ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Διασύνδεση απομακρυσμένων δρομολογητών με χρήση ασφαλούς επικοινωνίας σημείου προς σημείο, πάνω από Πρωτόκολλα δυναμικής δρομολόγησης

Σταύρος Χ. Μιχαλακάκος

Εισηγητής: Δρ Χαράλαμπος Πατρικάκης, Αναπλ.Καθηγητής

ΑΘΗΝΑ
ΜΑΡΤΙΟΣ 2018

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Διασύνδεση απομακρυσμένων δρομολογητών με χρήση ασφαλούς επικοινωνίας σημείου προς σημείο, πάνω από Πρωτόκολλα δυναμικής δρομολόγησης

Σταύρος Χ. Μιχαλακάκος
Α.Μ. 40968

Εισηγητής:

Δρ Χαράλαμπος Πατρικάκης, Αναπλ. Καθηγητής

Εξεταστική Επιτροπή:

, Καθηγητής
, Καθηγητής

Ημερομηνία εξέτασης / /2018

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος, **Μιχαλακάκος Σταύρος** του **Χρήστου**, με αριθμό μητρώου **40968** φοιτητής του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών του Πανεπιστημίου Δυτικής Αττικής, πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, και αποτελεί το τελευταίο στάδιο των προπτυχιακών μου Σπουδών. Την προσπάθειά μου αυτή υποστήριξε ο επιβλέπων καθηγητής μου Χαράλαμπος Πατρικάκης, τον οποίο θα ήθελα να ευχαριστήσω.

Ακόμα θα ήθελα να ευχαριστήσω την οικογένεια μου (τους γονείς μου αλλά κυρίως τον Παππού μου και την Γιαγιά μου) για την απεριόριστη Υποστήριξη και Συμπαράσταση και τον Παιδικό μου φίλο Μιχάλη Παπαδόπουλο.

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία έχει ως αντικείμενο μελέτης, την Δυναμική Δρομολόγηση και τα πρωτόκολλα ασφαλούς επικοινωνίας σε δίκτυα IP και χωρίζεται σε 2 μέρη:

1) Θεωρητικό (Κεφ. 1,2) στο οποίο γίνεται αναλυτική αναφορά στα ασύρματα και ενσύρματα δίκτυα ,στα πρωτόκολλα δικτύου, στους αλγόριθμους δρομολόγησης και στα είδη δρομολόγησης.

2) Πρακτικό (Κεφ. 3), όπου περιγράφεται η δημιουργία μιας εικονικής τοπολογίας δύο απομακρυσμένων καταστημάτων μιας εταιρείας, με χρήση του πρωτοκόλλου OSPF (**open shortest path first)** και με την μέθοδο επαλήθευσης MD5. Η δημιουργία της εικονικής τοπολογίας θα γίνει με την χρήση του εικονικού προσομοιωτή GNS3.

Πιο αναλυτικά, στο πρώτο κεφάλαιο γίνεται αναφορά στα Ασύρματα Δίκτυα και ειδικότερα στα Ασύρματα Δίκτυα Νέας Γενιάς και στις Ασφαλείς Υπηρεσίες αυτών καθώς είναι Ευαίσθητα σε πολλές απειλές, στις δικτυακές συσκευές και στα μέσα μετάδοσης, στο μοντέλο OSI και τα επτά επίπεδα του και στο μοντέλο TCP/IP που πήρε το όνομά του από τα δύο κυριότερα πρωτόκολλα που χρησιμοποιεί. Επίσης αναλύεται η υποδικτύωση με VLSM και γίνεται αναφορά στις διευθύνσεις IP και τον μηχανισμό NAT.

Στο δεύτερο κεφάλαιο γίνεται αναφορά στα πρωτόκολλα δικτύων, στα πρωτόκολλα δρομολόγησης και στις ιδιότητες τους. Ακόμα, περιγράφονται τα πρωτόκολλα RIP και OSPF, που αποτελούν πρωτόκολλα εσωτερικής εφαρμογής (IGP), τα πρωτόκολλα εξωτερικής εφαρμογής και το πρωτόκολλο IpSec. Αναλύεται η Δρομολόγηση, οι αλγόριθμοι δρομολόγησης ,οι δρομολογητές και οι ιδιότητες που πρέπει να χαρακτηρίζουν τους Αλγόριθμους Δρομολόγησης. Στο ίδιο κεφάλαιο, αναλύονται οι μετρικές των αλγορίθμων δρομολόγησης, γίνεται η κατηγοριοποίηση τους και η ανάλυση των κατηγοριών. Στην συνέχεια αναφέρεται η ιεραρχική Δρομολόγηση και τα Πλεονεκτήματα/Μειονεκτήματα της στατικής και δυναμικής Δρομολόγησης.

Στο τρίτο κεφάλαιο, περιγράφεται βήμα-βήμα η εγκατάσταση του εικονικού προσομοιωτή GNS3. Στην συνέχεια, με την χρήση του GNS3, αναλύεται ο τρόπος δημιουργίας μιας εικονικής τοπολογίας που περιγράφει δύο απομακρυσμένα καταστήματα, και εκχώρηση διευθύνσεων στους δρομολογητές, η δρομολόγηση τους με χρήση πρωτοκόλλου OSPF και την χρήση της μεθόδου MD5 για την προστασία από ανεπιθύμητες ενέργειες.

Τέλος στο Τέταρτο κεφάλαιο γίνεται μια ανακεφαλαίωση της εργασίας, με τους στόχους που επιτεύχθηκαν και τα συμπεράσματα που προέκυψαν.

ABSTRACT

This project has as object of study, Dynamic routing and secure communication protocols in IP networks and is divided into 2 parts:

1) Theoretical (Chapter 1,2), where wireless and wired networks and their security, network protocols, algorithm routes, and routing types are being studied.

2) Practice (Chapter 3), describing the creation of a virtual topology of two remote stores in a company, using the OSPF protocol (open shortest route) and the MD5 verification method. The creation of the virtual topology will be done using the GNS3 virtual simulator.

More specifically, the first chapter refers to Wireless Networks and specifically to Wireless New Generation Networks and their Secure Services as they are Sensitive to Many Threats, to Network Devices and Transmission Media, to the OSI and its Seven Layers, and to the TCP / IP named after the two major protocols it uses. It also analyzes subnetworking with VLSM and refers to IP addresses and the NAT mechanism.

The second chapter refers to network protocols, routing protocols, and properties. In addition, the RIP and OSPF protocols, which are IGPs, the external application protocols, and the IpSec protocol, are described. Routing, routing algorithms, routers, and attributes that should characterize Route Algorithms are analyzed. In the same chapter, we analyze the metrics of the route algorithms, categorize them and analyze the categories. The following is the hierarchical routing and the advantages / disadvantages of static and dynamic routing.

The third chapter describes the installation of the GNS3 virtual simulator step by step. Then, using GNS3, we analyze how to create a virtual topology that describes two remote stores, assigning addresses to routers, routing them using OSPF, and using the MD5 configuration method to protect against unwanted actions.

Finally, the fourth chapter provides a summary of the work, with the objectives achieved and the conclusions that have emerged.

Διασύνδεση απομακρυσμένων δρομολογητών με χρήση ασφαλούς επικοινωνίας σημείου προς σημείο, πάνω από Πρωτόκολλα δυναμικής δρομολόγησης

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Γενικά

Η ανάπτυξη των Υπολογιστικών Συστημάτων και του Διαδικτύου τα τελευταία χρόνια γίνεται με ραγδαίους ρυθμούς, σε σχέση με την ανάπτυξη των δικτύων που δεν μπορεί να ‘’φτάσει’’ αυτούς τους ρυθμούς με αποτέλεσμα να υπάρχουν προβλήματα Απόδοσης, Διαχείρισης και Ασφάλειας στα Ήδη Υπάρχοντα δίκτυα.

Η έννοια της **ασφάλειας Δικτύου Υπολογιστών** σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Εκτός αυτού, θεωρείται ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών. Τα θέματα ασφαλείας σε δικτυακές υποδομές και υπολογιστικά συστήματα μπορούν να επηρεάσουν σημαντικά την εξέλιξη και την πορεία μιας επιχείρησης ή οργανισμού

Σύμφωνα με τον προηγούμενο ορισμό η ασφάλεια στα δίκτυα Υπολογιστών σχετίζεται με:

- **Πρόληψη(Preventation)** : Το σύνολο των ενεργειών για να αποφευχθούν τυχόν φθορές
- **Ανιχνευση(detection)**:Λήψη μέτρων για την ανίχνευση του χρόνου, του τρόπου και από ποιον προκλήθηκε κάποια φθορά
- **Αντίδραση(reaction)**:Οι ενέργειες για την αποκατάσταση ή ανάκτηση των συστατικών ενός δικτύου

Οι σύγχρονες επιχειρήσεις και οργανισμοί, πρέπει να θεωρείται δεδομένο, ότι έχουν τα δίκτυα τους συνδεδεμένα με το διαδίκτυο, που σημαίνει ότι προσπαθούν να παρέχουν όσο μεγαλύτερη ασφάλεια γίνεται . Η έννοια της ασφάλειας σήμερα, συνδέεται στενά με τρεις βασικές έννοιες :

- **Διαθεσιμότητα(Availability)** :η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός δικτύου υπολογιστών όταν τις χρειάζεται. Για παράδειγμα, οι χρήστες σε ένα δίκτυο οργανισμού να έχουν πρόσβαση στα δεδομένα και οι υπηρεσίες λειτουργούν ακόμα και να συμβούν απρόβλεπτες διαταραχές. Για τους σκοπούς της ασφάλειας, μας απασχολεί κυρίως η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών.
- **Εμπιστευτικότητα(Confidentiality)** : πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Άλλες εκφάνσεις της εμπιστευτικότητας είναι:

  Άλλες εκφάνσεις της εμπιστευτικότητας είναι:

  Η ιδιωτικότητα, προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και

  Η μυστικότητα, προστασία των δεδομένων που ανήκουν σε έναν οργανισμό ή μια επιχείρηση**.**

- **Ακεραιότητα (Integrity)** : η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.

Σκοπός

Η Παρούσα Πτυχιακή Εργασία με θέμα ‘’Μελέτη Δυναμικής Δρομολόγησης και πρωτοκόλλων ασφαλούς επικοινωνίας μέσω IP’’ ,έχει ως αντικείμενο την δημιουργία μιας εικονικής τοπολογίας δύο απομακρυσμένων καταστημάτων μιας εταιρείας, με σκοπό την επίτευξη ασφαλούς και αδιάκοπης επικοινωνίας μεταξύ τους , ακόμα και αν υπάρξουν ανεπιθύμητες διαταραχές. Η επίτευξη της επικοινωνίας θα γίνει με χρήση του πρωτοκόλλου OSPF (**open shortest path first)** και με την μέθοδο επαλήθευσης MD5 θα εξασφαλίζεται ταχύτητα και α-σφάλεια στο δίκτυο μας. Η δημιουργία της εικονικής τοπολογίας θα γινει με την χρήση του εικονικού προσομοιωτή GNS3.

ΘΕΩΡΗΤΙΚΟ ΜΕΡΟΣ

1. Ασύρματα Δίκτυα

Τόσο η αύξηση των τηλεπικοινωνιών στην αγορά όσο και η εμφάνιση νέων τεχνολογιών χαμηλού κόστους αλλά και η δημιουργία ετερογενών ασύρματων δικτύων πρόσβασης συντελούν στην διαθεσιμότητα των υπηρεσιών σε όλο και περισσότερους παρόχους τηλεπικοινωνιακών υπηρεσιών. Ήδη, οι τεχνολογίες πολυμέσων παρουσιάζουν ιδιαίτερη ανάπτυξη τις τελευταίες δεκαετίες, ιδιαίτερα λόγω της αύξησης της διείσδυσης του διαδικτύου (Internet) στο ευρύ κοινό που δίνει νέες δυνατότητες για παροχές επικοινωνιακών υπηρεσιών σε δημοφιλείς τομείς όπως η ενημέρωση και η ψυχαγωγία. Παρά το γεγονός ότι η εμπορική επιτυχία των νέων τεχνολογιών πρόσβασης και των ασύρματων δικτύων συνδέεται με πολλούς παράγοντες, η υποστήριξη πολυμεσικών εφαρμογών και η παροχή νέων αξιόπιστων υπηρεσιών στους χρήστες αποτελεί σημαντικό παράγοντα.

Η πρόοδος στην ανάπτυξη, υλοποίηση και διαχείριση μεγάλων και αξιόπιστων τηλεπικοινωνιακών δικτύων ήταν αποτέλεσμα όχι μόνο της εξέλιξης νέων υπηρεσιών, αλλά κυρίως της εξέλιξης των υποδομών που οδήγησαν στην παροχή ευρείας κλίμακας εμπορικών υπηρεσιών τόσο σε ιδιωτικό όσο και σε επαγγελματικό επίπεδο, οι οποίες είναι ιδιαίτερα αποδοτικές σε σχέση με τις παραδοσιακές υποδομές από πλευράς απόδοσης αλλά και οικονομικού κόστους.

Με ασύρματη δικτύωση ενώνονται πλέον δύο ή περισσότεροι υπολογιστές, οι οποίοι μπορούν να επικοινωνήσουν χρησιμοποιώντας πρωτόκολλα δικτύωσης. Τα ασύρματα δίκτυα (wireless networks) είναι δίκτυα στα οποία η πληροφορία δε μεταφέρεται μέσω καλωδίων κάνοντας με αυτόν τον τρόπο, ευέλικτη την ανταλλαγή δεδομένων, ενώ χρησιμοποιούνται υπέρυθρα, υπεριώδη ή ράδιο κύματα για να συνδέσουν τα υπολογιστικά συστήματα στο δίκτυο.

Τα ασύρματα δίκτυα μπορούν να ταξινομηθούν ως εξής:

- Δίκτυα Ασύρματης Προσωπικής Περιοχής / Wireless Personal Area- (WPAN): είναι ένα ασύρματο δίκτυο χαμηλής εμβέλειας που καλύπτει μια

έκταση μόλις μερικών δεκάδων μέτρων. Αυτό το είδος δικτύου χρησιμοποιείται γενικά για τη σύνδεση περιφερειακών συσκευών (όπως εκτυπωτές, κινητά τηλέφωνα και οικιακές συσκευές). Μία τέτοια τεχνολογία είναι η τεχνολογία Bluetooth, η οποία χρησιμοποιήθηκε ως βάση για ένα νέο πρότυπο, το IEEE 802.15.

- Ασύρματα LANs / Wireless LAN (WLAN): είναι ένα ασύρματο δίκτυο που συνδέει δύο ή περισσότερες συσκευές που χρησιμοποιούν ασύρματη επικοινωνία σε μια συγκεκριμένη περιοχή όπως σπίτι, σχολείο, εργαστήριο ηλεκτρονικών υπολογιστών ή κτίριο γραφείων. Αυτό δίνει στους χρήστες τη δυνατότητα να μετακινούνται μέσα σε μια περιοχή τοπικής κάλυψης και να παραμένουν συνδεδεμένοι στο δίκτυο. Μέσω μιας πύλης, ένα WLAN μπορεί επίσης να παρέχει σύνδεση με το ευρύτερο Διαδίκτυο.

1.1 Wi-Fi

Η τεχνολογία ασύρματης δικτύωσης Wi-Fi αποτελεί τη δημοφιλέστερη τεχνολογία ασύρματης δικτύωσης, καθώς καθημερινά χρήστες απ' όλο τον κόσμο τη χρησιμοποιούν για την σύνδεση τους στο διαδίκτυο. Η τεχνολογία ασύρματης δικτύωσης βασίζεται στην προδιαγραφή IEEE 802.11 b/g/n και εκπέμπει στα 2.4 GHz.

1.2 Το Πρότυπο 802.11

Το πρότυπο 802.11 έχει δύο καταστάσεις λειτουργίας, η πρώτη είναι η κατάσταση υποδομής και η δεύτερη η κατάσταση ειδικού σκοπού. Η πρώτη αποτελεί την τεχνολογία ασύρματης δικτύωσης στην οποία ο χρήστης συνδέεται από ένα σημείο πρόσβασης (access point) το οποίο αναλαμβάνει την μετάβαση της πληροφορίας από το δίκτυο στο χρήστη μέσω ραδιοκυμάτων.

Η δεύτερη κατάσταση η οποία είναι λιγότερο συνηθισμένη, αφορά δίκτυα Ad-Hoc τα οποία αποτελούνται από ένα σύνολο υπολογιστών συνδεδεμένων μεταξύ τους με σκοπό την απευθείας αποστολή πακέτων μεταξύ τους. Η ύπαρξη σημείου πρόσβασης σε αυτή την κατάσταση δεν υφίσταται.

1.3 Το μοντέλο OSI (Open System Interconnection)

Το μοντέλο αρχιτεκτονικής δικτύων OSI (Open System Interconnection) ή μοντέλο αναφοράς OSI (Reference Model) σχεδιάστηκε από τον Διεθνή Οργανισμό Τυποποίηση ISO (International Standards Organization). Το όνομά του οφείλεται στην αναφορά του σε ανοικτά συστήματα, δηλαδή συστήματα που είναι ανοικτά στην μεταξύ τους επικοινωνία.

Το μοντέλο OSI αποτελείται από επτά στρώματα και δεν αποτελεί από μόνο του μια αρχιτεκτονική δικτύου, διότι δεν προδιαγράφει επακριβώς τις υπηρεσίες και τα πρωτόκολλα που πρέπει να χρησιμοποιηθούν σε κάθε στρώμα. Το κάθε επίπεδο εκτός από το πρώτο, χρησιμοποιεί τις υπηρεσίες των κατώτερων επιπέδων σε συνδυασμό με τις δικές του λειτουργίες για να δημιουργήσει νέες υπηρεσίες που μπορούν να χρησιμοποιηθούν από το ανώτερο επίπεδο.

Οι αρχές που εφαρμόστηκαν για να προκύψουν τα επτά στρώματα του OSI είναι οι ακόλουθες:

- Ένα στρώμα πρέπει να δημιουργηθεί οπουδήποτε χρειάζεται ένα διαφορετικό επίπεδο αφαίρεσης.
- Κάθε στρώμα πρέπει να εκτελεί μια καλά προσδιορισμένη λειτουργία.
- Η λειτουργία του καθενός στρώματος πρέπει να επιλέγεται με προοπτική τον καθορισμό διεθνώς τυποποιημένων πρωτοκόλλων.
- Τα όρια των στρωμάτων πρέπει να επιλέγονται έτσι ώστε να ελαχιστοποιείται η ροή της πληροφορίας μέσω των διεπαφών.
- Ο αριθμός των στρωμάτων πρέπει να είναι αρκετά μεγάλος ώστε να μην στριμώχνονται διακεκριμένες λειτουργίες στο ίδιο στρώμα, και αρκετά μικρός ώστε να μην γίνεται η αρχιτεκτονική δύσχρηστη.

Τα επτά επίπεδα του μοντέλου OSI είναι τα εξής:

1. Το **φυσικό επίπεδο** (Physical Layer) :Είναι το πρώτο επίπεδο της αρχιτεκτονικής και είναι υπεύθυνο για τη μετάδοση ανεπεξέργαστων δυαδικών ψηφίων μέσω ενός καναλιού επικοινωνίας. Παρέχει τα μηχανικά, ηλεκτρικά, λειτουργικά και διαδικαστικά μέσα για την ενεργοποίηση, υποστήριξη και απενεργοποίηση της φυσικής διασύνδεσης και για τη μετάδοση δυαδικών ψηφίων, μεταξύ δύο συστημάτων(πιο συγκεκριμένα μεταξύ δύο οντοτήτων γραμμής δεδομένων). Τα τυπικά ερωτήματα εδώ είναι το πόσα volt απαιτούνται για την ανα-

παράσταση ενός δυαδικού ψηφίου, κατά πόσο μπορεί να διεξάγεται η μετάδοση και προς τις δύο κατευθύνσεις ταυτόχρονα, πώς εγκαθίσταται η αρχική σύνδεση και πώς απολύεται όταν τελειώσουν και οι δύο πλευρές , πόσες ακίδες θα έχει ο ακροδέκτης του δικτύου και ποιος είναι ο ρόλος της καθεμιάς.

2. Το **επίπεδο σύνδεσης ή ζεύξης δεδομένων** (Data Link Layer): Το επίπεδο αυτό παρέχει τα λειτουργικά και διαδικαστικά μέσα για την εγκατάσταση, υποστήριξη και απόλυση συνδέσεων γραμμής δεδομένων, μεταξύ οντοτήτων επιπέδου δικτύου. Επίσης είναι υπεύθυνο για τη μεταφορά δεδομένων εξυπηρέτησης (SDUs) επιπέδου γραμμής. Μια σύνδεση γραμμής δεδομένων δημιουργείται πάνω από μία ή περισσότερες φυσικές συνδέσεις. Βασικό τμήμα του επιπέδου γραμμής αποτελούν οι διαδικασίες ανάγνωσης και διόρθωσης λαθών που μπορούν να συμβούν στο φυσικό επίπεδο.

3. Το **επίπεδο δικτύου** (Network Layer): Το επίπεδο δικτύου παρέχει υπηρεσίες για την εγκατάσταση, την υποστήριξη και τον τερματισμό συνδέσεων δικτύου, καθώς επίσης και την ανταλλαγή Μονάδων Δεδομένων Εξυπηρέτησης Δικτύου (NSDUs) μεταξύ οντοτήτων μεταφοράς. Πολλά προβλήματα μπορεί να ανακύψουν, όταν ένα πακέτο πρέπει να ταξιδέψει από ένα δίκτυο σε άλλο για να φτάσει στον προορισμό του. Η διευθυνσιοδότηση που χρησιμοποιείται από το δεύτερο δίκτυο μπορεί να είναι διαφορετική από εκείνη του πρώτου. Το δεύτερο δίκτυο μπορεί να μην δέχεται καθόλου το πακέτο επειδή είναι πολύ μεγάλο. Μπορεί να διαφέρουν τα πρωτόκολλα και πολλά άλλα. Η επίλυση αυτών των προβλημάτων, ώστε να επιτραπεί η διασύνδεση ετερογενών δικτύων ,είναι έργο του στρώματος δικτύου. Στα δίκτυα εκπομπής, το πρόβλημα δρομολόγησης είναι απλό, με συνέπεια το στρώμα δικτύου να είναι συχνά ισχνό ή ακόμα και ανύπαρκτο.

4. Το **επίπεδο μεταφοράς** (Transport Layer): Βασική του λειτουργία είναι να δέχεται δεδομένα από το ανώτερο επίπεδο, να τα διασπά αν χρειάζεται σε μικρότερες μονάδες, να τα μεταβιβάζει στο επίπεδο δικτύου, και να εξασφαλίζει ότι όλα τα τμήματα φτάνουν σωστά στο άλλο άκρο. Παρέχει έναν αξιόπιστο μηχανισμό για την ανταλλαγή δεδομένων μεταξύ διεργασιών σε διαφορετικά συστήματα. Θεωρείται ως το ανώτερο από τα “κατώτερα” πρωτόκολλα. Η θεώρηση αυτή προκύπτει από το γεγονός ότι ο βασικός προσανατολισμός του επιπέδου μεταφοράς και των επιπέδων που βρίσκονται κάτω από αυτό, είναι η μετάδοση των δεδομένων μεταξύ των συστημάτων, μέσω του επικοινωνιακού

δικτύου. Αντίθετα, πάνω από το επίπεδο μεταφοράς οι υπηρεσίες που παρέχονται από τα ανώτερα επίπεδα είναι προσανατολισμένες προς τις εφαρμογές και τις απαιτήσεις του χρήστη. Τα πρωτόκολλα που καθορίζονται στο επίπεδο μεταφοράς έχουν την έννοια του “τελικού σημείου-προς –τελικό σημείο ”(end-to-end). Τα τελικά σημεία ορίζονται σε αντιστοιχία με οντότητες του επιπέδου αναφοράς.

5. Το **επίπεδο συνδιάλεξης** (Session Layer): Το επίπεδο συνδιάλεξης παρέχει το μηχανισμό για τον έλεγχο του διαλόγου μεταξύ δύο οντοτήτων του επιπέδου παρουσίασης. Παρέχει τα μέσα ώστε δύο οντότητες του επιπέδου παρουσίασης να εγκαταστήσουν και να χρησιμοποιήσουν μια σύνδεση η οποία ονομάζεται “συνδιαλέξεις” (session). Μια συνδιάλεξη επιτρέπει τη συνηθισμένη μεταφορά δεδομένων, όπως δηλαδή και το στρώμα μεταφοράς, αλλά παρέχει επίσης επιπρόσθετες υπηρεσίες, χρήσιμες σε μερικές εφαρμογές. Μια συνδιάλεξη μπορεί να χρησιμοποιηθεί για να επιτρέψει την είσοδο ενός χρήστη σ’ ένα απομακρυσμένο σύστημα ή τη μεταφορά ενός αρχείου μεταξύ δύο συστημάτων. Μια υπηρεσία συνδιάλεξης είναι η διαχείριση σκυτάλης (token management). Για κάποια πρωτόκολλα είναι ουσιώδες το να μην αποπειρώνται και οι δύο πλευρές την ίδια λειτουργία κατά την ίδια στιγμή. Για να διαχειρίζεται αυτές τις δραστηριότητες, το στρώμα συνόδου παρέχει σκυτάλες που μπορούν να ανταλλάσσονται. Μόνο η πλευρά που κατέχει τη σκυτάλη μπορεί να εκτελέσει την κρίσιμη λειτουργία. Μια άλλη υπηρεσία συνδιάλεξης είναι ο συγχρονισμός (synchronization), η οποία είναι υπεύθυνη για τήρηση σημείων ελέγχου σε μακρόχρονες μεταδόσεις έτσι ώστε αυτές να μπορούν να συνεχιστούν από το σημείο που διακόπηκαν, μετά από μια κατάρρευση συστήματος.

6. Το **επίπεδο Παρουσίασης** (Presentation Layer) : Το επίπεδο παρουσίασης ασχολείται με την παρουσίαση της πληροφορίας στις οντότητες του επιπέδου εφαρμογής. Σκοπός του επιπέδου αυτού είναι η μετάφραση της πληροφορίας, έτσι ώστε να εξασφαλίζει ότι τα τελικά συστήματα θα επικοινωνούν με επιτυχία, ακόμα και αν χρησιμοποιούν διαφορετικές αναπαραστάσεις δεδομένων για την πληροφορία. Αυτό μπορεί να γίνει ορίζοντας με αφαιρετικό τρόπο τις δομές δεδομένων που θα ανταλλάσσονται, μαζί με μια τυποποιημένη κωδικοποίηση. Το επίπεδο παρουσίασης αυτές τις αφαιρετικές δομές δεδομένων και επιτρέπει τον ορισμό και την ανταλλαγή δεδομένων υψηλού επιπέδου.

7. Το **επίπεδο Εφαρμογής** (Application Layer): Το επίπεδο εφαρμογής είναι το σύνορο μεταξύ του περιβάλλοντος των ανοικτών συστημάτων και των διεργασιών εφαρμογής που χρησιμοποιεί το περιβάλλον αυτό για την ανταλλαγή δεδομένων. Αποτελεί το στοιχείο εκείνο του ανοικτού συστήματος, που εκτελεί την επεξεργασία της πληροφορίας για μια συγκεκριμένη εφαρμογή. Τα πρωτόκολλα (και οι υπηρεσίες) του επιπέδου αυτού είναι πολλά και ποικίλα, λόγω της ανάγκης υποστήριξης του ευρέως φάσματος των δυνατών εφαρμογών. Όλες οι λειτουργίες που δεν εκτελούνται από τα κατώτερα επίπεδα περιέχονται στο επίπεδο εφαρμογής και μπορούν να εκτελούνται είτε από προγράμματα, είτε από τους αντίστοιχους χειριστές. Η βασική διαφοροποίηση σε σχέση με τα προηγούμενα επίπεδα βρίσκεται στο γεγονός ότι το επίπεδο εφαρμογής δεν παρέχει υπηρεσίες σε κάποιο ανώτερο επίπεδο, αλλά σε διεργασίες εφαρμογών που βρίσκονται εκτός της αρχιτεκτονικής του μοντέλου OSI. Έτσι οι υπηρεσίες του επιπέδου αυτού δεν αντιστοιχίζονται σε «σημεία πρόσβασης για εξυπηρέτηση» (SAPs). [16]

1.4 Το μοντέλο TCP/IP

Το μοντέλο OSI παρέμεινε θεωρητικό εξαιτίας του μεγάλου αριθμού επιπέδων που έχει, αλλά και λόγω άλλων παραγόντων, ωστόσο, έβαλε τις βάσεις ανάπτυξης άλλων μοντέλων με ευρεία εφαρμογή. Η πρώτη στοιβάδα πρωτοκόλλων που εμφανίστηκε ήταν το ζεύγος πρωτοκόλλων TCP/IP. Το μοντέλο αυτό αναπτύχθηκε όταν το αμερικάνικο δίκτυο ARPANET άρχισε να συνδέεται με ασύρματα και δορυφορικά δίκτυα. Γι’ αυτό είχε από την αρχή την προοπτική της διαδικτύωσης.

Μετά από μελέτες που έγιναν, δημιουργήθηκε το μοντέλο αναφοράς TCP/IP (TCP/IP Reference Model) το οποίο πήρε το όνομα του από τα δύο κυριότερα πρωτόκολλα που χρησιμοποιεί (TCP και IP). Βασικός σκοπός του μοντέλου αυτού ήταν η εξασφάλιση της αξιοπιστίας του δικτύου σε περίπτωση βλαβών κάποιων τμημάτων του υποδικτύου. Δηλαδή, το δίκτυο έπρεπε να παραμένει σε κατάσταση λειτουργίας, ακόμη και αν διαπιστωνόταν βλάβη σε κάποιο σημείο του[6].

