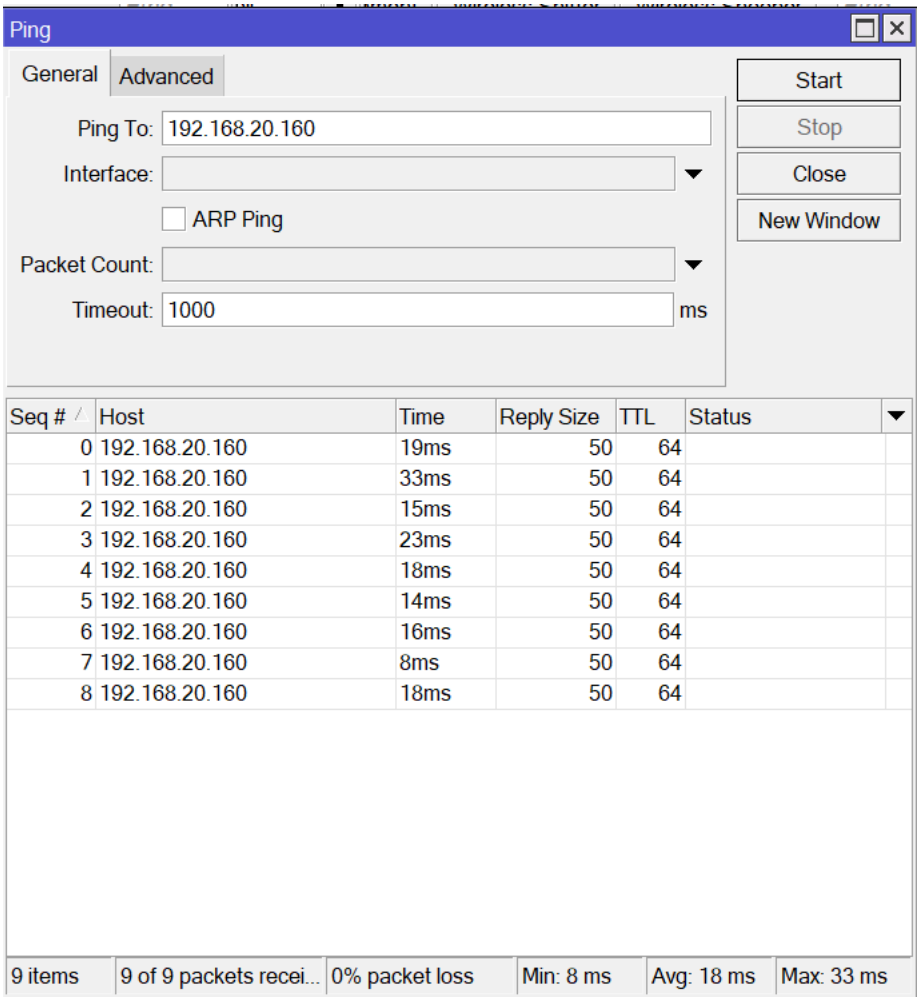
Η/Υ τμήματος IT : 192.168.40.150

Στις παρακάτω εικόνες μπορεί να δει κανείς πως όλες οι συσκευές έχουν επικοινωνία με τον κεντρικό δρομολογητή, επομένως το δίκτυο είναι έτοιμο. Πιο συγκεκριμένα στην εικόνα 12 αυτή φαίνεται η επιτυχής επικοινωνία μεταξύ του κεντρικού δρομολογητή και του Η/Υ του Λογιστηρίου με IP Address : 192.168.20.150



