ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Αυτοματοποίηση συμπεριφοράς για αντιμετώπιση επιθέσεων και σενάρια ασφαλούς κίνησης σε σύγχρονα δίκτυα υπολογιστών.

ΚΑΡΑΡΡΗΓΑΣ ΙΩΑΝΝΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Δρ. Γιώργος Γιάννακας
Επιστημονικός Συνεργάτης Τμήματος Πληροφορικής και Τηλεπικοινωνιών

ΣΥΝΕΠΙΒΛΕΠΩΝ

Ξενάκης Απόστολος
Επίκουρος καθηγητής του Τμήματος Ψηφιακών Συστημάτων

Λαμία 14 Ιουλίου έτος 2022

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

Behavior automation for dealing with attacks and secure traffic scenarios on modern computer networks.

KARARRIGAS JOHN

FINAL THESIS

ADVISOR

Dr. George Giannakas
Scientific Department Associate of Information Technology and Telecommunications

CO ADVISOR

Xenakis Apostolos
Assistant professor of the Department of Digital Systems

Lamia 14 July year 2022

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 14/07/2022

Ο Δηλ.
Καραρρήγας Γιάννης

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΠΕΡΙΛΗΨΗ

Η πτυχιακή εργασία αποτελείται από έξι κεφάλαια. Το πρώτο κεφάλαιο αφορά κάποια βασικά στοιχεία στα δίκτυα υπολογιστών και γίνεται μια ανασκόπηση πρωτοκόλλων , αλγορίθμων και τεχνολογιών. Το δεύτερο κεφάλαιο παρουσιάζει μια αρχική προσέγγιση ενός δικτύου , αναφέρει τεχνολογίες και πρωτόκολλα που αυτό χρησιμοποιεί. Στο τρίτο κεφάλαιο παρουσιάζονται οι αλλαγές που το δίκτυο χρειάζεται και παρουσιάζεται το νέο βελτιωμένο δίκτυο. Στο τέταρτο κεφάλαιο αναλύεται το κομμάτι της ασφάλειας και των επιθέσεων . Στο πέμπτο κεφάλαιο αυτοματοποιούμε το δίκτυο και κάποιες λειτουργίες χρησιμοποιώντας τη γλώσσα προγραμματισμού python κυρίως για ζητήματα ασφάλειας αλλά και χρόνου ρύθμισης συσκευών. Τέλος το κεφάλαιο έξι αναφέρει συμπεράσματα και μελλοντικές επεκτάσεις τη πτυχιακής . Στο πρακτικό κομμάτι των κεφαλαίων γίνεται χρήση του GNS3 και του KALI LINUX, για την κατασκευή και κατανόηση του δικτύου καθώς και των επιθέσεων.

Λέξεις κλειδιά: GNS3,Kali Linux, OSPF, DMZ, Τείχος Προστασίας, Python, Αυτοματισμός ,VirtualBox,Windows10, Pycharm, Ασφάλεια, Επιθέσεις,SQL

ABSTRACT

This Thesis consists of six chapters. The first chapter deals with some basic elements in computer networks and provides an overview of protocols, algorithms and technologies. The second chapter presents an initial approach of a network, mentions technologies and protocols that it uses. The third chapter presents the changes that the network needs and presents the new improved network. The fourth chapter analyzes the part of security and attacks. In the fifth chapter we automate the network and some functions using the python programming language mainly for security issues but also device setup time. Finally, chapter six mentions conclusions and future extensions of the thesis. In the practical part of the chapters, GNS3 and KALI LINUX are used, for the construction and understanding of the network as well as the attacks.

Keywords: GNS3, Kali Linux, OSPF, DMZ, Firewall, Python, Automation, VirtualBox, Windows10, Pycharm, Security, Attacks, SQL.

Πίνακας αρκτικόλεξων και βραχυγραφιών

LAN	Local Area Network
MAN	Metropolitan Area Network
WAN	Wide Area Network
OSI	Open Systems Interconnection
MAC	Media Access Control
Ipv4	Internet Protocol Version 4
Ipv6	Internet Protocol Version 6
ICMP	Internet Control Message Protocol
LLC	Logical Link Control
IPsec	Internet Protocol Security
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
TFTP	Trivial File Transfer Protocol
HTTP	Hypertext Transfer Protocol
NTP	Network Time Protocol
SMTP	Simple Mail Transfer Protocol
DHCP	Dynamic Host Configuration Protocol
ARP	Address Resolution Protocol
NIC	Network Interface Controller
VLSM	Variable Length Subnet Mask
FLSM	Fixed Length Subnet Mask
ISP	Internet Service Provider
NAT	Network Address Translation
OSPF	Open Shortest Path First
LSDB	Link State Database
Gbps	Gigabit Per Second
VLAN	Virtual Local Area Network
SVI	Switch Virtual Interface
LACP	Link Aggregation Control Protocol
Pagp	Port Aggregation Protocol
PAT	Port Address Translation
VPN	Virtual Private Network
MITM	Man In the Middle
SQL	Structured Query Language
DoS	Denial of Service

DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
ACL	Access Control List
BGP	Border Gateway Protocol
HSRP	Hot Standby Router Protocol
STP	Spanning Tree Protocol

Κατάλογος εικόνων

Περιεχόμενα

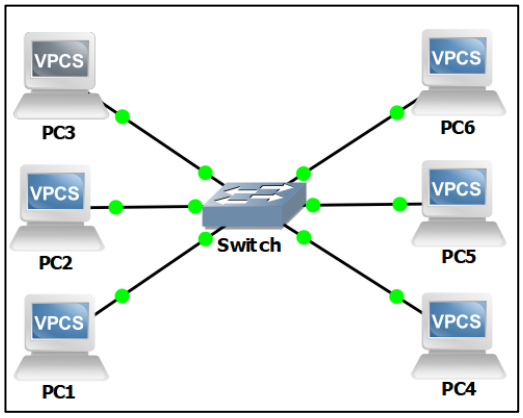
ΚΕΦΑΛΑΙΟ 1 : Τεχνολογίες και Σχεδίαση Τοπικών Δικτύων

1.1 Εισαγωγή στα δίκτυα υπολογιστών

Το δίκτυο υπολογιστών είναι ένα τηλεπικοινωνιακό σύστημα από αυτόνομους ή μη αυτόνομους διασυνδεδεμένους υπολογιστές καθώς και διάφορες δικτυακές συσκευές όπως δρομολογητές και μεταγωγείς που θα δούμε στη συνέχεια. Τα δίκτυα υπολογιστών ταξινομούνται ανάλογα με κάποια χαρακτηριστικά όπως το φυσικό μέσο διασύνδεσης το οποίο τα διαχωρίζει σε ενσύρματα και ασύρματα, τον τρόπο πρόσβασης, με τον οποίο διαχωρίζονται σε δημόσια και ιδιωτικά και τέλος ανάλογα με τη γεωγραφική τους κάλυψη σε τοπικά, μητροπολιτικά και ευρείας κάλυψης.

1.1.1 Τοπικά Δίκτυα LAN

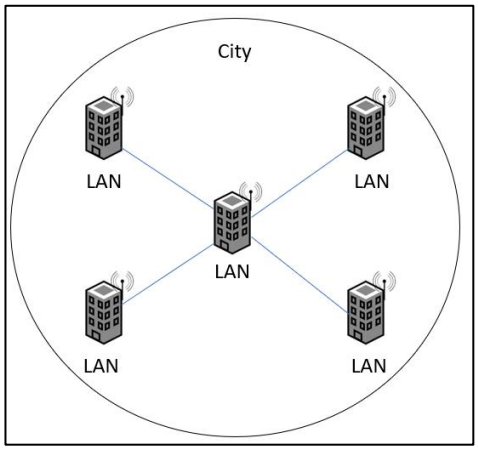
Τα τοπικά δίκτυα ή και LAN είναι δίκτυα που συνδέουν υπολογιστές σε περιορισμένο γεωγραφικό χώρο, για παράδειγμα από υπολογιστές που βρίσκονται σε ένα κτίριο μέχρι υπολογιστές που απέχουν μερικά χιλιόμετρα μεταξύ τους. Χρησιμοποιούνται συνήθως για τη σύνδεση προσωπικών υπολογιστών και σταθμών εργασίας σε εταιρικά γραφεία, εργοστάσια, πανεπιστήμια και άλλες εγκαταστάσεις. Τα τοπικά δίκτυα είναι εγκατεστημένα μέσα στο χώρο που καταλαμβάνει το τμήμα μιας εταιρίας, δηλαδή μερικοί σταθμοί κατανεμημένοι στα γραφεία μερικών ορόφων. Βασικός σκοπός είναι η επικοινωνία διαφόρων υπολογιστικών συστημάτων όπως για παράδειγμα το δίκτυο Ethernet. Στα επόμενα κεφάλαια θα παρουσιάσουμε τις τεχνολογίες ενός τοπικού δικτύου μιας εταιρείας.



Εικόνα 1.1 LAN

1.1.2 Μητροπολιτικά Δίκτυα MAN

Ένα Δίκτυο Μητροπολιτικής Περιοχής ή MAN είναι μια μεγαλύτερη έκδοση ενός τοπικού δικτύου επειδή καλύπτει μεγαλύτερες αποστάσεις, όπως μια ομάδα γειτονικών γραφείων σε μια εταιρεία ακόμα και σε μια πόλη.



Εικόνα 1.1 MAN

1.1.3 Ευρείας περιοχής WAN

Ένα Δίκτυο ευρείας περιοχής ή WAN καλύπτει μια μεγάλη γεωγραφική περιοχή, όπως τη σύνδεση διαφορετικών πόλεων ή ολόκληρων ηπείρων, και μπορεί ακόμη και να συνδέσει πολλά τοπικά δίκτυα και ομάδες τοπικών δικτύων. Τα περισσότερα ευρυζωνικά δίκτυα χρησιμοποιούν το τηλεφωνικό δίκτυο ή τους τηλεπικοινωνιακούς δορυφόρους.

1.2 Δικτυακές Συσκευές

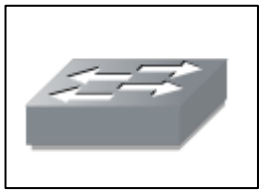
Μέσα σε μια δικτυακή τοπολογία θα συναντήσουμε αρκετές συσκευές όπως δρομολογητές, μεταγωγείς και τείχη προστασίας, καθώς και τερματικές συσκευές όπως υπολογιστές και διακομιστές.

1.2.1 Router-Δρομολογητής

Εικόνα 1.3 Δρομολογητής σε GNS3

Είναι μια ηλεκτρονική συσκευή η οποία αναλαμβάνει την αποστολή και λήψη πακέτων δεδομένων μεταξύ ενός ή περισσοτέρων διακομιστών, άλλων δρομολογητών και πελατών, κατά μήκος πολλαπλών δικτύων. Η δρομολόγηση, δηλαδή η διαδικασία μεταφοράς δεδομένων από ένα σημείο σε ένα άλλο αποτελεί κεντρική λειτουργία του επιπέδου δικτύου, γίνεται με βάση διάφορα κριτήρια και τελικώς επιλέγεται μία ανάμεσα σε διάφορες πιθανές διαδρομές. Οι δρομολογητές ανήκουν στο επίπεδο 3 (layer 3) του μοντέλου OSI το επίπεδο δικτύου.

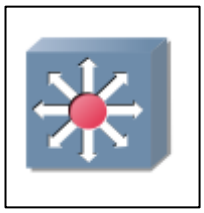
1.2.2 Switch-Μεταγωγέας



Εικόνα 1.4 Μεταγωγέας σε GNS3

Ο μεταγωγέας είναι μια ηλεκτρονική συσκευή που χρησιμοποιείται σε δίκτυα υπολογιστών. Ένας μεταγωγέας Ethernet είναι μια γέφυρα δικτύου πολλαπλών θυρών που χρησιμοποιεί διευθύνσεις MAC για την προώθηση δεδομένων στο επίπεδο σύνδεσης δεδομένων (επίπεδο 2) του μοντέλου OSI και δημιουργεί έναν ξεχωριστό τομέα σύγκρουσης για κάθε θύρα μεταγωγής. Ένας μεταγωγέας δικτύου είναι το υλικό δικτύωσης που συνδέει συσκευές σε δίκτυο υπολογιστών χρησιμοποιώντας πακέτα εναλλαγής για λήψη και προώθηση δεδομένων στη συσκευή προορισμού.

1.2.3 Multilayer Switch-Μεταγωγέας Πολλαπλών Επίπεδων



Εικόνα 1.5 Μεταγωγέας Πολλαπλών Επίπεδων σε GNS3

Μερικοί μεταγωγείς μπορούν επίσης να προωθήσουν δεδομένα στο επίπεδο δικτύου (επίπεδο 3), το οποίο θα εξηγήσουμε παρακάτω, με επιπλέον ενσωμάτωση λειτουργικότητα δρομολόγησης. Τέτοιοι μεταγωγείς είναι κοινώς γνωστά ως L3 switches ή multilayer switches ή μεταγωγείς πολλαπλών επιπέδων. Το switch πολλαπλών επιπέδων (MLS) είναι μια συσκευή δικτύωσης υπολογιστών που αλλάζει στο επίπεδο OSI 2 σαν ένα συνηθισμένο μεταγωγέα δικτύου και παρέχει επιπλέον λειτουργίες σε υψηλότερα επίπεδα OSI. Η μεταγωγή πολλαπλών επιπέδων μπορεί να μετακινήσει την κυκλοφορία με ταχύτητα καλωδίου και επίσης να παρέχει δρομολόγηση επιπέδου 3. Η μεταγωγή πολλαπλών επιπέδων μπορεί να λάβει αποφάσεις δρομολόγησης και μεταγωγής με βάση τα ακόλουθα:

1)Τη διεύθυνση MAC σε πλαίσιο σύνδεσης δεδομένων

2)Το πεδίο πρωτοκόλλου στο πλαίσιο σύνδεσης δεδομένων

3)Τη διεύθυνση IP στην κεφαλίδα του επιπέδου δικτύου

4)Το πεδίο πρωτοκόλλου στην κεφαλίδα του επιπέδου δικτύου

5)Τους αριθμούς θυρών στην κεφαλίδα του επιπέδου μεταφοράς

1.2.4 Firewall-Τείχος Προστασίας

Εικόνα 1.6 Τείχος Προστασίας σε GNS3

Ο όρος firewall ή τείχος προστασίας χρησιμοποιείται για να δηλώσει κάποια συσκευή ή πρόγραμμα που είναι έτσι ρυθμισμένο ούτως ώστε να επιτρέπει ή να απορρίπτει πακέτα

δεδομένων που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο. Η κύρια λειτουργία ενός τείχους προστασίας είναι να ρυθμίζει τη ροή δεδομένων μεταξύ δύο δικτύων υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το διαδίκτυο και το τοπικό ή εταιρικό δίκτυο. Ένα τείχος προστασίας εισάγεται μεταξύ δύο δικτύων με διαφορετικά επίπεδα εμπιστοσύνης. Το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης, ενώ ένα δίκτυο εταιρείας ή ένα οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό εμπιστοσύνης. Ο σκοπός της εγκατάστασης ενός τείχους προστασίας είναι η πρόληψη και η αντιμετώπιση επιθέσεων στο τοπικό δίκτυο. Ωστόσο, τα τείχη προστασίας μπορεί να μην είναι χρήσιμα εάν δεν έχουν ρυθμιστεί σωστά. Είναι καλύτερο να διαμορφώσουμε το τείχος προστασίας μας ώστε να απορρίπτει όλες τις συνδέσεις εκτός από αυτές που επιτρέπεται από τον διαχειριστή του δικτύου. Περισσότερα για τα τείχη προστασίας και πως πρέπει να τα ρυθμίσουμε θα δούμε στο κεφάλαιο 4.

1.2.5 Server-Εξυπηρετητής

Εικόνα 1.7 Διακομιστής σε GNS3

Εξυπηρετητής ή διακομιστής είναι είτε υλικό είτε λογισμικό που αναλαμβάνει την παροχή διάφορων υπηρεσιών, «εξυπηρετώντας» αιτήσεις άλλων προγραμμάτων, γνωστών ως πελάτες (clients) που μπορούν να τρέχουν στον ίδιο υπολογιστή ή σε σύνδεση μέσω δικτύου. Όταν ένας υπολογιστής εκτελεί κυρίως τέτοια προγράμματα εξυπηρετητές συνεχόμενα, 24 ώρες την ημέρα, τότε μπορούμε να αναφερθούμε σε όλον τον υπολογιστή ως εξυπηρετητή, αφού αυτή είναι η κύρια λειτουργία του. Παρομοίως, ως πελάτη μπορούμε να θεωρήσουμε είτε κάποιο λογισμικό που επικοινωνεί και υποβάλλει αιτήματα στον εξυπηρετητή, είτε όλο τον υπολογιστή όταν ο εξυπηρετητής είναι άλλος υπολογιστής και οι 2 υπολογιστές είναι συνδεδεμένοι σε ένα δίκτυο.

1.3 OSI Model-Μοντέλο OSI

Το μοντέλο αναφοράς Ανοικτής Διασύνδεσης Συστημάτων, ή αλλιώς μοντέλο αναφοράς OSI είναι μια διαστρωματωμένη περιγραφή που αφορά τη σχεδίαση τηλεπικοινωνιακών και δικτυακών πρωτοκόλλων . Είναι γνωστό και ως μοντέλο των επτά επιπέδων.

Επίπεδο 1	**Φυσικό (Physical Layer)**
Επίπεδο 2	**Σύνδεσης Δεδομένων (Data Link Layer)**
Επίπεδο 3	**Δικτύου (Network Layer)**
Επίπεδο 4	**Μεταφοράς (Transport Layer)**
Επίπεδο 5	**Συνόδου (Session Layer)**
Επίπεδο 6	**Παρουσίασης (Presentation Layer)**
Επίπεδο 7	**Εφαρμογής (Application Layer)**

Εικόνα 1.8 Μοντέλο OSI

1.3.1 Πρωτόκολλα ανά επίπεδο του μοντέλου OSI

Το κάθε επίπεδο στο μοντέλο αυτό έχει δικά του πρωτόκολλα, τα οποία παρουσιάζονται στον παρακάτω πίνακα.

OSI LAYER	PROTOCOLS
Layer 1	RS232,DSL,802.11, BLUETOOTH,SONET/SDH..
Layer 2	ARP,LLC,MAC,ATM…
Layer 3	IPv4,IPv6,ICMP,IPsec…
Layer 4	TCP,UDP…
Layer 5	SAP,RTP,NETBIOS…
Layer 6	ASCII,PGP…
Layer 7	DNS,FTP,HTTP,NTP,SMTP, DHCP, Telnet

Εικόνα 1.9 Πρωτόκολλα Ανά Επίπεδο OSI

1.3.2 Φυσικό Επίπεδο - Physical Layer (Layer 1)

Το επίπεδο αυτό προδιαγράφει τις ηλεκτρικές, χρονικές, και άλλες διασυνδέσεις μέσω των οποίων τα Bit στέλνονται ως σήματα σε κανάλια. Είναι υπεύθυνο για την πραγματική φυσική σύνδεση μεταξύ των συσκευών. Το επίπεδο αυτό περιέχει πληροφορίες με τη μορφή bit. Είναι

υπεύθυνο για τη μετάδοση μεμονωμένων bit από τον έναν κόμβο στον επόμενο. Κατά τη λήψη δεδομένων, αυτό το επίπεδο θα πάρει το σήμα που λαμβάνεται και θα το μετατρέψει σε 0 και 1 και θα τα στείλει στο επίπεδο σύνδεσης δεδομένων, το οποίο θα ενώσει ξανά το πλαίσιο. Οι κύριες λειτουργίες του φυσικού στρώματος είναι:

- Ο συγχρονισμός των bit: Το φυσικό επίπεδο καθιστά το συγχρονισμό των bit παρέχοντας ένα ρολόι. Αυτό το ρολόι ελέγχει τόσο τον αποστολέα όσο και τον δέκτη παρέχοντας έτσι συγχρονισμό σε επίπεδο bit.
- Ο έλεγχος ρυθμού των bit: Το φυσικό επίπεδο ορίζει επίσης τον ρυθμό μετάδοσης, για παράδειγμα τον αριθμό των bit που αποστέλλονται ανά δευτερόλεπτο.
- Οι φυσικές τοπολογίες: Το φυσικό επίπεδο καθορίζει τον τρόπο με τον οποίο οι διαφορετικές συσκευές ή αλλιώς κόμβοι είναι διατεταγμένοι σε ένα δίκτυο, για παράδειγμα τοπολογία διαύλου, αστεριού ή πλέγματος.
- Ο τρόπος μετάδοσης: Το φυσικό επίπεδο ορίζει επίσης τον τρόπο με τον οποίο ρέουν τα δεδομένα μεταξύ των δύο συνδεδεμένων συσκευών. Οι διάφοροι δυνατοί τρόποι μετάδοσης είναι Simplex, half-duplex και full-duplex.

1.3.3 Επίπεδο Συνδέσμου Μετάδοσης Δεδομένων-Data Link Layer (Layer 2)

Το επίπεδο σύνδεσης δεδομένων είναι υπεύθυνο για την παράδοση του μηνύματος από κόμβο σε κόμβο. Η κύρια λειτουργία αυτού του επιπέδου είναι να διασφαλίζει ότι η μεταφορά δεδομένων είναι χωρίς σφάλματα από τον ένα κόμβο στον άλλο, πάνω από το φυσικό επίπεδο. Όταν ένα πακέτο φτάνει σε ένα δίκτυο, είναι ευθύνη αυτού του επιπέδου να το μεταδώσει στον κεντρικό υπολογιστή χρησιμοποιώντας τη διεύθυνση MAC του. Το επίπεδο σύνδεσης δεδομένων χωρίζεται σε δύο υποστρώματα:

- Το Logical Link Control (LLC)

Το LLC παρέχει μηχανισμούς πολυπλεξίας που καθιστούν δυνατή τη συνύπαρξη πολλών πρωτοκόλλων δικτύου μέσα σε ένα δίκτυο πολλαπλών σημείων και τη μεταφορά τους μέσω του ίδιου μέσου δικτύου. Μπορεί επίσης να παρέχει μηχανισμούς διαχείρισης σφαλμάτων ελέγχου ροής και αυτόματης επανάληψης αιτημάτων.

- Το Media Access Control (MAC)

Το πακέτο που λαμβάνεται από το επίπεδο δικτύου χωρίζεται περαιτέρω σε πλαίσια ανάλογα στο μέγεθος πλαισίου της NIC (Κάρτα Διασύνδεσης Δικτύου). Το επίπεδο 2 ενσωματώνει

επίσης τον αποστολέα και τη διεύθυνση MAC του παραλήπτη στην κεφαλίδα. Η διεύθυνση MAC του δέκτη λαμβάνεται με την τοποθέτηση ενός ARP (Address Resolution Protocol) αιτήματος στο καλώδιο ρωτώντας "Ποιος έχει αυτήν τη διεύθυνση IP;" και ο οικοδεσπότης προορισμού θα απαντήσει με τη διεύθυνση MAC του. Τα πρωτόκολλα MAC και ARP θα αναλυθούν σε επόμενα κεφάλαια. Οι λειτουργίες του επιπέδου Data Link είναι:

- Πλαισιοποίηση-Framing: Είναι μια συνάρτηση η οποία παρέχει έναν τρόπο για ένα αποστολέα να μεταδώσει ένα σύνολο bits που έχουν νόημα για τον δέκτη. Αυτό μπορεί να επιτευχθεί με την προσάρτηση ειδικών μοτίβων κομματιών στην αρχή και στο τέλος του πλαισίου.
- Φυσική διευθυνσιοδότηση: Μετά τη δημιουργία πλαισίων, το επίπεδο προσθέτει φυσικές διευθύνσεις (διεύθυνση MAC) του αποστολέα και του παραλήπτη στην κεφαλίδα κάθε πλαισίου.
- Έλεγχος σφαλμάτων: Παρέχει ένα μηχανισμό ελέγχου σφαλμάτων στον οποίο ανιχνεύει και αναμεταδίδει κατεστραμμένα ή χαμένα καρέ.
- Έλεγχος ροής: Ο ρυθμός δεδομένων πρέπει να είναι σταθερός και στις δύο πλευρές, διαφορετικά μπορεί να ληφθούν τα δεδομένα κατεστραμμένα έτσι, ο έλεγχος ροής συντονίζει την ποσότητα των δεδομένων που μπορούν να σταλούν πριν την λήψη αναγνώρισης.
- Έλεγχος πρόσβασης: Όταν ένα μονό κανάλι επικοινωνίας είναι κοινόχρηστο από πολλές συσκευές, το υποεπίπεδο MAC του επιπέδου σύνδεσης δεδομένων βοηθά στον προσδιορισμό της συσκευής που έχει τον έλεγχο πάνω από το κανάλι σε μια δεδομένη στιγμή.

Στόχος λοιπόν αυτού του επιπέδου είναι να παρέχει υπηρεσίες στο επίπεδο δικτύου, αξιοποιώντας τις υπηρεσίες του φυσικού επιπέδου. Ο μεταγωγέας είναι μια συσκευή που ανήκει στο επίπεδο συνδέσμου μετάδοσης δεδομένων.

1.3.4 Επίπεδο Δικτύου - Network Layer (Layer 3)

Το επίπεδο αυτό ασχολείται με τη μεταφορά πακέτων από την προέλευση τους μέχρι τον προορισμό τους. Για να φτάσουν τα πακέτα στον προορισμό τους μπορεί να χρειαστεί να κάνουν πολλά άλματα (hops) μέσω ενδιάμεσων δρομολογητών που υπάρχουν στην διαδρομή. Για να πέτυχει τους στόχους του το επίπεδο δικτύου πρέπει να γνωρίζει την τοπολογία του δικτύου και να επιλεγεί κατάλληλες διαδρομές μέσα από αυτό. Το επίπεδο δικτύου λειτουργεί

για τη μετάδοση δεδομένων από έναν κεντρικό υπολογιστή σε άλλο σε διαφορετικό δίκτυο. Φροντίζει επίσης για τη δρομολόγηση πακέτων, δηλαδή την επιλογή της συντομότερης διαδρομής για τη μετάδοση του πακέτου, από τον αριθμό των διαθέσιμων διαδρομών. Οι διευθύνσεις IP του αποστολέα και του παραλήπτη τοποθετούνται στην κεφαλίδα από το επίπεδο δικτύου. Οι λειτουργίες του επιπέδου Δικτύου είναι:

- Δρομολόγηση: Τα πρωτόκολλα του επιπέδου δικτύου καθορίζουν ποια διαδρομή είναι κατάλληλη από την πηγή στον προορισμό.
- Λογική Διεύθυνση: Προκειμένου να αναγνωρίζεται κάθε συσκευή στο διαδίκτυο μοναδικά, το επίπεδο δικτύου ορίζει ένα σχήμα διευθύνσεων. Οι διευθύνσεις IP του αποστολέα και του παραλήπτη είναι τοποθετημένες στην κεφαλίδα από το επίπεδο δικτύου. Μια τέτοια διεύθυνση διακρίνει κάθε συσκευή μοναδικά και καθολικά.

1.3.5 Επίπεδο Μεταφοράς - Transport Layer (Layer 4)

Το επίπεδο μεταφοράς παρέχει υπηρεσίες στο επίπεδο εφαρμογής και λαμβάνει υπηρεσίες από το επίπεδο δικτύου. Τα δεδομένα στο επίπεδο μεταφοράς αναφέρονται ως Τμήματα-segments. Είναι υπεύθυνο για την παράδοση από άκρο σε άκρο του πλήρους μηνύματος. Το επίπεδο μεταφοράς παρέχει επίσης την επιβεβαίωση της επιτυχούς μετάδοσης δεδομένων και μεταδίδει εκ νέου τα δεδομένα εάν εντοπιστεί σφάλμα.

• Από τη μεριά του αποστολέα:

Το επίπεδο μεταφοράς λαμβάνει τα μορφοποιημένα δεδομένα από τα ανώτερα επίπεδα, εκτελεί τμηματοποίηση, και εφαρμόζει επίσης έλεγχο ροής και σφάλματος για να διασφαλίσει τη σωστή μετάδοση δεδομένων. Προσθέτει επίσης τους αριθμούς θύρας πηγής και προορισμού στην κεφαλίδα του και προωθεί τα τμηματοποιημένα δεδομένα στο επίπεδο δικτύου.

• Από τη μεριά του δέκτη:

Το επίπεδο μεταφοράς διαβάζει τον αριθμό θύρας από την κεφαλίδα του και προωθεί τα δεδομένα που έχει παραλάβει στην αντίστοιχη αίτηση. Εκτελεί επίσης αλληλουχία και επανασυναρμολόγηση των τμηματοποιημένων δεδομένων. Οι λειτουργίες του επιπέδου μεταφοράς είναι:

- Τμηματοποίηση και επανασυναρμολόγηση: Αυτό το επίπεδο δέχεται το μήνυμα από το επίπεδο συνεδρίας, σπάει το μήνυμα σε μικρότερες μονάδες. Κάθε ένα από τα τμήματα που παράγονται έχει μια κεφαλίδα συνδεδεμένη με αυτό. Το επίπεδο μεταφοράς στο σταθμό προορισμού επανασυναρμολογεί το μήνυμα.

- Διεύθυνση σημείου εξυπηρέτησης: Για να παραδοθεί το μήνυμα στη σωστή διαδικασία, η κεφαλίδα του επιπέδου μεταφοράς περιλαμβάνει έναν τύπο διεύθυνσης που ονομάζεται διεύθυνση σημείου εξυπηρέτησης ή διεύθυνση θύρας. Έτσι, προσδιορίζοντας αυτή τη διεύθυνση, το επίπεδο μεταφοράς διασφαλίζει ότι το μήνυμα παραδίδεται στη σωστή διαδικασία.

1.3.6 Επίπεδο Συνεδρίας - Session Layer (Layer 5)

Αυτό το επίπεδο είναι υπεύθυνο για τη δημιουργία σύνδεσης, τη συντήρηση των συνεδριών, τον έλεγχο ταυτότητας και επίσης διασφαλίζει την ασφάλεια. Οι λειτουργίες του επιπέδου συνεδρίας είναι:

- Δημιουργία συνεδρίας, συντήρηση και τερματισμός: Το επίπεδο επιτρέπει τις δύο διαδικασίες για τη δημιουργία, τη χρήση και τον τερματισμό μιας σύνδεσης.
- Συγχρονισμός: Αυτό το επίπεδο επιτρέπει σε μια διαδικασία να προσθέσει σημεία ελέγχου που λαμβάνονται υπόψη σαν σημεία συγχρονισμού στα δεδομένα. Αυτά τα σημεία συγχρονισμού βοηθούν στον εντοπισμό του σφάλματος έτσι ώστε τα δεδομένα να συγχρονιστούν ξανά σωστά και τα άκρα των μηνυμάτων να μην κόβονται πρόωρα και να αποφεύγεται η απώλεια δεδομένων.
- Ελεγκτής διαλόγου: Το επίπεδο συνεδρίας επιτρέπει σε δύο συστήματα να ξεκινήσουν την επικοινωνία το ένα με το άλλο σε ημιαμφίδρομη ή πλήρης αμφίδρομη όψη.

1.3.7 Επίπεδο Παρουσίασης - Presentation Layer (Layer 6)

Το επίπεδο παρουσίασης ονομάζεται επίσης επίπεδο μετάφρασης. Τα στοιχεία από το επίπεδο εφαρμογής εξάγονται εδώ και χειρίζονται σύμφωνα με την απαιτούμενη μορφή για μετάδοση μέσω του δικτύου. Οι λειτουργίες του επιπέδου παρουσίασης είναι:

- Μετάφραση: Για παράδειγμα, ASCII σε EBCDIC.
- Κρυπτογράφηση/Αποκρυπτογράφηση: Η κρυπτογράφηση δεδομένων μεταφράζει τα δεδομένα σε άλλη μορφή ή κώδικα. Τα κρυπτογραφημένα δεδομένα είναι γνωστά ως κρυπτογραφημένο κείμενο και τα αποκρυπτογραφημένα δεδομένα είναι γνωστά ως απλό κείμενο. Μια βασική τιμή χρησιμοποιείται για την κρυπτογράφηση καθώς και την αποκρυπτογράφηση δεδομένων.
- Συμπίεση: Μειώνει τον αριθμό των bit που πρέπει να μεταδοθούν στο δίκτυο.

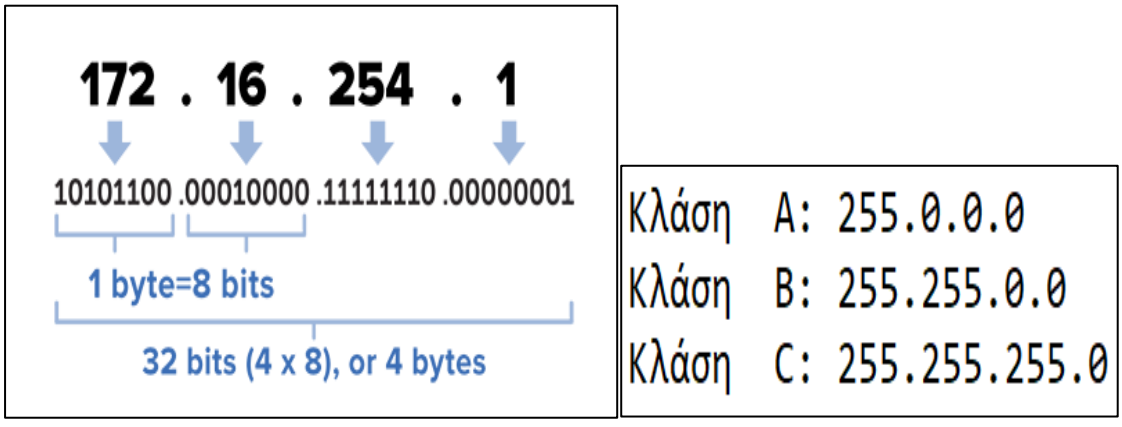
1.3.8 Επίπεδο Εφαρμογής - Application Layer (Layer 7)

Στην κορυφή της στοίβας επιπέδων του μοντέλου αναφοράς OSI, βρίσκουμε το επίπεδο εφαρμογής που υλοποιείται από τις εφαρμογές δικτύου. Αυτές οι εφαρμογές παράγουν τα δεδομένα, που πρέπει να μεταφερθούν μέσω του δικτύου. Αυτό το επίπεδο χρησιμεύει επίσης ως παράθυρο για τις υπηρεσίες εφαρμογών για πρόσβαση στο δίκτυο και για εμφάνιση των ληφθέντων πληροφοριών στον χρήστη. Οι λειτουργίες του επιπέδου εφαρμογής είναι:

- Εικονικό τερματικό δικτύου
- Πρόσβαση και διαχείριση μεταφοράς αρχείων
- Υπηρεσίες αλληλογραφίας
- Υπηρεσίες καταλόγου

1.4 Διεύθυνση (IP) Και Μάσκα (Mask) Δικτύου

Μια λογική αριθμητική διεύθυνση που εκχωρείται σε κάθε υπολογιστή, μεταγωγέα, δρομολογητή ή οποιαδήποτε άλλη συσκευή που αποτελεί μέρος ενός δικτύου. Κάθε συσκευή έχει μια διεύθυνση IP με δυο μέρη. Το πρώτο μέρος αφορά τη διεύθυνση πελάτη ή κεντρικού υπολογιστή και τη διεύθυνση διακομιστή η δικτύου. Οι διευθύνσεις IP είτε διαμορφώνονται από ένα DHCP διακομιστή είτε με μη αυτόματο τρόπο, την στατική διευθυνσιοδότηση. Η μάσκα υποδικτύου είναι ένας 32-bit αριθμός ο οποίος διαχωρίζει τη διεύθυνση IP σε διευθύνσεις κεντρικού υπολογιστή και δικτύου ορίζοντας έτσι ποιο τμήμα της διεύθυνσης IP ανήκει στη συσκευή και ποιο τμήμα ανήκει στο δίκτυο.