Οι αυξημένες ακόμη, απαιτήσεις σε καινούργιες εφαρμογές, όπως η ανταλλαγή αρχείων ή η μετάδοση ομιλίας σε πραγματικό χρόνο απαιτούσαν μια νέα

αρκετά ευέλικτη αρχιτεκτονική, την οποία μπορούσε να προσφέρει το μοντέλο TCP/IP.

Επίπεδο Διαδικτύου (Internet Layer)

Όλες αυτές οι απαιτήσεις οδήγησαν στην επιλογή ενός δικτύου μεταγωγής πακέτων που βασίζεται σε ένα ασυνδεσμικό επίπεδο διαδικτύου.Το επίπεδο αυτό, που ονομάστηκε επίπεδο διαδικτύου, είναι ο συνδετικός κρίκος του μοντέλου και είναι σε αντιστοιχία με το επίπεδο δικτύου του μοντέλου OSI. Έργο του είναι να επιτρέπει στους κόμβους να στέλνουν πακέτα σε οποιοδήποτε δίκτυο, που θα ταξιδεύουν ανεξάρτητα το ένα από το άλλο στον προορισμό τους, πιθανώς ακολουθώντας διαφορετική διαδρομή. Όταν συμβεί να φθάσουν με διαφορετική σειρά από την σειρά αναχώρησης από τον πομπό, στόχος αυτού του επιπέδου είναι να τα επαναδιατάξει στη σωστή σειρά. Το επίπεδο Διαδικτύου καθορίζει μία τυπική μορφή πακέτου και το πρωτόκολλο αυτό ονομάζεται IP (Internet Protocol). Στο επίπεδο αυτό στέλνονται πακέτα IP στον προορισμό τους. Κύρια αποστολή του επιπέδου είναι η δρομολόγηση των πακέτων με ταυτόχρονη αποφυγή της συμφόρησης. Για όλους τους παραπάνω λόγους συμπεραίνουμε ότι το επίπεδο διαδικτύου του TCP/IP παρουσιάζει πολλές ομοιότητες με το επίπεδο του δικτύου του μοντέλου OSI.

Επίπεδο Μεταφοράς (Transport Layer)

Το επίπεδο μεταφοράς του μοντέλου TCP/IP είναι αντίστοιχο με το πρωτόκολλο μεταφοράς του μοντέλου OSI. Δύο βασικά πρωτόκολλα έχουν αναπτυχθεί στο επίπεδο αυτό. Το πρώτο ονομάζεται πρωτόκολλο ελέγχου μετάδοσης TCP (Transmission Control Protocol) και είναι ένα αξιόπιστο πρωτόκολλο με σύνδεση, το οποίο επιτρέπει τη μετάδοση δεδομένων χωρίς σφάλματα από ένα σύστημα σε ένα άλλο μέσω του δικτύου του Internet. Τεμαχίζει τα bytes της προς μετάδοση πληροφορίας και τα περνάει μέσω του επιπέδου διαδικτύου. Στον προορισμό το επίπεδο μεταφοράς του δέκτη επανασυνδέει τα δεδομένα ώστε να αναπαραχθεί η αρχική πληροφορία. Το πρωτόκολλο TCP/IP διαχειρίζεται επίσης τον έλεγχο ροής, ώστε να υπάρχει απόλυτη βεβαιότητα ότι ένας γρήγορος πομπός δε θα υπερφορτώσει ένα αργό δέκτη. Το δεύτερο πρωτόκολλο αυτού του επιπέδου ονομάζεται πρωτόκολλο UDP (User Datagram Protocol). Το πρωτόκολλο αυτό είναι χωρίς σύνδεση πρωτόκολλο, δεν είναι

τόσο αξιόπιστο με εφαρμογές που δεν επιτρέπουν έλεγχο ροής με το TCP. Επίσης, δεν διορθώνει σφάλματα που μπορεί να προκόψουν. Ωστόσο, χρησιμοποιείται ευρέως για εφαρμογές και αναζητήσεις ερώτησης - απάντησης τύπου πελάτη - εξυπηρετητή, στις οποίες η γρήγορη παράδοση είναι περισσότερο επιθυμητή από την ακριβή παράδοση, όπως σε μετάδοση ήχου και εικόνας.

Επίπεδο Εφαρμογών (Application Layer)

Το μοντέλο TCP/IP δεν έχει επίπεδα παρουσίασης και συνδιάλεξης, επειδή δεν υπήρχε κανένας λόγος χρησιμοποίησης τους και έτσι δεν συμπεριλήφθησαν. Η εμπειρία από το μοντέλο OSI οδήγησε στη χρήση του ελάχιστου δυνατού αριθμού επιπέδων. Έτσι, το επίπεδο εφαρμογής είναι το μόνο ανώτερο επίπεδο που συμπεριλαμβάνει τα πρωτόκολλα των ανώτερων στρωμάτων. Τα καινούργια πρωτόκολλα περιλαμβάνουν: εικονικά τερματικά (Telnet), μεταφορά αρχείων (FTP) και ηλεκτρονικό ταχυδρομείο (SMTP). Το εικονικό τερματικό πρωτόκολλο επιτρέπει σε ένα χρήστη να συνδεθεί με μία απομακρυσμένη μηχανή και να εργαστεί σε αυτή. Το πρωτόκολλο μεταφοράς αρχείων παρέχει έναν αποδοτικό τρόπο για μεταφορά αρχείων από μία μηχανή σε μία άλλη. Η υπηρεσία ηλεκτρονικού ταχυδρομείου αρχικά έκανε μεταφορά αρχείων, αλλά αργότερα αναπτύχθηκε ένα νέο πρωτόκολλο ηλεκτρονικού ταχυδρομείου. Πολλά άλλα πρωτόκολλα έχουν προστεθεί σε αυτό τα τελευταία χρόνια όπως το DNS (Domain Name Service) για απεικόνιση ονομάτων κόμβων στις διευθύνσεις δικτύων, το NTTP για μεταφορά αρχείων και το HTTP για σχεδίαση ιστοσελίδων στο Internet.

Επίπεδο Διασύνδεσης μεταξύ υπολογιστή υπηρεσίας & δικτύου

Το επίπεδο αυτό είναι σε αντιστοιχία με το φυσικό επίπεδο και το επίπεδο ελέγχου γραμμής δεδομένων του μοντέλου 081. Δεν καθορίζεται σαφώς και μπορεί να διαφέρει από υπολογιστή (κόμβο) σε υπολογιστή (κόμβο) και από δίκτυο σε δίκτυο. Το μόνο που καθορίζεται είναι η σύνδεση που δημιουργείται μεταξύ του υπολογιστή (κόμβου) και του δρομολογητή.

1.5 Ασφαλείς υπηρεσίες και ασύρματα δίκτυα νέας γενιάς

Στις μέρες μας οι υπηρεσίες πολυμέσων έχουν πολλαπλασιαστεί σε σχέση με τα προηγούμενα χρόνια λόγω των νέων μηχανισμών κωδικοποίησης πληροφοριών, των ευζωνικών δικτύων και της ευελιξίας του πρωτοκόλλου IP. Όλο και περισσότεροι χρήστες έχουν πλέον πρόσβαση στο Διαδίκτυο είτε μέσω οικιακών συνδρομών όσο και μέσω των κινητών συσκευών. Τα σύγχρονα δίκτυα υπόσχονται σημαντική αύξηση του διαθέσιμου εύρους ζώνης, το οποίο όμως δεν είναι αρκετό αν δεν εξελιχθούν οι μηχανισμοί κωδικοποίησης και τα πρωτόκολλα μετάδοσης αλλά και οι τρόποι ασφάλειας από τους διάφορους κινδύνους.

Τα ασύρματα δίκτυα είναι ιδιαίτερα ευαίσθητα σε διάφορες απειλές όπως:

- Ασύρματοι εισβολείς
- Εφαρμογές Rogue
- Υποκλοπή δεδομένων
- Επιθέσεις DoS

Για την αντιμετώπιση των απειλών από ασύρματους εισβολείς και την προστασία των δεδομένων έγινε αρχικά χρήση:

- SSID: Τα σημεία πρόσβασης(Access Points) και ορισμένοι ασύρματοι δρομολογητές επιτρέπουν στο SSID να είναι απενεργοποιημένο. Οι χρήστες που θέλουν να συνδεθούν πρέπει να προσδιορίσουν χειροκίνητα το SSID για τη σύνδεση με το δίκτυο.
- MAC addresses filtering: Ο διαχειριστής μπορεί χειροκίνητα να επιτρέψει ή να αρνηθεί στους πελάτες ασύρματη πρόσβαση με βάση τη φυσική τους MAC.

Επίσης, υπάρχουν τεχνικές πιστοποίησης για την προστασία των ασύρματων δικτύων όπως :

- **Ενσύρματη Ισοδύναμη Προστασία Προσωπικών Δεδομένων / Wired Equivalent Privacy (WEP)**. Με το WEP μπορούν να χρησιμοποιηθούν δύο μέθοδοι πιστοποίησης:
  - Πιστοποίηση Ανοικτού Συστήματος (Open System authentication) και
  - Πιστοποίηση Διαμοιραζόμενου Κλειδιού (Shared Key authentication).

Στην Πιστοποίηση Ανοικτού Συστήματος, δεν απαιτείται ο πελάτης του Ασύρματου Δικτύου (WLAN) να προβεί σε διαδικασία πιστοποίησης. Στη συνέχεια όμως πρέπει να χρησιμοποιηθούν τα κλειδιά για την κρυπτογράφηση των πλαισίων και επομένως ο πελάτης πρέπει να έχει τα σωστά κλειδιά.

Στην Πιστοποίηση Διαμοιραζόμενου Κλειδιού, χρησιμοποιείται το κλειδί WEP σε μία διαδικασία τεσσάρων βημάτων:

1. Ο πελάτης στέλνει μία αίτηση πιστοποίησης στο Σημείο Πρόσβασης (Access Point).
2. Το Access Point απαντά με μία πρόσκληση Απλού Κειμένου (μη κρυπτογραφημένου)
3. Ο πελάτης κρυπτογραφεί το κείμενο της πρόσκλησης με το κλειδί WEP και το στέλνει πίσω.
4. Το Access Point αποκρυπτογραφεί την απόκριση. Εάν το κείμενο ταιριάζει με το κείμενο της πρόσκλησης, τότε το Access Point στέλνει πίσω μία θετική απόκριση.

Μετά την πιστοποίηση και τη σύνδεση, το WEP κλειδί χρησιμοποιείται για την κρυπτογράφηση των πλαισίων χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης RC4. Όμως παρόλο που η πιστοποίηση Διαμοιραζόμενου Κλειδιού φαίνεται να είναι πιο ασφαλής από την πιστοποίηση Ανοικτού Συστήματος, στην πραγματικότητα συμβαίνει το ακριβώς αντίθετο. Υποκλέπτοντας τα πλαίσια απόκρισης κατά την διάρκεια της χειραψίας στην πιστοποίηση διαμοιραζόμενου κλειδιού, είναι δυνατόν να παραχθεί η ακολουθία του κλειδιού.

- **Προστατευμένη Πρόσβαση Wi-Fi / Wi-Fi Protected Access (WPA)**: Ένα πρότυπο Wi-Fi Alliance, που χρησιμοποιεί WEP, αλλά εξασφαλίζει τα δεδομένα με το κατά πολύ ισχυρότερο πρωτόκολλο Temporal Key Integrity Protocol (TKIP) αλγόριθμο κρυπτογράφησης. Το TKIP αλλάζει το κλειδί για κάθε πακέτο και το καθιστά πολύ πιο δύσκολο να παραβιαστεί.

1.6 Δικτυακές συσκευές και μέσα μετάδοσης

Για την ασύρματη σύνδεση των δικτύων είναι απαραίτητη η χρήση ορισμένων διαδικτυακών συσκευών ή μέσων μετάδοσης. Παρακάτω αναλύονται ορισμένα από αυτά τα μέσα.

1. ***Modem***

Για την σύνδεση των απομακρυσμένων υπολογιστών γίνεται η χρήση του τηλεφωνικού δικτύου και η χρήση μιας συσκευής που ονομάζεται modem. Η ψηφιακή πληροφορία των υπολογιστών είναι αδύνατο να μεταδοθεί από μόνη της στο τηλεφωνικό δίκτυο, διότι τα σήματα ανήκουν σε μια ζώνη συχνοτήτων εύρους από 300 Hz έως 3100 Hz. Όμως, ένα ειδικά διαμορφωμένο συνεχές σήμα στην περιοχή από 1000 Hz έως 2000 Hz μπορεί να μεταφέρει την ψηφιακή πληροφορία (κατάσταση 0 και 1).

2. ***Διανομέας (HUB)***

Ένας διανομέας είναι η πιο βασική συσκευή δικτύωσης που συνδέει πολλούς υπολογιστές ή άλλες συσκευές δικτύου μαζί. Σε αντίθεση με έναν μεταγωγέα δικτύου ή δρομολογητή, ένας διανομέας δικτύου δεν έχει πίνακες δρομολόγησης ή πληροφορίες σχετικά με το πού πρέπει να στείλει πληροφορίες και να μεταδίδει όλα τα δεδομένα δικτύου. Οι περισσότεροι διανομείς μπορούν να ανιχνεύσουν βασικά σφάλματα δικτύου, αλλά η ύπαρξη όλων των πληροφοριών που μεταδίδονται σε πολλαπλές θύρες, μπορεί να αποτελέσει κίνδυνο ασφαλείας και να προκαλέσει κωλύματα.[21]

3. ***Αναμεταδότης***

Ο αναμεταδότης δουλεύει στο φυσικό επίπεδο. Η εγκατάστασή του καθαρίζει το σήμα από τους θορύβους πριν το αλλοιώσουν εντελώς. Δηλαδή δέχεται στην είσοδο του το σήμα πριν αλλοιωθεί και το αναπαράγει στέλνοντας το αντίγραφο του στην έξοδο.

4. ***Γέφυρα - Bridge***

Μια γέφυρα είναι ένας τύπος δικτυακής συσκευής υπολογιστών που παρέχει διασύνδεση με άλλα δίκτυα γέφυρας που χρησιμοποιούν το ίδιο πρωτόκολλο. Οι συσκευές Bridge λειτουργούν στο επίπεδο σύνδεσης δεδομένων του μοντέλου OSI, συνδέοντας δύο διαφορετικά δίκτυα μαζί και παρέχοντας επικοινωνία μεταξύ τους.[22]

5. ***Μεταγωγείς - Switches***

Ο μεταγωγέας είναι σαν την γέφυρα αλλά πιο εξελιγμένος γιατί οι καθυστερήσεις είναι λιγότερες από την γέφυρα. Λειτουργεί στο δεύτερο επίπεδο του μοντέλου TCP/IP. Έχει περισσότερες υποδοχές και μπορεί να δημιουργεί διασυνδέσεις με διαφορετικούς ρυθμούς πχ 10 Mbps, 100 Mbps κ.τ.λ. Επιτρέπει αμφίδρομη επικοινωνία μεταξύ πομπού και δέκτη δηλαδή κάθε συσκευή που είναι συνδεδεμένη με τον μεταγωγέα μπορεί να στέλνει και να λαμβανεί πλαίσια ταυτόχρονα.

6. ***Δρομολογητής (Router)***

Ο δρομολογητής είναι η συσκευή που παραλαμβάνει και προωθεί τα πακέτα στα διάφορα υποδίκτυα. Μπορεί να συνδέεται με έναν ή και περισσότερους συνδέσμους που συνδέουν κόμβους-δρομολογητές του ίδιου δικτύου αλλά και κόμβους-δρομολογητές διαφορετικών δικτύων. Είναι μια εξελιγμένη συσκευή που λειτουργεί σε φυσικό επίπεδο, επίπεδο σύνδεσης δεδομένων και επίπεδο δικτύου.

Τα τμήματα ενός δρομολογητή είναι η CPU, η Memory η οποία αποτελείται από τη Ram και αφορά τον πίνακα δρομολόγησης και running - configuration, η Flash, η Nvram για το startup - configuration και η Rom. Επιπλέον, παρέχει Interfaces με τα οποία γίνεται η σύνδεση του Router με κάποιο LAN ή WAN, Buses για την επικοινωνία μεταξύ cpu, interfaces και slots. Επίσης, υπάρχουν και οι ασύγχρονες σειριακές συνδέσεις για την διαχείριση του δρομολογητή, Console και Auxiliary Ports καθώς και Power Supply για την τροφοδοσία του δρομολογητή. Τέλος, στο Router μπορούν να συνδεθούν διάφορα καλώδια όπως : RolloverCable (για Configuration), CAT-5 Cable, SerialtoUsbAdaptor και V.35 Cable.

7. ***Πύλη - Gateway***

Η πύλη λειτουργεί και στα 7 επίπεδα. Αυτό που κάνει είναι να ενώνει δίκτυα που λειτουργούν με διαφορετικές αρχιτεκτονικές (αρχιτεκτονική TCP/IP, αρχιτεκτονική OSI).

8. Οπτικές ίνες

Με την οπτική ίνα η μετάδοση των πληροφοριών γίνεται με παλμούς φωτός και όχι με ηλεκτρικά σήματα. Με μια συσκευή που ονομάζεται συζευκτής μετατρέπει τα ηλεκτρικά σήματα σε παλμούς φωτός και το αντίστροφο. Το φώς μεταδίδεται προς μία πάντα κατεύθυνση μέσα από τον πυρήνα της οπτικής ίνας και συνήθως είναι από γυαλί ή πλαστικό μορφής κυλίνδρου. Ο πυρήνας περιβάλλεται από μια μονωτική επικάλυψη και αυτή από ένα περίβλημα. Ο πυρήνας και η επικάλυψη έχουν διαφορετικό δείκτη διάθλασης με σκοπό τις ανακλάσεις του φωτός στον πυρήνα. Οι οπτικές ίνες χωρίζονται σε μονότροπες όπου μόνο μια ακτίνα φωτός μεταδίδεται στην ίνα και πολύτροπη όπου πολλές ακτίνες φωτός μεταδίδονται ταυτόχρονα. Η οπτική ίνα δεν παρουσιάζει παρεμβολές και έχει την δυνατότητα, να μεταδίδει πληροφορίες σε μεγάλες αποστάσεις με υψηλές ταχύτητες όπως 2 Gbps όπου γίνεται προσπάθεια να ξεπεραστεί και αυτός ο ρυθμός. Επίσης υπάρχουν και οι Connectors (ST, SC, LC) που τερματίζουν το τέλος μιας οπτικής ίνας[1].

9. Συνεστραμμένα ζεύγη καλωδίων

Από τα παραδοσιακά μέσα μετάδοσης είναι το συνεστραμμένο ζεύγος καλωδίων. Αποτελείται από σύρματα με πυρήνα χαλκού και περιβάλλονται από μονωτικό υλικό. Όταν τα δύο σύρματα συστραφούν το ένα γύρω από το άλλο δημιουργούν κύκλωμα το οποίο μπορεί να μεταφέρει δεδομένα. Ένα καλώδιο αποτελείται από ένα ή περισσότερα ζεύγη τα οποία έχουν μονωτικό υλικό γύρω τους. Υπάρχουν δύο τύποι καλωδίων:

α) το αθωράκιστο καλώδιο συνεστραμμένου ζεύγους (UTP), το οποίο συνήθως είναι για τηλεφωνικά δίκτυα και

β) το θωρακισμένο καλώδιο συνεστραμμένου ζεύγους (STP) που έχει προστασία από το θόρυβο ή τις παρεμβολές.

10. Ομοαξονικό καλώδιο

Το ομοαξονικό καλώδιο έχει ρυθμούς μετάδοσης όπως το UTP αλλά παρέχει καλύτερη θωράκιση από τα STP και καλύπτει μεγαλύτερες αποστάσεις. Ωστόσο, οι νέες τυποποιήσεις συστημάτων δομημένης καλωδίωσης απαιτούν καλώδιο συνεστραμμένου ζεύγους ή οπτική ίνα για ψηφιακή μετάδοση γιατί

μπορούν να μεταδίδουν σε ρυθμούς από 100 Mbps έως 1 Gbps, πολύ περισσότερο σε σχέση με το ομοαξονικό καλώδιο.

1.7 Εικονικά τοπικά δίκτυα (VLANS)

Τα VLANs είναι κυρίως ενσωματωμένα στον σχεδιασμό ενός δικτύου διευκολύνοντας έτσι το δίκτυο να μπορεί να υποστηρίξει τους στόχους ενός οργανισμού. Η πρόσβαση σε ένα LAN δίκτυο συνήθως γίνεται μέσω ενός μεταγωγέα (switch). Ένα εικονικό τοπικό δίκτυο (VLAN) μπορεί να δημιουργηθεί σε έναν μεταγωγέα επιπέδου 2 για να μειώσει το μέγεθος των ονομάτων τομέα για την εκπομπή. Ενώ τα VLANs χρησιμοποιούνται κυρίως μέσα σε τοπικά δίκτυα μεταγωγής, παρόλα αυτά σύγχρονες εφαρμογές των VLANs τους επιτρέπουν να γεφυρώνουν τα MANs και WANs.

Με τα VLANs ο διαχειριστής μπορεί να ξεχωρίζει δίκτυα με κριτήρια όπως η λειτουργία, η ομάδα εργασίας ή η εφαρμογή, χωρίς να λαμβάνεται υπόψη η φυσική τοποθεσία του χρήστη ή της συσκευής. Συσκευές μέσα σε ένα VLAN λειτουργούν σαν να βρίσκονται στο δικό τους ανεξάρτητο δίκτυο, ακόμα κι αν μοιράζονται κοινή υποδομή με άλλα VLANs. Κάθε θύρα του μεταγώγεα μπορεί να ανήκει σε ένα VLAN, και unicast, broadcast αλλά και multicast πακέτα μπορούν να προωθούνται και να φτάνουν στους τελικούς χρήστες που ανήκουν στο ίδιο VLAN, με το VLAN των πακέτων που προωθούνται. Κάθε VLAN θεωρείται ένα ξεχωριστό δίκτυο, και τα πακέτα που έχουν προορισμό χρήστες διαφορετικών VLANs, θα πρέπει να προωθούνται σε συσκευή που υποστηρίζει δρομολόγηση, όπως σε έναν δρομολογητή (router).

Ένα VLAN δημιουργεί ένα λογικό τομέα εκπομπής (logical broadcast domain) που μπορεί να γεφυρώσει πολλαπλά φυσικά LAN τμήματα. Τα VLANs βελτιώνουν την απόδοση δικτύου, διαχωρίζοντας μεγάλους Broadcast Domains σε μικρότερους. Εάν μια συσκευή σε ένα VLAN στέλνει ένα πλαίσιο εκπομπής πρωτοκόλλου Ethernet (Ethernet frame), τότε όλες οι συσκευές σε αυτό το VLAN λαμβάνουν το πλαίσιο, ενώ συσκευές σε διαφορετικό VLAN όχι[2].

Τα VLANs διευκολύνουν την υλοποίηση πολιτικών πρόσβασης και ασφάλειας σύμφωνα με συγκεκριμένες ομαδοποιήσεις χρηστών. Κάθε θύρα του μεταγωγέα μπορεί να ανατεθεί σε ένα μόνο VLAN (με εξαίρεση μια θύρα που συνδέεται σε ένα τηλέφωνο με IP η σε κάποιο άλλο μεταγωγέα).

Τα VLANs διακρίνονται από μια σειρά προτερημάτων όπως:

- Ασφάλεια: Οι ομάδες που έχουν ευαίσθητα δεδομένα διαχωρίζονται από το υπόλοιπο δίκτυο, μειώνοντας έτσι τις πιθανότητες παράνομης πρόσβασης σε εμπιστευτικές πληροφορίες. Οι υπολογιστές για παράδειγμα στο πανεπιστήμιο Θεσσαλίας των σχολών βρίσκονται σε VLAN και είναι απόλυτα διαχωρισμένοι από την κυκλοφορία δεδομένων των σπουδαστών και των επισκεπτών.
- Μειωμένο κόστους: Η εξοικονόμηση κόστους απορρέει από την ανάγκη για ακριβοπληρωμένη αναβάθμιση δικτύων και από την πιο αποτελεσματική χρήση των ήδη υπάρχοντος εύρους.
- Καλύτερη απόδοση: Με τον διαχωρισμό των δικτύων επιπέδου 2 σε πολλαπλά ονόματα τομέα μειώνεται η πλεονάζουσα κυκλοφορία στο δίκτυο και ενισχύεται η απόδοση του.
- Συρρίκνωση πεδίων αναμετάδοσης: Διαχωρίζοντας ένα δίκτυο σε VLANs, μειώνεται ο αριθμός των συσκευών - παραληπτών πακέτων broadcast στο VLAN αυτό.
- Βελτιωμένη απόδοση του IT προσωπικού: Τα VLANs διευκολύνουν την οργάνωση του δικτύου, επειδή χρηστές με παρόμοιες ανάγκες / απαιτήσεις δικτύου μοιράζονται το ίδιο VLAN. Όταν τίθεται σε λειτουργία ένας καινούριος μεταγωγέας, όλες οι πολιτικές και οι διαδικασίες που έχουν ήδη ρυθμιστεί για το συγκεκριμένο VLAN εφαρμόζονται πάνω στις θύρες. Είναι επίσης εύκολο για το προσωπικό IT να αναγνωρίσει την λειτουργιά ενός VLAN δίνοντας του ένα κατάλληλο όνομα.
- Απλουστέρα project και οργάνωση εφαρμογών: Τα VLAN συναθροίζουν τους χρήστες και τις συσκευές δικτύου για να υποστηρίξουν επιχειρησιακές ή γεωγραφικές ανάγκες. Οι ξεχωριστές λειτουργιές που έχουν κάνουν με την ευκολότερη οργάνωση ενός project ή την εργασία πάνω σε μια εξειδικευμένη εφαρμογή. Ένα παράδειγμα για αυτήν την εφαρμογή αποτελεί μια πλατφόρμα απομακρυσμένης εκμάθησης για μια σχολή.[13]

Υπάρχουν διάφοροι τύποι VLAN όπως:

- VLAN Δεδομένων (Data VLAN): είναι VLAN που έχει ρυθμιστεί για να εκτελεί κυκλοφορία που παράγεται μόνο από τον χρήστη. Ένα VLAN δεδομένων αναφέρεται και ως το VLAN χρήστη. Τα VLANs δεδομένων χρησιμοποιούνται για να ξεχωρίσουν το δίκτυο σε ομάδες χρηστών ή συσκευών.[23]
- Προκαθορισμένο VLAN (Default VLAN) : Όλες οι θύρες του μεταγωγέα, ανήκουν στο προκαθορισμένο VLAN μετά από την εκκίνησή του με τις αρχικές ρυθμίσεις, το οποίο τα καθιστά όλα μέρος της ίδιας εκπομπής τομέα (Broadcast Domain). Αυτό επιτρέπει σε οποιαδήποτε συσκευή δικτύου συνδεδεμένη σε οποιαδήποτε θύρα μεταγωγής να επικοινωνεί με άλλες συσκευές σε άλλες θύρες μεταγωγέων .[23]

- Τοπικό VLAN (Local VLAN): Δύο μεταγωγείς μπορούν να συνδεθούν και να ανταλλάξουν δεδομένα μέσω θυρών που υποστηρίζουν το πρωτόκολλο IEEE 802.1Q.
- VLAN Διαχείρισης (Management VLAN) : Ένα VLAN διαχείρισης είναι ένα VLAN που έχει ρυθμιστεί για να έχει πρόσβαση στις ικανότητες διαχείρισης ενός μεταγωγέα. [14]

Η αρχιτεκτονική του VLAN απλοποιεί την διατήρηση δικτύου και βελτιώνει την απόδοση, αλλά επίσης δημιουργεί δυνατότητες για επιθέσεις από κακόβουλους χρήστες. Έτσι έχουμε τις εξής δύο τεχνικές «επίθεσης»:

- VLAN hopping: Είναι μία τεχνική που επιτρέπει η κίνηση από ένα VLAN να είναι ορατή και σε κάποιο άλλο VLAN. Επιπροσθέτως η τεχνική switch spoofing είναι ένας τύπος VLAN hopping επίθεσης που λειτουργεί εκμεταλλευόμενη την λανθασμένη παραμετροποίηση κάποιου trunk port.
- Double-tagging: Αποτελεί μία ακόμη επικίνδυνη επίθεση που αφορά τα VLANs. Αυτού του είδους η επίθεση εκμεταλλεύεται τον τρόπο που λειτουργεί το υλικό σε πολλά από τα switches. Τα περισσότερα εκτελούν μόνο ένα επίπεδο του 802.1 Q αποενθυλλάκωσης (de-encapsulation), που επιτρέπει στον εισβαλλόμενο να ενσωματώσει ένα κρυφό 802.1 Q tag εντός του αρχικού frame. Αυτό το tag, επιτρέπει το frame να προωθηθεί σε VLAN που δεν επιτρεπόταν αρχικά. Ένα σημαντικό πλεονέκτημα αυτής της τεχνικής επίθεσης είναι ότι η διπλή ενθυλάκωση (double-encapsulation) μπορεί να λειτουργήσει ακόμη

και όταν τα trunk ports είναι απενεργοποιημένα, διότι ένας απλός χρήστης στέλνει πάντα ένα frame του σε σύνδεση που δεν είναι trunk.