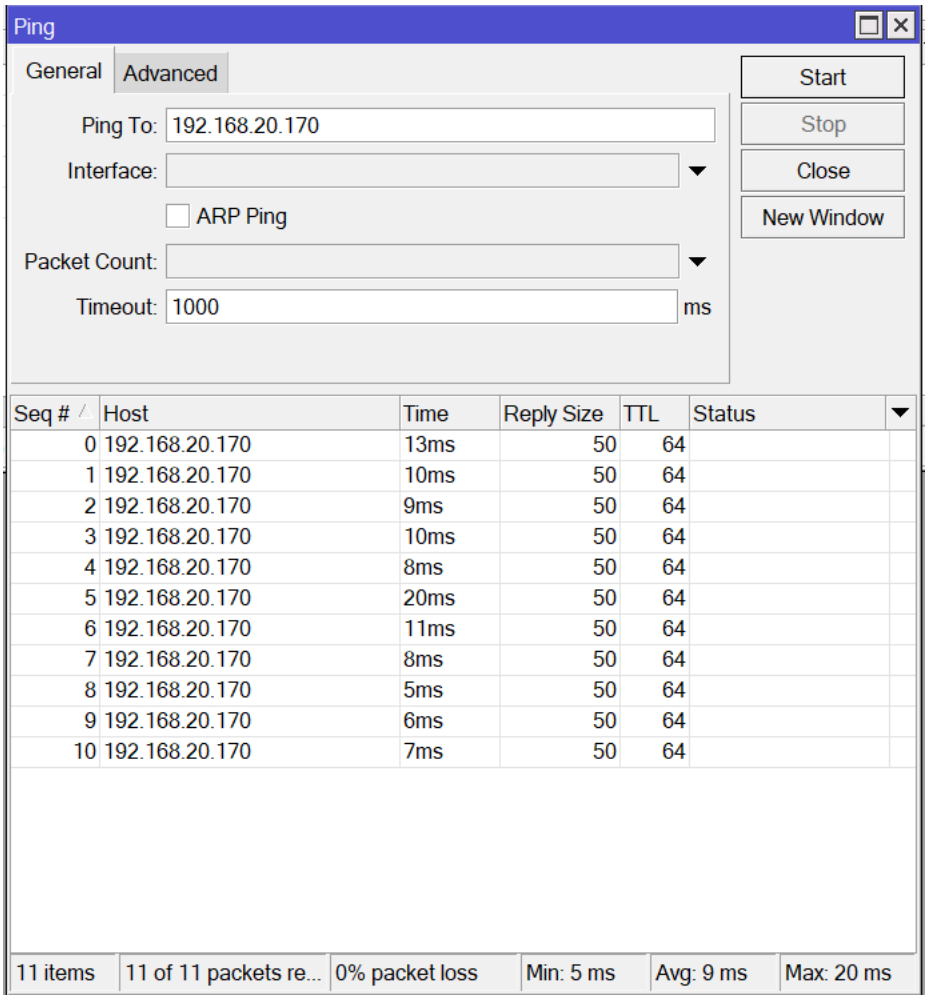
Εικόνα 12 Ping στον Η/Υ του Λογιστηρίου

Στην εικόνα 13 αυτή φαίνεται η επιτυχής επικοινωνία μεταξύ του κεντρικού δρομολογητή και του Η/Υ του Management με IP Address : 192.168.20.160



