ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

«Βασικές αρχές δρομολόγησης σε σύνθετα δίκτυα μεταγωγής και εφαρμογή αυτών κάνοντας χρήση του Cisco Packet Tracer»

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

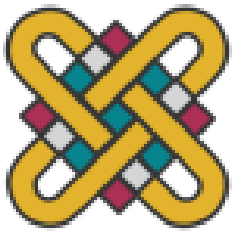
του

Νατσιόπουλου Οδυσσέα ΑΕΜ: 2471

Επιβλέπων:

Μπιμπίρης Αθανάσιος

Καστοριά, Μάιος – 2020



ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

«Βασικές αρχές δρομολόγησης σε σύνθετα δίκτυα μεταγωγής και εφαρμογή αυτών κάνοντας χρήση του Cisco Packet Tracer»

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

Νατσιόπουλου Οδυσσέα ΑΕΜ: 2471

Επιβλέπων:

Μπιμπίρης Αθανάσιος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ημερομηνία εξέτασης

.....	.....	.....
Ον/μο Μέλους	Ον/μο Μέλους	Ον/μο Μέλους
Ιδίοτητα Μέλους	Ιδιότητα Μέλους	Ιδιότητα Μέλους

Καστοριά, Μάιος – 2020

Ευχαριστίες

Με την ολοκλήρωση της παρούσας εργασίας θα ήθελα να ευχαριστήσω την οικογένειά μου για τη στήριξη της όλα αυτά τα χρόνια των σπουδών μου καθώς και τον καθηγητή μου Μπιμπίρη Αθανάσιο για την καθοδήγηση και εμπιστοσύνη που μου έδειξε στην πορεία της πτυχιακής μου εργασίας. Τέλος, θα ήθελα να ευχαριστήσω τους φίλους μου για την ψυχολογική υποστήριξη που μου παρείχαν όλο αυτό το διάστημα.

Περίληψη

Η παρούσα εργασία έχει ως σκοπό την δημιουργία και κατανόηση μιας τοπολογίας δικτύου με την χρήση του εργαλείου packet tracer. Η συγκεκριμένη εργασία αποτελείται από το θεωρητικό και το πρακτικό κομμάτι. Στο θεωρητικό κομμάτι γίνεται μία αναφορά στις βασικές έννοιες των δικτύων και στα πρωτόκολλα που χρησιμοποιούνται. Στο πρακτικό κομμάτι πραγματοποιείται η υλοποίηση μιας τοπολογίας δικτύου με το εργαλείο cisco packet tracer, όπου ο αναγνώστης, με τη συμβολή των παρεχόμενων οδηγιών, έχει τη δυνατότητα να δημιουργήσει βήμα προς βήμα ένα δίκτυο.

Λέξεις κλειδιά: Πρωτόκολλα δρομολόγησης, Τοπολογία δικτύου, IPv4 διευθύνσεις, IPv6 διευθύνσεις, DHCP, NAT , ACL, IPsec VPN Tunnel

Abstract

The purpose of this paper is to create and understand a network topology using the packet tracer tool. This work consists of the theoretical and the practical part. In the theoretical part, reference is made to the basic concepts of networks and the protocols that being used. In the practical part, a network topology is implemented with the cisco packet tracer tool, where the reader, according to the instructions that being provided, will get the opportunity to create a network step by step.

Key words: Routing Protocols, IPv4 Addresses, IPv6 Addresses, Network Topology, DHCP, NAT, ACL, IPsec VPN Tunnel

Περιεχόμενα

Λίστα Εικόνων

Εισαγωγή

Με αυτήν την εργασία ο αναγνώστης θα είναι σε θέση να κατανοήσει κάποιες βασικές έννοιες των δικτύων καθώς και την εφαρμογή τους με το λογισμικό Packet Tracer. Με το συγκεκριμένο λογισμικό προσομοίωσης δικτύου ο αναγνώστης θα μπορεί να δημιουργήσει βήμα προς βήμα μία τοπολογία δικτύου. Στόχοι της εργασίας είναι η κατανόηση της λειτουργικότητας των συσκευών δικτύου, της λειτουργίας των IPv4 και IPv6 διευθύνσεων και τέλος τον τρόπο μεταφοράς των πληροφοριών στο δίκτυο.

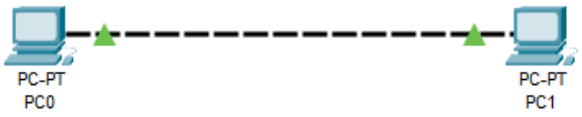
Η συγκεκριμένη πτυχιακή εργασία αποτελείται από έξι κεφάλαια. Στα πρώτα πέντε αναπτύσσεται το θεωρητικό κομμάτι, ενώ στο έκτο το πρακτικό. Στο πρώτο κεφάλαιο αναλύεται η έννοια του δικτύου, τι ακριβώς είναι τα Lan, Wan, Man και ο ρόλος κάθε συσκευής που υπάρχει σε ένα δίκτυο όπως είναι τα Hubs, Switches και Routers. Επίσης δίνονται οι πληροφορίες για τις διευθύνσεις IPv4, IPv6 καθώς και για τις MAC διευθύνσεις. Έπειτα, ο αναγνώστης εξοικειώνεται με τα διάφορα πρωτόκολλα δικτύων που υπάρχουν, αλλά και πως αυτά χρησιμοποιούνται στην δημιουργία ενός δικτύου. Στην συνέχεια, στο δεύτερο κεφάλαιο της εργασίας αναλύεται η στατική δρομολόγηση των πακέτων καθώς και η δυναμική. Στην δυναμική δρομολόγηση γίνεται η χρήση των πρωτοκόλλων δρομολόγησης RIP σε συνδυασμό με το OSPF για τις IPv4 διευθύνσεις. Στο τρίτο κεφάλαιο, γίνεται μία αναφορά στα VLAN, με ποιον τρόπο πραγματοποιείται η υλοποίησή τους, αλλά και πως μπορούμε να τα χρησιμοποιήσουμε αποτελεσματικά στο δίκτυό μας. Στο επόμενο κεφάλαιο, αναλύονται οι ACL, πως μπορούμε να τις χρησιμοποιήσουμε στο δίκτυο που θα δημιουργηθεί, καθώς και τους διάφορους τύπους ACL που υπάρχουν όπως είναι οι standard ACL, extended ACL. Στην συνέχεια του κεφαλαίου παρατίθενται πληροφορίες για τα NAT. Δίνεται η δυνατότητα στον αναγνώστη να κατανοήσει τις κατηγορίες δυναμικού και στατικού NAT, καθώς και η λειτουργία του PAT. Έπειτα, αναφέρονται συνοπτικά οι λειτουργίες των PPP και του DHCP server. Θα αποτελούσε σοβαρή παράλειψη να μην γίνει αναφορά στο πρωτόκολλο IPsec VPN Tunnel. Τέλος, στο έκτο κεφάλαιο, γίνεται η δημιουργία μιας ολοκληρωμένης τοπολογίας δικτύου, η οποία περιέχει όλα όσα έχουν προαναφερθεί. Ο αναγνώστης σύμφωνα με τις γνώσεις που έχει αποκτήσει από τα προηγούμενα κεφάλαια θα μπορεί βήμα-βήμα να υλοποιήσει μία τοπολογία δικτύου.

Κεφάλαιο 1 Βασικές έννοιες Δικτύων

1.1 Τι είναι ένα δίκτυο

Από την στιγμή που το internet μπήκε στις ζωές μας, η ανάγκη να προσαρμοστούμε σε αυτό έγινε γρήγορα αντιληπτή μιας και συμβάλει στην διευκόλυνση της καθημερινότητάς μας. Έτσι, στις μέρες μας οι επιχειρήσεις δύσκολα λειτουργούνε χωρίς κάποιο είδος δικτύου. Εύλογα προκύπτει το ερώτημα, *τι σημαίνει ένα δίκτυο.*

Δίκτυο μπορεί να θεωρηθεί ένα σύστημα από συνδεδεμένες συσκευές με σκοπό να επικοινωνήσουν μεταξύ τους με την χρήση κάποιων πρωτοκόλλων. Στην παρακάτω εικόνα διακρίνουμε ένα απλό δίκτυο υπολογιστών, το οποίο αποτελείται από δύο υπολογιστές συνδεδεμένους μεταξύ τους.



Εικόνα 1. Σύνδεση δύο υπολογιστών
Πηγή: https://study-ccna.com/what-is-a-network/

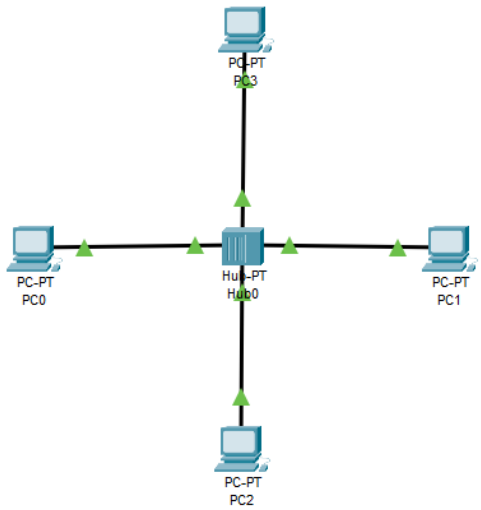
Έτσι, αυτοί οι δύο υπολογιστές μπορούν ανταλλάξουν πληροφορίες μεταξύ τους αλλά μόνο μεταξύ τους. Τι γίνεται στην περίπτωση που θα θέλαμε να συνδέσουμε δύο, ή και περισσότερους υπολογιστές;

1.2 Συσκευές Δικτύων και πώς συνδέονται μεταξύ τους

1.2.1 Hubs

Για να συνδέσουμε περισσότερους από δύο υπολογιστές χρησιμοποιούμε ένα Hub[1]. Το Hub είναι μία συσκευή η οποία δέχεται μια πληροφορία και την μεταδίδει σε όλους τους υπόλοιπους υπολογιστές εξασφαλίζοντας έτσι ότι ο υπολογιστής που θέλουμε, θα λάβει την πληροφορία. Ο τρόπος αυτός λειτουργίας δεν είναι απόλυτα ασφαλής, καθώς οι πληροφορίες διανέμονται σε ολόκληρο το δίκτυο (Odom, 2013b).

Στην παρακάτω εικόνα βλέπουμε ένα δίκτυο το οποίο αποτελείται από 4 υπολογιστές οι οποίοι είναι συνδεδεμένοι με μία συσκευή Hub.



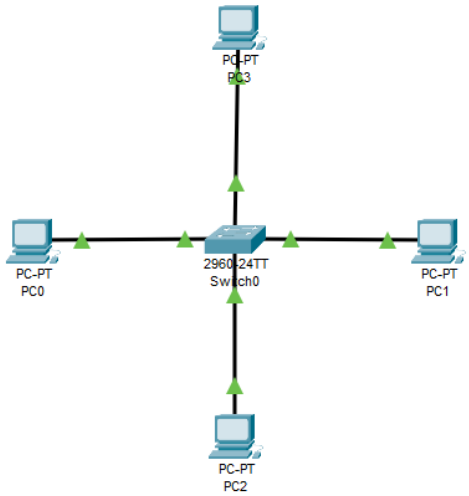
Εικόνα 2. Σύνδεση με συσκευή Hub
Πηγή: https://study-ccna.com/what-is-a-network/

Σύμφωνα με τα στοιχεία που απεικονίζονται εδώ, εάν ο υπολογιστής PC0 θέλει να στείλει μία πληροφορία στον υπολογιστή PC2, η πληροφορία θα φτάσει στο Hub και ύστερα θα σταλεί σε όλους τους υπολογιστές συμπεριλαμβανομένου και του PC2. Ο PC2 με την σειρά του θα ενεργήσει με τον ίδιο ακριβώς τρόπο (Odom, 2013b).

[1] Το Hub είναι ο συνηθέστερος όρος, ωστόσο στη βιβλιογραφία η εν λόγω συσκευή συναντάται και ως «ομφαλός», βλ. περισσότερα McQuerry (2004)

1.2.2 Μεταγωγέας

Η λειτουργία των μεταγωγέων (Switches) είναι ίδια με αυτή των Hubs αλλά με περισσότερα πλεονεκτήματα. Ένα switch είναι υπεύθυνο για την επικοινωνία πολλαπλών συσκευών φιλτράροντας τις πληροφορίες που ανταλλάσσονται. Στην παρακάτω εικόνα παρατηρούμε μία τοπολογία όπου 4 υπολογιστές είναι συνδεδεμένοι μεταξύ τους με ένα μεταγωγέα (Switch).



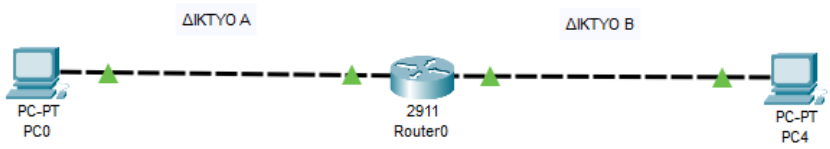
Εικόνα 3. Σύνδεση συσκευών με μεταγωγέα
Πηγή: http://cisco-packet-tracer-tutorial.blogspot.com/2014/04/tutorial-ecrit-sur-les-vlans-dans-cisco.html

Σύμφωνα με τα στοιχεία που απεικονίζονται ο υπολογιστής PC0 στέλνει μία πληροφορία στον PC1. Αφού η πληροφορία φτάσει στον μεταγωγέα, θα σταλεί μόνο στον υπολογιστή PC1 και όχι στους υπόλοιπους.

1.2.3 Δρομολογητές

Ο δρομολογητής (Router) είναι μία συσκευή δικτύου η οποία προωθεί τα πακέτα από ένα δίκτυο σε ένα άλλο. Συνήθως είναι συνδεδεμένος σε δύο ή περισσότερα δίκτυα. Ο τρόπος με τον οποίο λειτουργεί έχει ως εξής, όταν μία πληροφορία από ένα δίκτυο φτάνει σε έναν δρομολογητή εκείνος ελέγχει τον

προορισμό και στην συνέχεια την δρομολογεί με σκοπό να φτάσει στον προορισμό της. Ένα παράδειγμα δρομολόγησης πακέτου βλέπουμε στην εικόνα 4, υπολογιστές από δύο διαφορετικά δίκτυα προσπαθούν να επικοινωνήσουν μεταξύ τους (Odom, 2013b).

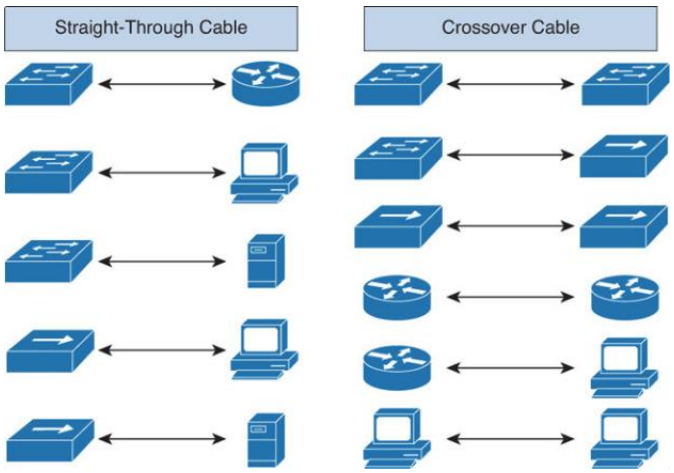


Εικόνα 4. Σύνδεση υπολογιστών από διαφορετικό δίκτυο
Πηγή: https://study-ccna.com/what-is-ip-routing/

Στην συγκεκριμένη περίπτωση, ο υπολογιστής του δικτύου Α στέλνει ένα πακέτο στον δρομολογητή με σκοπό να φτάσει στον υπολογιστή του Β δικτύου. Αφού φτάσει στον δρομολογητή εκείνος με την σειρά του βλέπει το προορισμό και στέλνει το πακέτο στον υπολογιστή του Β δικτύου.

1.3 Καλωδίωση συσκευών

Υπάρχουν δύο τύποι καλωδίων όσον αφορά στην σύνδεση συσκευών. Τα straight-through καλώδια και τα crossover. Στη συνέχεια διακρίνουμε τις περιπτώσεις στις οποίες χρησιμοποιείται το κάθε καλώδιο.



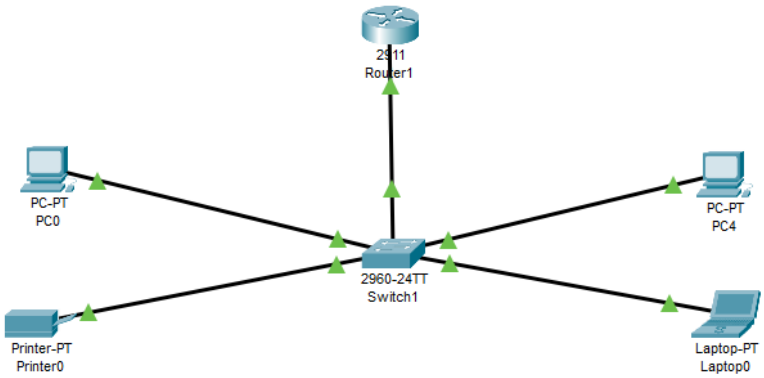
Εικόνα 5. Καλωδίωση συσκευών
Πηγή: http://www.cables-solutions.com/difference-between-straight-through-and-crossover-cable.html

1.4 Είδη δικτύων

1.4.1 Lan

Ο όρος Lan (Local area network) περιγράφει ένα δίκτυο από διάφορες συσκευές οι οποίες είναι συνδεδεμένες μεταξύ τους σε ένα συγκεκριμένο χώρο (ένα σπίτι, το γραφείο).

Ένα τυπικό SOHO (small office/home office) LAN αποτελείται από διάφορους υπολογιστές, εκτυπωτές, μεταγωγείς και την συγκεκριμένη καλωδίωση η οποία συνδέει αυτές τις συσκευές μεταξύ τους (Odom, 2013b).

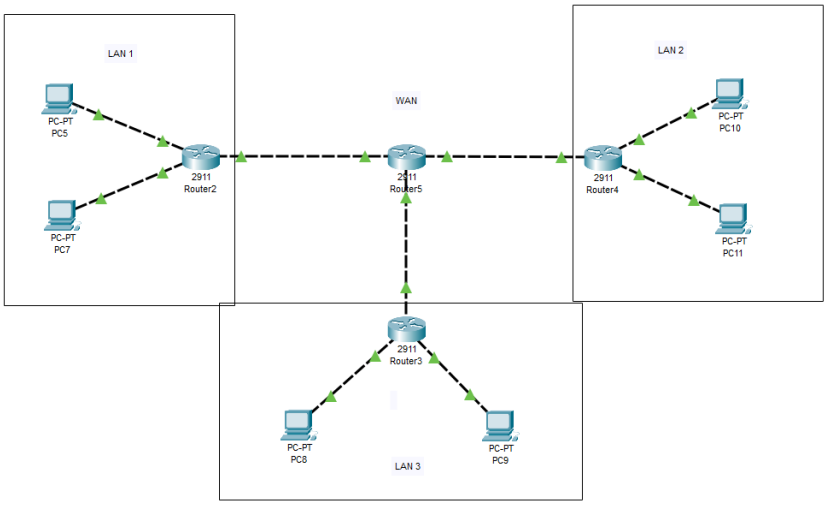


Εικόνα 6. Soho Lan
Πηγή: https://www.internold.com/lesson/fundamentals-of-ethernet-lans/

Κατά αυτόν τον τρόπο σε ένα τυπικό SOHO LAN παρατηρούμε ότι 4 συσκευές (3 υπολογιστές και ένας εκτυπωτής) είναι συνδεδεμένες σε ένα μεταγωγέα και εκείνος με την σειρά του συνδέεται σε ένα δρομολογητή. Σε αυτό το σημείο αξίζει να σημειωθεί, ότι μερικές από τις πιο δημοφιλείς LAN τεχνολογίες είναι το Ethernet, Token Ring και FDDI. Από τα επικρατέστερα θεωρείται το Ethernet, το οποίο κατέχει ιδιαίτερη θέση στον χώρο των LAN.

1.4.2 Wan

Ο όρος Wan (Wide area network) χρησιμοποιείται για να περιγράψει ένα δίκτυο το οποίο συνδέει διάφορα δίκτυα LAN. Στην παρακάτω εικόνα απεικονίζονται τρία δίκτυα LAN τα οποία συνδέονται μεταξύ τους δημιουργώντας έτσι ένα WAN.



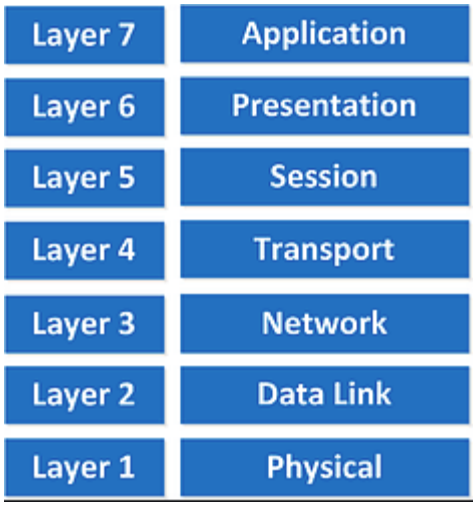
Εικόνα 7. Τοπολογία Wan
Πηγή: https://study-ccna.com/wide-area-network/

Όπως παρατηρούμε έχουν δημιουργηθεί 3 LAN, το 1,2 και 3 όπου το καθένα βρίσκεται σε διαφορετικές τοποθεσίες. Επίσης, φαίνεται πως έχει δημιουργηθεί και ένα WAN το οποίο συνδέει τα τρία αυτά LAN. Η κύρια διαφορά του LAN με το WAN, είναι ότι το δεύτερο το προμηθεύεται η εταιρία από τον πάροχο (ISP). Κάποια είδη τεχνολογιών WAN είναι το Frame Relay, ATM και το X.25.

Είναι σκόπιμο να γίνει αναφορά στο MAN (Metropolitan area network).Ο λόγος είναι, πως πρόκειται για ένα δίκτυο υπολογιστών, το οποίο συνήθως είναι μεγαλύτερο από ένα LAN και μικρότερο από ένα WAN. Ένα παράδειγμα για το εν λόγω είδος δικτύου αποτελεί η σύνδεση δύο εταιρικών γραφείων μέσα στην ίδια πόλη.