1.8 Διευθύνσεις IP - DNS και κλάσεις

Οι διευθύνσεις IP έχουν μέγεθος 4 byte που χωρίζονται μεταξύ τους με μία τελεία και παριστάνονται σε δεκαδική μορφή. Λόγω δυσκολίας απομνημόνευσης αυτής της μορφής οι διευθύνσεις IP αντιστοιχίζονται με κάποιο όνομα τομέα (Domain Name System). Σε μία διεύθυνση IP διακρίνεται το τμήμα δικτύου προσδιορίζοντας το δίκτυο που είναι συνδεδεμένος ένας υπολογιστής και το τμήμα υπολογιστή που αναφέρεται στον συγκεκριμένο υπολογιστή[3]. Τα βασικά είδη διευθύνσεων συνοψίζονται ως εξής:

- Διεύθυνση δικτύου: Η διεύθυνση αυτή προσδιορίζει το δίκτυο που περιέχει όλες τις συσκευές.
- Διεύθυνση broadcast: Η διεύθυνση εκπομπής χρησιμοποιείται για την μετάδοση δεδομένων προς όλους τους κόμβους του δικτύου.
- Διεύθυνση υπολογιστή: Εκχωρείται στις συσκευές που υπάρχουν στο δίκτυο.
- Δημόσιες διευθύνσεις: Χρησιμοποιούνται στο Διαδίκτυο.
- Ιδιωτικές διευθύνσεις: Προορίζονται για τα ιδιωτικά δίκτυα και δεν επιτρέπονται δημόσια.

Οι διευθύνσεις IP μπορούν να χωριστούν σε κλάσεις που ορίζουν τα μεγέθη των τμημάτων δικτύου και υπολογιστή. Οι κλάσεις κατηγοριοποιούνται ως εξής:

- Κλάση A: Έχει εύρος 1 ως 127 και για το τμήμα δικτύου δεσμεύονται 8 bit, ενώ για το τμήμα υπολογιστή 24.
- Κλάση B: Έχει εύρος 128 ως 191 δεσμεύοντας 16 bit για καθένα από τα δύο τμήματα.
- Κλάση C: Έχει εύρος 129 ως 223 και για το τμήμα δικτύου χρησιμοποιούνται 24 bit, ενώ για το τμήμα υπολογιστή 8.

Κλάσεις D και E: Περιέχουν διευθύνσεις για πολυεκπομπή και για μελλοντική χρήση αντίστοιχα.

1.9 IPv6

Ο οργανισμός IETF στις αρχές του 1990 προέβλεψε ότι ο χώρος διευθύνσεων του IPV4 καθώς ήταν το πρωτόκολλο που χρησιμοποιούνταν και το οποίο διέθετε 4.294.967.296 διευθύνσεις (32 bit) έως το 2005 θα τελείωνε. Για να λυθεί το πρόβλημα των διευθύνσεων έφερε στο προσκήνιο το IPV6, το οποίο έχει 155 δισεκατομμύρια IPV4 δίκτυα και το οποίο προβλέπεται ότι θα εξασφαλίσει χώρο διευθύνσεων για τα επόμενα 30 τουλάχιστον χρόνια.

Η συνολική επικεφαλίδα του IPV6 είναι μόνο 40bytes παρόλο που τα πεδία διευθύνσεων είναι 4 φορές μεγαλύτερα απ' ότι στο IPV4.

Για την καλύτερη απόδοση του μοντέλου έγιναν οι εξής βελτιώσεις:

- Η επικεφαλίδα του IPv6 έχει σταθερό μήκος, ενώ διαθέτει 64 bit για επεξεργασία.
- Αφαιρέθηκε το checksum της επικεφαλίδας IPv4 που υπολογίζεται κάθε φορά που 1 πακέτο περνά από 1 δρομολογητή ενώ τέλος δεν χρειάζεται οι δρομολογητές να διαιρούν ένα μεγάλο πακέτο σε μικρότερα κομμάτια και μπορούν απλά να στείλουν σήμα να τους έρχονται μικρότερα πακέτα.

Το broadcast αντικαταστάθηκε με τα multicast στο IPv6 με τα οποία δεν σταματούν όλες οι δικτυακές συσκευές για να επεξεργαστούν το μήνυμα που έρχεται αλλά μόνο όσες είναι ενεργές εκείνη τη στιγμή[4].

1.10 NAT

Οι υπηρεσίες μετάφρασης ιδιωτικών διευθύνσεων σε δημόσιες, υλοποιούνται στις συσκευές που βρίσκονται στο άκρο ενός ιδιωτικού δικτύου και ονομάζονται υπηρεσίες μετάφρασης διευθύνσεων δικτύου (Network Address Translation). Η NAT αποφεύγει τις συγκρούσεις εκχωρώντας σε κάθε υπολογιστή μια τοπικά μοναδική διεύθυνση. Για να μην καταναλώνονται γρήγορα οι διευθύνσεις IP, οι τοπικές αυτές διευθύνσεις είναι ιδιωτικές. Πράγμα που σημαίνει ότι δεν ισχύουν για το παγκόσμιο Internet. Για παράδειγμα, ένας υπολογιστής αν θέλει να στείλει ένα πάκετο σε έναν άλλο Υπολογιστή , πρέπει η διεύθυνση αφετηρίας του

πακέτου να μεταφραστεί από ιδιωτική σε δημόσια ώστε να αναγνωρίζεται παντού στο Internet. Με την ίδια λογική, η NAT μεταφράζει τη διεύθυνση προορισμού σε μια ιδιωτική διεύθυνση που χρησιμοποιείται τοπικά.

Η NAT περιλαμβάνει τέσσερις τύπους διευθύνσεων:

- Εσωτερικές τοπικές διευθύνσεις.
- Εσωτερικές παγκόσμιες διευθύνσεις.
- Εξωτερικές τοπικές διευθύνσεις.
- Εξωτερικές παγκόσμιες διευθύνσεις

Η NAT έχει πολλά οφέλη, ωστόσο όμως έχει και αρκετά μειονεκτήματα. Από τα πλεονεκτήματα της NAT είναι ότι:

- Διατηρεί το νόμιμα κατοχυρωμένο σύστημα διευθύνσεων επιτρέποντας την ιδιωτικότητα των intranets. Με την NAT σε υπερφόρτωση (NAT overload), οι εσωτερικοί δέκτες μπορούν να μοιραστούν μια ενιαία δημόσια διεύθυνση IPv4 για όλες τις εξωτερικές επικοινωνίες. Σε αυτού του είδους το σχηματισμό, πολύ λίγες εξωτερικές διευθύνσεις είναι απαραίτητες για να υποστηρίξουν πολλούς εσωτερικούς δέκτες.
- Αυξάνει την ευελιξία των συνδέσεων με το δημόσιο δίκτυο.
- Παρέχει συνεκτικότητα για τα συστήματα εσωτερικού δικτύου διεύθυνσης.
- Παρέχει ασφάλεια στο δίκτυο. Τα ιδιωτικά δίκτυα παραμένουν αρκετά ασφαλή, όταν χρησιμοποιούνται σε συνδυασμό με τη NAT για να αποκτήσουν ελεγχόμενη εξωτερική πρόσβαση. Ωστόσο, η NAT δεν αντικαθιστά τα τείχη προστασίας (firewalls).

Μερικά μειονεκτήματα της NAT είναι ότι:

- Η χρήση NAT συνδέεται με την απόδοση του δικτύου, ιδιαίτερα για πρωτόκολλα σε πραγματικό χρόνο, όπως το VoIP. Η NAT αυξάνει τις καθυστερήσεις των μεταγωγέων, επειδή η μετάφραση της κάθε διεύθυνσης εντός των πακέτων κεφαλίδων απαιτεί χρόνο. Το πρώτο πακέτο είναι η διαδικασία μεταγωγής, πηγαίνει πάντα από το πιο αργό μονοπάτι. Ο δρομολογητής πρέπει να εξετάσει το κάθε πακέτο για να αποφασίσει αν χρειάζεται μετάφραση. Ο δρομολογητής πρέπει να αλλάξει την επικεφαλίδα του IP, και, ενδεχομένως να τροποποιήσει τις επικεφαλίδες των TCP ή UDP. Η επικεφαλίδα IP ολοκληρωτικού

ελέγχου πακέτου (checksum), μαζί με τον ολοκληρωτικό έλεγχο TCP ή UDP πρέπει να υπολογίζονται εκ νέου κάθε φορά που γίνεται μετάφραση. Τα εναπομείναντα πακέτα περνούν από μια σύντομη διαδρομή μεταγωγέα εάν υπάρχει καταχώρηση μνήμης cache, αλλιώς και αυτά επίσης καθυστερούν.

- Μερικές εφαρμογές δεν λειτουργούν με NAT. Για παράδειγμα, κάποιες εφαρμογές ασφαλείας, όπως οι ψηφιακές υπογραφές, αποτυγχάνουν επειδή η πηγή της διεύθυνσης IP αλλάζει προτού φτάσει στον προορισμό. Μερικές φορές το πρόβλημα αυτό μπορεί να αποφευχθεί με την εφαρμογή καθορισμών στατικής NAT.

1.11 Υποδικτύωση και Διευθυνσιοδότηση (Subnetting and Addressing)

Προκειμένου να μπορεί να γίνει ανταλλαγή πακέτων είναι απαραίτητη η εκχώρηση λογικών διευθύνσεων σε όλους τους κόμβους που συμμετέχουν στο διαδίκτυο. Μία διεύθυνση δικτύου αποτελεί την ταυτότητα ενός κόμβου στο διαδίκτυο. Με βάση την διεύθυνση προορισμού στα πακέτα, κάθε συσκευή αναγνωρίζει τον προορισμό παράδοσης των πακέτων.

Το πρόβλημα της επάρκειας των διευθύνσεων το λύνουν τα υποδίκτυα και επιτρέπουν αποτελεσματικότερη διαχείριση. Κάθε δίκτυο διαμοιράζεται σε μικρότερα δίκτυα που καλούνται υποδίκτυα. Έστω μια εταιρία διαθέτει 5 ανεξάρτητα τοπικά δίκτυα με δυναμική 25 κόμβων στο κάθε ένα. Θα χρειαστεί να δεσμεύσει 5 διαφορετικές διευθύνσεις. Με την υποδικτύωση θα δεσμεύσει μόνο μία και θα διαμοιράσει τις 256 διευθύνσεις σε υποδίκτυα των 32 διευθύνσεων και για τα 5 τμήματά της. Με λίγα λόγια, μοιράζεται ο αριθμός κόμβου μίας τυπικής διεύθυνσης IP σε δύο τμήματα: στον αριθμό υποδικτύου και στον αριθμό κόμβου.

Η διευθυνσιοδότηση στα δίκτυα IP μετατρέπεται τώρα από ιεραρχική δύο επιπέδων σε ιεραρχική τριών επιπέδων. Το πλήθος των bits που χρησιμοποιούνται για τον ορισμό του αριθμού υποδικτύου δηλώνονται στην μάσκα υποδικτύου (subnet mask).

1.12 Μάσκα Υποδικτύου

Για τον καθορισμό με ακρίβεια bit των τμημάτων δικτύου και υπολογιστή, σε μία διεύθυνση IP χρησιμοποιείται η μάσκα υποδικτύου μεγέθους 4 byte που χωρίζονται μέσω μίας τελείας και παριστάνονται σε δεκαδική μορφή. Με αυτό τον τρόπο όπου τα ψηφία της μάσκας υποδικτύου έχουν τιμή 1, τα αντίστοιχα ψηφία της διεύθυνσης IP ανήκουν στο τμήμα δικτύου. Μία μάσκα 255.255.255.0 για συντομογραφία μπορεί να γραφτεί ως /24. Σύμφωνα με την διεύθυνση IP και τη μάσκα υποδικτύου, μπορεί να βρεθεί το δίκτυο που ανήκει η συγκεκριμένη διεύθυνση IP εκτελώντας τη λογική πράξη AND. Από το ακόλουθο σχήμα εφαρμόζοντας τη πράξη AND μεταξύ της μάσκας 255.255.0.0 και της IP διεύθυνσης 192.0.0.1 προκύπτει το δίκτυο 192.0.0.0 που ανήκει η συγκεκριμένη IP. [15]

1.13 Υποδικτύωση & VLSM

Η αντιμετώπιση του προβλήματος της σπατάλης των διευθύνσεων IP αποτελεί το βασικό σκοπό της υποδικτύωσης. Ένα δίκτυο μπορεί να χωριστεί σε μικρότερα υποδίκτυα με την διαδικασία δανεισμού bit από το τμήμα του υπολογιστή. Για κάθε ψηφίο που δανειζόμαστε διπλασιάζουμε τον αριθμό των υποδικτύων μειώνοντας παράλληλα τον αριθμό των υπολογιστών που μπορούν να κατανεμηθούν σε κάθε υποδίκτυο. Ο τύπος υπολογισμού των υποδικτύων είναι 2n , όπου n ο αριθμός των bit δανεισμού. Η μάσκα υποδικτύωσης μεταβλητού μήκους (Variable Length Subnet Mask) σχεδιάστηκε για να μεγιστοποιηθεί η αποδοτικότερη κατανομή IP διευθύνσεων σε δίκτυα. Σύμφωνα με το μηχανισμό αυτό ένα δίκτυο μπορεί να υποδιαιρεθεί σε μικρότερα υποδίκτυα διαφορετικού μεγέθους.

Διαθέτοντας την αρχική διεύθυνση 172.10.0.0 /24 μπορούμε να ορίσουμε ένα παράδειγμα λειτουργίας του μηχανισμού VLSM.

- Υποδίκτυο A: 110 (hosts) άρα 27(host bits) = 128 - 2 = 126 όπου καλύπτει το 110.
- Υποδίκτυο B: 59 (hosts) άρα 26(host bits) = 64 - 2 = 62 όπου καλύπτει το 59.
- Υποδίκτυο C: 2 (hosts) άρα 22(host bits) = 4 - 2 = 2 όπου καλύπτει το 2.

Για το υποδίκτυο A απαιτούνται 7 bit για τους υπολογιστές επομένως θα χρησιμοποιηθεί μάσκα /25 οπότε προκύπτουν τα ακόλουθα:

172. 10. 0. 00000000

255. 255. 255. 10000000

(Πρώτος host) 0000001

(Τελευταίος) 1111110

(Broadcast) 1111111

- Subnet mask: 255.255.255.128
- Network: 172.10.0.0
- Host-range: 172.10.0.1 - 172.10.0.126
- Broadcast: 172.10.0.127

Για το υποδίκτυο B απαιτούνται 6 bit για τους υπολογιστές επομένως θα χρησιμοποιηθεί μάσκα /26 και η διεύθυνση είναι η 172.10.1.128 οπότε προκύπτουν τα ακόλουθα:

172. 10. 0. 10000000

255. 255. 255.11000000

(Πρώτος host) 000001

(Τελευταίος) 111110

(Broadcast) 111111

- Subnet mask: 255.255.255.192
- Network: 172.10.0.128
- Host-range: 172.10.0.129 - 172.10.0.190
- Broadcast: 172.10.0.191

Για το υποδίκτυο C απαιτούνται 2 bit για τους υπολογιστές επομένως θα χρησιμοποιηθεί μάσκα /30 και η διεύθυνση είναι η 172.10.1.192 οπότε προκύπτουν τα ακόλουθα:

172. 10. 0. 11000000

255. 255. 255.11111100

(Πρώτος host) 01

(Τελευταίος) 10

(Broadcast) 11

- Subnet mask: 255.255.255.252
- Network: 172.10.0.192

- Host-range: 172.10.0.193 - 172.10.0.194
- Broadcast: 172.10.0.195

2. Πρωτόκολλα επικοινωνίας και Δρομολόγηση σε Δίκτυα IP

Τα πρωτόκολλα δικτύων, είναι πρότυπα που επιτρέπουν στους υπολογιστές να επικοινωνούν ο ένας με τον άλλον. Καθορίζουν το πώς, οι υπολογιστές πρέπει να προσδιορίσουν ο ένας τον άλλον στο δίκτυο, τη μορφή που πρέπει να λάβουν τα στοιχεία κατά τη διέλευσή τους και πώς πρέπει οι πληροφορίες να αναδιαμορφωθούν μόλις φτάσουν στον τελικό προορισμό τους. Δηλαδή, το πρωτόκολλο είναι το αντίστοιχο ενός σχεδίου κατασκευής συγκεκριμένου έργου που καθοδηγεί την κατασκευή αλλά δεν αποτελεί τμήμα αυτής. Για παράδειγμα ένα δίκτυο TCP/IP ή δίκτυο Ethernet δεν είναι δίκτυο TCP/IP ή δίκτυο Ethernet αλλά δίκτυο που χρησιμοποιεί το πρωτόκολλο TCP/IP ή αντίστοιχα το πρωτόκολλο Ethernet.

Τα πρωτόκολλά έχουν την εξής λειτουργία. Για να πραγματοποιηθεί η τεχνική διαδικασία της αποστολής δεδομένων μέσω ενός δικτύου, πρέπει να σπάσει σε ένας αριθμό συγκεκριμένων συστηματικών βημάτων. Σε κάθε βήμα λαμβάνουν χώρα συγκεκριμένες ενέργειες, οι οποίες δεν μπορούν να εκτελεστούν από άλλα βήματα. Κάθε βήμα έχει τους δικούς του κανόνες και διαδικασίες, δηλαδή το δικό του πρωτόκολλο. Τα παραπάνω βήματα, πρέπει να εκτελεστούν με συγκεκριμένη σειρά, ίδια για κάθε υπολογιστή του δικτύου. Στον αποστολέα-υπολογιστή, κάθε βήμα πρέπει να εκτελεστεί από πάνω προς τα κάτω. Συγκεκριμένα το πρωτόκολλο :

- Σπάει τα δεδομένα σε μικρότερα τμήματα που ονομάζονται πακέτα (packets) τα οποία διαχειρίζονται από τα πρωτόκολλα.
- Εισάγει πληροφορίες διευθυνσιοδότησης στα πακέτα, έτσι ώστε ο παραλήπτης-υπολογιστής στο δίκτυο, να ξέρει ότι τα δεδομένα ανήκουν σ’ αυτόν.
- Προετοιμάζει τα δεδομένα για την αποστολή τους, μέσω της κάρτας δικτύου στο μέσο μεταφοράς. Στον παραλήπτη-υπολογιστή, το πρωτόκολλο διενεργεί τα ίδια βήματα με την αντίστροφη σειρά. Συγκεκριμένα:
- Παίρνει τα δεδομένα από το καλώδιο
- Φέρνει τα δεδομένα στον υπολογιστή μέσω της κάρτας δικτύου.

- «Απογυμνώνει» τα πακέτα από τις πληροφορίες μετάδοσης που προστέθηκαν στον αποστολέα.
- Αντιγράφει τα δεδομένα από τα πακέτα σε μια προσωρινή μνήμη για επανασυναρμολόγηση.
- Δίνει τα συναρμολογημένα δεδομένα στην εφαρμογή σε εύχρηστη μορφή.

2.1 Routing Protocols

Τα πρωτόκολλα δρομολόγησης ορίζουν τον τρόπο επικοινωνίας μεταξύ δρομολογητών, διαδίδοντας πληροφορίες που τους επιτρέπουν να επιλέγουν δρομολόγια μεταξύ κόμβων του δικτύου. Κάθε δρομολογητής έχει γνώση για τα γειτονικά του δίκτυα και στη συνέχεια το πρωτόκολλο δρομολόγησης διαμοιράζει τη γνώση αυτή αρχικά στους άμεσους γείτονες του δρομολογητή και στη συνέχεια στο υπόλοιπο δίκτυο. Οι δρομολογητές έτσι, επεκτείνουν τις γνώσεις τους αναφορικά με την τοπολογία του δικτύου.

Τα πρωτόκολλα δρομολόγησης έχουν τις εξής γενικές ιδιότητες:

- τον τρόπο που είτε επιχειρούν την αποτροπή σχηματισμού βρόχων δρομολογίων είτε επιχειρούν την καταστροφή των βρόχων σε περίπτωση που αν έχουν δημιουργηθεί.
- τον τρόπο με τον οποίο επιλέγουν δρομολόγια χρησιμοποιώντας πληροφορία που διατηρούν αναφορικά με τα κόστη των αλμάτων
- το χρόνο σύγκλισης
- την κλιμάκωση τους

Τα πρωτόκολλα δρομολόγησης αναφέρονται στη βιβλιογραφία και ως δρομολογούμενα πρωτόκολλα (routed protocols) (TCP/IP protocol suites). Είναι γνωστό πως τα πακέτα που παράγει ένας υπολογιστής αποτελούνται από πρωτόκολλα (Δρομολογούμενα). Τα πρωτόκολλα αυτά, με τη σειρά τους, πρέπει να δρομολογηθούν για να φτάσουν στον προορισμό τους. Τον τρόπο με τον οποίον τα πακέτα τελικά φτάνουν τον προορισμό τους ορίζεται από τους αλγορίθμους και τα πρωτόκολλα δρομολόγησης.

Τα πρωτόκολλα δρομολόγησης αποτελούν στην ουσία το λογισμικό που επιτρέπει στους δρομολογητές τη δυναμική μετάδοση και γνώση των δρομολογίων, αλλά και να αποφασίσουν με τη βοήθεια των αλγορίθμων δρομολόγησης ποια είναι τα διαθέσιμα και τα πιο αποδοτικά δρομολόγια προς ένα προορισμό.

Τα πρωτόκολλα δρομολόγησης μπορούν να ταξινομηθούν σε διαφορετικές ομάδες ανάλογα με τα χαρακτηριστικά τους. Ειδικότερα, τα πρωτόκολλα δρομολόγησης μπορούν να ταξινομηθούν σύμφωνα με:

- **Σκοπό** :Πρωτόκολλο Εσωτερικών Πυλών (Interior Gateway Protocol / IGP) ή Πρωτόκολλο Εξωτερικών Πυλών (Exterior Gateway Protocol / EGP).
- **Λειτουργία**: Διανύσματα Αποστάσεων (distance vector protocols), πρωτόκολλο κατάστασης σύνδεσης (link state protocols) ή πρωτόκολλο path-vector / διανύσματος-μονοπατιού.
- **Συμπεριφορά**: Classful ή classless, δηλαδή το αν υποστηρίζουν σχήμα διευθυνσιοδότησης (IP addressing scheme) που να βασίζεται σε κλάσεις διευθύνσεων ή όχι.

2.1.1 Interior Gateway Protocol (IGP):

Είναι πρωτόκολλα εσωτερικής εφαρμογής, τα οποία χρησιμοποιούνται σε εσωτερικά δίκτυα. Τα πρωτόκολλα που ανήκουν σε αυτή την κατηγορία αναζητούν τρόπους για τη μετάβαση ενός πακέτου μεταξύ δρομολογητών ενός δικτύου. Αυτά τα πρωτόκολλα δρομολόγησης είναι δυναμικά και διατηρούν αρχείο των μονοπατιών που έχουν χρησιμοποιήσει για τη μεταφορά δεδομένων από ένα τελικό σύστημα σε ένα άλλο μέσα στο ίδιο δίκτυο ή σε ένα σύνολο δικτύων που αποτελούν ένα αυτόνομο σύστημα.

2.1.1.1 Το πρωτόκολλο RIP

Από τα πιο ευρέως διαδεδομένα πρωτόκολλα IGP, είναι το πρωτόκολλο RIP. Είναι ένα πρωτόκολλο που χρησιμοποιεί τη μέθοδο των διανυσμάτων απόστα-

σης για να διαδίδει πληροφορίες δρομολόγησης μέσα σε ένα αυτόνομο σύστημα. Ο αρχικός σχεδιασμός του ήταν για να παρέχει συνεπείς πληροφορίες δρομολόγησης και προσπελασιμότητας μεταξύ κόμβων στα τοπικά δίκτυα. Επιπλέον, παρέχει τη δυνατότητα εκπομπής φυσικών δικτύων για την γρήγορη ανταλλαγή πληροφοριών δρομολόγησης.

Το RIP στηρίζεται στην τεχνική distance vector, επιτρέποντας σε ένα router να ενημερώνει τους υπόλοιπους router του δικτύου, για το ποια δίκτυα μπορεί να προσπελάσει και σε ποια απόσταση βρίσκονται από αυτόν.

Ο RIP χρησιμοποιεί τον αλγόριθμο Distance Vector Routing για να μπορέσει να εκτελέσει τις εξής λειτουργίες:

- Εκπομπή από κάθε Node σε όλους τους κοντινότερους Nodes.
- Μέτρηση του Path Cost για κάθε Router.
- ΄Υπαρξη μιας σχετικής καθυστέρησης.
- ΄Υπαρξη μεγάλης ποσότητας δεδομένων.

Το Πρωτόκολλο Πληροφοριών Δρομολόγησης υλοποιεί άμεσα τη δρομολόγηση διανύσματος-απόστασης για τοπικά δίκτυα. Οι κόμβοι του δικτύου χωρίζονται σε ενεργούς και παθητικούς. Οι ενεργοί κοινοποιούν τις διαδρομές τους στους υπόλοιπους. Οι παθητικοί δεν κάνουν κοινοποιήσεις αλλά δέχονται RIP μηνύματα τα οποία τα χρησιμοποιούν για ενημέρωση του πίνακα δρομολόγησής τους. Από τα στοιχεία-κόμβους του δικτύου, οι δρομολογητές εκτελούν το πρωτόκολλο σε ενεργητική κατάσταση ενώ οι υπολογιστές υπηρεσίας σε παθητική. Κάθε 30 δευτερόλεπτα οι δρομολογητές εκπέμπουν περιοδικά ένα μήνυμα ενημέρωσης δρομολόγησης. Το μήνυμα αυτό περιλαμβάνει πληροφορίες από την τρέχουσα βάση δεδομένων του δρομολογητή και περιέχει ένα σύνολο ζευγών, όπου κάθε ζεύγος αποτελείται από μια δικτυακή διεύθυνση IP και μια ακέραια απόσταση από το δίκτυο (δίκτυο προορισμού, σχετική απόσταση). Οι αποστάσεις υπολογίζονται από ένα μετρικό σύστημα καταμέτρησης αλμάτων. Σύμφωνα με το σύστημα αυτό, ο δρομολογητής απέχει ένα άλμα από το άμεσα συνδεδεμένο δίκτυο, δύο άλματα από δίκτυο που προσπελαύνεται μέσω έτερου δρομολογητή κ.ο.κ. Τελικά, το πλήθος των αλμάτων κατά μήκος της διαδρομής που συνδέει μια προέλευση με έναν προορισμό αναφέρεται στον αριθμό των δρομολογητών που συναντά στην πορεία του κάποιο πακέτο. [2]

2.1.1.2 Το πρωτόκολλο OSPF (Open Shortest Path First)

Ωστόσο, η χρήση της μεθόδου αυτής δεν έχει πάντα τα καλύτερα δυνατά αποτελέσματα. Όσο τα συστήματα ήταν μικρά το πρωτόκολλο RIP ήταν αρκετά ικανοποιητικό. Όταν όμως τα AS μεγάλωσαν δημιουργήθηκε πρόβλημα μέτρησης προς το άπειρο και από την αργή σύγκλιση. Έτσι, δημιουργήθηκε η ανάγκη για ένα νέο πρωτόκολλο κατάστασης ζεύξεων, το οποίο ονομάστηκε OSPF (Open Shortest Path First).

Το Πρωτόκολλο προτεραιότητας ανοίγματος της συντομότερης διαδρομής (OSPF) είναι ένα δημοφιλές πρωτόκολλο που χρησιμοποιείται για την διάδοση πληροφοριών δρομολόγησης μέσα σε ένα μεμονωμένο αυτόνομο σύστημα[7].

Το OSPF είναι ένα εσωτερικό πρωτόκολλο αρκετά πολυπλοκότερο του RIP, που χρησιμοποιεί την τεχνική Link state ο οποίος πλημμυρίζει την πληροφορία δρομολόγησης μέσα σ' ένα δίκτυο και έχει μικρή σχετικά ποσότητα δεδομένων.

Το νέο πρωτόκολλο εσωτερικών πυλών (IGP) Open Shortest Path First (OSPF) που σχεδιάστηκε προκειμένου να καλύψει τις νέες ανάγκες έχει τα εξής χαρακτηριστικά:

• Δρομολόγηση μέσα σε ένα αυτόνομο σύστημα. Το OSPF είναι ένα πρωτόκολλο εσωτερικών πυλών (IGP), το οποίο χρησιμοποιείται για τη μεταβίβαση πληροφοριών δρομολόγησης μεταξύ δρομολογητών μέσα σε ένα αυτόνομο σύστημα.

• Πλήρης υποστήριξη διευθυνσιοδότησης CIDR και υποδικτύου. Το OSPF συμπεριλαμβάνει μια μάσκα διεύθυνσης των 32 bit μαζί με κάθε διεύθυνση, η οποία επιτρέπει στην διεύθυνση να είναι με κλάσεις (classful), χωρίς κλάσεις (classless), ή με υποδίκτυο.

• Ανταλλαγή μηνυμάτων με πιστοποίηση ταυτότητας. Ένα ζεύγος δρομολογητών που χρησιμοποιούν το πρωτόκολλο OSPF μπορούν να πιστοποιούν την ταυτότητα κάθε μηνύματος, ώστε να εξασφαλίζεται ότι θα γίνονται δεκτά μόνο τα μηνύματα που προέρχονται από έμπιστη πηγή.

