Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Μηχανικών Πληροφορικής

Πτυχιακή Εργασία

"Σχεδιασμός και ασφάλεια εταιρικού δικτύου με χρήση εικονικού προσομοιωτή GNS3 (Graphical Network Simulator)"

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: **ΑΛΕΞΑΝΔΡΟΣ ΜΠΡΙΤΖΟΛΑΚΗΣ**
ΗΜΕΡΟΜΗΝΙΑ: **29/05/2015**

ΕΙΣΗΓΗΤΗΣ: **Δρ. ΧΑΡΑΛΑΜΠΟΣ ΜΑΝΙΦΑΒΑΣ**

Ευχαριστίες

Με την ολοκλήρωση αυτής της πτυχιακής θα ήθελα να ευχαριστήσω τα εξής σημαντικά προς εμένα άτομα: την μητέρα μου για όλη την ψυχολογική και ηθική στήριξη που μου παρείχε σε όλα τα δύσκολα μαθητικά και φοιτητικά μου χρόνια, τον πατέρα μου που ήταν πάντα δίπλα μου σε όποιο πρόβλημα κι αν είχα, την Μαρίνα και την αδερφή μου Κατερίνα για όλη την αγάπη τους και την υπομονή τους και τον Λάζαρο Αγαπίδη καθότι χωρίς την πολύτιμη και καθοριστική του βοήθεια δεν θα ήταν δυνατή η ολοκλήρωση αυτής της πτυχιακής.
Πάνω απ' όλα θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της πτυχιακής μου Δρ. Χαράλαμπο Μανιφάβα τον οποίο θαυμάζω και εκτιμώ απεριόριστα καθότι η βοήθεια του και οι συμβουλές του ήταν πολύ σημαντικές σε όλη την πορεία των φοιτητικών μου σπουδών και κυριότερα στο να μπορέσω να κατανοήσω τις πραγματικές μου δυνατότητες.

Abstract

This thesis with the subject "Design and security of a company network with using the Graphical Network Simulator (GNS3)" has as its main focus of study the design of an Internet Service Provider – telecommunication company – that has its main headquarters with its various working segments (e.x. Accounting Office, IT department, Marketing Office etc.) and a remote second store which will be booth located within the city of Heraklion, Crete, Greece.
To accomplish this, a graphical network simulator called GNS3 will be used. This program provides virtual routers, as well as firewalls that simulate the Command Line Interface – CLI of Cisco Systems Inc. Furthermore, security methods will be studied at both, theoretical level (security and communication protocols, security policies, strategies for future network development and so on) and practical level (network design in GNS3, the selection of Cisco device equipment, command parameters regulation within CLI provided by GNS3).

More specifically the main objectives of this thesis are:

1. The general understanding of computer networks and how they serve the human society

2. The recording and documentation of communication protocols that will be implemented within this network, such as, protocols for file transfer (i.e. FTP) or for communication security (i.e. SSH).

3. The documented and ergonomic network designing based on the company's desires, by selecting the suitable models of network devices that are already promoted in market by Cisco Systems Inc.

4. The analysis of these devices, the designed network's financial cost for the company in terms of the Greek market, as well as the searching of the needed initial funding.

5. The security techniques at both "exploit" level (i.e. router code setting measures, user authorization and the network firewall setup) and in case of natural disaster (i.e. backup connections in order to prevent complete network destruction in case that one of these connections is set off)

The main purpose of this thesis is the documentation of real conditions and challenges that a network engineer faces when designing and establishing a network. The documentation of the modern network equipment sold by Cisco Systems Inc is included, as well as the documentation of the network itself, in regards to the fulfillment of the company's market needs.

Σύνοψη

Η παρούσα πτυχιακή εργασία με θέμα «Σχεδιασμός και ασφάλεια εταιρικού δικτύου με χρήση εικονικού προσομοιωτή GNS3 (Graphical Network Simulator)» έχει ως αντικείμενο τον σχεδιασμό ενός εικονικού εταιρικού τηλεπικοινωνιακού οργανισμού που θα διαθέτει τα κεντρικά της γραφεία με τα διάφορα τμήματα εργασίας (π.χ. τμήμα λογιστηρίου, πληροφορικής, marketing κλπ) και ένα απομακρυσμένο υποκατάστημα όπου θα εδρεύουν στα πλαίσια της πόλης του Ηρακλείου, Κρήτης. Για να επιτευχθεί αυτό θα χρησιμοποιηθεί ένας εικονικός προσομοιωτής δικτύων που είναι το GNS3 (Graphical Network Simulator). Αυτό το πρόγραμμα παρέχει εικονικούς δρομολογητές (routers) καθώς και firewalls που προσομοιώνουν Command Line Interface – CLI της εταιρίας Cisco. Θα αναφερθούν μέθοδοι ασφάλειας σε θεωρητικό επίπεδο όπως ανάλυση των πρωτοκόλλων ασφάλειας και επικοινωνίας που θα εφαρμοστούν, δημιουργία πολιτικών ασφάλειας, καταγραφή στρατηγικής για μελλοντική ανάπτυξη του δικτύου κλπ αλλά και σε πρακτικό επίπεδο όπως την δημιουργία του δικτύου στο GNS3, την επιλογή εξοπλισμού συσκευών Cisco που θα χρησιμοποιήσουμε, ρύθμιση παραμέτρων εντολών σε αυτές μέσω του CLI που παρέχει το GNS3.

Αναλυτικά ο σκοπός αυτής της πτυχιακής εργασίας είναι:

1. Η γενική κατανόηση των δικτύων υπολογιστών και πως αυτά εξυπηρετούν την ανθρώπινη κοινωνία

2. Καταγραφή και τεκμηρίωση των πρωτοκόλλων επικοινωνίας που θα χρησιμοποιηθούν σε αυτό το δίκτυο όπως πρωτόκολλα για μεταφορά αρχείων π.χ. FTP ή για ασφαλή επικοινωνία π.χ. SSH κλπ.

3. Τεκμηριωμένος, και εργονομικός σχεδιασμός του δικτύου στα μέτρα της εταιρίας, με την επιλογή των κατάλληλων μοντέλων δικτυακών συσκευών που προωθεί στην καταναλωτική αγορά η εταιρία Cisco.

4. Ανάλυση των εν λόγω συσκευών, το οικονομικό κόστος που θα καταβάλει η εταιρία γι' αυτό το δίκτυο σε Ελληνικά δεδομένα καθώς και την εύρεση του αρχικού κεφαλαίου που θα χρειαστεί να διαθέσει.

5. Τεχνικές ασφάλειας τόσο σε επίπεδο exploit (για παράδειγμα την ρύθμιση κωδικών σε routers, την εξουσιοδότηση χρηστών, την ρύθμιση firewalls στο δίκτυο κλπ) αλλά και σε επίπεδο φυσικών καταστροφών (για παράδειγμα εφεδρικές συνδέσεις ώστε σε περίπτωση που χαλάσει η μια σύνδεση να μην καταστραφεί όλο το δίκτυο)

Ο βασικός σκοπός της πτυχιακής αυτής είναι η καταγραφή των πραγματικών συνθηκών και προκλήσεων που καλείται να αντιμετωπίσει ένας μηχανικός δικτύου τόσο στον σχεδιασμό όσο και στην εφαρμογή αυτού. Αυτό περιλαμβάνει την καταγραφή σύγχρονων δικτυακών εξοπλισμών της εταιρίας Cisco καθώς και την δημιουργία καταγραφής και τεκμηρίωσης του δικτύου με άμεσο σκοπό την εκπλήρωση των αναγκών της εταιρίας στα πλαίσια της καταναλωτικής αγοράς.

Πίνακας περιεχομένων

Κεφάλαιο 3ο: Προφίλ της Εταιρείας

Πίνακας εικόνων

Κεφάλαιο 1ο: Εισαγωγή

Κεφάλαιο 2ο: Εισαγωγή στον κόσμο των δικτύων

Κεφάλαιο 3ο: Προφίλ εταιρίας

Κεφάλαιο 4ο: Εισαγωγή στο GNS3

Κεφάλαιο 5ο: Δημιουργία δικτύου στο GNS3

Ευρετήριο πινάκων

Κεφάλαιο 1ο: Εισαγωγή

Κεφάλαιο 2ο: Εισαγωγή στον κόσμο των δικτύων

Κεφάλαιο 3ο: Προφίλ εταιρίας

Κεφάλαιο 4ο: Εισαγωγή στο GNS3

Κεφάλαιο 5ο: Δημιουργία δικτύου στο GNS3

Ευρετήριο σχημάτων

Κεφάλαιο 2ο: Εισαγωγή στον κόσμο των δικτύων

Ακρωνύμια

A

ARP – Address Resolution Protocol (Πρωτόκολλο Μετατροπής διευθύνσεων)
ADSL – Asymmetric Digital Subscriber Line
ASA Firewall – Adaptive Security Appliance Firewall
AES – Advanced Encryption Standard

B

BGP – Boarder Gateway Protocol
BPDU – Bridge Protocol Data Unit

C

CDP – Cisco Discovery Protocol
CIDR – Classless Inter-Domain Routing (Αταξική δρομολόγηση δικτυακών περιοχών)

D

DHCP - Dynamic Host Configuration Protocol
DNS – Domain Name System (Σύστημα ονοματοδοσίας περιοχών)

E

e-mail – Electronic mail (Ηλεκτρονικό ταχυδρομείο)
EGP – Exterior Gateway Routing Protocol
RIP – Routing Information Protocol
EIGRP – Enhanced Interior Gateway Routing Protocol

F

FTP – File Transfer Protocol (Πρωτόκολλο Μεταφοράς Αρχείων)

G

Gbps – Gigabit per second

H

HTTP – HyperText Transfer Protocol (Πρωτόκολλο μεταφοράς υπερκειμένου)
HTTPS – HyperText Transfer Protocol Secure (Ασφαλές πρωτόκολλο μεταφοράς υπερκειμένου)
HSRP – Hot Standby Router Protocol

I

ISP - Internet Service Provider (Παροχέας διαδικτύου)
ITE – Ίδρυμα τεχνολογίας και Έρευνας
IP – Internet Protocol (Πρωτόκολλο διαδικτύου)

IEEE – Institute of Electrical and Electronic Engineers (Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών)
IMAP – Internet Message Access Protocol
ITU – Telecommunication Standardization Sector
IPTV – Internet Protocol Television
IOS – Internetworking Operating System
ICMP – Internet Control Message Protocol (Πρωτόκολλο Μηνυμάτων Ελέγχου διαδικτύου)
IGMP – Internet Group Management (Πρωτόκολλο Διαχείρισης Ομάδας Internet)
IPV4 – Internet Protocol version 4
IPV6 – Internet Protocol version 6
IPsec – Internet Protocol Security
IDP – Internet Datagram Protocol
IGRP – Interior Gateway Routing Protocol

J

K

L

LAN – Local Area Networks
LED – Light Emitting Diodes
LASER – Light Amplification by Stimulated Emission off Radiation

M

MAN – Metropolitan Area Networks
MAC – Media Access Control
MS-DOS – Microsoft disk operating system

N

NAT – Network Address Translation
NIC – Network Interface Card

O

OSI – Open Systems Interconnection
OSPF – Open Shortest Path First

P

PSTN – Public Switched Telephone Network
PPP – Point-To-Point (Πρωτόκολλο σημείου προς σημείο)

Q

QoS – Quality of Service

R

rlogin – Remote Login
POP3 – Post Office Protocol version 3
RTP – Real-time Transport Protocol
RARP – Reverse Address Resolution Protocol (Ανάστροφης Μετατροπής διευθύνσεων)

S

SMTP – Simple Mail Transfer Protocol (Πρωτόκολλο Απλού ταχυδρομείου)
SSH – Secure Shell
STP – Spanning Tree Protocol
SFTP – Secure File Transfer Protocol
SPX – Sequenced Packet Exchange
SRI – Stanford Research Institute

T

TCP – Transmission Control Protocol (Πρωτόκολλο Ελέγχου Μεταφοράς)
TFTP – Trivial File Transfer Protocol (Πρωτόκολλο Απλής Μεταφοράς Αρχείων)
TTL – Time –to –Live
Telnet – Telecommunication Network (Απομακρυσμένη σύνδεση)
3DES – Triple Data Encryption Standard
TKIP – Temporal Key Integrity Protocol

U

UTP – Unshielded Twisted Pair
UDP – User Datagram Protocol (Πρωτόκολλο Αυτοδύναμων Πακέτων Χρήστη)
UPS – Universal Power Supply

V

VTP – VLAN Trunking Protocol
VLAN – Virtual Local Area Network
VoIP – Voice Over Internet Protocol
VPN – Virtual Private Network
VDSL – Very-high-bit-rate digital subscriber line

W

WAN – Wide Area Networks
Wi–Fi – Wireless fidelity
WPA2 – Wi-Fi Protected Access 2

1.1 Τι είναι Δίκτυο Υπολογιστών

Με τον όρο δίκτυο υπολογιστών αναφερόμαστε σε ένα σύστημα επικοινωνίας, στο οποίο πραγματοποιείται ανταλλαγή δεδομένων μεταξύ πολλών (πάνω από δύο) διασυνδεδεμένων αυτόνομων υπολογιστικών συσκευών ή ακόμα και IP ενεργοποιούμενων συσκευών.

1.2 Σκοπός των Δικτύων

Ο σκοπός για τον οποίον τα δίκτυα δημιουργήθηκαν είναι για να εξυπηρετήσουν τις ολοένα και αυξανόμενες ανάγκες που δημιουργήθηκαν από την ευρεία χρήση των υπολογιστών συσκευών. Ο βασικότερος όμως σκοπός για τον οποίο είναι αρκετά σημαντικό ύπαρξης των δικτύων είναι ο διαμερισμός των πόρων σε συστήματα καθώς και η ανταλλαγή πληροφοριών (προγράμματα, αρχεία, δεδομένα). Πόροι του συστήματος μπορούν να είναι είτε

- υλικό (hardware), π.χ. υπολογιστές, εκτυπωτές, plotters, σκληροί δίσκοι
- είτε λογισμικό (software), π.χ. δεδομένα, προγράμματα εφαρμογών, υπηρεσίες.

Τα προγράμματα, τα δεδομένα και οι συσκευές (σκληροί δίσκοι, εκτυπωτές, κλπ) είναι διαθέσιμα σε οποιονδήποτε είναι συνδεδεμένος στο δίκτυο, ανεξάρτητα από την θέση στην οποία βρίσκεται. Έτσι επιτυγχάνεται εξοικονόμηση χρημάτων, αύξηση της απόδοσης του συστήματος, κεντρικός έλεγχος και εύκολη επεκτασιμότητα.

Σε ένα δίκτυο υπολογιστών μπορούμε να έχουμε ανταλλαγή δεδομένων, προγραμμάτων, χρήση κοινών βάσεων δεδομένων, αρχείων, αποστολή μηνυμάτων (electronic mail). Όμως, ανεξάρτητα απ' όλα αυτά ένα δίκτυο υπολογιστών αποτελεί ένα αρκετά ισχυρό μέσο επικοινωνίας μεταξύ ανθρώπων που βρίσκονται σε διαφορετικά ή διάσπαρτα σημεία.

1.2.1 Αρχιτεκτονική των Δικτύων

Με τον όρο αρχιτεκτονική ενός δικτύου αναφερόμαστε στον τρόπο με τον οποίο οι υπολογιστές και οι λοιπές συσκευές συνδέονται μεταξύ τους με άμεσο σκοπό την δυνατότητα διαμοιρασμού πληροφοριών και συσκευών που διαθέτει αυτό. Ένα δίκτυο δεδομένων μπορεί να περιλαμβάνει τις εξής οντότητες:

1. Τερματικούς Κόμβους.
   Όπου είναι σημεία τα οποία ελέγχουν τους πόρους του δικτύου (λογισμικό και υλικό).

2. Υποδίκτυα
   Φυσικά μέσα μετάδοσης, πρωτόκολλα επικοινωνίας, τοπολογία, τερματικοί κόμβοι, πόροι που μπορεί να διαφέρουν πολύ σε κάθε υποδίκτυο.

3. Συσκευές Διασύνδεσης
   Όπου διασύνδεουν ετερογενή υποδίκτυα με άμεσο σκοπό την εξασφάλιση επικοινωνίας των τερματικών κόμβων που βρίσκονται σε διαφορετικά υποδίκτυα.

1.3 Είδη Δικτύων

1.3.1 Με βάση την γεωγραφική ανάπτυξη:

Δίκτυα ευρείας περιοχής (Wide Area Networks – WAN), είναι δίκτυα τα οποία καλύπτουν αποστάσεις μερικών χιλιομέτρων (συνήθως άνω των 5 km) και καλύπτουν μια εκτεταμένη γεωγραφική περιοχή (π.χ. χώρες, κράτη ακόμα και ηπείρους). Αποτελούνται από υπολογιστές, τηλεπικοινωνιακές συσκευές και γραμμές. Παραδείγματα τέτοιων δικτύων μπορεί να θεωρηθούν τα δίκτυα των αεροπορικών εταιρειών, τα τραπεζικά δίκτυα, τα δημόσια δίκτυα δεδομένων κλπ.