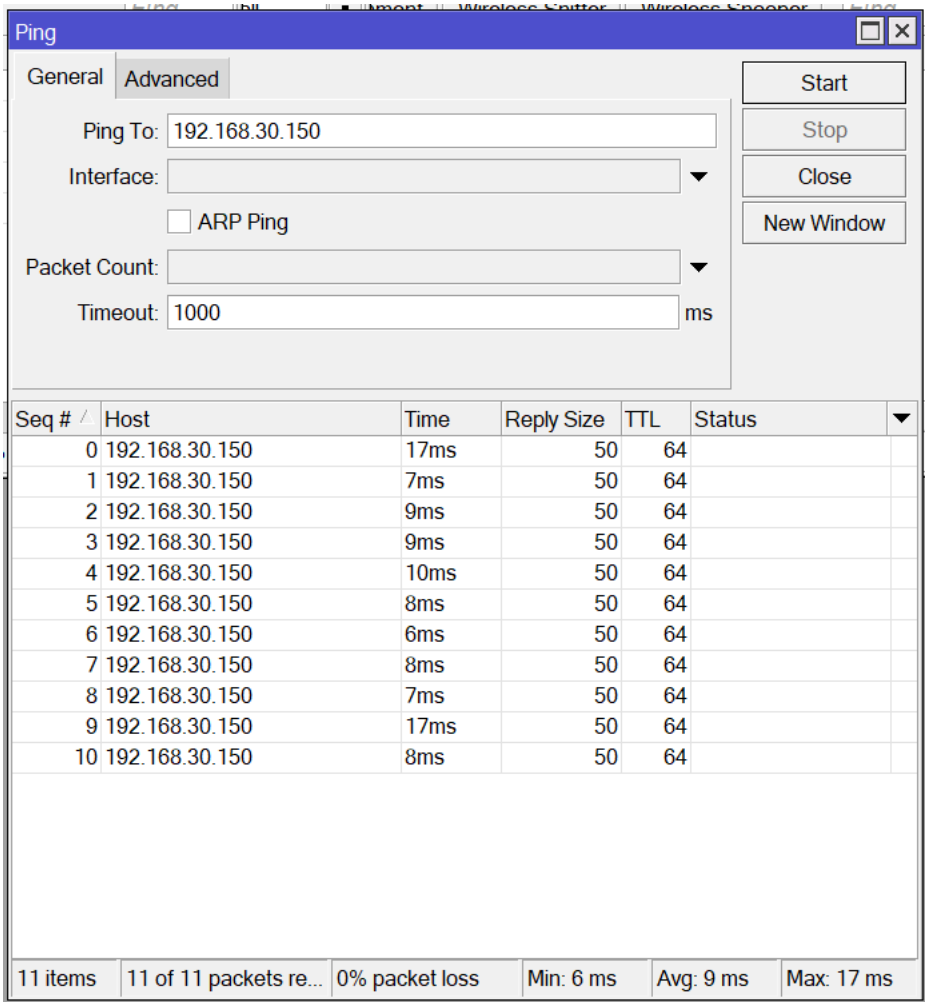
Εικόνα 13Ping στον Η/Υ του Management

Στην εικόνα 14 αυτή φαίνεται η επιτυχής επικοινωνία μεταξύ του κεντρικού δρομολογητή και του Η/Υ του Administration με IP Address : 192.168.20.170



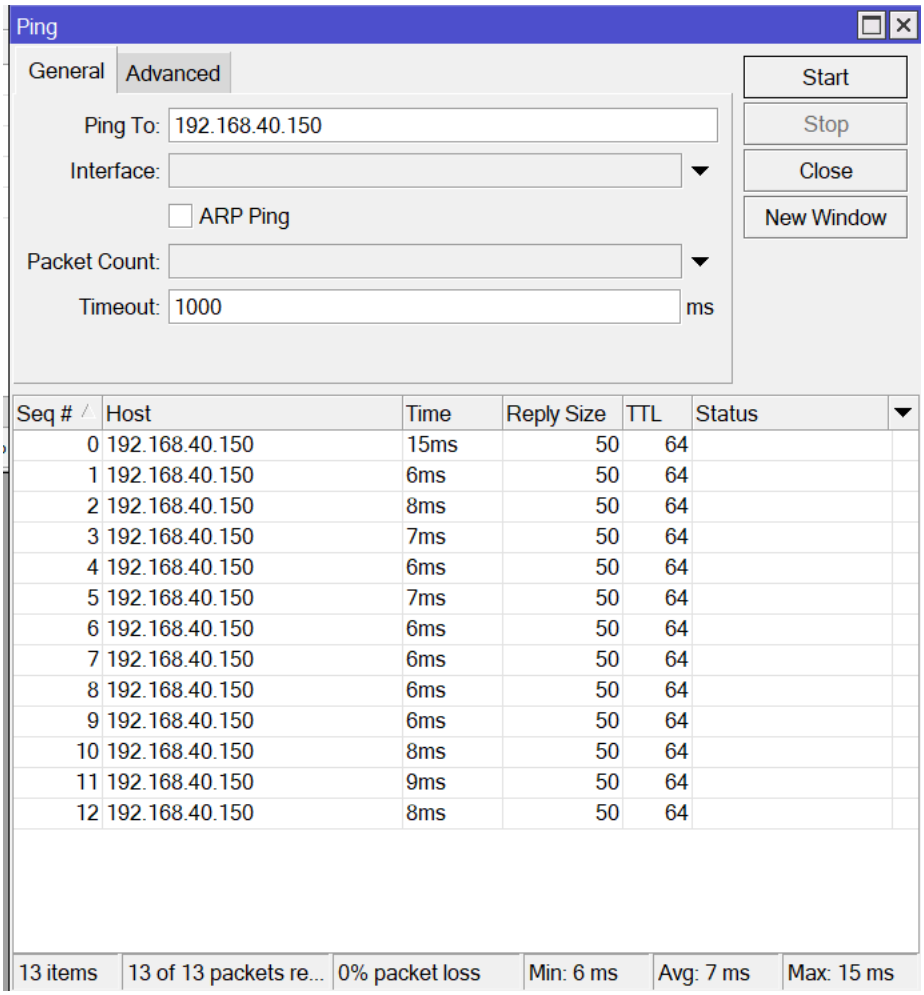
Εικόνα 14 Ping στον Η/Υ της Διαχείρισης

Στην εικόνα 15 αυτή φαίνεται η επιτυχής επικοινωνία μεταξύ του κεντρικού δρομολογητή και του Η/Υ του Marketing με IP Address : 192.168.30.150



Εικόνα 15 Ping στον Η/Υ του Marketing

Στην εικόνα 16 αυτή φαίνεται η επιτυχής επικοινωνία μεταξύ του κεντρικού δρομολογητή και του Η/Υ του IT με IP Address : 192.168.40.150



Εικόνα 16 Ping στον Η/Υ του IT

5.3 Απαραίτητες παραμετροποιήσεις για την επίτευξη της ασφάλειας στο εταιρικό δίκτυο.