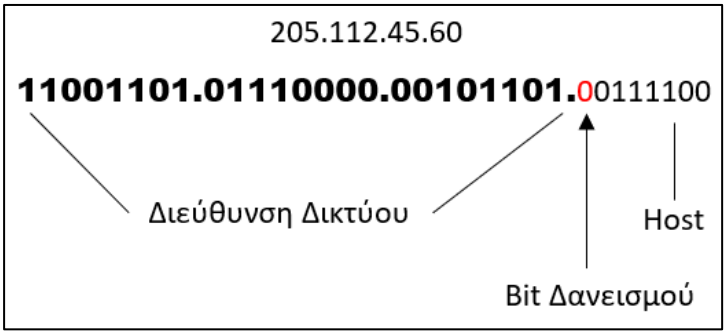
Εικόνα 1.10 Διεύθυνση IP και Κλάσεις

- Μια μάσκα υποδικτύου Κατηγορίας A αντικατοπτρίζει το τμήμα δικτύου στην πρώτη οκτάδα και αφήνει τις οκτάδες 2, 3 και 4 για τον διαχειριστή δικτύου να διαιρεθεί σε κεντρικούς υπολογιστές και υποδίκτυα ανάλογα με τις ανάγκες. Η κλάση A είναι για δίκτυα με περισσότερους από 65.536 κεντρικούς υπολογιστές.
- Μια μάσκα υποδικτύου Κατηγορίας B διεκδικεί τις δύο πρώτες οκτάδες για το δίκτυο, αφήνοντας το υπόλοιπο τμήμα της διεύθυνσης, τα 16 bit των οκτάδων 3 και 4, για το τμήμα του υποδικτύου και του κεντρικού υπολογιστή. Η κλάση B είναι για δίκτυα με 256 έως 65.534 κεντρικούς υπολογιστές.
- Σε μια μάσκα υποδικτύου Κατηγορίας C, το τμήμα δικτύου είναι οι τρεις πρώτες οκτάδες με τους κεντρικούς υπολογιστές και τα υποδίκτυα μόνο στα υπόλοιπα 8 bit της οκτάδας 4. Η κλάση C είναι για μικρότερα δίκτυα με λιγότερους από 254 κεντρικούς υπολογιστές.

1.5 Υποδικτύωση και Μάσκα Υποδικτύου

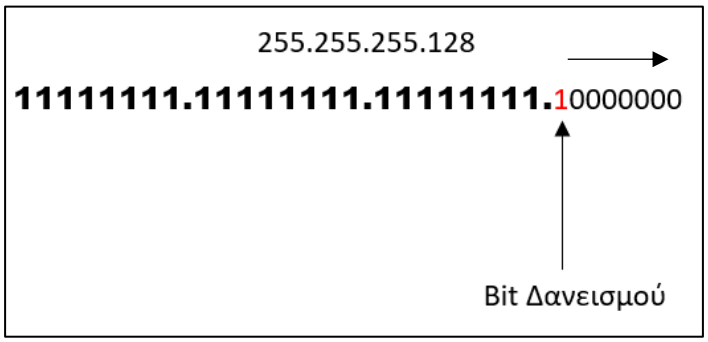
Ένα υποδίκτυο, είναι ένα ξεχωριστό και αναγνωρίσιμο τμήμα του δικτύου ενός οργανισμού, συνήθως διατεταγμένο σε έναν όροφο, κτίριο ή γεωγραφική τοποθεσία. Τα υποδίκτυα κάνουν τα δίκτυα πιο αποτελεσματικά. Μέσω του υποδικτύου, η κίνηση του δικτύου μπορεί να διανύσει μικρότερη απόσταση χωρίς να περάσει από περιττούς δρομολογητές για να φτάσει στον προορισμό της. Η μάσκα υποδικτύου είναι ένας αριθμός 32-bit που χρησιμοποιείται για τη διαφοροποίηση του στοιχείου δικτύου μιας διεύθυνσης IP διαιρώντας τη διεύθυνση IP σε μια διεύθυνση δικτύου και μια διεύθυνση κεντρικού υπολογιστή η οποία προορίζεται μόνο για εσωτερική χρήση σε ένα δίκτυο. Οι δρομολογητές χρησιμοποιούν μάσκες υποδικτύου για να δρομολογούν πακέτα δεδομένων στη σωστή θέση. Οι μάσκες υποδικτύου δεν υποδεικνύονται στα πακέτα δεδομένων που διασχίζουν το Διαδίκτυο, αυτά τα πακέτα υποδεικνύουν μόνο τη διεύθυνση IP προορισμού, την οποία ένας δρομολογητής θα αντιστοιχίσει με ένα υποδίκτυο. Το υποδίκτυο ενός δικτύου σημαίνει επίσης τη δημιουργία λογικών τμημάτων του δικτύου. Η υποδικτύωση ισχύει για διευθύνσεις IP επειδή αυτό γίνεται με δανεισμό bit από το τμήμα κεντρικού υπολογιστή της διεύθυνσης IP. Κατά μία έννοια, η διεύθυνση IP έχει τότε τρία στοιχεία, το τμήμα δικτύου, το τμήμα υποδικτύου και τέλος, το τμήμα υποδοχής. Δημιουργούμε ένα υποδίκτυο παίρνοντας λογικά το τελευταίο bit από το στοιχείο δικτύου της διεύθυνσης και χρησιμοποιώντας το για να προσδιορίσουμε τον αριθμό των υποδικτύων που απαιτούνται.

Στο παρακάτω παράδειγμα, μια διεύθυνση Κατηγορίας C έχει συνήθως 24 bit για τη διεύθυνση δικτύου και οκτώ για τον κεντρικό υπολογιστή, αλλά πρόκειται να δανειστούμε το αριστερό bit της διεύθυνσης κεντρικού υπολογιστή και να το δηλώσουμε ως αναγνώριση του υποδικτύου.



Εικόνα 1.11 Διεύθυνση IP για Υποδικτύωση

Εάν το bit είναι 0, τότε αυτό θα είναι ένα υποδίκτυο. Εάν το bit είναι 1, αυτό θα ήταν το δεύτερο υποδίκτυο. Φυσικά, με ένα μόνο δανεισμένο bit μπορούμε να έχουμε μόνο δύο πιθανά υποδίκτυα. Με την ίδια λογική, αυτό μειώνει επίσης τον αριθμό των κεντρικών υπολογιστών που μπορούμε να έχουμε στο δίκτυο σε 127 από 255. Με μια μάσκα υποδικτύου δηλαδή μπορούμε να δούμε πόσα bit πρέπει να δανειστούμε ή με άλλα λόγια πόσα υποδίκτυα θέλουμε να έχουμε στο δίκτυο μας. Αυτό που κάνει μια μάσκα υποδικτύου είναι να υποδεικνύει πόσα bit δανείζονται από το στοιχείο κεντρικού υπολογιστή μιας διεύθυνσης IP. Στην παρακάτω εικόνα, υπάρχει μια μάσκα υποδικτύου για μια διεύθυνση Κατηγορίας C. Η μάσκα υποδικτύου είναι 255.255.255.128, η οποία, όταν μεταφράζεται σε bit, υποδεικνύει ποια bit του κεντρικού τμήματος της διεύθυνσης θα χρησιμοποιηθούν για τον προσδιορισμό του αριθμού υποδικτύου.



Εικόνα 1.12 Διεύθυνση IP για Υποδικτύωση

Φυσικά, περισσότερα bit δανεισμένα σημαίνει λιγότερους μεμονωμένα διευθυνσιοδοτούμενους κεντρικούς υπολογιστές που μπορούν να βρίσκονται στο δίκτυο. Μερικές φορές, όλοι οι συνδυασμοί και οι μεταθέσεις μπορεί να προκαλούν σύγχυση, επομένως εδώ είναι ένας πίνακας με τις δυνατότητες υποδικτύου για την κλάση B.

Subnet Mask Bits	Subnet Mask	Hosts	Subnets
/30	255.255.252.252	2	16384
/29	255.255.252.248	6	8192
/28	255.255.252.240	14	4096
/27	255.255.252.224	30	2048
/26	255.255.252.192	62	1024
/25	255.255.252.128	126	512
/24	255.255.255.0	254	256
/23	255.255.254.0	510	128
/22	255.255.252.0	1022	64

Εικόνα 1.13 Δυνατότητες Υποδικτύων

1.6 Τεχνική VLSM

Η μάσκα υποδικτύου μεταβλητού μήκους ή αλλιώς VLSM αφορά το σχεδιασμό του υποδικτύου και χρησιμοποιεί περισσότερες από μία μάσκες στο ίδιο δίκτυο, πράγμα που σημαίνει ότι χρησιμοποιούνται περισσότερες από μία μάσκες για διαφορετικά υποδίκτυα μιας κατηγορίας A,B,C ή ενός δικτύου. Χρησιμοποιείται για την αύξηση της αποτελεσματικότητας των υποδικτύων καθώς μπορεί να είναι μεταβλητού μεγέθους. Ορίζεται επίσης ως η διαδικασία υποδικτύωσης ενός υποδικτύου.

Στο VLSM, τα υποδίκτυα χρησιμοποιούν μέγεθος μπλοκ με βάση την απαίτηση, επομένως η υποδικτύωση απαιτείται πολλές φορές. Ας υποθέσουμε ότι υπάρχει ένας διαχειριστής που έχει τέσσερα τμήματα για διαχείριση. Πρόκειται για το τμήμα προγραμματιστών με 120 υπολογιστές, το τμήμα ασφάλειας με 50 υπολογιστές, το τμήμα προώθησης με 26 υπολογιστές και το τμήμα διαχείρισης με 5 υπολογιστές. Εάν ο διαχειριστής έχει την διεύθυνση IP 192.168.1.0/24, μπορούμε να εκχωρήσουμε IP από το τμήμα ακολουθώντας αυτά τα βήματα:

1)Για κάθε τμήμα επιλέγουμε το μέγεθος του μπλοκ που είναι μεγαλύτερο ή ίσο με την πραγματική απαίτηση, που είναι το άθροισμα των διευθύνσεων κεντρικού υπολογιστή, των διευθύνσεων εκπομπής και των διευθύνσεων δικτύου. Διαθέτουμε μια λίστα υποδικτύων:

Subnet Mask Bits	Hosts
/30	2
/29	6
/28	14
/27	30
/26	62
/25	126
/24	254

Εικόνα 1.14 Λίστα Υποδικτύων

2)Τακτοποιούμε όλα τα τμήματα σε φθίνουσα σειρά με βάση το μέγεθος του μπλοκ που είναι από την υψηλότερη στη χαμηλότερη απαίτηση.

Προγραμματιστές: 120

Ασφάλεια: 50

Προώθηση: 26

Διαχείριση: 5

3)Η υψηλότερη διαθέσιμη IP πρέπει να εκχωρηθεί στην υψηλότερη απαίτηση, ώστε το τμήμα προγραμματιστών να λάβει 192.168.1.0/25 που έχει 126 έγκυρες διευθύνσεις που μπορούν εύκολα να είναι διαθέσιμες για 120 κεντρικούς υπολογιστές. Η μάσκα υποδικτύου που χρησιμοποιείται είναι 255.255.255.128

4)Το επόμενο τμήμα απαιτεί μια IP για να χειριστεί 50 κεντρικούς υπολογιστές. Το υποδίκτυο IP με αριθμό δικτύου 192.168.1.128/26 είναι το επόμενο υψηλότερο που μπορεί να εκχωρηθεί σε 62 κεντρικούς υπολογιστές, ικανοποιώντας έτσι την απαίτηση του τμήματος ανάπτυξης. Η μάσκα υποδικτύου που χρησιμοποιείται είναι 255.255.255.192

5)Ομοίως, το επόμενο υποδίκτυο IP 192.168.1.192/27 μπορεί να ικανοποιήσει τις απαιτήσεις του τμήματος προώθησης καθώς διαθέτει 30 έγκυρες IP κεντρικών υπολογιστών που μπορούν να εκχωρηθούν σε 26 υπολογιστές. Η μάσκα που χρησιμοποιείται είναι 255.255.255.224

6)Το τελευταίο τμήμα απαιτεί 5 έγκυρους κεντρικούς υπολογιστές IP που μπορούν να εκπληρωθούν από το υποδίκτυο 192.168.1.224/29 που έχει τη μάσκα ως 255.255.255.248 επιλέγεται σύμφωνα με την απαίτηση. Θα μπορούσε να επιλεγεί η IP με τη μάσκα 255.255.255.240, αλλά έχει 14 έγκυρες IP κεντρικού υπολογιστή και η απαίτηση είναι μικρότερη σε σύγκριση, επομένως επιλέγεται αυτή που είναι συγκρίσιμη με την απαίτηση. Έτσι, υπάρχει λιγότερη σπατάλη IP στο VLSM σε σύγκριση με το FLSM.

Στο υποδίκτυο μάσκας υποδικτύου σταθερού μήκους (FLSM), όλα τα υποδίκτυα είναι ίσου μεγέθους και έχουν ίσο αριθμό κεντρικών υπολογιστών, αλλά στο VLSM το μέγεθος είναι μεταβλητό και μπορεί να έχει μεταβλητό αριθμό κεντρικών υπολογιστών, καθιστώντας έτσι τη διεύθυνση IP πιο αποτελεσματική επιτρέποντας ένα σύστημα δρομολόγησης με διαφορετικό μήκος μάσκας να ταιριάζει στις απαιτήσεις. Στο FLSM υπάρχει σπατάλη διευθύνσεων IP, αλλά στο VLSM υπάρχει ελάχιστη σπατάλη διευθύνσεων IP. Το FLSM προτιμάται για ιδιωτικές διευθύνσεις IP ενώ για δημόσιες διευθύνσεις IP το VLSM είναι η καλύτερη επιλογή. Έτσι μπορούμε να συμπεράνουμε ότι το VLSM υπερτερεί του FLSM.

1.7 Πρωτόκολλο ICMP

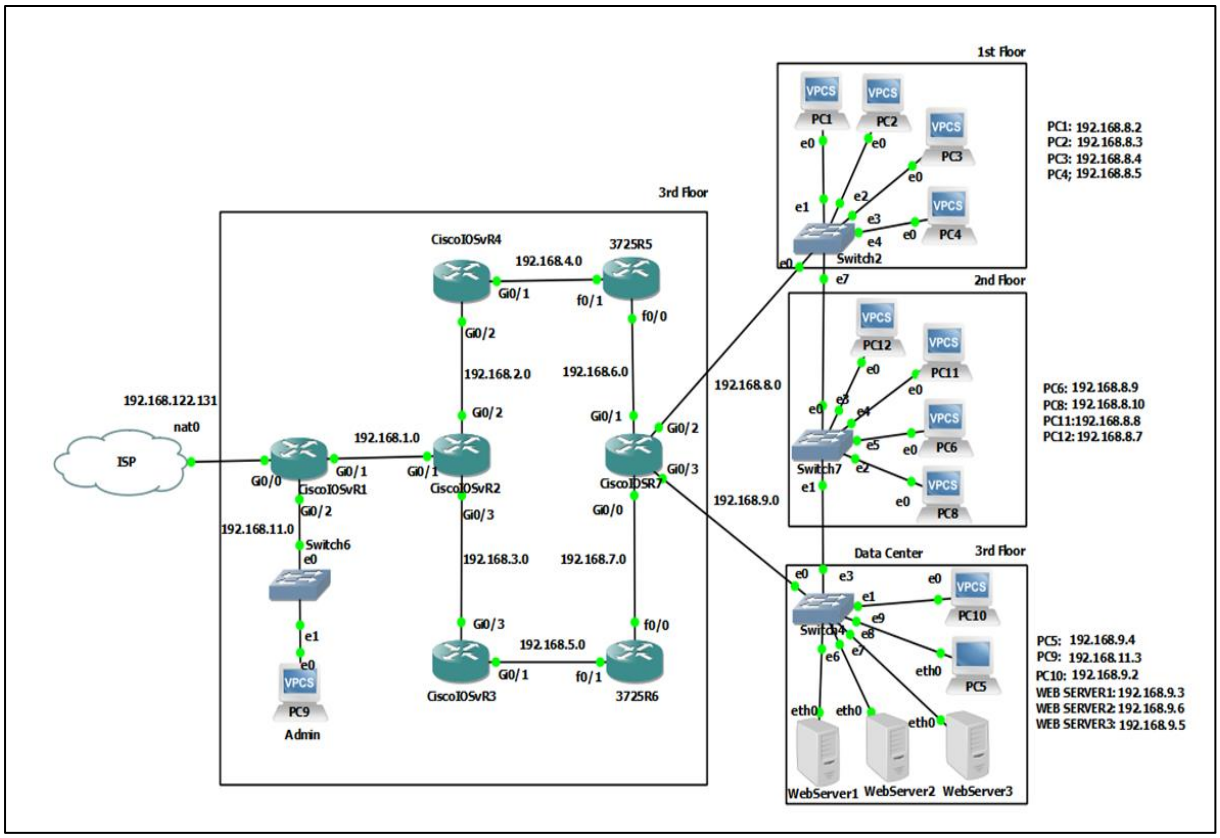
Το πρωτόκολλο Internet Control Message Protocol (ICMP) χρησιμοποιείται σε μεγάλο βαθμό από τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών που βρίσκονται σε ένα δίκτυο για την ανταλλαγή μηνυμάτων σφάλματος , όπως είναι η έλλειψη κάποιας υπηρεσίας από έναν διακομιστή ή την απουσία ενός υπολογιστή από το δίκτυο. Το πρωτόκολλο ICMP δεν χρησιμοποιείται από τις εφαρμογές που εκτελούνται σε κάποιον υπολογιστή, αλλά από το λειτουργικό του σύστημα. Εξαίρεση σε αυτό τον κανόνα αποτελεί το εργαλείο ping, το οποίο στέλνει μηνύματα ICMP Echo Request σε κάποιον υπολογιστή του δικτύου για να διαπιστώσει εάν ο υπολογιστής αυτός υπάρχει ή όχι και επίσης πόσο χρόνο χρειάζεται το μήνυμα να φτάσει σε αυτόν. Εάν ο υπολογιστής αυτός υπάρχει, θα απαντήσει με μηνύματα Echo Response. Περισσότερα για το εργαλείο ping θα δούμε στα επόμενα κεφάλαια καθώς γίνεται συχνά η χρήση του για να ελέγξουμε τη συνδεσιμότητα μεταξύ συσκευών ώστε να δούμε αν επικοινωνούν είτε μεταξύ τους είτε με το διαδίκτυο.

ΚΕΦΑΛΑΙΟ 2 : Σχεδιαστικές Απαιτήσεις Δικτύου

2.1 Εισαγωγή

Υπάρχουν πολλοί λόγοι για την κατασκευή μιας τοπολογίας ικανή να ανταποκριθεί στις ανάγκες των σύγχρονων δικτύων. Οι λόγοι αυτοί αφορούν είτε το σκοπό που εξυπηρετεί το δίκτυο , είτε το κόστος κατασκευής, είτε τη διαχείριση κάποιας ζημιάς, είτε την ταχύτερη εξυπηρέτηση των πελατών. Η εταιρεία που παρουσιάζεται ασχολείται με Hosting και Web Developing υπηρεσίες , το προσωπικό αποτελείται κυρίως από προγραμματιστές και διαθέτει ένα data center το οποίο έχει τους web/host servers. Το δίκτυο της εταιρείας κατασκευάστηκε έτσι ώστε να εξυπηρετεί τις βασικές λειτουργίες της επιχείρησης. Παρόλο που το δίκτυο είναι αρκετά λειτουργικό στα παρακάτω κεφάλαια θα εξηγήσουμε αναλυτικά τα ζητήματα και τα προβλήματα που υπάρχουν στο δίκτυο και θα δείξουμε αναλυτικά το πως αντιμετωπίζονται με αλλαγές σε τοπολογία και ρυθμίσεις.

2.2 Αρχικό Δίκτυο Εταιρείας.



Εικόνα 2.1 Τοπολογία Αρχικού Δικτύου Εταιρείας

Παρακάτω βλέπουμε το υλικό και το λογισμικό το οποίο χρησιμοποιούμε για την παρουσίαση του δικτύου και ένα πίνακα με τις διευθύνσεις των συσκευών. Τα configurations των συσκευών είναι στο appendix 1 στο τέλος του κεφαλαίου.

Hardware
CPU: AMD RYZEN 5 2400G
RAM: Patriot Viper 24G 3000GHz
GPU: AMD Radeon Vega 11

Software
OS: Windows 10 pro
GNS3 Version 2.2.22

Device	Interface 0/0	Interface 0/1	Interface 0/2	Interface 0/3
CiscoIOSv1	Dhcp	192.168.1.1	192.168.11.1	No Ip
CiscoIOSv2	No Ip	192.168.1.2	192.168.2.1	192.168.3.1
CiscoIOSv3	No Ip	192.168.5.1	No Ip	192.168.3.2
CiscoIOSv4	No Ip	192.168.4.1	192.168.2.2	No Ip
CiscoIOSv7	192.168.7.2	192.168.6.2	192.168.8.1	192.168.9.1
3725R5	192.168.6.1	192.168.4.2	No Ip	No Ip
3725R6	192.168.7.1	192.168.5.2	No Ip	No Ip

Εικόνα 2.2 Πίνακας Διευθύνσεων Δικτύου

Ο πάροχος σε αυτό το κεφάλαιο έχει προσομοιωθεί με το NAT Cloud Appliance του GNS3 και έχει δώσει την IP 192.168.122.131 στον αρχικό δρομολογητή ο οποίος χρησιμοποιεί DHCP για να πάρει διεύθυνση. Το αρχικό δίκτυο, χρησιμοποιεί πέντε IOSV Router τα οποία βγάζουν GigabitEthernet ports, δυο 3725 Router των οποίων οι κάρτες υποστηρίζουν fast Ethernet. Τέσσερα Switch επιπέδου δύο , έντεκα υπολογιστές και τρεις Web Server. Οι διακομιστές οφείλονται στο ότι η εταιρεία παρέχει hosting υπηρεσίες, λειτουργούν σαν host servers και έχουν προσομοιωθεί με το Toolbox appliance. Περισσότερα για αυτές τις συσκευές θα δούμε στα επόμενα κεφάλαια.

2.2.1 Πρωτόκολλο DHCP

Το DHCP είναι ένα πρωτόκολλο διαχείρισης δικτύου που χρησιμοποιείται για την αυτόματη εκχώρηση διευθύνσεων IP και άλλων παραμέτρων επικοινωνίας σε συσκευές συνδεδεμένες στο δίκτυο χρησιμοποιώντας αρχιτεκτονική πελάτη-διακομιστή. Η τεχνολογία εξαλείφει την ανάγκη για μεμονωμένη ρύθμιση των συσκευών δικτύου χειροκίνητα και αποτελείται από έναν κεντρικό εγκατεστημένο διακομιστή δικτύου DHCP και παρουσίες

πελάτη της στοίβας πρωτοκόλλων σε κάθε υπολογιστή ή συσκευή. Το DHCP μπορεί να εφαρμοστεί σε δίκτυα διαφορετικών μεγεθών, από οικιακά δίκτυα έως μεγάλα δίκτυα εταιρειών και περιφερειακά δίκτυα ISP. Πολλοί δρομολογητές έχουν δυνατότητα διακομιστή DHCP. Σε ένα τοπικό δίκτυο, ένας διακομιστής DHCP εκχωρεί μια τοπική διεύθυνση IP σε κάθε συσκευή.

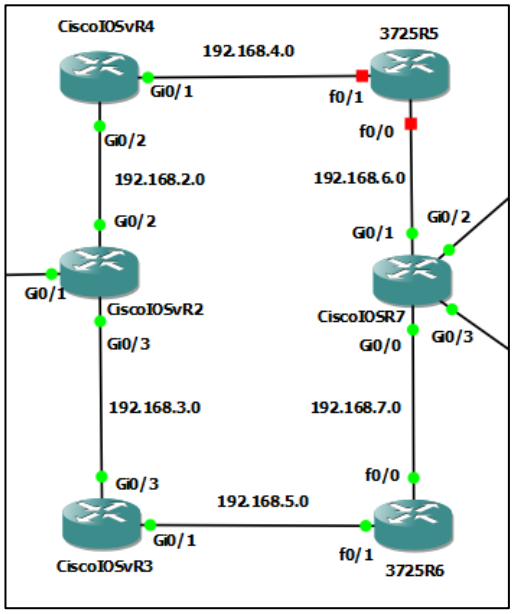
2.2.2 Δρομολόγηση

Πηγαίνοντας στο δίκτυο θα παρατηρήσουμε το μονοπάτι που ακολουθεί το PC1 για να φτάσει στο διαδίκτυο.

```
PC1> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   192.168.8.1   97.727 ms  4.739 ms  7.835 ms
 2   192.168.6.1   13.399 ms  9.613 ms  8.588 ms
 3   192.168.4.1   22.553 ms  19.398 ms  20.493 ms
 4   192.168.2.1   18.218 ms  20.780 ms  20.892 ms
 5   192.168.1.1   78.949 ms  213.780 ms  31.056 ms
 6   192.168.122.1   225.847 ms  232.716 ms  213.790 ms
 7   192.168.119.2   224.112 ms  213.482 ms  223.466 ms
 8     *  *  *
```

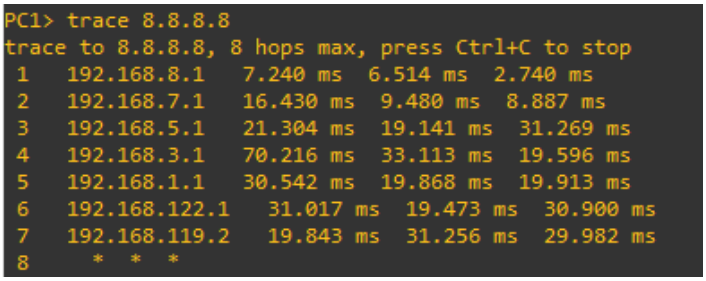
Εικόνα 2.3 Εκτέλεση Εντολής trace 8.8.8.8 από PC1

Στο Δίκτυο έχει εφαρμοστεί το πρωτόκολλο OSPF και για να το ελέγξουμε θα βγάλουμε εκτός λειτουργίας την συσκευή: 3725R5



Εικόνα 2.4 Τοπολογία Λειτουργίας OSPF

Στόχος αυτής της κίνησης είναι να δούμε αν το PC1 θα ακολουθήσει εναλλακτικό μονοπάτι για να φτάσει το ίντερνετ , πράγμα που ισχύει όπως φαίνεται παρακάτω.



Εικόνα 2.5 Εκτέλεση Εντολής trace 8.8.8.8 από PC1

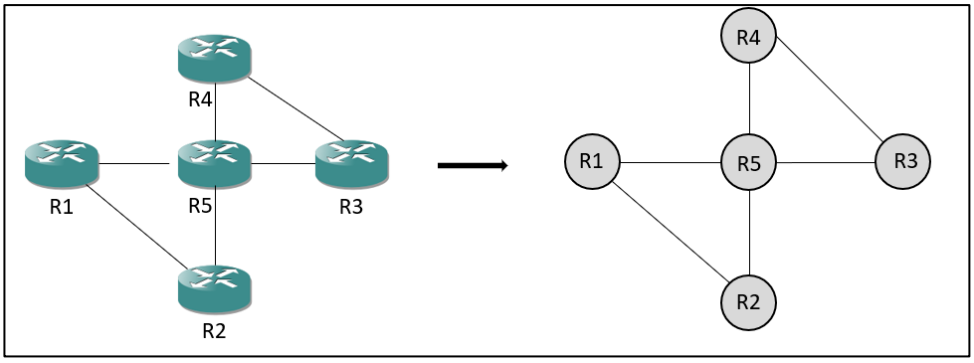
Το ίδιο ισχύει και αν πάθει κάτι και η συσκευή: CiscoIOSv4

2.3 Πρωτόκολλο OSPF

Στη συνέχεια παρατηρούμε ότι το δίκτυό μας χρησιμοποιεί ένα πρωτόκολλο δυναμικής δρομολόγησης, συγκεκριμένα το OSPF . Το Open Shortest Path First (OSPF) είναι ένα ιεραρχικό πρωτόκολλο εσωτερικής πύλης (IGP) που βασίζεται σε κατάσταση σύνδεσης και χρησιμοποιείται για δρομολόγηση σε δίκτυα υπολογιστών και δίκτυα ευρείας περιοχής. Ο αλγόριθμος του Dijkstra εφαρμόζεται για τον υπολογισμό του δέντρου της συντομότερης διαδρομής και χρησιμοποιεί το κόστος ως μέτρηση για τη δρομολόγηση. Δημιουργείται μια βάση δεδομένων κατάστασης σύνδεσης τοπολογίας δικτύου που είναι ίδια σε όλους τους δρομολογητές. Λειτουργεί με ασφάλεια, χρησιμοποιώντας MD5, έναν κρυπτογραφικό αλγόριθμο, για τον έλεγχο ταυτότητας των ομότιμων του πριν σχηματίσει γειτονιές και αποδεχτεί διαφημίσεις κατάστασης συνδέσμων.

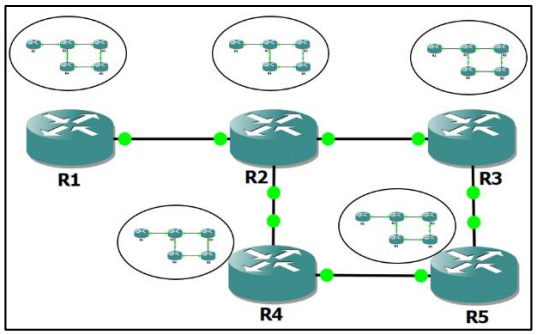
2.3.1 Ο αλγόριθμος του Dijkstra

Πρόκειται για έναν αλγόριθμο ο οποίος στόχο έχει την εύρεση συντομότερων διαδρομών από μια κοινή αφετηρία σε έναν (κατευθυνόμενο ή μη) γράφο ο οποίος έχει μη αρνητικά βάρη στις ακμές. Ο αλγόριθμος του Dijkstra είναι άπληστος. Δηλαδή, σε κάθε βήμα επιλέγει την τοπικά βέλτιστη λύση, ώσπου στο τελευταίο βήμα συνθέτει μια συνολικά βέλτιστη λύση για την επιλογή του μονοπατιού.



Εικόνα 2.6 Μετατροπή δρομολογητών σε κόμβους

Η δουλειά του OSPF είναι να αναπαραστήσει το πραγματικό δίκτυο με ένα τέτοιο γράφο και να χρησιμοποιήσει μετά τη μέθοδο κατάστασης συνδέσμων για να βάλει κάθε δρομολογητή να υπολογίσει τη συντομότερη διαδρομή από τον ίδιο προς όλους τους άλλους κόμβους. Λειτουργεί μοντελοποιώντας το σύνολο των πραγματικών δικτύων δρομολογητών και συνδέσμων μέσω ενός προσανατολισμένου γράφου, στον οποίο σε κάθε τόξο εκχωρείται ένα βάρος. Μπορεί να εντοπιστούν πολλές διαδρομές που να είναι εξίσου σύντομες στην περίπτωση αυτή το OSPF θυμάται το σύνολο των συντομότερων διαδρομών και κατά την προώθηση πακέτων μοιράζει την κυκλοφορία μεταξύ τους, αυτό βοηθά στην εξισορρόπηση φορτιού και αποκαλείται μέθοδος ECMP(equal cost multipath) ή αλλιώς (πολλαπλές διαδρομές ίσου κόστους). Στο OSPF, οι δρομολογητές ενημερώνουν τους υπόλοιπους για το ποιοι είναι οι γείτονες τους. Κυρίος στόχος αυτής της διαδικασίας είναι να δώσει σε όλους τους δρομολογητές μια συνολική κατανόηση της τοπολογίας. Κάθε δρομολογητής πρέπει να γνωρίζει το μέγεθος και το σχήμα του δικτύου. Άρα όπως φαίνεται και στο σχήμα όλοι οι δρομολογητές έχουν έναν χάρτη ολόκληρου του δικτύου.



Εικόνα 2.7 Χάρτης Δρομολογητών

Ο χάρτης που κατέχει κάθε δρομολογητής ονομάζεται βάση δεδομένων OSPF. Ωστόσο, όταν όλοι οι δρομολογητές έχουν μια ενημερωμένη βάση δεδομένων, δεν έχουμε ακόμα διαδρομές. Στην πραγματικότητα, ο δρομολογητής θα πάρει τη βάση δεδομένων και θα αναζητήσει σε

αυτήν τη συντομότερη διαδρομή προς οποιονδήποτε προορισμό. Μόλις βρεθεί, θα προσθέσει μια διαδρομή στον πίνακα δρομολόγησης. Για να γίνει αυτό, ο δρομολογητής εκτελεί τον αλγόριθμο του Dijkstra στη βάση δεδομένων.

2.3.2 Γειτονιές OSPF

Για να γίνει η επικοινωνία το OSPF εφαρμόζει το δικό του στρώμα μεταφοράς. Στην πραγματικότητα, δεν χρησιμοποιεί TCP ούτε UDP, αλλά απευθείας IP. Ο δρομολογητής τοποθετεί μηνύματα OSPF σε πακέτα IP και ορίζει τον αριθμό πρωτοκόλλου σε 89. Το OSPF θα πρέπει να χειρίζεται μόνο του τις επιβεβαιώσεις και τις αναμεταδόσεις. Το OSPF χρησιμοποιεί unicast για να στείλει μερικά πακέτα και multicast για κάποια άλλα. Για να αυξήσουμε την αποτελεσματικότητα, δεν χρησιμοποιούμε εκπομπή. Αντίθετα, χρησιμοποιούμε δύο διευθύνσεις πολλαπλής διανομής.

- Η 224.0.0.5 είναι η διεύθυνση πολλαπλής διανομής για όλους τους δρομολογητές OSPF στο ίδιο δίκτυο.
- Η 224.0.0.6 είναι η διεύθυνση πολλαπλής διανομής για όλους τους καθορισμένους δρομολογητές OSPF στο ίδιο δίκτυο.

Σε γενικές γραμμές, όλη η κίνηση που μπορεί να ενδιαφέρει πολλούς δρομολογητές πηγαίνει σε πακέτα πολλαπλής διανομής. Αντίθετα, συγκεκριμένες ανταλλαγές μεταξύ δύο δρομολογητών θα αξιοποιήσουν το unicast.

2.3.3 Το πακέτο Hello

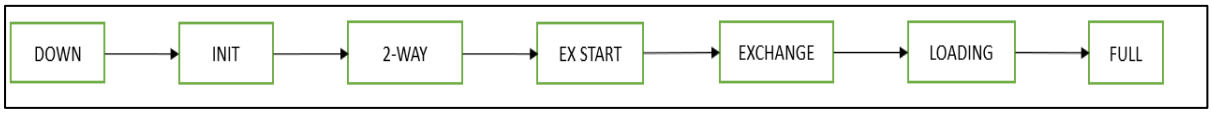
Προτού δύο δρομολογητές αρχίσουν να μιλούν για συνδέσμους, πρέπει να σχηματίσουν μια γειτονία, πολύ απλά να κατανοήσουν ότι είναι γείτονες και ότι έχουν τις ίδιες παραμέτρους OSPF. Οι δρομολογητές OSPF στέλνουν περιοδικά πακέτα Hello χρησιμοποιώντας τη διεύθυνση πολλαπλής διανομής «Όλοι οι δρομολογητές OSPF» για να δηλώσουν την ύπαρξη τους.

Εικόνα 2.8 Πακέτο Hello

Οι δρομολογητές τοποθετούν βασικές πληροφορίες για τον εαυτό τους στο πακέτο hello. Ο σκοπός αυτού είναι απλώς η ανακάλυψη νέων γειτόνων. Μόλις δύο δρομολογητές δουν (με πακέτα Hello) ότι είναι γείτονες, μπορούν να αρχίσουν να δημιουργούν μια γειτονία. Μόνο μετά από αυτό, θα αρχίσουν να ανταλλάσσουν λεπτομέρειες σχετικά με συνδέσμους. Για να γίνει όμως αυτό οι δρομολογητές πρέπει να περάσουν και από άλλες καταστάσεις.

2.3.4 Καταστάσεις OSPF

Δύο δρομολογητές θα πρέπει να περάσουν από 7 καταστάσεις για να συγκλίνουν. Οι 7 καταστάσεις είναι: Down, Init, 2-Way, ExStart, Exchange, Loading και Full.
Το διάγραμμα ροής για αυτές τις καταστάσεις είναι απλό: κάθε κατάσταση μπορεί να οδηγήσει μόνο στην επόμενη κατάσταση. Θεωρούμε ότι δύο δρομολογητές έχουν συγκλίνει μόνο όταν φτάσουν στην πλήρη κατάσταση. Οι καταστάσεις δεν αφορούν μόνο δρομολογητές. Υποδεικνύουν την κατάσταση ενός δρομολογητή προς έναν άλλο δρομολογητή. Ως αποτέλεσμα, ο ίδιος δρομολογητής μπορεί να βρίσκεται σε μια κατάσταση για τη σχέση με έναν δεύτερο δρομολογητή και σε διαφορετική κατάσταση για τη σχέση με έναν τρίτο δρομολογητή.