Μητροπολιτικά Δίκτυα (Metropolitan Area Networks – MAN), Είναι δίκτυα τα οποία περιορίζονται στα πλαίσια μιας πόλης. Ένα μητροπολιτικό δίκτυο συνήθως συνδέει τα διάφορα τοπικά δίκτυα υπολογιστών χρησιμοποιώντας ένα δίκτυο κορμού (backbone technology) υψηλού εύρους ζώνης, όπως οι οπτικές ίνες και παρέχει διασυνδέσεις προς τα δίκτυα ευρείας περιοχής ή το διαδίκτυο.

Τοπικά δίκτυα (Local Area Networks – LAN) είναι δίκτυα τα οποία εκτείνονται σε μια περιορισμένη γεωγραφική απόσταση (π.χ. κτήριο ή ένα συγκρότημα κτηρίων) και περιορίζεται στα πλαίσια ενός οργανισμού ή μιας εταιρίας. Χαρακτηρίζονται από υψηλούς ρυθμούς μεταφοράς δεδομένων (10 έως 100 Mbps), μικρή καθυστέρηση και αριθμό σφαλμάτων. Επίσης έχουν μικρό αριθμό διασυνδεδεμένων υπολογιστών και χρησιμοποιούν ιδιωτικά μέσα μετάδοσης. Τοπικά δίκτυα συναντάμε σε σχολεία, πανεπιστήμια, εταιρίες, οργανισμούς, ιδρύματα κλπ.

Πλεονεκτήματα των τοπικών δικτύων
✓ Χαμηλό κόστος ανά χρήστη. Για παράδειγμα μια ακριβή περιφερειακή συσκευή (π.χ. ένα πολυμηχάνημα ή ένας server) είναι ένας πόρος που μπορεί να χρησιμοποιηθεί από όλους τους χρήστες.
✓ Υψηλή ταχύτητα μεταφοράς δεδομένων
✓ Επεκτασιμότητα.
✓ Βελτιστοποίηση της χρήσης των μηχανημάτων
✓ Η παροχή υπηρεσιών είναι αρκετά ικανοποιητική για όλους τους χρήστες του δικτύου
✓ Ύπαρξη συμβατότητας για συσκευές οι οποίες υποστηρίζουν συγκεκριμένα πρότυπα.

Πίνακας 1.1. Πλεονεκτήματα που εμφανίζουν τα τοπικά δίκτυα

1.3.2 Με βάση τον τηλεπικοινωνιακό φορέα εξυπηρέτησης

Ιδιωτικά δίκτυα (Private Networks): Είναι δίκτυα τα οποία αποτελούν ιδιοκτησία ενός ιδιωτικού οργανισμού ή μιας εταιρίας. Πρόσβαση σε αυτό το δίκτυο έχουν μόνο εξουσιοδοτημένοι χρήστες (υπάλληλοι, εργαζόμενοι κτλ) οι οποίοι συνήθως πρέπει να βρίσκονται φυσικά εντός των εγκαταστάσεων του οργανισμού για να αποκτούν πρόσβαση σε αυτό. Η πρόσβαση σε ιδιωτικό δίκτυο από σημεία εκτός του οργανισμού είναι περιορισμένος ή ακόμα και ανύπαρκτος.

Δημόσια δίκτυα (Public Networks): Τα δημόσια δίκτυα είναι αυτά τα οποία μεταφέρουν τα δεδομένα πολλών χρηστών χωρίς ελέγχους ή διακρίσεις.

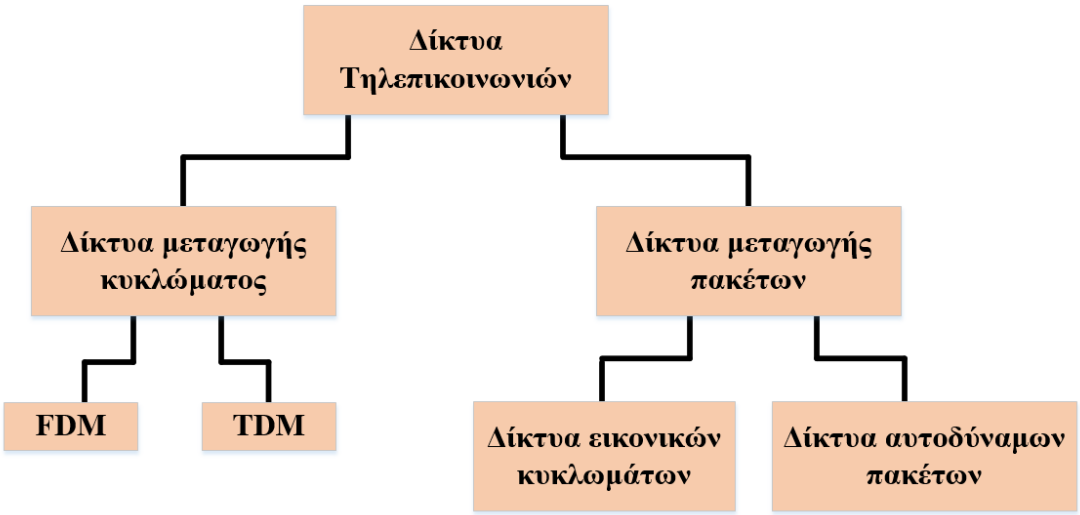
Εξυπηρετούν υπηρεσίες πολλών ειδών και προσφέρουν την διασύνδεση μεταξύ χρηστών σε όλο τον κόσμο. Το βασικότερο δημόσιο δίκτυο είναι το Διαδίκτυο και λειτουργεί για τα δεδομένα με τον ίδιο τρόπο που λειτουργεί το Παγκόσμιο Δημόσιο Τηλεφωνικό Δίκτυο ή PSTN (Public Switched Telephone Network).

1.3.3 Με βάση την τεχνική προώθησης πληροφορίας

Όπου έχουμε δύο κατηγορίες:

1. **Μεταγωγή κυκλώματος:** Όπου δημιουργείται ένα αποκλειστικό κύκλωμα για κάθε κλήση. Για να επικοινωνήσουν δύο σταθμοί αποκαθίσταται μια αποκλειστική φυσική σύνδεση μεταξύ τους που διατηρείται σταθερή καθ' όλη την διάρκεια της επικοινωνίας. Αποτελείται από μια σειρά συνδέσεων μεταξύ των κόμβων και του δικτύου.

2. **Μεταγωγή πακέτων:** Όπου εδώ τα δεδομένα μεταφέρονται μέσω δικτύου με την μορφή πακέτων. Τα προς μετάδοση μηνύματα τεμαχίζονται σε πακέτα (μέγιστο 1000 bytes). Κάθε πακέτο περιέχει ένα τμήμα ωφέλιμης πληροφορίας, μια διεύθυνση προορισμού και έναν αριθμό σειράς. Κάθε κόμβος μεταγωγής πακέτου χρησιμοποιεί την διεύθυνση προορισμού του πακέτου για να αποφασίσει σε ποίον κόμβο θα το προωθήσει. Οι αριθμοί σειράς πακέτων χρησιμοποιούνται από τον σταθμό προορισμού για να ανακατασκευάσει το μήνυμα.

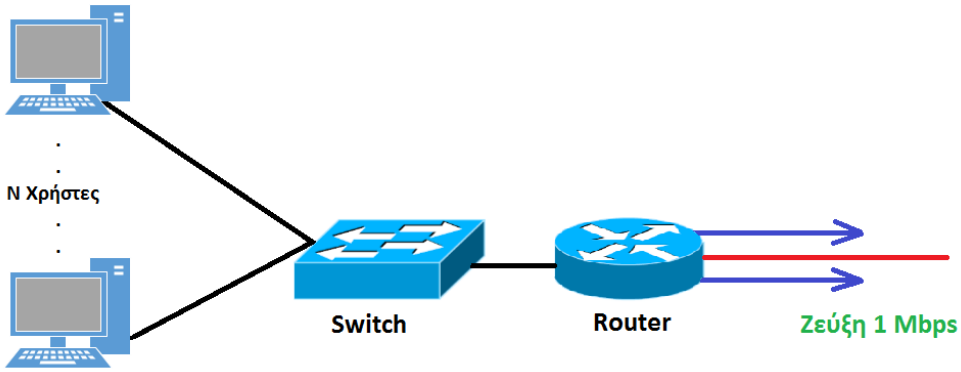


Εικόνα 1.1. Ιεραρχικός σχεδιασμός των τηλεπικοινωνιακών δικτύων

Θεμελιώδες ερώτημα:

Ποία από τις δύο τεχνικές μας δίνει την δυνατότητα να έχουμε περισσότερους χρήστες στο δίκτυο μας ;

Έστω ότι έχουμε το παρακάτω δίκτυο:



Εικόνα 1.2. Δίκτυο με ταχύτητα ζεύξης 1 Mbps

Όπου κάθε χρήστης:

- Έχει 100 kbps όταν είναι ενεργός
- Και είναι ενεργός στο 10% του χρόνου

Μεταγωγή Πακέτων	Μεταγωγή Κυκλώματος
Με 35 χρήστες πιθανότητα να είναι περισσότεροι από 10 ενεργοί χρήστες.	Μέχρι 10 ενεργούς χρήστες

Πίνακας 1.1. Επίδοση των εν λόγω τεχνικών προώθησης πληροφορίας

Η μεταγωγή πακέτων είναι ιδανική για δεδομένα που χαρακτηρίζονται από σποραδικότητα (bursty) διότι:

- Διαμοιράζει τους πόρους
- Είναι απλούστερη και δεν απαιτεί εγκαθίδρυση σύνδεσης

Το πρόβλημα είναι ότι η μεταγωγή πακέτων εμφανίζει υπερβολική συμφόρηση:

- Καθυστέρηση πακέτων και απώλειες
- Απαιτούνται πρωτόκολλα για την αξιόπιστη μεταφορά δεδομένων και έλεγχο συμφόρησης

Υπάρχει όμως τρόπος να συμπεριφερθεί όπως η μεταγωγή κυκλώματος ;

Υπάρχουν μηχανισμοί ποιότητας υπηρεσιών (Quality of Service - QoS) που δίνουν προτεραιότητα σε πακέτα που ανήκουν σε υπηρεσίες που απαιτούν σταθερή ροή πληροφοριών για την καλή λειτουργία τους όπως υπηρεσίες φωνής ή video.

Μεταγωγή Πακέτων	Μεταγωγή Κυκλώματος
Κάθε ροή δεδομένων διαιρείται σε πακέτα	Δέσμευση πόρων από άκρο σε άκρο
Κάθε πακέτο χρησιμοποιεί όλο το bandwidth της ζεύξης	Εύρος ζώνης ζεύξης, χωρητικότητα μεταγωγέα
Πόροι χρησιμοποιούνται μόνο όταν χρειάζεται	Αποκλειστική διάθεση δεσμευμένων πόρων στην κλήση
Συμφόρηση: πακέτα περιμένουν την σειρά τους για μετάδοση στην ουρά	Εγγυημένη απόδοση
Αποθήκευση και προώθηση κατά άλματα (hop by hop)	Απαιτείται εγκαθίδρυση κυκλώματος
Υπερβολική σπατάλη πόρων	Οι δικτυακοί πόροι (πχ bandwidth) διαιρούνται σε κομμάτια
Δεν χρησιμοποιεί τεχνικές όπως η διαίρεση bandwidth σε κομμάτια δέσμευση και αποκλειστική απονομή πόρου	Τα κομμάτια απονέμονται στις κλήσεις
	Πόροι δεν χρησιμοποιούνται όταν η πηγή είναι αδρανής
	Διαίρεση συχνότητας (FDM)
	Διαίρεση χρόνου (TDM)

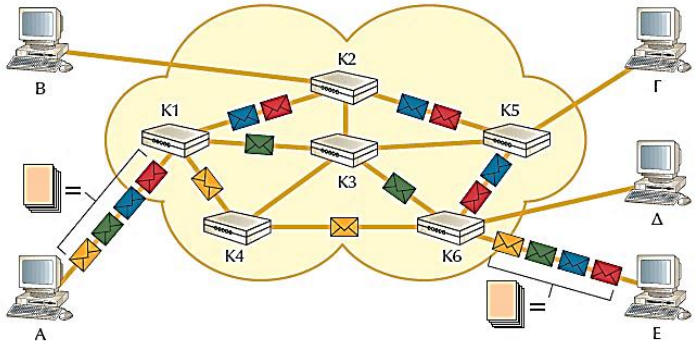
Πίνακας 1.2. Σύγκριση τεχνικών μεταγωγής πακέτου και μεταγωγής κυκλώματος

1.4 Προώθηση πακέτων στα δίκτυα μεταγωγής

Στόχος είναι η μετακίνηση των πακέτων απ' την πηγή στον προορισμό μέσω δρομολογητών (routers). Αυτό το αναλαμβάνουν αλγόριθμοι δρομολόγησης (routing algorithms) που επιλέγουν την διαδρομή μεταξύ πηγής και προορισμού. Για να μην μπερδευτούμε, τον τρόπο με τον οποίο λειτουργούν οι αλγόριθμοι δρομολόγησης θα την αναλύσουμε εκτεταμένα στο 2^{ο} κεφάλαιο.
Στα δίκτυα μεταγωγής υπάρχουν δύο μέθοδοι μετάδοσης τα **αυτοδύναμα πακέτα** και τα **εικονικά κυκλώματα.**

1.4.1 Αυτοδύναμα πακέτα

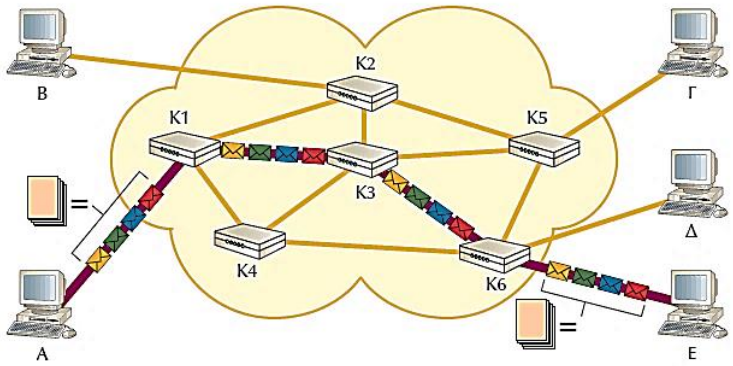
Όπου στην μέθοδο αυτή το κάθε πακέτο ακολουθεί την δική του διαδρομή μέσα στο δίκτυο. Η επιλογή αυτή εξαρτάται από τον αριθμό των πακέτων που περιμένουν να σταλούν σε κάθε κόμβο. Κάθε φορά, επιλέγεται η καλύτερη διαδρομή (π.χ. χρονικά συντομότερη).



Εικόνα 1.3. Προώθηση πακέτων με την μέθοδο αυτοδύναμου πακέτου

1.4.2 Εικονικά κυκλώματα

Στην μέθοδο του εικονικού κυκλώματος πριν αρχίσει η ανταλλαγή πακέτων, επιλέγεται η καλύτερη διαδρομή. Αυτήν την διαδρομή επιλέγουν όλα τα πακέτα από την έναρξη έως τον τερματισμό της σύνδεσης.



Εικόνα 1.4. Προώθηση πακέτων με την μέθοδο εικονικού κυκλώματος

1.4.3 Σύγκριση Αυτοδύναμων πακέτων με εικονικών κυκλωμάτων

Αυτοδύναμα Πακέτα	Εικονικά Κυκλώματα
Η διεύθυνση προορισμού που περιέχεται στο πακέτο προσδιορίζει τον επόμενο κόμβο Οι διαδρομές ενδέχεται να μεταβληθούν κατά την διάρκεια ενός session	Κάθε πακέτο φέρει μια «ετικέτα» (ID εικονικού κυκλώματος) που προσδιορίζει τον επόμενο κόμβο Η διαδρομή προσδιορίζεται κατά την εγκαθίδρυση κλήσης και παραμένει αμετάβλητη καθόλη την διάρκεια της Οι δρομολογητές διατηρούν πληροφορία για την κατάσταση κάθε κλήσης

Πίνακας 1.3. Σύγκριση μεθόδων αυτοδύναμων πακέτων και εικονικών κυκλωμάτων

Το πλεονέκτημα των εικονικών κυκλωμάτων έναντι του αυτοδύναμου πακέτου είναι ότι λαμβάνει ταξινομημένα τα πακέτα, κάτι που συνεπάγεται στην εύκολη και χωρίς ελέγχους και καθυστερήσεις μετάδοση και ανασύσταση του μηνύματος.