• Εισαγόμενα δρομολόγια. Το OSPF επιτρέπει σε ένα δρομολογητή να εισάγει δρομολόγια τα οποία έμαθε με άλλα μέσα (π.χ. από το πρωτόκολλο BGP).

• Αλγόριθμος κατάστασης συνδέσμων. Το OSPF χρησιμοποιεί την δρομολόγηση με κατάσταση συνδέσμων (link-state routing). Οι Link-state αλγόριθμοι κατακλύζουν με πληροφορίες δρομολόγησης όλους τους κόμβους του δικτύου.

Ο κάθε δρομολογητής κατασκευάζει μία εικόνα ολόκληρου του δικτύου μέσα στον πίνακα δρομολόγησης. Έτσι, ο κάθε δρομολογητής στέλνει μόνο το τμήμα του πίνακα δρομολόγησης που περιγράφει την κατάσταση των δικών του συνδέσεων προς άλλα συστήματα. Οι αλγόριθμοι link-state στέλνουν μικρά updates παντού, συγκλίνουν πιο γρήγορα, είναι λιγότερο επιρρεπείς στην δημιουργία βρόχων δρομολόγησης (routing loops) απαιτούν όμως, περισσότερη επεξεργαστική ισχύ και μνήμη.

• Υποστήριξη για δίκτυα πολλαπλής πρόσβασης. Η παραδοσιακή δρομολόγηση με κατάσταση συνδέσμων δεν είναι αποδοτική σε ένα δίκτυο πολλαπλής πρόσβασης, όπως είναι το Ethernet, επειδή όλοι οι δρομολογητές που είναι συνδεδεμένοι στο δίκτυο εκπέμπουν μηνύματα κατάστασης συνδέσμων. Το πρωτόκολλο OSPF βελτιστοποιεί τη μέθοδο, αναθέτοντας σε ένα μόνο δρομολογητή να εκπέμπει στο δίκτυο. [7]

Πλεονεκτήματα αυτής της τεχνικής έναντι της distance vector, είναι η δυνατότητα χρήσης ιεραρχικής τοπολογίας, η γρήγορη ανταπόκριση σε αλλαγές του δικτύου, η χρήση της σε μεγάλα δίκτυα, η εξισορρόπηση του φορτίου μεταξύ εναλλακτικών βέλτιστων διαδρομών κλπ. Για αυτόν τον λόγο είναι πιο ακριβοί στην υλοποίηση και στην υποστήριξη τους, από τους distance-vector. Οι αλγόριθμοι Distance Vector ή αλλιώς Bellman-Ford αλγόριθμοι, καλούν τον κάθε δρομολογητή να στέλνει τμήμα ή όλο τον πίνακα δρομολόγησης (routing table) αλλά μόνο στους γειτονικούς δρομολογητές, καθώς και μεγαλύτερα updates μόνο στους γειτονικούς δρομολογητές, και γνωρίζουν μόνο για τους συγκεκριμένους δρομολογητές.

Κάθε router διατηρεί την τοπολογία του δικτύου σε μια βάση δεδομένων, ενώ όλοι οι routers που συμμετέχουν στο δίκτυο, διατηρούν την ίδια βάση και τρέχουν τον ίδιο αλγόριθμο παράλληλα. Επίσης, κάθε router σχηματίζει ένα δίκτυο με τους συντομότερους δρόμους, θεωρώντας επίκεντρο τον εαυτό του. Το OSPF απαιτεί σε σχέση με το RIP περισσότερη επεξεργαστική ισχύ και περισσότερη διαθέσιμη μνήμη από τους routers του δικτύου.

2.1.2 Exterior Gateway Routing Protocol

Είναι πρωτόκολλα εξωτερικής εφαρμογής, για μεταφορά δεδομένων έξω από ένα τοπικό δίκτυο όπως είναι το Διαδίκτυο. Τα πρωτόκολλα που ανήκουν

σε αυτή την κατηγορία διαχειρίζονται τη δρομολόγηση εκτός του αυτόνομου συστήματος και επιτρέπουν τις μεταβάσεις από ένα τοπικό δίκτυο στο δίκτυο παρόχου του Internet και σε οποιοδήποτε άλλο δίκτυο.

Ένα από τα πιο γνωστά Exterior Gateway Protocols είναι το Border Gateway Protocol (BGP). Οι αρχές του μπορούν να εφαρμοστούν σε όλα τα δίκτυα ανεξαρτήτως οικογένειας πρωτοκόλλων που χρησιμοποιούν το πρωτόκολλο Border Gateway Protocol (BGP) .Οι δρομολογητές διαφορετικών αυτόνομων συστημάτων (AS) ανταλλάσσουν πληροφορία δρομολόγησης και από αυτήν υπολογίζουν τις καλύτερες διαδρομές. Οι βασικές διαδικασίες του πρωτοκόλλου είναι οι εξής:

- Απόκτηση Γειτόνων (Neighbour acquisition).
- Προσβασιμότητα στους γείτονες (Neighbour reachability).
- Προσβασιμότητα σε κάποιο υποδίκτυο (Network reachability).

Η διαδικασία «απόκτησης γειτόνων» έχει να κάνει με τη συμφωνία δύο δρομολογητών που ανήκουν σε διαφορετικά AS, αλλά συνδέονται στο ίδιο υποδίκτυο, ότι θα ανταλλάσσουν πληροφορία δρομολόγησης όποτε αυτό είναι απαραίτητο. Η διαδικασία αυτή είναι απαραίτητη γιατί μπορεί οι δύο δρομολογητές να συνδέονται στο ίδιο υποδίκτυο και να είναι γείτονες αλλά μπορεί ο ένας από αυτούς να είναι φορτωμένος με την δρομολόγηση μέσα στο AS στο οποίο ανήκει, και να μην θέλει να αναλάβει κίνηση πακέτων προερχόμενων από άλλο AS.

Η διαδικασία αυτή του πρωτοκόλλου δεν προβλέπει τον τρόπο που οι δρομολογητές γνωρίζουν τις διευθύνσεις των γειτόνων τους ή πως δύο δρομολογητές αποφασίζουν να ανταλλάξουν πληροφορία δρομολόγησης. Η διαδικασία «προσβασιμότητας στους γείτονες» διατηρεί μια σχέση γειτονικότητας την οποία έχουν συμφωνήσει οι δύο δρομολογητές με την προηγούμενη διαδικασία. Η τελευταία διαδικασία («προσβασιμότητα σε κάποιο υποδίκτυο») σκοπό έχει οι δρομολογητές να διατηρούν πληροφορία για την προσπέλαση των υποδικτύων. Έτσι κάθε δρομολογητής διατηρεί μια βάση δεδομένων με τα υποδίκτυα τα οποία μπορεί να προσπελάσει και την καλύτερη διαδρομή προς αυτά. Όταν συμβαίνει κάποια αλλαγή στη βάση δεδομένων, ο δρομολογητής, στέλνει κατάλληλα μηνύματα σε όλους τους δρομολογητές που υλοποιούν το BGP. Με τον τρόπο αυτό οι BGP δρομολογητές ενημερώνονται για αλλαγές που συμβαίνουν στο δίκτυο και προσαρμόζουν τις καλύτερες διαδρομές στους πίνακές δρομολόγησης τους.

2.2 IPsec Secure Protocol

Το IPsec είναι ένα πρωτόκολλο Επιπέδου 3 το οποίο υποστηρίζει την ασφαλή μετάδοση δεδομένων μέσω ενός IP δικτύου. Το IP Security σχεδιάστηκε ως ένας μηχανισμός για την ασφαλή μετάδοση δεδομένων από άκρο σε άκρο μέσω μιας IP σύνδεσης. Το πρωτόκολλο IPsec καθορίζει δύο βασικές λειτουργίες για τη διασφάλιση της εμπιστευτικότητας που είναι η κρυπτογράφηση των δεδομένων και η ακεραιότητά τους. Τα είδη των επικεφαλίδων στο πρωτόκολλο IPsec είναι τα εξής:

• Authentication Header (AH). Η επικεφαλίδα αυτή αφορά την ταυτοποίηση της προέλευσης του μηνύματος και την ακεραιότητά του χωρίς τη χρήση κρυπτογράφησης.

• Encapsulating Security Payload (ESP). Η επικεφαλίδα αυτή παρέχει ταυτοποίηση και ακεραιότητα δεδομένων με κρυπτογράφηση. Στο πρωτόκολλο IPsec μόνο ο αποστολέας και ο παραλήπτης γνωρίζουν το κλειδί ασφαλείας.

Το IPsec ορίζει επίσης, τη μορφή του πακέτου IP μέσω του IP τούνελ, το οποίο και ονομάζεται IPsec Tunnel Mode. Το IPsec Tunnel Mode χρησιμοποιεί μια μέθοδο διαπραγμάτευσης θεμάτων ασφαλείας για να ενθυλακώσει κρυπτογραφημένα IP πακέτα και να μεταδοθούν μέσω ενός ιδιωτικού ή δημόσιου IP δικτύου.

Τα κρυπτογραφημένα δεδομένα ενθυλακώνονται επιπλέον σε μια IP επικεφαλίδα τύπου απλού κειμένου και αποστέλλεται μέσω του δικτύου στον Εξυπηρετητή του τούνελ (tunnel server). Όταν ο εξυπηρετητής του τούνελ παραλάβει το datagram, το επεξεργάζεται και αφαιρεί την IP επικεφαλίδα απλού κειμένου. Έπειτα, αποκρυπτογραφεί τα περιεχόμενα της για να προκύψει το αρχικό IP πακέτο. Τέλος, το IP πακέτο δρομολογείται κανονικά προς τον προορισμό του στο τελικό δίκτυο.

Τα τούνελ είναι δύο ειδών, τα προαιρετικά και τα υποχρεωτικά. Το προαιρετικό τούνελ εγκαθίσταται ανάμεσα σε ένα σύστημα Πελάτη και ένα σύστημα Εξυπηρετητή στην περίπτωση που το σύστημα Πελάτη βρίσκεται στο ένα άκρο της σύνδεσης και λειτουργεί σαν Πελάτης στο τούνελ. Στην περίπτωση dial up σύνδεσης, ο πελάτης πρέπει να εκκινήσει μια dial up σύνδεση με το δίκτυο, συνδεόμενος συνήθως με έναν ISP για να αποκτήσει πρόσβαση στο Internet

πριν το τούνελ μέσω του Internet δημιουργηθεί. Στην περίπτωση ενός υπολογιστή συνδεδεμένου σε LAN, ο υπολογιστής Πελάτης είναι ήδη συνδεδεμένος με το εταιρικό δίκτυο το οποίο μπορεί να δροσολογήσει τα ενθυλακωμένα πακέτα στον tunnel server του LAN.

Από την άλλη πλευρά, στην περίπτωση του υποχρεωτικού τούνελ, ο υπολογιστής Πελάτης δεν αποτελεί το ένα άκρο της σύνδεσης. Μια άλλη συσκευή αποτελεί το άκρο της σύνδεσης, η οποία λειτουργεί σαν Εξυπηρετητής dial up πρόσβασης (dial up access server) ανάμεσα στον υπολογιστή Πελάτη και τον Εξυπηρετητή του τούνελ (tunnel server). Ο Εξυπηρετητής αυτός είναι γνωστός και ως FEP (Front End Processor) στο πρωτόκολλο PPTP, ή LAC (L2TP Access Concentrator) στο πρωτόκολλο L2TP ή IP Security Gateway στο πρωτόκολλο IPsec. [8]

Το πρωτόκολλο IPsec ελέγχεται από μια πολιτική ασφαλείας σε κάθε υπολογιστή καθώς και μια παραμετροποιημένη σύνδεση ασφαλείας ανάμεσα στον αποστολέα και τον παραλήπτη. Η πολιτική ασφαλείας αποτελείται από ένα σύνολο φίλτρων και δικαιωμάτων ασφαλείας. Ο τρόπος με τον οποίο σχετίζονται οι οντότητες μεταξύ τους χρησιμοποιώντας το IPsec ορίζεται ως Σύνδεση Ασφάλειας (Security Association – SA). Πρόκειται για μια διαπραγμάτευση ανάμεσα στα δύο μέρη που χρησιμοποιούν το IPsec για το τρόπο με τον οποίο θα ασφαλίσουν την επικοινωνία μεταξύ τους. Τα επιμέρους θέματα που ορίζονται από τη Σύνδεση Ασφαλείας είναι τα εξής:

- IP διεύθυνση Προέλευσης και Προορισμού
- Αλγόριθμος Ταυτοποίησης
- Αλγόριθμος Κρυπτογράφησης
- Τρόποι χρήσης και ανταλλαγής κλειδιών

Η Σύνδεση Ασφαλείας παρέχει τον τρόπο με τον οποίο τα δύο μέρη της σύνδεσης χρησιμοποιούν το πρωτόκολλο IPsec. Αφού οριστεί αυτή η Σύνδεση, τότε μπορεί να αρχίσει η μετάδοση δεδομένων εφαρμόζοντας την καθορισμένη ασφάλεια στα πακέτα. Η ασφάλεια μπορεί να διασφαλίσει μόνο την ακεραιότητα των μεταδιδόμενων πληροφοριών ή και να εφαρμόσει επιπλέον κρυπτογράφηση δεδομένων.

2.3 Δρομολόγηση σε δίκτυο IP

Η δρομολόγηση, γενικά, αφορά τη διαδικασία κατά την οποία αντικείμενα δρομολογούνται από κάποια πηγή προέλευσης (αποστολέα) σε κάποια πηγή προορισμού (παραλήπτη) και υλοποιείται σε δίκτυα διαφόρων ειδών (τηλεφωνικό δίκτυο, διαδίκτυο, δίκτυο επικοινωνιών, δίκτυο μεταφορών). Εκτός της διαδικασίας σε δίκτυα επικοινωνιών, αναφέρεται συχνά και στη χρονοδρομολόγηση διεργασιών για τον έλεγχο της CPU (Κεντρική Μονάδα Επεξεργασίας) σε έναν ηλεκτρονικό υπολογιστή.

Η δρομολόγηση στα δίκτυα επικοινωνιών και στα δίκτυα πληροφοριών (διαδίκτυο) είναι η διαδικασία κατά την οποία πακέτα δρομολογούνται από τη μηχανή προέλευσης (αποστολέα) στη μηχανή προορισμού (παραλήπτη). Η διαδικασία αυτή υλοποιείται στο τρίτο επίπεδο (επίπεδο δικτύου) βάσει της ιεραρχικής οργάνωσης των δικτύων σε στοίβα επιπέδων.

Αναλυτικότερα, κατά τη διαδικασία της δρομολόγησης, γίνεται η επιλογή των μονοπατιών σε ένα δίκτυο για τη διαμοίραση της κίνησής του. Στα περισσότερα υποδίκτυα απαιτούνται περισσότερα από ένα άλματα για να φτάσει κάποιο πακέτο στον προορισμό του. Αυτά τα άλματα περιλαμβάνουν ενδιάμεσους κόμβους, τις γνωστές δικτυακές συσκευές routers, gateways, bridges, firewalls, switches. Συνήθως η δρομολόγηση υλοποιείται με τη βοήθεια πινάκων δρομολόγησης που διατηρούν αρχείο διαδρομών για κάθε προορισμό. Η βασική αρχή της δρομολόγησης με χρήση πινάκων δρομολόγησης είναι απλή. Κάθε κόμβος του δικτύου διατηρεί έναν πίνακα με εγγραφές (αποστάσεις) για κάθε άλλο κόμβο. Κάνοντας χρήση των εγγραφών αυτών, μπορεί να αποφασιστεί από ποιά εξερχόμενη πύλη (ακμή) θα πρέπει να σταλεί κάποιο μήνυμα.

Συχνά η δρομολόγηση συγχέεται με την έννοια της γεφύρωσης. Ωστόσο, οι δύο έννοιες διαφέρουν στο ότι, στη δρομολόγηση, οι δομές διευθύνσεων υπονοούν το πόσο κοντά είναι μια παρόμοια διεύθυνση μέσα στο δίκτυο κι έτσι, με τη χρήση των πινάκων δρομολόγησης, μπορεί να αποφασιστεί η διαδρομή προς ένα σύνολο διευθύνσεων. Η δρομολόγηση, ως εκ τούτου, υπερέχει της γεφύρωσης, και έχει γίνει ο βασικός τρόπος εύρεσης της συντομότερης/καλύτερης διαδρομής στο Διαδίκτυο.

Γραφικά, η αναπαράσταση ενός δικτύου και των μονοπατιών δρομολογίων μπορεί να γίνει με τη βοήθεια κατευθυνόμενων και μη γράφων όπου οι κόμβοι

αναπαριστούν τους σταθμούς του δικτύου (υπολογιστές, δικτυακές συσκευές, συστήματα ελεγχόμενα από έναν πάροχο υπηρεσιών Διαδικτύου, ιστοσελίδες κ.ά) και οι ακμές τη ροή του δρομολογίου (φυσικοί σύνδεσμοι, ομότιμες σχέσεις, υπερσύνδεσμοι κ.ά). Η διαδικασία της δρομολόγησης επιτελείται σε κάθε κόμβο-δρομολογητή του δικτύου. Ο δρομολογητής είναι η συσκευή εκείνη που παραλαμβάνει και προωθεί τα πακέτα στα διάφορα υποδίκτυα.

2.4 Στατική Δρομολόγηση

Στη στατική δρομολόγηση ο διαχειριστής του δικτύου ρυθμίζει χειροκίνητα στο δρομολογητή το δρόμο για τα δίκτυα προορισμού. Όταν υπάρξει μια αλλαγή στην τοπολογία του δικτύου θα πρέπει ο διαχειριστής του να ενημερώνει τους πίνακες δρομολόγησης. Εύκολα γίνεται αντιληπτό ότι σε μεγάλα δίκτυα με πολλούς δρομολογητές η διαχείριση των πινάκων δρομολόγησης τους γίνεται πολύ δύσκολη.

Τα πλεονεκτήματα της στατικής δρομολόγησης είναι τα παρακάτω:

- μικρός φόρτος στον επεξεργαστή του δρομολογητή
- δε χρησιμοποιείται μέρος της χωρητικότητας της γραμμής για την ανταλλαγή πληροφοριών δρομολόγησης, όπως γίνεται στη δυναμική δρομολόγηση
- μεγαλύτερη ασφάλεια, διότι μόνο ο διαχειριστής επιτρέπει την πρόσβαση σε συγκεκριμένα δίκτυα.

Τα μειονεκτήματα της στατικής δρομολόγησης είναι τα εξής:

- σε μεγάλα δίκτυα θα πρέπει ο διαχειριστής να έχει πλήρη εικόνα του δικτύου
- αν προστεθεί ένα καινούργιο δίκτυο θα πρέπει ο διαχειριστής να ενημερώσει τους πίνακες δρομολόγησης σε κάθε δρομολογητή του δικτύου η διαχείριση του δικτύου είναι πολύ χρονοβόρα

2.5 Δυναμική Δρομολόγηση

Ένας δρομολογητής με δυναμικά διαμορφωμένους πίνακες δρομολόγησης είναι γνωστός ως δυναμικός δρομολογητής. Η δυναμική δρομολόγηση αποτελείται από πίνακες δρομολόγησης που δημιουργούνται και συντηρούνται αυτόματα μέσω μιας συνεχούς επικοινωνίας μεταξύ δρομολογητών. Αυτή η επικοινωνία διευκολύνεται από ένα πρωτόκολλο δρομολόγησης, μια σειρά από περιοδικά μηνύματα ή μηνύματα κατά παραγγελία που περιέχουν πληροφορίες δρομολόγησης που ανταλλάσσονται μεταξύ δρομολογητών. Εκτός από την αρχική διαμόρφωσή τους, οι δυναμικοί δρομολογητές απαιτούν μικρή συντήρηση και συνεπώς μπορούν να κλιμακωθούν σε μεγαλύτερα δίκτυα.

Η δυναμική δρομολόγηση είναι ανεκτική σε σφάλματα. Οι δυναμικές διαδρομές που έχουν μάθει από άλλους δρομολογητές έχουν πεπερασμένη διάρκεια ζωής. Αν ένας δρομολογητής ή ένας σύνδεσμος πέσει κάτω, οι δρομολογητές αισθάνονται την αλλαγή στην τοπολογία διαδικτύου μέσω της λήξης της διάρκειας ζωής της μαθησιακής διαδρομής στον πίνακα δρομολόγησης. Αυτή η αλλαγή μπορεί στη συνέχεια να μεταδοθεί σε άλλους δρομολογητές έτσι ώστε όλοι οι δρομολογητές στο διαδικτυακό δίκτυο να γνωρίζουν τη νέα τοπολογία διαδικτύου.

Η δυνατότητα κλιμάκωσης και ανάκτησης από εσωτερικά σφάλματα καθιστά τη δυναμική δρομολόγηση την καλύτερη επιλογή για μεσαία, μεγάλα και πολύ μεγάλα δίκτυα.[25]

2.6 Οι αλγόριθμοι δρομολόγησης

Συνήθως, κατά τη μεταγωγή αντικειμένων από μια μηχανή προέλευσης σε μια μηχανή προορισμού, εμφανίζονται διάφορα προβλήματα. Τα πιο συχνά από αυτά είναι η συσσώρευση πακέτων σε κάποιον ενδιάμεσο κόμβο και η αδράνεια σε κάποιον άλλο, το κυκλοφοριακό αδιέξοδο σε κάποιες ακμές του δικτύου κ.ά. Σε αυτά τα προβλήματα προστίθεται και η ανάγκη, δοσμένης μιας τοπολογίας δικτύου με κόμβους, ακμές και ζεύγη αποστολέων-παραληπτών, να οριστεί το πιο φθηνό ή/και το πιο σύντομο δρομολόγιο μεταξύ των αποστολέων και των παραληπτών.

Για την επίλυση αυτού του είδους των προβλημάτων που εμφανίζονται κατά τη δρομολόγηση πακέτων σε ένα δίκτυο, χρησιμοποιούμε αλγορίθμους δρομολόγησης που επιστρέφουν, ανάλογα με τις απαιτήσεις του εκάστοτε προβλήματος, δρομολόγια που επιλύουν, κατά τον καλύτερο τρόπο, το πρόβλημα.

Οι αλγόριθμοι δρομολόγησης (routing algorithms) ανήκουν στο τμήμα του λογισμικού στο επίπεδο δικτύου. Σε κάθε κόμβο του δικτύου υπάρχει ένας δρομολογητής ο οποίος, δεχόμενος κάποιο εισερχόμενο πακέτο, αποφασίζει σε ποια εξερχόμενη ακμή του θα το προωθήσει. Υπάρχουν δύο τρόποι δρομολόγησης συναρτήσει του αν το υποδίκτυο χρησιμοποιεί στο εσωτερικό του αυτοδύναμα πακέτα ή εικονικά κυκλώματα. Στην πρώτη περίπτωση, για κάθε πακέτο που φτάνει σε κάθε δρομολογητή, δημιουργείται μια αποκλειστική απόφαση προώθησής του.

Στην περίπτωση των εικονικών κυκλωμάτων καθορίζεται το δρομολόγιο βάσει του κυκλώματος και έχει ισχύ για όλη τη συνδιάλεξη. Η διαδικασία αυτή είναι αρμοδιότητα των αλγορίθμων δρομολόγησης και είναι γνωστή ως προώθηση. Η δρομολόγηση αυτή καθ’ αυτή αφορά στη δημιουργία και συμπλήρωση των πινάκων δρομολόγησης από τους οποίους ενημερώνονται οι δρομολογητές κατά τη φάση της προώθησης. [16]

2.7 Ιδιότητες Αλγορίθμων Δρομολόγησης

Στη βιβλιογραφία έχουν προταθεί, και κάθε χρόνο προστίθενται, αρκετοί αλγόριθμοι δρομολόγησης που προσπαθούν, ο καθένας από αυτούς, να βελτιώσει κάποιο πρόβλημα. Όσο διαφορετικοί κι αν είναι οι υπάρχοντες αλγόριθμοι, είναι επιθυμητό να χαρακτηρίζονται όλοι από μια σειρά ιδιότητες. Οι ιδιότητες αυτές επιθυμούμε να ισχύουν στους αλγορίθμους δρομολόγησης είτε αυτοί εφαρμόζονται σε υποδίκτυο με αυτόνομα πακέτα είτε σε υποδίκτυο με εικονικά κυκλώματα.

Επιγραμματικά, οι ιδιότητες αυτές είναι οι εξής:

- Ορθότητα (correctness)
- Απλότητα (simplicity)
- Βέλτιστη απόδοση (optimal efficiency)
- Ανθεκτικότητα (robustness)

• Σταθερότητα (stability)

• Δικαιοσύνη (fairness) [24]

Οι ιδιότητες της ορθότητας, της απλότητας και της απόδοσης είναι προφανείς. Γενικά, κάθε αλγόριθμος που δημιουργείται απαιτείται να είναι απλός στη διατύπωσή του και σαφής ώστε να μην επιτρέπει θολά σημεία που θα μπορούσαν να μεταφραστούν με μη ντετερμινιστικό τρόπο. Επιπλέον, θέλουμε ο αλγόριθμός μας να δουλεύει, δηλαδή να φέρει ως αποτέλεσμα τη λύση για την οποία τον σχεδιάσαμε. Τέλος, θέλουμε να είναι και αποδοτικός. Στον ευρύτερο χώρο των αλγορίθμων η αποδοτικότητα ορίζεται ως εξής: Ένας αλγόριθμος είναι αποδοτικός αν έχει πολυωνυμικό χρόνο εκτέλεσης.

Αν και υπάρχουν αρκετοί ορισμοί για την αποδοτικότητα ενός αλγορίθμου, ο προτεινόμενος φέρει το χαρακτηριστικό της απολυτότητας. Βάσει αυτού, προβλήματα για τα οποία δεν υπάρχει γνωστός αλγόριθμος πολυωνυμικού χρόνου, τείνουν να είναι πολύ δύσκολα στην πράξη.

Η ιδιότητα της ανθεκτικότητας αφορά στην ικανότητα του αλγορίθμου να αντιμετωπίζει ενδεχόμενες αποτυχίες στο υλικό και στο λογισμικό (κατάρρευση δρομολογητών, servers, γραμμών, αλλαγή της τοπολογίας του δικτύου) χωρίς να απαιτείται, σε κάθε αποτυχία, ο τερματισμός όλων των εργασιών στους servers και η επανεκκίνηση του δικτύου (re-boost).

Η σταθερότητα είναι η ιδιότητα εκείνη που εγγυάται πως ένας αλγόριθμος δρομολόγησης θα φτάσει σε κατάσταση ισορροπίας (και θα παραμείνει εκεί) σε ένα λογικό χρονικό πλαίσιο. Το λογικό χρονικό πλαίσιο απαιτείται διότι πολλοί αλγόριθμοι λειτουργούν για πολύ μεγάλο διάστημα χωρίς να φτάσουν ποτέ σε κατάσταση ισορροπίας.

Η δικαιοσύνη είναι η ανάγκη της ικανοποίησης όλων των αιτήσεων που φτάνουν σε κάποιο δρομολογητή ελαχιστοποιώντας τη μέση καθυστέρηση ανά πακέτο. Αυτή η ιδιότητα είναι συνήθως σε αντικρουόμενη κατάσταση σε σχέση με την ιδιότητα της βέλτιστης απόδοσης, όπου είναι επιθυμητή η μεγιστοποίηση της συνολικής διαικπεραιωτικής ικανότητας. Ως μέση λύση, στα περισσότερα δίκτυα, επιλέγεται η μείωση του πλήθους των ενδιάμεσων αλμάτων για κάθε πακέτο έτσι ώστε να μειωθεί η καθυστέρηση και η ποσότητα του εύρους ζώνης που καταναλώνεται.

2.8 Δρομολογητές (Routers)

Ο δρομολογητής, όπως ειπώθηκε και παραπάνω, είναι η συσκευή εκείνη που παραλαμβάνει και προωθεί τα πακέτα στα διάφορα υποδίκτυα. Μπορεί να συνδέεται με έναν ή και περισσότερους συνδέσμους που συνδέουν κόμβους-δρομολογητές του ίδιου δικτύου αλλά και κόμβους-δρομολογητές διαφορετικών δικτύων.

Στα τοπικά δίκτυα (δίκτυα μικρής εμβέλειας), για τη σύνδεση των υπολογιστών στο δίκτυο και μεταξύ τους, υπάρχουν κάποιες πολύ σημαντικές δικτυακές συσκευές (κάρτες δικτύου, hubs, switches) που λειτουργούν στο Επίπεδο 2 (επίπεδο συνδέσμου μετάδοσης δεδομένων). Για να μπορούν οι χρήστες αυτού του δικτύου να συνδέονται με το Διαδίκτυο ή με απομακρυσμένες συσκευές, απαιτείται η συσκευή «δρομολογητής» (router).

Οι δρομολογητές μεταφέρουν δεδομένα μεταξύ πολλαπλών δικτύων και λειτουργούν στο Επίπεδο 3 (επίπεδο δικτύου). Η λειτουργία των δρομολογητών στο 3ο επίπεδο σημαίνει πως, ένας δρομολογητής πρέπει να μπορεί να κατανοήσει τα πακέτα δεδομένων για να μπορεί να τα δρομολογήσει στον προορισμό τους.