Εικόνα 2.9 Καταστάσεις OSPF

Οι καταστάσεις από το Down έως το 2-Way έχουν τον κύριο στόχο να σχηματίσουν μια γειτονιά. Μόλις σχηματίσουν τη γειτονία, οι καταστάσεις από το ExStart έως το Loading επιτρέπουν στους δύο δρομολογητές να μιλήσουν για συνδέσμους. Μόλις συμφωνήσουν στην τοπολογία, μετακινούνται στην κατάσταση FULL που αντιπροσωπεύει τη σύγκλιση. Κάτω είναι το αρχικό στάδιο, οι δρομολογητές απλώς δεν γνωρίζουν ο ένας για τον άλλον. Στην κατάσταση Init, ο δρομολογητής έχει λάβει ένα πακέτο Hello. Και οι δύο δρομολογητές πρέπει να μετακινηθούν σε αυτήν την κατάσταση πριν συνεχίσουν. Αυτό σημαίνει ότι κάθε δρομολογητής έχει δει το πακέτο Hello του άλλου. Μόλις και οι δύο δρομολογητές ακούσουν ο ένας τον άλλον, μετακινούνται στην κατάσταση 2-Way. Σε αυτήν την κατάσταση, έχουν δημιουργήσει μια αμφίδρομη επικοινωνία που μπορεί να χρησιμοποιηθεί για να μιλήσει για συνδέσμους. Το ExStart υποδεικνύει ότι οι δρομολογητές αρχίζουν να

ανταλλάσσουν πληροφορίες συνδέσμων. Στην κατάσταση Exchange, οι δρομολογητές στέλνουν ο ένας στον άλλο μια περίληψη της βάσης δεδομένων OSPF τους. Αυτό επιτρέπει στους άλλους δρομολογητές να έχουν μια ιδέα για τους συνδέσμους που γνωρίζει ο γείτονας Με την κατάσταση φόρτωσης, κάθε δρομολογητής ζητά από τον γείτονα λεπτομέρειες σχετικά με τις νέες συνδέσεις. Στην πραγματικότητα, με το προηγούμενο βήμα, ο δρομολογητής μπορεί να πει ποιες είναι οι συνδέσεις που δεν γνωρίζει (αλλά που γνωρίζει ο γείτονας). Με αυτό το βήμα, οι δύο δρομολογητές θα καταλήξουν να έχουν την ίδια βάση δεδομένων OSPF. Η κατάσταση Πλήρης υποδεικνύει ότι οι δύο δρομολογητές έχουν την ίδια βάση δεδομένων OSPF.

2.3.5 Το αναγνωριστικό του δρομολογητή

Για να αναγνωρίσουμε κάθε σύνδεσμο, πρέπει να αναγνωρίσουμε τους δύο δρομολογητές που σχηματίζουν τη σύνδεση. Για να το κάνουμε αυτό, δεν χρησιμοποιούμε το όνομα κεντρικού υπολογιστή. Δεν χρησιμοποιούμε καν τη διεύθυνση IP, καθώς κάθε δρομολογητής μπορεί να έχει πολλές από αυτές. Χρειαζόμαστε κάτι μοναδικό. Για να το πετύχουμε αυτό, δημιουργήθηκε το Router ID. Το Router ID είναι ένα αριθμητικό αναγνωριστικό 32-bit του δρομολογητή. Το αντιπροσωπεύουμε με διακεκομμένο συμβολισμό (X.X.X.X), όπως ακριβώς μια διεύθυνση IP. Ωστόσο, αυτή δεν είναι διεύθυνση IP. Όταν διαμορφώνουμε για πρώτη φορά το OSPF στο δρομολογητή μας, θα προσπαθήσει να δημιουργήσει μόνος του ένα αναγνωριστικό δρομολογητή.

2.3.6 Η βάση δεδομένων OSPF

Οι δρομολογητές διαθέτουν έναν χάρτη της τοπολογίας. Αυτή είναι η βάση δεδομένων OSPF, τεχνικά γνωστή ως Link State Database (LSDB). Κάθε κατάσταση σύνδεσης είναι μια σειρά που περιέχει τα αναγνωριστικά δρομολογητή των δύο δρομολογητών που αποτελούν τους συνδέσμους και ένα κόστος. Το κόστος υποδεικνύει πόσο κοστίζει να ακολουθήσουμε αυτό το σύνδεσμο. Προφανώς, όσο χαμηλότερο είναι το κόστος, τόσο το καλύτερο. Στην κατάσταση Exchange, οι δρομολογητές βλέπουν μια σύνοψη του LSDB του γείτονα. Αυτή η σύνοψη είναι γνωστή ως Περιγραφή Βάσης Δεδομένων (DBD) και είναι ένα συγκεκριμένο πακέτο OSPF που πρέπει να μεταδοθεί. Με βάση αυτό, αποφασίζουν για ποιες καταστάσεις σύνδεσης πρέπει να γνωρίζουν περισσότερες πληροφορίες. Στη συνέχεια, χρησιμοποιούν την κατάσταση φόρτωσης για να ανακτήσουν τέτοιες πληροφορίες. Σε αυτήν την κατάσταση, ο δρομολογητής που δεν έχει σύνδεσμο το ζητά με ένα μήνυμα αίτημα κατάστασης σύνδεσης

(LSR). Ο άλλος δρομολογητής θα απαντήσει με ένα μήνυμα διαφήμιση κατάστασης σύνδεσης (LSA). Όπως αναφέραμε το OSPF είναι πρωτόκολλο master-slave. Κατά την ανταλλαγή δεδομένων, ένας δρομολογητής ρωτά και ο άλλος απαντά. Δεν κάνουν και τα δύο πράγματα ταυτόχρονα, αλλά ανταλλάσσουν ρόλους μόλις τελειώσει το πρώτο.

2.3.7 Υπολογισμός του κόστους OSPF

Κάθε σύνδεσμος έχει ένα κόστος. Αυτό το κόστος βασίζεται αποκλειστικά στο εύρος ζώνης του συνδέσμου: όσο μεγαλύτερο είναι το εύρος ζώνης, τόσο χαμηλότερο είναι το κόστος. Συγκεκριμένα, το OSPF έχει την έννοια του εύρους ζώνης αναφοράς. Αυτό είναι το εύρος ζώνης για το οποίο θέλουμε να έχει κόστος 1 και από προεπιλογή είναι 100 Mbps. Δεδομένου ότι το κόστος είναι ακέραιος αριθμός , εάν έχουμε ταχύτερους συνδέσμους (όπως 1 Gbps), θα συνεχίσουν να κοστίζουν 1. Ωστόσο, η Cisco μάς επιτρέπει να αλλάξουμε το εύρος ζώνης αναφοράς για να ταιριάζει στις ανάγκες μας.

$$Cost = \frac{ReferenceBandwidth}{InterfaceBandwidth}$$

Εικόνα 2.10 Υπολογισμός Κόστους

Ο υπολογισμός του κόστους μιας σύνδεσης είναι απλός, είναι το εύρος ζώνης αναφοράς σε σχέση με το πραγματικό εύρος ζώνης. Ο υπολογισμός του κόστους μιας διαδρομής πολλαπλών συνδέσμων είναι επίσης απλός: είναι το άθροισμα του κόστους όλων των συνδέσμων στη διαδρομή. Όταν το OSPF παράγει δύο διαδρομές προς τον ίδιο προορισμό, αυτό με το χαμηλότερο κόστος θα μπει στον πίνακα δρομολόγησης.
Ο παρακάτω πίνακας δείχνει το κόστος που έχει κάθε σύνδεσμος, με βάση διαφορετικά εύρη ζώνης αναφοράς (100Mbps, 1Gbps και 10Gbps).

Link	Speed	100Mbps	1Gbps	10Gbps
Gigabit Ethernet	1Gbps	1	1	10
FastEthernet	100Mbps	1	10	100
Ethernet	10Mbps	10	100	1000

Εικόνα 2.11 Εύρος Ζώνης Αναφοράς και Κόστη

2.4 Στατική Και Δυναμική Δρομολόγηση

Στη στατική δρομολόγηση, οι διαδρομές δείχνουν τη διαδρομή μεταξύ δύο δρομολογητών που δεν μπορούν να ενημερωθούν αυτόματα. Η διαδρομή ενημερώνεται χειροκίνητα. Εάν οι αλλαγές συμβαίνουν στην πλευρά του δικτύου, πρέπει να ενημερώσουμε τη διαδρομή αλλαγής του πίνακα δρομολόγησης. Οι πίνακες δρομολόγησης είναι οι πίνακες που περιέχουν τις πληροφορίες δρομολόγησης. Η στατική δρομολόγηση είναι εύκολο να σχεδιαστεί και να εφαρμοστεί, καθώς δεν υπάρχει πολύπλοκη διαδρομή.

Στη δυναμική δρομολόγηση, οι δρομολογητές δείχνουν τη διαδρομή μεταξύ δύο δρομολογητών που μπορούν να ενημερώνονται αυτόματα. Εάν οι αλλαγές συμβαίνουν στην πλευρά του δικτύου οι διαδρομές δρομολόγησης θα ενημερωθούν αυτόματα. Όταν πραγματοποιούνται αλλαγές στο δίκτυο ο δρομολογητής ενημερώνει για τις αλλαγές και χρησιμοποιώντας τον αλγόριθμο δρομολόγησης οι διαδρομές, δρομολόγησης υπολογίζονται και ενημερώνονται στον πίνακα. Στον παρακάτω πίνακα φαίνονται οι κύριες διαφορές τους:

Τομέας	Στατική Δρομολόγηση	Δυναμική Δρομολόγηση
Τεχνική Ρύθμισης	Οι πίνακες δρομολόγησης ανανεώνονται χειροκίνητα	Οι πίνακες δρομολόγησης ανανεώνονται αυτόματα
Εύρος Ζώνης	Χρειάζεται λιγότερο εύρος ζώνης	Χρειάζεται περισσότερο εύρος ζώνης
Περιοχή Εφαρμογής	Μικρά Δίκτυα	Μεγάλα Δίκτυα
Πρωτόκολλα	Δεν χρησιμοποιεί πρωτόκολλα	Χρησιμοποιεί πρωτόκολλα όπως RIP,EIGRP,OSPF
Αλγόριθμοι	Δεν χρησιμοποιεί περίπλοκους αλγορίθμους	Χρησιμοποιεί περίπλοκους αλγορίθμους
Ασφάλεια	Υψηλή ασφάλεια	Χαμηλή ασφάλεια

Εικόνα 2.12Διαφορές Δυναμικής Και Στατικής Δρομολόγησης

2.5 APPENDIX 1: Εντολές Συσκευών Αρχικού Δικτύου

Στο συγκεκριμένο appendix έχουμε βάλει τις εντολές που έχουν χρησιμοποιηθεί στο αρχικό δίκτυο της εταιρείας και πιο συγκεκριμένα στους δρομολογητές.

CISCO IOSV ROUTER 1

```
#hostname R1
#ip name-server 8.8.8.8
#interface GigabitEthernet0/0
#ip address dhcp
#ip nat outside
#interface GigabitEthernet0/1
#ip address 192.168.1.1 255.255.255.0
#ip nat inside
#interface GigabitEthernet0/2
#ip address 192.168.11.1 255.255.255.0
#ip nat inside
#interface GigabitEthernet0/3
#no ip address
#router ospf 10
#network 192.168.1.0 0.0.0.3 area 1
#network 192.168.11.0 0.0.0.3 area 1
#ip nat inside source list 1 interface GigabitEthernet0/0 overload
#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 dhcp
#access-list i permit any
```

CISCO IOSV ROUTER 2

```
#hostname R2
#ip name-server 8.8.8.8
#interface GigabitEthernet0/0
#no ip address
#shutdown
#interface GigabitEthernet0/1
#ip address 192.168.1.2 255.255.255.0
#interface GigabitEthernet0/2
#ip address 192.168.2.1 255.255.255.0
#interface GigabitEthernet0/3
#ip address 192.168.3.1 255.255.255.0
#router ospf 10
#network 192.168.1.0 0.0.0.3 area 1
#network 192.168.2.0 0.0.0.3 area 1
#network 192.168.3.0 0.0.0.3 area 1
#network 192.168.8.0 0.0.0.3 area 1
#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

CISCO IOSV ROUTER 3

```
#hostname R3
#ip name-server 8.8.8.8
#interface GigabitEthernet0/0
#no ip address
#shutdown
#interface GigabitEthernet0/1
#ip address 192.168.5.1 255.255.255.0
#interface GigabitEthernet0/2
#no ip address
#shutdown
#interface GigabitEthernet0/3
#ip address 192.168.3.2 255.255.255.0
#router ospf 10
#network 192.168.3.0 0.0.0.3 area 1
#network 192.168.5.0 0.0.0.255 area 1
#ip route 0.0.0.0 0.0.0.0 192.168.3.1
```

CISCO IOSV ROUTER 4

```
#hostname R4
#ip name-server 8.8.8.8
#interface GigabitEthernet0/0
#no ip address
#shutdown
#interface GigabitEthernet0/1
#ip address 192.168.4.1 255.255.255.0
#interface GigabitEthernet0/2
#ip address 192.168.2.2 255.255.255.0
#interface GigabitEthernet0/3
#no ip address
#shutdown
#router ospf 10
#network 192.168.2.0 0.0.0.3 area 1
#network 192.168.4.0 0.0.0.255 area 1
#ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

CISCO IOSV ROUTER 5

```
#hostname R5
#ip name-server 8.8.8.8
#interface FastEthernet0/0
#ip address 192.168.6.1 255.255.255.0
#interface FastEthernet0/1
#ip address 192.168.4.2 255.255.255.0
#router ospf 10
#network 192.168.4.0 0.0.0.3 area 1
#network 192.168.6.0 0.0.0.255 area 1
#ip route 0.0.0.0 0.0.0.0 192.168.4.1
#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 04
#login
#end
```

CISCO IOSV ROUTER 6

```
#no service password-encryption
#hostname R6
#ip name-server 8.8.8.8
#interface FastEthernet0/0
#ip address 192.168.7.1 255.255.255.0
#interface FastEthernet0/1
#ip address 192.168.5.2 255.255.255.0
#interface FastEthernet1/0
#interface FastEthernet1/1
#interface FastEthernet1/2
#interface FastEthernet1/3
#interface FastEthernet1/4
#interface FastEthernet1/5
#interface FastEthernet1/6
#interface FastEthernet1/7
#interface FastEthernet1/8
#interface FastEthernet1/9
#interface FastEthernet1/10
#interface FastEthernet1/11
#interface FastEthernet1/12
#interface FastEthernet1/13
#interface FastEthernet1/14
#interface FastEthernet1/15
#interface vlan1
#no ip address
#router ospf 10
#network 192.168.5.0 0.0.0.3 area 1
#network 192.168.7.0 0.0.0.255 area 1
#ip route 0.0.0.0 0.0.0.0 192.168.5.1
```

CISCO IOSV ROUTER 7

```
#no service password-encryption
#hostname R7
#ip name-server 8.8.8.8
#interface GigabitEthernet0/0
#ip address 192.168.7.2 255.255.255.0
#interface GigabitEthernet0/1
#ip address 192.168.6.2 255.255.255.0
#interface GigabitEthernet0/2
#ip address 192.168.8.1 255.255.255.0
#interface GigabitEthernet0/3
#ip address 192.168.9.1 255.255.255.0
#router ospf 10
#network 192.168.6.0 0.0.0.3 area 1
#network 192.168.7.0 0.0.0.3 area 1
#network 192.168.8.0 0.0.0.3 area 1
#network 192.168.9.0 0.0.0.3 area 1
#ip route 0.0.0.0 0.0.0.0 192.168.6.1
#ip route 0.0.0.0 0.0.0.0 192.168.7.1
```

ΚΕΦΑΛΑΙΟ 3 : Σχεδιαστική Βελτίωση και Επέκταση Δικτύου

3.1 Εισαγωγή

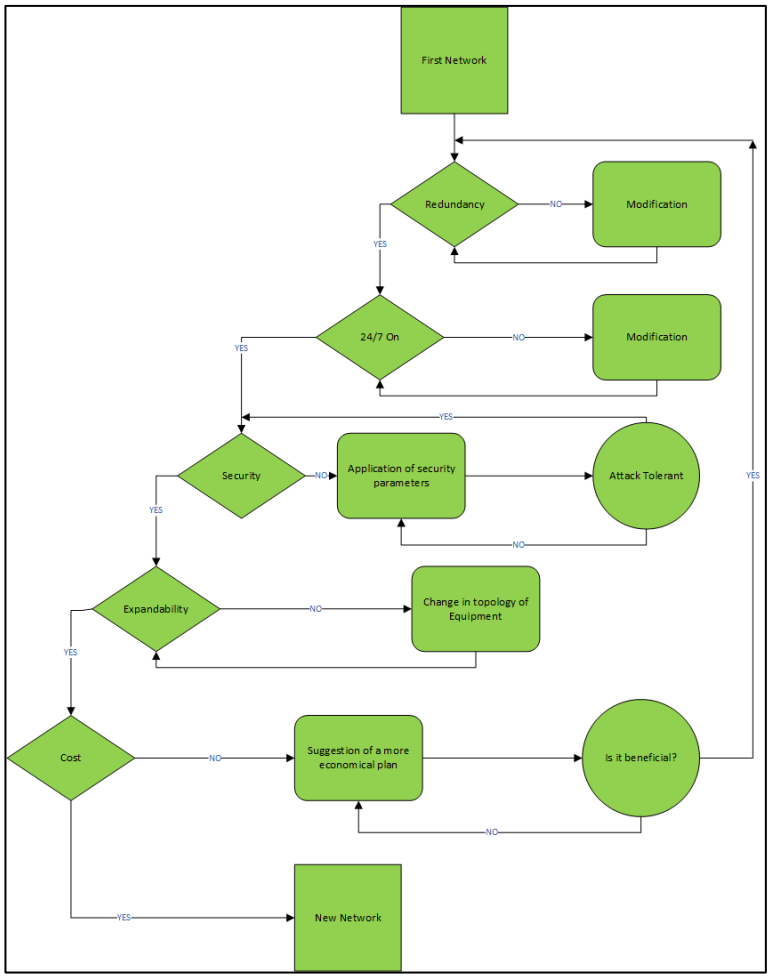
Στόχος αυτού του κεφαλαίου είναι να δείξουμε καλύτερες προσεγγίσεις σε τοπολογίες δικτύων και πιο συγκεκριμένα στην τοπολογία της εταιρείας μας , για την καλύτερη και πιο ομαλή λειτουργία του δικτύου. Το δίκτυο που παρουσιάζεται σε αυτό το κεφάλαιο αφορά μια διαφορετική προοπτική η οποία στοχεύει κυρίως στο κομμάτι του redundancy. Η διαμόρφωση του νέου δικτύου εξασφαλίζει ότι μπορεί να καλύψει οποιαδήποτε ζημιά στις συσκευές του δικτύου ακόμα και σε πολλαπλές συσκευές. Γίνεται παρουσίαση μιας ενναλακτικής πάνω στο αρχικό δίκτυο η οποία αφορά αρκετές τροποποιήσεις όπως για παράδειγμα σύνδεση σε δυο παρόχους καθώς πολλές φορές όσο καλά και να είναι στημένο το δίκτυο αν υπάρξει πρόβλημα στον πάροχο τότε η εταιρεία έχει άμεσα πρόβλημα και αυτή και κάποιες εταιρείες όπως η εταιρεία που παρουσιάζεται δεν έχουν την πολυτέλεια να μην εξυπηρετούν τους πελάτες τους για μεγάλο χρονικό διάστημα οπότε χρειάζονται μια αντίστοιχη λύση. Βέβαια αυτό επηρεάζει το κόστος που αφορά είτε τα έξοδα σε δυο παρόχους πλέον ή ακόμα και για καινούργιο εξοπλισμό αλλά πολλές εταιρείες είναι αυτές που προτιμούν την συνδεσιμότητα έναντι του κόστους και το να παρέχουν τις υπηρεσίες τους χωρίς να υπάρξει διακοπή λειτουργίας. Έτσι λοιπόν η εταιρεία λόγο εξέλιξης χρειαζόταν ένα πιο οργανωμένο πλάνο διαχείρισης του δικτύου και των συσκευών. Στο προηγούμενο κεφάλαιο παρουσιάστηκε το αρχικό δίκτυο και τι τεχνολογίες υποστηρίζει. Σε αυτό το κεφάλαιο παρουσιάζονται αναλυτικά οι αλλαγές που προκύπτουν στο δίκτυο ώστε να μετατραπεί στην τελική του μορφή, με περισσότερες και νέες τεχνολογίες . Παρουσιάζονται επίσης σενάρια τα οποία οδηγούν σε τροποποιήσεις του δικτύου. Η εταιρεία εξελίχθηκε και χρειάζεται νέα διαμόρφωση στην τοπολογία διότι προσέλαβε περισσότερο προσωπικό, τοποθετήθηκαν περισσότεροι διακομιστές και αναβάθμισε το Data Center της .Στην αρχική κατασκευή του δικτύου δεν λήφθηκαν υπόψη σημαντικοί παράγοντες: Redundancy, Ασφάλεια, συνεχής συνδεσιμότητα και επεκτασιμότητα και όλο αυτό σε συνδυασμό με κάποιο οικονομικό πλάνο.

3.2 Διάγραμμα Τροποποιήσεων

Για να στήσουμε ένα δίκτυο θα πρέπει να λάβουμε κάποιους παράγοντες.

1) Redundancy
2) 24/7 on
3) Security
4) Expandability
5) Cost

Κάθε αλλαγή στο δίκτυο αιτιολογείται στο παρακάτω διάγραμμα:



Εικόνα 3.1 Διάγραμμα Τροποποιήσεων

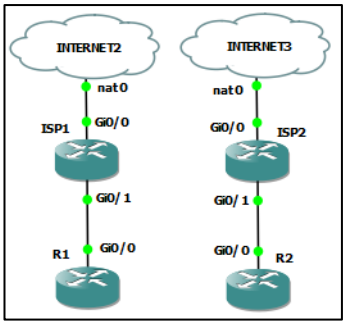
3.3 Αλλαγές Δικτύου Για Αντιμετώπιση Προβλημάτων

Παρόλο που υπάρχει το πρωτόκολλο OSPF μπορεί κανείς να δει ότι δεν μπορεί να υποστηρίξει προβλήματα που αφορούν συγκεκριμένες συσκευές. Για παράδειγμα να καλύψει

μια ζημιά στα Router 4 - Router 5 ή κάποια ζημιά στα Router 3 - Router 6 , αν τα Router 1, Router 2 και Router 7 πάθουν κάτι τότε το δίκτυο θα πέσει πράγμα που προσπαθούμε να αποφύγουμε στο νέο δίκτυο ή στην χειρότερη να το ελαττώσουμε. Η αλλαγή αυτή θα πραγματοποιηθεί με κύριο στόχο ένα καλό και αποδοτικό redundancy.

3.3.1 Αλλαγές Στο Μέρος Των Δρομολογητών

Παρακολουθώντας το διάγραμμα παρατηρούμε ότι ο πρώτος κόμβος είναι το redundancy. Όπως αναφέραμε και σε προηγούμενο κεφάλαιο το αρχικό δίκτυο χρησιμοποιεί το πρωτόκολλο OSPF και παράλληλα έχει μια εναλλακτική ώστε να συνεχίσει να παρέχει υπηρεσίες το δίκτυο αν κάποιες συσκευές βγουν εκτός. Αυτό όμως δεν συμβαίνει για όλες τις συσκευές οπότε πρώτος στόχος στο νέο δίκτυο θα είναι να αξιοποιήσουμε redundant links. Έτσι λοιπόν η νέα πρόταση μπορεί να υποστηρίξει ζημιά από οποιαδήποτε συσκευή ακόμα και σε πιο ειδικές περιπτώσεις να καλύψει και παραπάνω από μια συσκευές αν πάθουν κάποια ζημιά. Το πρώτο σκέλος αφορά τον πάροχο. Το αρχικό δίκτυο συνδέεται σε ένα πάροχο. Όσο καλά και να είναι σχεδιασμένο το δίκτυο αν ο πάροχος αντιμετωπίσει πρόβλημα τότε το δίκτυο μας θα έχει πρόβλημα και αυτό. Έτσι λοιπόν μιας και που ο ρόλος της εταιρείας είναι η συνεχής παροχή υπηρεσιών χωρίς εξαιρέσεις η πρώτη αλλαγή θα είναι να ,επεκταθεί το δίκτυο και σε δεύτερο πάροχο. έτσι ώστε αν ο πάροχος αντιμετωπίσει κάποιο πρόβλημα η εταιρεία να συνεχίσει να έχει πρόσβαση στο δίκτυο μέσω του εφεδρικού παρόχου. Με δυο παρόχους έχουμε εξασφαλίσει ότι το πρόβλημα σε έναν πάροχο δεν θα δημιουργήσει πρόβλημα στην εταιρεία μας. Το NAT node appliance αποτελεί το ίντερνετ ενώ οι πάροχοι πλέον αναπαρίστανται με δυο router ISP1-ISP2 για να είναι πιο ρεαλιστική η τοπολογία με βάση τα δίκτυα υπολογιστών σε πραγματικές συνθήκες . Τι συμβαίνει όμως όταν το αρχικό μας router πάθει κάποια ζημιά? Ακόμα και δύο πάροχοι να είναι συνδεδεμένοι στο Router άμα αυτό πέσει χάνουμε τη συνδεσιμότητα. Έτσι λοιπόν εγκαθιστούμε ένα δεύτερο Router στην αρχή έτσι ώστε ο ένας πάροχος να παρέχει συνδεσιμότητα μέσω του ενός Router και ο δεύτερος μέσω του νέου. Άρα όποιο από τα δυο Router πάθει ζημιά η σύνδεση παραμένει. Στο παρακάτω σχήμα φαίνεται πως διαμορφώνεται το πρώτο κομμάτι του δικτύου.



Εικόνα 3.2 Τοπολογία Δύο Παρόχων

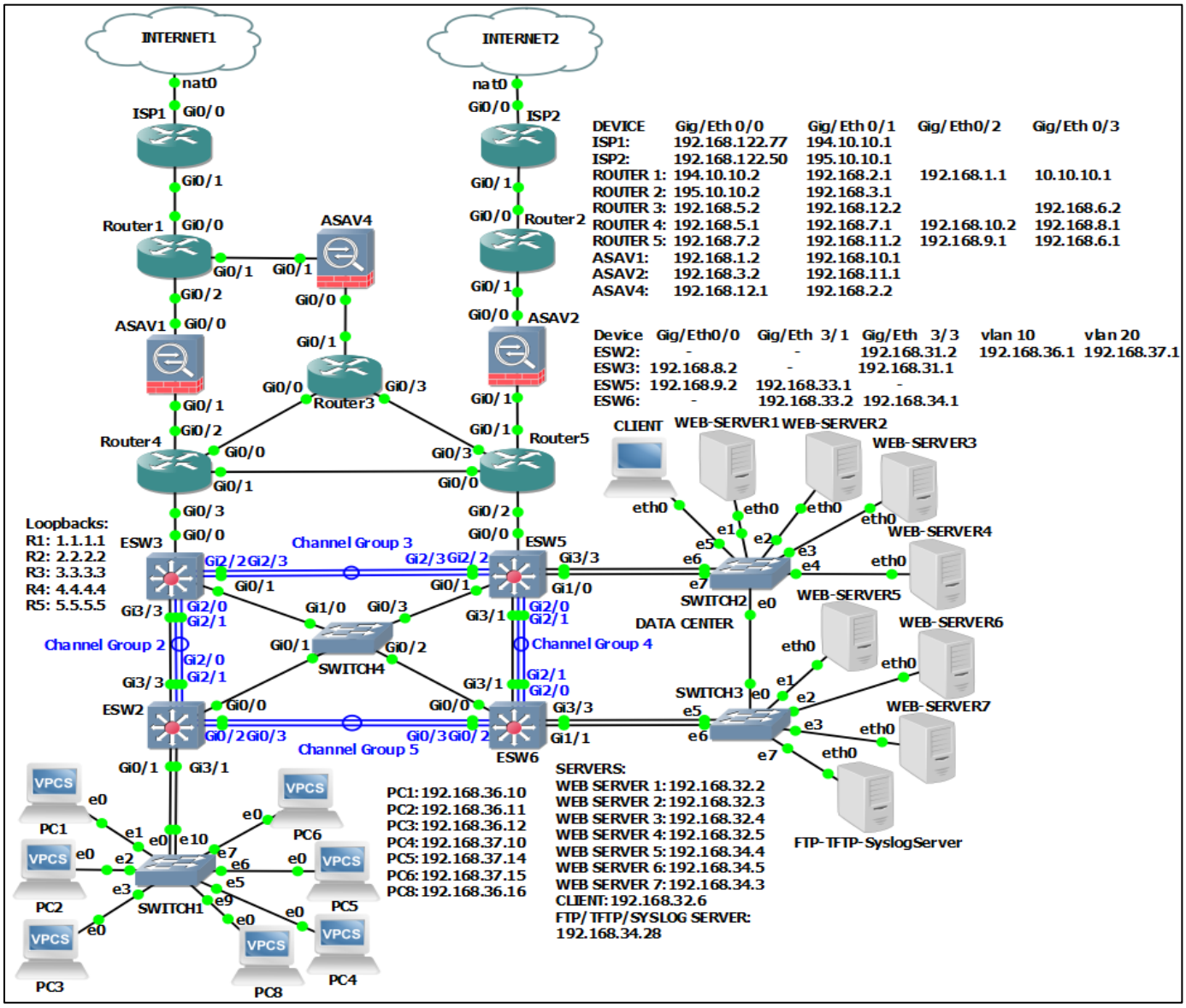
Μετά την αναβάθμιση των Router πρώτον στο κομμάτι της τοπολογίας από θέμα συνδεσιμότητας και δεύτερον αναβάθμιση της ίδιας της συσκευής με νέο Router, έχουν τοποθετηθεί τα firewall για τα οποία θα μιλήσουμε σε επόμενο κεφάλαιο. Τα Router μειώθηκαν από 7 σε 5 παρόλα αυτά έχουν τοποθετηθεί καταλληλά και με καλύτερη διάταξη ώστε να προσφέρουν στο δίκτυο εναλλακτικές σε περίπτωση βλάβης. Αφαιρέθηκαν τα 3725 Router και τοποθετήθηκαν IOSv διότι τα ports τους δεν ήταν καταλληλά για gigabit Ethernet συνδεσιμότητα και δημιουργούσαν θέματα στο επίπεδο 3. Στο κομμάτι της δρομολόγησης διατηρήσαμε σαν δυναμικό πρωτόκολλο το OSPF δίνοντας του βέβαια περισσότερες επιλογές ανάκαμψης, διότι είναι το ιδανικό πρωτόκολλο για να καλύψει τις απαιτήσεις της εταιρείας.

3.3.2 Αλλαγές Στο Μέρος Των Μεταγωγών

Μαζί με τα αρχικά switch τοποθετήθηκαν και switch επιπέδου 3 τα οποία όπως θα δούμε παρακάτω θα αποτελέσουν τα core και distribution επίπεδα του δικτύου.. Αυξήθηκε το πλήθος των switch επιπέδου 2 διότι έχουμε διαχωρισμό στα 3 επίπεδα access-distribution-core και το κάθε switch είναι για ξεχωριστή χρήση. Το πλήθος τους δείχνει ότι έχει γίνει καλή δουλειά στο κομμάτι του redundancy ώστε να παρέχονται αρκετά μονοπάτια σαν εναλλακτικές.. Εκτός από αυτά που εξυπηρετούν την δρομολόγηση και την κάλυψη βλαβών υπάρχουν αυτά που ανήκουν στο επίπεδο Access τα οποία πλέον έχουν το δικό τους ρόλο. Υπάρχει το Switch 1 το οποίο είναι αποκλειστικά για τους προγραμματιστές. Αυτό αφορά είτε τους παλιούς είτε τους νέους προγραμματιστές αλλά παρόλο που είναι στο ίδιο switch ανήκουν σε διαφορετικά VLAN. Υπάρχει το Switch2 το οποίο είναι εφεδρικό, σε περίπτωση κάποιας ζημιάς. Τα υπόλοιπα δύο, Switch3 και Switch4 αφορούν το Data Center και είναι αποκλειστικά για τους διαφορετικούς διακομιστές. Το data center ενώ μεγάλωσε χωρίστηκε σε δυο μέρη με διαφορετικά switch σαν τελευταίο μέτρο redundancy ώστε αν δημιουργηθεί

σοβαρό θέμα στα switch στο Access layer του δικτύου με αρκετές συσκευές χαμένες να ελαττωθούν σε νούμερο οι πελάτες οι οποίοι έχουν πρόβλημα.

3.4 Παρουσίαση Τεχνολογιών Νέου Δικτύου



Εικόνα 3.3 Τοπολογία Νέου Δικτύου Εταιρείας

3.4.1 Πρωτόκολλο VLAN

Ένα πρωτόκολλο που χρησιμοποιήθηκε στο νέο δίκτυο είναι το VLAN. Σε ένα VLAN οι υπολογιστές ,οι διακομιστές και άλλες δικτυακές συσκευές είναι λογικά συνδεδεμένες μεταξύ τους ανεξάρτητα από την φυσική τους τοποθεσία.

Οι λόγοι του να στηθούν VLAN είναι οι εξής :

- Βελτιωμένη ασφάλεια

- Διαχείριση κυκλοφορίας
- Πιο απλό δίκτυο

Ένα VLAN είναι μια συλλογή συσκευών ή κόμβων δικτύου που επικοινωνούν μεταξύ τους σαν να αποτελούν ένα ενιαίο LAN, ενώ στην πραγματικότητα υπάρχουν σε ένα ή περισσότερα τμήματα LAN. Κάθε τμήμα διαχωρίζεται από το υπόλοιπο LAN με ένα δρομολογητή ή μεταγωγό και συνήθως χρησιμοποιείται για ένα συγκεκριμένο τμήμα, έτσι, όταν ένας σταθμός εργασίας εκπέμπει πακέτα, αυτά φτάνουν σε όλους τους άλλους σταθμούς εργασίας στο VLAN αλλά σε κανέναν εκτός αυτού. Όταν δύο σταθμοί εργασίας στέλνουν πακέτα δεδομένων ταυτόχρονα σε ένα LAN συνδεδεμένο μέσω ενός διανομέα, τα δεδομένα συγκρούονται και δεν μεταδίδονται σωστά. Η σύγκρουση διαδίδεται σε ολόκληρο το δίκτυο, πράγμα που σημαίνει ότι το LAN είναι απασχολημένο και απαιτεί από τους χρήστες να περιμένουν έως ότου η σύγκρουση μεταφερθεί πλήρως σε όλο το δίκτυο προτού να λειτουργήσει ξανά οπότε τα αρχικά δεδομένα πρέπει να σταλούν εκ νέου. Τα VLAN μειώνουν τη συχνότητα συγκρούσεων και μειώνουν τον αριθμό των πόρων του δικτύου που σπαταλούνται λειτουργώντας ως τμήματα LAN. Τα πακέτα δεδομένων που αποστέλλονται από έναν σταθμό εργασίας σε ένα τμήμα μεταφέρονται από μια γέφυρα ή μεταγωγέα, τα οποία δεν θα προωθήσουν τις συγκρούσεις, αλλά θα στείλουν σε εκπομπές σε κάθε συσκευή δικτύου. Για αυτόν τον λόγο, τα τμήματα ονομάζονται "τομείς σύγκρουσης" επειδή περιέχουν συγκρούσεις εντός των ορίων αυτής της ενότητας. Ωστόσο, τα VLAN έχουν περισσότερη λειτουργικότητα ακόμη και από ένα τμήμα LAN επειδή επιτρέπουν αυξημένη ασφάλεια δεδομένων. Πολλοί οργανισμοί διαθέτουν WAN λόγω των εκτεταμένων γραφείων και των μεγάλων ομάδων τους. Σε αυτά τα σενάρια, η ύπαρξη πολλαπλών VLAN θα επιταχύνει σημαντικά τις λειτουργίες του δικτύου. Τα VLAN διαμορφώνονται συνήθως σε μεταγωγείς τοποθετώντας ορισμένες διεπαφές σε έναν τομέα εκπομπής και ορισμένες διεπαφές σε έναν άλλο. Ακολουθούν οι κύριοι λόγοι για τους οποίους χρησιμοποιούνται τα VLAN:

- Τα VLAN αυξάνουν τον αριθμό των τομέων εκπομπής ενώ μειώνουν το μέγεθός τους.
- Τα VLAN μειώνουν τους κινδύνους ασφαλείας μειώνοντας τον αριθμό των κεντρικών υπολογιστών που λαμβάνουν αντίγραφα πλαισίων που πλημμυρίζουν τους μεταγωγείς.
- Μπορούμε να διατηρήσουμε κεντρικούς υπολογιστές που διατηρούν ευαίσθητα δεδομένα σε ξεχωριστό VLAN για να βελτιωθεί η ασφάλεια.
- Μπορούμε να δημιουργήσουμε πιο ευέλικτα σχέδια δικτύου που ομαδοποιούν τους χρήστες ανά τμήμα αντί για φυσική τοποθεσία.