Ζήτημα	Αυτοδύναμα πακέτα	Εικονικά κυκλώματα
Εγκαθίδρυση σύνδεσης	Δεν χρειάζεται	Απαραίτητη
Διευθυνσιοδότηση	Κάθε πακέτο περιέχει την πλήρη διεύθυνση προορισμού	Κάθε πακέτο περιέχει ένα μικρό αριθμό εικονικού κυκλώματος
Πληροφορίες κατάστασης	Οι δρομολογητές δεν διατηρούν πληροφορίες για τις συνδέσεις	Κάθε εικονικό κύκλωμα απαιτεί χώρο στους πίνακες δρομολόγησης ανά σύνδεση
Δρομολόγηση	Κάθε πακέτο δρομολογείται ανεξάρτητα	Το δρομολόγιο επιλέγεται όταν εγκαθιδρύεται το κύκλωμα, και όλα τα πακέτα το ακολουθούν
Επιπτώσεις κατάρρευσης δρομολογητών	Καμία, εκτός από τα πακέτα που χάνονται κατά την κατάρρευση	Όλα τα κυκλώματα τα οποία περνούσαν από το δρομολογητή που κατέρρευσε τερματίζονται
Ποιότητα υπηρεσιών	Δύσκολη	Εύκολη, εφόσον μπορούν να εκχωρηθούν προκαταβολικά επαρκείς πόροι για κάθε εικονικό κύκλωμα
Έλεγχος συμφόρησης	Δύσκολη	Εύκολος, εφόσον μπορούν να εκχωρηθούν προκαταβολικά επαρκείς πόροι για κάθε εικονικό κύκλωμα

Πίνακας 1.4. Ζητήματα που προκύπτουν σε αυτοδύναμα πακέτα και εικονικά κυκλώματα

1.5 Υλοποίηση της Διασύνδεσης

Για να επικοινωνήσουν δύο υπολογιστικές συσκευές πρέπει να υπάρξει μεταξύ τους **φυσική** και **λογική διασύνδεση**.

1.5.1 Διασύνδεση σε Φυσικό επίπεδο. Η διασύνδεση επιτυγχάνεται χρησιμοποιώντας:

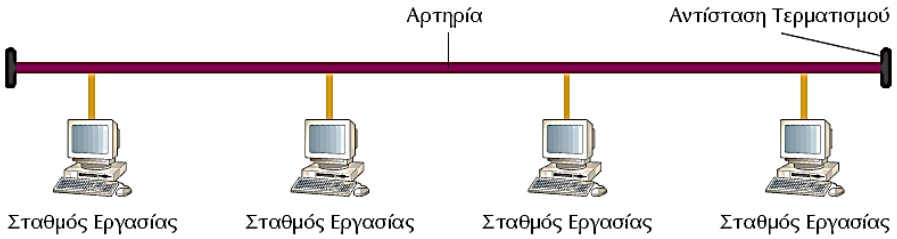
1. **Φυσικά Μέσα Μετάδοσης:** Είναι τα μέσα ή οι φορείς που διακινούν την πληροφορία. Τα πιο συνηθισμένα μέσα μετάδοσης είναι το ομοαξονικό καλώδιο, το συνεστραμμένο ζεύγος καλωδίων και οι οπτικές ίνες. Κάθε φυσικό μέσο διασύνδεσης έχει τα δικά του χαρακτηριστικά, αυτά μπορεί να είναι το εύρος ζώνης και ανοχή στον θόρυβο τα οποία επηρεάζουν σημαντικά τον τρόπο και την ταχύτητα μετάδοσης

2. **Τοπολογία Δικτύου:** Καθορίζει τον τρόπο με τον οποίο θα διασυνδέονται οι συσκευές που υπάρχουν σε ένα δίκτυο. Ένα απλό παράδειγμα τοπολογίας μπορεί να θεωρηθεί η σύνδεση σημείου προς σημείο (point to point). Οι υπόλοιπες τοπολογίες θεωρούνται απλά ως δίκτυα μεταγωγής κυκλώματος, όπου σε αυτήν

την περίπτωση κάθε κόμβος συνδέεται με όλους τους υπόλοιπους. Οι τοπολογίες δικτύων που χρησιμοποιούνται είναι οι εξής:

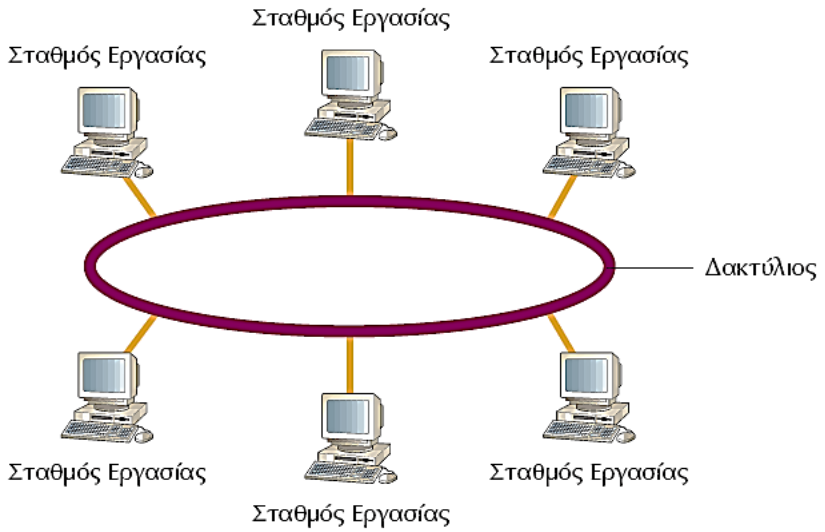
Βασικές τοπολογίες:

- **Αρτηρίας ή διαύλου (bus):** Όπου οι σταθμοί εργασίας συνδέονται σε ένα κοινό διαμοιραζόμενο επικοινωνιακό φυσικό μέσο.



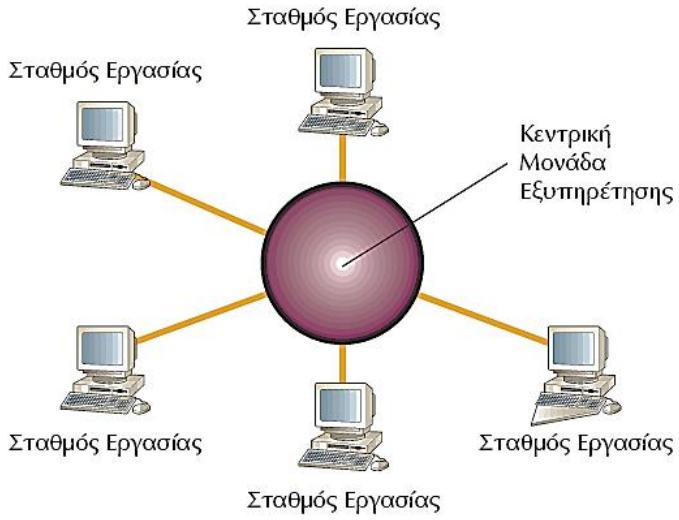
Εικόνα 1.5. Παράδειγμα τοπολογίας διαύλου

- **Δακτυλίου (ring):** Όπου στην τοπολογία αυτή υπάρχει κλειστή διαδρομή του φυσικού μέσου και οι σταθμοί εργασίας συνδέονται κανονικά.



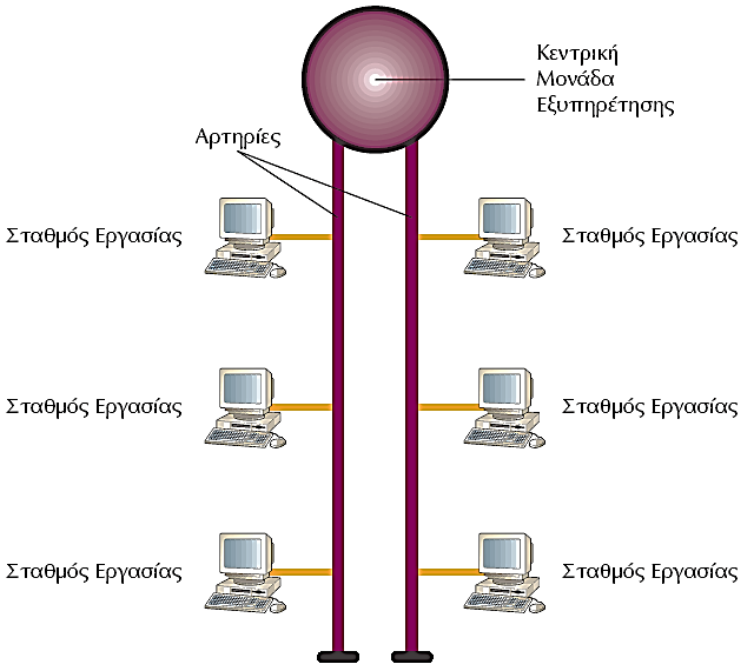
Εικόνα 1.6. Παράδειγμα τοπολογίας δακτυλίου

- **Αστέρα (star):** Όπου οι σταθμοί εργασίας συνδέονται με μητρική μονάδα εξυπηρέτησης.



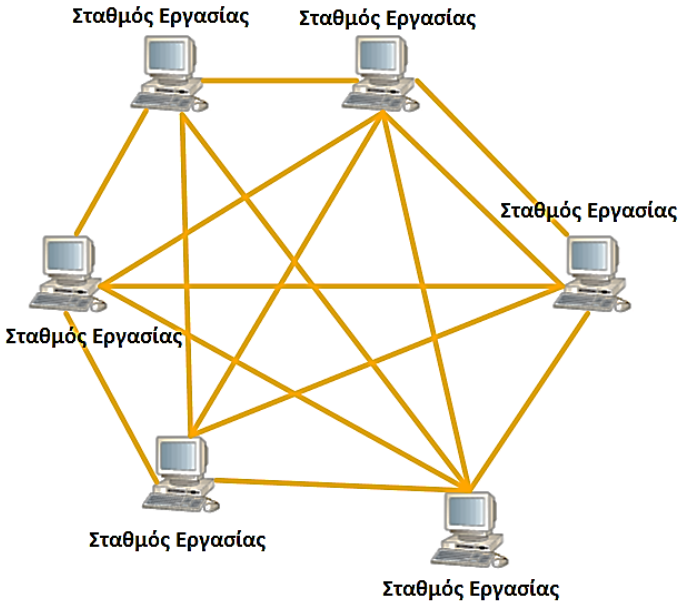
Εικόνα 1.7. Παράδειγμα τοπολογίας αστέρα

- **Δευτερεύοντες τοπολογίες:**
  - **Δέντρου (tree):** Η τοπολογία δέντρου είναι συνδυασμός των τοπολογιών αστέρα και διαύλου. Το δίκτυο έχει έναν κεντρικό κόμβο όπου πάνω σε αυτόν συνδέονται με τοπολογία αρτηρίας.



Εικόνα 1.8. Παράδειγμα τοπολογίας δέντρου

- **Δικτυωτή (mesh):** Όπου κάθε υπολογιστική συσκευή ή/και συσκευή δικτύου είναι διασενδεδεμένες μεταξύ τους με μια άλλη αντίστοιχα. Αυτό επιτρέπει την δυνατότητα να διανεμηθούν περισσότερες μεταδόσεις ακόμη και σε περίπτωση που μία από τις συνδέσεις δεν λειτουργεί. Αυτή η τοπολογία δεν είθισται να χρησιμοποιείται για διασύνδεση υπολογιστών καθότι είναι πολύ δύσκολο αλλά και πολύ δαπανηρό να υπάρχουν περιττές συνδέσεις σε κάθε υπολογιστή.



Εικόνα 1.9. Παράδειγμα δικτυωτής τοπολογίας

3. **Μέθοδος πρόσβασης στο μέσο.** Στα δίκτυα μεταγωγής κυκλώματος, όπου όλοι οι κόμβοι έχουν πρόσβαση σε κοινό μέσο, απαιτείται μια μέθοδος που θα εξασφαλίζει ποιος κόμβος μεταδίδει κάθε φορά. Οι βασικές μέθοδοι είναι τρεις:
   - με ανταγωνισμό (π.χ. Ethernet)
   - με διαβούλευση (π.χ. Token Ring)
   - με πολυπλεξία (π.χ. Time Division Multiplexing)

4. **Τεχνική Μετάδοσης και κωδικοποίησης δεδομένων.** Για να σταλεί η πληροφορία στον παραλήπτη, θα πρέπει να μετατραπεί στη μορφή που το μέσο μπορεί να μεταδώσει. Οι κυριότερες τεχνικές μετάδοσης είναι:
   - βασικής / ευρείας ζώνης
   - ψηφιακού / αναλογικού σήματος
   - διαμόρφωση / αποδιαμόρφωση
   - σύγχρονη / ασύγχρονη

5. **Ταχύτητα μετάδοσης.** Η ταχύτητα μετάδοσης εξαρτάται πάντα από το μέσο και από την τεχνική που χρησιμοποιείται κατά την μετάδοση. Μετρείται σε bits/sec.

6. **Εξοπλισμός διασύνδεσης.** Είναι όλα τα απαραίτητα εξαρτήματα που συνδέουν τις συσκευές με το μέσο επικοινωνίας.

1.5.2 Διασύνδεση σε Λογικό επίπεδο

Πέραν από την φυσική διασύνδεση είναι αναμενόμενο ότι θα πρέπει να δημιουργηθεί και μια λογική σύνδεση μεταξύ των κόμβων που πρόκειται να επικοινωνήσουν. Η λογική σύνδεση αυτή πρέπει να περιλαμβάνει τα εξής:

1. **Αποκατάσταση σύνδεσης.** Η οποία πραγματοποιείται με μηχανισμούς λογικής σύνδεσης και ανεύρεσης του κόμβου προορισμού μέσω διευθυνσιοδότησης.

2. **Μεταφορά δεδομένων.** Η οποία υλοποιείται με λειτουργίες τεμαχισμού της προς μετάδοση πληροφορίας σε πακέτα μεταφοράς ίσου μεγέθους το καθένα. Ο κατακερματισμός της πληροφορίας είναι αναγκαίος διότι αλλιώς δεν μπορούμε να στείλουμε όλα τα δεδομένα κατευθείαν στο φυσικό μέσο λόγω του ότι θα έχουμε πολλά σφάλματα, αρκετή καθυστέρηση μέχρι να φτάσει στον δέκτη, συμφόρηση στο δίκτυο κλπ. Στην συνέχεια αφού η πληροφορία τεμαχιστεί σε πακέτα ίσου μεγέθους πραγματοποιείται:

    - Δρομολόγηση των πακέτων
    - Ανίχνευση λαθών και επαναμετάδοση
    - Έλεγχος ροής και ακολουθίας των πακέτων
    - Και τέλος η επανασυναρμολόγηση των πακέτων η οποία πραγματοποιείται στον κόμβο προορισμού προκειμένου να εξαχθεί η αρχική πληροφορία.

3. **Τερματισμός σύνδεσης.** Η οποία πραγματοποιείται με μηχανισμούς τερματισμού της σύνδεσης. Όλες οι διασυνδέσεις απαιτούν την χρήση πρωτοκόλλων επικοινωνίας τα οποία, ανεξάρτητα της αρχιτεκτονικής που χρησιμοποιείται, οργανώνονται σε ομάδες.

2.1 Εισαγωγή στα τοπικά δίκτυα LAN

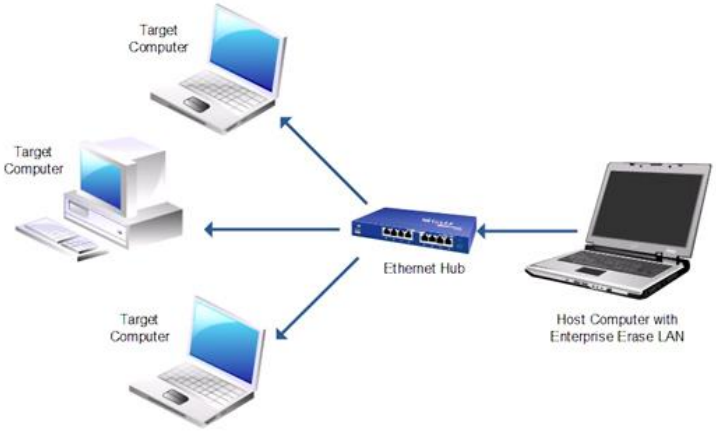
Όταν αναφερόμαστε για δίκτυα LAN, αναφερόμαστε σε δίκτυα τα οποία διαθέτουν:

- Έναν μικρό αριθμό υπολογιστών (π.χ. 10 διασυνδεδεμένους υπολογιστές),
- Και έχουν περιορισμένη γεωγραφική έκταση (π.χ. 1000 μέτρα)

Βέβαια δεν είναι απαραίτητο ότι πρέπει να κυμαίνονται αναγκαστικά σε αυτό το ποσοστό, οι αριθμοί που δώσαμε είναι ενδεικτικοί. Μπορούμε λοιπόν να συμπεράνουμε ότι:

- Όσο μικρότερη έκταση καλύπτει ένα δίκτυο τόσο και μεγαλύτερες ταχύτητες θα έχουμε (έως και Gbps) και συνεπώς θα συμβαίνουν λιγότερα λάθη (1 στα 10^{12} σφάλματα) κατά την μετάδοση δεδομένων.