1.5 Μοντέλο αναφοράς OSI model

Στον χώρο της δικτύωσης αρκετές φορές συναντάται το μοντέλο αναφοράς OSI (open systems interconnection). Το συγκεκριμένο μοντέλο δημιουργήθηκε από τον διεθνή οργανισμό τυποποίησης (ISO – International organization for standardization) με σκοπό την περιγραφή των λειτουργιών ενός τηλεπικοινωνιακού συστήματος. Πιο συγκεκριμένα, το μοντέλο αυτό περιγράφει τον τρόπο με τον οποίο διάφορες διαδικτυακές εφαρμογές μπορούν να επικοινωνήσουν μεταξύ τους με την χρήση πρωτοκόλλων (Odom, 2013a). Το μοντέλο OSI έχει 7 επίπεδα, όπως φαίνεται παρακάτω.



Εικόνα 8. Μοντέλο OSI

Πηγή : https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/introduction-to-the-osi-model

- Επίπεδο 1, φυσικό: Το φυσικό επίπεδο είναι αυτό που καθορίζει πώς θα πραγματοποιηθεί η ανταλλαγή των δεδομένων (bits) από μία συσκευή στην άλλη. Επίσης περιγράφει τον τρόπο με τον οποίο λειτουργεί η καλωδίωση των συσκευών, οι συνδετήρες (connectors) και οι κάρτες δικτύου διεπαφών (Μαργαρίτη & Στεργίου , 2006).

- Επίπεδο 2, σύνδεσης δεδομένων: Το συγκεκριμένο επίπεδο είναι υπεύθυνο για την επικοινωνία μεταξύ των συσκευών. Σε αυτό το επίπεδο γίνεται η ενθυλάκωση των πακέτων σε ένα πλαίσιο. Κάθε πλαίσιο περιέχει μία κεφαλίδα (header) και ένα τρέιλερ (trailer). Στην κεφαλίδα συνήθως βρίσκεται η MAC διεύθυνση του αποστολέα και του παραλήπτη. Στο τρέιλερ περιλαμβάνεται το πεδίο εντοπισμού λαθών (Frame check sequence – FCS), το οποίο είναι υπεύθυνο για την ανίχνευση σφαλμάτων μετάδοσης. Το επίπεδο σύνδεσης δεδομένων χωρίζεται σε δύο υποεπίπεδα:
    - Υποεπίπεδο ελέγχου λογικού συνδέσμου (Logical Link Control): Χρησιμοποιείται για τον έλεγχο της κίνησης και τον εντοπισμό λαθών (Μαργαρίτη & Στεργίου , 2006).
    - Υποεπίπεδο ελέγχου πρόσβασης πολυμέσων (Media access control): Ασχολείται με τον πραγματικό έλεγχο των μέσων.

- Επίπεδο 3, δικτύου: Αυτό το επίπεδο περιγράφει τρεις βασικές λειτουργίες, τη λογική διευθυνσιοδότηση, τη δρομολόγηση πακέτων και την αξιολόγηση της καλύτερης διαδρομής. Ειδικότερα, η λογική διευθυνσιοδότηση καθορίζει τον τρόπο με τον οποίο κάθε συσκευή μπορεί να έχει μία IP διεύθυνση, η οποία χρησιμοποιείται κατά τη διαδικασία δρομολόγησης. Η δρομολόγηση πακέτων αναφέρεται στην διαδικασία με την οποία τα πακέτα δρομολογούνται με σκοπό να φτάσουν στον προορισμό τους. Τέλος, η αξιολόγηση της καλύτερης διαδρομής περιγράφει τον τρόπο με τον οποίο τα πρωτόκολλα δρομολόγησης μαθαίνουν όλες τις πιθανές διαδρομές και επιλέγουν την καλύτερη (Odom, 2013b).

- Επίπεδο 4, μεταφοράς: Το επίπεδο μεταφοράς είναι υπεύθυνο για την σύνδεση δύο τερματικών σταθμών και για την ομαλή μεταφορά των πακέτων. Πιο συγκεκριμένα, τμηματοποιεί τα πακέτα που δέχεται από το επίπεδο συνδιάλεξης, εξασφαλίζοντας τη σωστή διανομή τους. Επιπλέον σε αυτό το επίπεδο γίνεται και ο έλεγχος ροής των πακέτων από το ένα άκρο στο άλλο (McQuerry, 2004).

- Επίπεδο 5, συνδιάλεξης: Αυτό το επίπεδο καθορίζει την αρχή και το τέλος μιας επικοινωνίας μεταξύ δύο συστημάτων. Για παράδειγμα, εάν ένας υπολογιστής θέλει να επικοινωνήσει με έναν άλλον υπολογιστή, το επίπεδο συνδιάλεξης είναι υπεύθυνο για την διασφάλιση της επικοινωνίας τους (Doherty, Anderson, & Maggiora, 2010).

- Επίπεδο 6, παρουσίασης: Το επίπεδο αυτό είναι υπεύθυνο για την μορφοποίηση των δεδομένων ώστε να σταλούν με επιτυχία στον διαδίκτυο. Πιο συγκεκριμένα, είναι αρμόδιο για την κρυπτογράφηση και αποκρυπτογράφηση, για την συμπίεση και την αποσυμπίεση, καθώς και για την μετάφραση του περιεχομένου ενός μηνύματος (Simoneau, 2006).

- Επίπεδο 7, εφαρμογής: Το επίπεδο εφαρμογής βρίσκεται πιο κοντά στον χρήστη σε σχέση με όλα τα προηγούμενα. Σε αυτό το σημείο αναφερόμαστε στις ίδιες τις εφαρμογές και πώς αυτές λειτουργούνε μεταξύ τους (Odom, 2013b).

Σε αυτό το σημείο αξίζει να ειπωθεί ότι όλα τα επίπεδα επικοινωνούνε μεταξύ τους. Πιο αναλυτικά, τα επίπεδα 5-7 θεωρούνται επίπεδα εφαρμογής καθώς είναι αυτά που έχουν άμεση σχέση με τον χρήστη και είναι υπεύθυνα για την διασφάλιση της επικοινωνίας τους. Τα υπόλοιπα επίπεδα, από το 1-4 θεωρούνται επίπεδα ροής καθώς είναι υπεύθυνα για τον τρόπο με τον οποίο τα δεδομένα μεταφέρονται από τον ένα χρήστη στον άλλο και για τα πρωτόκολλα που χρησιμοποιούνται. Συνοψίζοντας, όταν ένας χρήστης δέχεται μία πληροφορία από έναν άλλο, η πληροφορία ξεκινάει από το επίπεδο 1 σε μορφή bit μέχρι και το επίπεδο 7 σε μορφή κατάλληλη έτσι ώστε να είναι κατανοητό το περιεχόμενο του μηνύματος από τον χρήστη. Η ίδια διαδικασία επαναλαμβάνεται συνεχώς μέχρι να τερματιστεί η σύνδεσή τους (Doherty, Anderson, & Maggiora, 2010).

Στην παρακάτω εικόνα αποτυπώνονται ξεχωριστά τα επίπεδα του μοντέλου αναφοράς OSI καθώς τα πρωτόκολλα και οι συσκευές που τα απαρτίζουν.

Layer Name	Protocols and Specifications	Devices
Application, presentation, session (Layers 5–7)	Telnet, HTTP, FTP, SMTP, POP3, VoIP, SNMP	Hosts, firewalls
Transport (Layer 4)	TCP, UDP	Hosts, firewalls
Network (Layer 3)	IP	Router
Data link (Layer 2)	Ethernet (IEEE 802.3), HDLC	LAN switch, wireless access point, cable modem, DSL modem
Physical (Layer 1)	RJ-45, Ethernet (IEEE 802.3)	LAN hub, LAN repeater, cables

Εικόνα 9. Μοντέλο OSI (1)[2]
Πηγή: (Odom, (2013)

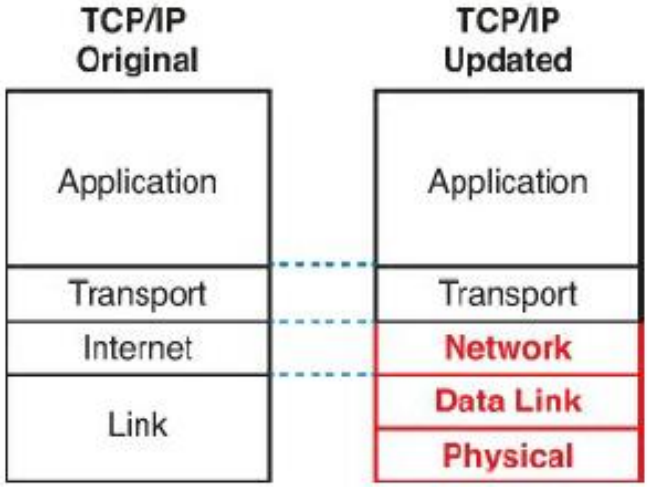
1.6 Μοντέλο TCP/IP

Λίγο αργότερα ήρθε και η δημιουργία του μοντέλου TCP/IP. Όπως και το μοντέλο OSI έτσι και το TCP/IP περιγράφει τα διάφορα στάδια σχεδιασμού και εφαρμογής των πρωτοκόλλων. Αρχικά το συγκεκριμένο πρωτόκολλο σχεδιάστηκε με

[2] Περισσότερες πληροφορίες για τις συσκευές των επιπέδων 1,2,3 αντίστοιχα ανήκουν οι συσκευές ομφαλός, μεταγωγέας, δρομολογητής βλέπε στο κεφάλαιο 1.2

4 επίπεδα ενώ στην συνέχεια διαμορφώθηκε άλλο ένα για την καλύτερη κατανόησή του (Odom, 2013b).

Στην εικόνα αριστερά παρατηρούμε το αρχικά μοντέλο ενώ στην εικόνα δεξιά το αναβαθμισμένο.



Εικόνα 10. Μοντέλο TCP/IP
Πηγή: https://certwhiz.com/2016/06/16/100-105-icnd1-video-series-1-1-compare-and-contrast-osi-and-tcpip-models-part-1/

Όπως φαίνεται στην παραπάνω εικόνα στο αναβαθμισμένο TCP/IP τα πρώτα τέσσερα επίπεδα είναι ίδια με το μοντέλο OSI. Παρατηρούμε όμως πως το επίπεδο της συνδιάλεξης και της παρουσίασης έχουν καταργηθεί. Αυτό προκύπτει για τον λόγο ότι τα δύο αυτά επίπεδα δεν χρειάζονται (Tanenbaum & Wetherall, 2011)

OSI Layer Equivalent	TCP/IP Layer	TCP/IP Protocol Examples
Application, session, presentation	Application	NFS, NIS, DNS, LDAP, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP,
Transport	Transport	TCP, UDP, SCTP
Network	Internet	IPv4, IPv6, ARP, ICMP
Data link	Data link	PPP, IEEE 802.2
Physical	Physical network	Ethernet (IEEE 802.3), Token Ring, RS-232, FDDI, and others

Εικόνα 11. Σύγκριση μοντέλου OSI και TCP/IP
Πηγή: (Odom, (2013)

1.6.1 Σουίτα πρωτοκόλλων TCP/IP

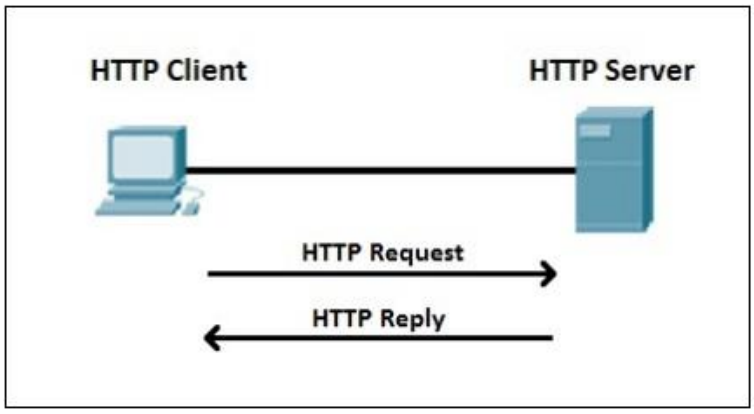
Σε αυτό το σημείο θα γίνει η επεξήγηση κάποιων πρωτοκόλλων της σουίτας TCP/IP τα οποία χρησιμοποιούνται και στην τοπολογία που θα δημιουργήσουμε στην συνέχεια της εργασίας.

1.6.1.1 DNS

Το πρωτόκολλο DNS (Domain Name System), όπως φαίνεται και στο παραπάνω σχήμα, είναι πρωτόκολλο του επιπέδου εφαρμογής. Χρησιμοποιείται για την μετάφραση των IP διευθύνσεων στα αντίστοιχα ονόματα διάφορων ιστοσελίδων (Cisco, 2020). Πιο συγκεκριμένα, όταν ο χρήστης θέλει να συνδεθεί σε μία ιστοσελίδα (π.χ. www.cisco.com) στέλνει ένα αίτημα με την βοήθεια του πρωτοκόλλου DNS σε έναν DNS server στον οποίο είναι καταχωρημένες διάφορες IP διευθύνσεις με τα αντίστοιχα ονόματα ιστοσελίδων. Ο DNS server βλέπει αν υπάρχει η συγκεκριμένη ιστοσελίδα με την αντίστοιχη IP διεύθυνση στην βάση δεδομένων του και συνδέει τον χρήστη. Ο σχεδιασμός του συγκεκριμένου πρωτοκόλλου αποσκοπεί στην διευκόλυνση του χρήστη ώστε να μην χρειάζεται να θυμάται τις IP διευθύνσεις κάθε ιστοσελίδας (π.χ. 216.58.207.206) (Odom, 2013b). Συνεπώς, έχει να θυμάται μόνο το όνομα της ιστοσελίδας (π.χ. www.google.com).

1.6.1.2 HTTP

Το πρωτόκολλο HTTP (HyperText Transfer Protocol) ανήκει στο επίπεδο εφαρμογής. Είναι ένα πρωτόκολλο μεταξύ πελάτη-εξυπηρετητή (client-server). Ο σκοπός του συγκεκριμένου πρωτοκόλλου είναι να παρέχει στον χρήστη τον ιστότοπο που επιθυμεί. Πιο συγκεκριμένα, όταν ο χρήστης επιθυμεί να συνδεθεί σε μία συγκεκριμένη σελίδα στέλνει μία αίτηση (request) στον εξυπηρετητή και εκείνος του δίνει πρόσβαση με ένα μήνυμα απόκρισης (respond). Για την καλύτερη κατανόηση του θέματος παρακάτω παρατίθεται μία εικόνα για την σύνδεση μεταξύ πελάτη και εξυπηρετητή (Kurose & Ross, 2017).



Εικόνα 12. Επικοινωνία HTTP client με HTTP server
Πηγή: https://study-ccna.com/dhcp-dns/

1.6.1.3 HTTPS

Το πρωτόκολλο HTTPS (HyperText Transfer Protocol Secure) παρομοιάζεται με το HTTP αλλά χαρακτηρίζεται από μεγαλύτερη ασφάλεια. Πιο συγκεκριμένα, με τη χρήση της κρυπτογράφησης ενεργοποιεί μία ασφαλέστερη επικοινωνία μεταξύ χρήστη και εξυπηρετητή. Για την κρυπτογράφηση χρησιμοποιείται το πρωτόκολλο SSL (Secure Sockets Layer) (Cisco, 2020).

Εικόνα 13. Παράδειγμα HTTPS
Πηγή: https://www.howtogeek.com/181767/htg-explains-what-is-https-and-why-should-i-care/

1.6.1.4 TELNET

Το TELNET είναι πρωτόκολλο του επιπέδου εφαρμογής. Χρησιμοποιείται για τη σύνδεση ενός χρήστη με μία απομακρυσμένη συσκευή. Αυτή η συσκευή μπορεί να είναι ένας εξυπηρετητής ή ακόμη και ένας δρομολογητής. Συνήθως, χρησιμοποιείται από τους διαχειριστές για να αποκτήσουν απομακρυσμένη πρόσβαση και να τροποποιήσουν τις συσκευές. Ένα από τα κύρια μειονεκτήματα του συγκεκριμένου πρωτοκόλλου είναι η έλλειψη ασφάλειας, καθώς τα δεδομένα που μεταφέρονται από τον χρήστη προς την απομακρυσμένη συσκευή δεν είναι κρυπτογραφημένα (Garrett, 2006).

1.6.1.5 SSH

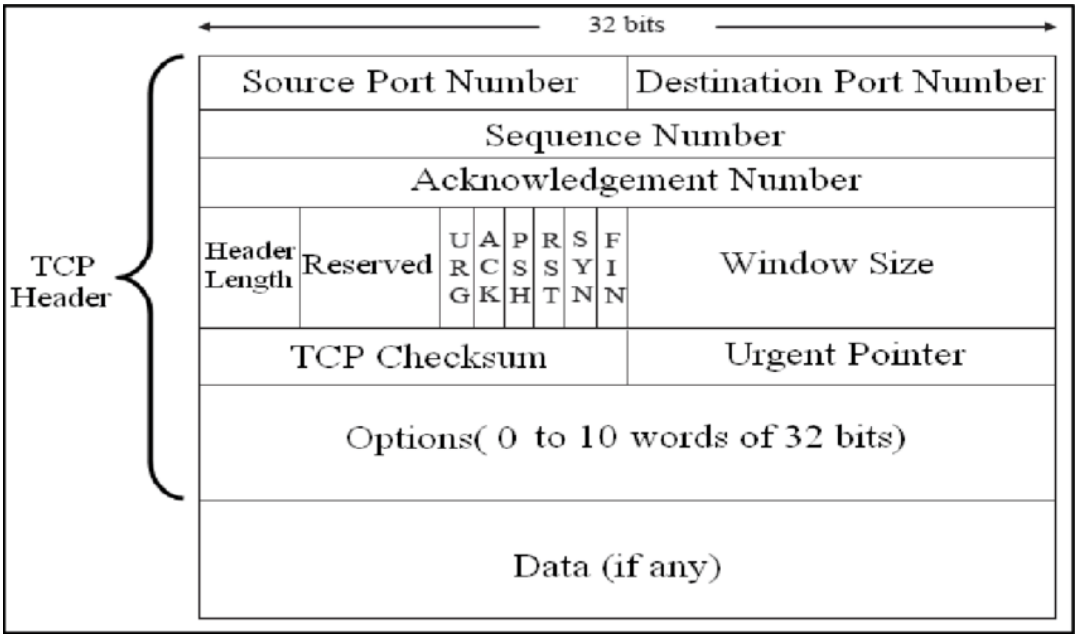
Το SSH είναι πρωτόκολλο του επιπέδου εφαρμογής. Είναι μία προτιμότερη εναλλακτική του TELNET καθώς προστατεύει τα δεδομένα του χρήστη από διάφορες επιθέσεις και παρέχοντας ασφάλεια στην μεταφορά των αρχείων (Garrett, 2006).

1.6.1.6 TCP

Ένα από τα βασικά πρωτόκολλα της σουίτας πρωτοκόλλων TCP/IP είναι το πρωτόκολλο TCP (Transmission Control Protocol). Το συγκεκριμένο πρωτόκολλο παρέχει αξιόπιστη και διατετμημένη μεταφορά των δεδομένων μεταξύ των εφαρμογών που χρησιμοποιούν οι χρήστες. Βρίσκεται στο επίπεδο μεταφοράς και χρησιμοποιείται από εφαρμογές που απαιτούν υψηλή αξιοπιστία όπως SSH, HTTP, HTTPS, FTP. Το πρωτόκολλο TCP είναι συνδεσμικό (connection-oriented), διότι πριν ξεκινήσει η διαδικασία αποστολής και λήψης δεδομένων, πρέπει πρώτα να πραγματοποιηθεί η σύνδεση μεταξύ των δύο χρηστών. Για να γίνει αυτό, στέλνονται συνολικά 3 πακέτα αναγνώρισης μεταξύ των δύο χρηστών. Αυτή η διαδικασία εγκαθίδρυσης της σύνδεσης ονομάζεται τριμερής χειραψία (three-way handshake).

Ένα ακόμη σημαντικό χαρακτηριστικό του TCP είναι η αξιοπιστία στην μεταφορά πακέτων. Το πρωτόκολλο TCP χρησιμοποιεί αριθμούς ακολουθίας για να αναγνωρίζει την σειρά με την οποία στέλνονται τα Bytes μεταξύ των δύο χρηστών. Αν ένα πακέτο χαθεί κατά την διάρκεια της αποστολής, τότε μπορεί να ξαναγίνει η αποστολή του (Odom, 2013b).

Στην παρακάτω εικόνα διακρίνουμε την δομή ενός TCP πακέτου.



Εικόνα 14. Δομή TCP
Πηγή: http://mars.netanya.ac.il/~unesco/cdrom/booklet/HTML/NETWORKING/node040.html

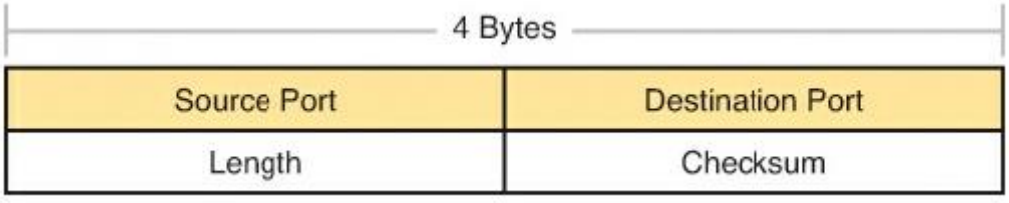
Αναλυτικότερα το τμήμα TCP αποτελείται από ένα πεδίο κεφαλίδας το οποίο έχει μέγεθος 20 Bytes και ένα πεδίο δεδομένων που συνήθως έχει μέγεθος 1 Byte.