Οι δρομολογητές είναι βελτιστοποιημένοι υπολογιστές με σκοπό τη διαχείριση πακέτων που πρέπει να μεταφερθούν μεταξύ δικτύων. Υποχρέωσή τους είναι η αποστολή των πακέτων από την πηγή τους (αποστολέα) στον προορισμό τους (παραλήπτη) με το γρηγορότερο δυνατό τρόπο. Μια σημαντική παρατήρηση που πρέπει να τονιστεί είναι πως, ο γρηγορότερος τρόπος δεν ταυτίζεται πάντα με το συντομότερο μονοπάτι που μπορεί να ακολουθήσει ένα πακέτο, αν και αυτή είναι γενικώς η επιθυμία μας.

Σε ένα δίκτυο, τα πακέτα με προορισμό στο ίδιο δίκτυο μεταφέρονται άμεσα από τη μηχανή προέλευσης στην πηγή προορισμού χωρίς ενδιάμεσους σταθμούς. Ωστόσο, αν η διεύθυνση του προορισμού ενός πακέτου είναι εκτός του δικτύου του, η μηχανή προέλευσης στέλνει το πακέτο στο δρομολογητή που είναι γνωστός (για τη μηχανή προέλευσης) ως η default πύλη του δικτύου, και δεν ασχολείται περαιτέρω με το πακέτο. Όταν ο δρομολογητής αυτός λάβει πακέτο που προορίζεται για κάποιον παραλήπτη εκτός του δικτύου, αναζητά έναν

δρομολογητή στο δίκτυο του προορισμού για να προωθήσει το πακέτο. Όταν το βρει, θα προωθήσει το πακέτο στον επόμενο σταθμό (δρομολογητή).

Θα μπορούσαμε να φανταστούμε αυτή τη διαδικασία δρομολόγησης που ακολουθούν οι δρομολογητές σαν τη διαδικασία που ακολουθούν τα ταχυδρομεία για την αποστολή των γραμμάτων μας λαμβάνοντας υπόψη τον προορισμό της επιστολής. Ένα γράμμα με αποστολέα στην Αθήνα και παραλήπτη στο Λονδίνο θα πρέπει να διέλθει μέσα από πολλούς ενδιάμεσους σταθμούς (ταχυδρομεία), όπου το κάθε ένα προωθεί κάθε φορά το γράμμα σε κάποιο ταχυδρομείο πύλη (δρομολογητές πύλες) σε κάθε δίκτυο. Αντίθετα, ένα γράμμα με αποστολέα και παραλήπτη στην Αθήνα θα μπορούσε να δοθεί άμεσα (ο ίδιος ο αποστολέας να το δώσει στον ίδιο τον παραλήπτη), ωστόσο το κόστος θα αυξανόταν σημαντικά αλλά το γράμμα θα ακολουθούσε (λογικά) τη συντομότερη διαδρομή.

Με την ίδια λογική, οι δρομολογητές προωθούν τα πακέτα που φτάνουν σε αυτούς ανάλογα με τους διαθέσιμους δρομολογητές μεταξύ των δικτύων και προσπαθούν να αποφασίσουν (με τη βοήθεια αλγορίθμων δρομολόγησης) τη συντομότερη δυνατή διαδρομή κάθε φορά.

Σε κάθε δρομολογητή υπάρχει αυτό το σύνολο δεδομένων που περιλαμβάνει όλα τα πιθανά δρομολόγια που γνωρίζει ο δρομολογητής και προτεραιότητες για τις προς χρήση συνδέσεις (αφορούν σε κανόνες για τη διαχείριση κίνησης και φυσιολογικής ροής κίνησης). Οι πίνακες δρομολόγησης είναι δυναμικοί, δηλαδή, ανανεώνονται με τη βοήθεια των αλγορίθμων δρομολόγησης και των πρωτοκόλλων δρομολόγησης . Οι δρομολογητές συμβουλεύονται τους πίνακες για να αποφασίσουν αν υπάρχει δρομολόγιο προς ένα συγκεκριμένο προορισμό.

Οι πίνακες δρομολόγησης μπορεί να είναι μικροί και απλοί (πίνακες μερικών γραμμών κώδικα για μικρούς δρομολογητές και μικρά δίκτυα) αλλά μπορεί να είναι και τεράστιου μεγέθους και πολυπλοκότητας (για δρομολογητές που διαχειρίζονται την κίνηση στο Διαδίκτυο). Αυτό έρχεται σε συμφωνία με τους πολλούς διαθέσιμους τύπους δρομολογητών ανάλογα με τις ανάγκες και την εφαρμογή τους. Υπάρχουν οι δρομολογητές που χρησιμοποιούνται καθημερινά σε σπίτια και επιχειρήσεις μικρής εμβέλειας, οι οποίοι ανταλλάσουν απλώς δεδομένα μεταξύ των υπολογιστών και της καλωδίωσης ή DSL modem που παρέχει

το Internet (ISP). Υπάρχουν και πιο εξελιγμένοι δρομολογητές για μεγαλύτερης κλίμακας εφαρμογές και απαιτήσεις.

Η απλή δουλειά ενός δρομολογητή, έχει ένα κόστος. Όταν ένας δρομολογητής προωθεί ένα πακέτο από έναν κόμβο του δικτύου σε έναν άλλο, προσπαθεί να το κάνει με το λιγότερο δυνατό κόστος. Το κόστος αυτό αφορά σε άλματα. Με κάθε προώθηση ενός πακέτου μεταξύ δύο δρομολογητών, ένας μετρητής αλμάτων στο πακέτο αυξάνει κατά ένα. Αν αυτός ο μετρητής φτάσει σε κάποιο προκαθορισμένο ανώτατο όριο πριν φτάσει στον προορισμό του, το πακέτο μπορεί να απορριφθεί ως μη παραδομένο. Το ανώτατο όριο ορίζεται από τα πρωτόκολλα δρομολόγησης και ποικίλει σε κάθε περίπτωση.

Ωστόσο, για τους δρομολογητές, το κόστος δεν αποτελεί μια απόλυτη παράμετρο, διότι, σε κάποιες περιπτώσεις, δεν είναι τόσο περισσότερο “ακριβό” να επιλέξει τη μεγαλύτερη διαδρομή μεταξύ αποστολέα και προορισμού (όπως στο Διαδίκτυο). Αυτό συμβαίνει για μια σειρά από λόγους, όπως:

- Τα δεδομένα κινούνται με την ταχύτητα του φωτός (ή πολύ κοντά σε αυτή την ταχύτητα), έτσι, κάποια επιπλέον απόσταση δεν κάνει διαφορά.
- Το Διαδίκτυο έχει σχεδιαστεί έτσι ώστε να είναι πλεονάζον. Αν ο πρώτος δρομολογητής καταρρεύσει, επιλέγεται ο δεύτερος, ο τρίτος κ.ο.κ.

Ο σχεδιασμός του Διαδικτύου είναι σταθερός γιατί επαναδρομολογεί πακέτα συνεχώς λόγω διαφόρων γεγονότων (φυσικές καταστροφές, πτώσεις τάσεις κτλ.)

Όσον αφορά στην ασφάλεια, οι δρομολογητές αποτελούν τις συσκευές εκείνες που μπορούν να προστατεύσουν ένα δίκτυο. Τα δίκτυα με πολύ κίνηση είναι πιθανοί στόχοι εισβολέων, χάκερς, ιών κτλ. Στη σύγχρονη εποχή, οι δρομολογητές διαθέτουν μια σειρά από χαρακτηριστικά, όπως ενσωματωμένους firewalls, ανιχνευτές εισβολέων, πιστοποίηση, κρυπτογράφηση κ.ά που έχουν ως σκοπό την προστασία του δικτύου από κακόβουλα στοιχεία. [10]

2.9 Μετρικές

Εκτός των επιθυμητών ιδιοτήτων/χαρακτηριστικών που αναζητούμε στους αλγόριθμους που σχεδιάζουμε για τη διαδικασία της δρομολόγησης πακέτων σε δίκτυα, υπάρχουν κάποιες μετρικές βάσει των οποίων ο κάθε αλγόριθμος

δρομολόγησης υπολογίζει το βέλτιστο μονοπάτι για την πορεία που θα πρέπει να ακολουθήσει το εκάστοτε πακέτο ή όλα τα πακέτα σε μια συνδιάλεξη. Συγκεκριμένα, κάποια μετρική αποτελεί χαρακτηριστικό του πρωτοκόλλου δρομολόγησης και η τιμή της χρησιμοποιείται για την απόφαση του καλύτερου μονοπατιού.

Οι μετρικές που έχουν χρησιμοποιηθεί είναι η μέτρηση της χρήσης των συνδέσμων, το πλήθος των ενδιάμεσων αλμάτων, η ταχύτητα του μονοπατιού, το μήκος του, η απώλεια πακέτων, η καθυστέρηση, η αξιοπιστία του μονοπατιού, το εύρος του μονοπατιού, ο ρυθμός διεκπαιρεωτικής ικανότητας, το μέγεθος της ουράς και το κόστος. Αυτές οι μετρικές, στον αλγόριθμο δρομολόγησης που χρησιμοποιούνται, θεωρούνται, με μια αφηρημένη έννοια, ως κόστος. Ωστόσο, αυτή η έννοια του κόστους διαφέρει από τη μετρική “κόστος“ που αφορά στο κόστος της επικοινωνίας. [6]

Από τις παραπάνω μετρικές, οι πιο συχνά χρησιμοποιούμενες είναι οι εξής :

- ***το μήκος του μονοπατιού (path’s length),*** αφορά στο συνολικό μήκος του μονοπατιού που διασχίζει ένα πακέτο από την πηγή προέλευσής του έως τη μηχανή προορισμού. Μερικοί αλγόριθμοι δρομολόγησης ταυτίζουν τη μετρική αυτή με τη μετρική που βασίζεται στο πλήθος των ενδιάμεσων αλμάτων.
- ***η απώλεια πακέτων (packet loss),*** πιο συχνά αναφερόμενη ως ποσοστό απώλειας πακέτων (Packet Loss Ratio). Αυτή η μετρική αποτελεί σημαντική παράμετρο καθώς, ένα υψηλό ποσοστό απώλειας μειώνει την ποιότητα της επικοινωνίας σε αναξιόπιστα δίκτυα (ειδικά σε εφαρμογές πολυμέσων και συνδιαλέξεων πραγματικού χρόνου (π.χ. VoIP) ενώ στα αξιόπιστα, αυξάνει τις αναμεταδόσεις, καθυστερεί την επικοινωνία, μειώνει το διαθέσιμο εύρος κ.ά.
- ***η καθυστέρηση (delay),*** αφορά στο χρόνο που απαιτείται για ένα πακέτο που στέλνεται από κάποια πηγή να φτάσει στον προορισμό του. Σε αυτό το χρόνο εμπεριέχονται και άλλοι χρόνοι, όπως, ο χρόνος που απαιτείται για την κωδικοποίηση της μετάδοσης του πακέτου, ο χρόνος μετάδοσής του, ο χρόνος που απαιτείται για τα δεδομένα να διασχίσουν το μονοπάτι, και ο χρόνος λήψης και αποκωδικοποίησης των δεδομένων. Στις πραγματικές εφαρμογές, η καθυστέρηση περιέχει και επιπρόσθετο χρονικό κόστος που αφορά στην κίνηση που συναντά το πακέτο στη διαδρομή του.

- ***το μέγεθος της ουράς (queue length),*** που αφορά στον αποθηκευτικό χώρο όπου εισερχόμενα πακέτα παραμένουν μέχρι να προωθηθούν σε κάποιο εξερχόμενο σύνδεσμο. Αν η ουρά είναι γεμάτη, τότε πακέτα που φτάνουν δεν μπορούν να αποθηκευτούν και χάνονται (packet loss). Αν η ουρά είναι άδεια τότε ο δρομολογητής μπορεί να ικανοποιήσει μεγαλύτερα ποσά κίνησης (throughput).
- ***το εύρος του μονοπατιού (path bandwidth),*** που αφορά στο μέγεθος των δεδομένων που μπορούν να διέλθουν από ένα σημείο του μονοπατιού σε ένα άλλο σε μια δεδομένη χρονική περίοδο. Με άλλα λόγια, το εύρος μετράει τα διαθέσιμα ή καταναλισκόμενα αποθέματα δεδομένων και εκφράζεται σε bits/second ή πολλαπλάσια. Στους αλγορίθμους δρομολόγησης το εύρος χρησιμοποιείται για να αποφασίσουν ποιός τύπος σύνδεσης είναι προτιμότερος (π.χ.GigabitEthernet, FastEthernet). Μια σημαντική παρατήρηση είναι πως, οι εντολές για το εύρος δεν επηρεάζουν τη χωρητικότητα του φυσικού μέσου.
- ***το κόστος (cost)***, όπου εδώ αναφέρεται ως το επικοινωνιακό κόστος και αφορά στο χρηματικό κόστος της χρήσης των συνδέσεων του δικτύου. Η μετρική αυτή είναι αρκετά σημαντική στις περιπτώσεις που στο δίκτυο εμπλέκονται ιδιωτικά υποδίκτυα με επαυξημένη ή επιπλέον χρέωση χρήσης των συνδέσεών τους ή σε περιπτώσεις χρονοχρέωσης. [17]

Οι μετρικές δρομολόγησης μπορεί να υπολογίζονται αθροιστικά, κατ' ελάχιστον ή πολλαπλασιαστικά. Στις περισσότερες περιπτώσεις ισχύει ο αθροιστικός υπολογισμός, όπου, το συνολικό κόστος της διαδρομής είναι το άθροισμα των κοστών κάθε ενός συνδέσμου σε όλο το μονοπάτι. [9]

Στον ελάχιστο υπολογισμό (concave) το συνολικό κόστος του μονοπατιού είναι το ελάχιστο από τα κόστη του κάθε συνδέσμου του μονοπατιού, ενώ στον πολλαπλασιαστικό, το συνολικό κόστος είναι το γινόμενο των κοστών κάθε συνδέσμου του μονοπατιού.

2.10 Κατηγοριοποίηση αλγορίθμων δρομολόγησης

Οι αλγόριθμοι δρομολόγησης, για ευκολία μελέτης τους, μπορούν να κατηγοριοποιηθούν σε διάφορες ομάδες βάσει κάποιων διακριτικών χαρακτηριστικών τους. Η βασική ομαδοποίηση χωρίζει το σύνολο των αλγορίθμων δρομολόγησης σε δύο ομάδες, τους προσαρμοστικούς και τους μη προσαρμοστικούς αλγορίθμους (adaptive και non-adaptive). Οι προσαρμοστικοί αλγόριθμοι δρομολόγησης συχνά συναντούνται και ως δυναμικοί αλγόριθμοι ενώ οι μη προσαρμοστικοί ως στατικοί (dynamic και static). Μια δεύτερη βασική κατηγοριοποίηση χωρίζει τους αλγορίθμους σε γενικούς και σε αποκεντρικοποιημένους (global και decentralized). Μια ενδιαφέρουσα κατηγοριοποίηση αφορά σε αλγορίθμους κατάστασης συνδέσμων και σε αλγορίθμους διανύσματος απόστασης.

2.11 Στατικοί και δυναμικοί αλγόριθμοι δρομολόγησης

Η κατηγοριοποίηση των αλγορίθμων δρομολόγησης σε στατικούς (μη προσαρμοστικούς) και σε δυναμικούς (προσαρμοστικούς) βασίζεται στην αλλαγή του δρομολογίου για ένα δεδομένο δίκτυο. Στους στατικούς αλγορίθμους, οι αποφάσεις δρομολόγησης δε βασίζονται στην τρέχουσα τοπολογία ή στην τρέχουσα κίνηση του δικτύου. Με άλλα λόγια, δε λαμβάνουν υπόψιν κάποια από τις μετρικές που αναφέρθηκαν προηγούμενα. Αυτό που συμβαίνει είναι ο σχεδιασμός ενός δρομολογίου εξ' αρχής και η εφαρμογή του στους δρομολογητές κατά την εκκίνηση του δικτύου. Συνήθως, ένα συγκεκριμένο δρομολόγιο ορίζεται για κάποιο αρκετά μεγάλο διάστημα και για ένα συγκεκριμένο δίκτυο και για αυτό η στατική δρομολόγηση θεωρείται ως η αργή αλλαγή δρομολογίων σε κάποιο δίκτυο.

Στους δυναμικούς αλγορίθμους, η αλλαγή του δρομολογίου συμβαίνει με γρήγορους ρυθμούς, συνήθως περιοδικά, λαμβάνοντας υπόψη το κόστος αλλαγής των συνδέσμων και τις αλλαγές στην τοπολογία του δικτύου και στην κίνησή του. Στην πιο ακραία περίπτωση, το δρομολόγιο αλλάζει για κάθε πακέτο που παράγεται από την πηγή προέλευσης.

Οι αλγόριθμοι δυναμικής δρομολόγησης κατηγοριοποιούνται περαιτέρω βάσει του αν λαμβάνουν τις πληροφορίες τους μόνο από τους γειτονικούς δρομολογητές ή από όλους τους δρομολογητές του δικτύου, αν λαμβάνουν απόφαση

για νέα δρομολόγια σε περιοδική βάση ή μόνο αν αλλάζει η τοπολογία ή η κίνηση του δικτύου περισσότερο από ένα ανώτερο κατώφλι που έχει θέσει ο σχεδιαστής, ή, δοθέντων των κοστών κάθε συνδέσμου του δικτύου, οι δρομολογητές μπορούν να ορίζουν διαφορετικό (βέλτιστο) δρομολόγιο για κάθε ζεύγος κόμβων αποστολέων-παραληπτών. [19]

2.12 Γενικοί και αποκεντρικοποιημένοι αλγόριθμοι δρομολόγησης

Η δεύτερη βασική κατηγοριοποίηση που γίνεται στους αλγόριθμους δρομολόγησης χωρίζει τους αλγορίθμους σε γενικούς αλγορίθμους, που βασίζονται στην κατάσταση των συνδέσμων του δικτύου και σε αποκεντρικοποιημένους, που υλοποιούν δρομολόγηση με διανύσματα απόστασης.

Στους γενικούς αλγορίθμους, όλοι οι δρομολογητές γνωρίζουν την πλήρη τοπολογία του δικτύου και μαζεύουν πληροφορίες για τα κόστη των συνδέσεων. Σε αυτή την κατηγορία ανήκει ο διάσημος αλγόριθμος δρομολόγησης του Dijkstra που αναφέρουμε και αναλύουμε παρακάτω.

Στους αποκεντρικοποιημένους αλγορίθμους, οι δρομολογητές έχουν γνώση των δρομολογητών με τους οποίους βρίσκονται σε φυσική γειτνίαση και μαζεύουν πληροφορίες για τα κόστη των συνδέσεων των γειτόνων τους. Επιπλέον, στους αποκεντρικοποιημένους αλγορίθμους δρομολόγησης υλοποιούνται επαναληπτικοί υπολογισμοί και ανταλλαγή πληροφοριών με τους γείτονες.

Στο σημείο αυτό θα πρέπει να τονίσουμε πως το επιθυμητό είναι οι αλγόριθμοι δρομολόγησης που εφαρμόζουμε στην πράξη στα δίκτυά μας να είναι δυναμικοί και αποκεντρικοποιημένοι. [19]

2.13 Ιεραρχική Δρομολόγηση

Η μέχρι στιγμής κατηγοριοποίηση των αλγορίθμων δρομολόγησης σε στατικούς ή δυναμικούς και γενικούς ή αποκεντρικοποιημένους αντιμετωπίζει τα δίκτυα με εξιδανικευμένο τρόπο. Θεωρεί πως όλοι οι δρομολογητές του δικτύου είναι πανομοιότυποι και πως το δίκτυο είναι επίπεδο. Αυτό θα μπορούσε να

εφαρμοστεί στην πράξη σε μικρού εύρους δίκτυα. Ωστόσο, στη σημερινή εποχή και καθώς τα δίκτυα μεγαλώνουν σε μέγεθος, το πλήθος των δρομολογητών αυξάνει εκθετικά. Η εκθετική αύξηση των δρομολογητών επιφέρει μια σημαντική επίπτωση. Δεδομένου ότι οι αλγόριθμοι δρομολογητών διατηρούν πίνακες με εγγραφές για τα μονοπάτια μεταξύ κάθε ζεύγους δρομολογητών του δικτύου, είναι αντιληπτό το μέγεθος του πίνακα στα σημερινά δίκτυα. Εκτός, όμως, της απαίτησης για τεράστια μνήμη, για τον ίδιο λόγο απαιτείται πολλαπλάσιος χρόνος επεξεργασίας για τη σάρωση του πίνακα, περισσότερο εύρος και τελικά, επέρχεται τέλμα στο δίκτυο.

Για τους παραπάνω λόγους απαιτείται η διάρθρωση του δικτύου ιεραρχικά. Από την άποψη πως και το Διαδίκτυο αποτελεί ένα δίκτυο υποδικτύων, οι δρομολογητές του ιεραρχικού δικτύου διαιρούνται σε περιφέρειες. Οι περιφέρειες είναι αυτόνομα συστήματα όπου, κάθε δρομολογητής που υπάρχει σε μια περιφέρεια γνωρίζει μόνο λεπτομέρειες για δρομολόγηση μέσα στην περιφέρειά του. Έτσι, διαφορετικές περιφέρειες του ίδιου δικτύου χρησιμοποιούν διαφορετικούς αλγορίθμους δρομολόγησης. Ένα σημαντικό πλεονέκτημα της ιεραρχικής δρομολόγησης είναι το κέρδος σε χώρο. Το πιο σημαντικό μειονέκτημα είναι πως, τελικά, υπάρχει κόστος και σε αυτή την περίπτωση αλλά με τη μορφή διαδρομών επαυξημένου μήκους. [19]

ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ

3. Μελέτη Περίπτωσης

Το Project το οποίο θα υλοποιήσουμε, περιγράφει μια εταιρεία με 2 Υποκαταστήματα (routers), τα οποία απέχουν αρκετά χιλιόμετρα μεταξύ τους. Σκοπός της εργασίας είναι να επιτευχθεί η σύνδεση των δύο απομακρυσμένων καταστημάτων με τέτοιο τρόπο ώστε ακόμα και αν κάποιος δρομολογητής τεθεί εκτός ή υπάρξει κάποιο «φόρτωμα» σε κάποιο υποδίκτυο, η λειτουργία του δικτύου να μην σταματήσει, αλλά να αναζητήσει την αμέσως πιο σύντομη διαδρομή, αλλά με ασφάλεια ώστε να μην είναι εύκολη μία κακόβουλη εισβολή. Η επικοινωνία των 2 καταστημάτων θα επιτυγχάνεται με την σύνδεση τους στην περιοχή δικτύου κορμού (BackBone Area) , η οποία αποτελεί έναν ξεχωριστό κόμβο , ανάμεσα στα 2 καταστήματα.

Περιοχή Δικτύου Κορμού(Backbone Area)

Η περιοχή του δικτύου κορμού αποτελεί τον πυρήνα των δικτύων OSPF και OSPFv3. Όλες οι περιοχές OSPF και OSPFv3 συνδέονται στην συγκεκριμένη περιοχή (γνωστή και ως περιοχή 0 ή περιοχή 0.0.0.0), η οποία αποτελεί τον πυρήνα των δικτύων OSPF και OSPFv3. Όλες οι άλλες περιοχές συνδέονται με αυτήν και η δρομολόγηση μεταξύ τους, πραγματοποιείται μέσω δρομολογητών συνδεδεμένων στην περιοχή δικτύου κορμού και στις δικές τους συναφείς περιοχές. Είναι υπεύθυνη για τη διανομή πληροφοριών δρομολόγησης στις περιοχές που δεν αποτελούν μέρος του δικτύου κορμού . Η σύνδεση της περιοχής μπορεί να δημιουργηθεί και να διατηρηθεί μέσω της διαμόρφωσης των εικονικών συνδέσεων.

3.1 Προφίλ Εταιρείας

Η εταιρεία για την οποία σχεδιάζουμε το δίκτυο, δραστηριοποιείται στο χώρο των πωλήσεων τα τελευταία πέντε χρόνια με μεγάλη επιτυχία. Η διαρκής ζήτηση προϊόντων και υπηρεσιών από περιοχές της Λακωνίας , σε συν-

δυασμό με το κόστος Αποστολής των προϊόντων αλλά και την αδυναμία άμεσης παροχής υπηρεσιών Service οδήγησε την Εταιρεία στην απόφαση να επεκταθεί και να ανοίξει 2ο κατάστημα στην πόλη της Σπάρτης.

Κάθε κατάστημα, αποτελείται από 4 τμήματα 1) CentralStore, 2) AccountingOffice, 3) ITSupport, 4) Warehouse, είναι χωρισμένο σε υποδίκτυα, και έχει έναν ενδιάμεσο δρομολογητή ο οποίος συνδέεται με τον κεντρικό server (Βρίσκεται στην περιοχή Δικτύου Κορμού) και έτσι, τα 2 καταστήματα μπορούν και επικοινωνούν μεταξύ τους.

3.2 Απαιτήσεις

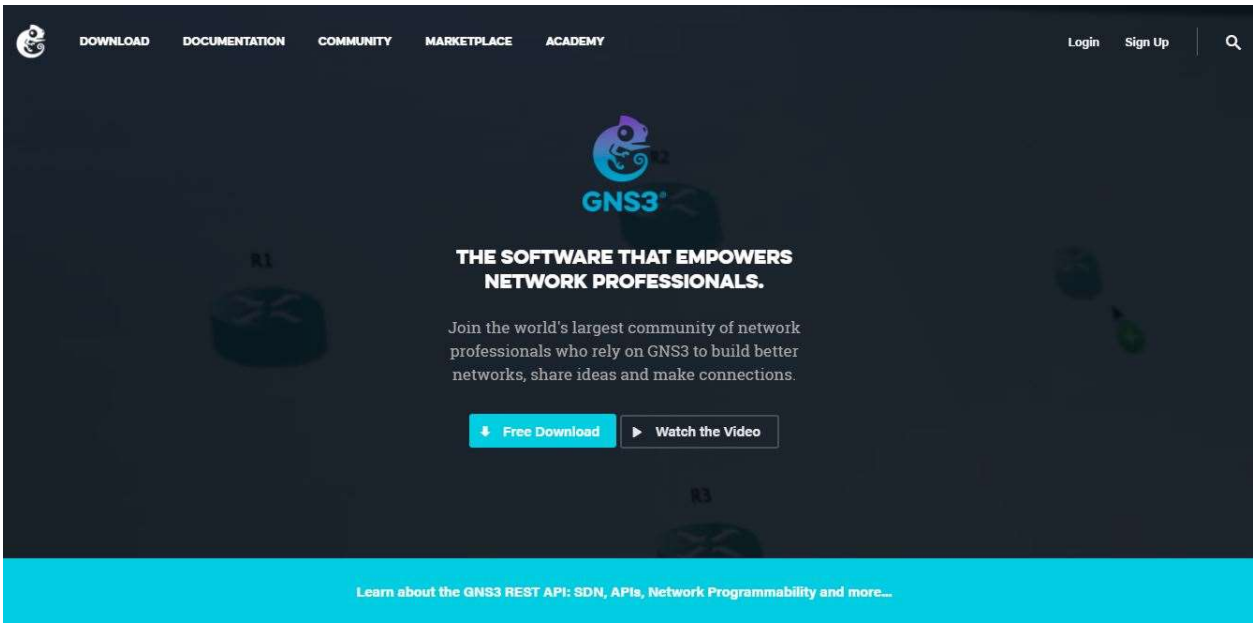
Υπάρχουν καθημερινά κάποιες ώρες που ένα δίκτυο υπερφορτώνεται , με αποτέλεσμα να δημιουργούνται κάποιες καθυστερήσεις (π.χ. στην επικοινωνία δυο περιφερειακών συσκευών), ή ακόμα μέρος του δικτύου να τίθεται εκτός λειτουργίας με αποτέλεσμα, αν δεν επιλυθεί άμεσα το οποιοδήποτε πρόβλημα να υπάρχουν σοβαρές επιπτώσεις για την Εταιρεία στην οποία ανήκει το δίκτυο. Αδιαμφισβήτητα, τα 2 αυτά καταστήματα πρέπει να είναι σε συνεχή επικοινωνία μεταξύ τους ακόμα και αν κάποιο-α τμήματα τεθούν εκτός λειτουργίας. Ακόμα, θα πρέπει να εξασφαλίζεται η προστασία του δικτύου από κάθε είδους ανεπιθύμητων ενεργειών/επιθέσεων που μπορούν να βλάψουν σε μεγάλο βαθμό την εταιρεία. Όσον αφορά το θέμα του εξοπλισμού πρέπει να είναι σύγχρονος και φιλικός στους χρήστες του ώστε να παρέχεται η μέγιστη δυνατή υποστήριξη. Για αυτό τον λόγο, οι δρομολογητές που επιλέχθηκαν είναι Cisco C7200 καθώς υποστηρίζουν μεγάλη ποικιλία εφαρμογών και είναι και αρκετά φιλικό το περιβάλλον τους.

3.3 Εργαλεία

Για την Εκτέλεση του Πρακτικού Μέρους της Πτυχιακής Εργασίας μας είναι απαραίτητη η εγκατάσταση ενός προσομοιωτή Δικτύων ο οποίος θα επιτρέπει την προσομοίωση περίπλοκων δικτύων. Επιλέχθηκε ο προσομοιωτής GNS3 ο οποίος είναι και ο πιο διαδεδομένος για χρήση Cisco Routers .