- Το φυσικό μέσο μετάδοσης που χρησιμοποιείται στα LAN είναι το UTP καλώδιο (δηλαδή το καλώδιο Ethernet).



Εικόνα 2.1. Παράδειγμα διασύνδεσης ενός δικτύου LAN

2.1.1 Παραδείγματα LAN

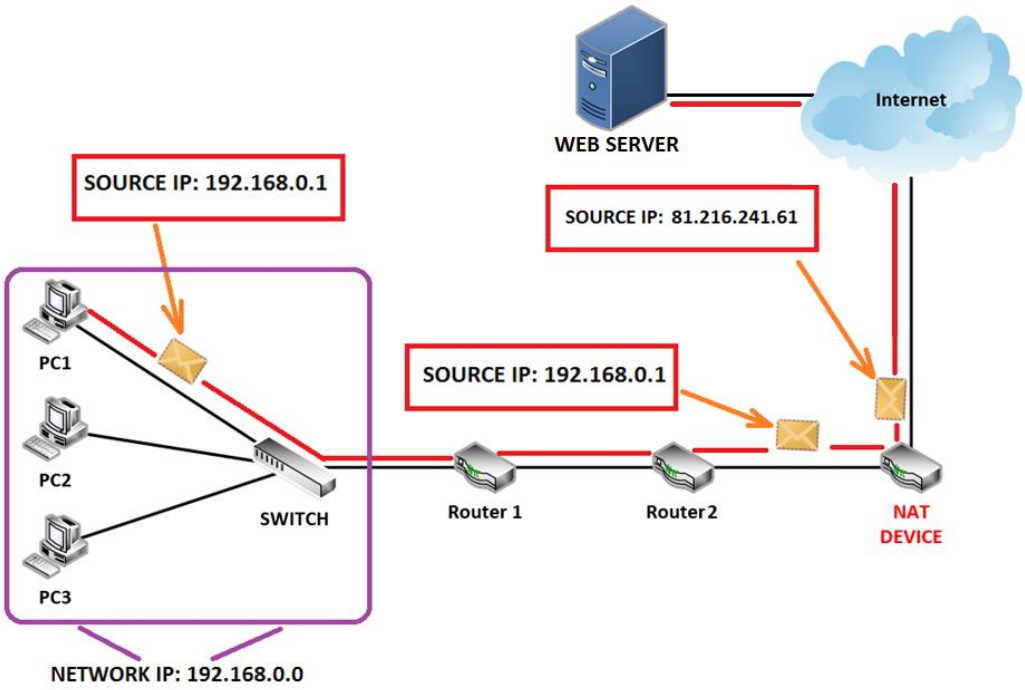
- Το τοπικό δίκτυο μέσα στο σπίτι μας
- Το εσωτερικό δίκτυο μιας εταιρίας
- Το τοπικό δίκτυο σε ένα εργαστήριο με υπολογιστές

2.1.2 Πώς λειτουργεί ένα τοπικό δίκτυο

- Στην εικόνα 2.1 απεικονίζεται ένα απλό παράδειγμα δημιουργίας ενός LAN δικτύου. Αυτό που παρατηρούμε από την εικόνα 2.1 είναι ότι αν συνδέσουμε 2 ή περισσότερους υπολογιστές μεταξύ τους μέσω ενός HUB (διανομέας) ή ενός switch (μεταγωγέα) έχουμε φτιάξει ένα μικρό τοπικό δίκτυο.

- Βέβαια αυτό δεν σημαίνει ότι είναι αρκετό για να πραγματοποιηθεί διασύνδεση με το διαδίκτυο (internet). Χρειάζονται και άλλες διασυνδέσεις πέραν του ενός switch ή ενός hub για την διασύνδεση στο διαδίκτυο. Στην ουσία αυτό που κάνει ένας switch είναι να διασυνδέει πολλούς υπολογιστές παρέχοντας συνήθως μια τελική έξοδο η οποία μπορεί να καταλήγει σε έναν δρομολογητή (router) κοκ.

- Οπότε ένα τοπικό δίκτυο LAN είναι ένα μικρό ιδιωτικό δίκτυο το οποίο διαθέτει πάνω από δύο υπολογιστές οι οποίοι διασυνδέονται μεταξύ τους πάνω σε ένα switch. Η έξοδος αυτού του switch όπως αναφέραμε μπορεί να καταλήγει σε έναν δρομολογητή (router) κοκ. Βέβαια ένα τοπικό δίκτυο LAN έχει την δική του τοπική ιδιωτική διεύθυνση δικτύου IP (private IP). Για να μπορέσει μπορέσει όμως ένα δίκτυο LAN να επικοινωνήσει με το διαδίκτυο χρειάζεται μια δημόσια διεύθυνση IP (public IP). Ο λόγος αυτός οφείλεται διότι σε ένα τοπικό δίκτυο μπορεί να υπάρχουν πολλοί υπολογιστές (παραπάνω του ενός) που να ζητούν πρόσβαση στο διαδίκτυο (internet). Αυτήν την δουλειά λοιπόν αναλαμβάνει μια ειδική συσκευή που ονομάζεται NAT. Το NAT (Network Address Translation) αναλαμβάνει να εκχωρήσει μια εσωτερική IP διεύθυνση για κάθε τοπικό υπολογιστή. Αν το πακέτο βγει από το τοπικό ιδιωτικό δίκτυο μας προς τον ISP (Internet Service Provider) τότε μεταφράζει την τοπική IP σε δημόσια. Για να ξέρει το NAT σε ποίον αντιστοιχεί το πακέτο ή αν λάβει μια απάντηση, κρατάει έναν πίνακα που περιέχει την τοπική διεύθυνση IP.



Εικόνα 2.2. Παράδειγμα λειτουργίας μιας NAT συσκευής σε ένα LAN δίκτυο

Στην εικόνα 2.2 απεικονίζεται η δομή με την οποία λειτουργεί μια NAT συσκευή. Στο παράδειγμα αυτό έχουμε ένα τοπικό δίκτυο LAN με διεύθυνση δικτύου IP την 192.168.0.0. Ο PC1 έχει διεύθυνση IP 192.168.0.1 και επιθυμεί να επικοινωνήσει στο διαδίκτυο. Στο πακέτο αίτησης που θα στείλει ο PC1 περιέχεται η IP διεύθυνση προέλευσης του πακέτου (δηλαδή η IP διεύθυνση του PC1) ώστε να ξέρει ο παραλήπτης ποίος του έστειλε αυτό το πακέτο. Αυτό λοιπόν το πακέτο περνάει μέσα από το δίκτυο και όταν αυτό φτάσει στην NAT συσκευή, στην έξοδο της, θα γίνει η αντιστοίχηση της IP διεύθυνσης πηγής που περιέχεται στο πακέτο με αυτήν του NAT. Δηλαδή, θα γίνει μετάφραση της ιδιωτικής IP 192.168.0.1 σε δημόσια IP που στο παράδειγμα μας είναι η 81.216.241.61 ώστε ο PC1 να μπορεί να έχει επικοινωνία με τον έξω κόσμο (δηλαδή στο διαδίκτυο).

2.1.3 Συνοψίζοντας ένα τοπικό δίκτυο (LAN) περιλαμβάνει

- Έναν αριθμό διασυνδεδεμένων υπολογιστών (πάνω από 2)
- Μια τουλάχιστον συσκευή σύνδεσης (hub ή switch)
- Καλώδια σύνδεσης UTP

- Όπως είδαμε οι IP διευθύνσεις που έχουν οι υπολογιστές μέσα στο LAN δεν έχουν σχέση με τις IP του έξω κόσμου. Για παράδειγμα όλοι σπίτι μας έχουμε την IP 192.168.1.65, και σε πολλές κατοικίες υπάρχουν LAN οπότε θα βρούμε πολλές φορές την IP 192.168.1.65. Οι διευθύνσεις ενός LAN δεν φαίνονται προς τα έξω.

2.2 Βασικά στοιχεία υλοποίησης δικτύων

Ένα δίκτυο αποτελείται από τα εξής βασικά μέρη:

2.2.1 Εξυπηρετητές (Servers)

Οι εξυπηρετητές είναι εξειδικευμένοι υπολογιστές που διαθέτουν λειτουργικό σύστημα και προσφέρουν δικτυακές υπηρεσίες στους τελικούς χρήστες. Κάποιοι βασικοί εξυπηρετητές που λειτουργούν σε ένα δίκτυο περιλαμβάνουν:

- ✓ Αποθήκευση των προγραμμάτων του λειτουργικού συστήματος του δικτύου καθώς και βοηθητικών προγραμμάτων.
- ✓ Αποθήκευση των προγραμμάτων και των δεδομένων των χρηστών του δικτύου.
- ✓ Διαχείριση του συστήματος αρχείων, των διαμοιραζόμενων περιφερειακών συσκευών, δυνατότητα προσπέλασης των χρηστών και της ασφάλειας του δικτύου.
- ✓ Παρακολούθηση της λειτουργίας και της αποδοτικότητας του δικτύου. Είναι πιθανόν να υπάρχουν πολλοί servers (περισσότεροι του ενός) για να υποστηρίξουν τις παραπάνω λειτουργίες. Αυτοί αναφέρονται σαν dedicated servers (αφιερωμένοι servers). Τέτοιοι servers μπορεί να ειναι:

1. **Communication servers (επικοινωνιών)** Όπου διαχειρίζονται τις συνδέσεις μεταξύ των κόμβων του δικτύου καθώς και τις συνδέσεις με άλλα τοπικά δίκτυα ή μεγαλύτερα συστήματα (mainframes) και παρέχουν τη δυνατότητα χρήσης ηλεκτρονικού ταχυδρομείου (e-mail).
2. **file server**: Οπου χρησιμοποιείται σαν χώρος αποθήκευσης αρχείων στον οποίο οι χρήστες έχουν πρόσβαση δικτυακά. Είναι εξυπηρετητές με μεγάλες αποθηκευτικές ικανότητες (συνήθως με σκληρούς δίσκους μερικών TeraBytes) και μεγάλη κεντρική μνήμη.
3. **Backup servers**: Εξυπηρετούν τη λήψη αντιγράφων ασφαλείας των αρχείων και των δεδομένων.
4. **Database servers**: Αποθηκεύουν βάσεις δεδομένων ή αντικειμενοστρεφείς (object-oriented) πληροφορίες που μπορούν να προσπελαστούν από τους χρήστες.
5. **Print servers**: Εξυπηρετούν τις εκτυπώσεις στο δίκτυο δίνοντας το δικαίωμα στους χρήστες να προσαρτώνται στους εκτυπωτές του δικτύου μέσω των ουρών εκτύπωσης. Ο print server εγκαθίσταται συνήθως στον file server ή σε κάποιον αφιερωμένο (dedicated) σταθμό του δικτύου.

Εικόνα 2.3. Εξυπηρετητές (servers) σε ένα server room

2.2.2 Σταθμοί εργασίας (workstations).

Με τον όρο σταθμοί εργασίας αναφερόμαστε σε προσωπικούς υπολογιστές που έχουν το δικό τους λειτουργικό σύστημα και είναι βέβαια διασυνδεδεμένοι στο δίκτυο μέσω καλωδίων και καρτών επικοινωνίας (ή αλλιώς και κάρτες δικτύου). Αντίθετως, μπορούμε να αναφέρουμε έναν σταθμό εργασίας και ως κόμβο επικοινωνίας (communication node).

Εικόνα 2.4. Σταθμοί εργασίας σε μια εταιρία

2.2.3 Κάρτα διασύνδεσης δικτύου (Network Interface Card – NIC)

Όπως αναφέραμε κάθε σταθμός εργασίας περιέχει μια κάρτα διασύνδεσης δικτύου μέσω της οποίας συνδέεται με όλες τις υπόλοιπες συσκευές. Οι κάρτες δικτύων μετατρέπουν τα καθαρά bits του υπολογιστή, σε πληροφορία συμβατή με τα ηλεκτρικά και λειτουργικά χαρακτηριστικά του πρωτοκόλλου του δικτύου. Κάθε κάρτα δικτύου σχεδιάζεται για να περιέχει μια μοναδική φυσική διεύθυνση που εδώ ονομάζεται φυσική διεύθυνση MAC. Η τοποθέτηση μιας κάρτας δικτύου απαιτεί

προσοχή. Πρέπει η διεύθυνση μιας κάρτας δικτύου να μην συμπίπτει με άλλες όπως π.χ. της σειριακής ή της παράλληλης θύρας.

Εικόνα 2.5. Κάρτα δικτύου Ethernet (PCI Express)

Εικόνα 2.6. Ασύρματη κάρτα δικτύου (PCI)

2.2.4 Περιφερειακές συσκευές

Κάθε συσκευή που συνδέεται με ένα υπολογιστικό σύστημα, δεν αποτελεί μέρος αυτού και εξαρτάται περισσότερο ή λιγότερο από αυτό. Οι περιφερειακές συσκευές διευρύνουν τις δυνατότητες του συστήματος, αλλά δεν επηρεάζουν την επεξεργαστική ισχύ (π.χ. εκτυπωτές, σαρωτές, μικρόφωνα κλπ.).

Εικόνα 2.7. Παράδειγμα περιφερειακής συσκευής

2.2.5 Καλώδιο σύνδεσης

Τα πιο συνηθισμένα καλώδια διασύνδεσης υπολογιστικών συσκευών είναι τα χάλκινα καλώδια και οι οπτικές ίνες. Τα χάλκινα καλώδια είναι φθηνά και αποτελούν την πλειοψηφία των εγκαταστάσεων, ενώ οι οπτικές ίνες κερδίζουν συνεχώς έδαφος, λόγω της μείωσης του κόστους, της απλοποίησης των τεχνικών εγκατάστασης και των αναγκών για υψηλότερες ταχύτητες. Υπάρχουν τρεις τύποι χάλκινων καλωδίων:

- Ομοαξονικό
- Συνεστραμμένου ζεύγους με θωράκιση και χωρίς θωράκιση

2.3 Δικτυακές συσκευές διαμεσολάβησης (Intermediary Network Devices)

Οι δικτυακές συσκευές διαμεσολάβησης αναλαμβάνουν τον ρόλο του «διαμεσολαβητή» σε ένα δίκτυο, δηλαδή είναι συσκευές που εξυπηρετούν όλες τις ανάγκες ώστε να γίνει εφικτή η μεταφορά δεδομένων. Τέτοιες συσκευές μπορεί να είναι οι δρομολογητές (routers), μεταγωγείς (switches) και εξειδικευμένες συσκευές όπως συσκευές τείχη προστασίας (firewalls).

2.2.3 Δρομολογητές (routers):

Οι δρομολογητές είναι ηλεκτρονικές συσκευές οι οποίες αναλαμβάνουν την αποστολή και λήψη πακέτων δεδομένων μεταξύ ενός ή περισσοτέρων εξυπηρετητών, άλλων δρομολογητών και πελατών, κατά μήκος πολλαπλών δικτύων. Η δρομολόγηση, δηλαδή η διαδικασία μεταφοράς δεδομένων από το ένα σημείο στο άλλο αποτελεί κεντρική λειτουργία του 3^{ου} επιπέδου (επιπέδου δικτύου) και πραγματοποιείται με βάση διαφόρων κριτήριων (π.χ. καλύτερη δυνατή διαδρομή, χρονικά συντομότερη κλπ). Οι δρομολογητές μπορούν να αξιοποιήσουν ένα ή περισσότερα πρωτόκολλα δρομολόγησης με βάση των οποίων ο δρομολογητής καθορίζει ποια διαδρομή – ζεύξη είναι η καταλληλότερη κάθε χρονική στιγμή και δρομολογεί τα πακέτα δεδομένων προς αυτήν.