- Source port number (αριθμός θύρας προέλευσης): Η θύρα προέλευσης έχει μέγεθος 16-bit και σε αυτή βρίσκεται ο αριθμός θύρας του χρήστη που στέλνει τα δεδομένα.
- Destination port number (αριθμός θύρας προορισμού): Η θύρα προορισμού έχει μέγεθος 16-bit και σε αυτή βρίσκεται ο αριθμός θύρας του χρήστη που λαμβάνει τα δεδομένα.
- Sequence number (αριθμός ακολουθίας): Έχει μέγεθος 32-bit και χρησιμοποιείται για να αναγνωρίσει κάθε Byte δεδομένων.
- Acknowledgment number (αριθμός επιβεβαίωσης): Έχει μέγεθος 32-bit και σε αυτόν βρίσκεται ο επόμενος αριθμός ακολουθίας που περιμένει ο παραλήπτης.
- Header length (μήκος κεφαλίδας): Έχει μέγεθος 4-bit και καθορίζει το μέγεθος της κεφαλίδας TCP.
- Reserved: Το πεδίο αυτό έχει μέγεθος 6-bit και είναι αχρησιμοποίητο.

- Flag Field (πεδίο σημαίας): Αυτό το πεδίο έχει μέγεθος 6-bit και σε αυτό βρίσκονται τα URG, ACK, PSH, RST, SYN, FIN τα οποία είναι υπεύθυνα για την εγκαθίδρυση και τον τερματισμό της σύνδεσης.
- Window size (μέγεθος παραθύρου): Έχει μέγεθος 16-bit και καθορίζει τον αριθμό των byte που ο αποστολέας είναι διατεθειμένος να δεχτεί.
- TCP checksum (πεδίο αθροίσματος κειμένου): Έχει μέγεθος 16-bit και είναι υπεύθυνο για τον έλεγχο λαθών της κεφαλίδας και των δεδομένων.
- Urgent pointer (δείκτης επειγόντων δεδομένων): Αυτός ο δείκτης έχει μέγεθος 16-bit και προστίθεται στο τέλος των επειγόντων δεδομένων για να ενημερώσει το παραλήπτη ότι υπάρχουν επείγοντα δεδομένα.
- Options (επιλογές): Σε αυτό το πεδίο βρίσκονται διάφορες επιλογές όπως το μέγιστο μέγεθος τμήματος (Maximum segment size – MSS) (Kurose & Ross, 2017).

1.6.1.7 UDP

Το UDP είναι ένα πρωτόκολλο μεταφοράς, σαν το TCP, και ανήκει στο επίπεδο μεταφοράς. Συγκριτικά με το TCP, το UDP είναι ασυνδεσμικό που σημαίνει ότι δεν εφαρμόζει κάποιου είδους σύνδεσης πριν την μεταφορά των δεδομένων, δεν παρέχει αξιοπιστία κατά την μεταφορά τους και δεν τμηματοποιεί τα δεδομένα σε κατάλληλα μεγέθη. Γι' αυτό τον λόγο το UDP χρησιμοποιεί κεφαλίδα των 8 Bytes σε αντίθεση με την κεφαλίδα του TCP, η οποία αποτελείται από 20 Bytes. Οι εφαρμογές που χρησιμοποιούν το πρωτόκολλο UDP είτε δεν έχουν πρόβλημα να χαθούν δεδομένα, είτε διαθέτουν κάποιο μηχανισμό ανάκτησης των χαμένων πακέτων. Για παράδειγμα, το VoIP (Voice over IP) χρησιμοποιεί το πρωτόκολλο UDP διότι αν χαθεί κάποιο πακέτο φωνής, μέχρι να αναμεταδοθεί το πακέτο θα έχει προκληθεί μεγάλη καθυστέρηση με αποτέλεσμα η συνομιλία να είναι δυσνόητη. Στην παρακάτω εικόνα διακρίνουμε την κεφαλίδα του UDP.



Εικόνα 15. Δομή UDP
Πηγή: (Odom, (2013)

Όπως παρατηρούμε η κεφαλίδα αποτελείται μόνο από τέσσερα πεδία: Source port (θύρα προέλευσης), Destination port (θύρα προορισμού), Length (μέγεθος κεφαλίδας και δεδομένων) και Checksum (πεδίο διόρθωσης λαθών) (Odom, 2013b).

1.7 IP διευθύνσεις και MAC διευθύνσεις

Για να μπορούν να επικοινωνούν οι υπολογιστές χρειάζονται κάποιου είδους ταυτότητας-διεύθυνσης έτσι ώστε να αναγνωρίζονται μεταξύ τους. Κάθε υπολογιστής έχει δύο διευθύνσεις την IP και την MAC (Doherty, Anderson, & Maggiora, 2010).

Η IP διεύθυνση είναι ένας αριθμός με τον οποίο αναγνωρίζεται ο χρήστης στο διαδίκτυο. Κάθε συσκευή που επιθυμεί να επικοινωνήσει με μία άλλη στο δίκτυο πρέπει να έχει διαμορφωμένη μία IP διεύθυνση (Tanenbaum & Wetherall, 2011). Υπάρχουν δύο είδη IP διευθύνσεων, οι ιδιωτικές και οι δημόσιες.

Οι ιδιωτικές διευθύνσεις χρησιμοποιούνται για να επικοινωνήσουν οι χρήστες μέσα στο ίδιο δίκτυο. Για παράδειγμα στην τοπολογία που έχουμε δημιουργήσει παρακάτω το δίκτυο μας έχει την ιδιωτική διεύθυνση 192.168.5.0. Το εύρος των ιδιωτικών διευθύνσεων είναι το εξής:

10.0.0.0 – 10.255.255.255 κλάση A

172.16.0.0 – 172.31.255.255 κλάση B

192.168.0.0 – 192.168.255.255 κλάση C

Οι δημόσιες διευθύνσεις χρησιμοποιούνται για να επικοινωνήσουν οι χρήστες έξω από το ίδιο δίκτυο, στο διαδίκτυο (Odom, 2013b).

Η διεύθυνση MAC είναι ένας αριθμός ο οποίος ορίζεται από τον κατασκευαστή και είναι μοναδικός για κάθε συσκευή. Η διεύθυνση MAC αποτελείται από 12 δεκαεξαδικά ψηφία όπως για παράδειγμα, D9-D5-84-EB-12-A3 (Doherty, Anderson, & Maggiora, 2010).

1.7.1 Κλάσεις των IP διευθύνσεων

Στις IP διευθύνσεις υπάρχουν 5 κλάσεις: η κλάση A, η κλάση B, η κλάση C, η κλάση D και η κλάση E. Οι κλάσεις από την A έως και την C χρησιμοποιούνται για τους υπολογιστές υπηρεσίας (hosts). Οι κλάσεις D και E χρησιμοποιούνται για τις διευθύνσεις πολλαπλής διανομής (multicast) και για πειραματικούς σκοπούς αντίστοιχα. Όπως θα παρατηρήσουμε στην παρακάτω εικόνα η κάθε κλάση έχει δημιουργηθεί με βάση το μέγεθος του δικτύου.

Class	First Octet Values	Purpose
A	1–126	Unicast (large networks)
B	128–191	Unicast (medium-sized networks)
C	192–223	Unicast (small networks)
D	224–239	Multicast
E	240–255	Experimental

Εικόνα 16. Κλάσεις δικτύων
Πηγή: (Odom, (2013)

Όπως παρατηρούμε, η κλάση A απευθύνεται σε μεγάλου μεγέθους δίκτυα, η B σε μεσαίου μεγέθους δίκτυα και η C για μικρά δίκτυα. (Odom, 2013b)

Η παρακάτω εικόνα θα μας βοηθήσει να κατανοήσουμε καλύτερα πως λειτουργούν οι IP διευθύνσεις.

	Class A	Class B	Class C
First octet range	1 – 126	128 – 191	192 – 223
Valid network numbers	1.0.0.0 – 126.0.0.0	128.0.0.0 – 191.255.0.0	192.0.0.0 – 223.255.255.0
Total networks	$2^7 - 2 = 126$	$2^{14} = 16{,}384$	$2^{21} = 2{,}097{,}152$
Hosts per network	$2^{24} - 2$	$2^{16} - 2$	$2^8 - 2$
Octets (bits) in network part	1 (8)	2 (16)	3 (24)
Octets (bits) in host part	3 (24)	2 (16)	1 (8)
Default mask	255.0.0.0	255.255.0.0	255.255.255.0

Εικόνα 17. Ανάλυση κλάσεων δικτύων
Πηγή: (Odom, (2013)

Όπως παρατηρούμε, κάθε μία κλάση αντιπροσωπεύει ένα συγκεκριμένο εύρος IP διευθύνσεων, τον αριθμό των δικτύων καθώς και τον αριθμό των υπολογιστών υπηρεσίας (hosts), δηλαδή τον αριθμό των υπολογιστών που μπορούν να διαθέσουν μία IP διεύθυνση. Πιο συγκεκριμένα, η κλάση Α μπορεί να χωριστεί σε 126 διαφορετικά δίκτυα, με αποτέλεσμα να μένουν 16.777.214 (24-bit) IP διευθύνσεις διαθέσιμες για τους χρήστες. Η κλάση Β μπορεί να χωριστεί σε 16,384 (2^{16}) δίκτυα που σημαίνει ότι 65.534 (16-bit) διαθέσιμες IP μένουν για τους χρήστες. Τέλος, η κλάση C χωρίζεται σε 2.097.152 (2^{24}) δίκτυα που σημαίνει ότι μόνο 254 (8-bit) διαθέσιμες IP μένουν για τους χρήστες (Odom, 2013b).

1.7.2 Μάσκα Υποδικτύου

Μία IP διεύθυνση, όπως προαναφέραμε, χωρίζεται σε δύο μέρη: Το μέρος του δικτύου και το μέρος των υπολογιστών υπηρεσίας (hosts). Για παράδειγμα, στην κλάση C το μέρος του δικτύου αποτελείται από 24 bits ενώ το μέρος των υπολογιστών υπηρεσίας από 8 bits. Αυτό συμβαίνει διότι η προεπιλεγμένη μάσκα υποδικτύου είναι η 255.255.255.0. Αναλυτικότερα, όπως και οι IP διευθύνσεις, οι μάσκες υποδικτύου αποτελούνται από 32 bits (Odom, 2013b). Η κάθε μία κλάση έχει και την δική της προεπιλεγμένη μάσκα υποδικτύου. Η Α την 255.0.0.0 (/8), η Β την 255.255.0.0 (/16) και η C την 255.255.255.0 (/24)[3] (Doherty, Anderson, & Maggiora, 2010). Για παράδειγμα, στην τοπολογία που έχουμε δημιουργήσει πιο κάτω χρησιμοποιούμε την IP διεύθυνση 192.168.5.0, η οποία όμως χωρίζεται σε αρκετά υποδίκτυα. Ο διαχωρισμός αυτός αποσκοπεί στην εξοικονόμηση των IP διευθύνσεων αλλά και στην μεγαλύτερη ασφάλεια, μιας και η κάθε περιοχή έχει το δικό της υποδίκτυο.

1.8 Εισαγωγή στις IPV6 Διευθύνσεις

Οι IPv6 διευθύνσεις είναι η νεότερη έκδοση των IPv4 διευθύνσεων. Δημιουργήθηκαν με σκοπό να λυθεί το πρόβλημα της ανεπάρκειας IPv4 διευθύνσεων. (Odom, 2013b). Εάν οι IPv4 διευθύνσεις με μέγεθος 32-bit είναι διαθέσιμες σε 4,294,967,296 υπολογιστές (2^{32}), οι IPv6 διευθύνσεις με μέγεθος 128-bit μπορούν να

[3] Το /8, /16, /24 ονομάζεται πρόθεμα (prefix) και υποδηλώνει το μέγεθος του δικτύου δηλαδή από πόσα bit αποτελείται το δίκτυο, βλέπε περισσότερα Doherty, Anderson, & Maggiora (2010)

διατεθούν σε περίπου 2^{128} υπολογιστές. Είναι εμφανές πως αυτός ο αριθμός είναι αρκετά μεγάλος. Η εναλλαγή από τις IPv4 διευθύνσεις γίνεται σταδιακά, ήδη κάποιες επιχειρήσεις χρησιμοποιούν τις IPv6 διευθύνσεις αντί των IPv4 (Doherty, Anderson, & Maggiora, 2010).

Κάποια από τα βασικότερα χαρακτηριστικά των IPv6 διευθύνσεων είναι τα ακόλουθα:

- Η αναβαθμισμένη ασφάλεια: Το IPsec το οποίο είναι πρωτόκολλο ασφάλειας είναι ενσωματωμένο στο IPv6 σε αντίθεση με το IPv4 που πρέπει να διαμορφώσει ο χρήστης.
- Δεν χρειάζεται NAT: Από την στιγμή που κάθε συσκευή έχει μία καθολική διεύθυνση δεν χρειάζεται το NAT[4].
- Αυτόματη διαμόρφωση διευθύνσεων: Οι συσκευές που χρησιμοποιούν IPv6 διευθύνσεις διαμορφώνουν από μόνες τους μία διεύθυνση IPv6 σε αντίθεση με τις IPv4 διευθύνσεις που χρειάζεται κάποιος DHCP εξυπηρετητής[5]. (Doherty, Anderson, & Maggiora, 2010)

1.8.1 Μορφή των IPv6

Όπως και στις IPv4 έτσι και οι IPv6 χωρίζονται σε δύο μέρη, στο μέρος του δικτύου το οποίο αποτελείται από τα πρώτα 64-bit και στο μέρος του υπολογιστή υπηρεσίας το οποίο αποτελείται από τα υπόλοιπα 64-bit, σύνολο 128-bit. Το πρόθεμα (prefix) είναι αυτό που χωρίζει το δίκτυο από τους υπολογιστές υπηρεσίας. Ένα παράδειγμα IPv6 διεύθυνσης είναι το εξής:

2008:0DB8:ACAD:00A1:0000:0000:0000:0001/64

Οι IPv6 διευθύνσεις διαμορφώνονται από 8 ομάδες τεσσάρων δεκαεξαδικών αριθμών. Η συγκεκριμένη διεύθυνση για λόγους συντόμευσης αναπαρίσταται εναλλακτικά και με αυτόν τον τρόπο:

[4] Η χρησιμότητα του NAT αναφέρεται στο κεφάλαιο 4.2

[5] Η χρησιμότητα του DHCP εξυπηρετητή έχει αναφερθεί στο κεφάλαιο 4.4

2008:DB8:ACAD:A1:0000:0000:0000:1/64

Για να αφαιρέσουμε τα μηδενικά μπορούμε να προσθέσουμε στο σύμβολο της άνω κάτω τελείας (::)

2008:DB8:ACAD:A1::1/64

Αυτός ο τρόπος είναι ο συνηθέστερος και ο πιο σύντομος (Doherty, Anderson, & Maggiora, 2010).

1.8.2 IPv6 Link-local Διευθύνσεις

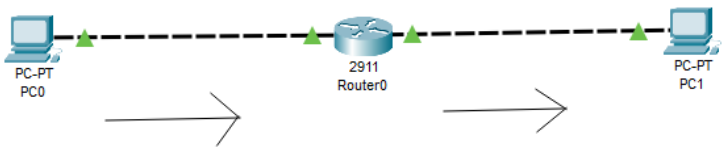
Οι Link-local είναι διευθύνσεις που χρησιμοποιούνται με σκοπό την εξερεύνηση των γειτονικών δικτύων. Διαμορφώνονται σε κάθε διεπαφή του δικτύου αλλά δεν προωθούν πακέτα. Κάθε υπολογιστής υπηρεσίας (host) μπορεί να διαμορφώσει είτε αυτόματα, είτε χειροκίνητα την Link-local διεύθυνση. (Odom, 2013b). Παρακάτω απεικονίζεται ένα παράδειγμα Link-local διεύθυνσης.

Εικόνα 18. Δομή Link-local
Πηγή: (Odom, (2013)

Κεφάλαιο 2 Στατική και Δυναμική Δρομολόγηση

2.1 IP δρομολόγηση

IP δρομολόγηση είναι η διαδικασία κατά την οποία ο χρήστης στέλνει πακέτα από ένα δίκτυο σε έναν χρήστη διαφορετικού δικτύου. Η διαδικασία αυτή συνήθως πραγματοποιείται από τους δρομολογητές. Πιο συγκεκριμένα, διαδραματίζουν τον ρόλο του ελέγχου του προορισμού του πακέτου και στην συνέχεια προωθούν το πακέτο (McQuerry, 2004). Ένα απλό παράδειγμα δρομολόγησης απεικονίζεται παρακάτω.

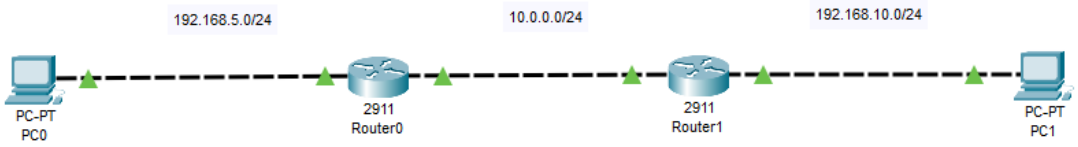


Εικόνα 19. IP Δρομολόγηση
Πηγή: https://study-ccna.com/what-is-ip-routing/

Στο συγκεκριμένο παράδειγμα ο υπολογιστής PC0 θέλει να επικοινωνήσει με τον υπολογιστή PC1. Στέλνει ένα πακέτο στον δρομολογητή εκείνος βλέπει ότι ο προορισμός του πακέτου βρίσκεται στον πίνακα δρομολόγησης και προωθεί το πακέτο στον PC1. Η ίδια διαδικασία γίνεται και αντιστρόφως.

2.1.1 Στατική δρομολόγηση

Με την στατική δρομολόγηση ένα πακέτο μεταφέρεται από έναν υπολογιστή-πηγή σε έναν υπολογιστή-προορισμός μέσω μιας συγκεκριμένης διαδρομής (Cisco, 2020). Με την προσθήκη στατικής δρομολόγησης, ένας δρομολογητής μπορεί να μάθει την διαδρομή για ένα απομακρυσμένο δίκτυο το οποίο δεν είναι άμεσα συνδεδεμένο σε κάποια από τις διεπαφές του (Dayle & Carroll, 2006). Στην παρακάτω εικόνα διακρίνουμε ένα παράδειγμα στατικής δρομολόγησης.



Εικόνα 20. Στατική Δρομολόγηση
Πηγή: https://linuxtiwary.com/2015/06/27/cisco-packet-tracer-labconfiguring-static-routing-using-three-routers/

Ας υποθέσουμε ότι ο υπολογιστής PC0 θέλει να επικοινωνήσει με τον υπολογιστή PC1. Απ' ότι φαίνεται όμως ο συγκεκριμένος υπολογιστής βρίσκεται σε δίκτυο το οποίο δεν είναι άμεσα συνδεδεμένο με τον δρομολογητή που συνδέει τον υπολογιστή PC0. Γι' αυτό τον λόγο πρέπει να διαμορφώσουμε μία στατική

δρομολόγηση στον δρομολογητή Router0 με το δίκτυο 192.168.10.0, ώστε να μπορεί να επικοινωνεί ο PC0 με τον PC1.

2.1.2 Δυναμική δρομολόγηση

Για να πραγματοποιηθεί η δυναμική δρομολόγηση σε έναν δρομολογητή θα πρέπει να ενεργοποιηθεί κάποιο πρωτόκολλο δρομολόγησης. Τα πρωτόκολλα δρομολόγησης χρησιμοποιούνται μεταξύ των δρομολογητών για να ανταλλάξουν πληροφορίες οι οποίες τους είναι χρήσιμες για την δημιουργία των πινάκων δρομολόγησης. Οι πίνακες δρομολόγησης είναι απαραίτητοι για την σωστή προώθηση των πακέτων. Τα πλεονεκτήματα της δυναμικής δρομολόγησης συνοψίζονται στο γεγονός ότι δεν χρειάζεται να ορίσουμε χειροκίνητα κάθε διαδρομή και ότι εάν κάποια διαδρομή σταματήσει να λειτουργεί, αυτόματα το πρωτόκολλο δρομολόγησης θα επιλέξει την αμέσως επόμενη διαθέσιμη. Το μειονέκτημα της δυναμικής δρομολόγησης εντοπίζεται στο γεγονός ότι χρησιμοποιεί μεγάλη επεξεργαστική ισχύος σε έναν δρομολογητή καθώς πρέπει να επεξεργαστεί κάθε πληροφορία που λαμβάνει αλλά και τον ίδιο τον πίνακα δρομολόγησης (Malhotra, 2002).

2.2 Τύποι πρωτοκόλλων δρομολόγησης

Τα πρωτόκολλα δρομολόγησης χωρίζονται σε δύο διαφορετικούς τύπους: Στα Distance Vector και Link State.

2.2.1 Distance Vector

Τα πρωτόκολλα Distance Vector βασίζονται κυρίως στην απόσταση της καλύτερης διαδρομής σε ένα απομακρυσμένο δίκτυο. Στην περίπτωση των δικτύων η απόσταση θεωρείται ο αριθμός των αλμάτων (hops), δηλαδή δρομολογητών μέχρι το δίκτυο προορισμού. Γι' αυτό τον λόγο κάθε δρομολογητής μαθαίνει τις διαδρομές από τους γειτονικούς δρομολογητές μέχρι όλοι οι δρομολογητές να έχουν τις απαραίτητες πληροφορίες για την δρομολόγηση των πακέτων. Ένα χαρακτηριστικό των Distance

Vector πρωτοκόλλων είναι ότι στέλνουν ολόκληρο τον πίνακα δρομολόγησης σε κάθε γειτονικό δρομολογητή. Κάποια Distance Vector πρωτόκολλα δρομολόγησης είναι τα RIP και EIGRP (Doyle, 1998).