- Οι αλλαγές δικτύου επιτυγχάνονται με ευκολία διαμορφώνοντας απλώς μια θύρα στο κατάλληλο VLAN.

Οι προγραμματιστές που ήταν στην εταιρεία εξαρχής ανήκουν στο VLAN 10 ένα VLAN το οποίο έχει πρόσβαση σε όλο το δίκτυο εκτός του DMZ, μιας ζώνης που θα παρουσιαστεί στο κεφάλαιο 4. Το Data Center ανήκει στο VLAN 10 έτσι μόνο οι χρήστες που ανήκουν σε αυτό το VLAN έχουν πρόσβαση στους διακομιστές. Οι νέοι προγραμματιστές τοποθετήθηκαν στο VLAN 20 το οποίο έχει περιορισμένη πρόσβαση στο δίκτυο. Τέλος το DMZ ανήκει στο VLAN 30 το οποίο είναι ανεξάρτητο του υπολοίπου δικτύου.

3.4.2 Δρομολόγηση Inter-VLAN

Μια νέα τεχνολογία που χρησιμοποιείται στο δίκτυο μας είναι το Inter VLAN. Τα VLAN χρησιμοποιούνται για την τμηματοποίηση δικτύων επιπέδου 2 με μεταγωγή για διάφορους λόγους. Ανεξάρτητα από τον λόγο, οι κεντρικοί υπολογιστές σε ένα VLAN δεν μπορούν να επικοινωνήσουν με κεντρικούς υπολογιστές σε άλλο VLAN εκτός εάν υπάρχει ένας δρομολογητής ή ένας διακόπτης επιπέδου 3 για την παροχή υπηρεσιών δρομολόγησης. Η δρομολόγηση Inter-VLAN είναι η διαδικασία προώθησης της κυκλοφορίας δικτύου από ένα VLAN σε άλλο VLAN. Όπως αναφέραμε το δίκτυο μας χρησιμοποιεί 3 VLAN εκ των οποίων οι υπολογιστές που βρίσκονται στα δυο εσωτερικά του δικτύου (VLAN 10- VLAN 20) θα πρέπει να επικοινωνούν μεταξύ τους. Για να ελέγξουμε ότι η τεχνολογία αυτή λειτουργεί, στο ESW2 το οποίο είναι ένα Layer 3 Switch θα χρησιμοποιήσουμε το SVI (switched virtual interface) το οποίο είναι μια εικονική διεπαφή και θα δοκιμάσουμε με Ping μεταξύ των PC1 και PC6 τα οποία ανήκουν σε διαφορετικά VLAN.

```
PC1> ping 192.168.37.15

84 bytes from 192.168.37.15 icmp_seq=1 ttl=63 time=5.858 ms
84 bytes from 192.168.37.15 icmp_seq=2 ttl=63 time=7.661 ms
84 bytes from 192.168.37.15 icmp_seq=3 ttl=63 time=13.196 ms
84 bytes from 192.168.37.15 icmp_seq=4 ttl=63 time=9.474 ms
84 bytes from 192.168.37.15 icmp_seq=5 ttl=63 time=8.101 ms
```

Εικόνα 3.4 Εντολη Ping από PC1 σε PC6

3.4.3 Διεύθυνση Loopback

Η διεύθυνση αυτή μπορεί να χρησιμοποιηθεί για την εκτέλεση μιας υπηρεσίας δικτύου σε έναν κεντρικό υπολογιστή χωρίς να απαιτείται φυσική διεπαφή δικτύου ή χωρίς να καθίσταται η υπηρεσία προσβάσιμη από δίκτυα με τα οποία δημιουργεί σύνδεση ο υπολογιστής. Το όνομα

localhost συνήθως επιλύεται στη διεύθυνση βρόχου IPv4 127.0.0.1 και στη διεύθυνση βρόχου IPv6 ::1. Στο νέο δίκτυο λοιπόν οι δρομολογητές έχουν ρυθμιστεί να έχουν και διεύθυνση loopback

3.4.4 Τεχνολογία Etherchannel

Σημαντική αλλαγή για το δίκτυο είναι και η προσθήκη μιας τεχνολογίας που μας εξυπηρετεί στο redundancy, το Etherchannel. Η τεχνολογία EtherChannel είναι μια τεχνολογία ομαδοποίησης συνδέσμων που καθιστά δυνατό τον συνδυασμό πολλών φυσικών συνδέσεων μεταξύ μεταγωγών σε μία λογική σύνδεση για την παροχή συνδέσεων υψηλής ταχύτητας και πλεονασμού. Δημιουργήθηκε με δύο πρωτόκολλα, το πρωτόκολλο συνάθροισης θυρών (PAgp) και το πρωτόκολλο ελέγχου συνάθροισης συνδέσεων (LACP) .

- Πρωτόκολλο συγκέντρωσης θυρών (PAgp)

Το πρωτόκολλο συνάθροισης θυρών (PAgp) είναι ένα πρωτόκολλο που βασίζεται σε τεχνολογία Cisco και εκτελείται σε μεταγωγείς με άδεια προμηθευτή που υποστηρίζουν PAgp. Διευκολύνει την αυτόματη δημιουργία συνδέσμων καναλιών αιθέρα ανιχνεύοντας τη διαμόρφωση συνδέσμων σε κάθε πλευρά και διασφαλίζοντας ότι οι σύνδεσμοι είναι συμβατοί για το σχηματισμό μιας σύνδεσης καναλιού αιθέρα. Στον παρακάτω πίνακα βλέπουμε το αποτέλεσμα σύνδεσης μεταξύ δυο μεταγωγών ανάλογα με ποιον τρόπο έχουν ρυθμιστεί.

Switch 1 mode	Switch 2 mode	Etherchannel Formation
On	On	Yes
On	Desirable or Auto	No
Desirable	Desirable or Auto	Yes
Auto	Desirable	Yes
Auto	Auto	No

Εικόνα 3.5 Λειτουργίες Πρωτοκόλλου PAgp

- Πρωτόκολλο ελέγχου συγκέντρωσης συνδέσμων (LACP)

Το πρωτόκολλο ελέγχου συνάθροισης συνδέσμων (LACP) είναι όπως το πρωτόκολλο PAgp, αλλά είναι ένα ανοιχτό τυπικό πρωτόκολλο και διευκολύνει τη διαμόρφωση των καναλιών αιθέρα σε περιβάλλοντα πολλών προμηθευτών. Δεν περιορίζεται μόνο στους μεταγωγείς Cisco. Επιτρέπει τόσο ενεργούς συνδέσμους όσο και συνδέσμους αναμονής. Ο

παρακάτω πίνακας δείχνει διάφορους συνδυασμούς λειτουργιών και αν αυτοί δημιουργούν σύνδεση.

Switch 1 mode	Switch 2 mode	Etherchannel Formation
On	On	Yes
On	Active or Passive	No
Active	Active or Passive	Yes
Passive	Active	Yes
Passive	Passive	No

Εικόνα 3.6 Λειτουργίες Πρωτοκόλλου LACP

3.4.5 Κανάλι θύρας ή Port Channel

Μια ομάδα καναλιών θύρας είναι μια ομαδοποίηση πολλαπλών φυσικών διεπαφών για το σχηματισμό μιας λογικής διεπαφής. Ένα κανάλι θύρας δεσμεύει έως και τέσσερις μεμονωμένες διεπαφές σε μια ομάδα για να παρέχει αυξημένο εύρος ζώνης και πλεονασμό. Η φόρτωση θύρας εξισορροπεί επίσης την κυκλοφορία σε αυτές τις φυσικές διεπαφές. Το κανάλι θύρας παραμένει λειτουργικό για όσο διάστημα λειτουργεί τουλάχιστον μία φυσική διεπαφή εντός του καναλιού θύρας. Η τεχνολογία αυτή έχει χρησιμοποιηθεί 4 φορές στο δίκτυο μας στις εξής συσκευές:

Port Channel 2: ESW3-ESW2

Port Channel 3: ESW3-ESW5

Port Channel 4: ESW5-ESW6

Port Channel 5: ESW2-ESW6

3.4.6 Network address translation (NAT)

Το ROUTER 1 χρησιμοποιεί την τεχνολογία Network Address Translation ώστε να μετατρέψει την δημόσια διεύθυνση IP σε ιδιωτική. Αυτό γίνεται διότι με αυτόν τον τρόπο δεν γίνεται γνωστή η IP των υπολογιστών των ατόμων που εργάζονται στην εταιρεία από άτομα που μπορούν να την χρησιμοποιήσουν ώστε να κάνουν ζημιά κυρίως στο δίκτυο αλλά και στους υπολογιστές των εργαζομένων. Η μετάφραση διευθύνσεων δικτύου (NAT) είναι μια μέθοδος αντιστοίχισης ενός χώρου διευθύνσεων IP σε έναν άλλο, τροποποιώντας τις πληροφορίες διεύθυνσης δικτύου στην κεφαλίδα IP των πακέτων ενώ αυτά βρίσκονται σε διαμετακόμιση μέσω μιας συσκευής δρομολόγησης κυκλοφορίας. Η τεχνική χρησιμοποιήθηκε αρχικά για να αποφευχθεί η ανάγκη εκχώρησης μιας νέας διεύθυνσης σε κάθε κεντρικό

υπολογιστή κατά τη μετακίνηση ενός δικτύου ή κατά την αντικατάσταση του παρόχου υπηρεσιών διαδικτύου στο upstream, αλλά δεν ήταν δυνατή η δρομολόγηση του χώρου διευθύνσεων του δικτύου. Καθώς η μετάφραση διευθύνσεων δικτύου τροποποιεί τις πληροφορίες διεύθυνσης IP στα πακέτα, οι υλοποιήσεις NAT ενδέχεται να διαφέρουν ως προς τη συγκεκριμένη συμπεριφορά τους σε διάφορες περιπτώσεις διευθυνσιοδότησης και την επίδρασή τους στην κυκλοφορία του δικτύου. Υπάρχουν 3 τύποι NAT:

- Το στατικό NAT

Σε αυτό, μια μεμονωμένη ιδιωτική διεύθυνση IP αντιστοιχίζεται με μία μόνο δημόσια διεύθυνση IP, δηλαδή μια ιδιωτική διεύθυνση IP μεταφράζεται σε μια δημόσια διεύθυνση IP. Χρησιμοποιείται στη φιλοξενία Ιστού.

- Το δυναμικό NAT

Σε αυτόν τον τύπο NAT, πολλαπλές ιδιωτικές διευθύνσεις IP αντιστοιχίζονται σε μια ομάδα δημόσιων διευθύνσεων IP. Χρησιμοποιείται όταν γνωρίζουμε τον αριθμό των σταθερών χρηστών που θέλουν να έχουν πρόσβαση στο διαδίκτυο σε μια δεδομένη χρονική στιγμή.

- Τη μετάφραση διεύθυνσης θύρας PAT

Αυτό είναι επίσης γνωστό ως υπερφόρτωση NAT. Σε αυτό, πολλές τοπικές ιδιωτικές διευθύνσεις IP μπορούν να μεταφραστούν σε μία μόνο δημόσια διεύθυνση IP. Οι αριθμοί θύρας χρησιμοποιούνται για τη διάκριση της κίνησης, δηλαδή ποια κίνηση ανήκει σε ποια διεύθυνση IP. Χρησιμοποιείται πιο συχνά, καθώς είναι οικονομικά αποδοτικό, καθώς χιλιάδες χρήστες μπορούν να συνδεθούν στο διαδίκτυο χρησιμοποιώντας μόνο μία πραγματική δημόσια διεύθυνση IP.

Το πρωτόκολλο αυτό όσο αφορά το κομμάτι της ασφάλειας:

-Αποκρύπτει τη διεύθυνση IP οποιωνδήποτε συσκευών στο δίκτυό μας από τον έξω κόσμο, δίνοντάς τους όλες μια ενιαία διεύθυνση.

-Απαιτεί κάθε εισερχόμενο πακέτο πληροφοριών να έχει ζητηθεί από μια συσκευή. Εάν ένα κακόβουλο πακέτο δεδομένων δεν περιλαμβάνεται στη λίστα των αναμενόμενων επικοινωνιών, απορρίπτεται.

-Ορισμένα τείχη προστασίας μπορούν να χρησιμοποιήσουν τη λίστα επιτρεπόμενων για τον αποκλεισμό της μη εξουσιοδοτημένης εξερχόμενης κυκλοφορίας, επομένως, εάν συνάψουμε ένα κακόβουλο λογισμικό, το τείχος προστασίας μπορεί να το εμποδίσει να επικοινωνήσει με τη συσκευή μας.

Στην παρακάτω εικονα βλέπουμε το εύρος των διευθύνσεων ανά κλάση.

Κλάση	Εύρος Διευθύνσεων	Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Εικόνα 3.7 Εύρος Διευθύνσεων Ανά Κλάση

Εφαρμογή Στο Δίκτυο Της Εταιρείας

Στο Router 1 χρησιμοποιήθηκε το δυναμικό NAT.

- Αρχικά ορίζουμε ποιες θύρες είναι inside και ποιες outside και ορίζουμε μια λίστα δημόσιων διευθύνσεων IP με την εντολη:

  ip nat pool 1 194.10.10.5 194.10.10.254 netmask 255.255.255.0

- Στην συνέχεια ορίζουμε μια ACL με τις ιδιωτικές διευθύνσεις που πρέπει να μεταφραστούν.

  access-list 1 permit 192.168.0.0 0.0.255.255

- Τέλος συνδέουμε την ACL με τη λίστα pool 1 που φτιάξαμε

  ip nat inside source list 1 pool 1

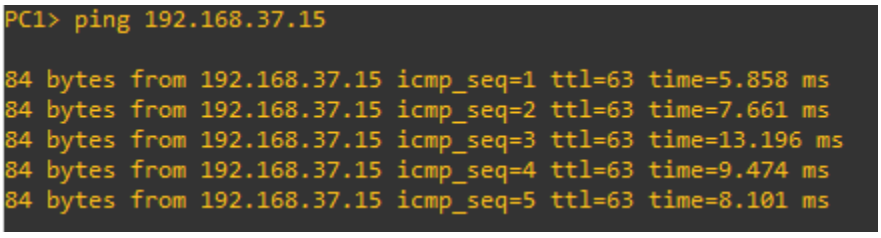
Στο Router ISP1, ο πάροχος κάνει και αυτός μια παρόμοια λειτουργία χρησιμοποιώντας την εντολη:

ip nat inside source list 1 interface GigabitEthernet0/0 overload

Με την εξής ACL:

access-list 1 permit 192.168.0.0 0.0.255.255
access-list 1 permit 194.10.10.0 0.0.255.255
access-list 1 permit 10.10.0.0 0.0.255.255

Για να ελέγξουμε ότι λειτουργεί από το PC1 θα κάνουμε ping το google.com στη διεύθυνση 8.8.8.8.



Εικόνα 3.8 Εκτέλεση Εντολής Ping από PC1

Στις παρακάτω εικόνες ελέγχουμε αν λειτουργεί το NAT στις συσκευές μας.

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 194.10.10.5:5488  192.168.1.2:5488   8.8.8.8:5488       8.8.8.8:5488
icmp 194.10.10.5:5744  192.168.1.2:5744   8.8.8.8:5744       8.8.8.8:5744
icmp 194.10.10.5:6000  192.168.1.2:6000   8.8.8.8:6000       8.8.8.8:6000
icmp 194.10.10.5:6256  192.168.1.2:6256   8.8.8.8:6256       8.8.8.8:6256
icmp 194.10.10.5:6512  192.168.1.2:6512   8.8.8.8:6512       8.8.8.8:6512
--- 194.10.10.5        192.168.1.2        ---                ---
```

Εικόνα 3.9 Εκτέλεση Εντολής show ip nat translations Στο Router1

```
ISP1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.122.77:34160 194.10.10.5:34160 8.8.8.8:34160    8.8.8.8:34160
icmp 192.168.122.77:34416 194.10.10.5:34416 8.8.8.8:34416    8.8.8.8:34416
icmp 192.168.122.77:34928 194.10.10.5:34928 8.8.8.8:34928    8.8.8.8:34928
icmp 192.168.122.77:35184 194.10.10.5:35184 8.8.8.8:35184    8.8.8.8:35184
icmp 192.168.122.77:35440 194.10.10.5:35440 8.8.8.8:35440    8.8.8.8:35440
```

Εικόνα 3.10 Εκτέλεση Εντολής show ip nat translations Στο ISP1

3.5 Ροή Δρομολόγησης

- Προγραμματιστές

Έστω ότι ξεκινάμε από τα τερματικά. Η δρομολόγηση πηγαίνει στο Switch 1 στη συνέχεια στο ESW2 και μετα ESW3. Έπειτα συνεχίζει στο Router4 στο ASAV1 στο Router1 και τέλος στον πάροχο ISP 1 για να βγει έξω στο ίντερνετ. Σε περίπτωση βλάβης του Switch 1 τότε το δίκτυο των προγραμματιστών χάνει την πρόσβαση στο δίκτυο. Βέβαια αυτό δεν θα προκαλέσει προβλήματα στους εξυπηρετητές το οποίο είναι το κυριότερο κομμάτι του δικτύου διότι όπως είπαμε και στο κομμάτι των αλλαγών διαχωρίσαμε τη θέση των προγραμματιστών και των εξυπηρετητών. Αν το ESW2 υποστεί κάποια βλάβη τότε πάλι οι προγραμματιστές χάνουν την πρόσβαση αλλά οι εξυπηρετητές είναι πλήρως λειτουργικοί. Τώρα αν το ESW3 πάθει κάποια βλάβη τότε στο δίκτυο δίνονται δυο εναλλακτικές είτε η δρομολόγηση να πάει από το Switch2 είτε από το ESW6 και να συνεχιστεί η δρομολόγηση στο ESW5 (και μετα Router5,Asav2,Router2 και μετα στον εναλλακτικό πάροχο). Επιπλέον το δίκτυο μπορεί να υποστηρίξει βλάβη στο Router4 δρομολογώντας τα πακέτα ως εξής: Switch1-ESW2-ESW3-ESW5-Router5.

- Εξυπηρετητές μέρος 1

Σε αυτό το κομμάτι η δρομολόγηση πηγαίνει ESW8- ESW 5- ESW - Router4. Αν το ESW 8 πάθει κάποια βλάβη τότε η σύνδεση των εξυπηρετητών χάνεται αλλά όχι όλων καθώς διαχωρίσαμε τους πελάτες. Αν το ESW 5 πάθει κάποια ζημιά τότε οι εξυπηρετητές

χρησιμοποιούν τον μεταγωγέα των υπολοίπων εξυπηρετητών δηλαδή το Switch 3 και μετα ESW 6 και μετα δίνονται δυο δυνατότητες είτε μέσω Switch 2 είτε μέσω ESW 2 ώστε να φτάσουν το ESW 3. Σημαντικό πρόβλημα αποτελεί το να πάθει κάποια ζημιά το ESW5 και ESW6 μαζί οπού μόνο τότε χάνεται η σύνδεση όλων των πελατών της εταιρείας. Υπό άλλες συνθήκες είδαμε ότι το δίκτυο μπορεί να διαχειριστεί αρκετές βλάβες σε συσκευές ακόμα και ζημίες σε πολλαπλές συσκευές.

- Εξυπηρετητές μέρος 2

Εδώ η δρομολόγηση πάει ως εξής: Switch 3-ESW6-ESW2-ESW3. Με μια ζημιά στο Switch3 η σύνδεση στους web server χάνεται αλλά όσο αφορά τους εξυπηρετητές που ανήκουν σε αυτό το μεταγωγέα. Αν το ESW 6 υποστεί κάποια βλάβη τότε η δρομολόγηση γίνεται από το ESW8. Αν πάθει κάτι το ESW 2 τότε Switch 3- ESW 6 και μετα έχουμε τη δυνατότητα να πάμε είτε μέσω ESW 5 είτε μέσω Switch 2 και μετα ESW 3.

- Εναλλακτικές στα router

Οι τερματικές συσκευές έχοντας φτάσει στο Router4 αρχικά θα δρομολογήσουν τα πακέτα στον πάροχο Isp1 μέσω Router 1 έχοντας περάσει από το Asav1. Αν το Asav1 πάθει κάτι τότε επιλεγεί το Router2 και έτσι φτάνει στο Router 1 μέσω του Asav 4. Τώρα αν πάθουν κάτι οι συσκευές Router1 ή Asav4 ή Router3, το Router4 θα επιλέξει το Router5 για να δρομολογήσει τα πακέτα στον δεύτερο πάροχο μέσω του Asav 2 και του Router 2.

3.6 Αρχιτεκτονική Δικτύου

Αρχικά το δίκτυο της εταιρείας ήταν επίπεδο και όχι ιεραρχικό. Το οποίο σημαίνει ότι δεν έχουμε διαχωρισμό και στήσιμο στα επίπεδα core,distribution και access. Στόχος του νέου βελτιωμένου δικτύου είναι να μετατραπεί σε ιεραρχικό. Ένα ιεραρχικό δίκτυο είναι ευκολότερο να διαχειριστεί και η αντιμετώπιση προβλημάτων είναι ευκολότερη από ότι σε ένα επίπεδο δίκτυο.

3.6.1 Επίπεδο Πρόσβασης -Access layer

Το επίπεδο πρόσβασης είναι το πρώτο επίπεδο του ιεραρχικού μοντέλου τριών επιπέδων της Cisco. Αυτό το επίπεδο επιτρέπει στους τελικούς χρήστες να έχουν πρόσβαση στο δίκτυο.
Οι συσκευές χρήστη που συνδέονται σε αυτό το επίπεδο χρησιμοποιούν διαφορετικά πρωτόκολλα για να ανακαλύψουν το ένα το άλλο, να αφαιρέσουν βρόχους και να ανταλλάξουν

δεδομένα. Σε αυτό το επίπεδο διαμορφώνονται και επιβάλλονται επίσης διάφορες υπηρεσίες και πολιτικές ασφαλείας. Οι κύριες λειτουργίες αυτού του στρώματος είναι οι ακόλουθες.

• Σύνδεση διαφόρων τύπων τελικών συσκευών στο δίκτυο LAN.

• Παροχή μεταγωγής επιπέδου 2 και υλοποίηση διαφόρων υπηρεσιών μεταγωγής επιπέδου 2, όπως εκτεινόμενο δέντρο, εικονικός έλεγχος πρόσβασης, ποιότητα υπηρεσιών (QoS) και ARP.

• Αποτρέπει τη σύνδεση μη εξουσιοδοτημένων συσκευών στο LAN επιβάλλοντας διάφορες πολιτικές ασφαλείας, όπως η ασφάλεια θύρας, η παρακολούθηση DHCP και η διαμόρφωση στατικής διεύθυνσης MAC.

Οι μεταγωγείς που συνδέονται σε αυτό το επίπεδο είναι γνωστοί ως μεταγωγείς πρόσβασης. Οι τελικές συσκευές συνδέονται στο δίκτυο LAN μέσω των μεταγωγών πρόσβασης. Με άλλα λόγια, ένας μεταγωγός πρόσβασης προωθεί την κυκλοφορία μεταξύ των συνδεδεμένων συσκευών και του υπόλοιπου LAN. Στο δίκτυο μας οι μεταγωγείς που ανήκουν σε αυτό το επίπεδο είναι τα SWITCH1, SWITCH2, SWITCH3.

3.6.2 Επίπεδο Διανομής -Distribution layer

Το επίπεδο διανομής είναι το δεύτερο επίπεδο του ιεραρχικού μοντέλου τριών επιπέδων της Cisco. Οι μεταγωγείς που συνδέονται σε αυτό το επίπεδο είναι γνωστοί ως μεταγωγείς διανομής. Σε αντίθεση με τους μεταγωγείς πρόσβασης, οι μεταγωγείς διανομής δεν παρέχουν καμία υπηρεσία στις τελικές συσκευές. Οι μεταγωγείς διανομής συνδέουν τους μεταγωγείς πρόσβασης. Οι κύριες λειτουργίες των μεταγωγών στρώματος διανομής είναι οι ακόλουθες.

• Παροχή συνδεσιμότητας μεταξύ των μεταγωγών επιπέδου πρόσβασης

• Συνάθροιση συνδέσεων LAN και WAN και κυκλοφορίας

• Έλεγχος και φιλτράρισμα της κυκλοφορίας με την εφαρμογή ACL

• Έλεγχος εκπομπής μέσω VLAN

• Παροχή πλεονασμού και εξισορρόπησης φορτίου

• Παροχή υπηρεσιών δρομολόγησης μεταξύ διαφορετικών VLAN και τομέων δρομολόγησης

• Λειτουργεί ως σημείο οριοθέτησης μεταξύ διαφορετικών LAN και τομέων εκπομπής

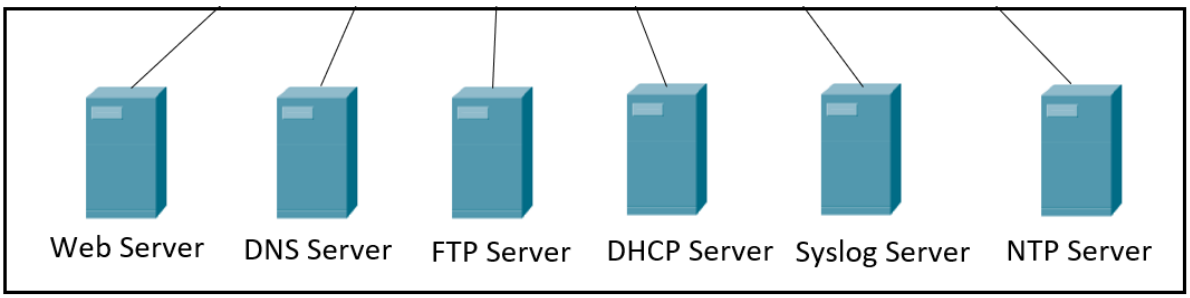
Εάν το δίκτυο περιέχει ένα ξεχωριστό επίπεδο πυρήνα, το επίπεδο διανομής συνδέει το επίπεδο πρόσβασης με το επίπεδο πυρήνα. Στο δίκτυο μας οι μεταγωγείς που ανήκουν σε αυτό το επίπεδο είναι τα ESW6, SWITCH4, ESW2.

3.6.3 Επίπεδο Πυρήνα -Core layer

Αυτό είναι το τρίτο επίπεδο του ιεραρχικού μοντέλου τριών επιπέδων της Cisco. Οι μεταγωγείς που λειτουργούν σε αυτό το επίπεδο είναι γνωστοί ως μεταγωγείς πυρήνα. Οι μεταγωγείς πυρήνα συνδέουν μεταγωγούς διανομής. Σε ένα πολύπλοκο και μεγάλο δίκτυο, οι μεταγωγείς πυρήνα μειώνουν τις ανάγκες καλωδίωσης και αλλάζουν θύρες, ενώ παράλληλα επιτρέπουν σε όλες τις συσκευές να στέλνουν δεδομένα σε όλες τις άλλες συσκευές στο LAN. Συνήθως, τα μικρά ή μεσαία δίκτυα LAN δεν σχεδιάζουν το βασικό στρώμα. Αντί να σχεδιάζουν ένα ξεχωριστό στρώμα πυρήνα, συνδέουν απευθείας μεταγωγούς διανομής. Αυτή η προσέγγιση δεν λειτουργεί σε μεγάλα δίκτυα. Για παράδειγμα, εάν ένα δίκτυο LAN έχει δύο μεταγωγούς διανομής, μπορεί να τους συνδέσει απευθείας. Αλλά εάν ένα LAN έχει πολλούς μεταγωγούς διανομής, δεν θα πρέπει να τους συνδέσει απευθείας. Για να συνδέσουμε όλους τους μεταγωγείς διανομής, ένα LAN απαιτεί συνδέσεις **N*N-1** και **N-1** διαθέσιμες θύρες σε κάθε μεταγωγό διανομής. Για παράδειγμα, εάν ένα LAN έχει 8 μεταγωγείς διανομής, χρειάζεται 8*8-1 = 56 συνδέσεις και 8-1 = 7 θύρες σε κάθε μεταγωγέα διανομής. Το LAN μπορεί να μειώσει τον απαιτούμενο αριθμό συνδέσεων και θυρών συνδέοντας μεταγωγούς διανομής μέσω μερικών επιπλέον μεταγωγών. Ένας μεταγωγός που συνδέει τους μεταγωγείς διανομής είναι γνωστός ως μεταγωγός πυρήνα. Στο δίκτυο μας οι μεταγωγείς που ανήκουν σε αυτό το επίπεδο είναι τα ESW3, ESW5.

3.7 Διακομιστές

Για την προσομοίωση των διακομιστών της πτυχιακής θα χρησιμοποιηθεί το Appliance Networkers Toolbox και το Ubuntu Server Appliance. Σε όλα τα τερματικά έχουν δοθεί στατικά οι διευθύνσεις IP. Χρησιμοποιώντας το Web Term Appliance, στο οποίο έχουμε δώσει στατικά διεύθυνση θα ελέγξουμε ορισμένες λειτουργίες των διακομιστών.



Εικόνα 3.11 Διακομιστές

3.7.1 Διακομιστής FTP

Το πρωτόκολλο μεταφοράς αρχείων FTP είναι ένα πρωτόκολλο πελάτη και διακομιστή που χρησιμοποιείται για τη μεταφορά ή την ανταλλαγή εγγράφων με έναν κεντρικό υπολογιστή. Το ανώνυμο FTP βοηθά τους χρήστες να έχουν πρόσβαση σε αρχεία, προγράμματα και άλλα δεδομένα στο Διαδίκτυο χωρίς αναγνώριση χρήστη ή κωδικό πρόσβασης. Ο διακομιστής αυτός προσφέρει αυτή την υπηρεσία στο δίκτυο μας όπου πρόσβαση έχουν μόνο οι προγραμματιστές του VLAN 10.

3.7.2 Διακομιστής TFTP

Το TFTP χρησιμοποιεί λογισμικό πελάτη και διακομιστή για να κάνει συνδέσεις μεταξύ δύο συσκευών. Από έναν πελάτη TFTP, μεμονωμένα αρχεία μπορούν να μεταφορτωθούν ή να ληφθούν από τον διακομιστή. Ο διακομιστής φιλοξενεί τα αρχεία και ο πελάτης στέλνει αιτήματα για ανταλλαγή αρχείων. Το TFTP μπορεί επίσης να χρησιμοποιηθεί για την απομακρυσμένη εκκίνηση ενός υπολογιστή και τη δημιουργία αντιγράφων ασφαλείας αρχείων διαμόρφωσης δικτύου ή δρομολογητή, είναι πιο απλό από το FTP ωστόσο, δεν παρέχεται έλεγχος ταυτότητας χρήστη και μερικές ακόμα χρήσιμες λειτουργίες που υποστηρίζονται από το FTP. Ενώ το FTP χρησιμοποιεί TCP, το TFTP χρησιμοποιεί UDP, γεγονός που το καθιστά αναξιόπιστο πρωτόκολλο. Αυτός ο διακομιστής έχει ρυθμιστεί με το Toolbox και έτσι κάθε φορά που ο χρήστης εκτελεί την εντολη: **copy running-config tftp** από μια συσκευή και βάλει την διεύθυνση IP του διακομιστή και το όνομα θα αποθηκεύει τις ρυθμίσεις στον εξυπηρετητή.

3.7.3 Διακομιστής Syslog

Όλες οι συσκευές δικτύου, όπως οι δρομολογητές, οι διακομιστές και τα τείχη προστασίας δημιουργούν ή ζητούν αρχεία καταγραφής σχετικά με τις καταστάσεις και τα συμβάντα που συμβαίνουν. Όταν έχουμε να κάνουμε με μεγάλα συστήματα η παρακολούθηση όλων αυτών των αρχείων καταγραφής και των πληροφοριών γίνεται δύσκολη. Για να αντιμετωπιστεί αυτό το πρόβλημα χρησιμοποιούμε το Syslog με έναν διακομιστή καταγραφής γνωστό ως διακομιστή Syslog. Ένας διακομιστής Syslog μας επιτρέπει να στέλνουμε τις πληροφορίες καταγραφής όλων των συσκευών δικτύου μας σε ένα κεντρικό μέρος.

Το Syslog είναι ένα πρωτόκολλο που αφορά την καταγραφή μηνυμάτων που χρησιμοποιούν τα συστήματα υπολογιστών για την αποστολή αρχείων καταγραφής συμβάντων σε έναν διακομιστή Syslog για αποθήκευση. Σε συσκευές δικτύου, το Syslog μπορεί να χρησιμοποιηθεί για την καταγραφή συμβάντων όπως αλλαγές στην κατάσταση της διεπαφής, επανεκκινήσεις συστήματος και άλλα . Μπορούν να καταγραφούν πολλοί διαφορετικοί τύποι συμβάντων. Τα αρχεία καταγραφής είναι απαραίτητα για την αντιμετώπιση προβλημάτων και την εξέταση της αιτίας των συμβάντων. Για να ελέγξει ο διαχειριστής τα μηνύματα εκτελεί την εντολη **loging host** και την IP του διακομιστή σε global configuration λειτουργία και μετα στο διακομιστή στη θέση: /var/log/syslog βλέπει τα μηνύματα με την εντολη **cat syslog.**

3.7.4 Διακομιστής Ιστού Web Server

Η ορολογία διακομιστής ιστού αναφέρεται είτε σε υλικό ή λογισμικό είτε και στα δύο μαζί σε συνδυασμό. Από την πλευρά του υλικού, ένας διακομιστής ιστού είναι ένας υπολογιστής που αποθηκεύει το λογισμικό διακομιστή ιστού και τα αρχεία στοιχείων ενός ιστότοπου όπως για παράδειγμα αρχεία με κώδικα ιστοσελίδων. Ένας διακομιστής ιστού συνδέεται στο διαδίκτυο και υποστηρίζει φυσική ανταλλαγή δεδομένων με άλλες συσκευές συνδεδεμένες. Από την πλευρά του λογισμικού, ένας διακομιστής ιστού περιλαμβάνει πολλά μέρη που ελέγχουν τον τρόπο με τον οποίο οι χρήστες του ιστού έχουν πρόσβαση στα φιλοξενούμενα αρχεία. Ένας διακομιστής ιστού ή αλλιώς διακομιστής HTTP είναι προσβάσιμος μέσω των ονομάτων τομέα των ιστότοπων που αποθηκεύει και παραδίδει το περιεχόμενο αυτών των φιλοξενούμενων ιστότοπων στη συσκευή του τελικού χρήστη. Για να δημοσιευτεί ένας ιστότοπος, χρειάζεται είτε έναν στατικό είτε έναν δυναμικό διακομιστή ιστού. Ένας στατικός διακομιστής Ιστού, αποτελείται από έναν υπολογιστή (υλικό) με έναν διακομιστή HTTP (λογισμικό). Ένας δυναμικός διακομιστής Ιστού αποτελείται από έναν στατικό διακομιστή Ιστού συν επιπλέον λογισμικό, συνηθέστερα έναν διακομιστή εφαρμογών και μια βάση δεδομένων. Για τους διακομιστές WEB χρησιμοποιούμε το Web Term Appliance, έναν client ο οποίος έχει web browser και πληκτρολογώντας την διεύθυνση IP του διακομιστή τότε συνδέεται και βγάζει το αρχείο ιστοσελίδας που φιλοξενεί ο διακομιστής, το οποίο βρίσκεται στο /var/www μονοπάτι.

3.7.5 Διακομιστής NTP

Το πρωτόκολλο ώρας δικτύου (NTP) είναι ένα πρωτόκολλο δικτύωσης για συγχρονισμό ρολογιού μεταξύ συστημάτων υπολογιστών μέσω δικτύων δεδομένων μεταβλητής καθυστέρησης με μεταγωγή πακέτων. Προορίζεται για συγχρονισμό όλων των συμμετεχόντων υπολογιστών σε λίγα χιλιοστά του δευτερολέπτου της Συντονισμένης Παγκόσμιας Ώρας (UTC). Το NTP μπορεί συνήθως να διατηρήσει χρόνο εντός δεκάδων χιλιοστών του δευτερολέπτου μέσω του δημόσιου διαδικτύου και μπορεί να επιτύχει ακρίβεια μεγαλύτερη του ενός χιλιοστού του δευτερολέπτου σε τοπικά δίκτυα υπό ιδανικές συνθήκες. Οι ασύμμετρες διαδρομές και η συμφόρηση δικτύου μπορεί να προκαλέσουν σφάλματα 100 ms ή περισσότερα. Το πρωτόκολλο περιγράφεται συνήθως με όρους μοντέλου πελάτη-διακομιστή, αλλά μπορεί εύκολα να χρησιμοποιηθεί σε σχέσεις peer-to-peer όπου και οι δύο ομότιμοι θεωρούν το άλλο ως πιθανή πηγή χρόνου. Οι υλοποιήσεις στέλνουν και λαμβάνουν χρονικές σημάνσεις. χρησιμοποιώντας το User Datagram Protocol (UDP) στον αριθμό θύρας 123. Μπορούν επίσης να χρησιμοποιούν μετάδοση ή πολλαπλή μετάδοση, όπου οι πελάτες ακούν παθητικά τις ενημερώσεις ώρας μετά από μια αρχική ανταλλαγή βαθμονόμησης μετ' επιστροφής. Το NTP παρέχει μια προειδοποίηση για οποιαδήποτε επικείμενη αλλαγή δευτερολέπτου, αλλά δεν μεταδίδονται πληροφορίες σχετικά με τις τοπικές ζώνες ώρας ή τη θερινή ώρα.

3.7.6 Διακομιστής DNS

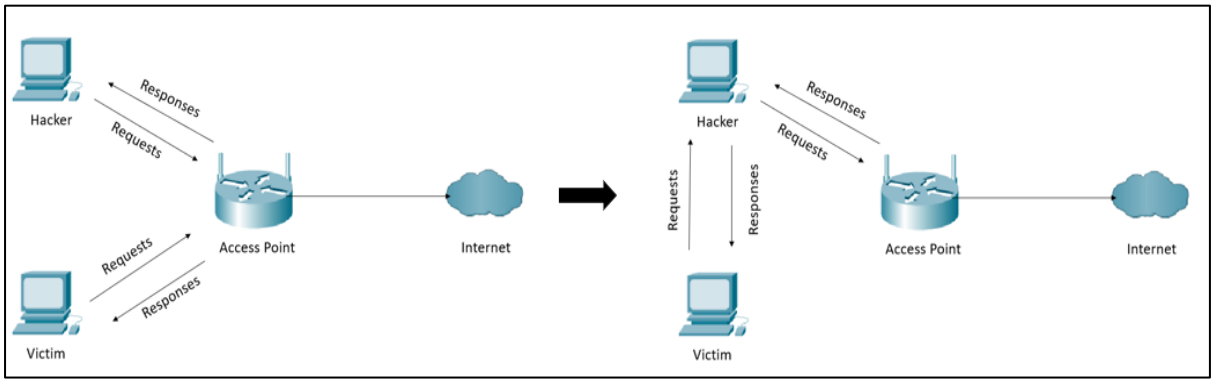
Το Σύστημα Ονομάτων Τομέα (DNS) είναι ο τηλεφωνικός κατάλογος του Διαδικτύου. Όταν κάποιος χρήστης πληκτρολογήσει ονόματα τομέα όπως «google.com» σε προγράμματα περιήγησης ιστού, το DNS είναι υπεύθυνο για την εύρεση της σωστής διεύθυνσης IP για αυτούς τους ιστότοπου. Στη συνέχεια, τα προγράμματα περιήγησης χρησιμοποιούν αυτές τις διευθύνσεις για να επικοινωνούν με τους διακομιστές προέλευσης. Ένας τέτοιος διακομιστής είναι μια συσκευή ή ένα πρόγραμμα αφιερωμένο στην παροχή υπηρεσιών σε άλλα προγράμματα, που αναφέρονται ως «πελάτες». Οι πελάτες DNS, οι οποίοι είναι ενσωματωμένοι στα περισσότερα σύγχρονα λειτουργικά συστήματα επιτραπέζιων υπολογιστών και φορητών υπολογιστών, επιτρέπουν στα προγράμματα περιήγησης ιστού να αλληλεπιδρούν με διακομιστές DNS. Οι διακομιστές DNS μπορεί να αποτύχουν για πολλούς λόγους, όπως διακοπές ρεύματος, κυβερνοεπιθέσεις και δυσλειτουργίες υλικού. Σε περίπτωση μεγάλης διακοπής του διακομιστή DNS, ορισμένοι χρήστες ενδέχεται να

αντιμετωπίσουν καθυστερήσεις λόγω του όγκου των αιτημάτων που χειρίζονται οι εφεδρικοί διακομιστές, αλλά θα χρειαζόταν διακοπή DNS πολύ μεγάλων διαστάσεων για να καταστεί μη διαθέσιμο ένα σημαντικό μέρος του Διαδικτύου. Στο επόμενο κεφάλαιο θα παρουσιάσουμε μια επίθεση ως προς το πρωτόκολλο DNS.

ΚΕΦΑΛΑΙΟ 4 : Σενάρια Επιθέσεων και Τρόποι Αντιμετώπισης

4.1. Man In the Middle-MITM επιθέσεις

Είναι οι επιθέσεις στις οποίες ένας χρήστης μπορεί να παρεμποδίσει-μπει αναμεσά στην επικοινωνία δυο συσκευών και να δει οτιδήποτε ανταλλάσσεται μεταξύ των δυο συσκευών. Σε αυτό το κεφάλαιο θα δούμε μερικές επιθέσεις αυτής της κατηγορίας όπως για παράδειγμα μια ARP Spoofing επίθεση και μια DNS Spoofing επίθεση.



Εικόνα 4.1 Λειτουργία Επίθεσης MITM

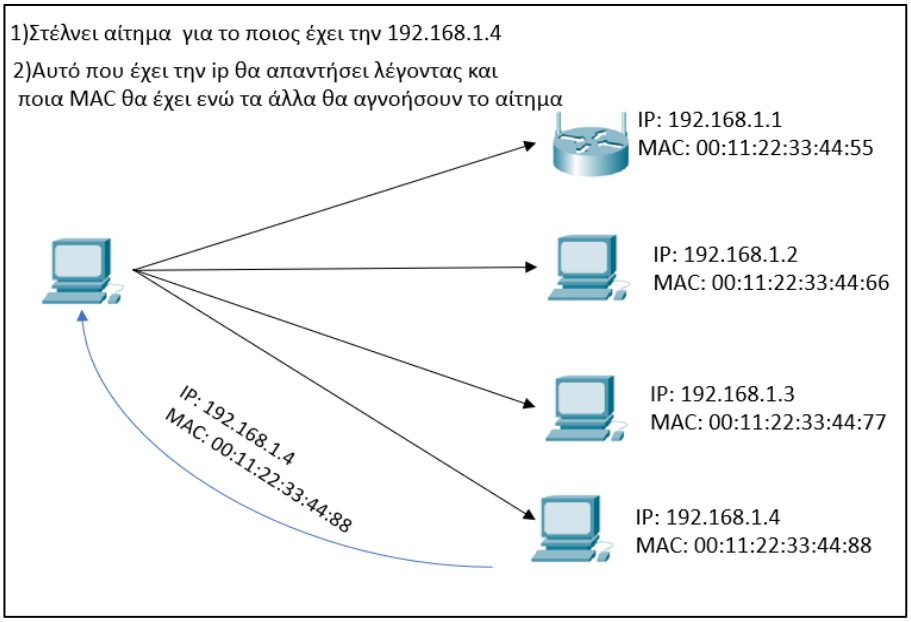
4.2.1 Επίθεση ARP Spoofing

Είναι μια επίθεση που εκτελείται σε μεγάλο βαθμό στα σύγχρονα δίκτυα υπολογιστών. Αυτή η επίθεση μας επιτρέπει να ανακατευθύνουμε τη ροή των πακέτων οπότε η φυσιολογική ροή της εικόνας 4.1 στα αριστερά θα μετατραπεί στη ροή που απεικονίζεται στην εικόνα 4.1 αριστερά. Έτσι τα αιτήματα και οι απαντήσεις του μηχανήματος που δέχεται την επίθεση θα πρέπει να περάσουν από τον εισβολέα, αυτό σημαίνει ότι μηνύματα, ιστοσελίδες, εικόνες, ονόματα, κωδικοί όλα θα περάσουν από τον υπολογιστή του εισβολέα. Αυτό του επιτρέπει να διαβάσει και να τροποποιήσει τις πληροφορίες

4.2.2 Πρωτόκολλο ARP

Το πρωτόκολλο αυτό χρησιμοποιείται για να βρεθεί μια διεύθυνση του επιπέδου συνδέσμου (link layer) ή διεύθυνση υλικού (hardware address) ενός ξένου υπολογιστή με βάση μια διεύθυνση του επιπέδου επικοινωνίας (network layer). Δηλαδή χρησιμοποιείται για να συνδέσει την διεύθυνση IP μιας συσκευής με την MAC διεύθυνση της. Το επίπεδο διαδικτύου

ενθυλακώνει στο πακέτο μια διεύθυνση IP προορισμού. Όμως το επίπεδο πρόσβασης δικτύου γνωρίζει μόνο διευθύνσεις MAC. Ο συνδετικός κρίκος λοιπόν αναμεσά στα δυο επίπεδα που απαντά στο ερώτημα ποια είναι η MAC του κόμβου με συγκεκριμένη IP είναι το πρωτόκολλο ανάλυσης διευθύνσεων ARP.



Εικόνα 4.2 Λειτουργία Πρωτοκόλλου ARP

4.2.3 Παρουσίαση επίθεσης ARP Spoofing με το εργαλείο Arpspoof

Τα εργαλεία που θα χρησιμοποιηθούν για την προσομοίωση της επίθεσης είναι το arpspoof και το bettercap και αντίστοιχα τα προγράμματα και λειτουργικά είναι το Virtual Box το Kali Linux και το Windows 10 όλα σε εικονικό περιβάλλον. Η επίθεση εκτελείται από ένα λειτουργικό βασισμένο σε αρχιτεκτονική Linux , το Kali Linux το οποίο είναι στημένο μέσα στο Virtual Box σαν εικονική μηχανή, σε ένα λειτουργικό Windows 10 και αυτό σε εικονικό περιβάλλον. Αρχικά με την εντολή **arp -a** μπορούμε να δούμε την αρχική κατάσταση του πίνακα ARP και στα δύο μηχανήματα.