Εικόνα 2.8. Συσκευή router της CISCO μοντέλο 2900

2.2.4 Μεταγωγείς (switches)

Ο μεταγωγέας (switch) είναι μια ηλεκτρονική συσκευή που χρησιμοποιείται σε δίκτυα υπολογιστών. Χρησιμοποιείται για την διασύνδεση δικτυακών τερματικών συσκευών (π.χ. υπολογιστές, εξυπηρετητές, εκτυπωτές κτλ) σε ένα δίκτυο δεδομένων. Οι περισσότερες σήμερα σχεδιάσεις τοπικών δικτύων γίνονται με δίκτυα τύπου Ethernet, τα βασικότερα εκ των οποίων αποτελούν οι μεταγωγείς Ethernet. Υπάρχουν δύο κατηγορίες μεταγωγών (switches):

1. **Μεταγωγέας επιπέδου ζεύξης (data link layer switch):** Όπου το κύριο χαρακτηριστικό του είναι ότι κάθε θύρα επικοινωνίας που διαθέτει προσφέρει καθορισμένο εύρος ζώνης σε αντίθεση με το hub, όπου όλες οι συσκευές που συνδέονται σε αυτό, διαμοιράζονται το εύρος ζώνης (bandwidth) του μέσου. Επίσης κάθε θύρα του μεταγωγέα αποτελεί

ξεχωριστό πεδίο συγκρούσεων (collision domain). Ένας μεταγωγέας (switch) δημιουργεί πίνακες προώθησης όπως και οι bridges (γέφυρες) και χρησιμοποιεί τον αλγόριθμο Spanning tree. Αυτόν τον αλγόριθμο θα τον αναλύσουμε στην υποπαράγραφο 2.8.3 προς το παρών ας εξετάσουμε ένα παράδειγμα όπου δυο σταθμοί θέλουν να επικοινωνήσουν και βρίσκονται σε διαφορετικές θύρες του μεταγωγέα (unicast πλαίσιο). Ο μεταγωγέας θα ελέγξει τον πίνακα προώθησης για να βρει την φυσική διεύθυνση MAC προορισμού και σε ποια θύρα καλείτε να το προωθήσει. Αφού βρεθεί η καταχώρηση αυτή θα προωθήσει το πακέτο στην κατάλληλη θύρα επικοινωνίας. Με αυτόν τον τρόπο ο μεταγωγέας (switch) μειώνει την κίνηση (trafic) και τις συγκρούσεις πακέτων (packet collisions) αυξάνοντας την επίδοση του δικτύου και το διαθέσιμο εύρος ζώνης των σταθμών εργασίας.

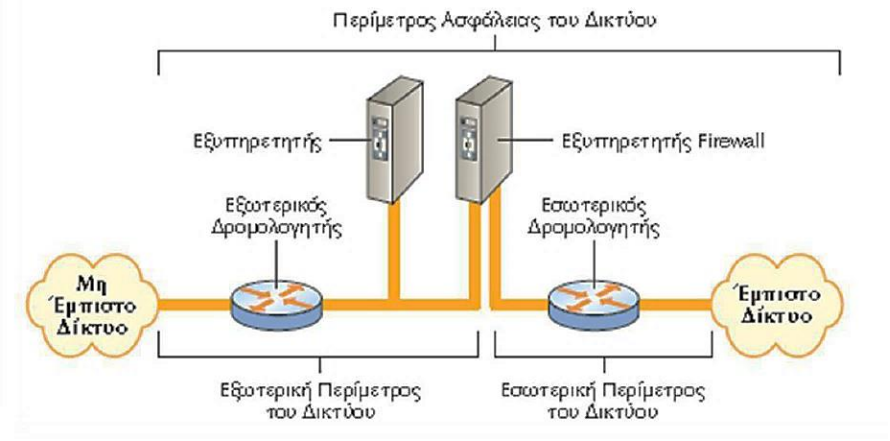
Εικόνα 2.9. Συσκευή switch επιπέδου ζεύξης της CISCO μοντέλο Catalyst 2960

2. **Μεταγωγέας επιπέδου δικτύου (network layer switch):** Όπως αναφέραμε παραπάνω ένας μεταγωγέας (switch) επιπέδου ζεύξης αναλαμβάνει την διασύνδεση υπολογιστικών τερματικών σε ένα δίκτυο και την διαδικασία διαμοιρασμού εύρους ζώνης στο καθένα. Την ίδια λειτουργία αναλαμβάνει και ένας μεταγωγέας (switch) επιπέδου δικτύου με την βασική διαφορά ότι ενσωματώνει βασικές λειτουργίες όπου ανήκουν σε αυτό το επίπεδο όπως δρομολόγηση πακέτων, υπηρεσίες DHCP κλπ. Συνοψίζοντας, ένας μεταγωγέας (switch) επιπέδου δικτύου είναι στην ουσία ένας συνδυασμός ενός μεταγωγέα (switch) και ενός δρομολογητή (router).

Εικόνα 2.10. Συσκευή switch επιπέδου δικτύου της CISCO μοντέλο 7604

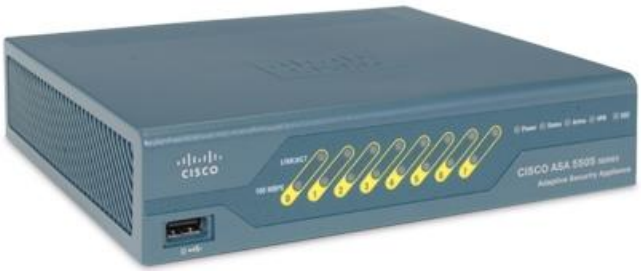
2.2.5 Τείχος Προστασίας (Firewall)

Το τείχος προστασίας (firewall) είναι ένα σύνολο από προγράμματα /φίλτρα, που έχουμε εγκαταστήσει σε πύλες (σημεία σύνδεσης) του εσωτερικού μας δικτύου με άλλα δίκτυα, π.χ. το Internet ή κάποιο άλλο δημόσιο δίκτυο, που δεν ελέγχονται από εμάς. Οι συσκευές που εγκαθίστανται τα προγράμματα/φίλτρα συνθέτουν ένα Firewall, είναι δρομολογητές και εξυπηρετητές ειδικοί για τον σκοπό αυτόν.



Εικόνα 2.11: Παράδειγμα δικτύου με χρήση Firewall

Στην εικόνα 2.11 απεικονίζετε διαχωρισμός ενός εσωτερικού δικτύου μιας επιχείρησης με τα υπόλοιπα δίκτυα με την βοήθεια αρχιτεκτονικής βασισμένης σε δρομολογητές και εξυπηρετητές. Οι χρήστες, που βρίσκονται στο τμήμα του δικτύου ευρείας περιοχής πίσω από τον εσωτερικό δρομολογητή, ανήκουν σε ένα έμπιστο δίκτυο αφού συνδέεται άμεσα από μια δομή που ελέγχεται, διαχειρίζεται και γενικά διέπεται από κανόνες ασφάλειας, που καθορίζονται πλήρως από την εκάστοτε επιχείρηση ή οργανσιμό που διαθέτει αυτό το δίκτυο. Αντιθέτως το δίκτυο ευρείας περιοχής, που συνδέεται με τον εξωτερικό δρομολογητή είναι ένα μη έμπιστο δίκτυο διότι η επιχείρηση δεν διαχειρίζεται εκεί τους χρήστες που ανήκουν σε αυτό. Δηλαδή δεν υπάρχουν διαδικασίες ελέγχου αυθεντικότητας με τους χρήστες του εσωτερικού δικτύου.
Οι κανόνες, που μπορούμε να εφαρμόσουμε σε ένα firewall, είναι να μπορούμε να επιτρέψουμε την πρόσβαση από τα μη έμπιστα δίκτυα προς συγκεκριμένους εξυπηρετητές του εσωτερικού μας δικτύου, καθώς επίσης και το είδος των εφαρμογών, που επιτρέπεται να χρησιμοποιήσουν οι μη έμπιστοι χρήστες, για να συνδεθούν σε αυτούς. Ένα παράδειγμα είναι η πρόσβαση σε συγκεκριμένες IP διευθύνσεις του εσωτερικού δικτύου και με συγκεκριμένα πρωτόκολλα, όπως HTTP, ενώ προσπάθειες σύνδεσης με άλλα πρωτόκολλα όπως telnet, FTP, TFTP rlogin κ.λ.π. να απορρίπτονται από το firewall.

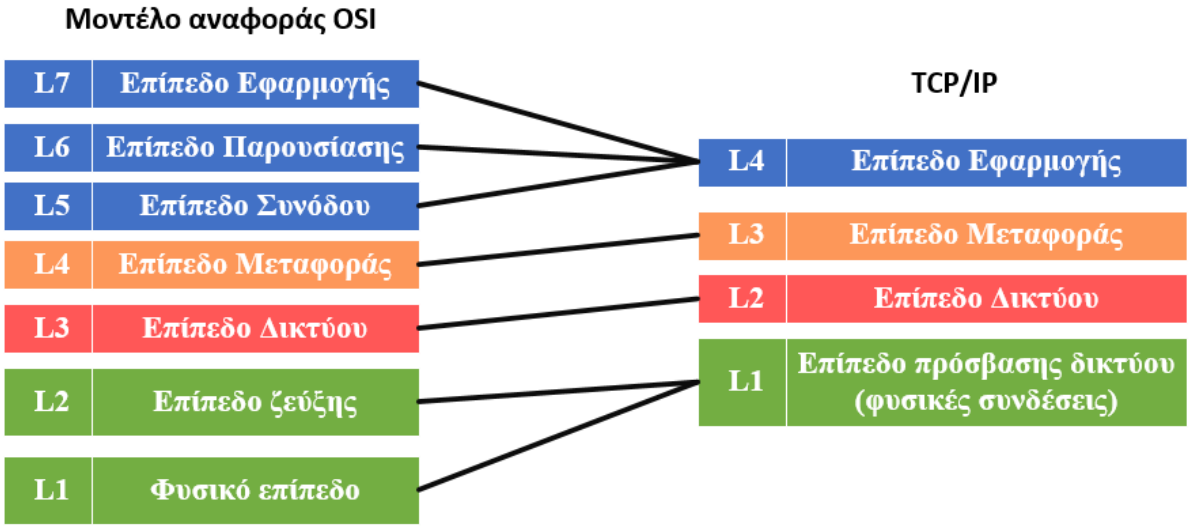


Εικόνα 2.12. Συσκευή ASA Firewall της CISCO μοντέλο 5505

2.4 Πρότυπα και πρωτόκολλα επικοινωνίας

Τα **πρότυπα επικοινωνίας** είναι κανόνες που ορίζουν συγκεκριμένα τμήματα της επικοινωνίας. Αυτά εκδίδονται και αναπτύσσονται από οργανισμούς όπως το IEEE (Institute of Electrical and Electronics Engineers). Όσον αφορά τις δικτυακές επικοινωνίες, το IEEE ορίζει τεχνολογίες όπως Token Ring (IEEE 802.5), Ethernet (IEEE 802.3) και Wi-Fi (IEEE 802.11). Η ύπαρξη των προτύπων βοηθά στη συμβατότητα ανάμεσα στους κατασκευαστές hardware και software.

Ενώ τα **πρωτόκολλα επικοινωνίας** αναφέρονται στους κανόνες που πρέπει να ακολουθεί ένα δίκτυο προκειμένου να επιτευχθεί η αποστολή και η λήψη δεδομένων μεταξύ των κόμβων. Τα πρωτόκολλα αυτά έχουν διάφορες κατηγορίες και λειτουργούν σε διάφορα επίπεδα **μοντέλων επικοινωνίας**. Το καθιερωμένο πλέον μοντέλο επικοινωνίας είναι το TCP/IP το οποίο αποτελεί τον «απόγονο» του μοντέλου αναφοράς OSI. Θα επικεντρωθούμε αργότερα στο μοντέλο επικοινωνίας TCP/IP προς το παρών θα κάνουμε μια μικρή αναφορά στο μοντέλο OSI. Ο λόγος που κάνουμε αυτήν την μικρή αναφορά στο OSI είναι διότι προσφέρει καλύτερη σαφήνεια όσον αφορά τα δύο τελευταία επίπεδα, δηλαδή το μοντέλο ζεύξης και το φυσικό επίπεδο σε σχέση με το TCP/IP που απλά αυτά τα δύο τελευταία επίπεδα τα «βλέπει» ως ένα ενιαίο επίπεδο (Επίπεδο πρόσβασης δικτύου). Το μοντέλο αναφοράς OSI δεν χρησιμοποιείται πλέον και έχει αντικατασταθεί από το TCP/IP. Η κύρια χρήση του μοντέλου αναφοράς OSI είναι περισσότερο για εκπαιδευτικούς σκοπούς. Το μοντέλο αναφοράς OSI αποτελείται από 7 επίπεδα τα οποία είναι το επίπεδο εφαρμογής, επίπεδο παρουσίασης, επίπεδο συνόδου, επίπεδο μεταφοράς, επίπεδο δικτύου, επίπεδο ζεύξης και τέλος το φυσικό επίπεδο. Στην εικόνα 2.13 απεικονίζεται το μοντέλο αναφοράς OSI και το TCP/IP και ποία επίπεδα του OSI αντιστοιχήθηκαν στο TCP/IP.

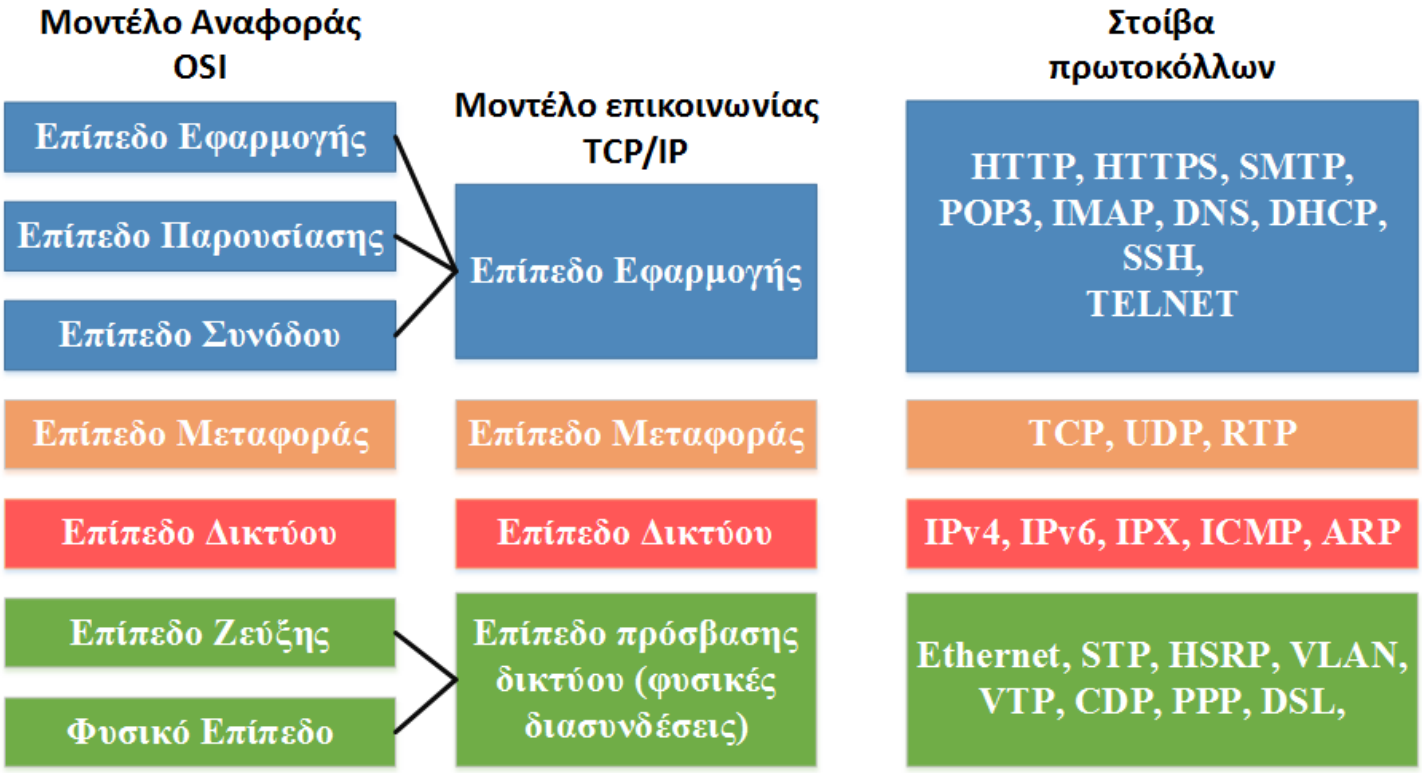


Εικόνα 2.13. Μοντέλο αναφοράς OSI και αντιστοίχιση του κάθε επίπεδου του στο TCP/IP

Όπως βλέπουμε από την εικόνα 2.13 τα επίπεδα του OSI που αντιστοιχήθηκαν στο TCP/IP είναι τα εξής:

- Το φυσικό επίπεδο και το επίπεδο ζεύξης στο Επίπεδο πρόσβασης δικτύου
- Τα επίπεδα δικτύου και μεταφοράς παρέμειναν ως έχει

- Τέλος το επίπεδο συνόδου, παρουσίασης και εφαρμογής ενώθηκαν στο επίπεδο εφαρμογής. Για να περιγράψουμε καλύτερα τα πρωτόκολλα επικοινωνίας εμείς θα επικεντρωθούμε στο μοντέλο OSI και συγκεκριμένα σε αυτά τα επίπεδα που αντιστοιχήθηκαν στο TCP/IP δηλαδή το φυσικό επίπεδο, το επίπεδο ζεύξης το επίπεδο δικτύου το επίπεδο μεταφοράς και το επίπεδο εφαρμογής. Προτού όμως αναφερθούμε στα πρωτόκολλα επικοινωνίας που είναι απαραίτητα για την επικοινωνία σε ένα δίκτυο και γενικά ποία πρωτόκολλα θα χρησιμοποιηθούν στο δίκτυο που έχουμε σκοπό να δημιουργήσουμε ας κάνουμε πρώτα μια γενική επισκόπηση στην στοίβα πρωτοκόλλων. Με τον όρο στοίβα πρωτοκόλλων εννοούμε την ιεραρχική τοποθέτηση των πρωτοκόλλων ανά επίπεδο στο TCP/IP. Κάθε πρωτόκολλο λειτουργεί σε κάποιο συγκεκριμένο επίπεδο του TCP/IP. Η εικόνα 2.14 απεικονίζει την στοίβα πρωτοκόλλων του OSI και του TCP/IP.