5.3.1 Βασικές παραμετροποιήσεις στις διάφορες συσκευές του δικτύου της εταιρίας :

1)Κεντρικός δρομολογητής – Main Router

Παρακάτω φαίνεται ο κώδικας ο οποίος χρησιμοποιήθηκε για την παραμετροποίηση του κεντρικού δρομολογητή . Πιο συγκεκριμένα φαίνεται η δημιουργία των VLAN, τα υποδίκτυα που δημιουργήθηκαν για το κάθε ένα VLAN καθώς φαίνεται και η ενεργοποίηση του DHCP Server σε όλα τα απαραίτητα interface του δρομολογητή. Επίσης

μπορεί κανείς να δει πως έχει χρησιμοποιηθεί και η μέθοδος της γεφύρωσης (Bridge) με σκοπό τον διαμοιρασμό των VLan. Τέλος έχει ενεργοποιηθεί και ο dhcp client στο ethernet port1 έτσι ώστε το δίκτυο να έχει πρόσβαση στο διαδίκτυο.

```
/interface bridge

add frame-types=admit-only-vlan-tagged name=BridgeMain vlan-filtering=yes

/interface vlan

add interface=BridgeMain name=VLanAccounting20 vlan-id=20

add interface=BridgeMain name=VLanAdmin26 vlan-id=26

add interface=BridgeMain name=VLanIT40 vlan-id=40

add interface=BridgeMain name=VLanMarketing30 vlan-id=30

/interface wireless security-profiles

set [ find default=yes ] supplicant-identity=MikroTik

/ip pool

add name=dhcp_pool0 ranges=192.168.20.10-192.168.20.253

add name=dhcp_pool1 ranges=192.168.40.10-192.168.40.253

add name=dhcp_pool2 ranges=192.168.30.10-192.168.30.253

add name=dhcp_pool3 ranges=192.168.50.10-192.168.50.253

add name=dhcp_pool4 ranges=192.168.26.10-192.168.26.253

/ip dhcp-server

add address-pool=dhcp_pool0 disabled=no interface=VLanAccounting20 \

    lease-time=3h name=dhcp1

add address-pool=dhcp_pool1 disabled=no interface=VLanIT40 lease-time=3h \
```

```
    name=dhcp2
add address-pool=dhcp_pool2 disabled=no interface=VLanMarketing30 lease-time=\
    3h name=dhcp3
add address-pool=dhcp_pool3 interface=VLanWifi50 lease-time=3h name=dhcp4
add address-pool=dhcp_pool4 disabled=no interface=VLanAdmin26 lease-time=3h \
    name=dhcp5
/interface bridge port
add bridge=BridgeMain frame-types=admit-only-vlan-tagged interface=ether9
add bridge=BridgeMain frame-types=admit-only-vlan-tagged interface=ether10
add bridge=BridgeMain interface=ether2
/interface bridge vlan
add bridge=BridgeMain tagged=ether9,ether10,BridgeMain vlan-ids=20,30,40,50
add bridge=BridgeMain tagged=ether9,ether10,BridgeMain vlan-ids=26
/ip address
add address=192.168.20.254/24 interface=VLanAccounting20 network=192.168.20.0
add address=192.168.30.254/24 interface=VLanMarketing30 network=192.168.30.0
add address=192.168.40.254/24 interface=VLanIT40 network=192.168.40.0
add address=192.168.50.254/24 interface=VLanWifi50 network=192.168.50.0
add address=192.168.26.254/24 interface=VLanAdmin26 network=192.168.26.0
/ip dhcp-client
add disabled=no interface=ether1
```

```
/ip dhcp-server lease
add address=192.168.26.253 client-id=1:c:19:33:31:0:0 mac-address=\
    0C:19:33:31:00:00 server=dhcp5
add address=192.168.26.251 client-id=1:c:e4:2c:93:0:1 mac-address=\
    0C:E4:2C:93:00:01 server=dhcp5
add address=192.168.26.252 client-id=1:c:a6:d8:42:0:0 mac-address=\
    0C:A6:D8:42:00:00 server=dhcp5
add address=192.168.26.250 client-id=1:c:ab:1a:c7:0:5 mac-address=\
    0C:AB:1A:C7:00:05 server=dhcp5
add address=192.168.26.248 client-id=1:c:ab:1a:c7:0:1 mac-address=\
    0C:AB:1A:C7:00:01 server=dhcp5
/ip dhcp-server network
add address=192.168.20.0/24 dns-server=8.8.8.8 gateway=192.168.20.254
add address=192.168.26.0/24 dns-server=8.8.8.8 gateway=192.168.26.254
add address=192.168.30.0/24 dns-server=8.8.8.8 gateway=192.168.30.254
add address=192.168.40.0/24 dns-server=8.8.8.8 gateway=192.168.40.254
add address=192.168.50.0/24 dns-server=8.8.8.8 gateway=192.168.50.254
/port remote-access
add
/system identity
set name=MainRouter
```