2.2.2 Link State

Τα πρωτόκολλα Link State σχεδιάστηκαν για τον ίδιο σκοπό με τα πρωτόκολλα Distance Vector, δηλαδή στον εντοπισμό της καλύτερης πιθανής διαδρομής σε ένα απομακρυσμένο δίκτυο, ωστόσο με διαφορετικό τρόπο. Η διαφορά τους εντοπίζεται στο γεγονός ότι σε αντίθεση με τα Distance Vector, τα Link State πρέπει να διαφημίσουν κάθε πιθανή πληροφορία σχετικά με το δίκτυο σε όλους τους δρομολογητές με αποτέλεσμα να έχουν τις ίδιες πληροφορίες (Cisco Networking Academy, 2014). Πιο συγκεκριμένα, αφού ενεργοποιηθεί το πρωτόκολλο δυναμικής δρομολόγησης, κάθε δρομολογητής στέλνει περιοδικά «hello» μηνύματα με σκοπό την αναγνώριση λειτουργικών ή μη δρομολογητών. Κάθε δρομολογητής δημιουργεί τρεις διαφορετικούς πίνακες δρομολόγησης και είναι οι εξής:

- Γειτονικός πίνακας: Διατίθενται πληροφορίες για τον κάθε γειτονικό δρομολογητή.
- Πίνακας τοπολογίας: Αποθηκεύεται η τοπολογία ολόκληρου του δικτύου.
- Πίνακας δρομολόγησης: Αποθηκεύονται οι καλύτερες διαδρομές για το δίκτυο.

Κάποια πρωτόκολλα Link State είναι τα OSPF και IS-IS.

2.2.3 Πρωτόκολλο δρομολόγησης RIP

Το πρωτόκολλο δυναμικής δρομολόγησης RIPv2 (version 2) ανήκει στα Distance Vector πρωτόκολλα. Αυτό σημαίνει πως βασίζεται στον αριθμό των αλμάτων (hop) και ο μέγιστος αριθμός τους είναι 15. Πιο συγκεκριμένα, εάν έχουμε ένα δίκτυο με 16 δρομολογητές και σε όλους είναι εφαρμοσμένο το πρωτόκολλο RIP τότε, ο πρώτος δρομολογητής με τον δέκατο έκτο δεν θα μπορούν να επικοινωνήσουν. Επίσης,

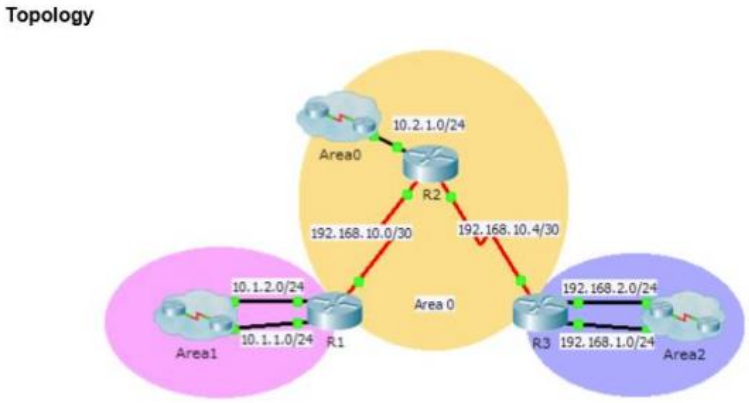
κάθε δρομολογητής στέλνει ενημερώσεις για την κατάστασή του κάθε 30 δευτερόλεπτα. Ένα μεγάλο χαρακτηριστικό του RIPv2 σε σύγκριση με το RIPv1 είναι ότι στο RIPv2 υπάρχει η δυνατότητα δημιουργίας VLSM (variable-length subnet mask) στο δίκτυό μας. (McQuerry, 2004)

2.2.4 Πρωτόκολλο δρομολόγησης OSPF

Το πρωτόκολλο δυναμικής δρομολόγησης OSPF θεωρείται το πιο δημοφιλές πρωτόκολλο link state. Οι δρομολογητές που έχουν ενεργοποιημένο το πρωτόκολλο OSPF, πριν ξεκινήσει η διαδικασία δρομολόγησης, πρέπει να «γνωριστούν» μεταξύ τους στέλνοντας μηνύματα «Hello». Στην συνέχεια κάθε δρομολογητής υπολογίζει την καλύτερη πιθανή διαδρομή με την χρήση ενός αλγορίθμου και την προσθέτει στον πίνακα δρομολόγησης. Κάθε δρομολογητής OSPF αποθηκεύει αυτές τις πληροφορίες σε τρεις πίνακες και είναι οι ακόλουθοι:

- Γειτονικός πίνακας: Διατίθενται πληροφορίες για τον κάθε γειτονικό δρομολογητή.
- Πίνακας τοπολογίας: Αποθηκεύεται η τοπολογία ολόκληρου του δικτύου.
- Πίνακας δρομολόγησης: Αποθηκεύονται οι καλύτερες διαδρομές για το δίκτυο.

Ένα ακόμη χαρακτηριστικό του συγκεκριμένου πρωτοκόλλου είναι η χρήση περιοχών (areas). Πιο συγκεκριμένα, η κάθε περιοχή αποτελείται από μία ομάδα δικτύων και δρομολογητών. Όλοι οι δρομολογητές της ίδιας περιοχής έχουν τον ίδιο πίνακα δρομολόγησης αλλά δεν γνωρίζουν πληροφορίες για τις άλλες περιοχές. Ο κύριος λόγος που δημιουργούνται οι περιοχές είναι για να μειωθεί το μέγεθος του πίνακα δρομολόγησης του κάθε δρομολογητή, έτσι ώστε να μην χρειάζεται να ενημερώνει όλο το δίκτυο για την κατάστασή του παρά μόνο την περιοχή που βρίσκεται. Στην παρακάτω εικόνα διακρίνουμε το πρωτόκολλο OSPF με διάφορες περιοχές (multiarea).



Εικόνα 21. OSPF Multi-Area
Πηγή: https://ccdtt.com/6-2-3-6-packet-tracer-configuring-multiarea-ospf/

Όπως παρατηρούμε υπάρχουν 3 διαφορετικές περιοχές η Area1, Area0, Area2. Σύμφωνα με όσα ειπώθηκαν πιο πάνω ο κάθε δρομολογητής γνωρίζει για την κατάσταση της περιοχής του και όχι για τις υπόλοιπες.

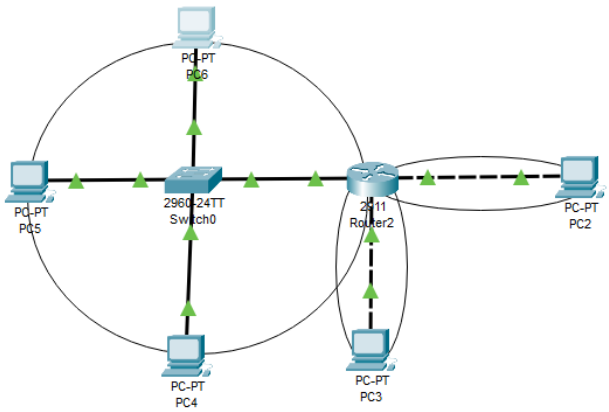
Κεφάλαιο 3 VLAN

3.1 Τι είναι ένα VLAN

Με απλά λόγια το VLAN (εικονικό Lan) είναι ένα υποδίκτυο στο οποίο μπορούν να συνδεθούν διάφορες συσκευές μεταξύ τους (Valentine & Whitaker, 2008). Ο παραπάνω ορισμός μοιάζει πολύ με τον ορισμό του Lan μόνο που εδώ αναφερόμαστε σε υποδίκτυα και όχι δίκτυα. Πιο συγκεκριμένα, σε ένα Lan μπορούν να βρίσκονται διάφορα VLAN τα οποία εξυπηρετούν τους εξής σκοπούς:

- Ασφάλεια: Ένας από τους κυριότερους λόγους που δημιουργούνται τα VLAN είναι η ασφάλεια. Για παράδειγμα, στο ένα VLAN μπορεί να υπάρχει ο τομέας της λογιστικής ενώ στο άλλο VLAN ο τομέας του εμπορίου. Η τοποθέτηση του κάθε τομέα σε ένα ξεχωριστό VLAN μας εξασφαλίζει την μέγιστη προστασία από διαρροές πληροφοριών (Tanenbaum & Wetherall, 2011).

- Περισσότεροι τομείς μετάδοσης (broadcast domains): Ένας τομέας μετάδοσης είναι ο τομέας στον οποίο προωθείται μία εκπομπή (broadcast), καθώς περιέχει όλες τις συσκευές που μπορούν να επικοινωνήσουν μεταξύ τους. Κάθε διεπαφή του μεταγωγέα περιέχει τον ίδιο τομέα μετάδοσης ενώ κάθε διεπαφή του δρομολογητή διαφορετικό. (Odom, 2013b) Η παρακάτω εικόνα βοηθάει στην κατανόηση της συγκεκριμένης έννοιας.

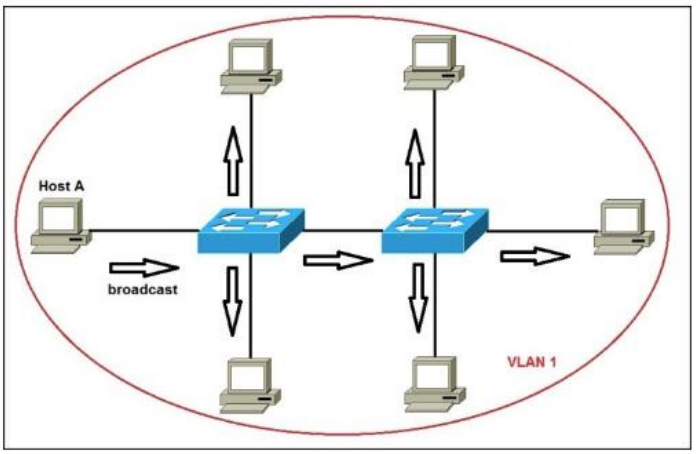


Εικόνα 22. Broadcast Domain
Πηγή: https://study-ccna.com/collision-broadcast-domain/

Όπως παρατηρούμε σε αυτή την εικόνα απεικονίζονται τρεις τομείς μετάδοσης, ένας για τις διεπαφές του μεταγωγέα και άλλοι δύο για κάθε διεπαφή του δρομολογητή.

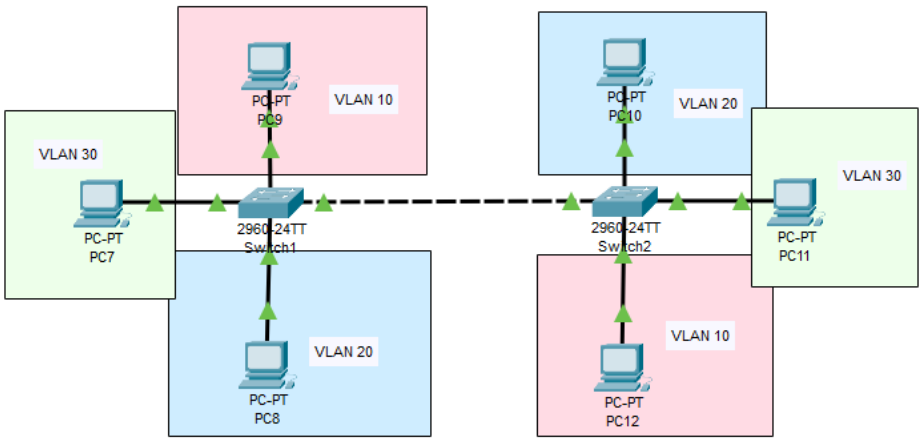
- Ευελιξία: Αντί να μεταφερθούν τα διάφορα τμήματα μιας εταιρίας σε άλλη τοποθεσία μπορούν απλά να ομαδοποιηθούν μέσω των VLAN παραμένοντας στην ίδια (Tanenbaum & Wetherall, 2011).

Στην παρακάτω εικόνα παρουσιάζεται ένα δίκτυο με ένα VLAN.



Εικόνα 23. Vlan 1
Πηγή: https://study-ccna.com/what-is-a-vlan/

Χωρίς πολλαπλά VLAN, μία εκπομπή (broadcast) στάλθηκε από τον HOST A σε όλο το δίκτυο αυξάνοντας την κίνηση και τον κίνδυνο ασφάλειας. Διαμορφώνοντας όμως διάφορα VLAN οι πληροφορίες που θέλουμε μένουν ασφαλείς χωρίς να προκαλούμε αυξημένη κίνηση στο δίκτυο.



Εικόνα 24. Πολλαπλά VLAN
Πηγή: https://study-ccna.com/what-is-a-vlan/

Όπως φαίνεται ο κάθε υπολογιστής επικοινωνεί μόνο με το δικό του VLAN χωρίς να έχει επικοινωνία με τα υπόλοιπα.

3.2 Access and Trunk Ports

Για να μπορέσει να λειτουργήσει το VLAN πρέπει να διαμορφωθούν με κατάλληλο τρόπο κάποιες διεπαφές ως θύρες πρόσβασης (access) και κάποιες ως θύρες κορμού (trunk).

- Οι θύρες πρόσβασης καθορίζονται σε κάθε ένα VLAN στις διεπαφές των μεταγωγών που είναι συνδεδεμένες με μία συσκευή
- Οι θύρες κορμού συνδέονται είτε από μεταγωγέα σε μεταγωγέα, είτε από μεταγωγέα σε δρομολογητή. Ο σκοπός τους είναι να μεταφέρουν τα δεδομένα από διάφορα VLAN μέσα από μία μόνο διεπαφή. (Tiso, 2014)

Στην παραπάνω εικόνα θύρες πρόσβασης θεωρούνται οι διεπαφές των μεταγωγών που συνδέονται με τους υπολογιστές, ενώ θύρες κορμού οι διεπαφές που συνδέουν τους δύο μεταγωγούς.

Κεφάλαιο 4 Οι λειτουργίες των ACL, NAT, PPP και DHCP

Σε αυτό το κεφάλαιο θα γίνει επεξήγηση των λιστών πρόσβασης (Access Lists), καθώς και των διάφορων τύπων και κατηγοριών που υπάρχουν. Στην συνέχεια θα αναλύσουμε την λειτουργία στατικού και δυναμικού NAT και PAT. Τέλος, θα γίνει μια αναφορά στην ενθυλάκωση PPP (Point-to-point protocol) με CHAP και PAP πιστοποίηση και στον τρόπο λειτουργίας του DHCP.

4.1 Τι είναι οι ACL

Οι λίστες πρόσβασης είναι ένα σύνολο κανόνων οι οποίοι ελέγχουν την κίνηση στο δίκτυο. Εφαρμόζονται στις διεπαφές των δρομολογητών για να φιλτράρουν είτε την εισερχόμενη, αλλά είτε και την εξερχόμενη κίνηση (Malik, 2003). Υπάρχουν δύο

τύποι λιστών πρόσβασης, οι τυπικές (standard) και οι εκτεταμένες (extended), καθώς και δύο κατηγορίες, οι ονομαστικές (named) και οι αριθμημένες (numbered).

4.1.2 Standard ACL

Οι τυπικές λίστες πρόσβασης επιτρέπουν στην αξιολόγηση μόνο της IP διεύθυνσης της πηγής του πακέτου. Συνήθως οι τυπικές λίστες πρόσβασης εφαρμόζονται για να επιτρέψουν ή να αποτρέψουν την σύνδεση διάφορων συσκευών σε ένα απομακρυσμένο δίκτυο. Για παράδειγμα, μπορούν να εφαρμοστούν διάφορες τυπικές λίστες πρόσβασης σε έναν δρομολογητή αποτρέποντας την σύνδεση στο διαδίκτυο. (Arregoces & Portolani, 2004)

4.1.3 Extended ACL

Όπως και στις τυπικές λίστες πρόσβασης, οι εκτεταμένες λίστες μπορούν και αυτές να φιλτράρουν την κίνηση με βάση την διεύθυνση της πηγής. Ωστόσο, στις εκτεταμένες λίστες δίνεται η δυνατότητα να ελεγχθεί ην κίνηση του δικτύου με βάση την διεύθυνση προορισμού και το είδος πρωτοκόλλου. Ένα βασικό στοιχείο των εκτεταμένων λιστών είναι ότι πάντα πρέπει να εφαρμόζονται όσο πιο κοντά στην διεύθυνση πηγής (Cisco Networking Academy, 2014).

4.1.4 Numbered ACL

Οι αριθμημένες λίστες πρόσβασης χρησιμοποιούνται για να καθορίσουν τον τύπο της λίστας πρόσβασης που επιθυμούμε. Πιο συγκεκριμένα, οι τυπικές λίστες πρόσβασης βρίσκονται στο εξής εύρος αριθμών: από 1 έως 99 και από 1300 έως 1999. Οπότε εάν επιθυμούμε να εφαρμόσουμε μία αριθμημένη λίστα πρόσβασης πρέπει να βεβαιωθούμε ότι βρίσκεται στο συγκεκριμένο εύρος αριθμών. Από την άλλη οι εκτεταμένες λίστες πρόσβασης, εφαρμόζονται στο εξής εύρος: από 100 έως 199 και από 2000 έως 2699 (Paquet, 2009).

4.1.5 Named ACL

Οι ονομαστικές λίστες πρόσβασης είναι μία εναλλακτική των αριθμημένων λιστών, καθώς δίνουν την δυνατότητα στο χρήστη να δημιουργήσει και να ονομάσει τις λίστες πρόσβασης που επιθυμεί. (Paquet, 2009)

4.2 Τι είναι το NAT

Στα προηγούμενα κεφάλαια έγινε μία αναφορά στις ιδιωτικές και δημόσιες διευθύνσεις. Εύλογα όμως προκύπτει το ερώτημα, *ποιος είναι ο λόγος δημιουργίας δύο είδη διευθύνσεων για ένα χρήστη;* Αν κάθε χρήστης είχε στην κατοχή του μία δημόσια διεύθυνση, μέχρι τώρα δεν θα υπήρχαν άλλες διαθέσιμες. Γι' αυτό τον λόγο δημιουργήθηκε το NAT. Το NAT (Network Address Translation) μεταφράζει μία ιδιωτική διεύθυνση σε μία δημόσια. Αυτό σημαίνει πως μία δημόσια διεύθυνση μπορεί να χρησιμοποιηθεί από πολλούς χρήστες. Με αυτόν τον τρόπο επιτυγχάνεται εξοικονόμηση των IPv4 διευθύνσεων (Lammle, 2007).

4.2.1 Static NAT

Το στατικό NAT (static NAT) αναφέρεται στην δημιουργία στατικής μετάφρασης της ιδιωτικής διεύθυνσης με την δημόσια. Πιο συγκεκριμένα, ένας υπολογιστής που έχει στατική μετάφραση διεύθυνσης διαθέτει μονίμως μία δική του δημόσια IP. Βέβαια, αυτός ο τρόπος μετάφρασης της IP διεύθυνσης δεν ενδείκνυται για ένα απλό δίκτυο με δέκα υπολογιστές διότι, δεν γίνεται εξοικονόμηση των διευθύνσεων. Συνήθως οι συσκευές που διαθέτουν στατική μετάφραση της διεύθυνσής τους είναι οι εξυπηρετητές, καθώς πρέπει να έχουν πάντα την ίδια διεύθυνση (Valentine & Whitaker, 2008).

4.2.2 Dynamic NAT

Μέσω της δυναμικής μετάφρασης διευθύνσεων (Dynamic NAT) ένας υπολογιστής μπορεί να αποκτήσει μία δημόσια διεύθυνση μόνο όταν την χρειάζεται,

δηλαδή όταν πρέπει συνδεθεί με το διαδίκτυο. Βέβαια και με αυτόν τον τρόπο δεν γίνεται εξοικονόμηση διευθύνσεων IP καθώς εάν έχουμε δέκα χρήστες συνδεδεμένους στο διαδίκτυο και οι δέκα πρέπει να έχουν στην διάθεσή τους μία δημόσια διεύθυνση IP. Αρκετά ενδιαφέρον κομμάτι της δυναμικής μετάφρασης διευθύνσεων είναι η δημιουργία δεξαμενής (NAT pool). Μία δεξαμενή αποτελείται από ένα σύνολο διευθύνσεων οι οποίες είναι διαθέσιμες για μετάφραση. Για παράδειγμα, εάν έχουμε 10 υπολογιστές σε ένα δίκτυο στη δεξαμενή μας θα πρέπει να περιλαμβάνονται 10 ή περισσότερες διευθύνσεις έτοιμες για μετάφραση. Αν έχουμε λιγότερες δεν θα μπορούν να συνδεθούν και οι 10 ταυτόχρονα στο διαδίκτυο (Valentine & Whitaker, 2008).

4.2.3 PAT (Port Address Translation)

Το PAT (Port Address Translation) ή αλλιώς και NAT overload δημιουργήθηκε μετά το δυναμικό NAT με σκοπό να μειώσει την χρήση των διαφορετικών δημοσίων διευθύνσεων. Πιο συγκεκριμένα, η μέθοδος PAT παρέχει στον χρήστη την ίδια IP διεύθυνση αλλά με διαφορετική θύρα. Για παράδειγμα, εάν έχουμε ένα δίκτυο το οποίο αποτελείται από 10 υπολογιστές, με την χρήση του PAT μπορούν και οι 10 να συνδεθούν στο δίκτυο με την ίδια δημόσια διεύθυνση IP αλλά με διαφορετική θύρα. Το γεγονός αυτό έχει ως αποτέλεσμα, την μέγιστη εξοικονόμηση διευθύνσεων IP (Lammle, 2007).

4.3 Περιγραφή του πρωτοκόλλου Peer-to-Peer

Το πρωτόκολλο Peer-to-Peer (PPP) ανήκει στο επίπεδο της σύνδεσης δεδομένων (επίπεδο 2) στο μοντέλο αναφοράς OSI. Παλαιότερα, το βασικότερο πρωτόκολλο στο επίπεδο 2 ήταν το HDLC (High-Level Data-Link Control) στην συνέχεια όμως δημιουργήθηκε το PPP με περισσότερες λειτουργίες (Odom, Healy & Donohue, 2010). Το πρωτόκολλο point-to-point είναι υπεύθυνο για την σύνδεση και μεταφορά πολλαπλών πρωτοκόλλων μεταξύ δύο άμεσα συνδεδεμένων συσκευών. Το συγκεκριμένο πρωτόκολλο αποτελείται από τρία βασικά συστατικά:

- Τρόπο ενσωμάτωσης πολλαπλών πρωτοκόλλων

- Το πρωτόκολλο ελέγχου συνδέσμου (Link Control Protocol – LCP) το οποίο δημιουργεί, διαμορφώνει και ελέγχει την σύνδεση.
- Το πρωτόκολλο ελέγχου δικτύου (Network Control Protocol – NCP) το οποίο ενθυλακώνει διάφορα πρωτόκολλα του επιπέδου δικτύου (Cisco, 2020).