```
root@kali:~# arp -a
? (10.0.2.5) at <incomplete> on eth0
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
root@kali:~#
```

Εικόνα 4.3 Εκτέλεση Εντολής arp-a Σε Μηχάνημα kali linux

Με αυτό τον τρόπο παρατηρούμε στην πρώτη γραμμή ότι γίνεται σύνδεση της διεύθυνσης IP του δρομολογητή με την διεύθυνση MAC του.

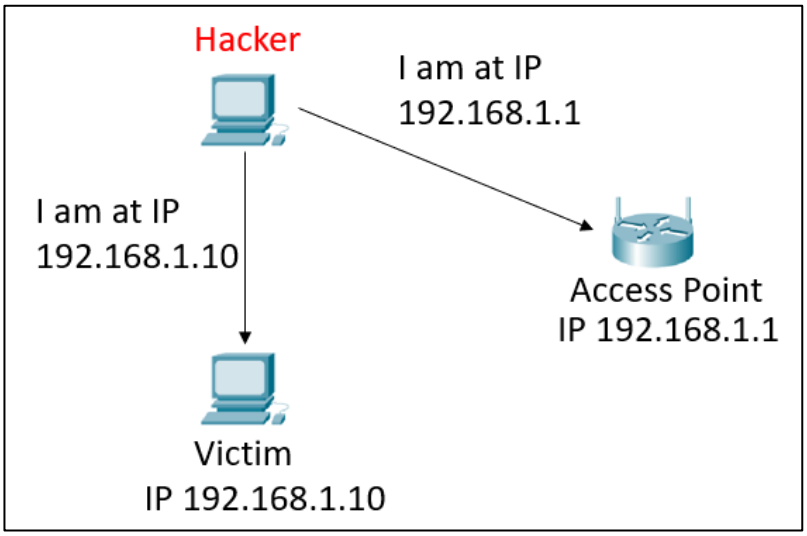
```
C:\Users\IEUser\Desktop>arp -a

Interface: 10.0.2.5 --- 0x7
  Internet Address      Physical Address      Type
  10.0.2.1              52-54-00-12-35-00     dynamic
  10.0.2.3              08-00-27-5f-4f-8f     dynamic
  10.0.2.4              08-00-27-d0-2e-c7     dynamic
  10.0.2.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Εικόνα 4.4 Εκτέλεση Εντολής arp-a Σε Μηχάνημα windows10

Έτσι λοιπόν αυτή η συσκευή κάθε φορά που θέλει να στείλει κάποιο αίτημα στο διαδίκτυο θα κατευθύνει αυτό το αίτημα σε αυτή τη MAC διεύθυνση, δηλαδή στην MAC η οποία είναι συνδεδεμένη με την IP του δρομολογητή.

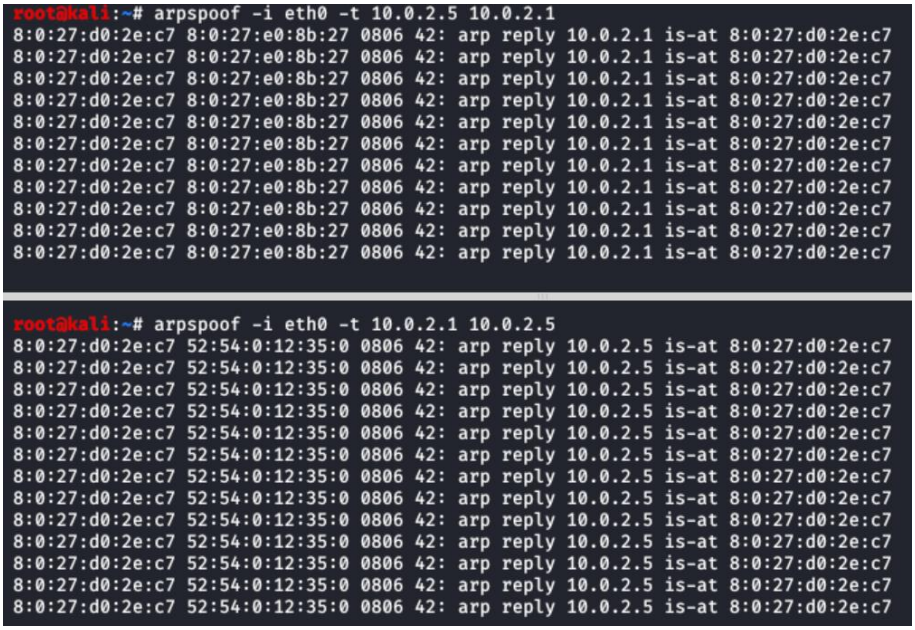
Αυτή η τιμή (MAC) μπορεί πολύ ευκολά να τροποποιηθεί αν εκμεταλλευτούμε το ARP πρωτόκολλο. Το επιτιθέμενο μηχάνημα στέλνει δυο απαντήσεις. Μια στο δρομολογητή και μια στο θύμα. Στο δρομολογητή δείχνει ότι έχει την διεύθυνση ip του θύματος ενώ στο θύμα δείχνει ότι έχει την διεύθυνση ip του δρομολογητή. Έτσι ο δρομολογητής θα ανανεώσει τον πίνακα ARP και θα συνδέσει την IP του θύματος με την MAC του επιτιθέμενου, και το θύμα θα συνδέσει την IP του δρομολογητή με την MAC του επιτιθέμενου. Έτσι το θύμα θα νομίζει ότι ο εισβολέας είναι ο δρομολογητής και ο δρομολογητής ότι ο εισβολέας είναι το θύμα. Κάθε φορά που το θύμα θα θέλει να στείλει κάτι θα το στέλνει πρώτα στον εισβολέα και αυτός μετά στο δρομολογητή και αντιστρόφως.



Εικόνα 4.5 Ο Ρόλος Του Επιτιθέμενου

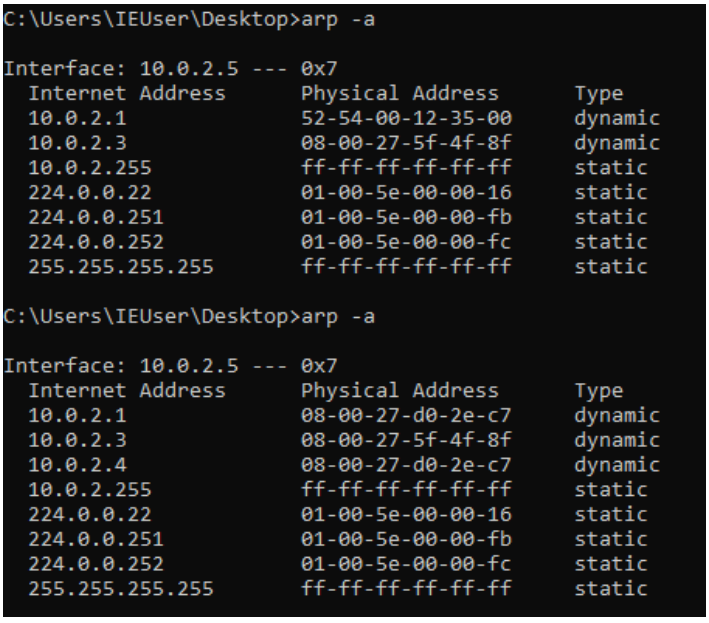
Όπως ήδη αναφέραμε για την επίθεση θα χρησιμοποιήσουμε ένα εργαλείο το arpspoof και στη συνέχεια θα δείξουμε την επίθεση και με δεύτερο εργαλείο το bettercap που βρίσκονται εγκατεστημένα στο λειτουργικό Kali Linux και πάντα σε εικονικό περιβάλλον. Στο ίδιο λειτουργικό σύστημα εκτελώ τις παρακάτω εντολές όπου η μια λέει στη συσκευή ότι είμαι ο δρομολογητής και η άλλη στο δρομολογητή ότι είμαι η συσκευή όπως εξηγήσαμε πιο πάνω.

- **arpspoof -I eth0 -t 10.0.2.5 10.0.2.1**
- **arpspoof -I eth0 -t 10.0.2.1 10.0.2.5**



Εικόνα 4.6 Εκτέλεση Επίθεσης Arpspoof

Για να ελέγξουμε το αποτέλεσμα της επίθεσης πάμε ξανά στο win10 machine και εκτελούμε την εντολή **arp -a.** Έτσι αν τα συγκρίνουμε βλέπουμε ότι η MAC διεύθυνση είναι πλέον διαφορετική.



Εικόνα 4.7 Σύγκριση Των Δύο MAC Διευθύνσεων

Αξίζει να σημειώσουμε ότι σε αυτό το σημείο η συσκευή που δέχτηκε την επίθεση δεν έχει πρόσβαση στο διαδίκτυο διότι ο επιτιθέμενος υπολογιστής δεν είναι δρομολογητής. Έτσι για να λυθεί αυτό και να στέλνονται τα πακέτα στο δρομολογητή θα πρέπει να ενεργοποιηθεί η προώθηση θύρας ή αλλιώς port forwarding. Για ενεργοποίηση χρησιμοποιούμε την εντολή:

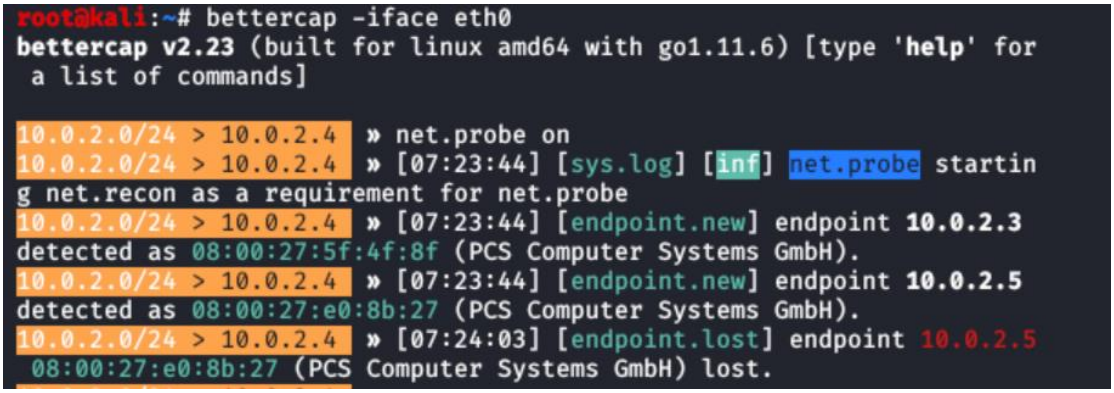
echo 1 > /proc/sys/net/ipv4/ip_forward

Και έτσι η συσκευή έχει πρόσβαση στο διαδίκτυο. Με αυτή την κίνηση ο επιτιθέμενος μπορεί να κάνει αρκετά πράγματα όπως να τοποθετήσει κώδικα στον browser του στόχου, να υποκλέψει κωδικούς, και να δει όλες τις πληροφορίες που στέλνει. Μετα από αυτή την επίθεση ο επιτιθέμενος μπορεί να χρησιμοποιήσει άλλα προγράμματα όπως το Wireshark ή άλλα packet sniffers σαν αυτό που παρουσιάζουμε παρακάτω, για να αναλύσει τα δεδομένα.

4.2.4 Παρουσίαση επίθεσης ARP Spoofing με το εργαλείο Bettercap

Η παραπάνω επίθεση μπορεί να γίνει και με ένα άλλο εργαλείο το οποίο ονομάζεται bettercap. Αυτό το εργαλείο μπορεί να χρησιμοποιηθεί και για άλλα πράγματα όπως να κάνουμε capture date και να τα αναλύσουμε, μπορούμε να κάνουμε bypass HTTPS,HSTS, αλλά και για DNS Spoofing, και για να βάλουμε κώδικα σε σελίδες. Για να ενεργοποιήσουμε το bettercap χρησιμοποιούμε την εντολή: **bettercap -iface eth0**

Σε αυτό το σημείο μας ενδιαφέρει η ενότητα **net.probe** το οποίο διερευνάει για νέους Host στο δίκτυο στέλνοντας UDP πακέτα σε κάθε πιθανή διεύθυνση του υποδικτύου. Για ενεργοποίηση χρησιμοποιώ την εντολή: **net.probe on**



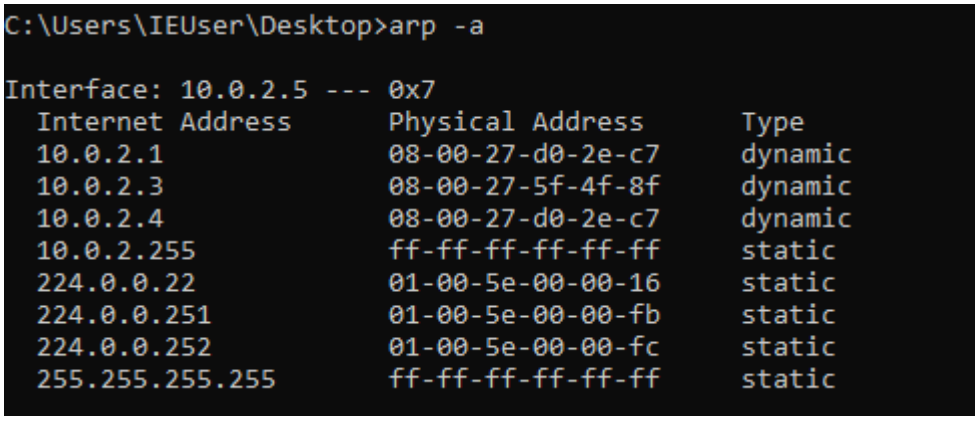
Εικόνα 4.8 Εκτέλεση Εντολής Bettercap

Στο πρώτο στάδιο ο επιτιθέμενος πρέπει να γίνει το άτομο στη μέση δηλαδή MITM, χρησιμοποιώντας μια ενότητα που ονομάζεται arp spoof με τη εντολή: **arp. spoof on**

Με την εντολή **set arp.spoof.fullduplex true** κάνει spoof και τον στόχο και το δρομολογητή. Αντί με τον προηγούμενο τρόπο που έπρεπε να εκτελέσουμε δυο φορές την εντολή. Στο επόμενο βήμα πρέπει να ορίσουμε το στόχο. Για να ορίσουμε το στόχο εκτελούμε την εντολή:

set arp. spoof.targets 10.0.2.5

Και τώρα είμαστε έτοιμοι να το τρέξουμε με την εντολή **arp.spoof on.**

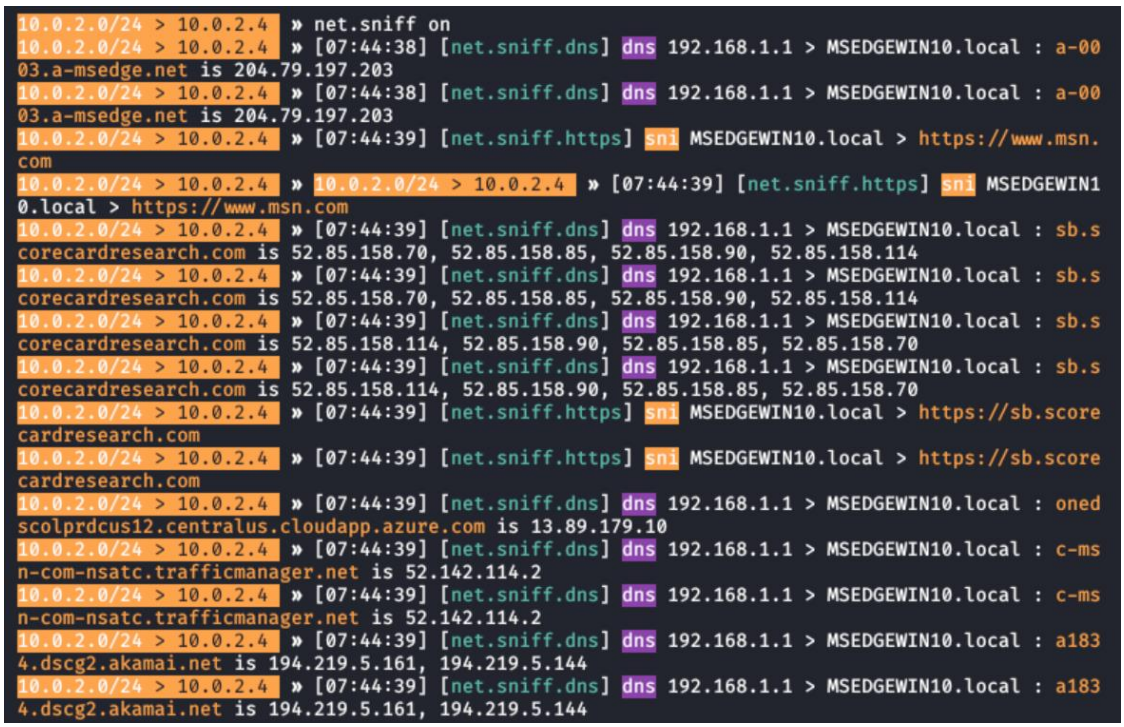


Εικόνα 4.9 Αποτέλεσμα Επίθεσης

Παρατηρώ ότι οι διευθύνσεις 10.0.2.1 και 10.0.2.4 έχουν την ίδια φυσική διεύθυνση.

Τέλος ο επιτιθέμενος μπορεί να αναλύει οποιοδήποτε δεδομένο η πακέτο περνάει από το στοχευμένο μηχάνημα χρησιμοποιώντας την εντολή: **net.sniff on .**

Έτσι οποιαδήποτε κίνηση και να κάνει το μηχάνημα-στόχος θα καταγραφεί.



Εικόνα 4.10 Εκτέλεση Εντολής net.sniff on

Η παραπάνω διαδικασία αν γίνει προς αρκετά μηχανήματα θα χρειαστεί να εκτελούνται όλες αυτές οι εντολές αρκετές φορές. Έτσι λοιπόν μπορούμε να αυτοματοποιήσουμε αυτή τη διαδικασία με ένα custom script το οποίο λέγεται caplet το οποίο πολύ απλά είναι ένα txt αρχείο το οποίο θα ονομάσουμε spoof.cap και θα το εκτελέσουμε με την εντολή: **bettercap -iface eth0 -caplet spoof.cap**

```
net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets 10.0.2.5
arp.spoof on
net.sniff on
```

Εικόνα 4.11 Κείμενο Εντολών "caplet"

4.2.5 Πρόληψη Επίθεσης με την Τεχνολογία VPN

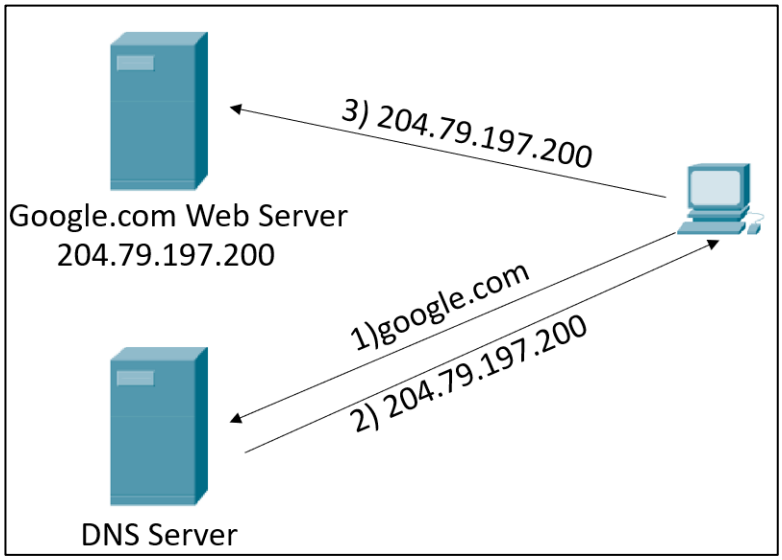
Ένα εικονικό ιδιωτικό δίκτυο ή αλλιώς VPN είναι ένα δίκτυο που χρησιμοποιεί κατά κύριο λόγο δημόσια τηλεπικοινωνιακή υποδομή, όπως το διαδίκτυο, και δίνει τη δυνατότητα σε απομακρυσμένα γραφεία ή σε χρήστες να έχουν πρόσβαση σε ένα κεντρικό οργανωτικό δίκτυο. Ένα VPN συνήθως απαιτεί από τους απομακρυσμένους χρήστες του δικτύου πιστοποίηση, και συχνά ασφαλίζει τα δεδομένα με τεχνολογίες κρυπτογράφησης για να εμποδιστεί η διάδοση των ιδιωτικών πληροφοριών σε μη εξουσιοδοτημένους τρίτους. Η τεχνολογία VPN μέσω του κοινόχρηστου διαδικτύου έχει αντικαταστήσει την ανάγκη διατήρησης ακριβών μισθωμένων γραμμών τηλεπικοινωνιακών κυκλωμάτων σε ευρείες περιοχές εγκαταστάσεων του δικτύου. Η τεχνολογία VPN μειώνει το κόστος, επειδή δεν χρειάζεται φυσική μισθωμένη γραμμή για τη σύνδεση απομακρυσμένων χρηστών σε ένα intranet. Τα συστήματα VPN μπορούν να ταξινομηθούν από:

- Τα πρωτόκολλα που χρησιμοποιούνται για την σήραγγα της κυκλοφορίας
- Το τερματικό σημείο της σήραγγας, δηλαδή, την άκρη πελάτη ή την άκρη του δικτύου παροχής
- Το εάν προσφέρουν από σελίδα-σε-σελίδα ή απομακρυσμένη σύνδεση πρόσβασης
- Τα επίπεδα ασφαλείας που παρέχονται
- Το στρώμα του OSI που παρουσιάζουν για τη σύνδεση του δικτύου, όπως κυκλώματα επιπέδου 2 ή επιπέδου 3 σύνδεσης με το δίκτυο.

Έτσι για να αντιμετωπίσει η εταιρεία μας αυτή την επίθεση θα μπορούσε να συνεργαστεί με κάποια εταιρεία παροχής εικονικού ιδιωτικού δικτύου.

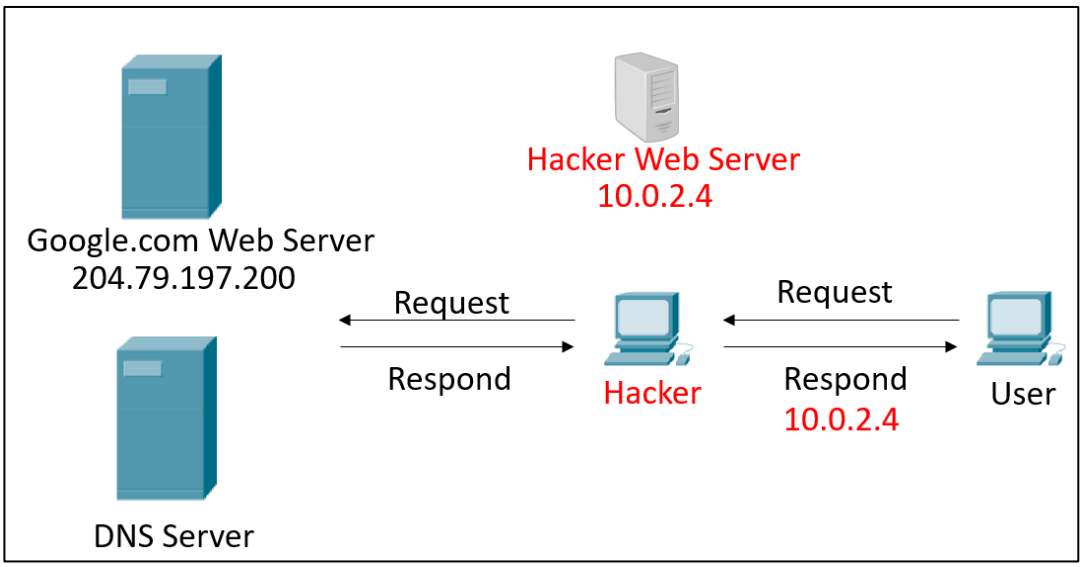
4.3 Εκτέλεση επίθεσης DNS Spoofing

Το πρωτόκολλο DNS παρουσιάστηκε στο κεφάλαιο 3 στο κομμάτι των διακομιστών. Όταν λοιπόν ένας χρήστης πληκτρολογήσει google.com σε ένα browser τότε το αίτημα πηγαίνει πρώτα στο διακομιστή DNS ο οποίος απαντάει με την διεύθυνση IP στην οποία τα αρχεία του google.com είναι αποθηκευμένα. Τέλος ο browser θα φορτώσει την ιστοσελίδα από αυτή τη διεύθυνση.



Εικόνα 4.12 Λειτουργία DNS

Ο επιτιθέμενος έχοντας κάνει τη διαδικασία να γίνει MITM όπως παρουσιάσαμε σε προηγούμενη ενότητα αντί να επιστρέψει την διεύθυνση του εξυπηρετητή μπορεί να δώσει οποία διεύθυνση IP αυτός θέλει. Μπορεί να ανακατευθύνει τον στόχο σε ιστοσελίδα ή δικό του διακομιστή.