2)Κεντρικό Switch - Main Switch

Παρακάτω παρατίθεται αναλυτικά ο κώδικας ο οποίος χρησιμοποιήθηκε για την παραμετροποίηση του κεντρικού Switch που υπάρχει στο εταιρικό δίκτυο που μελετάτε στην συγκεκριμένη πτυχιακή εργασία. Πιο συγκεκριμένα μπορεί κανείς να παρατηρήσει ότι αρχικά φαίνονται σε ποια interface ports έχουν πραγματοποιηθεί οι φυσικές συνδέσεις με τις υπόλοιπες συσκευές που υπάρχουν στο δίκτυο. Ωστόσο στην συνέχεια φαίνονται τα VLAN μαζί με τα υποδίκτυα τους αλλά και σε ποια ethernet ports βρίσκεται το καθένα.

```
/interface bridge

add name=BridgeMain vlan-filtering=yes

/interface ethernet

set [ find default-name=ether1 ] comment=ConnectionWithMainRouter

set [ find default-name=ether5 ] comment=SwitchGroundFloor

set [ find default-name=ether6 ] comment=SwitchFirstFloor

set [ find default-name=ether7 ] comment=SwitchSecondFloor

/interface vlan

add interface=BridgeMain name=VLanAdmin26 vlan-id=26

/interface wireless security-profiles

set [ find default=yes ] supplicant-identity=MikroTik

/interface bridge port

add bridge=BridgeMain frame-types=admit-only-vlan-tagged interface=ether1

add bridge=BridgeMain frame-types=admit-only-vlan-tagged interface=ether8

add bridge=BridgeMain frame-types=admit-only-vlan-tagged interface=ether6
```

```
add bridge=BridgeMain frame-types=admit-only-vlan-tagged interface=ether7

/interface bridge vlan

add bridge=BridgeMain tagged=ether1,ether8,ether6,ether7 vlan-ids=20,30,40,50

add bridge=BridgeMain tagged=ether1,ether8,ether6,ether7,BridgeMain vlan-ids=\

   26

/ip dhcp-client

add disabled=no interface=VLanAdmin26

/system identity

set name=SwitchMain
```

3)Switch Ισόγειου- Switch Ground Floor

Στο συγκεκριμένο Switch η υλοποίηση είναι ίδια ακριβώς όπως και στα Switches των επόμενων δύο ορόφων (Πρώτος και Δεύτερος όροφος). Το μόνο που αλλάζει κάθε φορά είναι το όνομα που δίνεται στο κάθε Switch και αυτό πραγματοποιείται μόνο και μόνο για να διαχωρίζονται οι συσκευές στον χώρο του διαχειριστή. Αρχικά, καλό είναι να αναφερθεί πως στα τρία αυτά Switch τροποποιήθηκαν τα ονόματα των ethernet ports για λόγους κατανόησης διότι στο περιβάλλον προσομοίωσης ήταν με διαφορετική σειρά. Στην συνέχεια φαίνεται πως διαμοιράζονται τα VLAN διότι έχουμε επιλέξει σε ποιες θύρες θα είναι το κάθε ένα σύμφωνα με τις ανάγκες της εταιρίας.

```
/interface bridge

add frame-types=admit-only-vlan-tagged name=BridgeMain vlan-filtering=yes

/interface ethernet

set [ find default-name=ether1 ] name=ether0
```

```
set [ find default-name=ether2 ] name=ether1
set [ find default-name=ether3 ] name=ether2
set [ find default-name=ether4 ] name=ether3
#set [ find default-name=ether5 ] name=ether4
set [ find default-name=ether6 ] name=ether5
set [ find default-name=ether7 ] name=ether6
set [ find default-name=ether8 ] name=ether7
set [ find default-name=ether9 ] name=ether8
set [ find default-name=ether10 ] name=ether9
set [ find default-name=ether11 ] name=ether10
set [ find default-name=ether12 ] name=ether11
set [ find default-name=ether13 ] name=ether12
set [ find default-name=ether14 ] name=ether13
/interface vlan
add interface=BridgeMain name=VLanAdmin26 vlan-id=26
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=BridgeMain interface=ether7 pvid=20
add bridge=BridgeMain interface=ether9 pvid=20
add bridge=BridgeMain interface=ether8 pvid=20
```

```
add bridge=BridgeMain interface=ether10 pvid=20

add bridge=BridgeMain interface=ether11 pvid=30

add bridge=BridgeMain interface=ether12 pvid=30

add bridge=BridgeMain frame-types=admit-only-vlan-tagged interface=ether1

add bridge=BridgeMain interface=ether13 pvid=40

add bridge=BridgeMain interface=ether14 pvid=40

/interface bridge vlan

add bridge=BridgeMain tagged=ether1,BridgeMain vlan-ids=26

add bridge=BridgeMain tagged=ether1 untagged=ether7,ether8,ether9,ether10 \

    vlan-ids=20

add bridge=BridgeMain tagged=ether1 untagged=ether11,ether12 vlan-ids=30

add bridge=BridgeMain tagged=ether1 untagged=ether14,ether13 vlan-ids=40

add bridge=BridgeMain tagged=ether1 untagged=ether0 vlan-ids=50

/ip dhcp-client

add disabled=no interface=vlan26

/system identity

set name=Switch_Ground_Floor
```