4.3.1 Πιστοποίηση PAP και CHAP

Το PAP (Password Authentication Protocol) και το CHAP (Challenge Handshake Authentication Protocol) είναι πρωτόκολλα για το PPP τα οποία πιστοποιούν τις δύο συσκευές μεταξύ τους. Το CHAP βέβαια είναι προτιμότερο καθώς παρέχει καλύτερη ασφάλεια, κατά την εναλλαγή κωδικών, χρησιμοποιώντας τον αλγόριθμο MD5 (Message Digest 5). Το PAP, από την άλλη μεριά, δεν χρησιμοποιεί κάποιον αλγόριθμο, καθώς μεταφέρει τους κωδικούς του σε μορφή απλού κειμένου (Odom, 2004).

4.4 Τρόπος λειτουργίας του DHCP

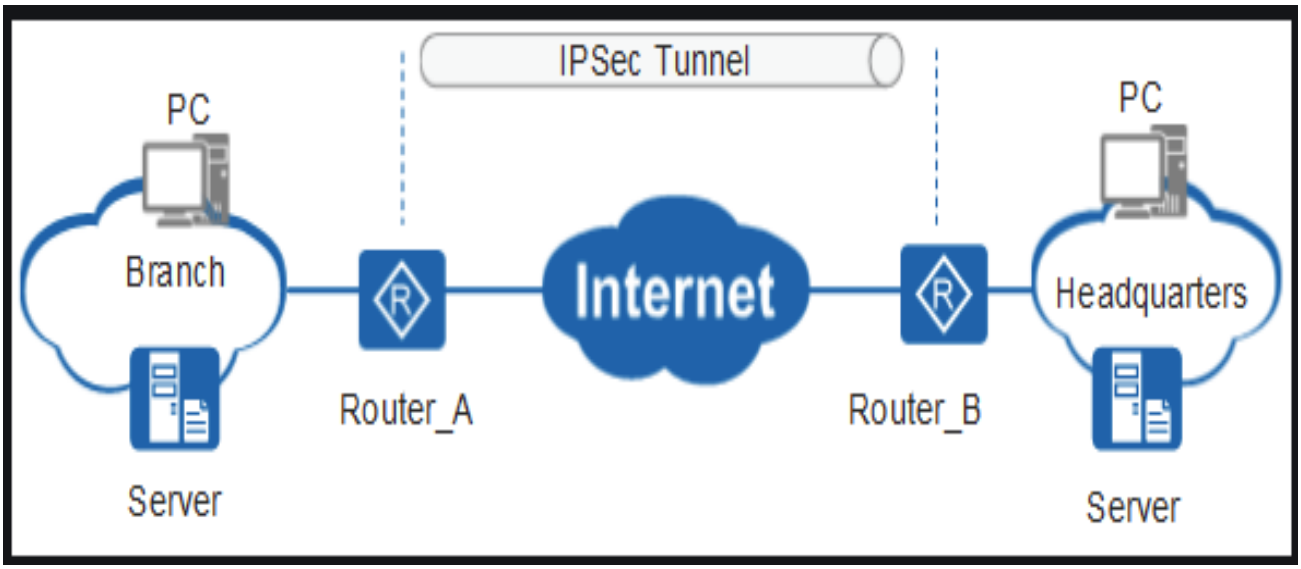
Το DHCP (Dynamic Host Configuration Protocol) είναι πρωτόκολλο το οποίο εκχωρεί διευθύνσεις IP σε τερματικές συσκευές αυτόματα. Το συγκεκριμένο πρωτόκολλο είναι πολύ σημαντικό καθώς παρέχει στον χρήστη την διεύθυνση IP, την μάσκα υποδικτύου, την προεπιλεγμένη πύλη καθώς και τον DNS server. Αν δεν υπήρχε ο DHCP server τότε όλες οι παραπάνω ενέργειες θα έπρεπε να γίνουν χειροκίνητα σε κάθε ένα χρήστη ξεχωριστά. Για παράδειγμα, εάν έχουμε μία εταιρία με 200 εργαζομένους και όλοι έχουν από ένα υπολογιστή, σημαίνει ότι χρειαζόμαστε 200 τουλάχιστον διευθύνσεις. Με τον DHCP server όλες αυτές οι διευθύνσεις εκχωρούνται αυτόματα. Τέλος, αξίζει να σημειωθεί ότι ένας DHCP server μπορεί να διαμορφωθεί σε έναν δρομολογητή αλλά και σε έναν εξυπηρετητή (Diaz, 2018).

Κεφάλαιο 5 IPsec VPN Tunnel

Το πρωτόκολλο IPsec (IP security) είναι ένα πρωτόκολλο ασφάλειας που βρίσκεται στο επίπεδο δικτύου. Είναι υπεύθυνο για την ακεραιότητα των πληροφοριών που ανταλλάσσονται μεταξύ δύο τερματικών σταθμών. Πιο αναλυτικά, το συγκεκριμένο πρωτόκολλο κρυπτογραφεί τα δεδομένα που στέλνει ένας υπολογιστής που βρίσκεται σε ένα δίκτυο σε έναν άλλο υπολογιστή που βρίσκεται σε ένα απομακρυσμένο δίκτυο, έτσι ώστε να μην μπορούν να υποκλαπούν από κάποιον τρίτο.

Μία εταιρία που εκτείνεται σε πολλαπλές περιοχές το ιδανικό για αυτή θα ήταν να έχει το δικό της ιδιωτικό δίκτυο, δηλαδή όλες οι περιοχές να επικοινωνούν μεταξύ τους σε ένα ιδιωτικό δίκτυο. Για να πραγματοποιηθεί αυτό, η εταιρία πρέπει να δεσμεύσει αρκετά χρήματα για την αγορά δρομολογητών, μεταγωγών και δικού τους DNS server έτσι ώστε να συνδέσει όλες τις περιοχές σε ένα δίκτυο χωρίς να μεσολαβεί το διαδίκτυο ενδιάμεσα. Αντί να δημιουργηθεί με αυτόν τον τρόπο ένα τέτοιο δίκτυο, αρκετές εταιρίες σήμερα χρησιμοποιούν τα εικονικά ιδιωτικά δίκτυα (VPN). Ένα εικονικό ιδιωτικό δίκτυο (VPN) παρέχει διαδικτυακό απόρρητο και ανωνυμία δημιουργώντας ένα ιδιωτικό δίκτυο πάνω στο δημόσιο διαδίκτυο.

Για να υπάρχει όμως ασφάλεια στο δίκτυο, η κίνηση ανάμεσα στις περιοχές κρυπτογραφείται πριν η πληροφορία φτάσει στο διαδίκτυο. Στην παρακάτω εικόνα βλέπουμε ένα παράδειγμα της λειτουργίας IPsec VPN Tunnel.

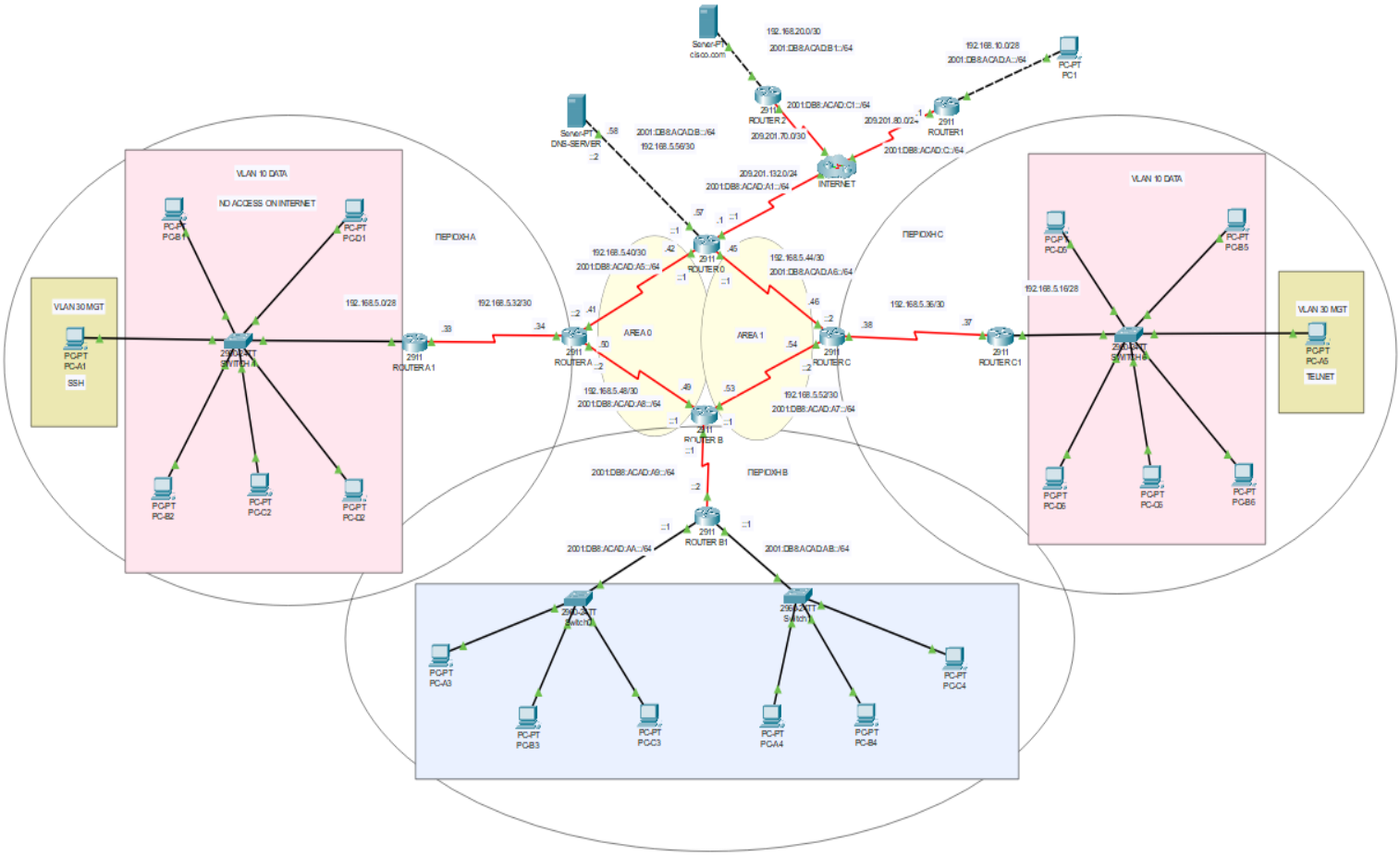


Εικόνα 25. IPsec VPN Tunnel
Πηγή: https://support.huawei.com/enterprise/en/doc/EDOC1000154777/f2298f86/using-ipsec-vpn-to-implement-secure-interconnection-between-lans

Όπως φαίνεται στην παραπάνω εικόνα το Brach με τα Headquarters επικοινωνούν μέσω του IPsec Tunnel παρακάμπτοντας το διαδίκτυο (Kurose & Ross, 2017).

Κεφάλαιο 6 Πειραματικό μέρος

6.1 Τοπολογία Δικτύου



Εικόνα 26. Η τοπολογία δικτύου

Στην παραπάνω εικόνα διακρίνουμε μία τοπολογία δικτύου η οποία αντιπροσωπεύει ένα εικονικό εταιρικό δίκτυο και την επικοινωνία του με το διαδίκτυο. Πιο συγκεκριμένα, έχουν δημιουργηθεί 3 περιοχές. Η περιοχή Α, η περιοχή Β και η περιοχή C. Στην περιοχή Α διακρίνουμε 2 VLAN τα οποία επικοινωνούν μεταξύ τους μέσω του δρομολογητή που τους συνδέει(A1). Στον συγκεκριμένο δρομολογητή έχει διαμορφωθεί ένας DHCP server όπου διανέμει τις διευθύνσεις IP στους υπολογιστές των δύο VLAN, Router on the stick για την σύνδεση των δύο VLAN μεταξύ τους, καθώς και το πρωτόκολλο SSH για απομακρυσμένη πρόσβαση. Στην περιοχή Β δεν διακρίνεται κάποιο VLAN καθώς, έχουν διαμορφωθεί IPv6 διευθύνσεις σε κάθε υπολογιστή, όχι μέσω DHCP server αλλά στατικά στον κάθε ένα. Στην περιοχή C δεν φαίνεται κάποια διαφορά σε σύγκριση με την περιοχή Α, καθώς υπάρχουν και εδώ δύο

VLAN τα οποία επικοινωνούν μεταξύ τους μέσω του δρομολογητή που τους συνδέει(C1), Router on the stick για την επικοινωνία των δύο VLAN, καθώς και το πρωτόκολλο TELNET για απομακρυσμένη πρόσβαση. Όσο αφορά στην επικοινωνία των πόλεων μεταξύ τους, ανάμεσα στους δρομολογητές A1-A και B1-B έχει εφαρμοστεί το πρωτόκολλο δυναμικής δρομολόγησης RIPv2 καθώς και το πρωτόκολλο point-to-point με pap. Στους 4 κεντρικούς δρομολογητές έχει εφαρμοστεί το πρωτόκολλο point-to-point(PPP) με chap και το πρωτόκολλο δυναμικής δρομολόγησης OSPF όπου εκεί διακρίνουμε, σύμφωνα με την παραπάνω τοπολογία, και τις δύο διαφορετικές περιοχές Area 0, Area 1. Η περιοχή Β δεν επικοινωνεί με κάποιο τρόπο με τις άλλες δύο περιοχές, παρά μόνο με το διαδίκτυο. Η επικοινωνία της όμως με το διαδίκτυο γίνεται με το πρωτόκολλο δυναμικής δρομολόγησης EIGRP. Οι δρομολογητές Router0, Router1 και Router2 εφαρμόζονται με NAT μεταφράζοντας τις ιδιωτικές IPv4 διευθύνσεις σε δημόσιες IPv4 διευθύνσεις για την είσοδο στο διαδίκτυο. Για την ασφαλέστερη επικοινωνία του Router0 με τον Router1 έχει εφαρμοστεί IPsec Vpn site to site tunnel. Σύμφωνα με την παραπάνω τοπολογία διακρίνουμε επίσης έναν DNS-SERVER και έναν HTTP-SERVER, όπου οι λειτουργίες αυτών των δύο θα διευκρινιστούν στην συνέχεια της περιγραφής. Αξίζει να σημειωθεί ότι έχουν εφαρμοστεί διάφορες ACL οι οποίες φιλτράρουν την κίνηση στο δίκτυο.

6.2 Διαδικασία δημιουργίας της τοπολογίας δικτύου

Η διαδικασία δημιουργίας της συγκεκριμένης τοπολογίας ξεκινάει με την τοποθέτηση των κατάλληλων συσκευών. Σε αυτή την τοπολογία έχουν χρησιμοποιηθεί:

- 8 Cisco Routers 2911
- 4 Cisco Switches 2960-24TT
- 2 Servers

Στην συνέχεια, αφού έχουν τοποθετηθεί οι συσκευές τις συνδέουμε μεταξύ τους με τα κατάλληλα καλώδια όπως έχουν διευκρινιστεί πιο πάνω στο κεφάλαιο 1. Εδώ αξίζει να σημειωθεί ότι για να συνδεθούν οι δρομολογητές μεταξύ τους θα πρέπει πρώτα να προστεθεί ένα συγκεκριμένο module σε κάθε δρομολογητή, το HWIC-2T το

οποίο επιτρέπει την σύνδεση μεταξύ των δρομολογητών μέσω της σειριακής θύρας(serial). Αφού έχουν τοποθετηθεί και συνδεθεί όλες οι συσκευές στην τοπολογία επιτυχώς μπορούμε να προσθέσουμε και τους υπολογιστές στην κατάλληλη θέση.

Τέλος, το μόνο που μένει, πριν ξεκινήσουμε την διαμόρφωση, είναι να θέσουμε σε λειτουργία τους δρομολογητές πατώντας το κατάλληλο κουμπί.

6.2.1 Εφαρμογή VLSM

Το δίκτυο με το οποίο θα ασχοληθούμε είναι το 192.168.5.0 και είναι Class C αυτό σημαίνει ότι μόνο τα τελευταία 8 bit είναι διαθέσιμα. Οπότε πρέπει να χωρίσουμε αυτό το δίκτυο σε διάφορα υποδίκτυα ανάλογα με τις ανάγκες μας. Για τις IPv6 διευθύνσεις δεν χρειάζεται να εφαρμόσουμε vlsm. Το δίκτυο με το οποίο θα ασχοληθούμε για τις IPv6 διευθύνσεις είναι το 2001:DB8:ACAD::/64

6.2.2 Δημιουργία VLAN

Αρχικά θα ξεκινήσουμε με την δημιουργία του VLAN στο switch της A και B περιοχής γράφοντας τις ακόλουθες εντολές:

```
Switch >enable

Switch #configure terminal

Switch (config) #vlan 10

Switch (config-vlan) #name DATA

Switch (config-vlan) #vlan 30

Switch (config-vlan) #name MGT

Switch (config-vlan) #exit
```

Στην συνέχεια με την εντολή switchport mode access ορίζουμε τις συγκεκριμένες διεπαφές(interfaces) να συνδεθούν με το κατάλληλο vlan.

```
Switch (config) #interface range fa0/1-5

Switch (config-if-range) #switchport mode access

Switch (config-if-range) #switchport access vlan 10

Switch (config-if-range) #exit

Switch (config) #interface range fa0/10

Switch (config-if-range) #switchport mode access

Switch (config-if-range) #switchport access vlan 30

Switch (config-if-range) #exit
```

Επίσης ορίζουμε την συγκεκριμένη διεπαφή ως trunk με την εντολή switchport mode trunk.

```
Switch(config) #interface g0/1

Switch(config-if) #switchport mode trunk

Switch(config-if) #exit
```

Τις συγκεκριμένες διαμορφώσεις τις εφαρμόζουμε και στα δύο switch όπως αναφέραμε πιο πάνω διότι και στις δύο περιπτώσεις τα VLAN είναι ίδια.

6.2.3 Εφαρμογή Router on the stick

Εφαρμόζουμε το Router on the stick στον δρομολογητή A1 και δημιουργούμε τα δύο subinterfaces για το VLAN 10 DATA και το VLAN 30 MGT.

```
Router >enable

Router #configure terminal

Router (config) #interface g0/0.10

Router (config-subif) #encapsulation dot1Q 10
```

Router (config-subif) #ip address 192.168.5.1 255.255.255.248

Router (config-subif) #exit

Router (config)interface g0/0.30

Router (config-subif) #encapsulation dot1Q 30

Router (config-subif) #ip address 192.168.5.9 255.255.255.248

Router (config-subif) #exit

Στην συνέχεια εφαρμόζουμε το Router on the stick στον δρομολογητή C1 και δημιουργούμε τα δύο subinterfaces για το VLAN 10 DATA και το VLAN 30 MGT όπως και πιο πάνω μόνο που τώρα με διαφορετικές ip διευθύνσεις.

Router >enable

Router #configure terminal

Router (config) #interface g0/0.10

Router (config-subif) #encapsulation dot1Q 10

Router (config-subif) #ip address 192.168.5.17 255.255.255.248

Router (config-subif) #exit

Router (config) #interface g0//0.30

Router (config-subif) #encapsulation dot1Q 30

Router (config-subif) #ip address 192.168.5.25 255.255.255.248

Router (config-subif) #exit

6.2.4 Ανάθεση IPv4 διευθύνσεων

Στην συνέχεια θα αναθέσουμε IPv4 διευθύνσεις σε κάθε διεπαφή στους δρομολογητές μας, στους server μας και στους υπολογιστές μας.

Αρχικά χρησιμοποιούμε την εντολή hostname για να δώσουμε ένα όνομα στον δρομολογητή. Με την εντολή IP address *ip address subnet mask* θέτουμε την ip

διεύθυνση στην συγκεκριμένη διεπαφή. Με την εντολή clock rate *bps* θέτουμε τον συγχρονισμό μεταξύ των δύο δρομολογητών σε bps(bits per second) και με την εντολή no shutdown ενεργοποιούμε τη συγκεκριμένη διεπαφή(interface). Ιδιαίτερα σημαντικό είναι να πούμε ότι το clock rate έχουμε την δυνατότητα να το θέσουμε μόνο σε μία διεπαφή μεταξύ δύο δρομολογητών.

A1:

Router >enable

Router #configure terminal

Router (config) #hostname RouterA1

Router (config) #interface serial 0/2/0

Router (config-if) #ip address 192.168.5.33 255.255.255.252

Router (config-if) #clock rate 64000

Router (config-if) #no shutdown

A:

Router >enable

Router #configure terminal

Router (config) #hostname RouterA

RouterA (config) #interface serial 0/2/0

RouterA (config-if) #ip address 192.168.5.34 255.255.252

RouterA (config-if) #no shutdown

RouterA (config-if) #interface serial 0/3/1

RouterA (config-if) #ip address 192.168.5.41 255.255.255.252

RouterA (config-if) #no shutdown

RouterA (config-if) #interface serial 0/3/0

RouterA (config-if) #ip address 192.168.5.50 255.255.255.252

RouterA (config-if) #no shutdown

RouterA (config-if) #exit

B:

Router >enable

Router #configure terminal

Router (config) #hostname RouterB

RouterB (config) #interface serial 0/3/0

RouterB(config-if) #ip address 192.168.5.49 255.255.255.252

RouterB (config-if) #clock rate 64000

RouterB (config-if) #no shutdown

RouterB (config-if) #interface serial 0/3/1

RouterB (config-if) #ip address 192.168.5.53 255.255.255.252

RouterB (config-if) #no shutdown

C:

Router >enable

Router #configure terminal

Router (config) #hostname RouterC

RouterC (config) #interface serial 0/3/1

RouterC (config-if) #ip address 192.168.5.54 255.255.255.252

RouterC (config-if) #clock rate 64000

RouterC (config-if) #no shutdown

RouterC (config-if) #interface serial 0/3/0

RouterC (config-if) #ip address 192.168.5.46 255.255.255.252

RouterC (config-if) #no shutdown

RouterC (config-if) #interface serial 0/2/0

RouterC (config-if) #ip address 192.168.5.38 255.255.255.252

RouterC (config-if) #no shutdown

C1:

Router >enable

Router #configure terminal

Router (config) #hostname RouterC1

RouterC1 (config) #interface serial 0/2/0

RouterC1 (config-if) #ip address 192.168.5.37 255.255.255.252

RouterC1 (config-if) #clock rate 64000

RouterC1 (config-if) #no shutdown

0:

Router >enable

Router #configure terminal

Router (config) #hostname Router0

Router0 (config) #interface serial 0/3/1

Router0 (config-if) #ip address 192.168.5.42 255.255.255.252

Router0 (config-if) #no shutdown

Router0 (config-if) #interface serial 0/3/0

Router0 (config-if) #ip address 192.168.5.45 255.255.255.252

Router0 (config-if) #clock rate 64000

Router0 (config-if) #no shutdown

Router0 (config-if) #interface gigabit 0/0

Router0 (config-if) #ip address 192.168.5.57

Router0 (config-if) #no shutdown

Router0 (config-if) #interface s0/2/0

Router0 (config-if) #ip address 209.201.132.1 255.255.255.0

Router0 (config-if) #no shutdown

INTERNET R1:

InternetR1>enable

InternetR1 #configure terminal

InternetR1 (config) #hostname InternetR1

InternetR1 (config) #interface serial 0/2/0

InternetR1 (config-if) #ip address 209.201.70.1 255.255.255.0

InternetR1 (config-if) #no shutdown

InternetR1 (config-if) #interface serial 0/3/1

InternetR1 (config-if) #ip address 209.201.132.2 255.255.255.0

InternetR1 (config-if) #clock rate 64000

InternetR1 (config-if) #no shutdown

InternetR1 (config-if) #interface serial 0/3/0

InternetR1 (config-if) #ip address 209.201.80.2 255.255.255.0

InternetR1 (config-if) #no shutdown

Όπως φαίνεται πιο πάνω στις διεπαφές 0/2/0, 0/3/1, 0/3/0 έχουν χρησιμοποιηθεί δημόσιες (public) IP διευθύνσεις και όχι οι ιδιωτικές όπως στους προηγούμενους δρομολογητές.