Εικόνα 4.13 Λειτουργία Επίθεσης DNS Spoofing

Στην συγκεκριμένη παρουσίαση ο στόχος θα ανακατευθυνθεί σε μια ιστοσελίδα που είναι τοπική στο μηχάνημα του επιτιθέμενου. Το Kali Linux έρχεται με δικό του web server και το χρησιμοποιεί σαν ιστοσελίδα. Για να ξεκινήσει ο Web Server εκτελούμε την εντολή:

service apache2 start

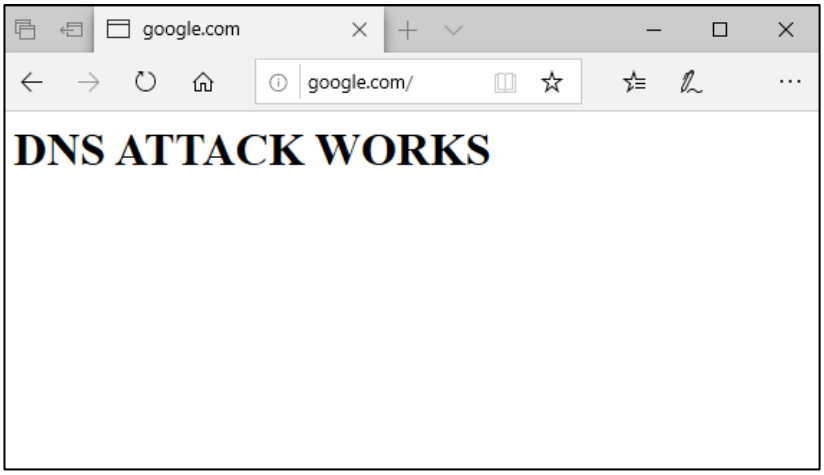
Για πρόσβαση στο web server αυτό που πρέπει να γίνει είναι να βάλουμε σε ένα browser την διεύθυνση του Kali Machine. Αυτό που θα γίνει είναι αν ο χρήστης πληκτρολογήσει κάποια ιστοσελίδα να τον οδηγεί στη συγκεκριμένη ιστοσελίδα.

- Αρχικά εκτελείται το bettercap με την εντολή:
  bettercap -iface eth0 -caplet /root/spoof.cap
- Στη συνέχεια χρησιμοποιείται μια ενότητα που ονομάζεται **dns.spoof.** Για να απαντήσει σε κάθε αίτημα DNS βάζουμε την εντολή: **set dns.spoof.all true**
- Τέλος, πρέπει να δηλωθούν τα domains που θα αποτελούν τον στόχο της επίθεσης.

Σε αυτή την ενότητα θα γίνει προσομοίωση ως προς το google.com με την εντολή **set dns. spoof. domains google.com** και τέλος **dns. spoof on**

Εικόνα 4.14 Εκτέλεση Εντολής dns. Spoof on

Οπότε τώρα αν ο στόχος βάλει το google.com στην αναζήτηση θα ανακατευθυνθεί σε οποία διεύθυνση έχουμε βάλει εμείς. Συγκεκριμένα στην custom σελίδα του kali.



Εικόνα 4.15 αποτέλεσμα Επίθεσης

4.4.1 Ο Ρόλος της Εταιρείας και η SQL

Η SQL είναι μία γλώσσα υπολογιστών στις βάσεις δεδομένων, που σχεδιάστηκε για τη διαχείριση δεδομένων, σε ένα σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων και η οποία, αρχικά, βασίστηκε στη σχεσιακή άλγεβρα. Η γλώσσα περιλαμβάνει δυνατότητες ανάκτησης και ενημέρωσης δεδομένων, δημιουργίας και τροποποίησης σχημάτων και σχεσιακών πινάκων, αλλά και ελέγχου πρόσβασης στα δεδομένα

Η SQL σημαίνει δομημένη γλώσσα ερωτημάτων. Χρησιμοποιείται για την επικοινωνία με μια βάση δεδομένων και είναι η τυπική γλώσσα για συστήματα διαχείρισης σχεσιακών βάσεων δεδομένων. Οι δηλώσεις SQL χρησιμοποιούνται για την εκτέλεση εργασιών όπως η ενημέρωση δεδομένων σε μια βάση δεδομένων ή η ανάκτηση δεδομένων από μια βάση δεδομένων.

Αν και τα περισσότερα συστήματα βάσεων δεδομένων χρησιμοποιούν SQL, τα περισσότερα από αυτά έχουν επίσης τις δικές τους πρόσθετες ιδιόκτητες επεκτάσεις που συνήθως χρησιμοποιούνται μόνο στο σύστημά τους. Ωστόσο, οι τυπικές εντολές SQL όπως «Select», «Insert», «Update», «Delete», «Create» και «Drop» μπορούν να χρησιμοποιηθούν για να ολοκληρώσουν σχεδόν οτιδήποτε χρειάζεται να κάνει κάποιος με μια βάση δεδομένων.

Ο ρόλος της εταιρείας που παρουσιάστηκε είναι να φιλοξενεί ιστοσελίδες στους εξυπηρετητές της. Πολλές από αυτές τις ιστοσελίδες χρησιμοποιούν βάσεις δεδομένων (οι οποίες φιλοξενούνται σε ένα εξυπηρετητή). Τα δεδομένα αυτά μπορεί να είναι είτε ονόματα χρηστών είτε κωδικοί είτε προϊόντα ηλεκτρονικών καταστημάτων. Η επίδραση με την βάση δεδομένων γίνεται με την SQL. Μια από τις πιο «σύνηθες» επιθέσεις που γίνονται σε εταιρείες σαν αυτή που παρουσιάσαμε είναι η SQL Injection.

4.4.2 Παρουσίαση Επίθεσης SQL Injection

Στόχος αυτής της επίθεσης είναι να περάσει κώδικας μέσα στη βάση δεδομένων. Για να εκτελεστεί αυτή η επίθεση, πρέπει να αλλάξει η πράξη και ο σκοπός του κατάλληλου ερωτήματος βάσης δεδομένων. Μια πιθανή μέθοδος για να γίνει αυτό είναι να γίνεται το ερώτημα πάντα αληθές και να εισάγεται ο κακόβουλος κώδικας μετά από αυτό. Η αλλαγή του ερωτήματος της βάσης δεδομένων σε πάντα αληθές μπορεί να πραγματοποιηθεί με απλό κώδικα όπως: **' ή 1=1;–**.

Έστω για παράδειγμα ότι μέσα στη βάση υπάρχει το εξής:

select * from customers cs where cs.job = 'search_job ';

Και με την παραπάνω μέθοδο να μετατραπεί σε:

select * from customers cs where cs.job = ' ' or 1=1; –

Σε αυτήν την περίπτωση, η παράμετρος κλείνει με το εισαγωγικό και μετά έχουμε κωδικό ή 1=1, που κάνει ένα ερώτημα πάντα αληθινό. Με το σύμβολο «–» σχολιάζουμε τον υπόλοιπο κώδικα ερωτήματος, ο οποίος δεν θα εκτελεστεί. Είναι ένας από τους πιο δημοφιλείς και ευκολότερους τρόπους για να ξεκινήσουμε τον έλεγχο του ερωτήματος. Μέσα λοιπόν σε αυτό μπορούμε να βάλουμε κώδικα ο οποίος θα δημιουργήσει πρόβλημα στη βάση δεδομένων για παράδειγμα να σβηστεί ένας πίνακας : **' or 1=1; drop table notes; — .**

Εάν αυτή η επίθεση πετύχει, τότε μπορεί να γραφτεί οποιοσδήποτε άλλος κακόβουλος κώδικας. Σε αυτήν την περίπτωση, θα εξαρτηθεί μόνο από τις γνώσεις και την πρόθεση του κακόβουλου χρήστη.

Στο λειτουργικό σύστημα Kali Linux μπορούμε να συνδεθούμε στη βάση ως εξής:

mysql -u root -h ip

mysql>show databases

mysql>use database_example

mysql>show tables;

mysql>select * from accounts;

Στην αρχή βάζω την διεύθυνση IP του διακομιστή, διαλέγω ποια βάση θέλω, και στο τέλος με το "*" επιλέγω τα πάντα από τη βάση.

Μπορώ να χρησιμοποιήσω το ΄ για να βάλω κώδικα σε ένα πεδίο συμπλήρωσης κωδικού για παράδειγμα:

Select * from accounts where username = 'admin' and password= '$PASSWORD'

Βάζω το **123456' and 1=1#** και οτιδήποτε μετα το "#" θα αγνοηθεί.

4.4.3 Πώς να εντοπιστεί η SQL Injection

Ο έλεγχος για αυτήν την ευπάθεια μπορεί να πραγματοποιηθεί πολύ εύκολα. Μερικές φορές αρκεί να πληκτρολογήσουμε « ή « στα δοκιμασμένα πεδία. Εάν επιστρέψει οποιοδήποτε απροσδόκητο ή ασυνήθιστο μήνυμα, τότε μπορούμε να είμαστε σίγουροι ότι η SQL Injection είναι δυνατή για αυτό το πεδίο. Για παράδειγμα, εάν λάβουμε ένα μήνυμα σφάλματος όπως "Εσωτερικό σφάλμα διακομιστή" ως αποτέλεσμα αναζήτησης, τότε μπορούμε να είμαστε σίγουροι ότι αυτή η επίθεση είναι δυνατή σε αυτό το μέρος του συστήματος.

Άλλα αποτελέσματα που ενδέχεται να ειδοποιήσουν μια πιθανή επίθεση περιλαμβάνουν:

• Φορτώθηκε κενή σελίδα.

• Χωρίς μηνύματα σφάλματος ή επιτυχίας – η λειτουργία και η σελίδα δεν αντιδρούν στην είσοδο.

• Μήνυμα επιτυχίας για κακόβουλο κώδικα.

Η πρώτη κιόλας δοκιμή συνήθως αποτελείται από την προσθήκη ενός μόνο εισαγωγικού ή ενός ερωτηματικού στο πεδίο ή στην παράμετρο υπό δοκιμή. Το πρώτο χρησιμοποιείται στην SQL ως τερματιστής συμβολοσειράς και εάν δεν φιλτραριστεί από την εφαρμογή, θα οδηγούσε σε εσφαλμένο ερώτημα. Το δεύτερο χρησιμοποιείται για τον τερματισμό μιας πρότασης SQL και εάν δεν φιλτράρεται, είναι επίσης πιθανό να δημιουργήσει ένα σφάλμα

Η επίθεση αυτή μπορεί να αντιμετωπιστεί με ορισμένες μεθόδους:

- Φίλτρα
- Χρήση μαύρης λίστας εντολών
- Χρήση λίστα επιτρεπόμενων εντολών
- Χρήση παραμετροποιημένων δηλώσεων, όπου τα δεδομένα και ο κώδικας είναι διαχωρισμένα.

Το σημαντικότερο είναι να προγραμματιστεί η εφαρμογή Web με έναν τρόπο που δεν επιτρέπει την εισαγωγή και εκτέλεση κώδικα.

4.5 Οι επιθέσεις ως προς το πρωτόκολλο MAC

Κατά την αποστολή δεδομένων σε άλλη συσκευή στο δίκτυο, το υποστρώμα MAC ενθυλακώνει πλαίσια υψηλότερου επιπέδου σε πλαίσια κατάλληλα για το μέσο μετάδοσης δηλαδή προσθέτει ένα προοίμιο συγχρονισμού, εντοπίζονται τα σφάλματα μετάδοσης με μια ακολουθία ελέγχου πλαισίου και στη συνέχεια προωθεί τα δεδομένα στο επίπεδο 1 μόλις το επιτρέψει η κατάλληλη μέθοδος πρόσβασης καναλιού. Επιπλέον, το MAC όπως αναφέραμε και στο κεφάλαιο 1 είναι επίσης υπεύθυνο για την αντιστάθμιση των συγκρούσεων με την έναρξη της αναμετάδοσης εάν ανιχνευθεί ένα σήμα εμπλοκής. Κατά τη λήψη δεδομένων από το φυσικό επίπεδο, με τη χρήση του MAC διασφαλίζεται η ακεραιότητα των δεδομένων με επαλήθευση των αλληλουχιών ελέγχου πλαισίου του αποστολέα.

Τα πρωτόκολλα ελέγχου πρόσβασης πολυμέσων (MAC) επιβάλλουν μια μεθοδολογία που επιτρέπει την πρόσβαση πολλών συσκευών σε ένα κοινόχρηστο δίκτυο πολυμέσων. Πριν από τα LAN, η επικοινωνία μεταξύ υπολογιστικών συσκευών ήταν από σημείο σε σημείο. Δηλαδή,

δύο συσκευές συνδέθηκαν με ένα αποκλειστικό κανάλι. Τα LAN είναι κοινόχρηστα δίκτυα πολυμέσων, στα οποία όλες οι συσκευές που είναι συνδεδεμένες στο δίκτυο λαμβάνουν κάθε μετάδοση και πρέπει να αναγνωρίζουν ποια πλαίσια πρέπει να δέχονται.

4.5.1 Επίθεση Mac address flooding

Για αυτή την επίθεση θα χρησιμοποιήσουμε το λειτουργικό Kali Linux και θα εκτελέσουμε την εντολή: **macof -I eth0**

Στο switch, εκτελώντας τις παρακάτω εντολές παρατηρούμε να έρχονται πακέτα από μια ύποπτη θύρα.

show mac address-table count

show mac address-table dynamic

Για να αντιμετωπίσουμε αυτή την επίθεση ενεργοποιούμε στο switch ένα χαρακτηριστικό ασφάλειας το port-security και αν μετά τρέξουμε τις ίδιες εντολές παρατηρούμε ότι μας βγάζει αρκετά μηνύματα.

- **Switchport mode access**
- **Switchport port-security**
- **Switchport port-security maximum 1**
- **Switchport port-security violation restrict**

Το Port Security μας επιτρέπει να προσδιορίσουμε τις διευθύνσεις MAC για κάθε θύρα, η ίδια η συσκευή μπορεί να ρυθμιστεί έτσι ώστε να μπλοκάρει κάποια ύποπτη MAC διεύθυνση ή να κλείσει τη θύρα και εμποδίζει το macof από το να γεμίσει τον πίνακα με τις MAC διευθύνσεις.

4.5.2 Επίθεση Mac Spoofing

Όπως αναφέραμε κάθε συσκευή που είναι συνδεδεμένη σε ένα δίκτυο διαθέτει μια μοναδική διεύθυνση MAC. Αυτή η εγγεγραμμένη διεύθυνση είναι τοποθετημένη στο υλικό από τον κατασκευαστή. Οι χρήστες δεν μπορούν να αλλάξουν ή να ξαναγράψουν τη διεύθυνση MAC. Αλλά είναι δυνατό να την καλύψουν από την πλευρά του λογισμικού. Αυτή η κάλυψη είναι αυτό που αναφέρεται ως πλαστογράφηση MAC ή αλλιώς MAC Spoofing.

Η διαδικασία για να γίνει αυτό είναι η εξής:

ifconfig wlan0 down

ifconfig wlan0 hw ether 00:11:22: 33:44:55

ifconfig wlan0 up

ifconfig wlan0

Αρχικά κλείνουμε τη θύρα, εκτελούμε την εντολή με μια δικιά μας διεύθυνση MAC και μετα ενεργοποιούμε τη θύρα.

4.6.1 Επίθεση DDOS

Άλλη μια αρκετά διαδεδομένη επίθεση που αντιμετωπίζουν τα δίκτυα εταιρειών σαν την δικιά μας είναι η Dos-DDoS. Μια επίθεση DOS (άρνηση υπηρεσίας) είναι μια κακόβουλη απόπειρα που γίνεται από παράγοντες απειλής για να επιτεθεί στη διαθεσιμότητα ενός στοχευμένου συστήματος. Αυτά τα στοχευμένα συστήματα μπορεί να είναι ένας ιστότοπος ή μια διαδικτυακή εφαρμογή. Σε αυτές τις επιθέσεις, οι εισβολείς δημιουργούν συνήθως μεγάλο όγκο πακέτων δεδομένων ή αιτημάτων με σκοπό να συντρίψουν το στοχευμένο σύστημα. Μια επίθεση DDoS μοιάζει πολύ με την επίθεση DOS, εκτός από το ότι οι εισβολείς χρησιμοποιούν πολλαπλές παραβιασμένες ή ελεγχόμενες πηγές για να δημιουργήσουν τεράστιους όγκους από αυτά τα αιτήματα ή πακέτα δεδομένων. Οι επιτιθέμενοι με DDoS το επιτυγχάνουν αυτό συντονίζοντας έναν στρατό από παραβιασμένες μηχανές σε ένα δίκτυο συσκευών που ελέγχουν από μια απομακρυσμένη τοποθεσία. Αυτά τα botnets ενδέχεται να πραγματοποιούν επιθέσεις DDoS με μια σειρά κακόβουλων τεχνικών όπως:

- Εξαντλώντας το εύρος ζώνης του δικτύου με τεράστιους όγκους κίνησης.
- Γεμίζοντας τους πόρους του συστήματός με μισάνοιχτα αιτήματα σύνδεσης.
- Συντρίβοντας διακομιστές εφαρμογών ιστού με ογκώδη αιτήματα για τυχαίες πληροφορίες.

4.6.2 Κατηγορίες Επιθέσεων Ανά Επίπεδο

Οι επιθέσεις DDoS μπορούν να διαχωριστούν ανάλογα με το επίπεδο του μοντέλου OSI που επιτίθενται. Είναι πιο συνηθισμένες στο επίπεδο δικτύου, μεταφοράς, παρουσίασης και εφαρμογής. Για παράδειγμα,

• Οι επιθέσεις ανάκλασης UDP στοχεύουν το επίπεδο δικτύου (Επίπεδο 3)

• Οι επιθέσεις SYN Flooding στοχεύουν το επίπεδο μεταφοράς (Επίπεδο 4)

• Η κατάχρηση SSL στοχεύει το επίπεδο παρουσίασης (Επίπεδο 6)

• Οι επιθέσεις HTTP Flooding και DNS Flooding στοχεύουν το επίπεδο εφαρμογής (Επίπεδο 7)

Έτσι, μπορούμε εύκολα να αναγνωρίσουμε 2 ευρείες κατηγορίες επιθέσεων DDoS:

- Επιθέσεις στρώματος υποδομής

Οι επιθέσεις στα επίπεδα 3 και 4 κατηγοριοποιούνται συνήθως ως επιθέσεις στο επίπεδο υποδομής. Αυτές είναι επίσης οι πιο συνηθισμένες επιθέσεις DDoS και περιλαμβάνουν φορείς όπως συγχρονισμένες πλημμύρες (SYN) και άλλες επιθέσεις ανάκλασης όπως πλημμύρες πακέτων δεδομένων γραμμάτων χρήστη (UDP), όπως αναφέραμε παραπάνω. Αυτές οι επιθέσεις είναι συνήθως μεγάλου όγκου και στοχεύουν στην υπερφόρτωση της χωρητικότητας του δικτύου ή των διακομιστών εφαρμογών. Αλλά ευτυχώς, είναι και αυτοί οι τύποι επιθέσεων που έχουν σαφείς υπογραφές. Γι' αυτό είναι πιο εύκολο να εντοπιστούν.

- 2. Επιθέσεις επιπέδου εφαρμογής

Οι επιθέσεις στα επίπεδα 6 και 7 συχνά κατηγοριοποιούνται ως επιθέσεις επιπέδου εφαρμογής. Αν και αυτές οι επιθέσεις είναι λιγότερο συχνές, τείνουν επίσης να είναι πιο περίπλοκες. Αυτές οι επιθέσεις είναι συνήθως μικρές σε όγκο σε σύγκριση με τις επιθέσεις του επιπέδου υποδομής, αλλά τείνουν να εστιάζουν σε συγκεκριμένα ακριβά μέρη της εφαρμογής καθιστώντας το μη διαθέσιμο για πραγματικούς χρήστες. Για παράδειγμα, μια πλημμύρα αιτημάτων HTTP.

4.6.3 Οι γενικοί τύποι επιθέσεων DDoS

Η κατανεμημένη άρνηση υπηρεσίας (DDoS) είναι μια ευρεία κατηγορία κυβερνοεπιθέσεων που διακόπτει τις διαδικτυακές υπηρεσίες και τους πόρους κατακλύζοντάς τους από επισκεψιμότητα. Αυτό καθιστά τη στοχευμένη διαδικτυακή υπηρεσία εκτός λειτουργίας κατά τη διάρκεια της επίθεσης DDoS. Το σήμα κατατεθέν των επιθέσεων DDoS είναι η κατανεμημένη φύση της κακόβουλης κυκλοφορίας, η οποία συνήθως προέρχεται από ένα botnet - ένα εγκληματικά ελεγχόμενο δίκτυο παραβιασμένων μηχανών που είναι εξαπλωμένο σε όλο τον κόσμο. Με τα χρόνια, οι εγκληματίες του κυβερνοχώρου έχουν αναπτύξει μια σειρά από τεχνικές προσεγγίσεις για την εξάλειψη διαδικτυακών στόχων μέσω DDoS. Οι επιμέρους τεχνικές τείνουν να εμπίπτουν σε τρεις γενικούς τύπους επιθέσεων DDoS:

- Ογκομετρικές επιθέσεις

Ο κλασικός τύπος DDoS, αυτές οι επιθέσεις χρησιμοποιούν μεθόδους για τη δημιουργία τεράστιου όγκου επισκεψιμότητας για πλήρη κορεσμό του εύρους ζώνης, δημιουργώντας

κυκλοφοριακή συμφόρηση που καθιστά αδύνατη τη ροή νόμιμης κυκλοφορίας προς ή έξω από τη στοχευμένη τοποθεσία.

- Επιθέσεις πρωτοκόλλου

Οι επιθέσεις πρωτοκόλλου έχουν σχεδιαστεί για να καταναλώνουν την ικανότητα επεξεργασίας των πόρων υποδομής δικτύου όπως διακομιστές, τείχη προστασίας και εξισορροπητές φορτίου στοχεύοντας επικοινωνίες πρωτοκόλλου επιπέδου 3 και επιπέδου 4 με κακόβουλα αιτήματα σύνδεσης.

- Επιθέσεις εφαρμογών

Μερικές από τις πιο εξελιγμένες επιθέσεις DDoS, αυτές εκμεταλλεύονται τις αδυναμίες στο επίπεδο εφαρμογής - Layer 7 - ανοίγοντας συνδέσεις και εκκινώντας αιτήματα διεργασιών και συναλλαγών που καταναλώνουν πεπερασμένους πόρους όπως ο χώρος στο δίσκο και η διαθέσιμη μνήμη.

Σε σενάρια επιθέσεων του πραγματικού κόσμου, οι εγκληματίες αρέσκονται να συνδυάζουν αυτούς τους τύπους επιθέσεων για να αυξήσουν την ζημιά. Έτσι, μια μεμονωμένη επίθεση DDoS μπορεί να στρώσει επιθέσεις πρωτοκόλλου και εφαρμογών πάνω από ογκομετρικές επιθέσεις.

4.6.4 Ανασκόπηση συγκεκριμένων επιθέσεων DDoS

- UDP and ICMP flood

Μερικές από τις πιο συνηθισμένες ογκομετρικές επιθέσεις είναι αυτές που κατακλύζουν τους πόρους του κεντρικού υπολογιστή είτε με πακέτα User Datagram Protocol (UDP) είτε με αιτήματα echo του Πρωτοκόλλου Ελέγχου Μηνυμάτων Διαδικτύου (ICMP), μέχρι να κατακλυστεί η υπηρεσία. Οι εισβολείς τείνουν να ενισχύουν τη ροή συντριβής αυτών των πλημμυρών μέσω επιθέσεων ανάκλασης, οι οποίες πλαστογραφούν τη διεύθυνση IP του θύματος για να υποβάλουν το αίτημα UDP ή ICMP. Το κακόβουλο πακέτο φαίνεται να προέρχεται από το θύμα και έτσι ο διακομιστής στέλνει την απάντηση πίσω στον εαυτό του.

- SYN flood

Μία από τις πιο κοινές επιθέσεις πρωτοκόλλου, οι επιθέσεις πλημμύρας SYN παρακάμπτουν την τριμερή διαδικασία χειραψίας που απαιτείται για τη δημιουργία συνδέσεων TCP μεταξύ πελατών και διακομιστών. Αυτές οι συνδέσεις γίνονται συνήθως με τον πελάτη να κάνει ένα αρχικό αίτημα συγχρονισμού (SYN) του διακομιστή, ο διακομιστής να απαντά με μια απόκριση επιβεβαίωσης (SYN-ACK) και ο πελάτης να ολοκληρώνει τη χειραψία με μια τελική επιβεβαίωση (ACK). Οι πλημμύρες SYN λειτουργούν κάνοντας μια ταχεία διαδοχή

αυτών των αρχικών αιτημάτων συγχρονισμού και αφήνοντας τον διακομιστή να κρέμεται χωρίς να μην απαντάτε ποτέ με μια τελική επιβεβαίωση. Τελικά ο διακομιστής καλείται να κρατήσει ανοιχτές μια δέσμη μισάνοιχτων συνδέσεων που τελικά κατακλύζουν τους πόρους, συχνά σε σημείο που ο διακομιστής διακόπτεται. Περισσότερα για αυτή την επίθεση θα δούμε στη συνέχεια του κεφαλαίου.

- Το ping του θανάτου

Ένας άλλος τύπος επίθεσης πρωτοκόλλου, οι επιθέσεις ping of death διαφέρουν από τις επιθέσεις πλημμύρας ICMP echo ping, καθώς το περιεχόμενο του ίδιου του πακέτου έχει σχεδιαστεί με κακόβουλο τρόπο ώστε να προκαλεί δυσλειτουργία του συστήματος από την πλευρά του διακομιστή. Τα δεδομένα που περιέχονται σε μια κανονική επίθεση πλημμύρας ping είναι σχεδόν ασήμαντα - προορίζονται απλώς να συντρίψουν το εύρος ζώνης με τον όγκο του. Σε μια επίθεση ping of death, ο εγκληματίας επιδιώκει να εκμεταλλευτεί τα τρωτά σημεία στο στοχευμένο σύστημα με περιεχόμενο πακέτου που προκαλεί το πάγωμα ή τη συντριβή του. Αυτή η μέθοδος μπορεί επίσης να επεκταθεί σε άλλα πρωτόκολλα πέρα από το ICMP, συμπεριλαμβανομένων των UDP και TCP. Μια τέτοια επίθεση μπορεί να εκτελεστεί με την εντολη: **ping <ip address> -1 65500 -w 1 -n 1** όπου στο κομμάτι του ip address βάζουμε την διεύθυνση του στόχου, και έτσι αυτή η εντολη θα στείλει ένα πακέτο μεγαλύτερο του 65500 Bytes στη συσκευή. Υπάρχουν δυο τρόποι για να αντιμετωπιστεί αυτή η επίθεση. Ο ένας είναι να μπλοκάρουμε το Ping από τα Iptables τα οποία είναι τείχη προστασίας γραμμής εντολών και ο δεύτερος τρόπος ο οποίος χρησιμοποιείται στο δίκτυο της εταιρείας μας είναι να μπλοκάρουμε τα ICMP Ping μηνύματα στο τείχος προστασίας μας.

- HTTP flood

Οι επιθέσεις πλημμύρας HTTP είναι ένας από τους πιο διαδεδομένους τύπους επιθέσεων DDoS επιπέδου εφαρμογής. Με αυτή τη μέθοδο, ο εγκληματίας κάνει κάτι που φαίνεται να είναι κανονικές αλληλεπιδράσεις με έναν διακομιστή ιστού ή μια εφαρμογή. Όλες οι αλληλεπιδράσεις προέρχονται από προγράμματα περιήγησης ιστού για να μοιάζουν με κανονική δραστηριότητα χρήστη, αλλά είναι συντονισμένες ώστε να χρησιμοποιούνται όσο το δυνατόν περισσότεροι πόροι από τον διακομιστή. Το αίτημα που θα μπορούσε να κάνει ο εισβολέας περιλαμβάνει οτιδήποτε, από την κλήση διευθύνσεων URL για εικόνες ή έγγραφα με αιτήματα GET έως την πραγματοποίηση κλήσεων επεξεργασίας από τον διακομιστή σε μια βάση δεδομένων από αιτήματα POST.

4.6.5 Εκτέλεση της επίθεσης

Έχοντας τις δυο εικονικές μηχανές kali Linux και Windows 10, αρχικά ελέγχω την συνδεσιμότητα τους. Στην μηχανή kali χρησιμοποιώντας το εργαλείο Metasploit εκτελώ τις εντολές:

- **Msfconsole**
- **Search synflood**
- **Use auxiliary/dos/tcp/synflood**
- **Show options**
- **Set RHOSTS IP**
- **Set RPORT 135**
- **Set NUM 10000**
- **Exploit**

Πριν την εκτέλεση της εντολής exploit θα ανοίξουμε ένα wireshark για να παρατηρήσουμε τι συμβαίνει και να μελετήσουμε τα πακέτα που ανταλλάσσονται.

4.6.6 Τρόπος αντιμετώπισης της επίθεσης

Οι προστασία από DDoS θα πρέπει να αποτελεί βασικό επίπεδο σε οποιαδήποτε ώριμη στρατηγική κυβερνοασφάλειας. Οι ομάδες ασφαλείας μπορούν να το επιτύχουν αυτό μέσω της προληπτικής ανάπτυξης άμυνας, της προετοιμασίας αποτελεσματικών σχεδίων απόκρισης DDoS και της διατήρησης των τάσεων απειλών για να τροποποιήσουν αυτές τις προετοιμασίες καθώς αλλάζουν οι μέθοδοι επίθεσης DDoS. Πρέπει να γίνει προετοιμασία της υποδομής με:

- Δυνατότητες παρακολούθησης για τον εντοπισμό πρώιμων ενδείξεων επιθέσεων DDoS.
- Υποδομές που μπορούν να εκτρέψουν και να εξαλείψουν την κυκλοφορία DDoS.
- Κατασκευή ανθεκτικών εξαρτημάτων δικτύου που μπορούν να φιλοξενήσουν σενάρια επιθέσεων που δημιουργούν φορτία κυκλοφορίας πάνω από τα κανονικά επίπεδα.
- Σχεδιασμός και εκτέλεση απόκρισης.
- Δημιουργία ενός σχεδίου και μια ομάδα εργασίας για την αποκατάσταση επιθέσεων DDoS όταν συμβαίνουν.
- Δημιουργία σχεδίων επικοινωνίας κατά τη διάρκεια μιας επίθεσης σε περίπτωση που επηρεαστούν οι υπηρεσίες που βασίζονται σε IP.

- Έρευνα τοπίου απειλών.
- Ενημέρωση για τις μεθόδους επίθεσης DDoS για να διασφαλιστεί ότι ο σχεδιασμός είναι επαρκής για μελλοντικές επιθέσεις.

4.6.7 Προσομοίωση της επίθεσης SYN Flood

Θα χρησιμοποιήσουμε το ανοιχτού κώδικα εργαλείο Kali Linux για να προσομοιώσουμε μια πλημμύρα SYN. Αυτό περιλαμβάνει το χτύπημα του διακομιστή-στόχου μας με μεγάλο αριθμό πακέτων SYN και να δούμε πώς επηρεάζει την εμπειρία χρήστη. Θα περιοριστούμε σε μια επίθεση χαμηλού όγκου με λίγους υπολογιστές. Ο όγκος επίθεσης: πέντε υπολογιστές οι οποίοι χρειάζονται root άδεια στους τρέχοντες χρήστες ,ξεκινώντας από 50.000 SYN πακέτα ανά δευτερόλεπτο.

Σε καθέναν από τους υπολογιστές, εκτελούμε την ακόλουθη εντολή:

$ sudo hping3 -i u20 -S -p 80 -c 50000 192.x.x.x

-S καθορίζει τα SYN πακέτα που στέλνονται

-p 80 στοχεύει τη θύρα 80

-i u20 περιμένει 20 microseconds μεταξύ των πακέτων άρα 50,000 πακέτα ανά δευτερόλεπτο

```
HPING 192.x.x.x (eth0 192.168.1.1): S set, 40 headers
+ 0 data bytes

--- 192.x.x.x hping statistic ---

50000 packets transmitted, 0 packets received, 100%
packet loss

round-trip min/avg/max = 0.0/0.0/0.0 ms
```

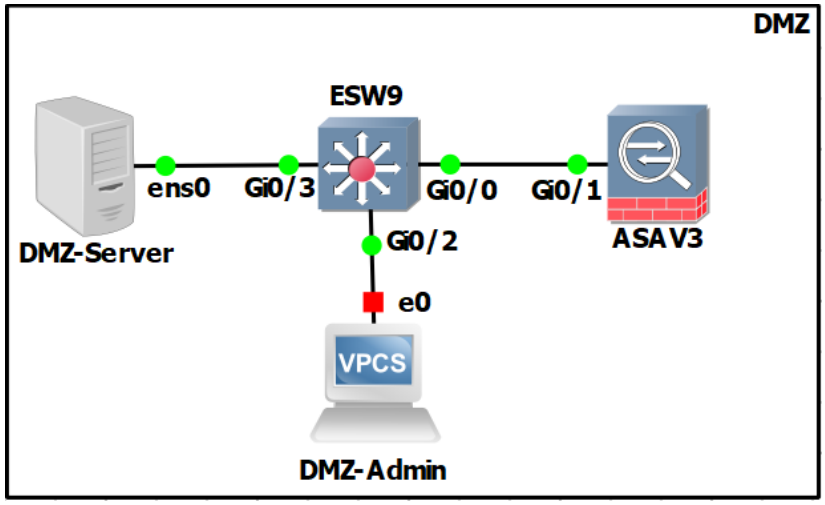
Εικόνα 4.16 Αποτέλεσμα Επίθεσης Syn Flood

4.7 Περιοχή DMZ

Σημαντική προσθήκη επίσης στο δίκτυο μας είναι το dmz zone (demilitarized zone). Αυτή η ζώνη χρησιμοποιείται για να βελτιώσει την ασφάλεια του δικτύου μιας εταιρείας διαχωρίζοντας συσκευές όπως υπολογιστές και εξυπηρετητές σε αντίθετες πλευρές του τείχους προστασίας. Είναι σαν να δημιουργεί δυο διαφορετικά δίκτυα. Σε αυτή την εταιρεία έχουμε διακομιστές στους οποίους έχουν πρόσβαση άτομα από το διαδίκτυο όπως για παράδειγμα διακομιστές WEB. Τώρα επειδή αυτοί οι διακομιστές είναι πίσω από το firewall είναι μέσα στο ιδιωτικό δίκτυο της εταιρείας. Αυτό σημαίνει ότι η εταιρεία επιτρέπει σε κόσμο από μη

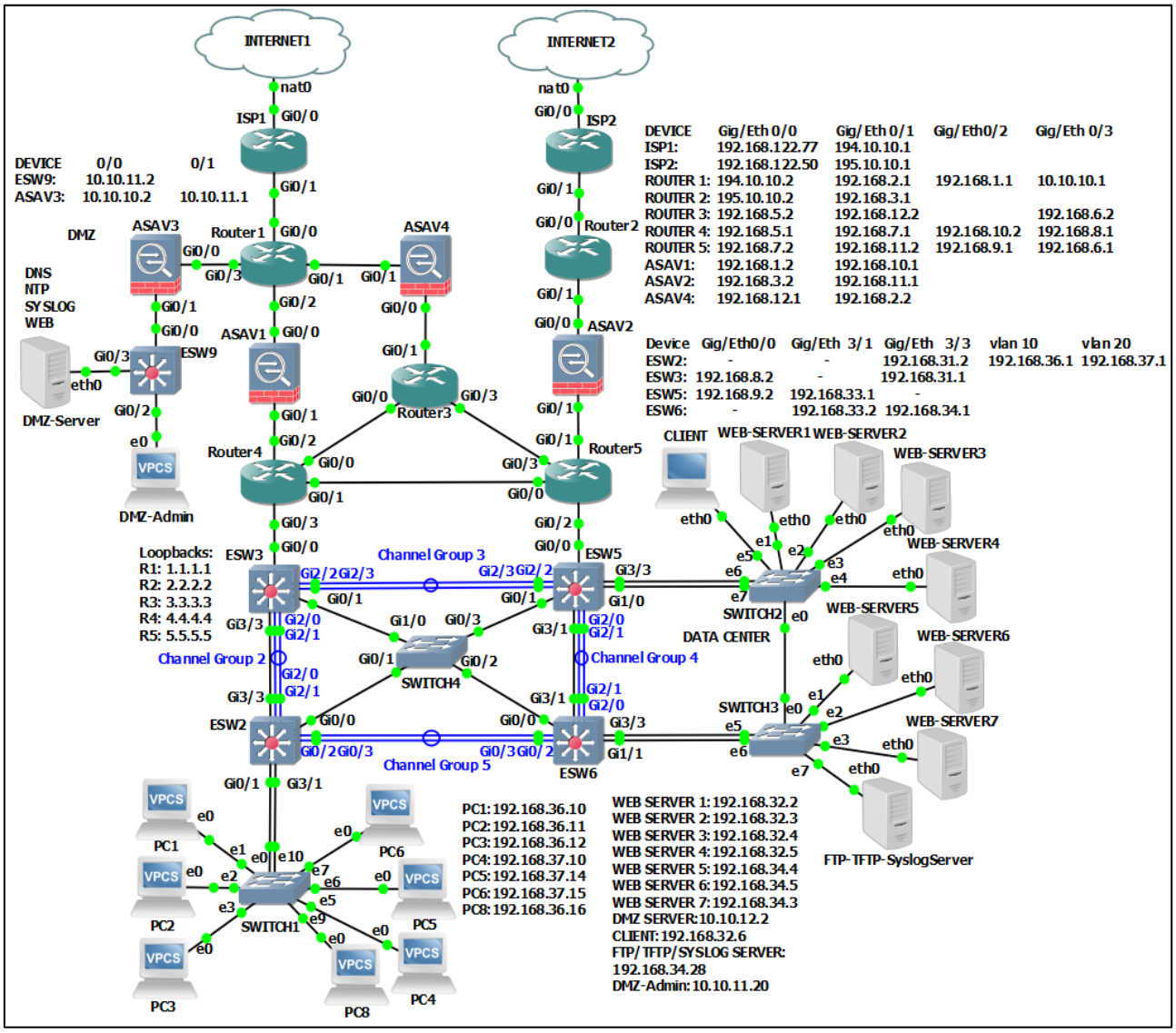
έμπιστα δίκτυα να έχουν πρόσβαση στο δίκτυο και αυτό προκαλεί ανησυχία στο κομμάτι της ασφάλειας επειδή όσο ο κόσμος έχει πρόσβαση στους διακομιστές αυτούς εισβολείς μπορούν να το χρησιμοποιήσουν σαν άνοιγμα για να προκαλέσουν ζημιά στο δίκτυο της εταιρείας. Έτσι οι εισβολείς μπορούν να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα από άλλες συσκευές που είναι πίσω από το firewall όπως για παράδειγμα ένας database server, ή ακόμα χειροτέρα να προσπαθήσουν να εγκαταστήσουν κάποιον ιό. Έτσι η εταιρεία πρέπει να τοποθετήσει κάποιες συσκευές εκτός του εσωτερικού δικτύου. Τώρα αυτές οι συσκευές ορίζουν το DMZ η αλλιώς περιμετρικό δίκτυο . Έτσι το DMZ χωρίζει το δίκτυο σε δυο μέρη παίρνοντας συσκευές μέσα από το δίκτυο και μετα βάζοντας τες εκτός firewall. Όμως μια καλύτερη τροποποίηση του δικτύου θα ήταν το DMZ να έχει και αυτό δικό του τείχος προστασίας. Αυτή η κίνηση προσθέτει ένα επιπλέον στάδιο προστασίας. Τέλος, για να υπάρξει συνδεσιμότητα του DMZ με το διαδίκτυο θα πρέπει να επιτραπεί από τον πάροχο με την τοποθέτηση της εντολής: **access-list 1 permit 10.10.10.0 0.0.255.255** στον ISP1.