4)Switch – Switch First Floor

Στο συγκεκριμένο Switch όπως αναφέρθηκε και παραπάνω η διαδικασία παραμετροποίησης του είναι ίδια με αυτή που χρησιμοποιήθηκε στο Switch του ισογείου.

Η μόνη αλλαγή που έχει γίνει στον κώδικα είναι στο πεδίο που ορίζεται το όνομα του Switch το οποίο στην περίπτωση αυτή είναι του πρώτου ορόφου.(Switch_First_Floor).

```
/interface bridge

add frame-types=admit-only-vlan-tagged name=BridgeMain vlan-filtering=yes

/interface ethernet

set [ find default-name=ether1 ] name=ether0

set [ find default-name=ether2 ] name=ether1

set [ find default-name=ether3 ] name=ether2

set [ find default-name=ether4 ] name=ether3

/interface vlan

add interface=BridgeMain name=VLanAdmin26 vlan-id=26

/interface wireless security-profiles

set [ find default=yes ] supplicant-identity=MikroTik

/interface bridge port

add bridge=BridgeMain interface=ether7 pvid=20

add bridge=BridgeMain interface=ether9 pvid=20

add bridge=BridgeMain interface=ether8 pvid=20

add bridge=BridgeMain interface=ether10 pvid=20

add bridge=BridgeMain interface=ether11 pvid=30

add bridge=BridgeMain interface=ether12 pvid=30

add bridge=BridgeMain frame-types=admit-only-vlan-tagged interface=ether1

add bridge=BridgeMain interface=ether13 pvid=40
```

```
add bridge=BridgeMain interface=ether14 pvid=40

/interface bridge vlan

add bridge=BridgeMain tagged=ether1,BridgeMain vlan-ids=26

add bridge=BridgeMain tagged=ether1 untagged=ether7,ether8,ether9,ether10 \

    vlan-ids=20

add bridge=BridgeMain tagged=ether1 untagged=ether11,ether12 vlan-ids=30

add bridge=BridgeMain tagged=ether1 untagged=ether14,ether13 vlan-ids=40

add bridge=BridgeMain tagged=ether1 untagged=ether0 vlan-ids=50

/ip dhcp-client

add disabled=no interface=VLanAdmin26

/system identity

set name=Switch_First_Floor
```