Εικόνα 2.14. Στοίβα πρωτοκόλλων ανά επίπεδο στο μοντέλο αναφοράς OSI και στο μοντέλο επικοινωνίας TCP/IP

Όπως βλέπουμε στην εικόνα 2.14 το κάθε πρωτόκολλο λειτουργεί σε ένα συγκεκριμένο επίπεδο είτε αυτό είναι το μοντέλο TCP/IP είτε το OSI. Υπάρχουν πάρα πολλά πρωτόκολλα τα οποία χρησιμοποιούνται σήμερα όποτε θα ήταν άσκοπο να αναφερθούμε σε όλα αυτά τα πρωτόκολλα που υπάρχουν. Εμείς θα επικεντρωθούμε στα πρωτόκολλα τα οποία είναι πολύ βασικά για την λειτουργία ενός δικτύου όπως για παράδειγμα το TCP, UDP, HTTP, SMTP, SSH, DHCP κλπ και σε αυτά τα οποία θα ικανοποιήσουν τις ανάγκες του δικού μας δικτύου. Οπότε σε αυτό το σημείο μπορούμε να ξεκινήσουμε την εισαγωγή μας στα διάφορα πρωτόκολλα επικοινωνίας, και να δούμε την λειτουργία και ποία η χρησιμότητα τους σε ένα δίκτυο.

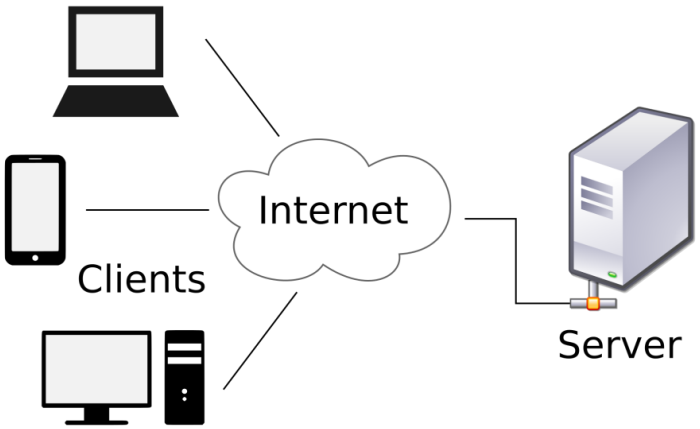
2.5 Επίπεδο εφαρμογής (Application Layer – Layer 7)

Προτού κάνουμε την αναφορά μας στα πρωτόκολλα αυτού του επίπεδου ας κάνουμε μια μικρή εισαγωγή πάνω σε αυτό. Το επίπεδο εφαρμογής είναι το μέρος όπου βρίσκονται οι διάφορες δικτυακές εφαρμογές μαζί με τα πρωτόκολλα που το απαρτίζουν. Το επίπεδο εφαρμογής περιλαμβάνει πολλά πρωτόκολλα όπως το HTTP (για υποστήριξη αίτησης και μεταφοράς εγγράφων του Web), το SMTP (για υποστήριξη μεταφοράς μηνυμάτων ηλεκτρονικού ταχυδρομείου) το FTP (για υποστήριξη μεταφοράς αρχείων ανάμεσα σε δύο τερματικά συστήματα) το DNS (που αναλαμβάνει να αποδώσει ένα domain σε μια IP διεύθυνση) κλπ.

Ας προχωρήσουμε όμως σε κάτι πολύ σημαντικό που είναι η αρχιτεκτονική εφαρμογής (application architecture). Με τον όρο αρχιτεκτονική εφαρμογής εννοούμε τον τρόπο με τον οποίο δομείται μια εφαρμογή σε διάφορα τερματικά συστήματα και σχεδιάζεται από τον αποκλειστικά προγραμματιστή εφαρμογών. Κατά πάσα πιθανότητα ένας προγραμματιστής εφαρμογών θα επιλέξει ανάμεσα σε δύο κυρίαρχα μοντέλα δικτυακών εφαρμογών, την **αρχιτεκτονική πελάτη – εξυπηρετητή** και την **αρχιτεκτονική ομότιμων συστημάτων (Peer-To-Peer ή P2P).**

2.5.1 Αρχιτεκτονική πελάτη εξυπηρετητή

Σε μια αρχιτεκτονική **πελάτη-εξυπηρετητή (client-server architecture)** υπάρχει ένας πάντα ενεργός σε λειτουργία κόμβος που είναι ο εξυπηρετητής (server) και σκοπός του είναι να εξυπηρετήσει πολλούς διαφορετικούς υπολογιστές οι οποίοι λέγονται πελάτες. Θα πρέπει όμως να σημειώσουμε ότι ένας και μόνο ένας εξυπηρετητής δεν είναι ικανός να ικανοποιήσει όλα τα αιτήματα από τους πελάτες του. Γι αυτόν τον λόγο χρησιμοποιείται ένα σύμπλεγμα υπολογιστών που ονομάζεται κέντρο δεδομένων (data center) το οποίο φιλοξενεί έναν μεγάλο αριθμό υπολογιστών, για να δημιουργήσει έναν ισχυρό εικονικό εξυπηρετητή (server).

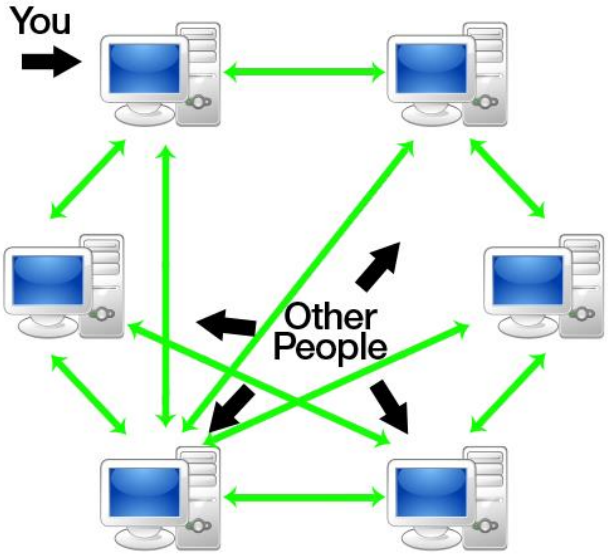


Εικόνα 2.15: Παράδειγμα επικοινωνίας πελάτη-εξυπηρετητή Client - Server

2.5.2 Αρχιτεκτονική ομότιμων συστημάτων

Σε μια αρχιτεκτονική peer-to-peer υπάρχει μικρή ή και καμία στήριξη σε αποκλειστικούς εξυπηρετητές (servers) σε κέντρα δεδομένων. Αντιθέτως, η εφαρμογή εκμεταλλεύεται την απευθείας επικοινωνία ανάμεσα σε ζεύγη κατά διαλλείματα συνδεδεμένων υπολογιστών που καλούνται ομότιμοι (peers). Οι ομότιμοι αυτοί υπολογιστές δεν ανήκουν σε αυτόν που παρέχει στην υπηρεσία αλλά μπορεί να είναι οποιοσδήποτε ακόμη και προσωπικοί υπολογιστές που βρίσκονται σε κατοικίες.

Με λίγα λόγια το peer-to-peer είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα.
Ένα απ' τα βασικότερα χαρακτηριστικά των αρχιτεκτονικών P2P είναι η αποκλιμάκωση τους (self-scalability). Για παράδειγμα, για το διαμοιρασμό αρχείων, πέραν του ότι κάθε ομότιμος ζητάει αρχεία δημιουργώντας φόρτο εργασίας δίνει επίσης την δυνατότητα εξυπηρέτησης στο σύστημα διανέμοντας κι αυτός με την σειρά του αρχεία προς άλλους ομότιμους. Ένα παράδειγμα χρήσης ομότιμων συστημάτων είναι το BitTorrent, μTorrent κλπ.



Εικόνα 2.16: Παράδειγμα peer-to-peer

2.5.3 Διεργασίες Πελάτη (Client) – Εξυπηρετητή (Server)

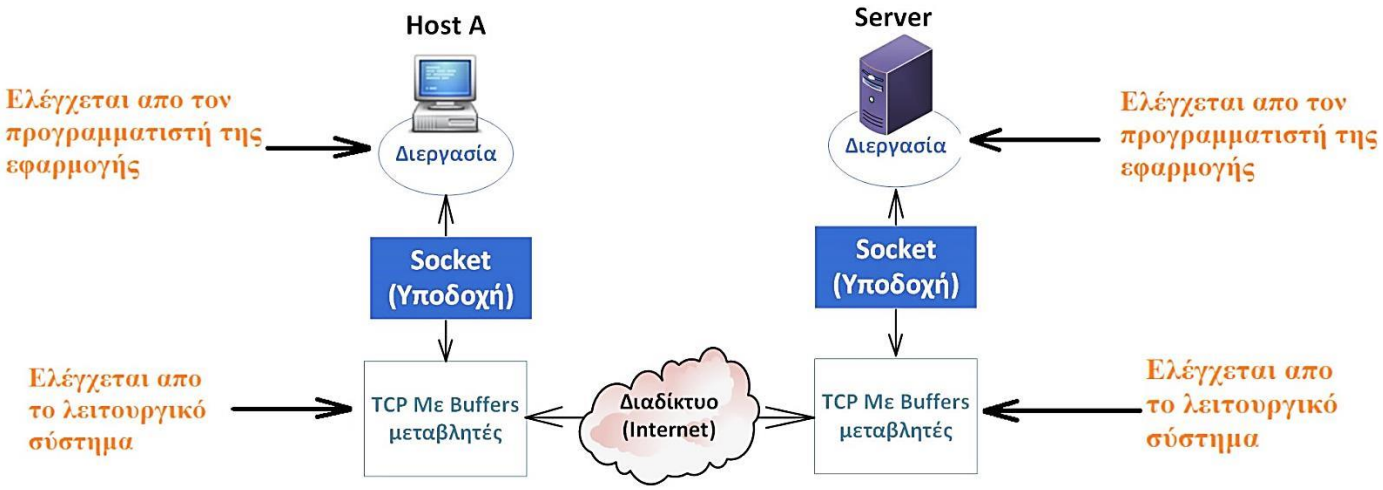
Μια δικτυακή εφαρμογή αποτελείται από ζεύγη διεργασιών, που στέλνουν μηνύματα η μία στην άλλη σε ένα δίκτυο. Για παράδειγμα, μια διεργασία πελάτης ανταλλάσει μηνύματα με μια διεργασία εξυπηρετητή. Σε ένα σύστημα διαμοιρασμένων αρχείων Peer-to-Peer, ένα αρχείο μεταφέρεται από μια διεργασία που βρίσκεται σε έναν ομότιμο, προς μια άλλη διεργασία που βρίσκεται σε έναν άλλο ομότιμο. Για κάθε ζεύγος διεργασιών που επικοινωνούν μεταξύ τους συνήθως λέμε την μια από τις δύο πελάτη (client) και την άλλη εξυπηρετητή (server).
Για παράδειγμα, έστω ότι εμείς χρησιμοποιούμε τον περιηγητή μας (browser) για να επισκεφτούμε μια ιστοσελίδα. Η διεργασία πελάτης είναι ο browser μας και η διεργασία εξυπηρετητής είναι ο server.

Σημαντική παρατήρηση

Κατά την διάρκεια μίας συνόδου επικοινωνίας ανάμεσα σε ένα ζεύγος διεργασιών, η διεργασία που εκκινεί την επικοινωνία (δηλαδή έρχεται αρχικά σε επαφή με την άλλη διεργασία, στην αρχή της συνόδου) προσδιορίζεται ως πελάτης. Η διεργασία που περιμένει να έρθει κάποια άλλη διεργασία σε επαφή μαζί της ώστε να αρχίσει την σύνοδο, είναι ο εξυπηρετητής.

2.5.4 Επικοινωνία διεργασιών μέσω δικτύου

Προηγουμένως αναφέραμε ότι οι περισσότερες εφαρμογές αποτελούνται από ζεύγη διεργασιών που επικοινωνούν μεταξύ τους στέλνοντας μηνύματα η μια στην άλλη. Μια διεργασία λοιπόν για να στείλει και να λάβει μηνύματα από το δίκτυο το κάνει μέσω μιας διεπαφής που ονομάζεται socket (υποδοχή). Για να καταλάβουμε τι είναι το socket και πως αυτό λειτουργεί σε μια λειτουργία εφαρμογής ας δούμε την εικόνα 2.17.



Εικόνα 2.17: Διεργασίες εφαρμογής, sockets και το υπερκείμενο πρωτόκολλο μεταφοράς

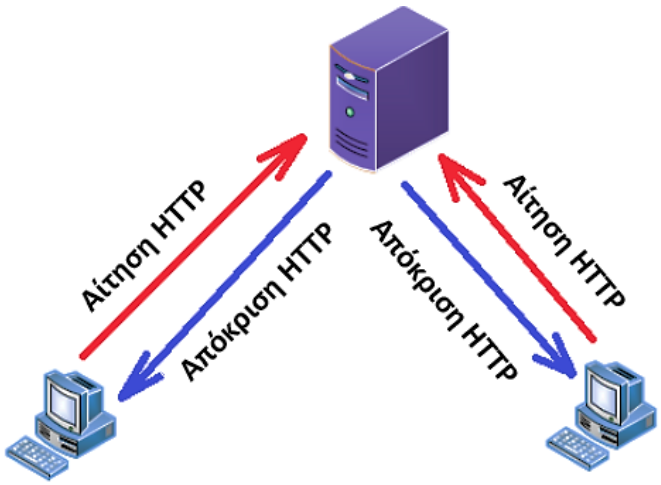
Όπως βλέπουμε η διεργασία του Host A στέλνει μήνυμα προς τον Server. Καθώς η διεργασία του Host A στέλνει το μήνυμα περνάει από το δικό της socket και στην συνέχεια αυτό είναι υπεύθυνο για την επικοινωνία με την εφαρμογή του Server. Την ίδια επίσης δουλειά μπορεί να κάνει και η διεργασία του server. Σε αυτό το επίπεδο έχουμε επικοινωνία μεταξύ δύο εφαρμογών.

Το διαδίκτυο και κατά συνέπεια ολόκληρη η τεχνολογία TCP/IP υποστηρίζει δύο τύπους μεταφοράς δεδομένων, το Transmission Control Protocol – TCP που χρησιμοποιείται για αξιόπιστη επικοινωνία και το User Datagram Protocol – UDP που χρησιμοποιείται για αναξιόπιστη επικοινωνία.