Η DMZ ζώνη στο δίκτυο μας αποτελείται από τις εξής συσκευές. Ένα Firewall-Asav 3, ένα Switch επιπέδου 3-ESW9, έναν υπολογιστή το DMZ-Admin PC για τον διαχειριστή της ζώνης, ένα εξυπηρετητή Ubuntu Server που παρέχει DNS,NTP,Syslog,WEB υπηρεσίες.



Εικόνα 4.17 Ζώνη DMZ

Με βάση τα παραπάνω το δίκτυο της εταιρείας όταν προστεθεί το DMZ θα τροποποιηθεί ως εξής:



Εικόνα 4.18 Τοπολογία Τελικού Δικτύου Εταιρείας

4.8 ACL

Στην ασφάλεια υπολογιστών, μια λίστα ελέγχου πρόσβασης (ACL) είναι μια λίστα δικαιωμάτων που σχετίζονται με έναν πόρο συστήματος. Μια ACL καθορίζει σε ποιους χρήστες ή διεργασίες συστήματος εκχωρείται πρόσβαση σε αντικείμενα, καθώς και ποιες λειτουργίες επιτρέπονται σε δεδομένα αντικείμενα. Κάθε καταχώρηση σε ένα τυπικό ACL καθορίζει ένα θέμα και μια λειτουργία. Μια λίστα ελέγχου πρόσβασης (ACL) περιέχει κανόνες που παρέχουν ή αρνούνται την πρόσβαση σε ορισμένα ψηφιακά περιβάλλοντα. Αρχικά, τα ACL ήταν ο μόνος τρόπος για να επιτευχθεί προστασία τείχους προστασίας. Σήμερα,

υπάρχουν πολλοί τύποι τειχών προστασίας και εναλλακτικές λύσεις για τα ACL. Ωστόσο, εταιρείες σαν την δικιά μας συνεχίζουν να χρησιμοποιούν ACL σε συνδυασμό με τεχνολογίες όπως τα εικονικά ιδιωτικά δίκτυα (VPN) που καθορίζουν ποια κίνηση πρέπει να κρυπτογραφηθεί και να μεταφερθεί μέσω μιας σήραγγας VPN. Όταν χρησιμοποιείται ένα ACL υπάρχει έλεγχος ροής της κυκλοφορίας, περιορισμένη κίνηση δικτύου για καλύτερη απόδοση και ομαλή παρακολούθηση της κυκλοφορίας εξόδου και εισόδου στο σύστημα. Ένα σύστημα αρχείων ACL είναι ένας πίνακας που ενημερώνει ένα λειτουργικό σύστημα υπολογιστή για τα δικαιώματα πρόσβασης που έχει ένας χρήστης σε ένα αντικείμενο συστήματος, συμπεριλαμβανομένου ενός μεμονωμένου αρχείου ή ενός καταλόγου αρχείων. Κάθε αντικείμενο έχει μια ιδιότητα ασφαλείας που το συνδέει με τη λίστα ελέγχου πρόσβασης. Η λίστα έχει μια καταχώρηση για κάθε χρήστη με δικαιώματα πρόσβασης στο σύστημα. Τα ACL δικτύωσης εγκαθίστανται σε δρομολογητές ή μεταγωγείς, όπου λειτουργούν ως φίλτρα κυκλοφορίας. Κάθε ACL δικτύου περιέχει προκαθορισμένους κανόνες που ελέγχουν ποια πακέτα ή ενημερώσεις δρομολόγησης επιτρέπεται ή απαγορεύεται η πρόσβαση σε ένα δίκτυο. Οι δρομολογητές και οι μεταγωγείς με ACL λειτουργούν σαν φίλτρα πακέτων που μεταφέρουν ή απορρίπτουν πακέτα με βάση κριτήρια φιλτραρίσματος. Ως συσκευή επιπέδου 3, ένας δρομολογητής φιλτραρίσματος πακέτων χρησιμοποιεί κανόνες για να δει εάν η κυκλοφορία πρέπει να επιτρέπεται ή να απαγορεύεται η πρόσβαση. Το αποφασίζει με βάση τις διευθύνσεις IP προέλευσης και προορισμού, τη θύρα προορισμού και τη θύρα προέλευσης και την επίσημη διαδικασία του πακέτου. Οι λίστες ελέγχου πρόσβασης μπορούν να προσεγγιστούν σε σχέση με δύο κύριες κατηγορίες:

- Τυπική ACL

Μια λίστα πρόσβασης που αναπτύσσεται αποκλειστικά χρησιμοποιώντας τη διεύθυνση IP προέλευσης. Αυτές οι λίστες ελέγχου πρόσβασης επιτρέπουν ή αποκλείουν ολόκληρη τη σουίτα πρωτοκόλλων. Χρησιμοποιούν αριθμούς 1-99 ή 1300-1999, ώστε ο δρομολογητής να μπορεί να αναγνωρίσει τη διεύθυνση ως τη διεύθυνση IP προέλευσης.

- Εκτεταμένη ACL

Μια λίστα πρόσβασης που χρησιμοποιείται ευρέως καθώς μπορεί να διαφοροποιήσει την κίνηση IP. Χρησιμοποιεί και διευθύνσεις IP προέλευσης και προορισμού και αριθμούς θυρών για να κατανοήσει την κίνηση IP. Μπορούμε επίσης να καθορίσουμε ποια κίνηση IP θα επιτρέπεται ή θα απορρίπτεται. Χρησιμοποιούν τους αριθμούς 100-199 και 2000-2699. Στο κεφάλαιο 3 έγινε χρήση των ACL στο κομμάτι του NAT ώστε να δείξουμε ποιο εύρος διευθύνσεων θα μεταφραστεί.

4.9 Τείχη Προστασίας Firewall

Μια νέα προσθήκη στο δίκτυο είναι τα firewall. Το τείχος προστασίας είναι ένα σύστημα ασφάλειας δικτύου που ελέγχει και παρακολουθεί την εισερχόμενη και εξερχόμενη κίνηση δικτύου. Τα τείχη προστασίας έχουν δύο τύπους, ο πρώτος είναι τείχη προστασίας υλικού και ο άλλος είναι τείχη προστασίας λογισμικού. Τα τείχη προστασίας υλικού έχουν ξεχωριστό υλικό με δικό τους λειτουργικό σύστημα, CPU, RAM και διαφορετικούς τύπους διεπαφών (θύρες). Τείχος προστασίας λογισμικού, είναι ένα λογισμικό που μπορεί να εγκατασταθεί σε άλλα λειτουργικά συστήματα όπως Windows, Linux και MAC. Οι συμπεριφορές του τείχους προστασίας εξαρτώνται πάντα από γραπτές πολιτικές. Στα τείχη προστασίας, πρέπει να γράψουμε κανόνες εισερχόμενους και εξερχόμενους και κάθε πακέτο που προσπαθεί να περάσει το όριο (Inbound to Outbound ή Outbound to Inbound), πρώτα ελέγχεται από τις γραπτές πολιτικές. Εάν το πακέτο επισημανθεί ως επιτρεπόμενο στη λίστα πολιτικών του τείχους προστασίας, τότε μπορεί να διασχίσει το τείχος προστασίας, διαφορετικά το τείχος προστασίας απορρίπτει αυτό το πακέτο. Τα τείχη προστασίας συνήθως βρίσκονται μεταξύ ενός αξιόπιστου δικτύου και ενός μη αξιόπιστου δικτύου. Μερικοί εισβολείς προσπαθούν να στείλουν κακόβουλη κίνηση σε τυχαίες θύρες με την ελπίδα ότι αυτές οι θύρες έχουν μείνει "ανοιχτές", που σημαίνει ότι μπορούν να λαμβάνουν κίνηση. Για το λόγο αυτό, τα τείχη προστασίας θα πρέπει να ρυθμιστούν ώστε να αποκλείουν την κυκλοφορία δικτύου που κατευθύνεται στις περισσότερες από τις διαθέσιμες θύρες. Τα σωστά διαμορφωμένα τείχη προστασίας αποκλείουν την κυκλοφορία σε όλες τις θύρες από προεπιλογή, εκτός από μερικές προκαθορισμένες θύρες που είναι γνωστό ότι χρησιμοποιούνται συνήθως. Για παράδειγμα, ένα εταιρικό τείχος προστασίας θα μπορούσε να αφήσει ανοιχτές μόνο τις θύρες 25 (email), 80 (διακίνηση Ιστού), 443 (ασφαλείς διακίνηση Ιστού) και μερικές άλλες, επιτρέποντας στους εσωτερικούς υπαλλήλους να χρησιμοποιούν αυτές τις βασικές υπηρεσίες και στη συνέχεια να αποκλείσουν τις υπόλοιπες 65.000+ θύρες.

- Ζώνες τείχους προστασίας

Στα τείχη προστασίας έχουμε 3 ζώνες. Στην εσωτερική ζώνη , έχουμε διάφορους μεταγωγείς και δρομολογητές. Οι περισσότεροι από τους τελικούς χρήστες είναι εκεί και εργάζονται για μια εταιρεία. Στην Εξωτερική Ζώνη, υπάρχει το παγκόσμιο διαδίκτυο. Στην αποστρατιωτικοποιημένη ζώνη, έχουμε τους διακομιστές μας όπως Web Server, FTP Server. Αυτή η ζώνη είναι κοινώς γνωστή ως DMZ. Άτομα εκτός του Διαδικτύου μπορούν να έχουν πρόσβαση στους διακομιστές στη ζώνη DMZ, όπως ο Διακομιστής Ιστού. Στο τείχος

προστασίας Cisco ASAv που χρησιμοποιούμε στο δίκτυο μας, πρέπει να ορίσουμε ένα επίπεδο ασφάλειας για κάθε διεπαφή. Όσο υψηλότερο είναι το επίπεδο ασφάλειας, τόσο μεγαλύτερη είναι η εμπιστοσύνη σε αυτό το πλευρικό δίκτυο. Στο παρακάτω σχήμα βλέπουμε πως έχουν ρυθμιστεί τα interfaces στα τείχη προστασίας μας. Οι θύρες οι οποίες είναι ορισμένες σαν εξωτερικές έχουν επίπεδο ασφαλείας 0 ενώ αυτές που είναι ορισμένες σαν εσωτερικές έχουν επίπεδο ασφαλείας 100.

FIREWALL	GigEth0/0	GigEth 0/1
ASAV 1:	outside	inside
ASAV 2:	outside	inside
ASAV 3:	outside	inside
ASAV 4:	inside	outside

Αρχικά στο δίκτυο του κεφαλαίου 3, οι εσωτερικές συσκευές του δικτύου μπορούν να κάνουν ping τους δρομολογητές Router 1 και Router 2 αλλά όχι το αντίθετο έτσι ώστε αν κάποιος εισβολέας συνδεθεί σε αυτούς τους δρομολογητές να μην μπορεί να φτάσει το δίκτυο. Αυτό γίνεται εξαιτίας ενός κανόνα που έχουμε βάλει στα τείχη προστασίας μας και αφορά την επιθεώρηση του ICMP πρωτοκόλλου που είδαμε σε προηγούμενο κεφάλαιο - ICMP Inspection. Η ίδια ρύθμιση έχει γίνει και για το τείχος προστασίας του DMZ.

4.10 Πρωτόκολλα και θύρες

Μια θύρα είναι ένα εικονικό σημείο όπου ξεκινούν και τελειώνουν οι συνδέσεις δικτύου. Οι θύρες βασίζονται σε λογισμικό και διαχειρίζονται από το λειτουργικό σύστημα ενός υπολογιστή. Κάθε θύρα σχετίζεται με μια συγκεκριμένη διαδικασία ή υπηρεσία. Οι θύρες επιτρέπουν στους υπολογιστές να κάνουν εύκολα διαφοροποίηση μεταξύ διαφορετικών ειδών κίνησης. Οι θύρες είναι τυποποιημένες σε όλες τις συσκευές που είναι συνδεδεμένες στο δίκτυο, με κάθε θύρα να εκχωρεί έναν αριθμό. Οι περισσότερες θύρες είναι δεσμευμένες για συγκεκριμένα πρωτόκολλα — για παράδειγμα, όλα τα μηνύματα Hypertext Transfer Protocol (HTTP) πηγαίνουν στη θύρα 80. Ενώ οι διευθύνσεις IP επιτρέπουν στα μηνύματα να μεταβαίνουν από και προς συγκεκριμένες συσκευές, οι αριθμοί θυρών επιτρέπουν τη στόχευση συγκεκριμένων υπηρεσιών ή εφαρμογών εντός αυτών των συσκευών. Στο επόμενο σχήμα βλέπουμε μερικά από τα πρωτόκολλα που αφορούν το δίκτυο μας και τι πύλες χρησιμοποιούν.

protocols	Port numbers
DNS	53
HTTP	80
HTTPS	443
SSH	22
Telnet	23
DHCP	67,68
FTP	20,21
TCP/UDP	135

Εικόνα 4.19 Αντιστοίχιση Πρωτοκόλλων Με Θύρες

Οι θύρες και τα πρωτόκολλα παίζουν ουσιαστικό ρόλο στη δικτύωση. Στη δικτύωση υπολογιστών, οι θύρες είναι μια εικονική διαδρομή από την πηγή στον προορισμό. Έτσι, κάθε φορά που ένας χρήστης ζητά υπηρεσίες σε διακομιστές, το ίδιο το σύστημά του προσθέτει έναν αριθμό θύρας προέλευσης και έναν αριθμό θύρας προορισμού. Οι θύρες έχουν τρεις τύπους Well Known, Registered και Private.

- Well known: 0-1023
- Registered: 1024 έως 49151
- Private: 49152 έως 65 535

4.11 Πρωτόκολλο SSH και Telnet

Το SSH (Secure Shell) είναι ένα ασφαλές δικτυακό πρωτόκολλο το οποίο επιτρέπει τη μεταφορά δεδομένων μεταξύ δύο υπολογιστών. Το SSH αρχικά κρυπτογραφεί τα δεδομένα που ανταλλάσσονται κατά τη συνεδρία και επίσης προσφέρει ένα ασφαλές σύστημα αναγνώρισης καθώς και άλλα χαρακτηριστικά όπως ασφαλή μεταφορά αρχείων. Το TELNET και το SSH είναι και τα δύο πρωτόκολλα επιπέδου εφαρμογής Layer - 7 όπως είδαμε στο κεφάλαιο 1, και τα δύο χρησιμοποιούν TCP (πρωτόκολλο ελέγχου μετάδοσης) στο επίπεδο μεταφοράς. Η διαφορά από το Telnet είναι ότι το Telnet είναι ένα πρωτόκολλο δικτύωσης περισσότερο γνωστό για την πλατφόρμα UNIX που έχει σχεδιαστεί ειδικά για τοπικά δίκτυα. Το SSH είναι ένα πρόγραμμα για τη σύνδεση σε άλλον υπολογιστή μέσω δικτύου, την εκτέλεση εντολών σε ένα απομακρυσμένο μηχάνημα και τη μεταφορά αρχείων από το ένα μηχάνημα στο άλλο. Σε σύγκριση με το SSH, το Telnet είναι λιγότερο ασφαλές. Από την άλλη

το SSH είναι ένα πολύ ασφαλές πρωτόκολλο γιατί μοιράζεται και στέλνει τις πληροφορίες σε κρυπτογραφημένη μορφή. Το Telnet μεταφέρει τα δεδομένα σε απλό κείμενο. Από την άλλη πλευρά, το SSH χρησιμοποιεί ένα ασφαλές κανάλι για την αποστολή δεδομένων σε κρυπτογραφημένη μορφή. Το SSH είναι πιο ασφαλές, χρησιμοποιεί κρυπτογράφηση δημόσιου κλειδιού για έλεγχο ταυτότητας και τέλος ιδιωτικά δίκτυα συνιστώνται για Telnet ενώ για δημόσια δίκτυα το SSH. Στο GNS3 η εντολη Telnet εκτελείται με το rlogin και δίπλα το port το ποιο έχει ορίσει το πρόγραμμα σε κάθε συσκευή. Για παράδειγμα αν θέλουμε να κάνουμε telnet από ένα υπολογιστή στο ESW2 θα χρησιμοποιήσουμε την εντολη **rlogin 5048** και έτσι έχουμε πρόσβαση στην συσκευή.

4.12 Κωδικοί Συσκευών Για Ασφάλεια

Ένα τελευταίο κομμάτι της ασφάλειας αφορά το να έχουν οι συσκευές κωδικούς στις λειτουργίες τους . Στις συσκευές υπάρχουν 3 λειτουργίες οι οποίες πρέπει να ασφαλισθούν με τις παρακάτω εντολές και κωδικούς.

- Τη Λειτουργία User Exec
  line console 0
  password uth
  login
- Τη Λειτουργία Privileged Exec
  enable secret company
- Τις VTY Lines
  line vty 0 15
  password uth
  login

Τέλος επειδή όλοι αυτοί οι κωδικοί θα εμφανίζονται σαν κείμενο, θα πρέπει να τους κρυπτογραφήσουμε με την εντολή: **service password-encryption**.

ΚΕΦΑΛΑΙΟ 5 : Αυτοματοποίηση Συμπεριφοράς και Απόκρισης Δικτύου

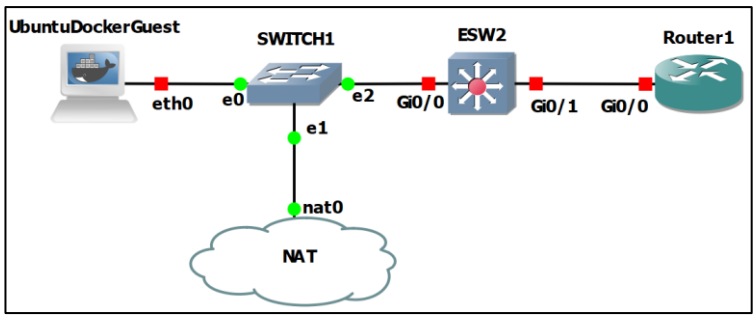
5.1 Εισαγωγή στην αυτοματοποίηση

Σε αυτό το κεφάλαιο κύριος στόχος είναι η αυτοματοποίηση του δικτύου. Σε μεγάλες τοπολογίες δικτύων όπου χρειάζεται να ρυθμίσουμε αρκετές συσκευές χρειαζόμαστε μια γρήγορη μέθοδο για να επιτευχθεί αυτό . Το δίκτυο της εταιρείας μεγάλωσε και χρειάστηκαν αρκετές αλλαγές και νέες ρυθμίσεις για να εξυπηρετήσουν τις ανάγκες της εταιρείας. Ένα δίκτυο όμως σαν αυτό μπορεί να χρειαστεί ξανά επέκταση οπότε η διαδικασία αυτή θα πρέπει να επαναληφθεί και ίσως σε μεγαλύτερο βαθμό . Το πρόβλημα που προκύπτει εδώ αφορά το χρόνο που χρειάζεται το δίκτυο να ρυθμιστεί με βάση τις νέες αλλαγές. Σε κάθε εταιρεία χρειάζεται οι αλλαγές που προκύπτουν να γίνουν γρήγορα και όσο το δυνατόν πιο εύκολα. Έτσι λοιπόν πρέπει να βρεθεί μια λύση με την οποία οι νέες αλλαγές θα προκύπτουν μαζικά για τις συσκευές.

5.2 Γλώσσα Προγραμματισμού Python

Μια γλώσσα προγραμματισμού που βοηθάει στην αυτοματοποίηση των δικτύων είναι η python. Η γλώσσα προγραμματισμού python έχει αρκετές δυνατότητες και όπως θα δείξουμε παρακάτω εκτός από ένα script σε κάποιον editor μπορούμε να ενσωματώσουμε και την python μέσα στο GNS3 δίκτυο μας και να τρέχει εικονικά κάποιους κώδικες ως προς τις εικονικές συσκευές του δικτύου. Η Python παρέχει δύο επίπεδα πρόσβασης σε υπηρεσίες δικτύου. Σε χαμηλό επίπεδο, μπορούμε να έχουμε πρόσβαση στη βασική υποστήριξη υποδοχής στο λειτουργικό σύστημα, το οποίο μας επιτρέπει να υλοποιούμε πελάτες και διακομιστές τόσο για πρωτόκολλα προσανατολισμένα στη σύνδεση όσο και για πρωτόκολλα χωρίς σύνδεση. Η Python διαθέτει επίσης βιβλιοθήκες που παρέχουν πρόσβαση υψηλότερου επιπέδου σε συγκεκριμένα πρωτόκολλα δικτύου σε επίπεδο εφαρμογής, όπως για παράδειγμα τα FTP και HTTP.

Ένα πλεονέκτημα του GNS3 είναι ότι έχουμε επίσης τη δυνατότητα να τρέξουμε κάποιο script της γλώσσας από συσκευή μέσα στο GNS3. Για τα script που παρουσιάζονται παρακάτω χρησιμοποιείται το gns3 appliance ubuntu docker container και την διάταξη των συσκευών όπως φαίνεται στην τοπολογία. Επίσης μπορούμε να χρησιμοποιήσουμε το appliance network automation ώστε να μην χρειάζεται κάθε φορά να κάνουμε Install την Python στην συσκευή.



Εικόνα 5.1 Τοπολογία Εγκατάστασης Ubuntu Docker Για Χρήση Της Python

5.3 Υποδοχές Socket

Οι υποδοχές ή αλλιώς sockets είναι τα τελικά σημεία ενός καναλιού αμφίδρομης επικοινωνίας. Οι υποδοχές μπορούν να επικοινωνούν μέσα σε μια διεργασία, μεταξύ διεργασιών στο ίδιο μηχάνημα ή μεταξύ διεργασιών σε διαφορετικά μηχανήματα. Οι υποδοχές μπορούν να υλοποιηθούν σε διάφορους τύπους καναλιών όπως για παράδειγμα υποδοχές τομέα Unix, TCP και UDP. Η βιβλιοθήκη socket παρέχει συγκεκριμένες κλάσεις για το χειρισμό των κοινών μεταφορών καθώς και μια γενική διεπαφή για το χειρισμό των υπολοίπων. Για να δημιουργήσουμε ένα socket θα χρησιμοποιήσουμε τη συνάρτηση *socket.socket()* η οποία έχει την παρακάτω σύνταξη:

s= socket. socket (socket_family, socket_type, protocol=0)

Η συνάρτηση αυτή έχει μερικές παραμέτρους τις οποίες αναλύουμε παρακάτω:

socket_family – είναι είτε AF_UNIX είτε AF_INET

socket_type – είναι είτε SOCK_STREAM είτε SOCK_DGRAM.

protocol – Αυτό το κομμάτι συνήθως δεν συμπληρώνεται και γίνεται 0 από προεπιλογή

5.4 Αυτοματοποίηση και ασφάλεια

Ένα σημαντικό κομμάτι των δικτύων όπως δείξαμε και στο κεφάλαιο 4 είναι η ασφάλεια. Όταν γίνει κάποια επίθεση θέλουμε να επιλυθεί όσο το δυνατόν πιο σύντομα αλλά κυρίως να δράσουμε προληπτικά ώστε να την αποφύγουμε εξ αρχής. Παρακάτω θα παρουσιαστεί ένα port scanner το οποίο έχει στόχο την πρόληψη επιθέσεων καθώς θα μας επιτρέψει να βρούμε ανοιχτές πύλες σε συσκευές, και κάποιοι κώδικες οι οποίοι εκτός από την αυτοματοποίηση θα στοχεύουν στην ασφάλεια όπως για παράδειγμα να ρυθμίζουν ACL σε κάποιο δρομολογητή.

5.5 Ανίχνευση ανοιχτών πυλών με ένα Port Scanner

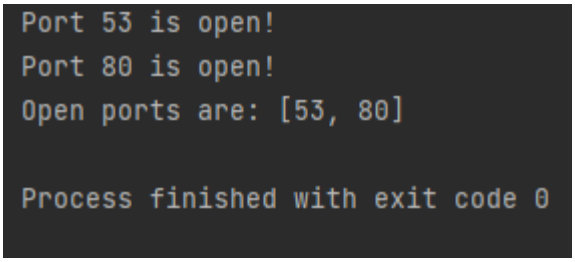
Το πρώτο πρόγραμμα που θα παρουσιαστεί είναι ένα Port Scanner. Αυτό το πρόγραμμα με επέκταση .py αφορά σε μεγάλο βαθμό το κομμάτι της ασφάλειας του δικτύου μας. Ο κώδικας φτιάχτηκε στο PyCharm και αφορά κώδικα γραμμένο σε γλώσσα προγραμματισμού python. Μια συσκευή όπως ένας web server στο δίκτυο μας είναι λογικό να έχει κάποια ανοιχτά ports λόγω των υπηρεσιών που προσφέρει. Πολλές συσκευές όμως έχουν ανοιχτά port τα οποία δεν χρησιμοποιούν και αυτό είναι πολύ πιθανό να δημιουργήσει κάποιο πρόβλημα στην ασφάλεια του δικτύου. Το πρώτο script που παρουσιάζεται παρακάτω είναι ένα port scanner το οποίο τρέχει για τις διευθύνσεις που θα του δώσει ο χρήστης ώστε να βρεθούν ανοιχτές πύλες στις συσκευές του δικτύου. Γνωρίζοντας τις ανοικτές πύλες των συσκευών μας επιτρέπει να δράσουμε προληπτικά. Μια ανοιχτή θύρα και συγκεκριμένα όταν δεν χρειάζεται μπορεί να δημιουργήσει ένα κενό ασφάλειας. Το πρόγραμμα μας χρησιμοποιεί sockets για να συνδεθεί σε ένα συγκεκριμένο στόχο και multithreading ώστε η διαδικασία να γίνει πιο γρήγορα.

Αρχικά δηλώνονται οι βιβλιοθήκες και τα imports από τις βιβλιοθήκες. Μετά βάζουμε σαν στόχο ποια συσκευή θέλουμε να ελέγξουμε. Στη συνέχεια δηλώνεται η συνάρτηση portscanner η οποία αρχικά ανοίγει το Internet socket και μετα συνδέεται στο στόχο στο port το οποίο έχουμε περάσει σαν παράμετρο στη συνάρτηση. Η συνάρτηση επιστρέφει την τιμή true αν το port scan έγινε με επιτυχία. Με την εκτέλεση του κώδικα παρατηρούμε ότι χρειάζεται αρκετή ώρα για να σκανάρει όλες τι θύρες στο εύρος που έχουμε δώσει οπότε θα βάλουμε multithreading με ουρές. Αυτό έχει σαν αποτέλεσμα να ελέγχονται πολλαπλές θύρες ταυτόχρονα για εξοικονόμηση χρόνου εκτέλεσης. Βάζουμε μια συνάρτηση που θα γεμίσει την ουρά, την fill_queue και στη συνέχεια η συνάρτηση worker είναι κατά βάση το τι θα χρησιμοποιήσουν τα Threads για την λειτουργία τους. Τέλος, γεμίζουμε την ουρά και στο συγκεκριμένο script δηλώνουμε 10 threads να τρέχουν ταυτόχρονα και με την join θα περιμένουμε όλα τα Threads να τελειώσουν.

```
#Port Scanner#
import socket
import threading
from queue import Queue
target = "192.168.1.1"
queue = Queue()
```

```
open ports = []
def portscannner(port):
   try:
      sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
      sock.connect((target, port))
      return True
   except:
      return False
def fill_queue(port_list):
   for port in port_list:
      queue.put(port)
def worker():
   while not queue.empty():
      port = queue.get()
      if portscan(port):
         print("Port {} is open!".format(port))
         open_ports.append(port)
port_list = range(1,1024)
fill_queue(port_list)
thread_list = []
for t in range(10):
      thread = threading.Thread(target=worker)
      thread_list.append(thread)
for thread in thread_list:
   thread.start()
for thread in thread_list:
   thread.join()
print("Open ports are:", open_ports)
```

Ο κώδικας έτρεξε στο οικιακό router 192.168.1.1 και στην παρακάτω εικονα βλέπουμε ότι έχει ανοιχτά το DNS port 53 και το HTTP port 80 . Με τον ίδιο τρόπο μπορούμε να χρησιμοποιήσουμε τον κώδικα για τις συσκευές του δικτύου μας.



Εικόνα 5.2 Αποτέλεσμα Port Scanner

5.6 Αυτοματοποίηση Ρυθμίσεων Σε Δρομολογητή

Μια συσκευή που συναντάμε αρκετές φορές στο δίκτυο της εταιρείας μας είναι ο δρομολογητής. Αυτό σημαίνει ότι έχουν γίνει αρκετές ρυθμίσεις χειροκίνητα και αν η εταιρεία επεκταθεί θα χρειαστεί να γίνουν ρυθμίσεις εκ νέου, στις νέες συσκευές γεγονός που θα κοστίσει κυρίως σε χρόνο. Έτσι λοιπόν χρειαζόμαστε μια λύση η οποία θα συμβάλει στο να γίνει πιο γρήγορα αυτή η διαδικασία και με λιγότερο κόστος και κόπο. Ο κώδικας που παρουσιάζεται παρακάτω αφορά την τοπολογία στην εικόνα: και στόχο έχει την αυτοματοποίηση των βασικών ρυθμίσεων των δρομολογητών.

Script 1

```
import getpass
import sys
import telnetlib

HOST = "192.168.122.219"
user = raw_input ("Enter your Telnet Username: ")
password = getpass.getpass()

tn = telnetlib. Telnet (HOST)

tn. read_until ("Username: ")
tn. write (user + "\n")
if password:
   tn.read_until("Password: ")
   tn.write(password + "\n")

tn.write("enable\n")
tn.write("uth\n")
tn.write("configure terminal\n")
tn.write("enable password uth\n")
tn.write("username admin password uth\n")
tn.write("line vty 0 4\n")
tn.write("login local\n")
tn.write("transport input all\n")
tn.write("exit\n")
tn.write("line console 0\n")
tn.write("password uth\n")
tn.write("login\n")
```

```
tn.write("enable secret company\n")
tn.write("int loop 0\n")
tn.write("ip address 1.1.1.1 255.255.255.255\n")
tn.write("router ospf 1\n")
tn.write("network 0.0.0.0 255.255.255.255 area 0\n")
tn.write("end\n")

tn.write("exit\n")
tn.write("wr\n")
print tn.read_all()
```

5.7 Αυτοματοποίηση Ρυθμίσεων σε Μεταγωγέα

Μια ακόμα συσκευή που υπάρχει σε μεγάλο βαθμό στο δίκτυο είναι οι μεταγωγείς. Ο διαχειριστής του δικτύου μας χρειάζεται ένα πρόγραμμα αυτοματοποίησης ώστε σε μελλοντική επέκταση της εταιρείας να μπορεί να ρυθμίσει τους νέους μεταγωγείς με μεγαλύτερη ευκολία.

Όπως είπαμε και σε προηγούμενο κεφάλαιο η εταιρεία χρησιμοποιεί συνολικά 3 vlan. Ένα είναι αυτό των προγραμματιστών που ήταν αρχικά στην εταιρεία το vlan 10, ένα των νέων προγραμματιστών όταν έγινε η επέκταση το vlan 20 και ένα που αφορά το DMZ το vlan 30 . Ο κώδικας αφορά μια μελλοντική επέκταση της εταιρείας όπου για νέα switch θα έχουμε να ρυθμίσουμε εκ νέου τα τρία vlan.

Port security σε access port να βαλω

Script 2

```
import getpass
import sys
import telnetlib

user = raw_input("Enter your Telnet Username: ")
password = getpass.getpass()

for n in range (10,20):
print "Telnet to host" + str(n)
HOST = "192.168.31." + str(n)
tn = telnetlib.Telnet(HOST)

tn.read_until("Username: ")
tn.write(user + "\n")
if password:
   tn.read_until("Password: ")
   tn.write(password + "\n")

tn.write("enable\n")
```

```
tn.write("uth\n")
tn.write("configure terminal\n")

for n in range (10,30,10):
   tn.write("vlan " + str(n) + "\n")
   if n==10:
   tn.write("name Developers Vlan" + str(n) + "\n")
   if n==20:
   tn.write("name New Developers Vlan" + str(n) + "\n")
   if n==30:
   tn.write("name Servers Vlan" + str(n) + "\n")

tn.write("exit\n")
tn.write(" interface GigabitEthernet 0/0 \n ")
tn.write(" switchport mode access \n")

tn.write(" switchport access vlan 10\n")
tn.write(" switchport port-security \n")

tn.write(" switchport port-security maximum 1 \n")

tn.write("switchport port-security violation restrict \n")

tn.write("exit\n")
tn.write("end\n")
tn.write("exit\n")
tn.write("wr\n")

print tn.read_all()
```

5.8 Βιβλιοθήκες Netmiko και Paramiko

Δυο πολύ γνωστές βιβλιοθήκες της γλώσσας προγραμματισμού python που αφορούν το κομμάτι των δικτύων είναι η βιβλιοθήκη Netmiko και η βιβλιοθήκη Paramiko. Η Paramiko είναι μια υλοποίηση του πρωτοκόλλου SSH που είδαμε στο κεφάλαιο 4 η οποία παρέχει τη λειτουργικότητα τόσο του πελάτη όσο και του διακομιστή. Η Netmiko είναι πολύ δημοφιλής και παρόμοια με το Paramiko με μερικές σημαντικές διαφορές. Σε δίκτυα πραγματικού κόσμου, συναντάμε διάφορα μοντέλα συσκευών. Επομένως, χρειαζόμαστε ένα αξιόπιστο εργαλείο που μπορεί να μας βοηθήσει να αυτοματοποιήσουμε τη διαδικασία. Σε ορισμένες περιπτώσεις, δεν μπορούμε να χρησιμοποιήσουμε την Paramiko λόγω περιορισμών υποστήριξης συσκευών, με αποτέλεσμα καθυστερήσεις και σφάλματα και επίσης είναι πολύ πιο αργή από την Netmiko. Η Paramiko είναι περισσότερο μια γενική μονάδα SSH που μπορούμε να χρησιμοποιήσουμε για να αυτοματοποιήσουμε συγκεκριμένες εργασίες SSH. Αντίθετα, η Netmiko είναι ευρύτερη και καλά βελτιστοποιημένη για τη διαχείριση συσκευών δικτύου όπως μεταγωγείς και δρομολογητές. Η Netmiko υπερισχύει της Paramiko διότι:

1)Γίνεται αυτόματη σύνδεση μέσω SSH σε συσκευές δικτύου.