5)Switch Δεύτερου ορόφου- Switch Second Floor

Στο συγκεκριμένο Switch όπως αναφέρθηκε και παραπάνω η διαδικασία παραμετροποίησης του είναι ίδια με αυτή που χρησιμοποιήθηκε στο Switch του ισογείου και του πρώτου ορόφου. Όπως αναφέρθηκε και στην περιγραφή του προηγούμενου Switch το μόνο που αλλάζει στον κώδικα είναι το όνομα του Switch.

```
/interface bridge

add frame-types=admit-only-vlan-tagged name=BridgeMain vlan-filtering=yes

/interface ethernet

set [ find default-name=ether1 ] name=ether0

set [ find default-name=ether2 ] name=ether1

set [ find default-name=ether3 ] name=ether2
```

```
set [ find default-name=ether4 ] name=ether3
set [ find default-name=ether15 ] name=ether4
/interface vlan
add interface=BridgeMain name=VLanAdmin26 vlan-id=26
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=BridgeMain interface=ether7 pvid=20
add bridge=BridgeMain interface=ether9 pvid=20
add bridge=BridgeMain interface=ether8 pvid=20
add bridge=BridgeMain interface=ether10 pvid=20
add bridge=BridgeMain interface=ether11 pvid=30
add bridge=BridgeMain interface=ether12 pvid=30
add bridge=BridgeMain frame-types=admit-only-vlan-tagged interface=ether1
add bridge=BridgeMain frame-types=admit-only-untagged-and-priority-tagged \
    interface=ether13 pvid=40
add bridge=BridgeMain frame-types=admit-only-untagged-and-priority-tagged \
    interface=ether14 pvid=40
/interface bridge vlan
add bridge=BridgeMain tagged=ether1,BridgeMain vlan-ids=26
add bridge=BridgeMain tagged=ether1 untagged=ether7,ether8,ether9,ether10 \
```

```
    vlan-ids=20
add bridge=BridgeMain tagged=ether1 untagged=ether11,ether12 vlan-ids=30
add bridge=BridgeMain tagged=ether1,BridgeMain untagged=ether14,ether13 \
    vlan-ids=40
add bridge=BridgeMain tagged=ether1 untagged=ether0 vlan-ids=50
/ip dhcp-client
add interface=VLanAdmin26
add disabled=no
/system identity
set name=Switch_Second_Floor
```

5.3.2 Κανόνες παραμετροποίησης του Firewall για την βέλτιστη ασφάλεια του εταιρικού δικτύου .

Στο συγκεκριμένο υποκεφάλαιο θα παρατεθεί αναλυτικά ο κώδικας ο οποίος χρησιμοποιήθηκε για να δημιουργηθούν οι απαραίτητοι κανόνες για την ύπαρξη του Firewall στο εταιρικό δίκτυο το οποίο μελετάτε στην πτυχιακή αυτή εργασία. Πιο συγκεκριμένα οι κανόνες αυτοί παραμετροποιήθηκαν στον κεντρικό δρομολογητή της εταιρίας καθώς εκεί γίνεται η είσοδος και η έξοδος των πακέτων από και προς το Internet. Όπως φαίνεται και στο παρακάτω κομμάτι κώδικα έχουν δημιουργηθεί κανόνες για τα forward αλλά και τα input πακέτα. Πιο συγκεκριμένα στην αρχή ξεκινάει ο κανόνας με το πρωτόκολλο icmp ο οποίος δημιουργήθηκε για να μπορεί ο διαχειριστής να κάνει ping και να βρίσκει τον δρομολογητή. Στην συνέχεια γίνεται drop οποιοδήποτε πακέτο εισέρχεται στον δρομολογητή. Έπειτα επιτρέπεται στον δρομολογητή να δέχεται πακέτα τα οποία έρχονται από συγκεκριμένη διεύθυνση η οποία ανήκει σε ένα pool διευθύνσεων που ονομάζεται ασφαλές διευθύνσεις (SafeAddresses). Η διαδικασία αυτή πραγματοποιείται τόσο για τα forward όσο και για τα input πακέτα. Αξίζει να σημειωθεί πως δημιουργήθηκε ένας κανόνας για τις νέες συνδέσεις οι οποίες θα γίνονται δεκτές μόνο εφόσον ανήκουν

στις ασφαλές διευθύνσεις και όλες οι υπόλοιπες δεν θα γίνονται δεκτές. Όλοι αυτοί οι κανόνες που περιεγράφηκαν βρίσκονται στον παρακάτω κώδικα :

```
/ip firewall address-list
add address=192.168.26.0/24 list=SafeAddresses
/ip firewall filter
add action=accept chain=input protocol=icmp
add action=drop chain=forward connection-state=invalid connection-type="" \
    src-address-list=""
add action=drop chain=input connection-state=invalid
add action=accept chain=input connection-state=new src-address-list=\
    SafeAddresses
add action=accept chain=input connection-state=established
add action=drop chain=input
add action=accept chain=forward connection-state=new connection-type="" \
    src-address-list=SafeAddresses
add action=accept chain=forward connection-state=established,related
add action=drop chain=forward
/ip firewall nat
add action=masquerade chain=srcnat
```

6. Συμπεράσματα

Ολοκληρώνοντας την μελέτη για την παραπάνω πτυχιακή εργασία αξίζει να σημειωθεί πως έγινε αντιληπτό το πόσο δύσκολο είναι στην σημερινή εποχή να καταφέρει κανείς να έχει ένα ασφαλές δίκτυο. Όσο η τεχνολογία και η επιστήμη της Πληροφορικής εξελίσσεται τόσο όλο ένα και περισσότεροι κίνδυνοι και απειλές θα δημιουργούνται. Παρόλα αυτά ένα καλό θεωρητικό υπόβαθρο θα είναι πολύ χρήσιμο για όποιον επιθυμεί να ασχοληθεί με αυτόν τον κλάδο. Στην λογική αυτή βασίζεται και η συγκεκριμένη πτυχιακή εργασία αφού μεγάλο μέρος της αποτελείται από σημαντικά κομμάτια θεωρίας των δικτύων που είναι απαραίτητα να τα γνωρίζει όποιος θέλει να αναπτυχθεί στον τομέα