ROUTER 2:

Router > enable

Router #configure terminal

Router (config) #hostname Router2

Router2 (config) #interface serial 0/3/0

Router2 (config-if) #ip address 209.201.70.2 255.255.255.0

Router2 (config-if) #clock rate 64000

Router2 (config-if) #no shutdown

Router2 (config-if) #interface gigabit 0/0

Router2 (config-if) #ip address 192.168.20.1 255.255.255.252

Router2 (config-if) #no shutdown

ROUTER 1:

Router > enable

Router #configure terminal

Router (config) #hostname Router1

Router1 (config) #interface serial 0/3/1

Router1 (config-if) #ip address 209.201.80.1 255.255.255.0

Router1 (config-if) #clock rate 64000

Router1 (config-if) #no shutdown

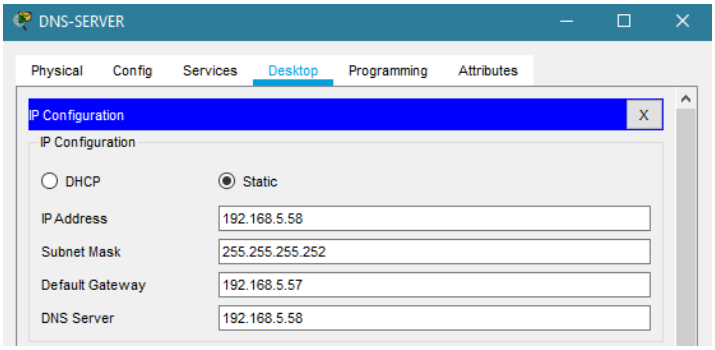
Router1 (config-if) #interface gigabit 0/0

Router1 (config-if) #ip address 192.168.10.1 255.255.255.240

Router1 (config-if) #no shutdown

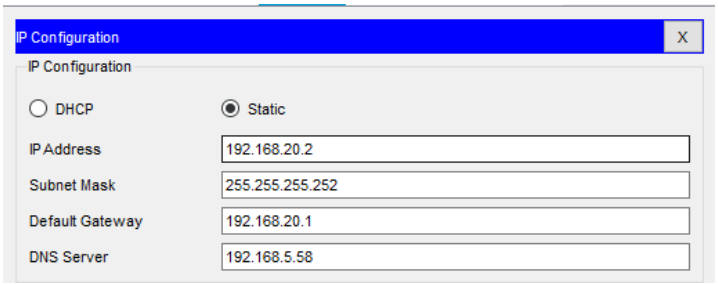
Ανάθεση Ip διευθύνσεων στους δύο Server.

DNS-SERVER:



Εικόνα 27. DNS-SERVER

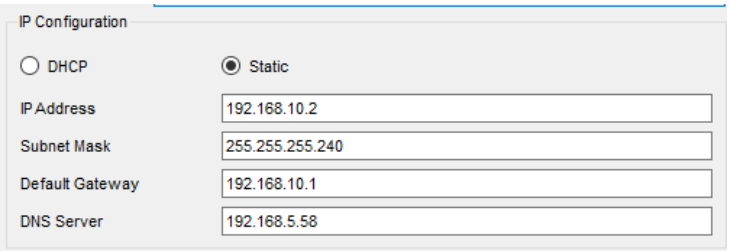
HTTP-SERVER:



Εικόνα 28. HTTP-SERVER

Ανάθεση IP διεύθυνσης στον υπολογιστή.

PC1:



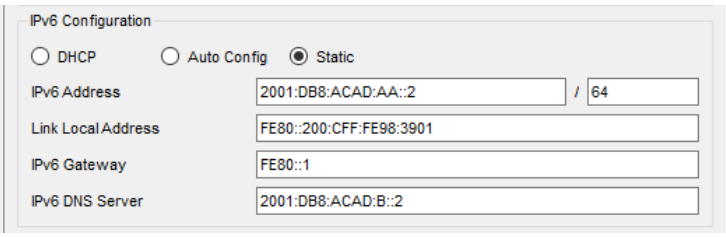
Εικόνα 29. PC-1

Στους υπολογιστές των δύο περιοχών A,C δεν θα αναθέσουμε κάποια IPv4 διεύθυνση χειροκίνητα διότι, οι DHCP server που θα δημιουργήσουμε θα είναι υπεύθυνοι για την συγκεκριμένη εργασία.

6.2.5 Ανάθεση IPv6 διευθύνσεων

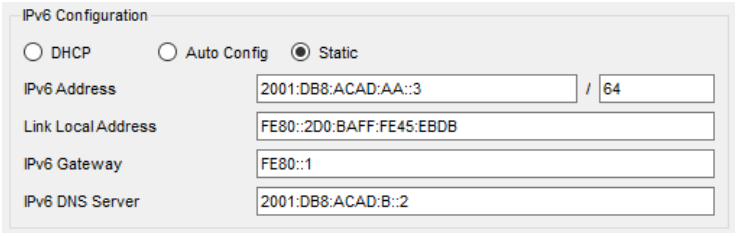
Στην συνέχεια θα θέσουμε IPv6 διευθύνσεις στους υπολογιστές της περιοχής C καθώς και στους κατάλληλους δρομολογητές και server.

PC-A3:



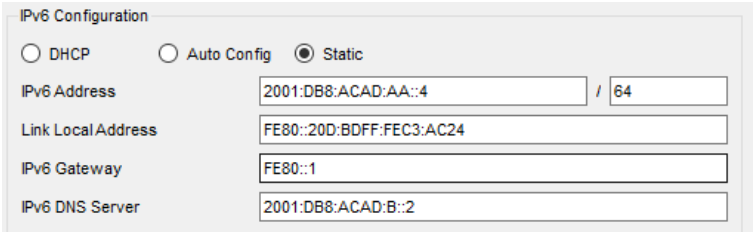
Εικόνα 30. PC-A3

PC-B3:



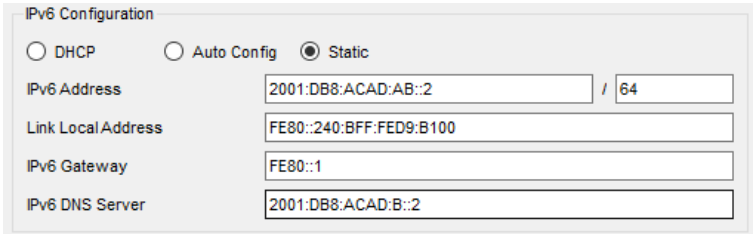
Εικόνα 31. PC-B3

PC-C3:



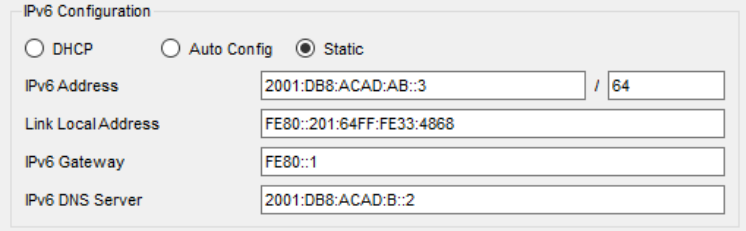
Εικόνα 32. PC-C3

PC-A4:



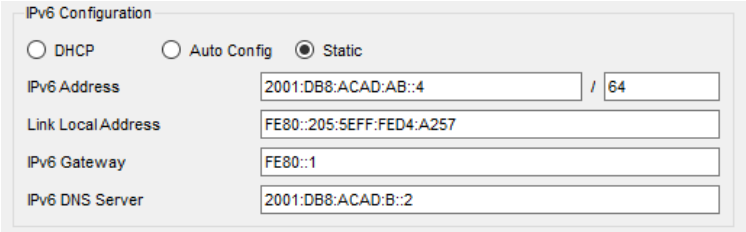
Εικόνα 33. PC-A4

PC-B4:



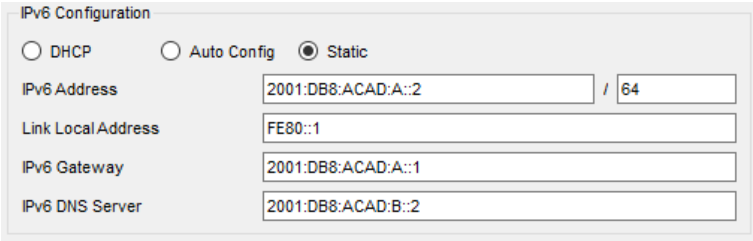
Εικόνα 34. PC-B4

PC-C4:



Εικόνα 35. PC-C4

PC1:



Εικόνα 36. PC1

Για να θέσουμε IPv6 διευθύνσεις στους δρομολογητές είναι σχεδόν η ίδια διαδικασία. Απλά πρέπει να χρησιμοποιήσουμε την εντολή *IPv6 unicast-routing* για να ενεργοποιήσουμε την προώθηση πακέτων στον δρομολογητή και την *IPv6 address {link-local} link-local* για να θέσουμε την link-local διεύθυνση χειροκίνητα όπου εμείς θέλουμε.

B1:

Router >enable

Router #configure terminal

Router (config) #hostname RouterB1

RouterB1 (config) #IPv6 unicast-routing

RouterB1 (config) #interface serial 0/2/0

RouterB1 (config-if) #IPv6 address 2001:DB8:ACAD:A9::2/64

RouterB1 (config-if) #clock rate 64000

RouterB1 (config-if) #no shutdown

RouterB1 (config-if) #interface gigabit 0/0

RouterB1 (config-if) #IPv6 address 2001:DB8:ACAD:AA::1/64

RouterB1 (config-if) #IPv6 address FE80::1 link-local

RouterB1 (config-if) #no shutdown

RouterB1 (config-if) #interface gigabit 0/1

RouterB1 (config-if) #IPv6 address 2001:DB8:ACAD:AB::1/64

RouterB1 (config-if) #IPv6 address FE80::1 link-local

RouterB1 (config-if) #no shutdown

B:

RouterB >enable

RouterB #configure terminal

RouterB (config) #IPv6 unicast-routing

RouterB (config) #interface serial 0/2/0

RouterB (config-if) #IPv6 address 2001:DB8:ACAD:A9::1/64

RouterB (config-if) #no shutdown

RouterB (config-if) #interface serial 0/3/0

RouterB (config-if) #IPv6 address 2001:DB8:ACAD:A8::1/64

RouterB (config-if) #no shutdown

RouterB (config-if) #interface serial 0/3/1

RouterB (config-if) #IPv6 address 2001:DB8:ACAD:A7::1/64

RouterB (config-if) #no shutdown

A:

RouterA >enable

RouterA #configure terminal

RouterA (config) #IPv6 unicast-routing

RouterA (config) #interface serial 0/3/0

RouterA (config-if) #IPv6 address 2001:DB8:ACAD:A8::2/64

RouterA (config-if) #no shutdown

RouterA (config-if) #interface serial 0/3/1

RouterA (config-if) #IPv6 address 2001:DB8:ACAD:A5::2/64

RouterA (config-if) #no shutdown

C:

RouterC >enable

RouterC #configure terminal

RouterC (config) #IPv6 unicast-routing

RouterC (config) #interface serial 0/3/1

RouterC (config-if) #IPv6 address 2001:DB8:ACAD:A7::2/64

RouterC (config-if) #no shutdown

RouterC (config-if) #interface serial 0/3/0

RouterC (config-if) #IPv6 address 2001:DB8:ACAD:A6::2/64

RouterC (config-if) #no shutdown

0:

Router0 >enable

Router0 #configure terminal

Router0 (config) #IPv6 unicast-routing

Router0 (config) #interface serial 0/3/1

Router0 (config-if) #IPv6 address 2001:DB8:ACAD:A5::1/64

Router0 (config-if) #no shutdown

Router0 (config-if) #interface serial 0/3/0

Router0 (config-if) #IPv6 address 2001:DB8:ACAD:A6::1/64

Router0 (config-if) #no shutdown

Router0 (config-if) #interface serial 0/2/0

Router0 (config-if) #IPv6 address 2001:DB8:ACAD:A1::1/64

Router 0(config-if) #no shutdown

Router0 (config-if) #interface gigabit 0/0

Router0 (config-if) #IPv6 address 2001:DB8:ACAD:B::1/64

Router0 (config-if) #IPv6 address FE80::1 link-local

Router0 (config-if) #no shutdown

INTERNET R1:

InternetR1 >enable

InternetR1 #configure terminal

InternetR1 (config) #IPv6 unicast-routing

InternetR1 (config) #interface serial 0/2/0

InternetR1 (config-if) #IPv6 address 2001:DB8:ACAD:C1::1/64

InternetR1 (config-if) #no shutdown

InternetR1 (config-if) #interface serial 0/3/0

InternetR1 (config-if) #IPv6 address 2001:DB8:ACAD:C::1/64

InternetR1 (config-if) #no shutdown

InternetR1 (config-if) #interface serial 0/3/1

InternetR1 (config-if) #IPv6 address 2001:DB8:ACAD:A1::2/64

InternetR1 (config-if) #no shutdown

ROUTER 2:

Router2 >enable

Router2 #configure terminal

Router2 (config) #IPv6 unicast-routing

Router2 (config) #interface serial 0/3/0

Router2 (config-if) #IPv6 address 2001:DB8:ACAD:C1::2/64

Router2 (config-if) #no shutdown

Router2 (config-if) #interface gigabit 0/0

Router2 (config-if) #IPv6 address 2001:DB8:ACAD:B1::1/64

Router2 (config-if) #IPv6 address FE80::1 link-local

Router2 (config-if) #no shutdown

ROUTER 1:

Router1 >enable

Router1 #configure terminal

Router1 (config) #interface gigabit 0/0

Router1 (config-if) #IPv6 address 2001:DB8:ACAD:A::1/64

Router1 (config-if) #IPv6 address FE80::1 link-local

Router1 (config-if) #no shutdown

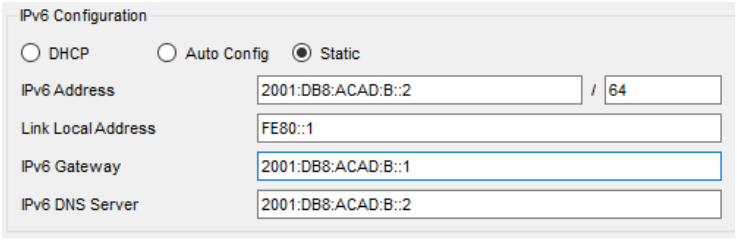
Router1 (config-if) #interface serial 0/3/1

Router1 (config-if) #IPv6 address 2001:DB8:ACAD:C::2/64

Router1 (config-if) #no shutdown

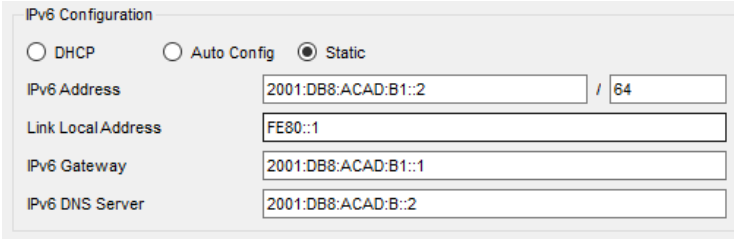
Ανάθεση IPv6 διευθύνσεων στους servers.

DNS-SERVER:



Εικόνα 37. DNS-SERVER IPv6

HTTP-SERVER:



Εικόνα 38. HTTP-SERVER IPv6

6.2.6 Δημιουργία RIP, OSPF και EIGRP IPv6

Αρχικά θα ξεκινήσουμε με την δημιουργία του πρωτοκόλλου δυναμικής δρομολόγησης RIPv2 το οποίο θα το εφαρμόσουμε στους δρομολογητές A1-A, B1-B, 0-R1, R1-1, R1-2. Αφού ενεργοποιήσουμε το πρωτόκολλο rip και την κατάλληλη έκδοση (version 2), στην συνέχεια απενεργοποιούμε την αυτόματη περίληψη του δικτύου μας (no auto-summary). Έπειτα θέτουμε ως passive-interface την διεπαφή που επιθυμούμε για να μην λαμβάνει ενημερώσεις και τέλος εισάγουμε το συνδεδεμένο δίκτυο που επιθυμούμε.

A1:

RouterA1 >enable

RouterA1 #configure terminal

RouterA1 (config) #router rip

RouterA1 (config-router) #version 2

RouterA1 (config-router) #no auto-summary

RouterA1 (config-router) # passive-interface gigabit 0/0

RouterA1 (config-router) #network 192.168.5.0

A:

RouterA >enable

RouterA #configure terminal

RouterA (config) #router rip

RouterA (config-router) #version 2

RouterA (config-router) #no auto-summary

RouterA (config-router) #passive-interface serial 0/3/0

RouterA (config-router) #passive-interface serial 0/3/1

RouterA (config-router) #network 192.168.5.0

C1:

RouterC1 >enable

RouterC1 #configure terminal

RouterC1 (config) #router rip

RouterC1 (config-router) #version 2

RouterC1 (config-router) #no auto-summary

RouterC1 (config-router) #passive-interface gigabit 0/0

RouterC1 (config-router) #network 192.168.5.0

C:

RouterC >enable

RouterC #configure terminal

RouterC (config) #router rip

RouterC (config-router) #version 2

RouterC (config-router) #no auto-summary

RouterC (config-router) #passive-interface serial 0/3/0

RouterC (config-router) #passive-interface serial 0/2/0

RouterC (config-router) #network 192.168.5.0

0:

Router0 >enable

Router0 #configure terminal

Router0 (config) #router rip

Router0 (config-router) #version 2

Router0 (config-router) #no auto-summary

Router0 (config-router) #passive-interface gigabit 0/0

Router0 (config-router) #passive-interface serial 0/3/0

Router0 (config-router) #passive-interface serial 0/3/1

Router0 (config-router) #network 209.201.132.0

Router0 (config-router) #network 192.168.5.0

INTERNET R1:

InternetR1 >enable

InternetR1 #configure terminal

InternetR1 (config) #router rip

InternetR1 (config-router) #version 2

InternetR1 (config-router) #no auto-summary

InternetR1 (config-router) #network 209.201.132.0

InternetR1 (config-router) #network 209.201.80.0

InternetR1 (config-router) #network 209.201.70.0

ROUTER 2:

Router2 >enable

Router2 #configure terminal

Router2 (config) #router rip

Router2 (config-router) #version 2

Router2 (config-router) #no auto-summary

Router2 (config-router) #network 192.168.20.0

Router2 (config-router) #network 209.201.70.0

Router2 (config-router) #passive-interface gigabit 0/0

ROUTER 1:

Router1 >enable

Router1 #configure terminal

Router1 (config) #router rip

Router1 (config-router) #version 2

Router1 (config-router) #no auto-summary

Router1 (config-router) #network 192.168.10.0

Router1 (config-router) #network 209.201.80.0

Rotuer1 (config-router) #passive-interface gigabit 0/0

Στην συνέχεια θα εφαρμόσουμε το πρωτόκολλο OSPF στους δρομολογητές A,B,C,0. Όπως και στο πρωτόκολλο δυναμικής δρομολόγησης RIP έτσι και εδώ ενεργοποιούμε πρώτα το πρωτόκολλο ospf. Ο αριθμός 1 είναι το process ID το οποίο δεν έχει σημασία αν διαφέρει από δρομολογητή σε δρομολογητή. Από την άλλη μεριά το router-id πρέπει να διαφέρει από δρομολογητή σε δρομολογητή διότι είναι αυτό που του παρέχει μία μοναδική ταυτότητα. Στην συνέχεια εισάγουμε τα δίκτυα που επιθυμούμε. Με την wildcard mask γίνεται η αναγνώριση του κάθε δικτύου και το area προσδιορίζει την περιοχή όπου εφαρμόζουμε το συγκεκριμένο δίκτυο.