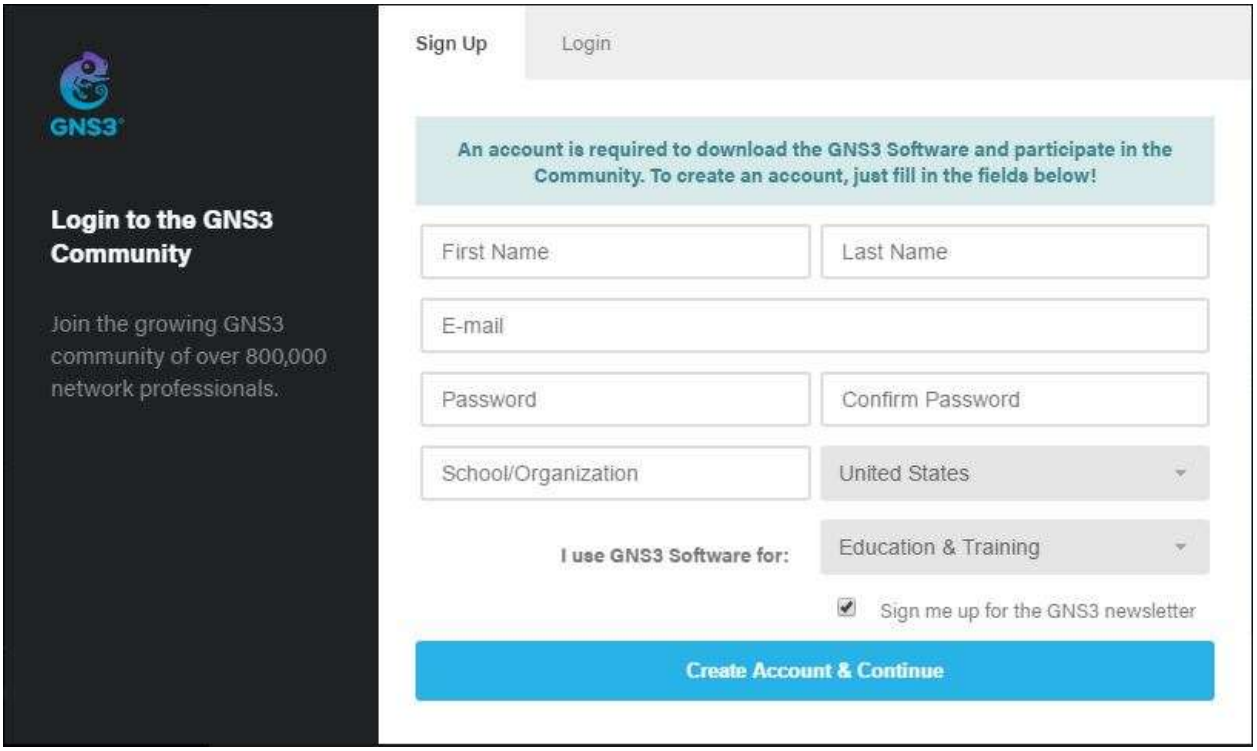
3.3.1 Εγκατάσταση GNS3

Αρχικά, για να κατεβάσουμε το λογισμικό θα πρέπει να συνδεθούμε στον Ιστότοπο https://www.gns3.com/



Εικόνα 4.1:Αρχική Σελίδα της Ιστοσελίδας https://www.gns3.com/

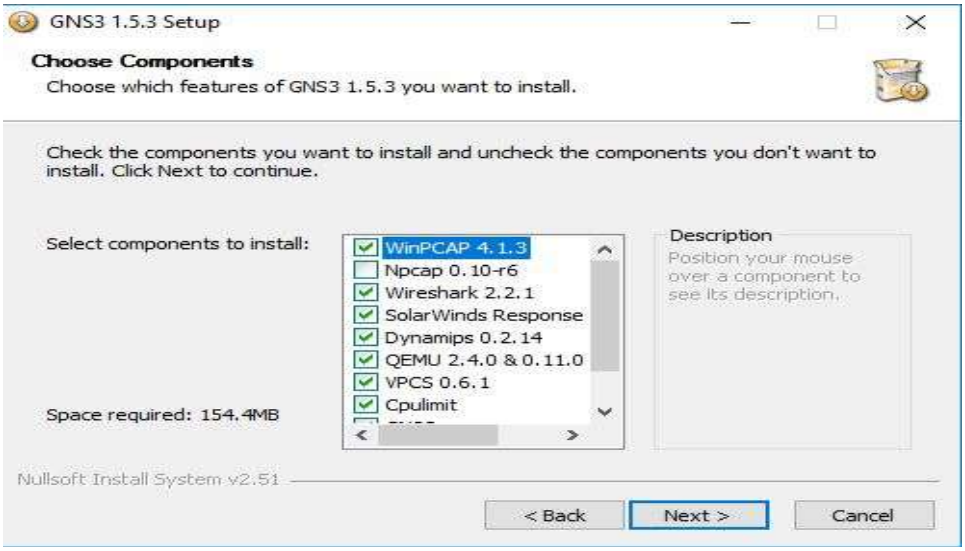
Μόλις πατήσουμε την επιλογή Free Download θα γίνει αυτόματη μετάβαση σε μία σελίδα όπου θα εμφανιστεί μία φόρμα εγγραφής , που θα μας ζητάει κάποια βασικά στοιχεία ώστε να μας επιτρέψει να κατεβάσουμε το πρόγραμμα. Η επιβεβαίωση της δημιουργίας του λογαριασμού θα πραγματοποιηθεί με την αποστολή ενός συνδέσμου στο mail μας.



Εικόνα 4.2: Φόρμα Εγγραφής για την δημιουργία λογαριασμού

Μετά την ολοκλήρωση των διαδικασιών εγγραφής και της λήψης του αρχείου εγκατάστασης του προγράμματος βρίσκουμε τον προορισμό στον οποίο αποθηκεύτηκε και ξεκινάμε την εγκατάσταση του, στον Υπολογιστή μας.

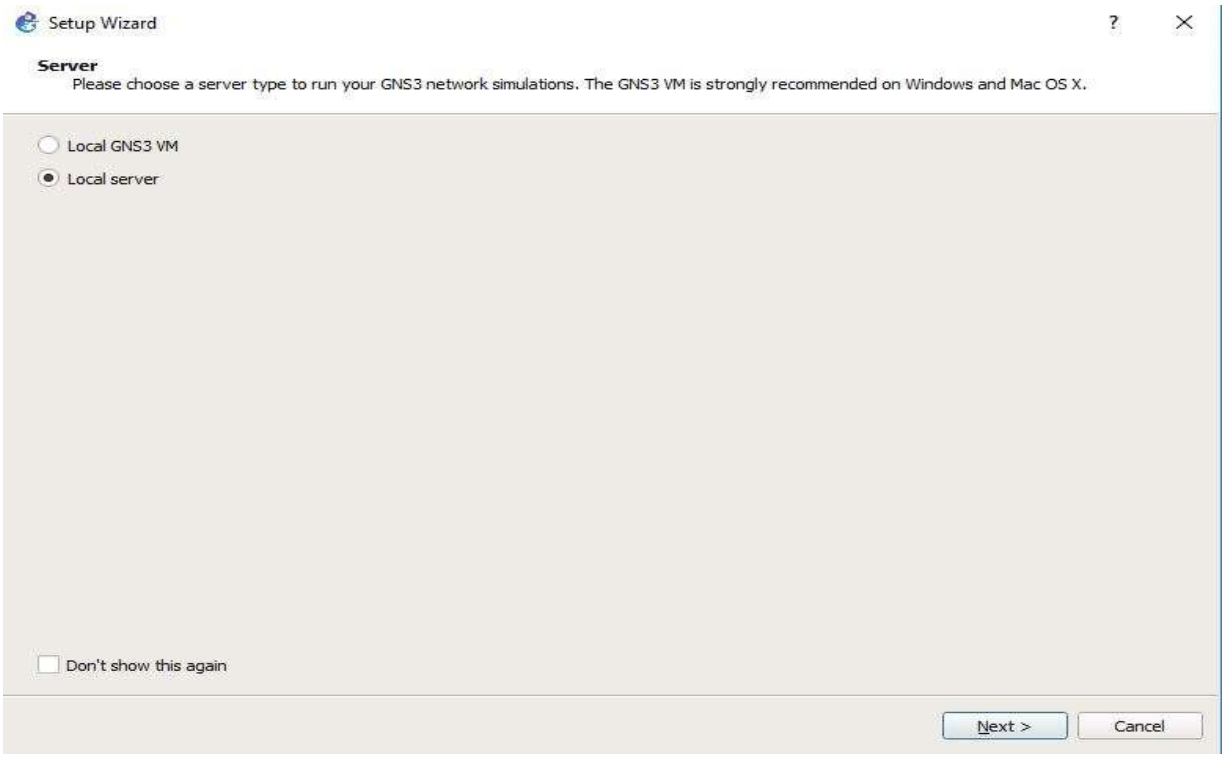
Στο αρχικό στάδιο της εγκατάστασης θα μας ζητηθεί να επιλέξουμε ποια προγράμματα θα εγκατασταθούν μαζί με το GNS3. Ιδιαίτερα θα πρέπει να αναφερθεί η δυνατότητα εγκατάστασης του Wireshark (και του WinPCAP) και, ξεκινώντας από την καινούργια έκδοση του GNS3, και του SolarWinds. Επίσης, πρέπει να επιλέξουμε και την εγκατάσταση του SupperPutty.



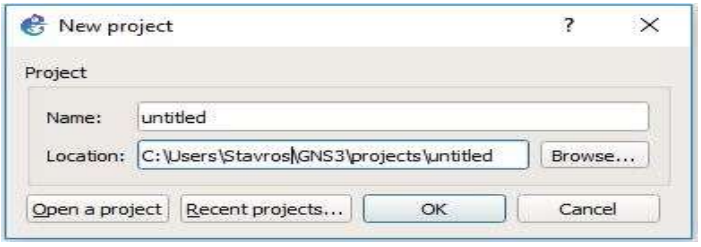
Εικόνα4.3 Παράθυρο επιλογής προγραμμάτων προς εγκατάσταση

Αφού ολοκληρωθεί η εγκατάσταση του GNS3 , θα πρέπει να κατεβάσουμε(εάν ήδη δεν έχουμε) αρχεία εικόνων για Cisco Routers , όπου στην αρχική τους μορφή έχουν .bin format ενώ αποσυμπιέζοντας τες θα δούμε να μετατρέπονται σε .image

Ανοίγοντας το GNS3 το πρώτο πράγμα που θα μας ρωτήσει το είναι τον τύπο του server για να τρέχουμε τις προσομοιώσεις δικτύου(Στο συγκεκριμένο project θα επιλεχθεί να τρέχει σε τοπικό server (Local Server) και αν θέλουμε να δημιουργήσουμε ένα καινούριο project ή να ανοίξουμε ένα υπάρχων.



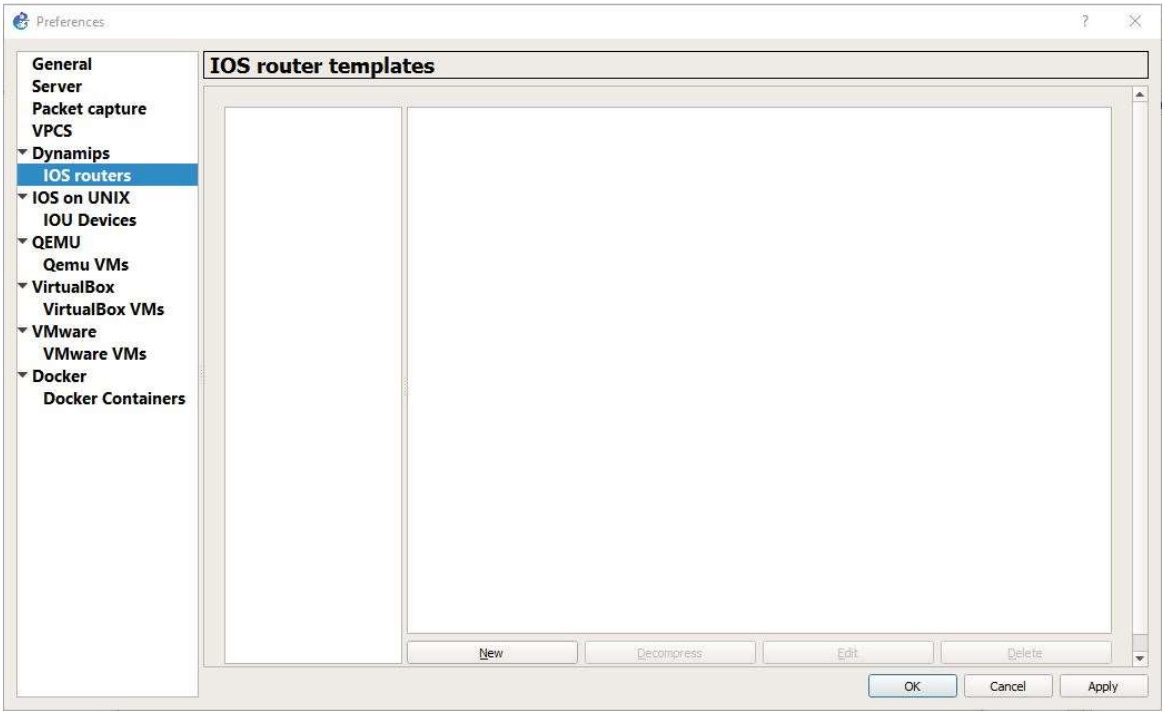
Εικόνα 4.4: Παράθυρο επιλογής τύπου serverγια να τρέξουμε τις προσομοιώσεις μας



Εικόνα 4.5:Παράθυρο Ονομασίας και Προορισμού Αποθήκευσης της Εργασίας

3.3.2 Εγκατάσταση Router

Για να μπορέσουμε να δουλέψουμε στο GNS3 θα πρέπει να παρέχουμε εμείς το αρχείο με το λειτουργικό του router που επιθυμούμε να χρησιμοποιήσουμε. Για να εισάγουμε τώρα τις εικόνες των λειτουργικών πατάμε πάλι επάνω στην καρτέλα ***Edit/Preferences*** και επιλέγουμε **Dynamips** και μετά στην επιλογή **IOS routers** επιλέγουμε το *New* κάτω αριστερά.

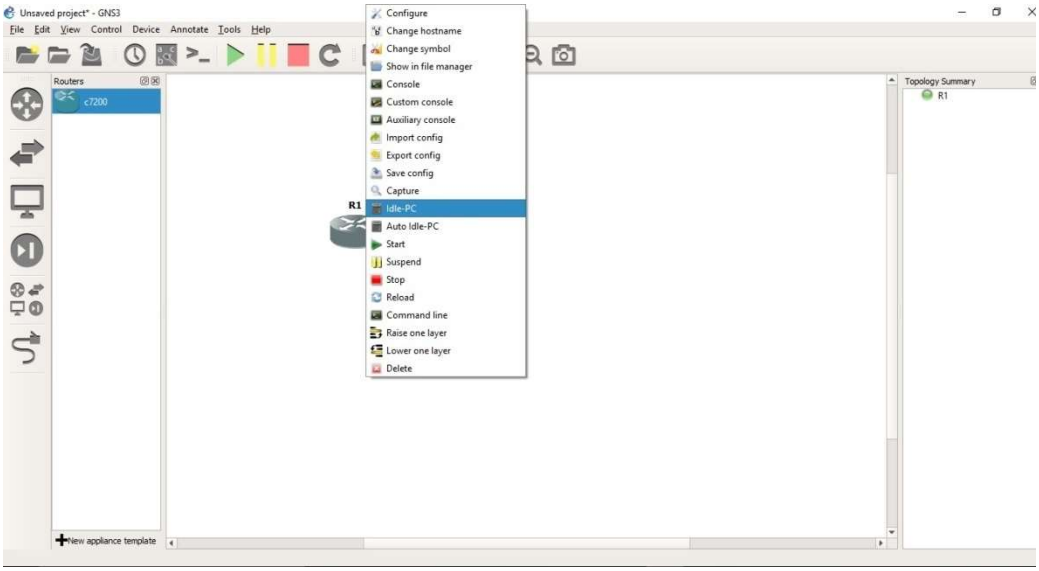


Εικόνα 4.6:Επιλέγουμε IOS routers και "New" για να ξεκινήσει η διαδικασία εγκατάστασης

Κατόπιν επιλέγουμε την τοποθεσία της εικόνας του λειτουργικού που έχουμε προμηθευτεί από την ηλεκτρονική πλατφόρμα του μαθήματος με τη βοήθεια του κουμπιού Browse και πατάμε *Next*. Στη συνέχεια ορίζουμε την αρχική τιμή για τη μνήμη RAM του router και ορίζουμε τα slots με τις κάρτες δικτύου που επιθυμούμε να έχει πάνω του ο router μας.

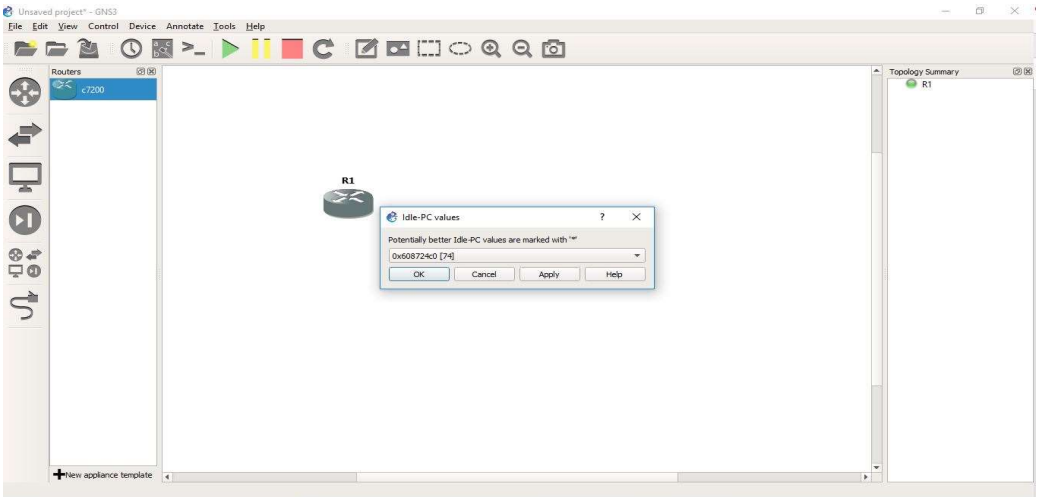
Εικόνα 4.7:Ορισμός slots με τις κάρτες δικτύου που επιθυμούμε

Στην τελευταία φάση της παραμετροποίησης, επιλέγουμε ένα από τα routers που έχουμε αποθηκεύσει την εικόνα του από το αριστερό πλαίσιο και το τοποθετούμε στην κύρια επιφάνεια εργασίας του GNS3. Στη συνέχεια πατώντας το πράσινο κουμπί PLAY από την επιφάνεια του GNS3 ξεκινάμε τη συσκευή. Αν όλα έχουν εκτελεστεί ορθά, στο δεξί πλαίσιο θα εμφανιστεί ένα πράσινο φως δίπλα στο router μας που θα σημαίνει ότι η συσκευή έχει ενεργοποιηθεί. Μία ακόμα ιδιαίτερα σημαντική διαδικασία, πριν ξεκινήσουμε την δημιουργία projects και τοπολογιών είναι να επιλέξουμε τα λεγόμενα Idle-Pc Values στον router μας. Αυτή η ρύθμιση είναι απαραίτητη έτσι ώστε να αποφευχθεί να δουλεύει ο επεξεργαστής μας στο 100%. Για να πραγματοποιήσουμε το βήμα κάνουμε δεξί κλικ πάνω στη συσκευή μας και από το μενού επιλέγουμε Idle PC.

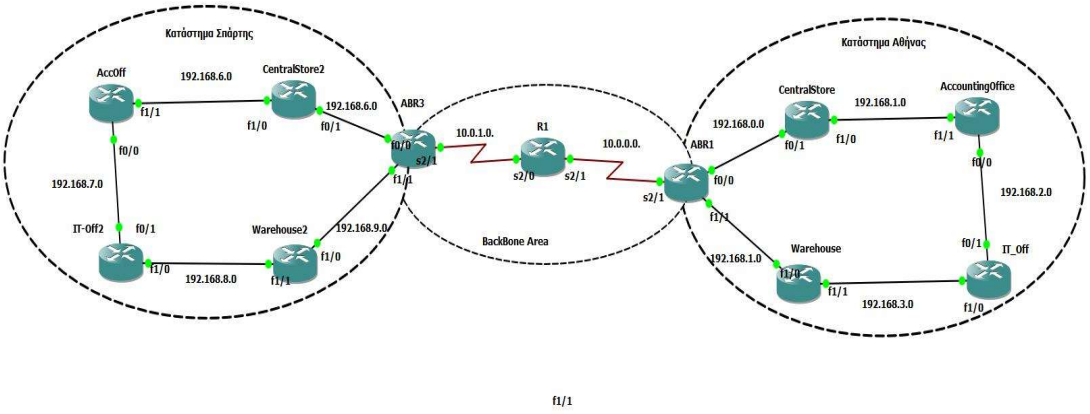


Εικόνα 4.8: Επιλογή Idle-PcValues

Όταν ολοκληρωθεί η διαδικασία θα εμφανιστεί ένα παράθυρο για να επιβεβαιώσουμε τις τιμές όπου και θα πατήσουμε *Apply*.



Εικόνα 4.9: Για να επιβεβαιωσουμε τις τιμές θα πατήσουμε Apply



Εικόνα 4.10: Η τοπολογία της παρούσας εργασίας ολοκληρωμένη

3.4 Υλοποίηση Project

Αφού έχουμε εκτελέσει τα παραπάνω βήματα μπορούμε τώρα να ξεκινήσουμε την υλοποίηση της εργασίας. Θα επιλέξω το router που εγκατέστησα προηγουμένως (Cisco C7200 series) και θα το χρησιμοποιήσω στην τοπολογία μου. Θα διαμορφώσω routers, που θα αντιστοιχούν στα 2 καταστήματα, και θα δρομολογηθούν με χρήση πρωτοκόλλου OSPF.

3.4.1 Hardware για την εκτέλεση του Project

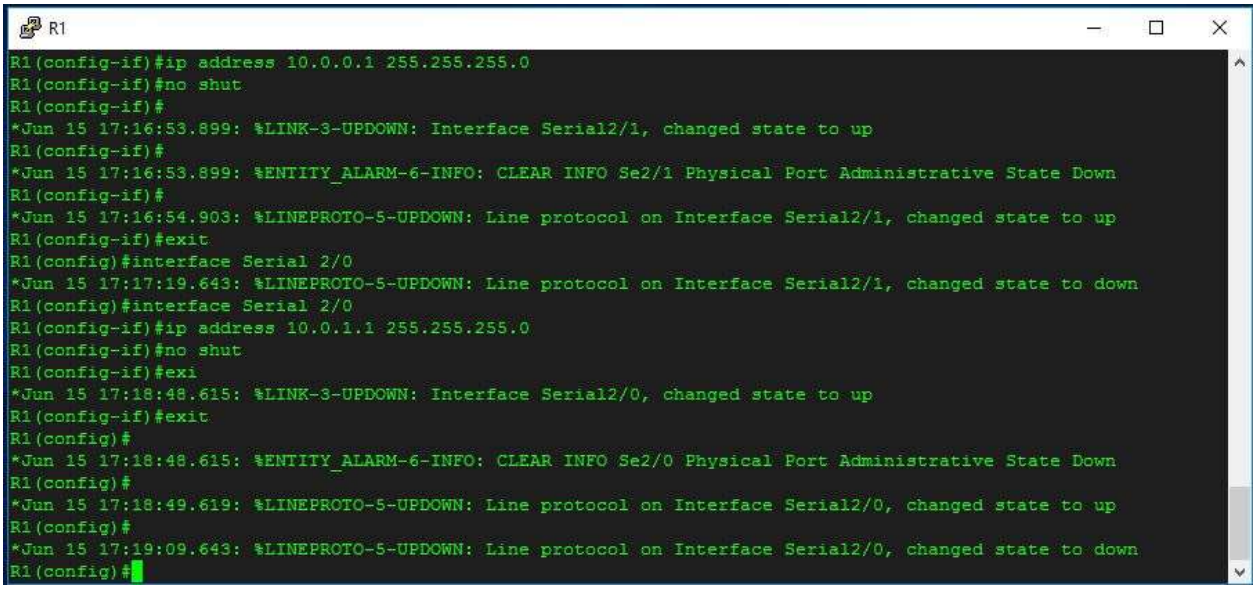
Για τις ανάγκες της εργασίας θα χρησιμοποιήσω 8GB RAM ώστε οι δρομολογητές να λειτουργήσουν αρμονικά χωρίς απρόβλεπτες συνέπειες.HCPU είναι ο τετραπύρηνος Intel Q8200 775 Socket, Σκληρός Δίσκος 500GB SATA 2 3.5’’ και OS Windows 10 Home

3.4.2 Διαμόρφωση Routers-Χρήση Πρωτοκόλλου OSPF

Θα ξεκινήσουμε με την διαμόρφωση 3 routers οι οποίοι θα αποτελούν την περιοχή δικτύου κορμού που είναι υπεύθυνη για την επικοινωνία των 2 απομακρυσμένων δικτύων.

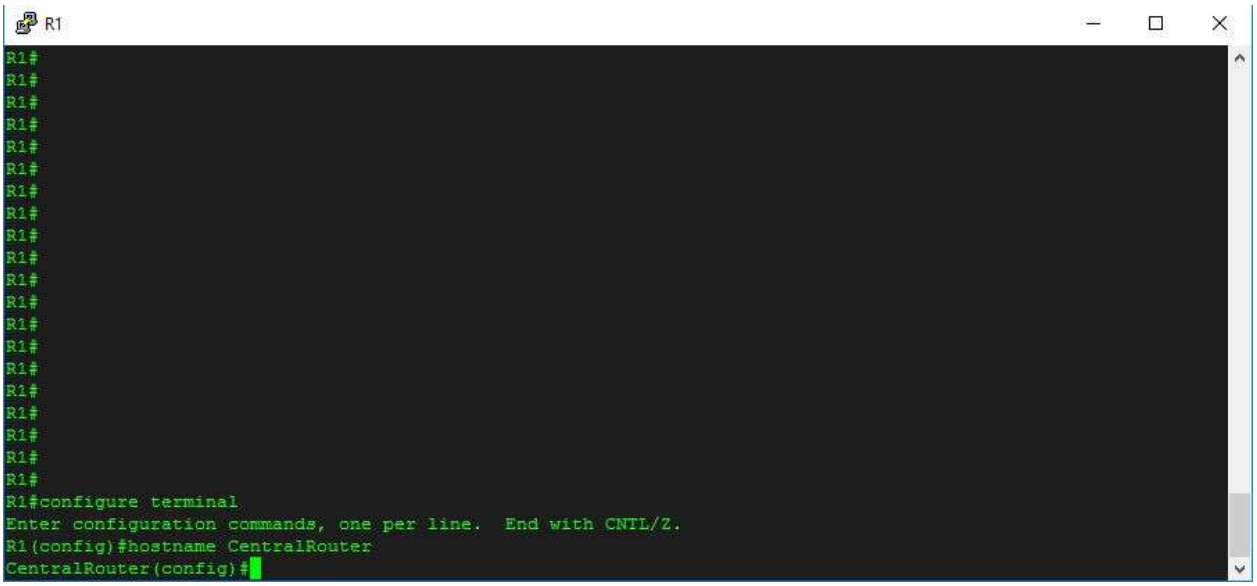
3.4.2.1 Διαμόρφωση R1 δρομολογητή

Θα αποτελέσει τον Κεντρικό Δρομολογητή της Τοπολογίας και της Περιοχής Δικτύου Κορμού. Ξεκινάω με την εκχώρηση IP διευθύνσεων σε 2 διεπαφές του με την χρήση των παρακάτω εντολών:

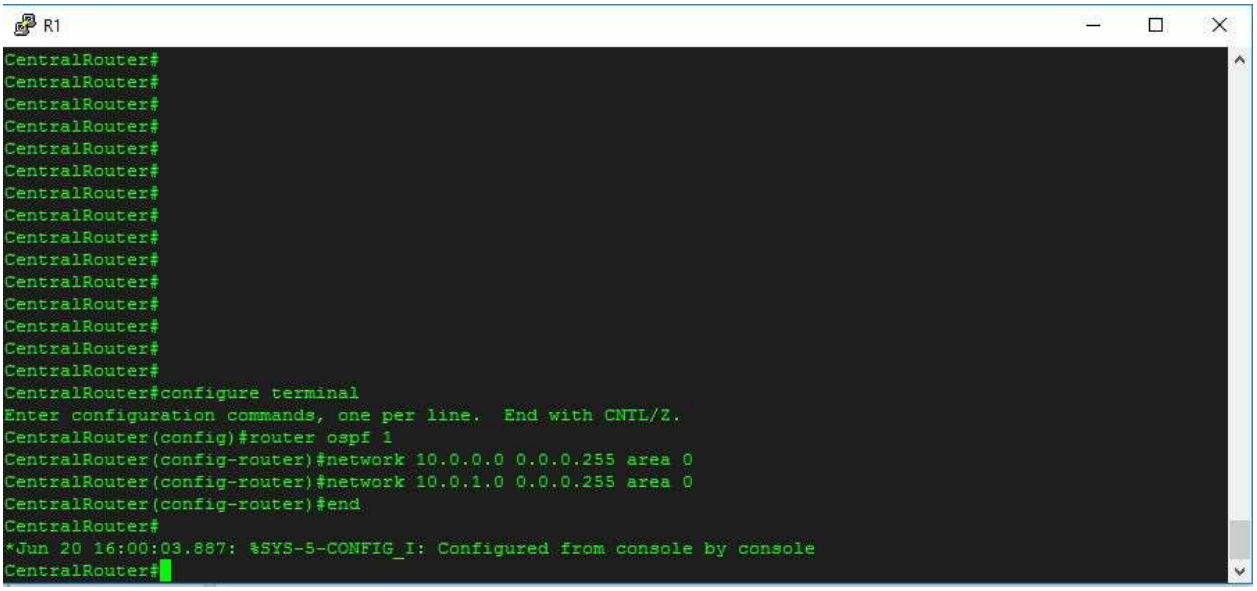


Εικόνα 4.11:Εκχώρηση διευθύνσεων **IP στις διεπαφές** του Δρομολογητή

Το αμέσως επόμενο βήμα είναι να δρομολογήσουμε και να δώσουμε όνομα-στο Router:



Εικόνα 4.12: Ορισμός HostName R1 δρομολογητή

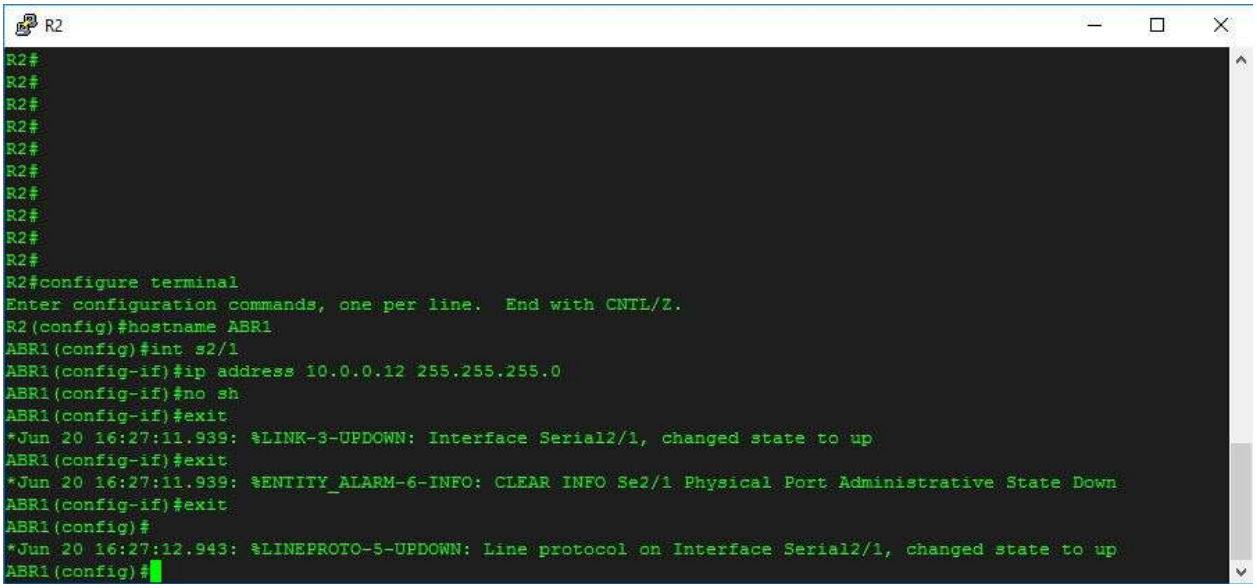


Εικόνα 4.13: Δρομολόγηση με χρήση OSPF

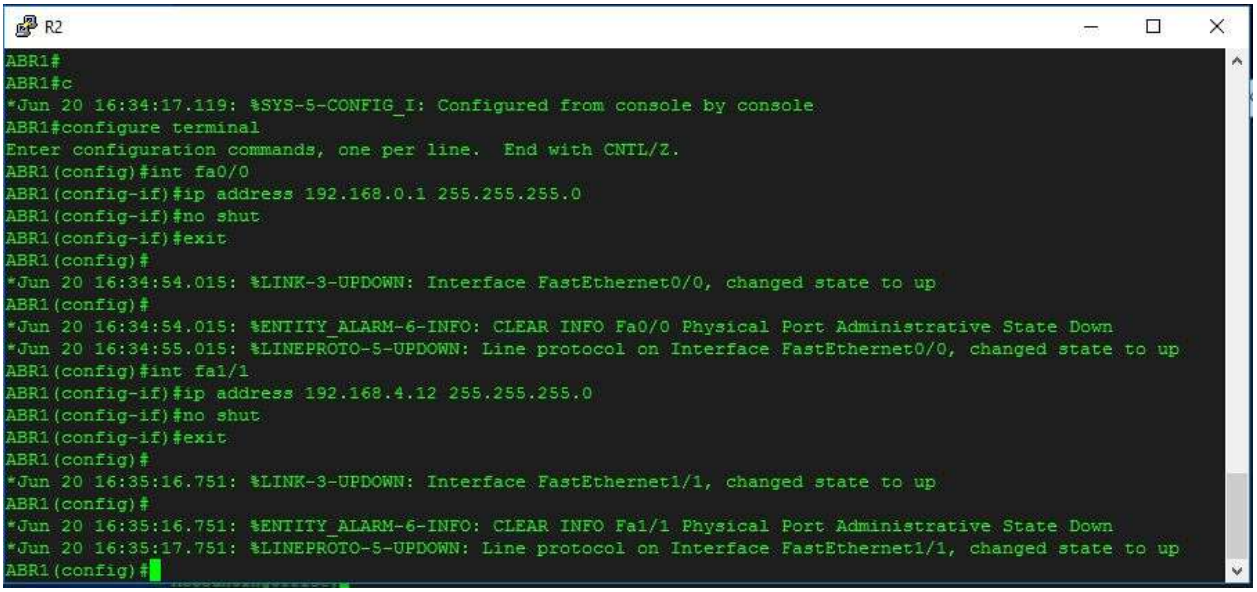
Τώρα, ο κεντρικός μας Δρομολογητής είναι έτοιμος (σχεδόν) και μπορούμε να προχωρήσουμε στην δημιουργία και διαμόρφωση των υπόλοιπων routers . Θα ορίσουμε άλλα δύο router τα οποία θα αποτελούν τους δρομολογητές (Area Border Router) που θα ‘’ενώνουν’’ τα απομακρυσμένα καταστήματα με την περιοχή δικτύου κορμού (Backbone Area).

3.4.2.2 Διαμόρφωση R2-R3 δρομολογητή

Όπως είπαμε οι R2-R3 δρομολογητές θα αποτελούν τα ενδιαμέσα router που θα ενώνουν τα καταστήματα με την περιοχή δικτύου κορμού. Θα πρέπει να ορίσουμε διαφορετικές περιοχές (areas) για τις διεπαφές (interfaces) που θα συνδεόνται με το R1 και με τα καταστήματα. Ξεκινάμε εκχωρώντας διεύθυνση στις IP στις διεπαφές και αλλάζοντας το hostname

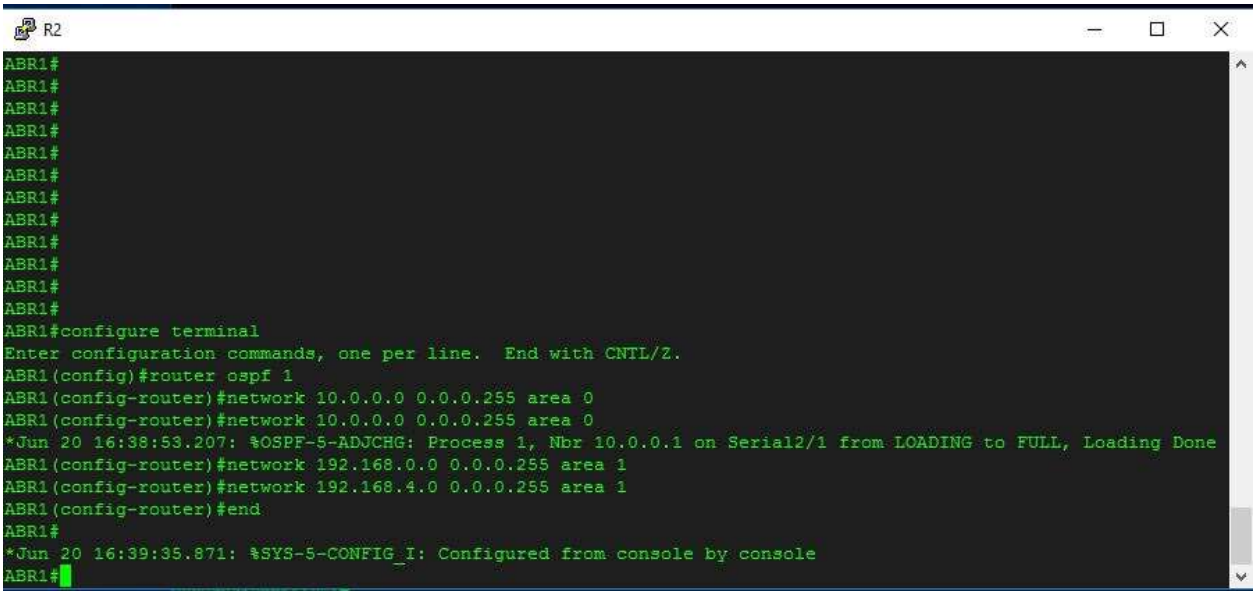


Εικόνα 4.14: Ορισμός HostName και Εκχώρηση διεύθυνσης IP στις διεπαφές



Εικόνα 4.15: Εκχώρηση διεύθυνσης IP στις υπόλοιπες διεπαφές

Προχωράμε και στην Δρομολόγηση με χρήση του πρωτοκόλλου OSPF όπου θα πρέπει να προσέξουμε ιδιαιτέρως στον ορισμό των areas ώστε να αποφύγουμε τυχόν αστοχίες στην ομαλή λειτουργία της τοπολογίας μας. Θα ορίσουμε 3 περιοχές(areas), 2 για τα Καταστήματα και 1 για την περιοχή Δικτύου Κορμού.



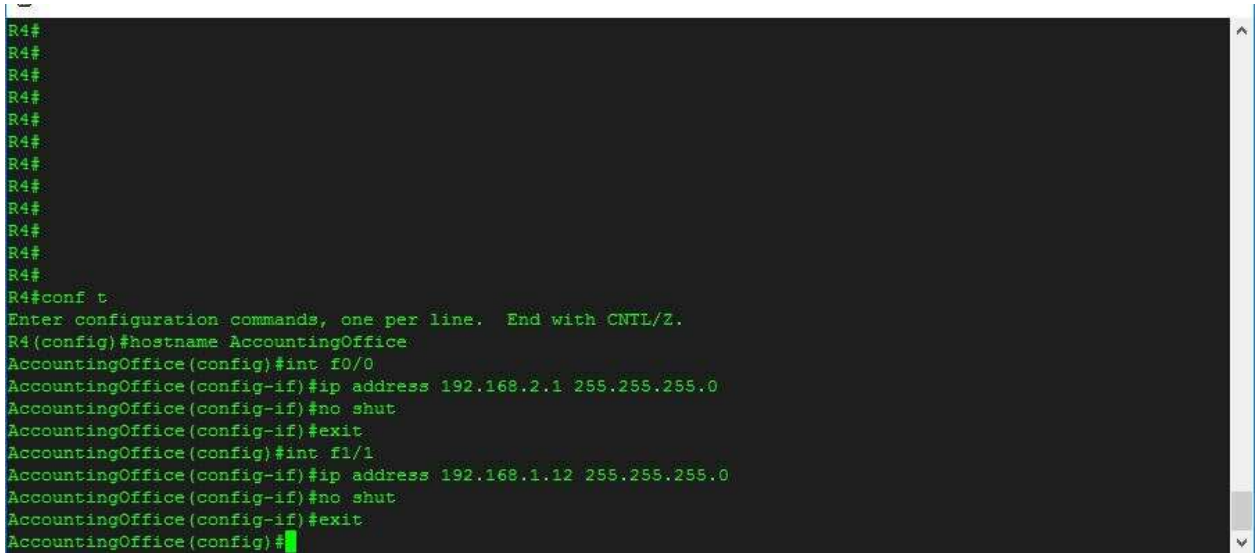
Εικόνα 4.16: Δρομολόγηση με χρήση OSPF

Αντίστοιχα με το R2 θα ορίσουμε και το R3 ώστε να συνδεθεί με το άλλο κατάστημα (άλλη περιοχή)

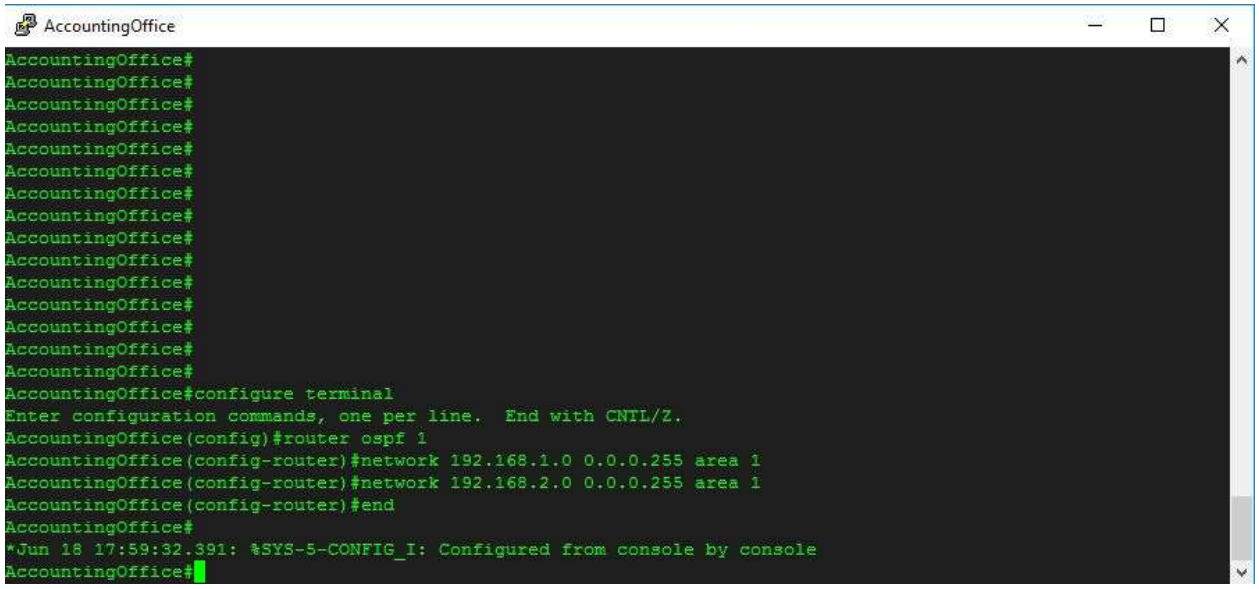
3.4.2.3 Κατάστημα Αθήνας(Area 1)

Σε αυτή την area θα ορίσουμε 4 δρομολογητές που θα αποτελέσουν το κατάστημα της Αθήνας. Κάθε ένα router θα έχει hostname που θα αντικατοπτρίζει την ιδιότητα του μέσα στο κατάστημα, χωρίς να επηρεάζει κάτι στην διαμόρφωση των υπολοίπων και την λειτουργία του συνολικού μας δικτύου. Για λόγους συντομίας θα δείξουμε την διαμόρφωση ενός από των τεσσάρων δρομολογητών.

Διαμόρφωση Router AccountingOffice



Εικόνα 4.17: Ορισμός HostName και Εκχώρηση διεύθυνσης IP στις διεπαφές

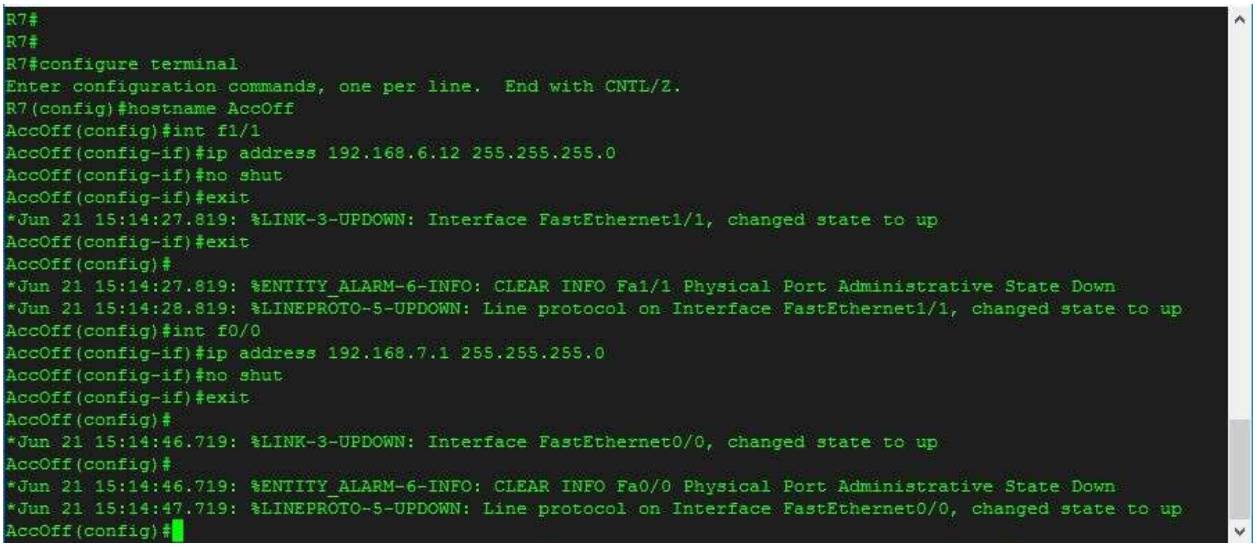


Εικόνα 4.18: Δρομολόγηση με χρήση OSPF

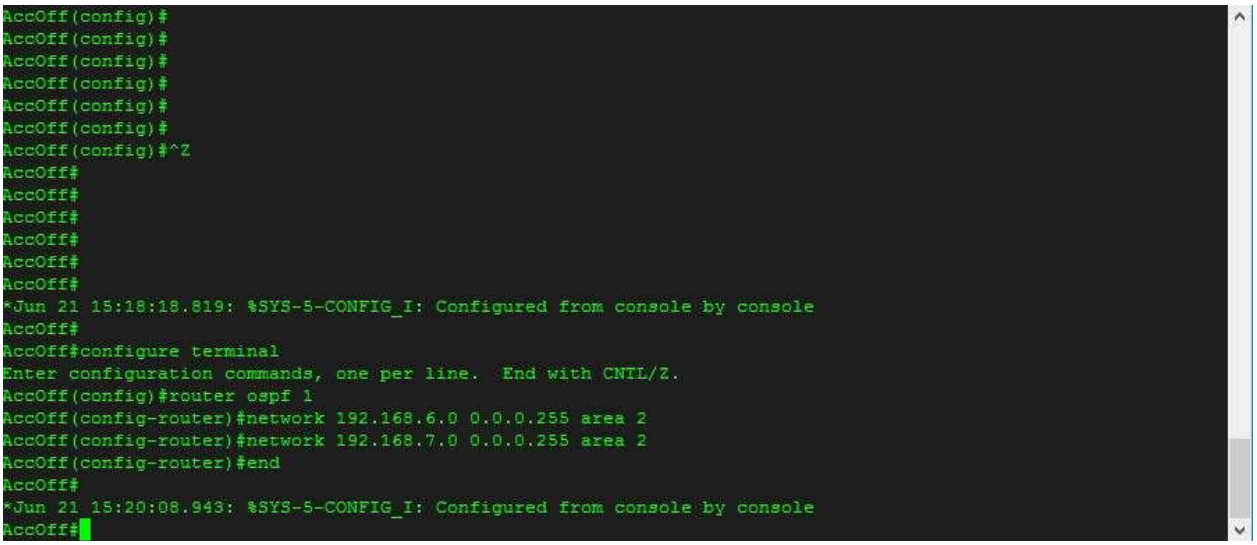
3.4.2.4 Κατάστημα Σπάρτης (area 2)

Σε αυτή την area θα ορίσουμε 4 δρομολογητές που θα αποτελέσουν το κατάστημα της Σπάρτης. Κάθε ένα router θα έχει hostname που θα απευθύνεται στην ιδιότητα μέσα στο κατάστημα όπως και στο κατάστημα της Αθήνας. Για λόγους συντομίας θα δείξουμε την διαμόρφωση ενός από των τεσσάρων δρομολογητών.

Διαμόρφωση Router AccOff



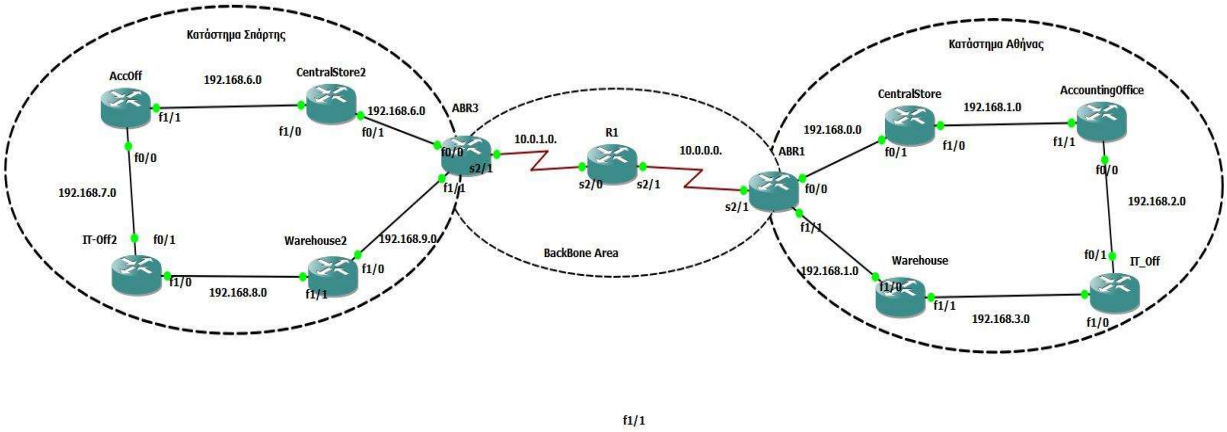
Εικόνα 4.19: Ορισμός HostName και Εκχώρηση διεύθυνσης IP στις διεπαφές



Εικόνα 4.20: Δρομολόγηση με χρήση OSPF

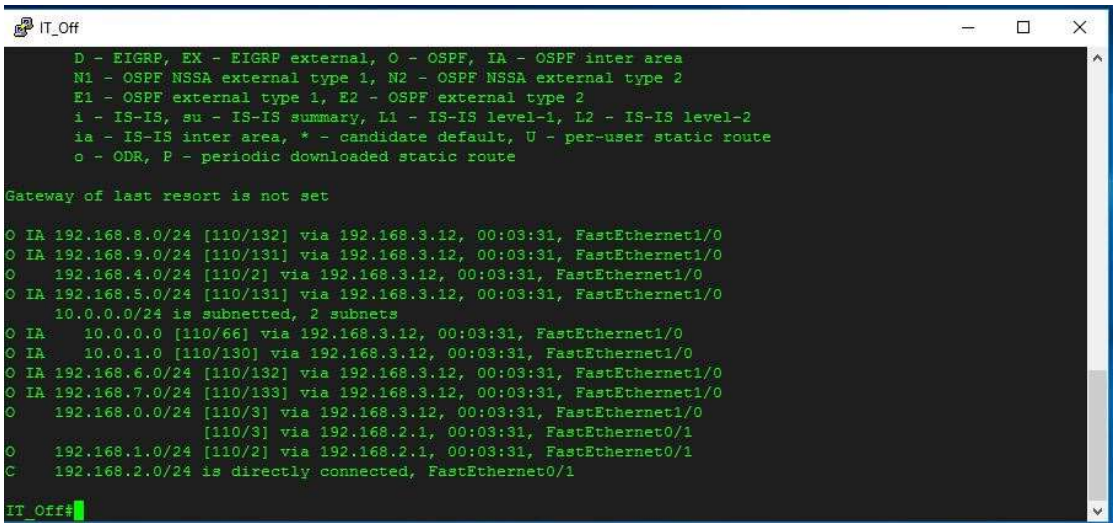
3.4.3 Η Τοπολογία ολοκληρωμένη

Αφού έχουμε διαμορφώσει όλους τους δρομολογητές η τοπολογία μας θα έχει την παρακάτω μορφή



Εικόνα 4.21:Η τοπολογία ολοκληρωμένη

Στη συνέχεια, θέλουμε να δείξουμε ό,τι πράγματι η διαμόρφωση είναι επιτυχημένη και όλοι οι δρομολογητές ‘’βλέπουν’’ (μπορούν να επικοινωνήσουν) τους άλλους. Διαλέγουμε ένα τυχαίο δρομολογητή και τρέχουμε την εντολή ‘’show ip route’’ η οποία θα μας το επαληθεύσει. Και πράγματι, παρακάτω βλέπουμε ότι ο δρομολογητής ‘’IT_Off’’ βλέπει όλους τους δρομολογητές:

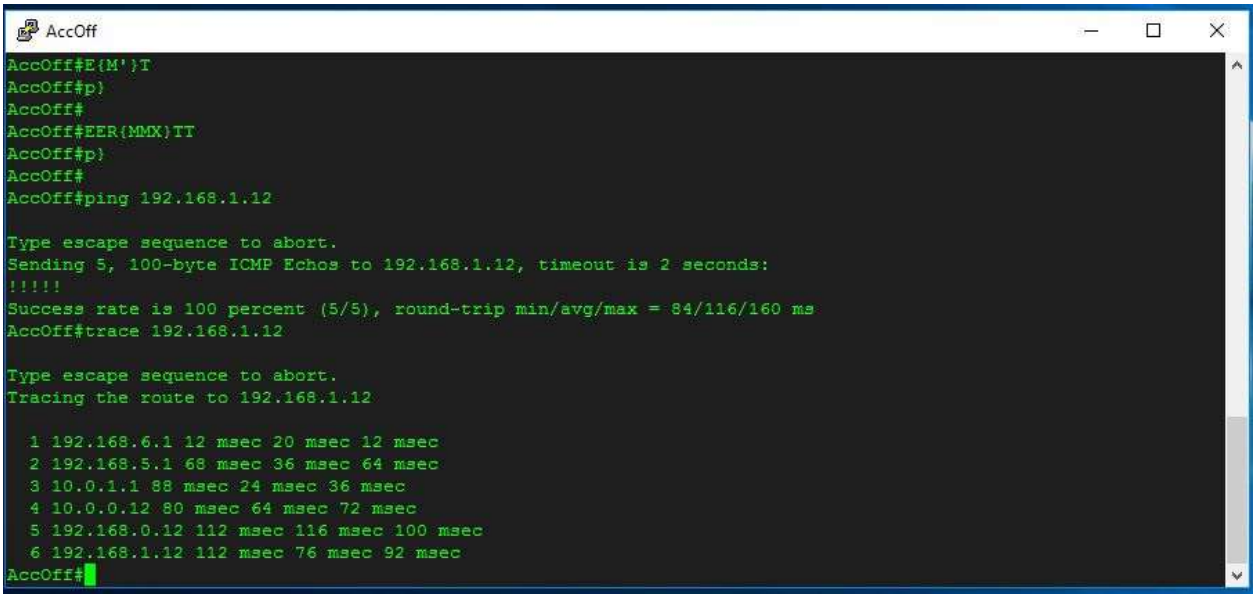


Εικόνα 4.22: Ο δρομολογητής "IT_Off" επικοινωνεί με όλους τους δρομολογητές

3.4.4 Πρωτόκολλο OSPF σε δράση

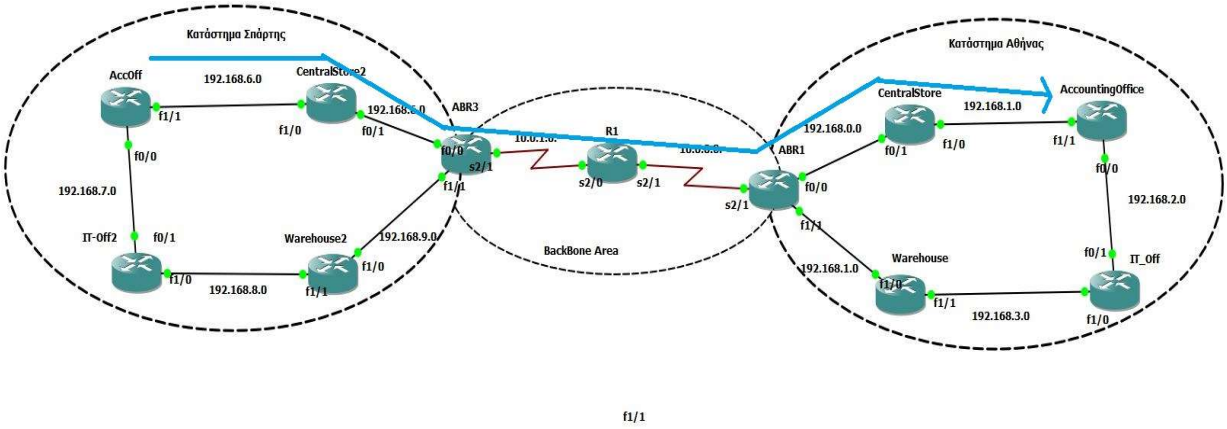
Τώρα θα δούμε την λειτουργία του πρωτοκόλλου OSPF και ποια διαδρομή επιλέγει για να έρθει σε επικοινωνία με έναν απομακρυσμένο δρομολογητή και πως αντιδρά όταν ένας ενδιάμεσος δρομολογητής για κάποιο λόγο τίθεται εκτός λειτουργίας.