αυτό. Στο εμπόριο θα βρει κανείς διάφορες εταιρίες λογισμικού για την υλοποίηση δικτύων, ωστόσο για την παραπάνω μελέτη επιλέχθηκε η εταιρία Mikrotik διότι είναι πολύ εύκολο το λογισμικό στην χρήση του αλλά και γιατί σου δίνει την δυνατότητα να ασφαλίσει κανείς σε πολύ καλά το δίκτυο που θα δημιουργήσει. Είναι γεγονός πως η μελέτη για την ασφάλεια των δεδομένων σε ένα δίκτυο είναι ένα δύσκολο αντικείμενο αλλά όχι ακατόρθωτο. Ο πιο διαδεδομένος τρόπος στην σημερινή εποχή για την ασφάλεια ενός δικτύου είναι η τεχνική του Firewall ωστόσο υπάρχουν και άλλες τεχνικές υλοποίησης μία από αυτές είναι η διαχώριση του κυρίως δικτύου σε υποδίκτυα με την τεχνική των VLAN. Η συγκεκριμένη τεχνική χρησιμοποιήθηκε στην μελέτη της πτυχιακής αυτής και θεωρείται πολύ σημαντική για μεγάλα δίκτυα όπως για παράδειγμα είναι το δίκτυο μιας εταιρίας. Καταληκτικά, η σημασία της Ασφάλειας σε ένα εταιρικό δίκτυο είναι πολύ μεγάλη διότι η Ασφάλεια είναι απαραίτητη για την προστασία των δεδομένων και των πληροφοριών που μεταφέρονται στο κάθε δίκτυο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Πουλημένος, Γ. (2019). Πρωτόκολλα ελέγχου ροής στο επίπεδο σύνδεσης δεδομένων.
2. Μαργαρίτη Σ.,Στεργίου Ε (2006), " Τοπικά και αστικά δίκτυα (LAN-MAN),εκδόσεις ΝΕΩΝ ΤΕΧΝΟΛΟΓΙΩΝ .
3. Μάριος Μπερέτας, "Πτυχιακή εργασία για την μελέτη και ανάπτυξη τοπολογιών ασύρματων δικτύων με συσκευές Mikrotik"[online]. Available: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/10902/Beretis_Marios.pdf?sequence=1&isAllowed=y
4. Μαυρίδης, Ι. (2016). Ασφάλεια πληροφοριών στο διαδίκτυο.
5. Βενιέρης, Ι. (2013). Δίκτυα Ευρείας Ζώνης: Τεχνολογίες και Εφαρμογές με Έμφαση στο Διαδίκτυο.
6. Κιτσικίδης, Σ. Ανάπτυξη εκπαιδευτικού λογισμικού για δίκτυα υπολογιστών.
7. Καψάλης, Β. (1995). ΣΧΕΔΙΑΣΗ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΥΒΡΙΔΙΚΟΥ ΠΡΩΤΟΚΟΛΛΟΥ ΠΡΟΣΠΕΛΑΣΗΣ ΓΙΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ΠΡΑΓΜΑΤΙΚΟΥ ΧΡΟΝΟΥ (Doctoral dissertation, Πανεπιστήμιο Πατρών. Σχολή Πολυτεχνική. Τμήμα Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών).
8. 2022. [online] Available at: <https://help.mikrotik.com/docs/display/ROS/VLAN> [Accessed 7 September 2022].
9. Discher, S., 2011. *RouterOS by example*. College Station, Texas: MicroTik.
10. 2022. [online] Available at: <https://www.gns3.com/software/download-vm> [Accessed 7 September 2022].
11. VMware. 2022. *Download VMware Workstation Pro*. [online] Available at: <https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html> [Accessed 7 September 2022].
12. Mikrotik.com. 2022. *MikroTik*. [online] Available at: <https://mikrotik.com/download> [Accessed 7 September 2022].
13. Αρβανιτάκης, Ι. (2017). *Ποιότητα υπηρεσιών και ασφάλεια σε τοπικά δίκτυα υπολογιστών (local access networks)* (Master's thesis, Πανεπιστήμιο Πειραιώς).

[Οπισθόφυλλο. Κενή σελίδα]