A:

RouterA >enable

RouterA #configure terminal

RouterA (config) #router ospf 1

RouterA (config-router) #router-id 1.1.1.1

RouterA (config-router) #network 192.168.5.48 0.0.0.3 area 0

RouterA (config-router) #network 192.168.5.40 0.0.0.3 area 0

B:

RouterB >enable

RouterB #configure terminal

RouterB (config) #router ospf 1

RouterB (config-router) #router-id 2.2.2.2

RouterB (config-router) #network 192.168.5.48 0.0.0.3 area 0

RouterB (config-router) #network 192.168.5.52 0.0.0.3 area 1

C:

RouterC >enable

RouterC #configure terminal

RouterC (config) #router ospf 1

RouterC (config-router) #router-id 3.3.3.3

RouterC (config-router) #network 192.168.5.44 0.0.0.3 area 1

RouterC (config-router) #network 192.168.5.52 0.0.0.3 area 1

0:

Router0 >enable

Router0 #configure terminal

Router0 (config) #router ospf 1

Router0 (config-router) #router-id 4.4.4.4

Router0 (config-router) #network 192.168.5.44 0.0.0.3 area 1

Router0 (config-router) #network 192.168.5.40 0.0.0.3 area 0

Όπως φαίνεται από τις παραπάνω εφαρμογές των δύο πρωτοκόλλων RIPv2 και OSPF διακρίνουμε πως στους δρομολογητές A,C και 0 έχουν εφαρμοστεί και τα δύο πρωτόκολλα. Για να δουλέψουν όμως και τα δύο μαζί πρέπει να προσθέσουμε την εντολή redistribute στους συγκεκριμένους δρομολογητές.

A:

RouterA >enable

RouterA #configure terminal

RouterA (config) #router rip

RouterA (config-router) #redistribute ospf 1 metric 3

RouterA (config-router) #exit

RouterA (config) #router ospf 1

RouterA (config-router) #redistribute rip subnets

B:

RouterB >enable

RouterB #configure terminal

RouterB (config) #router rip

RouterB (config-router) #redistribute ospf 1 metric 3

RouterB (config-router) #exit

RouterB (config) #router ospf 1

RouterB (config-router) #redistribute rip subnets

0:

Router0 >enable

Router0 #configure terminal

Router0 (config) #router rip

Router0 (config-router) #redistribute ospf 1 metric 3

Router0 (config-router) #exit

Router0 (config) #router ospf 1

Router0 (config-router) #redistribute rip subnets

Τέλος θα εφαρμόσουμε το πρωτόκολλο EIGRP στις IPv6 διευθύνσεις μας.

B1:

RouterB1>enable

RouterB1 #configure terminal

RouterB1 (config) #IPv6 router eigrp 1

RouterB1 (config-rtr) #eigrp router-id 1.1.1.1

RouterB1 (config-rtr) #passive-interface gigabit 0/0

RouterB1 (config-rtr) #passive-interface gigabit 0/1

RouterB1 (config-rtr) #no shutdown

RouterB1 (config-rtr) #interface serial 0/2/0

RouterB1 (config-if) #IPv6 eigrp 1

RouterB1 (config-if) #interface gigabit 0/0

RouterB1 (config-if) #IPv6 eigrp 1

RouterB1 (config-if) #interface gigabit 0/1

RouterB1 (config-if) #IPv6 eigrp 1

B:

RouterB >enable

RouterB #configure terminal

RouterB (config) #IPv6 router eigrp 1

RouterB (config-rtr) #eigrp router-id 2.2.2.2

RouterB (config-rtr) #no shutdown

RouterB (config-rtr) #interface serial 0/2/0

RouterB (config-if) #IPv6 eigrp 1

RouterB (config-if) #interface serial 0/3/1

RouterB (config-if) #IPv6 eigrp 1

RouterB (config-if) #interface serial 0/3/0

RouterB (config-if) #IPv6 eigrp 1

A:

RouterA >enable

RouterA #configure terminal

RouterA (config) #IPv6 router eigrp 1

RouterA (config-rtr) #eigrp router-id 4.4.4.4

RouterA (config-rtr) #passive-interface serial 0/2/0

RouterA (config-rtr) #no shutdown

RouterA (config-rtr) #interface serial 0/3/0

RouterA (config-if) #IPv6 eigrp 1

RouterA (config-if) #interface serial 0/3/1

RouterA (config-if) #IPv6 eigrp 1

C:

RouterC >enable

RouterC #configure terminal

RouterC (config) #IPv6 router eigrp 1

RouterC (config-rtr) #eigrp router-id 3.3.3.3

RouterC (config-rtr) #passive-interface s0/2/0

RouterC (config-rtr) #no shutdown

RouterC (config-rtr) #interface serial 0/3/0

RouterC (config-if) #IPv6 eigrp 1

RouterC (config-if) #interface serial 0/3/1

RouterC (config-if) #IPv6 eigrp 1

0:

Router0 >enable

Router0 #configure terminal

Router0 (config) #IPv6 router eigrp 1

Router0 (config-rtr) #eigrp router-id 5.5.5.5

Router0 (config-rtr) #passive-interface gigabit 0/0

Router0 (config-rtr) #passive-interface gigabit 0/1

Router0 (config-rtr) #no shutdown

Router0 (config-rtr) #interface serial 0/3/0

Router0 (config-if) #IPv6 eigrp 1

Router0 (config-if) #interface serial 0/3/1

Router0 (config-if) #IPv6 eigrp 1

INTERNET R1:

InternetR1 >enable

InternetR1 #configure terminal

InternetR1 (config) #IPv6 router eigrp 1

InternetR1 (config-rtr) #eigrp router-id 6.6.6.6

InternetR1 (config-rtr) #passive-interface gigabit 0/0

InternetR1 (config-rtr) #no shutdown

InternetR1 (config-rtr) #interface serial 0/2/0

InternetR1 (config-if) #IPv6 eigrp 1

ROUTER 2:

Router2 >enable

Router2 #configure terminal

Router2 (config) #IPv6 router eigrp 1

Router2 (config-rtr) #eigrp router-id 7.7.7.7

Router2 (config-rtr) #passive-interface gigabit 0/0

Router2 (config-rtr) #no shutdown

Router2 (config-rtr) #interface serial 0/3/0

Router2 (config-rtr) #IPv6 eigrp 1

Router2 (config-rtr) #interface serial gigabit 0/0

Router2 (config-rtr) #IPv6 eigrp 1

ROUTER 1:

Router1 >enable

Router1 #configure terminal

Router1 (config) #IPv6 eigrp 1

Router1 (config-rtr) #eigrp router-id 8.8.8.8

Router1 (config-rtr) #passive-interface gigabit 0/0

Router1 (config-rtr) #no shutdown

Router1 (config-rtr) #interface serial 0/3/1

Router1 (config-rtr) #IPv6 eigrp 1

Router1 (config-rtr) #interface gigabit 0/0

Router1 (config-rtr) #IPv6 eigrp 1

6.2.7 Διαμόρφωση DHCP

Η διαμόρφωση του DHCP server για την περιοχή Α θα γίνει στον δρομολογητή A1 και για την περιοχή C στον δρομολογητή C1. Αρχικά αποκλείουμε δύο διευθύνσεις σε κάθε δρομολογητή από το να ανατεθούν αυτόματα μέσω του DHCP διότι έχουν ήδη διαμορφωθεί σε συγκεκριμένες διεπαφές του δρομολογητή. Στην συνέχεια

δημιουργούμε την δεξαμενή με το όνομα που επιθυμούμε, εισάγουμε το δίκτυο στο οποίο θέλουμε να ανατεθούν οι διευθύνσεις και ορίζουμε την προεπιλεγμένη πύλη (default gateway). Τέλος εισάγουμε και την ip διεύθυνση του DNS-SERVER.

A1:

RouterA1 >enable

RouterA1 #configure terminal

RouterA1 (config) #ip dhcp excluded-address 192.168.5.1

RouterA1 (config) #ip dhcp pool DATA

RouterA1 (dhcp-config) #network 192.168.5.0 255.255.255.248

RouterA1 (dhcp-config) #default-router 192.168.5.1

RouterA1 (dhcp-config) #dns-server 192.168.5.58

RouterA1 (dhcp-config) #exit

RouterA1 (config) #ip dhcp excluded-address 192.168.5.9

RouterA1 (config) #ip dhcp pool MGT

RouterA1 (dhcp-config) #network 192.168.5.8 255.255.255.248

RouterA1 (dhcp-config) #default-router 192.168.5.9

RouterA1 (dhcp-config) #dns-server 192.168.5.58

C1:

RouterC1 >enable

RouterC1 #configure terminal

RouterC1 (config) #ip dhcp excluded-address 192.168.5.17

RouterC1 (config) #ip dhcp pool DATA

RouterC1 (dhcp-config) #network 192.168.5.16 255.255.255.248

RouterC1 (dhcp-config) #default-router 192.168.5.17

RouterC1 (dhcp-config) #dns-server 192.168.5.58

RouterC1 (dhcp-config) #exit

RouterC1 (config) #ip dhcp excluded-address 192.168.5.25

RouterC1 (config) #ip dhcp pool MGT

RouterC1 (dhcp-config) #network 192.168.5.24 255.255.255.248

RouterC1 (dhcp-config) #default-router 192.168.5.25

RouterC1 (dhcp-config) #dns-server 192.168.5.58

6.2.8 Διαμόρφωση NAT και PAT

Η διαδικασία ξεκινάει με την δημιουργία μιας extended acl, η οποία θα επιτρέπει την πρόσβαση στις διευθύνσεις που θα μεταφράζονται από τον NAT. Στην συνέχεια διαμορφώνουμε τον NAT δρομολογητή ορίζοντας το εύρος δημόσιων IP διευθύνσεων που θα μεταφράσει σε ιδιωτικές. Επίσης, ενεργοποιούμε το NAT με PAT με την κατάλληλη acl που έχουμε δημιουργήσει. Τέλος ορίζουμε τις εσωτερικές και εξωτερικές διεπαφές του δρομολογητή.

ROUTER 0:

Router0 >enable

Router0 #configure terminal

Router0 (config) #ip access-list extended NAT

Router0 (config-ext-nacl) #1 deny ip 192.168.5.0 0.0.0.255 host 192.168.10.2

Router0 (config-ext-nacl) #2 permit ip 192.168.5.0 0.0.0.255 any

Router0 (config-ext-nacl) #exit

Router0 (config) #ip nat pool NATPOOL 209.201.132.3 209.201.132.10 netmask 255.255.255.240

Router0 (config) #ip nat inside source list NAT pool NATPOOL overload

Router0 (config) #interface serial 0/2/0

Router0 (config-if) #ip nat outside

Router0 (config-if) #interface serial 0/3/1

Router0 (config-if) #ip nat inside

Router0 (config-if) #interface serial 0/3/0

Router0 (config-if) #ip nat inside

Router0 (config-if) #interface gigabit 0/1

Router0 (config-if) #ip nat inside

Στην συνέχεια θα διαμορφώσουμε στατικό NAT στον δρομολογητή Router2 για τον HTTP-SERVER (cisco.com).

ROUTER 2:

Router2 >enable

Router2 #configure terminal

Router2 (config) #ip nat inside source static 192.168.20.2 209.201.70.3

Router2 (config) #interface gigabit 0/0

Router2 (config-if) #ip nat inside

Router2 (config-if) #interface serial 0/3/0

Router2 (config-fi) #ip nat outside

Ύστερα, θα διαμορφώσουμε NAT στον δρομολογητή Router1 αλλά αυτή τη φορά με PAT στην συγκεκριμένη διεπαφή.

ROUTER 1:

Router1 >enable

Router1 #configure terminal

Router1 (config) #ip access-list extended NAT

Router1 (config-ext-nacl) #1 deny ip host 192.168.10.2 192.168.5.0 0.0.0.255

Router1 (config-ext-nacl) #2 permit ip host 192.168.10.2 any

Router1 (config-ext-nacl) #exit

Router1 (config) #ip nat inside source list NAT interface gigabit 0/0 overload

Router1 (config) #interface gigabit 0/0

Router1 (config-if) #ip nat inside

Router1 (config-if) #interface serial 0/3/1

Router1 (config-if) #ip nat outside

Όπως και στον δρομολογητή Router0 έτσι και εδώ η χρησιμότητα της συγκεκριμένης acl θα διευκρινιστεί στην συνέχεια όπου θα αναλύσουμε το VPN.

6.2.9 Διαμόρφωση SSH και TELNET

Το πρωτόκολλο SSH θα το εφαρμόσουμε στον δρομολογητή C1 ενώ το πρωτόκολλο TELNET στον δρομολογητή A1. Για την εφαρμογή του SSH αρχικά θα θέσουμε ένα όνομα για τον δρομολογητή, το domain-name καθώς και ένα όνομα χρήστη και ένα κωδικό για την είσοδό μας. Στην συνέχεια θα δημιουργηθεί το δημόσιο και ιδιωτικό κλειδί και τέλος θα ενεργοποιήσουμε το πρωτόκολλο SSH στον δρομολογητή.

RouterA1 >enable

```
RouterA1 #configure terminal

RouterA1 (config) #ip domain-name cisco

RouterA1 (config) #username cisco password ccna

RouterA1 (config) #crypto key generate rsa

RouterA1 (config) #line vty 0 15

RouterA1 (config-line) #login local

RouterA1 (config-line) #transport input ssh
```

Η εφαρμογή του TELNET είναι αρκετά πιο απλή διότι, το μόνο που χρειάζεται να κάνουμε είναι να ενεργοποιήσουμε το πρωτόκολλο TELNET στον δρομολογητή και να εισάγουμε ένα κωδικό επαλήθευσης.

```
RouterC1 >enable

RouterC1 #configure terminal

RouterC1 (config) #line vty 0 15

RouterC1 (config-line) #login

RouterC1 (config-line) #password ccna
```

Σύμφωνα με την παραπάνω τοπολογία θα παρατηρήσουμε ότι και στις δύο περιοχές Α και C έχουν δημιουργηθεί τα vlan 30 MGT(management). Οι υπολογιστές αυτών των vlan θα γνωρίζουν τους κωδικούς πρόσβασης των δρομολογητών για να μπορούν να τους τροποποιήσουν ανάλογα.

6.2.10 Δημιουργία ACL

Στην συνέχεια αυτής της τοπολογίας θα δημιουργήσουμε ACL οι οποίες θα εφαρμοστούν, εκτός από τους δρομολογητές 0 και 1 όπου ήδη υπάρχουν, στον δρομολογητή A1. Η συγκεκριμένη extended named ACL θα αποτρέπει την επικοινωνία των υπολογιστών του vlan 10 DATA με τον HTTP-SERVER.

A1:

Router >enable

Router #configure terminal

Router (config) #ip access-list extended NOTCP

Router(config-ext-nacl) #10 deny ip 192.168.5.0 0.0.0.7 host 209.201.70.3

Router(config-ext-nacl) #20 permit ip any any

Router(config-ext-nacl) #interface gigabit 0/0

Router(config-if) #ip access-group NOTCP in

6.2.11 PPP με CHAP και PAP πιστοποίηση

Όπως προαναφέραμε πιο πάνω στην περιγραφή της τοπολογίας, χρησιμοποιούμε PPP με ενθυλάκωση CHAP στους κεντρικού δρομολογητές (A, B, C, 0) και PPP με ενθυλάκωση PAP στους δρομολογητές A-A1 και B-B1.

ROUTER A:

RouterA >enable

RouterA #configure terminal

RouterA (config) #username RouterA1 password cisco

RouterA (config) #interface serial 0/2/0

RouterA (config-if) #encapsulation ppp

RouterA (config-if) #ppp authentication pap

RouterA (config-if) #ppp pap sent-username RouterA password cisco

ROUTER A1:

RouterA1 >enable

RouterA1 #configure terminal

RouterA1 (config) #username RouterA password cisco

RouterA1 (config) #interface serial 0/2/0

RouterA1 (config-if) #encapsulation ppp

RouterA1 (config-if) #ppp authentication pap

RouterA1 (config-if) #ppp pap sent-username RouterA1 password cisco

ROUTER C:

RouterC >enable

RouterC #configure terminal

RouterC (config) #username RouterC1 password cisco

RouterC (config) #interface serial 0/2/0

RouterC (config-if) #encapsulation ppp

RouterC (config-if) #ppp authentication pap

RouterC (config-if) #ppp pap sent-username RouterC password cisco

ROUTER C1:

RouterC1 >enable

RouterC1 #configure terminal

RouterC1 (config) #username RouterC password cisco

RouterC1 (config) #interface serial 0/2/0

RouterC1 (config-if) #encapsulation ppp

RouterC1 (config-if) #ppp authentication pap

RouterC1 (config-if) #ppp pap sent-username RouterC1 password cisco

Στην συνέχεια θα εφαρμόσουμε PPP με CHAP στους κεντρικούς δρομολογητές.

ROUTER A:

RouterA >enable

RouterA #configure terminal

RouterA (config) #username RouterB password cisco

RouterA (config) #interface serial 0/3/0

RouterA (config-if) #encapsulation ppp

RouterA (config-if) #ppp authentication chap

RouterA (config-if) #exit

RouterA (config) #username Router0 password cisco

RouterA (config) #interface serial 0/3/1

RouterA (config-if) #encapsulation ppp

RouterA (config-if) #ppp authentication chap

ROUTER B:

RouterB >enable

RouterB #configure terminal

RouterB (config) #username RouterA password cisco

RouterB (config) #interface serial 0/3/0

RouterB (config-if) #encapsulation ppp

RouterB (config-if) #ppp authentication chap

RouterC (config-if) #exit

RouterB (config) #username RouterC password cisco

RouterB (config) #interface serial 0/3/1

RouterB (config-if) #encapsulation ppp

RouterB (config-if) #ppp authentication chap

ROUTER C:

RouterC >enable

RouterC #configure terminal

RouterC (config) #username RouterB password cisco

RouterC (config) #interface serial 0/3/1

RouterC (config-if) #encapsulation ppp

RouterC (config-if) #ppp authentication chap

RouterC (config-if) #exit

RouterC (config) #username Router0 password cisco

RouterC (config) #interface serial 0/3/0

RouterC (config-if) #encapsulation ppp

RouterC (config-if) ppp authentication chap

ROUTER 0:

RouterC >enable

RouterC #configure terminal

RouterC (config) #username RouterA password cisco

RouterC (config) #interface serial 0/3/1

RouterC (config-if) #encapsulation ppp

RouterC (config-if) #ppp authentication chap

RouterC (config-if) #exit

RouterC (config) #username RouterC password cisco

RouterC (config) #interface serial 0/3/0

RouterC (config-if) #encapsulation ppp

RouterC (config-if) ppp authentication chap

6.2.12 Δημιουργία IPsec VPN tunnel

Τέλος θα δημιουργήσουμε IPsec VPN tunnel μεταξύ των δρομολογητών Router0-Router1. Αρχικά θα ενεργοποιήσουμε την άδεια ασφαλείας για τους δύο δρομολογητές. Στην συνέχεια θα εφαρμόσουμε μία ACL η οποία θα επιτρέπει την επικοινωνία των δύο δρομολογητών. Η διαδικασία δημιουργίας του IPsec VPN tunnel χωρίζεται σε 2 στάδια. Στο πρώτο στάδιο βρίσκεται η σύνδεση μεταξύ των δύο δρομολογητών εφαρμόζοντας τα ISAKMP policy και ISAKMP key. Στο δεύτερο στάδιο πραγματοποιείται η εφαρμογή του IPsec transform-set όπου σε αυτό το στάδιο γίνεται η κρυπτογράφηση των δεδομένων. Στην συνέχεια εφαρμόζουμε το Crypto map και τέλος τη διεπαφή στην οποία εφαρμόζεται το crypto map.