Από τον δρομολογητή ‘’AccOff’’ θα προσπαθήσουμε να έρθουμε σε επικοινωνία με τον απομακρυσμένο δρομολογητή ‘’AccountingOffice’’ και αν η προσπάθεια είναι επιτυχής θα δούμε την διαδρομή που διένυσε . Για να δούμε την διαδρομή αρκεί να πληκτρολογήσουμε την εντολή ‘’trace’



Εικόνα 4.23: Η διαδρομή που ακολούθησε το "AccOff"για να επικοινωνήσει με το "AccountingOffice”

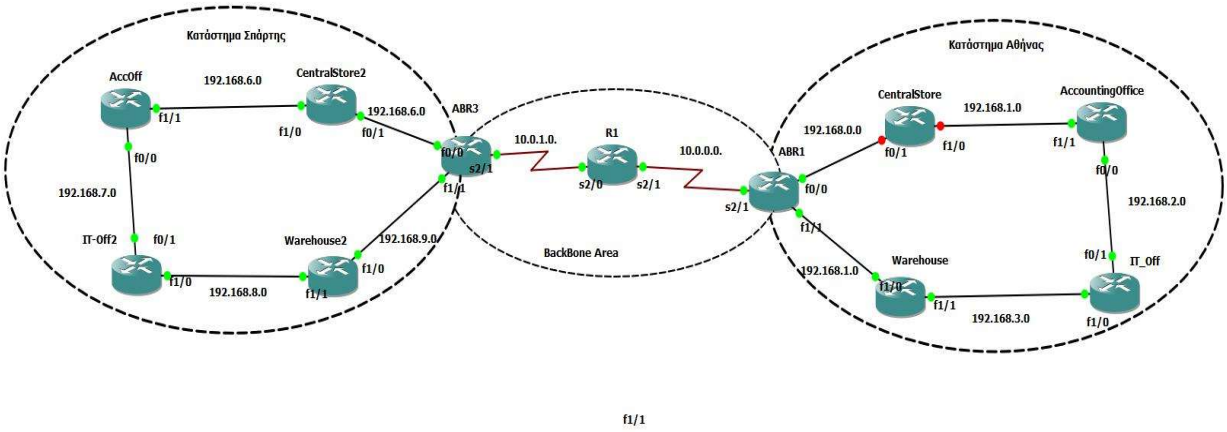
Η διαδρομή που ακολούθησε σχηματικά:



Εικόνα 4.24:Η διαδρομή που ακολούθησε ο Δρομολογητής AccOff

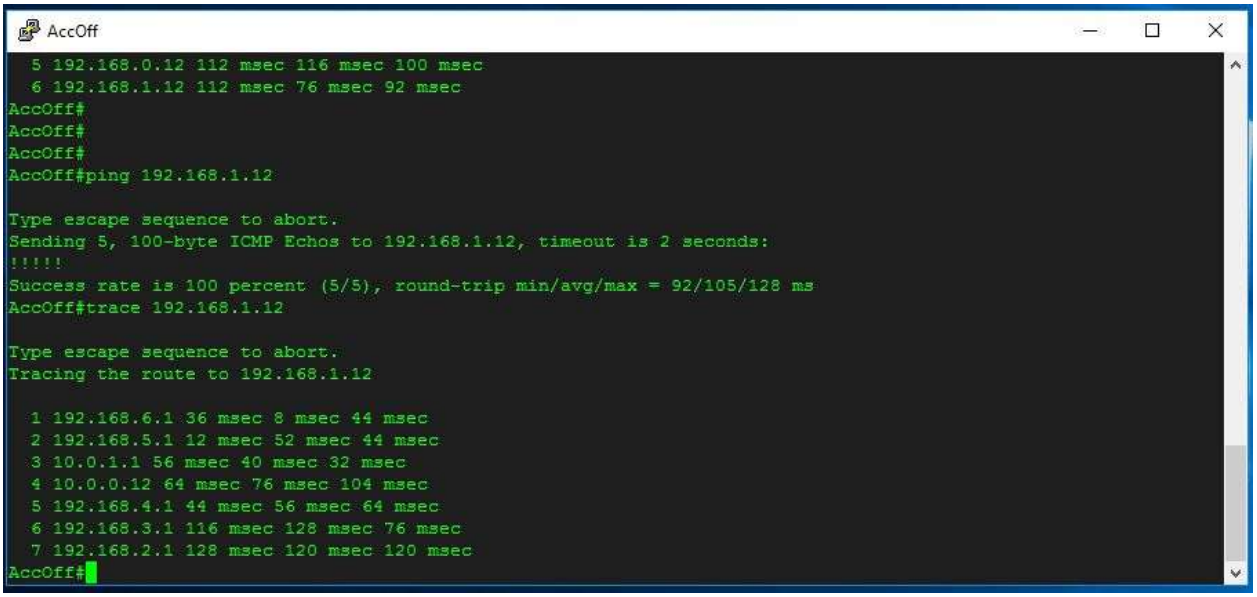
3.4.4.1 Εναλλαγή διαδρομής

Αν υποθέσουμε ότι λόγω κάποιας δυσλειτουργίας ο δρομολογητής CentralStore τεθεί εκτός λειτουργίας η επικοινωνία των Δρομολογητών θα συνεχιστεί κανονικά καθώς το πρωτόκολλο OSPF μας εξασφαλίζει ότι θα ακολουθήσει την αμέσως πιο σύντομη διαδρομή.



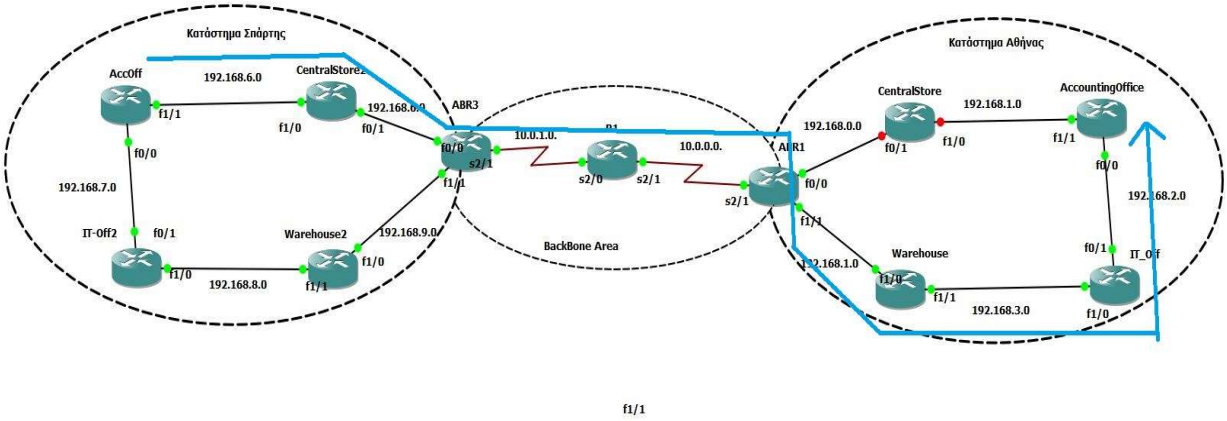
Εικόνα 4.25: Τοπολογία με δρομολογητή ''CentralStore'' εκτός λειτουργίας

Μπαίνοντας στο τερματικό του δρομολογητή AccOff και πληκτρολογώντας τις αντίστοιχες εντολές για να δούμε αν η επικοινωνία είναι εφικτή βλέπουμε το εξής:



Εικόνα 4.26: Εναλλακτική Διαδρομή Επικοινωνίας

Βλέπουμε λοιπόν ότι η επικοινωνία είναι ακόμα εφικτή και η διαδρομή που ακολούθησε είναι η παρακάτω:

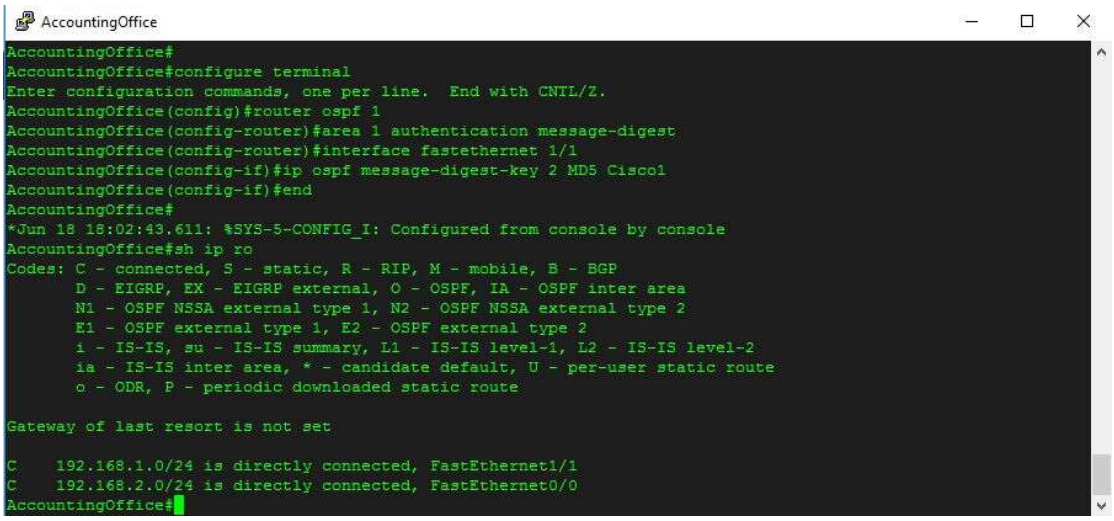


Εικόνα 4.27: Εναλλακτική διαδρομή σχηματικά

3.4.5 MD5 Configuraton

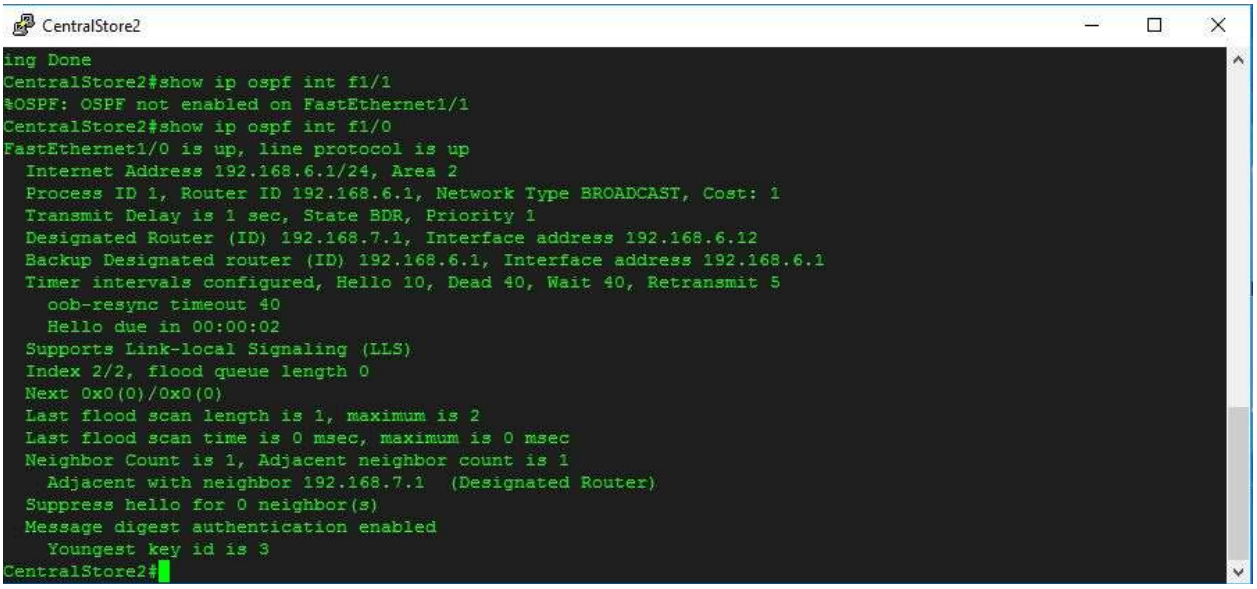
Πλέον το θέμα της απομακρυσμένης επικοινωνίας όπως είδαμε έχει επιτευχθεί αλλά αυτό που δεν έχει εξασφαλιστεί ακόμα είναι η ύπαρξη κάποιας προστασίας της τοπολογίας από ‘’εξωτερικούς κινδύνους’’ . Θα χρησιμοποιήσουμε την μέθοδο MD5 Configuration όπου κάθε περιοχή θα έχει το δικό της χαρακτηριστικό κωδικό .

Διαμόρφωση Accounting Office



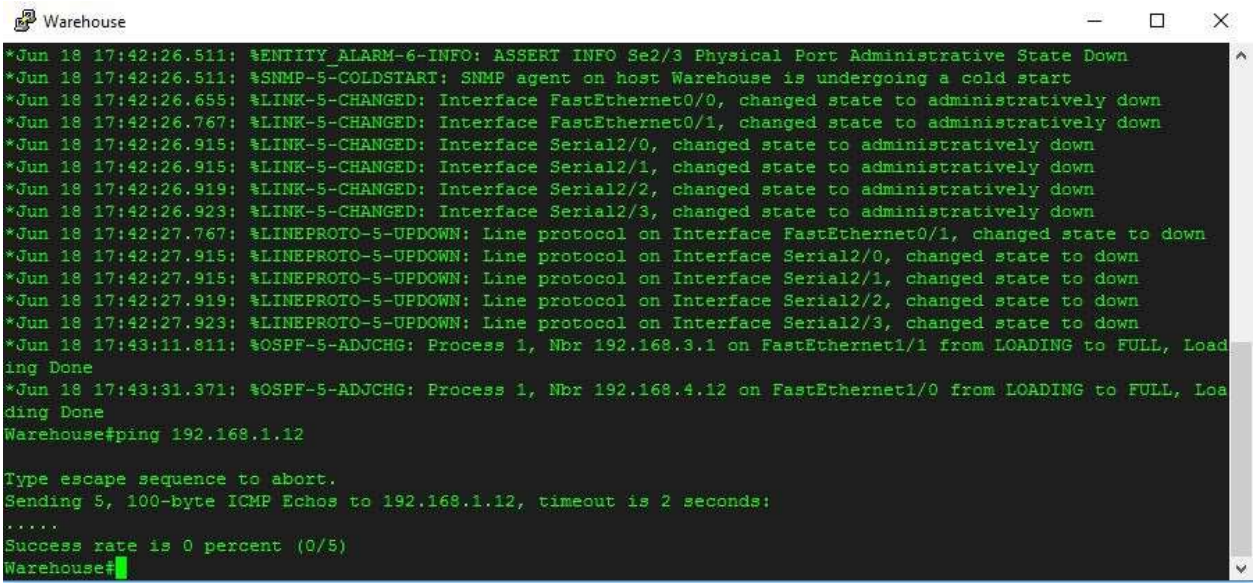
Εικόνα 4.28: Διαμορφώση της μεθόδου MD5

Χρησιμοποιώντας την εντολή **‘’show ip ospf interface FastEthernet 1/1’’** βλέπουμε ότι πράγματι η διαμόρφωση έγινε με επιτυχία



Εικόνα 4.29: Η διαμόρφωση έγινε με επιτυχία

Αν δοκιμάσουμε από τον δρομολογητή Warehouse να επικοινωνήσουμε με τον δρομολογητή Accounting Office που δεν γνωρίζει τον κωδικό για να επικοινωνήσει μαζί του θα δούμε ότι όντως η επικοινωνία θα αποτύχει.



Εικόνα 4.30: Αποτυχημένη προσπάθεια επικοινωνίας με τον Δρομολογητή Accounting Office

3.4.6 Συμπεριφορά του Δικτύου σε συνθήκες Φόρτου εργασίας

Πλέον, μετά την ολοκλήρωση του Δικτύου των Υποκαταστημάτων και των ρυθμίσεων/διαμορφώσεων που έγιναν σε αυτά, θα δούμε την συμπεριφορά του

Δικτύου σε συνθήκες “φόρτου εργασίας” ώστε να δούμε αν πληροί τις προδιαγραφές ενός σύγχρονου δικτύου.

Ας υποθέσουμε, ότι στο εμπορικό κατάστημα Σπάρτης, όλοι οι χρήστες μιλάνε στο τηλέφωνο για την προώθηση ενός προϊόντος που προμηθευτήκαν από την αποθήκη της Αθήνας. Αυτό σημαίνει ότι το bandwidth σε εκείνο το σημείο του δικτύου (διεπαφή) θα αυξηθεί σημαντικά, όπου αυτό συνεπάγεται αύξηση κόστους.

Ταυτόχρονα, το λογιστικό τμήμα θέλει να στείλει ένα e-mail στο αντίστοιχο τμήμα της Αθήνας για την διευκρίνιση κάποιων οικονομικών στοιχείων της παραγγελίας

Αν αυτό γινόταν σε συνθήκες κανονικές , όπως βλέπουμε παρακάτω η διαδρομή με το μικρότερο κόστος:

```
AccOff#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/156/160 ms
AccOff#trace 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.2.1

  1 192.168.6.1 16 msec 32 msec 32 msec
  2 192.168.5.1 92 msec 64 msec 64 msec
  3 10.0.1.1 124 msec 72 msec 84 msec
  4 10.0.0.12 140 msec 124 msec 124 msec
  5 192.168.0.12 144 msec 172 msec 188 msec
  6 192.168.1.12 140 msec 168 msec 176 msec
AccOff#ping 192.168.2.1
```

Εικόνα 4.31: Διαδρομή πριν την αύξηση του Bandwidth

Στην συνέχεια, θα αυξήσουμε χειροκίνητα το BandWidth ώστε να δούμε την συμπεριφορά του Δικτύου μας

```
CentralStore2#
CentralStore2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CentralStore2(config)#int f0/1
CentralStore2(config-if)#bandwidth 1500
CentralStore2(config-if)#no sh
CentralStore2(config-if)#exit
CentralStore2(config)#
```

Εικόνα 4.32: Χειροκίνητη αύξηση του Bandwidth

Και πράγματι βλέπουμε το εξής:

```
AccOff#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 204/246/308 ms
AccOff#trace 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.2.1

  1 192.168.7.12 32 msec 48 msec 28 msec
  2 192.168.8.12 24 msec 88 msec 52 msec
  3 192.168.9.12 60 msec 88 msec 64 msec
  4 10.0.1.1 108 msec 112 msec 140 msec
  5 10.0.0.12 156 msec 148 msec 116 msec
  6 192.168.0.12 204 msec 140 msec 204 msec
  7 192.168.1.12 220 msec 156 msec 220 msec
```

Εικόνα 4.33: Η πιό σύντομη διαδρομή μετά την αύξηση του Bandwidth

Συμπεραίνουμε , πως μετά την αύξηση του Bandwidth το κόστος αυξήθηκε και η διαδρομή που εκτελούσε μέχρι πρότινος δεν αποτελεί την πιο σύντομη και για αυτό τον λόγο το δίκτυό μας αυτόματα υπολογίζει την πλέον πιο σύντομη και την εφαρμόζει.

4. Ανακεφαλαίωση-Συμπεράσματα

Σε αυτό το κεφάλαιο θα γίνει μια σύντομη ανασκόπηση της πτυχιακής εργασίας και των αποτελεσμάτων αυτής.

Στο Θεωρητικό μέρος της εργασίας γίνεται αναφορά στα Ασύρματα Δίκτυα και ειδικότερα στα Ασύρματα Δίκτυα Νέας Γενιάς και στο πως μπορούν να προστατευθούν από διάφορες απειλές που μπορούν να προκύψουν αλλά και πόσο σημαντικό ρόλο μπορεί να διαδραματίσει στην ανάπτυξη μιας επιχείρησης ή οργανισμού. Παρουσιάστηκαν οι δικτυακές συσκευές και τα μέσα μετάδοσης, που συγκροτούν ένα δίκτυο και στη συνέχεια αναλύθηκε με παραδείγματα πως μπορεί να διευθυνσιοδοτηθεί και να χωριστεί σε υποδίκτυα.

Έγινε αναφορά στα πρωτόκολλα δικτύων, στο μόντελο OSI και τα επτά επίπεδα από τα οποία αποτελείται, στο μοντέλο TCP/IP, στα πρωτόκολλα δρομολόγησης και στις ιδιότητες τους. Ακόμα, περιγράφονται τα πρωτόκολλα RIP και OSPF, που αποτελούν πρωτόκολλα εσωτερικής εφαρμογής(IGP), τα πρωτόκολλα εξωτερικής εφαρμογής και το πρωτόκολλο IpSec.Αναλύθηκε η έννοια της Δρομολόγησης, οι αλγόριθμοι δρομολόγησης και οι ιδιότητες που πρέπει να τους χαρακτηρίζουν.

Στο πρακτικό μέρος, αναλύσαμε το προφίλ της εταιρείας, και τις απαιτήσεις της ώστε να έχει ένα υγιές δίκτυο, και έγινε αναφορά τόσο στα Hardware όσο και στα Software εργαλεία που ήταν απαραίτητα για να γίνει η υλοποίηση του Project. Ιδιαιτέρως έγινε αναλυτική περιγραφή, βήμα προς βήμα ,η εγκατάσταση του εικονικού προσομοιωτή GNS3 ο οποίος αποτέλεσε το βασικό μας εργαλείο για τον σχεδιασμό του Δικτύου. Στην συνέχεια, με την χρήση του GNS3,αναλύεται ο τρόπος δημιουργίας μιας εικονικής τοπολογίας που περιγράφει δύο απομακρυσμένα καταστήματα, κ εκχώρηση διευθύνσεων στους δρομολογητές, η δρομολόγηση τους με χρήση πρωτοκόλλου OSPF και την χρήση της μεθόδου MD5 για την προστασία από ανεπιθύμητες ενέργειες. Παρακάτω αναφέρονται συνοπτικά οι 3 στόχοι και το αποτέλεσμα του καθενός

Πρώτος στόχος μας ήταν η επιτυχημένη σύνδεση των 2 υποκαταστημάτων. Με λίγα λόγια, να μπορούν όλα τα τμήματα του κάθε Υποκαταστήματος να δουν

το ένα το άλλο. Πράγματι, μετά την σωστή διαμόρφωση, διευθυνσιοδότηση και δρομολόγηση όλα τα τμήματα ‘’βλέπουν’’ το ένα το άλλο.

Δεύτερος στόχος ήταν να δούμε την συμπεριφορά του πρωτοκόλλου OSPF σε περίπτωση που κάποιο τμήμα ενός Υποκαταστήματος(Δρομολογητής) τεθεί εκτός για προσωρινό διάστημα. Όντως, στο παράδειγμα που κάναμε, είδαμε ότι παρόλο που ένας δρομολογητής τέθηκε εκτός, η επικοινωνία μεταξύ των δύο δρομολογητών δεν σταμάτησε αλλά ακολούθησε την αμέσως πιο σύντομη διαδρομή

Τρίτο και πιο σημαντικός στόχο αποτελεί και ύπαρξη κάποιας προστασίας των Υποκαταστημάτων(της τοπολογίας) από ‘’εξωτερικούς κινδύνους’’ .Για αυτό τον λόγο χρησιμοποιήσαμε την μέθοδο MD5 Configuration όπου κάθε περιοχή θα είχε το δικό της χαρακτηριστικό κωδικό .Πράγματι, δοκιμάζοντας να φέρουμε σε επικοινωνία δύο τμήματα(δρομολογητές) όπου ο ένας δεν γνωρίζει τον κωδικό για να επικοινωνήσει με τον άλλον, η επικοινωνία θα αποτύχει.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Agrawa G. *Συστήματα Επικοινωνιών με Οπτικές Ίνες*, Εκδόσεις Τζιόλα, 2008.
2. Fluke Networks. VLAN Best Practices. Everett, WA USA, 2004.
3. Dye Mark A., McDonald, Rick, Rufi, Antoon W. *Network Fundamentals - CCNA Exploration Companion Guide,* Cisco Systems, 2008.
4. Bouras, Gkamas, Stamos, *From IPv4 to IPv6: The case of OpenH323 Library*, SAINT, 2003
5. Thornier, S. *Dynamic routing protocol implementation decision between EIGRP, OSPF and RIP based on technical background using OPNET Modeler*,in Proc. Second International Conference on Computer and Network Technology (ICCNT), Bangkok, Thailand, Apr. 2010.
6. James Edwards, R. B. *Networking - OSI, TCP/IP, LANs, MANs, WANs, Implementation, Management and Maintenance*. Indianapolis: Wiley, 2009.
7. Comer Douglas. *Δίκτυα και διαδίκτυα υπολογιστών και εφαρμογές τους στο Internet*. Εκδόσεις Κλειδάριθμος, 2007
8. Microsoft, Virtual Private Networking in Windows 2000: An Overview. White Paper, 1999.
9. Goodrich, M. *Efficient and Secure Network Routing Algorithms*. Provisional Patent Filing , USA. 2001.
10. Douglas E. Comer. Διαδίκτυα με TCP/IP { Τόμος 1: Αρχές, Πρωτόκολλα και Αρχιτεκτονικές, 4η Αμερικάνικη Εκδοση, Εκδόσεις Κλειδάριθμος, 2008.
11. Bollapragada, Vijay,Khalid, Mohamed, Wainner Scott. *IPSec VPN Desing,* Cisco Press, 2005.
12. Tanenbaum, AndrewS. *Δίκτυα Υπολογιστών*, Εκδόσεις Κλειδάριθμος, 2003.

ΣΥΝΔΕΣΜΟΙ

13. Wireless_network, Διαθέσιμο εδώ: https://en.wikipedia.org/wiki/Wireless_network
14. Benefits of Vlans, Διαθεσίμο εδώ: http://itknowledgeexchange.techtarget.com/itanswers/benefits-of-vlans/
15. Types of VLANs, Διαθέσιμο εδώ: http://blog.router-switch.com/2012/11/types-of-vlans/
16. Variable Length Subnet Mask (VLSM), Διαθέσιμο εδώ: https://network-lessons.com/subnetting/variable-length-subnet-mask-vlsm/
17. Four Layers of TCP/IP model, Comparison and Difference between TCP/IP and OSI models Διαθέσιμο εδώ: http://www.omnisecu.com/tcpip/tcpip-model.php
18. Metrics (networking), Διαθέσιμο εδώ: https://en.wikipedia.org/wiki/Metrics_(networking)
19. What is adaptive routing(dynamic routing), Διαθέσιμο εδώ: http://searchnetworking.techtarget.com/definition/adaptive-routing
20. Textbookexcerpts-routing, Διαθέσιμο εδώ: https://www.cs.unm.edu/~crandall/netsfall15/lecturenotes/textbookexcerpts-routing.pdf
21. What is a Hub?, Διαθέσιμο εδώ: https://www.computerhope.com/jargon/h/hub.htm
22. What is a Bridge? - Definition from Techopedia, Διαθέσιμο εδώ: https://www.techopedia.com/definition/3160/bridge
23. What are Types VLAN? Explained with Example, Διαθέσιμο εδώ: http://www.orbit-computer-solutions.com/types-vlan/
24. Routing protocols and architectures/Routing algorithms, Διαθέσιμο εδώ: https://en.wikibooks.org/wiki/Routing_protocols_and_architectures/Routing_algorithms
25. Routing protocols and architectures/Routing algorithms ,Διαθέσιμο εδώ: https://technet.microsoft.com/en-us/library/cc957844.aspx

ΣΥΜΠΛΗΡΩΜΑΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Doyle, Jeff. *Routing TCP/IP*, Volume I, Cisco Press,2005.
- Duato,J., Yalmanchili S., Ni L. *Interconnection Networks an Engineering Approach,* 1st Edition, 1997.
- Guichard,Ivan,Apcar Pepelnjak,Jeff.*MPLS and VPN architectures,* Cisco Press,2003.
- Hamza, F., Mohamed, A. Performance Comparison of Two Dynamic Routing Protocols: RIP and OSPF. *Journal of Emerging Trends in Computing and Information Sciences*, volume 2: October 2011.
- Moy, J. *OSPF: anatomy of an Internet routing protoco*l, Pearson Education, 1998.
- Hoffman, P., Cryptographic Suites for IPsec. IETF. RFC 4308, 2005.
- Nortel Networks, “Virtual Private Networks and IPsec”, White Paper 2002
- Rakheja, P., Kaur, P. Performance analysis of RIP, OSPF, IGRP and EIGRP routing protocols in network. *International Journal of Computer Applications* 48.18, 2012.
- Richardson, M.*A Method for Storing IPsec Keying Material in DNS*. IETF. RFC 4025, 2005.
- Rick Graziani, Allan Johnson. *Routing Protocols and Concepts - CCNA Exploration Companion Guide,* Cisco Systems, 2008.
- Scott,Ch.,Wolfe, P., Erwin M. *Virtual Private Networks, Turning the Internet Into Your Private Network,* O'Reilly Media, 1998.
- Vetriselvan, V., Patil, P., Mahendran, M. Survey on the RIP, OSPF, EIGRP Routing Protocols (IJCSIT). *International Journal of Computer Science and Information Technologies,* Vol. 5 (2), 2014.
- VLANs and Trunking. Retrieved from: http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3
- Wright, Robert. *IP Routing Configuration Basics*, Pearson Professional Education, 1998.
- Network OS Layer 3 Routing Configuration Guidehttp://www.brocade.com/content/html/en/configuration-

guide/NOS_600_LAYER3/GUID-4A416C0F-7FB6-47C5-AD24-CB933EFB6A45.html