2)Παρέχει απλούστερη εκτέλεση εντολών εκπομπών και εξόδου δεδομένων.

3)Παρέχει απλούστερη λειτουργικότητα για εντολές διαμόρφωσης, συμπεριλαμβανομένων των ενεργειών δέσμευσης.

4)Υποστήριξη πολλαπλών συσκευών σε προμηθευτές και πλατφόρμες συσκευών δικτύου.

Παρακάτω, παρουσιάζουμε μια απλή λειτουργία της netmiko η οποία μας βοηθάει να συνδεθούμε με SSH στα Router της εταιρείας.

```
# SSH to Multiple Devices from devices file
from netmiko import ConnectHandler

with open('devices.txt') as routers:
   for IP in routers:
      Router = {
         'device_type': 'cisco_ios',
         'ip': IP,
         'username': 'admin',
         'password': 'uth'
      }
      # Next establish the SSH connection
      net_connect = ConnectHandler(**Router)

      print ('Connecting to ' + IP)
      print('-'*79)
      # Then send the command and print the output
      output = net_connect.send_command('sh ip int brief')
      print(output)
      print()
      print('-'*79)

# Finally close the connection
net_connect.disconnect()
```

Οι διευθύνσεις των συσκευών είναι αποθηκευμένες μέσα στο αρχείο routers.txt στην παρακάτω εικονα.

```
192.168.1.1
192.168.2.1
192.168.3.1
192.168.4.1
192.168.5.1
192.168.6.1
```

Εικόνα 5.3 Κείμενο Διευθύνσεων Για Μαζική Ρύθμιση

5.9 Script Για Ρύθμιση ACL Σε Δρομολογητή

Στο κώδικα που παρουσιάσαμε για το δρομολογητή θα προσθέσουμε μερικές εντολές οι οποίες έχουν να κάνουν με τη ρύθμιση Access List (ACL) στο δρομολογητή. Σε πιθανή επέκταση της εταιρείας θα χρειαστεί να ρυθμιστούν αρκετά νέα μηχανήματα. Οπότε στο script θα προσθέσουμε τις εξής εντολές στο νέο δρομολογητή του δικτύου:

```
tn.write("interface GigabitEthernet 0/0 \n")
tn.write("ip access-list extended 10 \n")
tn.write("ip access-group 10 in\n")
tn.write("access-list 10 permit 192.168.1.1 0.0.255.255\n")
tn.write("access-list 10 deny tcp any 10.10.10.0 0.0.0.255 eq 21 \n")
tn.write("access-list 10 deny tcp any 195.10.10.0 0.0.0.255 eq 21 \n")
tn.write("access-list 10 deny tcp any 194.10.10.0 0.0.0.255 eq 21 \n")
tn.write("access-list 10 deny tcp any 10.10.10.0 0.0.0.255 eq 23 \n")
tn.write("access-list 10 deny tcp any 195.10.10.0 0.0.0.255 eq 23 \n")
tn.write("access-list 10 deny tcp any 194.10.10.0 0.0.0.255 eq 23 \n")
tn.write("access-list 10 permit ip any any\n")
```

Όπου στο interface GigabitEthernet 0/0 τοποθετείται η ACL 10 η οποία επιτρέπει τις συσκευές που ανήκουν στο εύρος 192.168.1.1 – 192.168.255.255 και αποκλείει τις υπόλοιπες διευθύνσεις από το να μπορούν να έχουν FTP και Telnet πρόσβαση τη συσκευή. Τέλος, επιτρέπει τα υπόλοιπα πακέτα και πρωτόκολλα να έχουν πρόσβαση στη συσκευή.

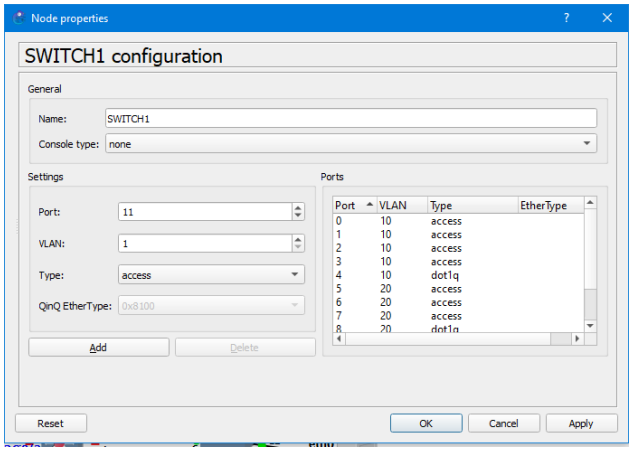
ΚΕΦΑΛΑΙΟ 6 Συμπεράσματα

6.1 Συμπεράσματα

Τα σύγχρονα δίκτυα υπολογιστών είναι ένας πολύ ενδιαφέρον τομέας της πληροφορικής. Καθώς ο πραγματικός εξοπλισμός είναι αρκετά ακριβώς, τα εικονικά περιβάλλοντα δίνουν την ευκαιρία σε κάποιον να πειραματιστεί και να δοκιμάσει ρυθμίσεις σε συσκευές όπως με πραγματικά μηχανήματα. Το GNS3 που επιλέξαμε για την παρουσίαση είναι μια πολύ καλή λύση διότι εκτός από το ότι δεν έχει περιορισμούς ως προς τις συσκευές, μπορεί να συνδυάσει λογισμικό και να γίνει επέκταση με πραγματικά μηχανήματα μέσα από αυτό. Παρουσιάστηκαν λοιπόν δυο δίκτυα τα οποία έχουν κοινό σκοπό αλλά διαφορετικό τρόπο εκτέλεσης και διαφορετικές τεχνολογίες. Στην συνέχεια αναφερθήκαμε σε ένα κρίσιμο τομέα των δικτύων που αφορά τις επιθέσεις και την ασφάλεια. Παρουσιάστηκαν επιθέσεις που πραγματοποιούνται σε τέτοιες εταιρείες και δόθηκαν τρόποι αντιμετώπισης αλλά και πρόληψης. Τέλος, στην εργασία εντάχθηκε και το κομμάτι της αυτοματοποίησης το οποίο χωρίστηκε σε τομείς ανάλογα με τις συσκευές που ρυθμίζει και την πρόληψη επιθέσεων.

6.2 Προβλήματα που δημιουργήθηκαν αλλά επιλυθήκαν

- Το GNS3 κατά την χρονική διάρκεια που στηνόταν το δίκτυο αναβάθμισε την έκδοση του και σταμάτησε να υποστηρίζει console σε L2 Switch. Επειδή το δίκτυο χρησιμοποιεί τέτοιες συσκευές ήταν δύσκολο να ρυθμίσουμε μερικές λειτουργίες όπως το InterVlan Routing διότι υπήρχε μια απλή διεπαφή όπως φαίνεται στην εικονα όπου ένα Link δεν μπορούσε να είναι trunk και ή θα ήταν στο VLAN 10 ή στο VLAN 20.



Εικόνα 6.1 Configuration Panel Συσκευής Switch1 Του Δικτύου

Για να λυθεί αυτό εφαρμόσαμε inter vlan στο ESW2 αλλά βάλαμε και δεύτερη θύρα στο μεταγωγό ένα για κάθε VLAN και έτσι οι τερματικές συσκευές διαφορετικών VLAN επικοινωνούσαν μεταξύ τους αλλά είχαν και πρόσβαση στο διαδίκτυο.

- Θέλοντας να βαλω στα appendix τις εντολές των συσκευών , υπήρξε πρόβλημα διότι δεν έκαναν export τα αρχεία των συσκευών. Αυτό επιλύθηκε με τη διαδικασία του να κάνω crop τις εντολές των συσκευών και να χρησιμοποιήσω ένα πρόγραμμα μετατροπής εικόνας σε κείμενο.
- Όσο μεγάλωνε το δίκτυο της εταιρείας κατανάλωνε όλο και περισσότερους πόρους από το μηχάνημα και έτσι έγινε αρκετά βαρύ. Για να αντιμετωπιστεί αυτό μείωσα την RAM από ορισμένες συσκευές του δικτύου όπως για παράδειγμα τις δευτερεύοντες συσκευές που είναι μόνο για υποστήριξη ζημίων.

6.3 Μελλοντικές επεκτάσεις

- Ένα κομμάτι που δεν έβαλα στην πτυχιακή είναι το κομμάτι της κρυπτογραφίας όπου θα γινόταν αναφορά στο κεφάλαιο 4 σχετικά με την ασφάλεια των δικτύων και θα έδειχνα κάποιους αλγορίθμους κρυπτογράφησης.
- Ένα επιπλέον κεφάλαιο θα αφορούσε το να φτιάξω κάτι δικό μου είτε αφορά αλγόριθμο είτε πρωτόκολλο το οποίο θα έχει πυλώνα κάποιο που ήδη υπάρχει και να έβρισκα κάποια στοιχεία τα οποία θα το μετέτρεπαν σε πιο αποδοτικό από αυτά που ήδη υπάρχουν.
- Στο κομμάτι της αυτοματοποίησης θα ήθελα να επεκταθώ και εκτός του τομέα της python για παράδειγμα με ansible.

- Στο κομμάτι του δικτύου αυτό που θα γίνει στη συνέχεια είναι να μπουν παραπάνω πρωτόκολλα όπως το HSRP,STP, για να γίνει πιο αποδοτικό το δίκτυο. Θα τοποθετηθεί και ένας DHCP server ώστε οι συσκευές να παίρνουν αυτόματα διευθύνσεις και όχι χειροκίνητα.
- Ένα port στο Router 2 εξυπηρετεί μελλοντική επέκταση της τοπολογίας με άλλη τοπολογία με μια εταιρεία παροχής VPN υπηρεσιών ώστε να ταιριάξει με το κεφάλαιο 4 όπου έγινε αναφορά του πρωτοκόλλου.
- Ένα πρωτόκολλο που τελικά αφαιρέθηκε λόγω του ότι το OSPF εξυπηρετούσε το δίκτυο μας είναι το BGP οπότε σίγουρα θα έχει και ένα επιπλέον δίκτυο άλλης εταιρείας με την οποία θα συνδέεται η εταιρεία μας με BGP. Η ακόμα και να είναι μέρος της εταιρείας σε κάποια άλλη γεωγραφική θέση.
- Μια μελλοντική τροποποίηση θα αφορά και το κομμάτι των OSPF areas διότι στην τοπολογία μας χρησιμοποιήθηκε μόνο μια περιοχή οπότε θα δείξω και τα πλεονεκτήματα επιπλέον περιοχών.
- Μια μελλοντική επέκταση η οποία αναφέρθηκε και πιο πριν είναι η επέκταση με κανονικά μηχανήματα.
- Στο κεφάλαιο 4 θα παρουσιαστεί και μια επίθεση που αφορά τα VLAN την VLAN Hopping Attack.

APPENDIX 2: Εντολές Συσκευών Τελικού Δικτύου

Στο Appendix 2 έχουμε βάλει τις εντολές που αφορούν το νέο βελτιωμένο δίκτυο της εταιρείας μετα τις τροποποιήσεις που έχουμε κάνει στα κεφάλαια 3 και 4. Αλλαγές που αφορούν προσθήκες τεχνολογιών αλλά και αλλαγές που αφορούν το κομμάτι της ασφάλειας.

Router 1

```
hostname R1
service password encryption
ip name-server 8.8.8.8
interface Loopback0
ip address 1.1.1.1 255.255.255.255
interface GigabitEthernet0/0
ip address 194.10.10.2 255.255.255.0
ip nat outside
interface GigabitEthernet0/1
ip address 192.168.2.1 255.255.255.0
ip nat inside
interface Gigabit Ethernet0/2
ip address 192.168.1.1 255.255.255.0
ip nat inside
interface GigabitEthernet0/3
ip address 10.10.10.1 255.255.255.0
ip nat outside
router ospf 10
network 10.10.10.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 194.10.10.0 0.0.0.255 area 0
ip nat pool 1 194.10.10.5 194.10.10.254
                netmask 255.255.255.0
ip nat inside source list 1 pool 1
ip route 0.0.0.0 0.0.0.0 194.10.10.1
access-list 1 permit 192.168.0.0 0.0.255.255
```

Router 2

```
hostname R2
service password encryption
ip name-server 8.8.8.8
interface Loopback0
ip address 2.2.2.2 255.255.255.255
interface GigabitEthernet0/0
ip address 195.10.10.2 255.255.255.0
interface GigabitEthernet0/1
ip address 192.168.3.1 255.255.255.0
router ospf 10
network 192.168.3.0 0.0.0.255 area 0
network 195.10.10.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 195.10.10.1
```

Router 3

```
hostname R3
service password encryption
ip name-server 8.8.8.8
interface Loopback0
ip address 3.3.3.3 255.255.255.255
interface GigabitEthernet0/0
ip address 192.168.5.2 255.255.255.0
interface GigabitEthernet0/1
ip address 192.168.12.2 255.255.255.0
interface GigabitEthernet0/2
no ip address
shutdown
interface GigabitEthernet0/3
ip address 192.168.6.2 255.255.255.0
router ospf 10
network 192.168.2.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255 area 0
network 192.168.12.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 192.168.12.1
```

Router4

```
hostname R4
service password encryption
ip name-server 8.8.8.8
interface Loopback0
ip address 4.4.4.4 255.255.255.255
interface GigabitEthernet0/0
ip address 192.168.5.1 255.255.255.0
interface GigabitEthernet0/1
ip address 192.168.7.1 255.255.255.0
interface GigabitEthernet0/2
ip address 192.168.10.2 255.255.255.0
interface GigabitEthernet0/3
ip address 192.168.8.1 255.255.255.0
router ospf 10
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.7.0 0.0.0.255 area 0
network 192.168.8.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.11.0 0.0.0.255 area 0
network 192.168.12.0 0.0.0.255 area 0
network 192.168.31.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip route 0.0.0.0 0.0.0.0 192.168.5.2 120
ip route 0.0.0.0 0.0.0.0 192.168.7.2 130
```

Router5

```
hostname R5
service password encryption
ip name-server 8.8.8.8
interface Loopback0
ip address 5.5.5.5 255.255.255.255
interface GigabitEthernet0/0
ip address 192.168.7.2 255.255.255.0
interface GigabitEthernet0/1
ip address 192.168.11.2 255.255.255.0
interface GigabitEthernet0/2
ip address 192.168.9.1 255.255.255.0
interface GigabitEthernet0/3
ip address 192.168.6.1 255.255.255.0
router ospf 10
network 192.168.3.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255 area 0
network 192.168.7.0 0.0.0.255 area 0
network 192.168.9.0 0.0.0.255 area 0
network 192.168.11.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 192.168.11.1
ip route 0.0.0.0 0.0.0.0 192.168.6.2 120
```

ESW9

```
hostname ESW9
enable secret 5 $1$KGN3$i304f/7yKXI
interface GigabitEthernet0/0
description Link to ASAV3
no switchport
ip address 10.10.11.2 255.255.255.0
interface GigabitEthernet0/2
switchport access vlan 30
switchport mode access
negotiation auto
interface GigabitEthernet0/3
description Link to DMZ-Server
switchport access vlan 30
interface Vlan30
ip address 10.10.12.20 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.10.11.1
line con 0
password 7 09595401
login
line aux 0
line vty 0 4
password 7 08345846
login
line vty 5 15
password 7 044E1FOE
login
```

ESW2

```
service password-encryption
hostname ESW2
interface Port-channel2
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dotiq
switchport mode trunk
interface Port-channel5
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dotiq
switchport mode trunk
interface GigabitEthernet0/0
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dotiq
switchport mode trunk
interface GigabitEthernet0/1
switchport access vlan 10
switchport mode access
switchport port-security violation restrict
switchport port-security
interface GigabitEthernet0/2
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dotiq
switchport mode trunk
channel-group 5 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet0/3
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dotiq
switchport mode trunk
channel-group 5 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet2/0
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dotiq
switchport mode trunk
channel-group 2 mode active
spanning-tree link-type point-to-point
interface Gigabit Ethernet2/1
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dotiq
switchport mode trunk
channel-group 2 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet3/0
no switchport
ip address 192.168.30.1 255.255.255.0
interface GigabitEthernet3/1
switchport access vlan 20
switchport mode access
switchport port-security violation restrict
switchport port-security
interface GigabitEthernet3/2
no switchport
ip address 192.168.35.1 255.255.255.0
interface GigabitEthernet3/3
no switchport
ip address 192.168.31.2 255.255.255.0
interface Vlan10
ip address 192.168.36.1 255.255.255.0
interface Vlan20
ip address 192.168.37.1 255.255.255.0
router ospf 10
network 192.168.8.0 0.0.0.255 area 0
network 192.168.31.0 0.0.0.255 area 0
network 192.168.35.0 0.0.0.255 area 0
network 192.168.36.0 0.0.0.255 area 0
network 192.168.37.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 192.168.31.1
```

ESW3

```
service password encryption
hostname ESW3
interface Port-channel2
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
interface Port-channel3
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
interface GigabitEthernet0/0
no switchport
ip address 192.168.8.2 255.255.255.0
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
interface GigabitEthernet2/0
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 2 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet2/1
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 2 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet2/2
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 3 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet2/3
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 3 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet3/0
switchport access vlan 10
switchport mode access
interface GigabitEthernet3/3
no switchport
ip address 192.168.31.1 255.255.255.0
interface Vlan1
ip address 192.168.20.20 255.255.255.0
router ospf 10
network 192.168.8.0 0.0.0.255 area 0
network 192.168.31.0 0.0.0.255 area 0
network 192.168.36.0 0.0.0.255 area 0
network 192.168.37.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 192.168.8.1
```

ESW5

```
service password encryption
hostname ESW5
interface Port-channel3
switchport trunk allowed vlan 10, 20
switchport trunk encapsulation dot1q
switchport mode trunk
interface Port-channel4
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
interface GigabitEthernet0/0
no switchport
ip address 192.168.9.2 255.255.255.0
interface GigabitEthernet0/1
switchport trunk allowed vlan 10
switchport trunk encapsulation dot1q
switchport mode trunk
interface GigabitEthernet1/0
switchport trunk allowed vlan 10
switchport trunk encapsulation dot1q
switchport mode trunk
shutdown
spanning-tree link-type point-to-point
interface Gigabit Ethernet2/0
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 4 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet2/1
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 4 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet2/2
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 3 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet2/3
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 3 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet3/1
no switchport
ip address 192.168.33.1 255.255.255.0
interface GigabitEthernet3/2
interface GigabitEthernet3/3
no switchport
ip address 192.168.32.1 255.255.255.0
router ospf 10
network 192.168.9.0 0.0.0.255 area 0
network 192.168.32.0 0.0.0.255 area 0
network 192.168.33.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 192.168.9.1
```

ESW6

```
service password encryption
hostname ESW6
interface Port-channel4
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
interface Port-channel5
switchport trunk allowed vlan 10
switchport trunk encapsulation dot1q
switchport mode trunk
interface GigabitEthernet0/0
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
switchport mode trunk
interface GigabitEthernet0/2
switchport trunk allowed vlan 10
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 5 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet0/3
switchport trunk allowed vlan 10
switchport trunk encapsulation dotiq
switchport mode trunk
channel-group 5 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet1/
interface GigabitEthernet1/1
switchport access vlan 10
switchport mode access
interface GigabitEthernet2/0
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dotiq
switchport mode trunk
channel-group 4 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet2/1
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dotiq
switchport mode trunk
channel-group 4 mode active
spanning-tree link-type point-to-point
interface GigabitEthernet3/1
no switchport
ip address 192.168.33.2 255.255.255.0
interface GigabitEthernet3/3
no switchport
ip address 192.168.34.1 255.255.255.0
negotiation auto
router ospf 10
network 192.168.33.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 0
ip route 0.0.0.0 0.0.0.0 192.168.33.1
```

ASAV1

```
hostname ASAV1
enable password $sha512$5000$ezona
interface Gigabit Ethernet0/0
nameif outside
security-level 0
ip address 192.168.1.2 255.255.255.0
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.10.1 255.255.255.0
ftp mode passive
object network obj_any
subnet 0.0.0.0 0.0.0.0
object network obj_any
nat (inside, outside) dynamic interface
router ospf 10
network 192.168.1.0 255.255.255.0 area 0
network 192.168.2.0 255.255.255.0 area 0
network 192.168.10.0 255.255.255.0 area 0
network 194.10.10.0 255.255.255.0 area 0
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```

ASAV2

```
hostname ASAV2
enable password $sha512$5000$ezona
interface Gigabit Ethernet0/0
nameif outside
security-level 0
ip address 192.168.3.2 255.255.255.0
interface Gigabit Ethernet0/1
nameif inside
security-level 100
ip address 192.168.11.1 255.255.255.0
ftp mode passive
object network obj_any
subnet 0.0.0.0 0.0.0.0
network obj_any nat (inside, outside) dynamic interface
router ospf 10 network 192.168.3.0 255.255.255.0 area 0
network 192.168.7.0 255.255.255.0 area 0
network 192.168.11.0 255.255.255.0 area 0
network 195.10.10.0 255.255.255.0 area 0
route outside 0.0.0.0 0.0.0.0 192.168.3.1 1
```

ASAV3

```
hostname ASAV3
enable password $sha512$5000$22jM7
interface Gigabit Ethernet0/0
nameif outside
security-level 0
ip address 10.10.10.2 255.255.255.0
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.11.1 255.255.255.0
ftp mode passive
object network obj any
subnet 0.0.0.0 0.0.0.0
nat (inside, outside) dynamic interface
route outside 0.0.0.0 0.0.0.0 10.10.10.1 1
router ospf 10
network 10.10.10.0 255.255.255.0 area 0
network 10.10.11.0 255.255.255.0 area 0
```

ASAV4

```
hostname ASAV4
enable password $sha512$5000$FJCI bkdf2
interface GigabitEthernet0/0
name if inside
security-level 100
ip address 192.168.12.1 255.255.255.0
interface Gigabit Ethernet0/1
name if outside
security-level 0
ip address 192.168.2.2 255.255.255.0
ftp mode passive
object network obj_any
subnet 0.0.0.0 0.0.0.0
object network obj_any
nat (inside, outside) dynamic interface
router ospf 10
network 192.168.2.0 255.255.255.0 area 0
network 192.168.5.0 255.255.255.0 area 0
network 192.168.12.0 255.255.255.0 area 0
route outside 0.0.0.0 0.0.0.0 192.168.2.1 1
```

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Βιβλίο:Tanenbaum,Wetherall: Δίκτυα Υπολογιστών Πέμπτη Αμερικάνικη Έκδοση
2. Βιβλίο: Ιωάννης Μαυρίδης “Ασφάλεια Πληροφοριών στο Διαδίκτυο”
3. Βιβλίο: “IP Routing: OSPF Configuration Guide”, Cisco Systems Inc.
4. Βιβλίο: “ Δικτύωση Υπολογιστών Προσέγγιση από πάνω προς τα κάτω, Έβδομη Έκδοση”,Kurose, Ross
5. Βιβλίο: “Ξεκινώντας με την Python Δεύτερη Βελτιωμένη Έκδοση ”,Tony Gaddis
6. Βιβλίο: “Κρυπτογραφία και Ασφάλεια Δικτύων αρχές και εφαρμογές, πρώτη ελληνική έκδοση ”William Stallings
7. Αναστασίου Θεοδώρα Πτυχιακή Εργασία: "Πρωτόκολλα Τοπικών Δικτύων" https://apothetirio.lib.uoi.gr/xmlui/bitstream/handle/123456789/249/tlp_000199.pdf?sequence=1,
8. Μπαμπέκος Παναγιώτης-Χρήστος, Βουλγαράκη Φωτεινή: «Ανάπτυξη και διαχείριση ενός αναχώματος ασφαλείας επιπέδου εφαρμογής (application level firewall) το οποίο θα δίνει τη δυνατότητα δημιουργίας αποστρατικοποιημένων ζωνών (demilitarized zones – DMZ)»
9. Kevin C. Costantini: “Development of a Cyber Attack Simulator for Network Modeling and Cyber Security Analysis” October, 2007
10. Sean Convery Cisco Systems: Hacking Layer 2: “Fun with Ethernet Switches”
11. A. Mahrouqi, P. Tobin, S. Abdalla, and T. Kechadi: “Simulating SQL-Injection Cyber-Attacks Using GNS3”
12. Παναγιώτα Αλμπάνη ,Αλέξανδρος Τσίνος: “ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ” ΑΡΤΑ 2006
13. Χαρίκλεια Συρτάρη: «ΠΡΟΣΟΜΟΙΩΣΗ ΔΙΚΤΥΩΝ ΜΕ ΤΗ ΧΡΗΣΗ ΤΟΥ RIVERBED MODELER»
14. Κατσάρας Δημήτρης: “Δίκτυα Καθοριζόμενα Από Λογισμικό” Αθήνα 2018
15. Natarajan Meghanathan: “A Tutorial on Network Security: Attacks and Controls”
16. Γεώργιος-Παναγιώτης Τερζόπουλος: “Εισαγωγή στα δίκτυα Η/Υ Μέσα από ασκήσεις και παραδείγματα” Αντίρριο 2015
17. Joseph Adebayo Ojeniyi, Maruf Olalekan Balogun, Fasola Sanjo, and Onwudebelu Ugochukwu: “Development of a Traffic Analyzer for the Detection of DDoS Attack Source”
18. ΑΒΡΑΑΜ ΚΥΡΙΑΚΙΔΗ: “ DDoS Επιθέσεις από Δίκτυα Botnet σε Κρίσιμες Υποδομές του Έξυπνου Δικτύου” Θεσσαλονίκη, Οκτώβριος 2015

19. Anatoliy Balyk, Mikolaj Karpinski, Artur Naglik, Gulmira Shangytbayeva, Ihor Romanets: “USING GRAPHIC NETWORK SIMULATOR 3 FOR DDOS ATTACKS SIMULATION”
20. Καραμάνης Νικόλαος : “Επιθέσεις Distributed Denial of Service (DDoS) και μέτρα προστασίας σε δίκτυα δεδομένων.”
21. Κυριάκος Στεφανίδης: “ Προστασία Συστημάτων από Κατανεμημένες Επιθέσεις στο Διαδίκτυο”
22. Paul MIHĂILĂ, Titus BĂLAN, Radu CURPEN, Florin SANDU: “Network Automation and Abstraction using Python Programming Methods”
23. Y. Aleksieva, H. Valchanov: “Network Simulator for Botnet DoS Attacks”
24. Αικατερίνη Βαιράμη: “ Ασφάλεια δικτύου και ανάλυση αδυναμιών του”
25. Βαρτζώκα Δήμητρα: “ΜΕΛΕΤΗ, ΕΛΕΓΧΟΣ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ ΥΛΟΠΟΙΗΣΕΩΝ ΔΙΚΤΥΩΝ ΚΑΘΟΡΙΖΟΜΕΝΩΝ ΑΠΟ ΛΟΓΙΣΜΙΚΟ”
26. Αντωνάτος Ιωάννης, Κρίκας Βελισσάριος: “Ασφάλεια Δικτύων και Συστήματα Ανίχνευσης Και Απόκρισης Επιθέσεων” Πάτρα Ιούνιος 2016
27. Alberto Simon Fernandez: “Automating the configuration of networking devices with Python”
28. A. Sardana and R. C. Joshi, "Autonomous dynamic honeypot routing mechanism for mitigating DDoS attacks in DMZ," 2008 16th IEEE International Conference on Networks, 2008, pp. 1-7, doi: 10.1109/ICON.2008.4772623.
29. M. Yoon, S. Chen and Z. Zhang, "Minimizing the Maximum Firewall Rule Set in a Network with Multiple Firewalls," in IEEE Transactions on Computers, vol. 59, no. 2, pp. 218-230, Feb. 2010, doi: 10.1109/TC.2009.172.
30. B. Nagpal, P. Sharma, N. Chauhan and A. Panesar, "DDoS tools: Classification, analysis and comparison," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 2015, pp. 342-346.
31. Y. Lan and Z. Chen, "The Research on the OSPF Security Optimizing of Campus Network," 2015 International Conference on Network and Information Systems for Computers, 2015, pp. 592-594, doi: 10.1109/ICNISC.2015.121.
32. L. P. Feng, L. B. Zheng and L. H. Li, "An experiment teaching of NAT application in firewall," 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011, pp. 126-128, doi: 10.1109/ICCSN.2011.6013792.

33. Y. Li, D. Li, W. Cui and R. Zhang, "Research based on OSI model," 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011, pp. 554-557, doi: 10.1109/ICCSN.2011.6014631.
34. Sanjay, B. Rajendran and P. Shetty D., "DNS Amplification & DNS Tunneling Attacks Simulation, Detection and Mitigation Approaches," 2020 International Conference on Inventive Computation Technologies (ICICT), 2020, pp. 230-236, doi: 10.1109/ICICT48043.2020.9112413.
35. D. Arnaldy and T. S. Hati, "Performance Analysis of Reverse Proxy and Web Application Firewall with Telegram Bot as Attack Notification On Web Server," 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE), 2020, pp. 455-459, doi: 10.1109/IC2IE50715.2020.9274592.
36. M. Naveed, S. un Nihar and M. Inayatullah Babar, "Network intrusion prevention by configuring ACLs on the routers, based on snort IDS alerts," 2010 6th International Conference on Emerging Technologies (ICET), 2010, pp. 234-239, doi: 10.1109/ICET.2010.5638482.
37. N. Jiang, L. Shan and J. Zhao, "Application of Dynamic Port VLAN Membership with Auxiliary VLAN in Campus Area Network," 2009 Ninth International Conference on Hybrid Intelligent Systems, 2009, pp. 279-282, doi: 10.1109/HIS.2009.168.
38. D. E. Kurniawan, M. Iqbal and A. Adhitya, "Implementation and Analysis of The EtherChannel Technology Using PAgP and LACP Protocols on Cisco Switch Devices," 2021 4th International Conference of Computer and Informatics Engineering (IC2IE), 2021, pp. 255-259, doi: 10.1109/IC2IE53219.2021.9649157.

ΔΙΚΤΥΟΓΡΑΦΙΑ

1. Μοντέλο OSI. Ανακτήθηκε από το:https://www.geeksforgeeks.org/layers-of-osi-model/
2. Μοντέλο OSI και Πρωτόκολλα. Ανακτήθηκε από το:https://www.guru99.com/layers-of-osi-model.html
3. Access, Distribution, and Core Layers. Ανακτήθηκε από το:https://www.computernetworkingnotes.com/ccna-study-guide/access-distribution-and-core-layers-explained.html
4. Διεύθυνση IP. Ανακτήθηκε από το:https://community.fs.com/blog/know-ip-address-and-subnet-mask.html
5. Υποδικτυωση. Ανακτήθηκε από το:https://www.cloudflare.com/learning/network-layer/what-is-a-subnet/
6. Μάσκα Υποδικτύου. Ανακτήθηκε από το:https://www.techopedia.com/6/28587/internet/8-steps-to-understanding-ip-subnetting
7. Τεχνική VLSM. Ανακτήθηκε από το:https://www.geeksforgeeks.org/introduction-of-variable-length-subnet-mask-vlsm/
8. Πρωτόκολλο OSPF. Ανακτήθηκε από το:https://www.ictshore.com/free-ccna-course/ospf-understanding/
9. Στατική και Δυναμική δρομολόγηση. Ανακτήθηκε από το:https://www.educba.com/static-routing-vs-dynamic-routing/
10. VLAN.Ανακτήθηκε από το: https://study-ccna.com/what-is-a-vlan/
11. Etherchannel. Ανακτήθηκε από το:https://www.section.io/engineering-education/etherchannel-technology/
12. NAT.Ανακτήθηκε από το: https://www.geeksforgeeks.org/types-of-network-address-translation-nat/?ref=lbp
13. FTP and TFTP Server. Ανακτήθηκε από το: https://www.educba.com/ftp-vs-tftp/
14. Διακομιστής Syslog. Ανακτήθηκε από το:https://www.geeksforgeeks.org/what-is-syslog-server-and-its-working/
15. Διακομιστής DNS. Ανακτήθηκε από το:https://www.cloudflare.com/learning/dns/what-is-a-dns-server/
16. SQL. Ανακτήθηκε από το:https://www.sqlcourse.com/beginner-course/what-is-sql/

17. DDOS. Ανακτήθηκε από το:https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained
18. Attacks per OSI layer. Ανακτήθηκε από το: https://training.nhlearninggroup.com/blog/7-layers-of-cybersecurity-threats-in-the-iso-osi-model
19. DMZ. Ανακτήθηκε από το:https://www.fortinet.com/resources/cyberglossary/what-is-dmz
20. ACL. Ανακτήθηκε από το:https://www.imperva.com/learn/data-security/access-control-list-acl/
21. Computer port. Ανακτήθηκε από το:https://www.cloudflare.com/learning/network-layer/what-is-a-computer-port/
22. SSH. Ανακτήθηκε από το:https://www.tutorialspoint.com/difference-between-ssh-and-telnet
23. Configure Password Settings. Ανακτήθηκε από το: https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5563-configure-password-settings-on-a-switch-through-the-command.html
24. Python. Ανακτήθηκε από το: https://www.tutorialspoint.com/python/python_networking.htm
25. Port Scanner. Ανακτήθηκε από το: https://www.neuralnine.com/threaded-port-scanner-in-python/
26. Netmiko και Paramiko. Ανακτήθηκε από το: https://linuxhint.com/paramiko-difference-netmiko/
27. TFTP.Ανακτήθηκε από το: https://www.filecatalyst.com/blog/tftp-vs-ftp-vs-filecatalyst/
28. 3Layers Model.Ανακτήθηκε από το: https://www.computernetworkingnotes.com/ccna-study-guide/access-distribution-and-core-layers-explained.html
29. Ζώνες τείχους προστασίας. Ανακτήθηκε από το: https://www.gns3network.com/complete-network-firewall-guide/
30. Wikipedia. Δίκτυο Υπολογιστών. URL: https://el.wikipedia.org/wiki/Δίκτυο υπολογιστών
31. Wikipedia. Network switch. URL: https://en.wikipedia.org/wiki/Network_switch
32. Wikipedia. Μεταγωγέας. URL: https://el.wikipedia.org/wiki/Μεταγωγέας

33. Wikipedia. Multilayer switch. URL: https://en.wikipedia.org/wiki/Multilayer_switch
34. Wikipedia.Δρομολογητής. URL: https://el.wikipedia.org/wiki/Δρομολογητής
35. Wikipedia. Firewall. URL: https://el.wikipedia.org/wiki/Firewall
36. Wikipedia.Εξυπηρετητής. URL: https://el.wikipedia.org/wiki/Εξυπηρετητής
37. Wikipedia.Μοντέλο αναφοράς OSI. URL: https://el.wikipedia.org/wiki/Μοντέλο αναφοράς OSI
38. Wikipedia. Medium access control. URL: https://en.wikipedia.org/wiki/Medium_access_control
39. Wikipedia. Logical link control. URL: https://en.wikipedia.org/wiki/Logical_link_control
40. Wikipedia. localhost. URL: https://en.wikipedia.org/wiki/Localhost
41. Wikipedia.Αλγόριθμος του Ντάικστρα. URL: https://el.wikipedia.org/wiki/Αλγόριθμος του Ντάικστρα
42. Wikipedia. ICMP. URL: https://el.wikipedia.org/wiki/ICMP
43. Wikipedia. Dynamic Host Configuration Protocol.URL: https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
44. Wikipedia. OSPF. URL: https://el.wikipedia.org/wiki/Open_Shortest_Path_First
45. Wikipedia. NAT. URL: https://en.wikipedia.org/wiki/Network_address_translation
46. Wikipedia. Network Time Protocol. URL: https://en.wikipedia.org/wiki/Network_Time_Protocol
47. Wikipedia. Address Resolution Protocol. URL: https://el.wikipedia.org/wiki/Address_Resolution_Protocol
48. Wikipedia. ARP spoofing. URL: https://en.wikipedia.org/wiki/ARP_spoofing
49. Wikipedia.Λίστα ελέγχου πρόσβασης. URL: https://el.wikipedia.org/wiki/Λίστα ελέγχου πρόσβασης
50. Wikipedia. DMZ. URL: https://en.wikipedia.org/wiki/DMZ_(computing)
51. Wikipedia. SSH. URL: https://el.wikipedia.org/wiki/SSH