ROUTER 0:

Router0 >enable

```
Router0 #configure terminal

Router0 (config) #license boot module c2900 technology-package securityk9

ACCEPT? [yes/no]: yes

Router0 #copy running-config startup-config

Router0 #reload

Router0 #configure terminal

Router0 (config) #access-list 100 permit ip 192.168.5.0 0.0.0.255 host 192.168.10.2

Router0 (config) #crypto isakmp policy 10

Router0 (config-isakmp) #encryption aes 256

Router0 (config-isakmp) #authentication pre-share

Router0 (config-isakmp) #group5

Router0 (config-isakmp) #exit

Router0 (config) #crypto isakmp key cisco address 209.201.80.1

Router0 (config) #crypto ipsec transform-set Router0-Router1 esp-aes 256 esp-sha-hmac

Router0 (config) #crypto map VPN 10 ipsec-isakmp

Router0 (config-crypto-map) #set peer 209.201.80.1

Router0 (config-crypto-map) #set pfs group5

Router0 (config-crypto-map) #set security-association lifetime seconds 86400

Router0 (config-crypto-map) #set transform-set Router0-Router1

Router0 (config-crypto-map) #match address 100

Router0 (config-crypto-map) #interface serial 0/2/0

Router0 (config-if) #crypto map VPN
```

ROUTER 1:

Router0 >enable

Router0 #configure terminal

Router0 (config) #license boot module c2900 technology-package securityk9

ACCEPT? [yes/no]: yes

Router0 #copy running-config startup-config

Router0 #reload

Router0 #configure terminal

Router0 (config) #access-list 100 permit host 192.168.10.2 192.168.5.0 0.0.0.255

Router0 (config) #crypto isakmp policy 10

Router0 (config-isakmp) #encryption aes 256

Router0 (config-isakmp) #authentication pre-share

Router0 (config-isakmp) #group5

Router0 (config-isakmp) #exit

Router0 (config) #crypto isakmp key cisco address 209.201.132.1

Router0 (config) #crypto ipsec transform-set Router1-Router0 esp-aes 256 esp-sha-hmac

Router0 (config) #crypto map VPN 10 ipsec-isakmp

Router0 (config-crypto-map) #set peer 209.201.132.1

Router0 (config-crypto-map) #set pfs group5

Router0 (config-crypto-map) #set security-association lifetime seconds 86400

Router0 (config-crypto-map) #set transform-set Router1-Router0

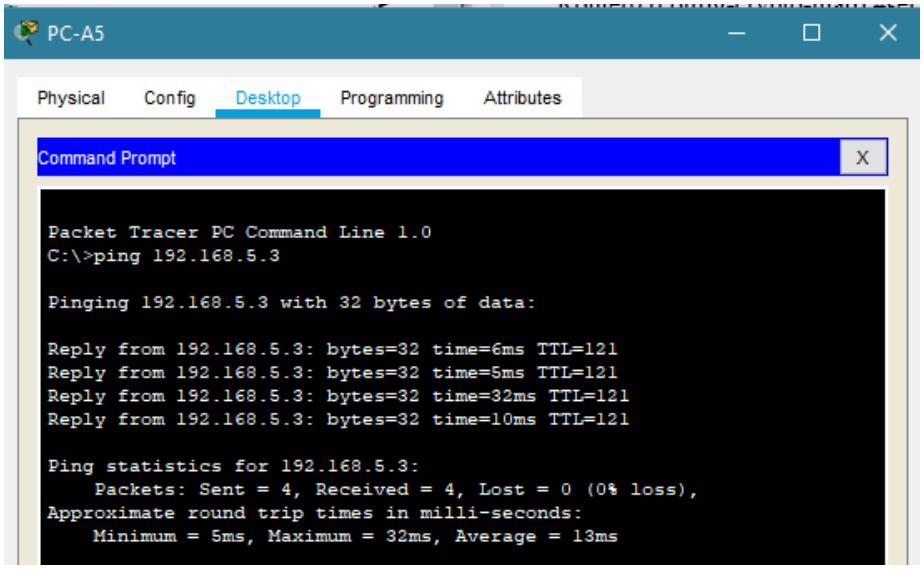
Router0 (config-crypto-map) #match address 100

Router0 (config-crypto-map) #interface serial 0/3/1

Router0 (config-if) #crypto map VPN

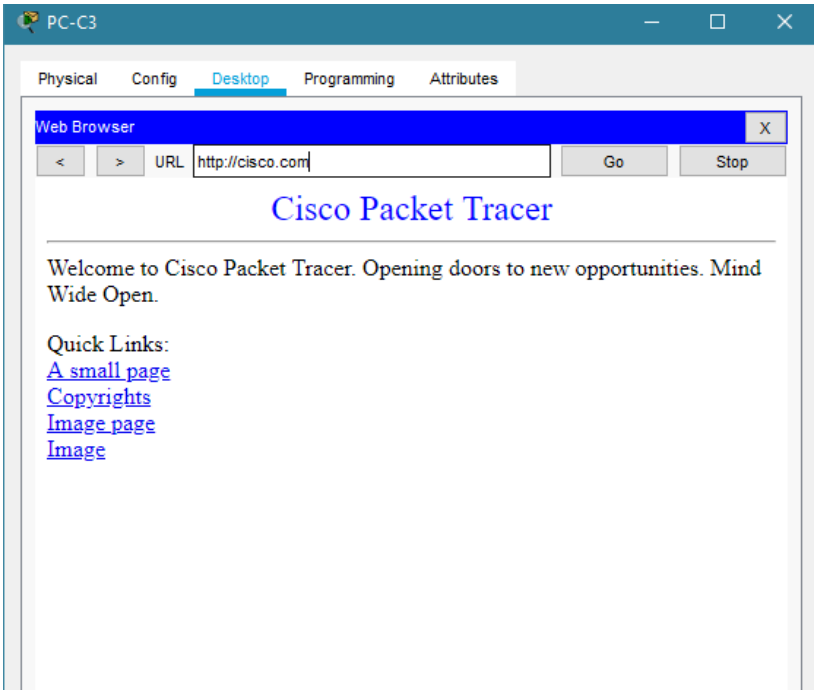
6.3 Έλεγχος επικοινωνίας

Σε αυτό το κομμάτι θα πραγματοποιηθεί ο έλεγχος της επικοινωνίας έτσι ώστε, να βεβαιωθούμε ότι οι παραπάνω εντολές εκτελέστηκαν σωστά. Αρχικά, θα ελέγξουμε την επικοινωνία μεταξύ των δύο περιοχών Περιοχή Α-Περιοχή C.



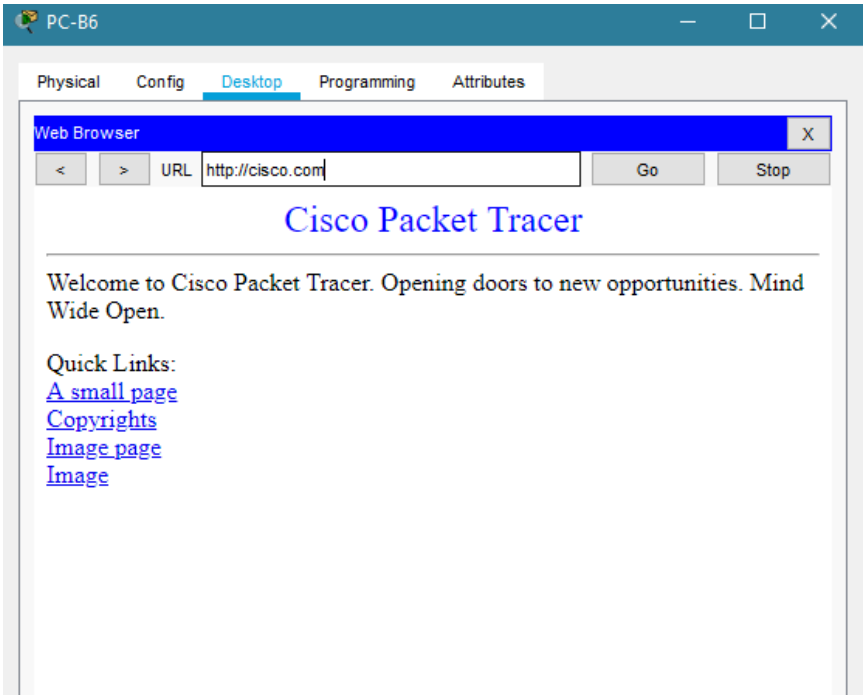
Εικόνα 39. Επικοινωνία Περιοχής C-Περιοχής Α

Όπως φαίνεται η επικοινωνία ανάμεσα στο PC-A5 της περιοχής C και στην IP διεύθυνση 192.168.5.3, η οποία αντιστοιχεί σε έναν υπολογιστή της περιοχής Α, είναι επιτυχημένη. Στην συνέχεια θα δοκιμάσουμε να συνδεθούμε στην ιστοσελίδα της cisco και από τις τρεις περιοχές.



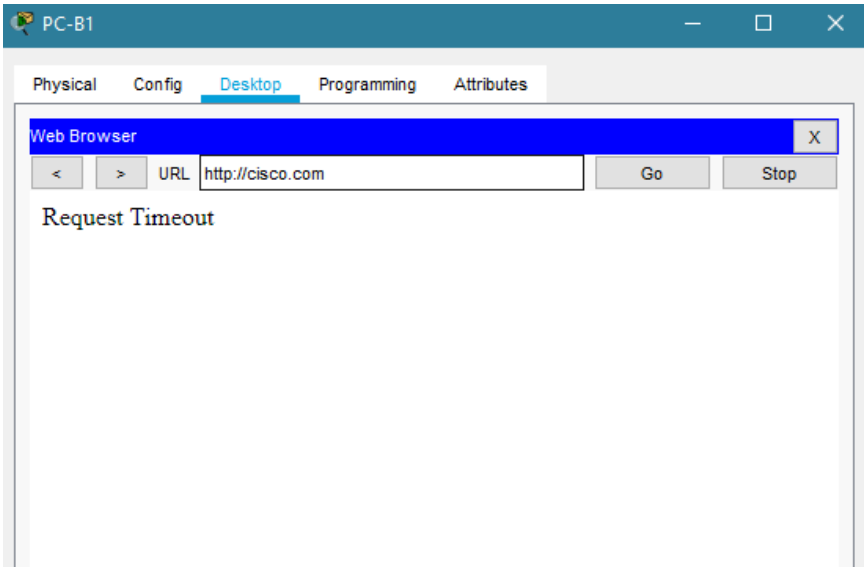
Εικόνα 40. Πρόσβαση στην cisco.com – Περιοχή Β

Από την περιοχή Β ο υπολογιστής PC-C3 έχει πρόσβαση στην συγκεκριμένη ιστοσελίδα με την IPv6 διεύθυνση.



Εικόνα 41. Πρόσβαση στην cisco.com – Περιοχή C

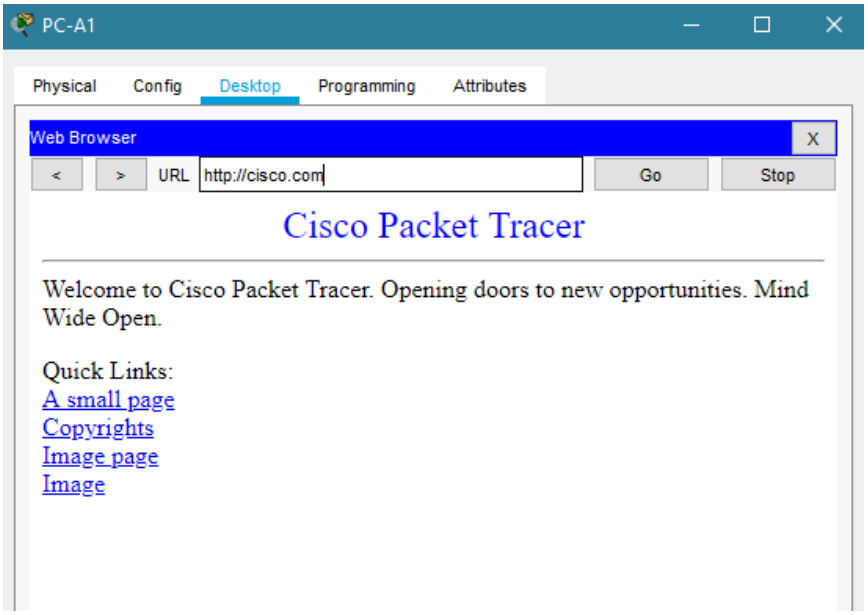
Από τον υπολογιστή της περιοχής C υπάρχει πρόσβαση στην σελίδα.



Εικόνα 42. Αποτυχία πρόσβασης στην cisco.com - PC-B1

Σε αυτή την περίπτωση διακρίνουμε μη επιτυχημένη σύνδεση στην ιστοσελίδα από τον υπολογιστή PC-B1 ο οποίος ανήκει στην περιοχή A στο VLAN 10 DATA. Αυτό συμβαίνει διότι, έχει εφαρμοστεί μία ACL η οποία δεν επιτρέπει την πρόσβαση του συγκεκριμένου VLAN 10 DATA στην ιστοσελίδα cisco.com.

Αν όμως προσπαθήσουμε να συνδεθούμε από το VLAN 30 MGT της ίδιας περιοχής η σύνδεση θα είναι επιτυχημένη, όπως φαίνεται και στην παρακάτω εικόνα.



Εικόνα 43. Πρόσβαση στην cisco.com - PC-A1

Στην συνέχεια με βάση την παρακάτω εικόνα θα διευκρινιστεί ο τρόπος με τον οποίο λειτούργησε ο NAT στον Router0.

```
Router0>enable
Router0#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 209.201.132.3:1024 192.168.5.10:1025  209.201.70.3:80    209.201.70.3:80
tcp 209.201.132.3:1025 192.168.5.22:1025  209.201.70.3:80    209.201.70.3:80
```

Εικόνα 44. Show ip nat translations

Με το αποτέλεσμα της εντολής show ip nat translations διακρίνουμε όλες τις μεταφράσεις που έκανε ο NAT. Όπως φαίνεται έγιναν δύο μεταφράσεις IP διευθύνσεων μία από τον PC-A1 με την IP 192.168.5.10 και μία από τον PC-B6 με IP διεύθυνση 192.168.5.22. Ο λόγος που και οι δύο υπολογιστές μοιράστηκαν την ίδια δημόσια IP διεύθυνση είναι επειδή χρησιμοποιούμε NAT με PAT. Στην συνέχεια, με την εντολή show running-config ελέγχουμε όλες τις τροποποιήσεις που έχουν εφαρμοστεί στους δρομολογητές. Στην παρακάτω εικόνα διακρίνουμε κάποιες από τις διαμορφώσεις του δρομολογητή A.

```
interface Serial0/2/0
 ip address 192.168.5.34 255.255.255.252
 encapsulation ppp
 ppp pap sent-username RouterA password 0 cisco
!
interface Serial0/2/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/3/0
 ip address 192.168.5.50 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 ipv6 address 2001:DB8:ACAD:A8::2/64
 ipv6 eigrp 1
!
interface Serial0/3/1
 ip address 192.168.5.41 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 ipv6 address 2001:DB8:ACAD:A5::2/64
 ipv6 eigrp 1
 clock rate 64000
!
```

Εικόνα 45. Router A Show running-config PPP με Chap και PAP

Όπως παρατηρούμε, στις διεπαφές του δρομολογητή Router A εμφανίζονται οι τροποποιήσεις που έχουμε εφαρμόσει. Για παράδειγμα, στην διεπαφή serial 0/2/0 διακρίνουμε την ενθυλάκωση ppp με την πιστοποίηση pap. Στην διεπαφή serial 0/3/0 εντοπίζουμε την ενθυλάκωση ppp με την πιστοποίηση chap, όπως αντίστοιχα και στην διεπαφή serial 0/3/1.

Έπειτα, εισάγουμε την ίδια εντολή (show running-config) στον δρομολογητή Router 0 και στον δρομολογητή Router 1 όπου διακρίνουμε, την δημιουργία του IPsec VPN tunnel.

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key cisco address 209.201.80.1
!
!
!
crypto ipsec transform-set R0-R1 esp-aes 256 esp-sha-hmac
!
crypto map VPN 10 ipsec-isakmp
 set peer 209.201.80.1
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set R0-R1
 match address 100
```

Εικόνα 46. Router 0 show running-config IPsec VPN Tunnel

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key cisco address 209.201.132.1
!
!
!
crypto ipsec transform-set R1-R0 esp-aes 256 esp-sha-hmac
!
crypto map VPN 10 ipsec-isakmp
 set peer 209.201.132.1
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set R1-R0
 match address 100
```

Εικόνα 47. Router 1 show running-config IPsec VPN Tunnel

Τέλος, με την εντολή show ip route εμφανίζονται όλες οι δρομολογήσεις των IPv4 διευθύνσεων του δρομολογητή Router C.

```
     192.168.5.0/24 is variably subnetted, 17 subnets, 3 masks
O E2    192.168.5.0/29 [110/20] via 192.168.5.53, 00:05:51, Serial0/3/1
O E2    192.168.5.8/29 [110/20] via 192.168.5.53, 00:05:51, Serial0/3/1
R       192.168.5.16/29 [120/1] via 192.168.5.37, 00:00:27, Serial0/2/0
R       192.168.5.24/29 [120/1] via 192.168.5.37, 00:00:27, Serial0/2/0
O E2    192.168.5.32/30 [110/20] via 192.168.5.53, 00:05:51, Serial0/3/1
C       192.168.5.36/30 is directly connected, Serial0/2/0
C       192.168.5.37/32 is directly connected, Serial0/2/0
L       192.168.5.38/32 is directly connected, Serial0/2/0
O IA    192.168.5.40/30 [110/128] via 192.168.5.45, 00:06:51, Serial0/3/0
C       192.168.5.44/30 is directly connected, Serial0/3/0
C       192.168.5.45/32 is directly connected, Serial0/3/0
L       192.168.5.46/32 is directly connected, Serial0/3/0
O IA    192.168.5.48/30 [110/128] via 192.168.5.53, 00:06:51, Serial0/3/1
C       192.168.5.52/30 is directly connected, Serial0/3/1
C       192.168.5.53/32 is directly connected, Serial0/3/1
L       192.168.5.54/32 is directly connected, Serial0/3/1
O E2    192.168.5.56/30 [110/20] via 192.168.5.45, 00:07:01, Serial0/3/0
     192.168.10.0/28 is subnetted, 1 subnets
O E2    192.168.10.0/28 [110/20] via 192.168.5.45, 00:07:01, Serial0/3/0
     192.168.20.0/30 is subnetted, 1 subnets
O E2    192.168.20.0/30 [110/20] via 192.168.5.45, 00:07:01, Serial0/3/0
O E2 209.201.70.0/24 [110/20] via 192.168.5.45, 00:07:01, Serial0/3/0
O E2 209.201.80.0/24 [110/20] via 192.168.5.45, 00:07:01, Serial0/3/0
O E2 209.201.132.0/24 [110/20] via 192.168.5.45, 00:07:01, Serial0/3/0
```

Εικόνα 48. Router C show ip route

Συμπεράσματα

Στην παρούσα εργασία δημιουργήθηκε μία τοπολογία δικτύου με το λογισμικό Cisco Packet Tracer. Το συγκεκριμένο εικονικό δίκτυο καλύπτει μεγάλο εύρος θεμάτων, με σημαντικότερα αυτών τα πρωτόκολλα δρομολόγησης και επικοινωνίας. Παρόλη την κάλυψη ποικίλων θεμάτων που παρέχει το δίκτυο, τόσο η μη προτιμώμενη πλέον χρήση σειριακών καλωδίων μεταξύ δρομολογητών, όσο και η χρήση της κλάσης C έναντι της ενδεδειγμένης κλάσης B που χρησιμοποιείται σε αντίστοιχα δίκτυα μεσαίου μεγέθους, αποτρέπουν την εφαρμογή του παρόντος δικτύου σε πραγματικές συνθήκες. Συνοψίζοντας, είναι χρήσιμο να αναφερθεί ότι ο σχεδιασμός του εικονικού αυτού δικτύου αποσκοπούσε στην κατανόηση βασικών εννοιών από τον αναγνώστη, εξυπηρετώντας έτσι την εκπαιδευτική προσέγγιση του δικτύου μέσω προσομοίωσης και όχι τόσο στην εφαρμογή του σε πραγματικές συνθήκες. Τόσο η συνεχώς αυξανόμενη πρόοδος της τεχνολογίας, όσο και ο στόχος που τέθηκε κατά την δημιουργία του δικτύου οδηγούν στην αναζήτηση των βέλτιστων τροποποιήσεων που θα συμβάλουν στην μελλοντική εξέλιξη της χρήσης του. Οι ιδανικότερες παρεμβάσεις που δύνανται να εφαρμοστούν στο δίκτυο αυτό είναι η χρήση οπτικών ινών, αυξάνοντας έτσι την ταχύτητα του δικτύου και η κατά κύριο λόγο διάθεση IPv6 διευθύνσεων, έναντι των IPv4, συνεισφέροντας θετικά στη βελτιστοποίηση της ασφάλειας και στο ενδεχόμενο εξάντλησής τους.

Βιβλιογραφικές Αναφορές

Arregoces, M., & Portolani, M. (2004). *Data Center Fundamentals*. Indianapolis: Cisco Press.

Cisco. (2020, Μάιος 8). Ανακτήθηκε από Cisco : https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/15-s/iri-15-s-book/iri-iprouting.pdf

Cisco. (2020, Μάιος 2). Ανακτήθηκε από Cisco : https://www.cisco.com/c/en/us/tech/wan/point-to-point-protocol-ppp/index.html

Cisco. (2020, Απρίλιος 24). Ανακτήθηκε από Cisco : https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/https/configuration/15-mt/https-15-mt-book/nm-https-sc-ssl3.html

Cisco. (2020, Μάιος 5). Ανακτήθηκε από Cisco: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dns/configuration/15-mt/dns-15-mt-book/dns-config-dns.html

Cisco Networking Academy. (2014). *Routing and Switching Essentials Companion Guide.* Indianapolis: 2014.

Dayle, J., & Carroll, J. (2006). *Routing TCP/IP*. Indianapolis: Cisco Press.

Diaz, L. (2018). *CCNA Routing and Switching 200-125 Certification Guide.* Birmigham: Packt Publishing Ltd.

Doherty, J., Anderson, N., & Maggiora, P. D. (2010). *Ο Οδηγός της Cisco για τη Δικτύωση* (Δεύτερη αμερικανική έκδοση εκδ.). (Π. Καναβός, Μεταφρ.) Αθήνα: Κλειδάριθμος.

Doyle, J. (1998). *Routing TCP/IP Volume I (CCIE Profesional Development).* Cisco Press.

Garrett, A. (2006). *JUNOS Cookbook.* Sebastopol: O'Reily Media.

Kurose, J. F., & Ross, K. W. (2017). *Δικτύωση Υπολογιστών Προσέγγιση από πάνω προς τα κάτω* (3η Ελληνική Επανέκδοση εκδ.). (Β. Γ. Σαμαράς, Μεταφρ.) Αθήνα: Μόσχος Γκιούρδας.

Lammle, T. (2007). *CCNA: Cisco Certified Network Associate Study Guide.* Indianapolis: Wiley Publishing, Inc.

Malhotra, R. (2002). *IP Routing.* Sebastopol: O' Reilly & Associates.

Malik, S. (2003). *Network Security Principles and Practices.* Indianapolis: Cisco Press.

McQuerry, S. (2004). *CCNA Αυτοδιδασκαλία: Διασύνδεση Συσκευών Δικτύου Cisco (ICND)* (Δεύτερη Αμερικανική έκδοση εκδ.). (Π. Κανναβός, Μεταφρ.) Αθήνα: Κλειδάριθμος.

Odom, W. (2004). *CCNA Self-Study CCNA ICND Exam Certification Guide.* Indianapolis: Cisco Press.

Odom, W. (2013a). *Cisco CCENT/CCNA ICND1 100-101 Academic Edition.* Indianapolis: Cisco Press.

Odom, W. (2013b). *Cisco CCNA Routing and Switching 200-120 Official Cert Guide Library.* Indianapolis: Cisco Press.

Odom, W., Healy, R., & Donohue, D. (2010). *CCIE Routing and Switching Certification Guide* (Fourth Edition εκδ.). Indianapolis: Cisco Press.

Paquet, C. (2009). *Implementing Cisco IOS Network Security (IINS).* Indianapolis: Cisco Press.

Simoneau, P. (2006). *The OSI Model: Understanding the Seven Layers of Computer Networks.*

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Δίκτυα Υπολογιστών* (5η εκδ.). (Φ. Σκουλαρίκης, & Γ. Ξυλωμένος, Μεταφρ.) Αθήνα: Κλειδάριθμος.

Tiso, J. (2014). *Interconnecting Cisco Network Devices, Part 2 (ICND2).* Indianapolis: Cisco Press.

Valentine, M., & Whitaker, A. (2008). *CCNA Exam Cram: (exam 640-802).* United States of America: Que Publishing.

Μαργαρίτη, Σ., & Στεργίου , Ε. (2006). *ΤΟΠΙΚΑ & ΑΣΤΙΚΑ ΔΙΚΤΥΑ (LAN-MAN).* Αθήνα: Εκδόσεις Νέων Τεχνολογιών.