Το TCP το χρησιμοποιούμε για εφαρμογές που απαιτούν αξιοπιστία (πχ. για μεταφορά δεδομένων) διότι υπάρχουν μηχανισμοί οι οποίοι ανακτούν ένα πακέτο σε περίπτωση που χαθεί κατά την μετάδοση. Με λίγα λόγια το πρωτόκολλο TCP εγγυάται ότι τα δεδομένα θα φτάσουν ακέραια στον προορισμό τους χωρίς να αλλοιωθούν.
Το UDP το χρησιμοποιούμε σε εφαρμογές που η απώλειες πακέτων δεν αποτελούν σοβαρό πρόβλημα (π.χ. για μεταφορά φωνής όπως Skype ή εικόνας Youtube) και μας ενδιαφέρει περισσότερο η ταχύτητα μεταφοράς δεδομένων. Παρόλα αυτά αν χαθεί ένα πακέτο υπάρχουν μηχανισμοί για να συγχρονίσει την ροή των δεδομένων ώστε να μην παρατηρήσουμε εμείς έντονα το πρόβλημα. Επειδή όμως τα πρωτόκολλα TCP και UDP ανήκουν στο επίπεδο μεταφοράς θα κάνουμε μια πιο εκτενή αναφορά σε αυτά όταν φτάσουμε σε αυτό. Τα πρωτόκολλα λοιπόν που χρησιμοποιεί το επίπεδο εφαρμογής είναι τα εξής:

2.5.5 HyperText Transfer Protocol – HTTP

Το πρωτόκολλο μεταφοράς υπερκειμένου (HyperText Transfer Protocol – HTTP) βασίζεται στο μοντέλο πελάτη – εξυπηρετητή (client – server). Δηλαδή χωρίζεται σε δύο προγράμματα, που το ένα είναι του πελάτη (client) και το άλλο είναι του εξυπηρετητή (server). Τα δύο αυτά προγράμματα συνομιλούν μεταξύ τους ανταλλάσοντας HTTP μηνύματα. Το HTTP ορίζει την δομή που θα έχουν αυτά τα μηνύματα.
Οι περιηγητές (browsers) που «τρέχουν» σε έναν σταθμό εργασίας αναλαμβάνουν την δουλειά του HTTP πελάτη και την δουλειά του HTTP εξυπηρετητή αναλαμβάνει κάποιος απομακρυσμένος server στον οποίο ζητά πρόσβαση ο HTTP πελάτης. Συνήθως οι HTTP πελάτες που τρέχουν περιηγητές (browsers) είναι απλοί υπολογιστές οι οποίοι είτε βρίσκονται σε κάποια κατοικία είτε σε κάποιον οργανισμό (π.χ. εταιρίες, πανεπιστήμια, ιδρύματα έρευνας όπως το ΙΤΕ κλπ).
Οι δε HTTP εξυπηρετητές όπως προαναφέραμε είναι απομακρυσμένοι servers οι οποίοι μπορεί να βρίσκονται σε κέντρα πληροφοριών (data centers) όπου φιλοξενούν αντικείμενα τα οποία μπορεί να ζητήσει ένας HTTP πελάτης.
Για παράδειγμα όταν ένας χρήστης ζητάει μια ιστοσελίδα πληκτρολογεί το αντίστοιχο σύνδεσμο (URL). Ο browser στέλνει ένα μήνυμα HTTP αίτησης για το αντικείμενο που έχει ο εξυπηρετητής. Ο εξυπηρετητής λαμβάνει αυτήν την αίτηση και απαντά με HTTP μηνύματα απόκρισης τα οποία περιέχουν τα αντικείμενα.
Το HTTP χρησιμοποιεί το πρωτόκολλο TCP και την θύρα επικοινωνίας 80. Υπάρχει επίσης και το HTTPS το οποίο προσφέρει ασφαλής επικοινωνία μεταξύ client και server χρησιμοποιώντας την θύρα 443.



Εικόνα 2.18. Παράδειγμα αίτησης και απόκρισης HTTP μηνυμάτων

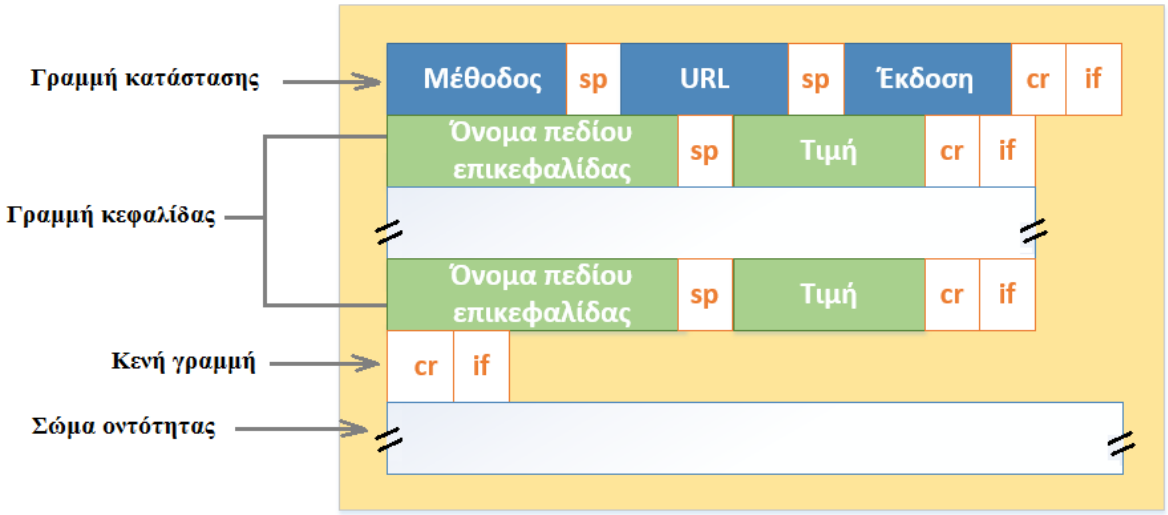
Στο παράδειγμα της εικόνας 2.18 έχουμε δύο HTTP πελάτες και ένα HTTP εξυπηρετητή. Το πρωτόκολλο μεταφοράς που χρησιμοποιείται είναι το TCP διότι όπως αναφέραμε παραπάνω το HTTP υποστηρίζει το TCP ως πρωτόκολλο μεταφοράς δεδομένων. Θα αναφερθούμε στο επίπεδο μεταφοράς γι αυτό, προς το παρών ας κρατήσουμε ότι το HTTP χρησιμοποιεί TCP επικοινωνία και ότι αυτό προσφέρει αξιόπιστη μεταφορά δεδομένων. Ο πελάτης HTTP λοιπόν ξεκινάει πρώτος την σύνδεση με τον HTTP εξυπηρετητή. Όταν πραγματοποιηθεί η σύνδεση οι διεργασίες του browser και του εξυπηρετητή προσπελαύνουν το TCP μέσω των διεπαφών socket τους. Ο πελάτης στέλνει μήνυμα αιτήσεων HTTP στην διεπαφή socket και λαμβάνει μηνύματα απόκρισης HTTP από την διεπαφή socket. Με τον ίδιο τρόπο ο HTTP εξυπηρετητής λαμβάνει μηνύματα αιτήσεως από την διεπαφή του socket του και στέλνει απαντητικά μηνύματα στην ίδια διεπαφή του.

Σημαντική παρατήρηση

Μια σημαντική παρατήρηση είναι ότι το πρωτόκολλο HTTP είναι ακαταστασιακό πρωτόκολλο (stateless protocol). Ο λόγος αυτός οφείλετε διότι ένας HTTP εξυπηρετητής (server) δεν κρατά πληροφορίες για τους πελάτες του. Εξού κι ο λόγος για τον οποίον το HTTP είναι stateless.

Υπάρχουν δύο τύποι HTTP συνδέσεων:

- HTTP με μη παραμένουσες συνδέσεις (Non persistent HTTP): Όπου ένα και μόνο αντικείμενο μπορεί να σταλεί μόνο μέσω μιας σύνδεσης. Παράδειγμα το HTTP/1.0
- HTTP με παραμένουσες συνδέσεις (persistent HTTP): Πολλά αντικείμενα μπορούν να σταλούν μέσω μιας TCP σύνδεσης. Παράδειγμα το HTTP/1.1



Εικόνα 2.19. Δομή ενός HTTP μηνύματος αίτησης

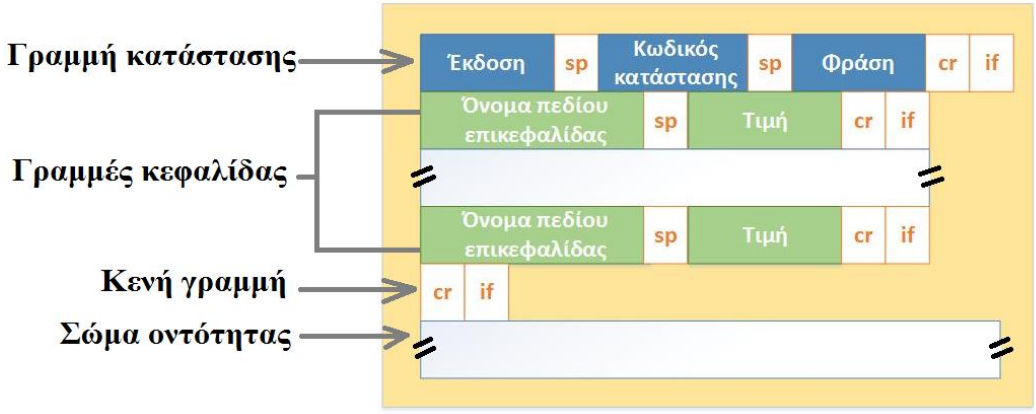
Ας αναλύσουμε λίγο την δομή ενός HTTP μηνύματος αίτησης. Η πρώτη γραμμή που καλείται γραμμή κατάστασης (status line) περιέχει τρία πεδία, το πεδίο μεθόδου, το πεδίο URL και το πεδίο έκδοσης HTTP. Το πεδίο μέθοδος μπορεί να έχει διαφορετικές τιμές οι οποίες μπορεί να είναι GET, POST, HEAD, PUT, DELETE κλπ. Η μέθοδος GET χρησιμοποιείται όταν ζητάμε ένα αντικείμενο ή μια πληροφορία από το URL. Στον πίνακα 1.1 ακολουθεί η κάθε τιμή που μπορεί να πάρει το πεδίο μεθόδου.

Α/Α	Τιμές	Περιγραφή
1	GET	Η τιμή GET χρησιμοποιείται όταν θέλουμε να ανακτήσουμε μια πληροφορία που περιέχεται στο πεδίο URL (που είναι ένας server). Οι αιτήσεις που έχουν την τιμή GET μπορούν μόνο να ανακτήσουν δεδομένα.
2	HEAD	Λειτουργεί με τον ίδιο τρόπο όπως η GET, με την διαφορά ότι μεταφέρει μόνο την γραμμή κατάστασης status line και την γραμμή επικεφαλίδας (header section) στο πακέτο HTTP.
3	POST	Η τιμή POST χρησιμοποιείται σε HTTP μηνύματα αίτησης για να στείλουμε πληροφορία στον server, για παράδειγμα, τις πληροφορίες που θέλει να στείλει ένας πελάτης, ανέβασμα αρχείων, κλπ μέσω μιας φόρμας HTML.
4	PUT	Αντικαθιστά όλες τις τρέχουσες αναπαραστάσεις των πόρων προορισμού με το ανεβασμένο περιεχόμενο (uploaded content)
5	DELETE	Διαγράφει όλες τις τρέχουσες αναπαραστάσεις των πόρων προορισμού που έχουν δοθεί από ένα URL.
6	CONNECT	Εγκαθιδρύει ένα επικοινωνιακό κανάλι με τον εξυπηρετητή (server) το οποίο ταχτοποιείται από το δοθέν URL.
7	OPTIONS	Περιγράφει όλες τις ιδιότητες επικοινωνίας για τους πόρους προορισμού
8	TRACE	Εκτελεί μια διαδικασία από τεστ βρόγχων επαναληπτικών μηνυμάτων (message loop-back test) σε όλη τη σύνδεση ως τους πόρους προορισμού.

Πίνακας 2.1. Πίνακας με τιμές που μπορεί να πάρει το πεδίο μέθοδος

Η γραμμή κεφαλίδας (header section) καθορίζει τον υπολογιστή στον οποίο βρίσκεται το αντικείμενο που ζητάμε. Το σώμα οντότητας είναι κενό με την τιμή GET αλλά χρησιμοποιείται όταν αποδίδεται στο πεδίο μεθόδου η τιμή POST.
Προηγουμένως αναλύσαμε την δομή απ' την οποία αποτελείται ένα HTTP μήνυμα αίτησης τι γίνετε όμως αν ο Server επιθυμεί να δώσει μια απάντηση στον HTTP client ; Θα υπάρξουν διαφορές ως προς την δομή του πακέτου ;

Ας δούμε σε αυτό το σημείο την μορφή ενός HTTP μηνύματος απάντησης. Έχει τρία σημεία τα οποία είναι μια γραμμή κατάστασης (status line), έξι γραμμές επικεφαλίδας και μετά το σώμα οντότητας. Το σώμα οντότητας αφορά το περιεχόμενο του μηνύματος. Η γραμμή κατάστασης περιέχει τρία πεδία, το πεδίο έκδοσης πρωτοκόλλου έναν κωδικό κατάστασης και ένα αντίστοιχο μήνυμα κατάστασης. Η εικόνα 2.20 δίνει μια σαφή απάντηση για την δομή ενός απαντητικού μηνύματος HTTP.



Εικόνα 2.20. Δομή ενός HTTP μηνύματος απάντησης

Το πεδίο κωδικός κατάστασης μπορεί να έχει διαφορετικές τιμές οι οποίες μπορεί να είναι 200, 301, 400, 404, 505 κλπ. Κάθε ένας απ' αυτούς τους κωδικούς ορίζει την απάντηση που θα δώσει στον client. Για παράδειγμα έστω ότι ένας HTTP πελάτης (client) στέλνει μια αίτηση στον HTTP εξυπηρετητή (server). Όταν λάβει ο HTTP εξυπηρετητής το αίτημα απ' τον HTTP πελάτη (client) θα ελέγξει με την σειρά του αν όλα είναι εντάξει και αφού το επιβεβαιώσει θα στείλει πίσω στον HTTP πελάτη ένα HTTP απαντητικό μήνυμα με κωδικό 200 που σημαίνει OK.

2.5.6 HyperText Transfer Protocol Secure – HTTPS

Το HTTPS δεν αποτελεί ένα ξεχωριστό πρωτόκολλο αλλά έναν συνδυασμό του πρωτοκόλλου HTTP και των δυνατοτήτων κρυπτογράφησης που παρέχει το πρωτόκολλο Secure Sockets Layer (SSL).
Η κρυπτογράφηση που χρησιμοποιείται εξασφαλίζει ότι τα κρυπτογραφημένα δεδομένα δεν θα υποκλαπούν από άλλους κακόβουλους χρήστες. Για να χρησιμοποιηθεί το HTTPS σε κάποιο server θα πρέπει ο διαχειριστής του να δημιουργήσει ένα ζεύγος κλειδιών (δημόσιο/ιδιωτικόο). Στην συνέχεια το δημόσιο κλειδί θα πρέπει να υπογραφεί από μία αρχή πιστοποίησης (certificate authority), η οποία εκδίδει ένα ψηφιακό πιστοποιητικό και η οποία πιστοποιεί ότι ο server που εμφανίζεται στο πιστοποιητικό είναι νόμιμος και ότι το πιστοποιητικό είναι έγκυρο. Με τον τρόπο αυτό οι χρήστες μπορούν να δουν την υπογραφή της αρχής πιστοποίησης και να βεβαιωθούν ότι το πιστοποιητικό είναι έγκυρο και ότι κανένας κακόβουλος χρήστης δεν το έχει πλαστογραφήσει. Το HTTPS χρησιμοποιείται κυρίως όταν απαιτείται μεταφορά ευαίσθητων προσωπικών δεδομένων (π.χ. υπηρεσίες cloud service όπως το Mega.co.nz). Το επίπεδο προστασίας δεδομένων εξαρτάται από το αν έχει εφαρμοστεί σωστά η διαδικασία ασφάλειας και από το πόσο ισχυροί είναι οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται. Πολλοί χρήστες πιστωτικών καρτών θεωρούν ότι το HTTPS προστατεύει ολοκληρωτικά τα στοιχεία της πιστωτικής τους κάρτας από κατάχρηση. Το HTTPS χρησιμοποιεί την κρυπτογράφηση για να μεταδώσει τον αριθμό από τον υπολογιστή του πελάτη προς τον server. Η μετάδοση είναι ασφαλής και τα δεδομένα φτάνουν στον server χωρίς κανείς να μπορέσει να τα υποκλέψει.

2.5.7 File Transfer Protocol – FTP

Το πρωτόκολλο μεταφοράς αρχείων (File Transfer Protocol – FTP) ορίζει τους κανόνες για την μεταφορά αρχείων. Για παράδειγμα σε μια τυπική σύνοδο FTP ο χρήστης έχει έναν τοπικό υπολογιστή που θέλει να μεταφέρει αρχεία προς έναν απομακρυσμένο εξυπηρετητή (server). Για να μπορέσει ο χρήστης να αποκτήσει πρόσβαση σε έναν απομακρυσμένο λογαριασμό, πρέπει να δώσει όνομα χρήστη (username) και ένα συνθηματικό (password). Αφού ο χρήστης δώσει αυτές τις πληροφορίες εξουσιοδότησης, μπορεί να μεταφέρει αρχεία απ' το τοπικό του σύστημα αρχείων (δηλαδή τον τοπικό υπολογιστή του) προς το απομακρυσμένο σύστημα αρχείων (δηλαδή έναν server) και το ανάστροφο. Το πρωτόκολλο HTTP που αναφέραμε προηγουμένως έχει πολλά κοινά χαρακτηριστικά. Ένα από αυτά τα κοινά χαρακτηριστικά είναι ότι και το FTP εκτελείται πάνω στο πρωτόκολλο μεταφοράς TCP. Το FTP χρησιμοποιεί τις TCP θύρες επικοινωνίας 20 για σύνδεση δεδομένων και την 21 για σύνδεση ελέγχου. Η εικόνα 2.21 δίνει ένα πιο σαφές παράδειγμα των TCP θυρών επικοινωνίας που χρησιμοποιεί το FTP.

Εικόνα 2.21. Συνδέσεις ελέγχου και δεδομένων FTP

Όπως παρατηρούμε από την εικόνα 2.21 η μεγάλη διαφορά ανάμεσα σε HTTP και FTP είναι ότι το δεύτερο χρησιμοποιεί δύο παράλληλες συνδέσεις TCP για μεταφορά ενός αρχείου. Η μια είναι για σύνδεση ελέγχου (control connection) και η άλλη για σύνδεση δεδομένων (data connection). Η σύνδεση ελέγχου χρησιμοποιείται για αποστολή πληροφοριών ελέγχου ανάμεσα σε δύο υπολογιστές όπως το όνομα χρήστη, κωδικοί πρόσβασης, εντολές για αλλαγή ενός απομακρυσμένου καταλόγου και εντολές για αποστολή και λήψη αρχείων. Η σύνδεση δεδομένων χρησιμοποιείται για να κάνει την πραγματική αποστολή ενός αρχείου. Επειδή λοιπόν το FTP χρησιμοποιεί μια ξεχωριστή σύνδεση ελέγχου, χαρακτηρίζεται ως εξωζωνικό (out-of-bound) πρωτόκολλο ενώ το HTTP χαρακτηρίζεται ως ενδοζωνικό (in-band) πρωτόκολλο.

Έχουμε δύο ειδών FTP ιστοσελίδων (sites) τα οποία είναι τα εξής:

- **Επώνυμες FTP ιστοσελίδες**: Όπου δίνουν πρόσβαση σε γνωστούς χρήστες που διαθέτουν λογαριασμό (user accounts). Για να επιτρέψουν την πρόσβαση στον χρήστη ζητάνε από τον ίδιο να δώσει το όνομα λογαριασμού του (username) και τον κωδικό του (password).

- **Ανώνυμες FTP ιστοσελίδες**: Όπου επιτρέπουν την λεγόμενη «ανώνυμη» πρόσβαση (anonymous login).

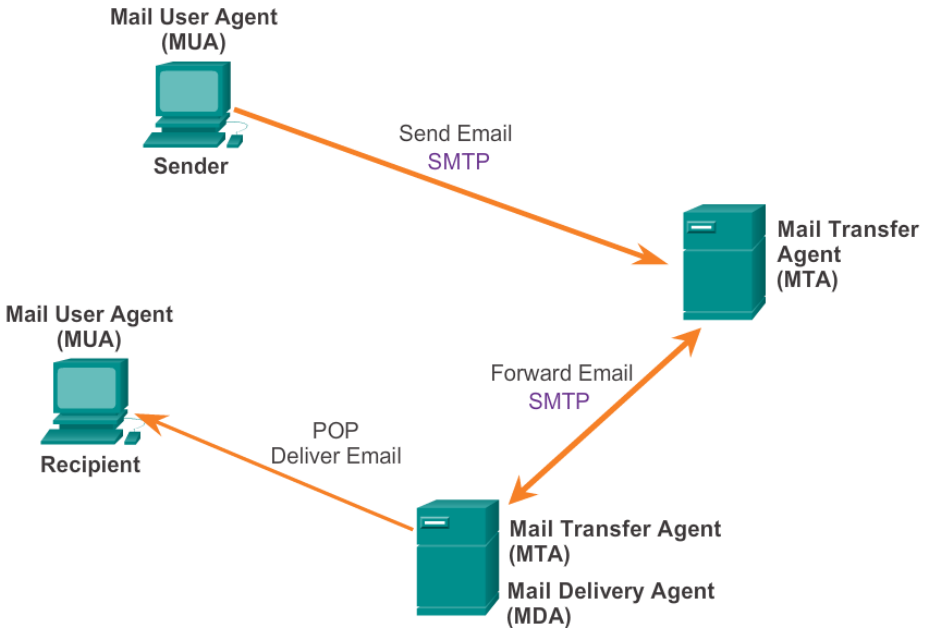
Σημαντική παρατήρηση

Μια σημαντική παρατήρηση είναι ότι ένας εξυπηρετητής (server) FTP κατά την διάρκεια μιας συνόδου πρέπει να διατηρεί την κατάσταση (state) για τον χρήστη. Δηλαδή ο εξυπηρετητής πρέπει να σχετίσει την σύνδεση ελέγχου με έναν συγκεκριμένο λογαριασμό χρήστη και παράλληλα να παρακολουθεί τον τρέχοντα κατάλογο του χρήστη.

2.5.8 Simple Mail Transfer Protocol – SMTP

Το ηλεκτρονικό ταχυδρομείο (e-mail) είναι μια από τις πιο διαδομένες σε χρήση εφαρμογές του διαδικτύου όπου επιτρέπει σε χρήστες να στέλνουν μηνύματα μέσα από το διαδίκτυο (internet). Προς το παρών, το πρωτόκολλο επικοινωνίας που χρησιμοποιεί το ηλεκτρονικό ταχυδρομείο (e-mail) για την αποστολή και την λήψη των μηνυμάτων είναι το πρωτόκολλο μεταφοράς απλού ταχυδρομείου (Simple Mail Transfer Protocol - SMTP). Το πρωτόκολλο SMTP στηρίζεται κι αυτό στο μοντέλο πελάτη - εξυπηρετητή (client – server) χρησιμοποιώντας επίσης για μεταφορά δεδομένων το TCP. Χρησιμοποιεί τρείς θύρες επικοινωνίας ανάλογα με τον τύπο SMTP επικοινωνίας που θέλουμε. Αυτές οι θύρες είναι οι εξής:

- TCP Θύρα 25 – Χρησιμοποιείται για απλή μη κρυπτογραφημένη SMTP επικοινωνία.
- TCP θύρα 2525 – Χρησιμοποιείται σε περίπτωση που η θύρα επικοινωνίας 25 είναι για κάποιο λόγω δεσμευμένη (π.χ. από τον ISP).
- TCP θύρα 465 – Χρησιμοποιείται για ανταλλαγή ασφαλών SMTP κρυπτογραφημένων μηνυμάτων



Εικόνα 2.22. Παράδειγμα λειτουργίας του MTA και του MUA σε μία αποστολή email

Η ανταλλαγή των ηλεκτρονικών μηνυμάτων πραγματοποιείται από έναν μηχανισμό που ονομάζεται πράκτορας μεταφοράς μηνυμάτων (Message Transfer Agent - MTA). Αντίστοιχα οι τερματικοί χρήστες (end users) ονομάζονται Mail User Agent (MUA). Ο μηχανισμός MTA ορίζεται από τους διαχειριστές του συστήματος. Η επικοινωνία ανάμεσα σε έναν SMTP πελάτη (SMTP client) και έναν SMTP εξυπηρετητή (SMTP server) πραγματοποιείται μέσω απλού κειμένου ASCII. Το SMTP βασίζεται στην απ' άκρο σε άκρο επικοινωνία. Για παράδειγμα ένας SMTP πελάτης επικοινωνεί με τον SMTP εξυπηρετητή προορισμού μέσω της TCP θύρας 25 για να παραδώσει το ηλεκτρονικό μήνυμα (e-mail). Σε αυτό το σημείο ο SMTP πελάτης αναμένει να λάβει από τον SMTP εξυπηρετητή ένα μήνυμα με κωδικό 220 "READY FOR MAIL" που σημαίνει ότι είναι έτοιμος για ανταλλαγή μηνυμάτων. Όταν λάβει αυτό το μήνυμα ο SMTP πελάτης θα στείλει με την σειρά του την εντολή HELLO. Ο SMTP εξυπηρετητής ανταποκρίνεται στον SMTP πελάτη με ένα μήνυμα που έχει τον κωδικό 250 "Requested mail action okay" για να επιβεβαιώσει ότι είναι έτοιμος για συναλλαγή ηλεκτρονικού μηνύματος.

Μετά από αυτό θα ξεκινήσει μια συναλλαγή μηνυμάτων που θα περιέχει την εντολή MAIL που δίνει τις πληροφορίες του αποστολέα όπως και το πεδίο FROM που περιέχει την ηλεκτρονική διεύθυνση ώστε να εντοπιστούν τυχόν σφάλματα.
Αφού εκτελεστεί επιτυχώς η εντολή MAIL ο αποστολέας θα εκδώσει μια σειρά από εντολές RCPT για να εντοπίσει τους παραλήπτες του ηλεκτρονικού μηνύματος. Ο παραλήπτης θα στείλει μια επιβεβαίωση για κάθε εντολή RCPT στέλνοντας ένα μήνυμα με κωδικό "250 OK" σε διαφορετική περίπτωση θα στείλει ένα μήνυμα σφάλματος (error message) με κωδικό "550 No such user here"

Αφού επιβεβαιωθούν όλες οι εντολές RCPT, ο αποστολέας θα εκδώσει την εντολή DATA για να ενημερώσει τον παραλήπτη ότι είναι έτοιμος για να στείλει ένα ολοκληρωμένο ηλεκτρονικό μήνυμα (mail message). Ο παραλήπτης ανταποκρίνεται με ένα μήνυμα που έχει τον κωδικό "354 Start mail input" με μια τελική ακολουθία που θα πρέπει να χρησιμοποιήσει ο αποστολέας, προκειμένου να τερματίσει τα δεδομένα που θα περιέχει το μήνυμα. Η τερματική αυτή ακολουθία αποτελείται από 5 χαρακτήρες <CRLF>.<CRLF>
Ο SMTP πελάτης στέλνει γραμμή προς γραμμή τα δεδομένα με τους 5 αυτούς χαρακτήρες στο τέλος της κάθε σειράς στην οποία ο παραλήπτης είτε θα στείλει ένα επιβεβαιωτικό μήνυμα με κωδικό "250 OK" είτε με ένα μήνυμα σφάλματος αν κάτι πήγε στραβά. Μετά απ' όλη αυτή την συνδιαλλαγή μηνυμάτων, ο πελάτης μπορεί να εκτελέσει τις παρακάτω ενέργειες.

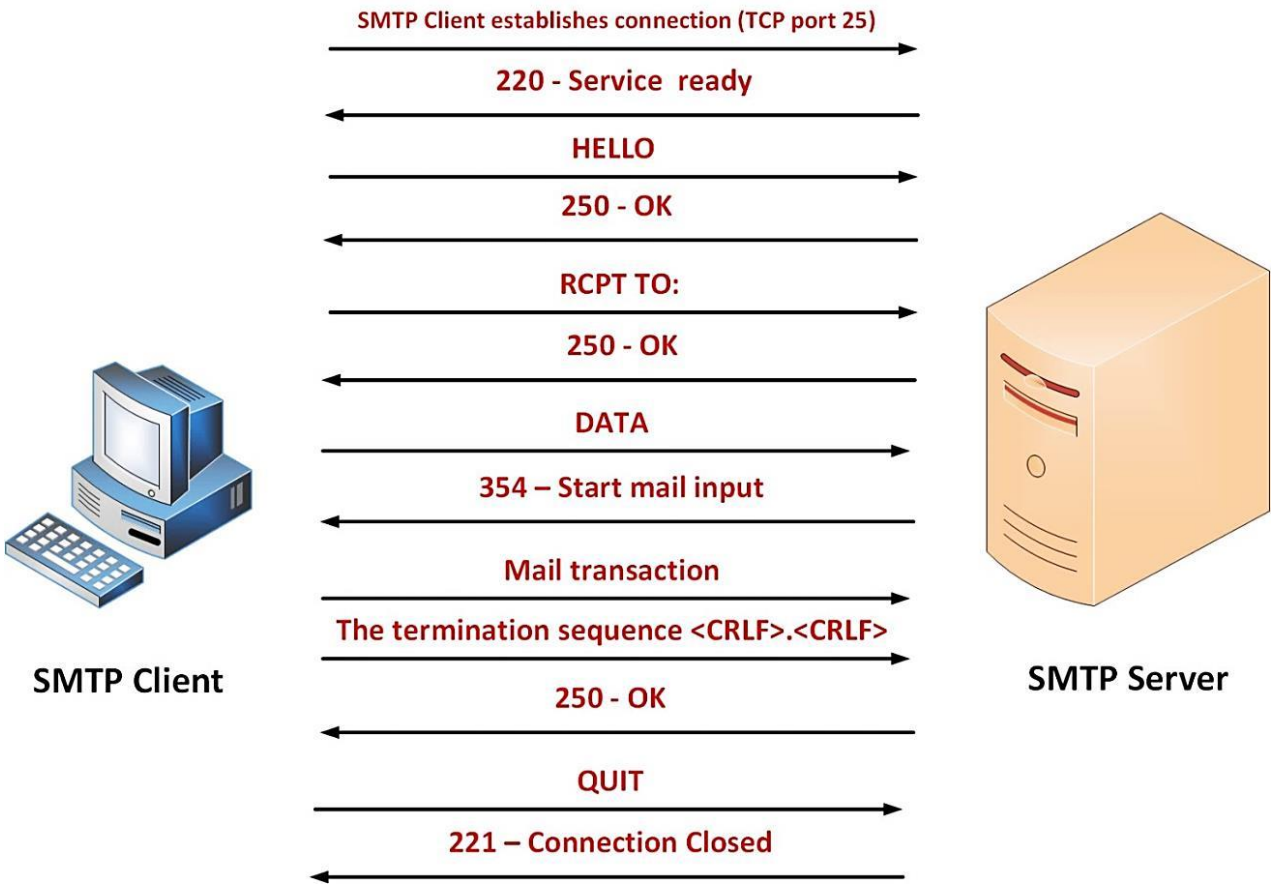
- Τερματισμός συνόδου (Terminate Session): Αν ο SMTP πελάτης για κάποιο λόγο δεν έχει να στείλει άλλα μηνύματα η σύνδεση μπορεί να τερματιστεί με την εντολή QUIT με την οποία θα λάβει απάντηση μηνύματος από τον SMTP εξυπηρετητή με κωδικό "221 Service closing transmission channel reply".

- Ανταλλαγή ρόλων (Exchange Roles): Αν ο SMTP πελάτης δεν έχει άλλα μηνύματα για να στείλει αλλά είναι σε θέση να δεκτή οποιοδήποτε μήνυμα από τον SMTP εξυπηρετητή τότε εκδίδει την εντολή TURN. Με αυτήν την εντολή ο SMTP πελάτης και ο SMTP εξυπηρετητής θα μπορούν να ανταλλάξουν ρόλους.

- Αποστολή επιπλέων μηνύματος (Send Another Mail): Αν ο SMTP πελάτης έχει να στείλει κι άλλα μηνύματα τότε μπορεί να εκδώσει μια νέα εντολή MAIL.

```
Server:   220 somewhere.com Simple Mail Transfer Service Ready

Client:   HELO example.edu
Server::  250 OK

Client:   MAIL FROM:<John_Q_Smith@example.edu>
Server:   250 OK

Client:   RCPT TO:<Mathew_Doe@somewhere.com>
Server:   550 No such user here

Client:   RCPT TO:<Paul_Jones@somewhere.com>
Server:   250 OK

Client:   DATA
Server:   354 Start mail input; end with <CR><LF>.<CR><LF>
Client:   ...sends body of mail message, which can contain
Client:   ...arbitrarily many lines of text
Client:   <CR><LF>.<CR><LF>
Server:   250 OK

Client:   QUIT
Server:   221 somewhere.com closing transmission channel
```

Εικόνα 2.23. Παράδειγμα επικοινωνίας SMTP μεταξύ ενός client κι ενός server



Εικόνα 2.24. Δομή επικοινωνίας SMTP client – server

Κώδικες Κατάστασης	Περιγραφή
211	Help reply - system status
214	Help message
220	Service ready
221	Closing connection
250	Requested action okay
251	User not local; will forward to <forward-path>
354	Start mail input
421	Service not available
450	Action not taken - mailbox busy
451	Action aborted - local error
452	Action not taken - insufficient storage
500	Command unrecognized or syntax error
501	Syntax error in parameters or arguments
502	Command not supported
503	Bad sequence of commands (given out of order)
504	Command parameter not supported
550	Action not taken - mailbox unavailable
551	Not a local user
552	Aborted: Exceeded storage allocation
553	Action not taken - mailbox name not allowed
554	Transaction failed

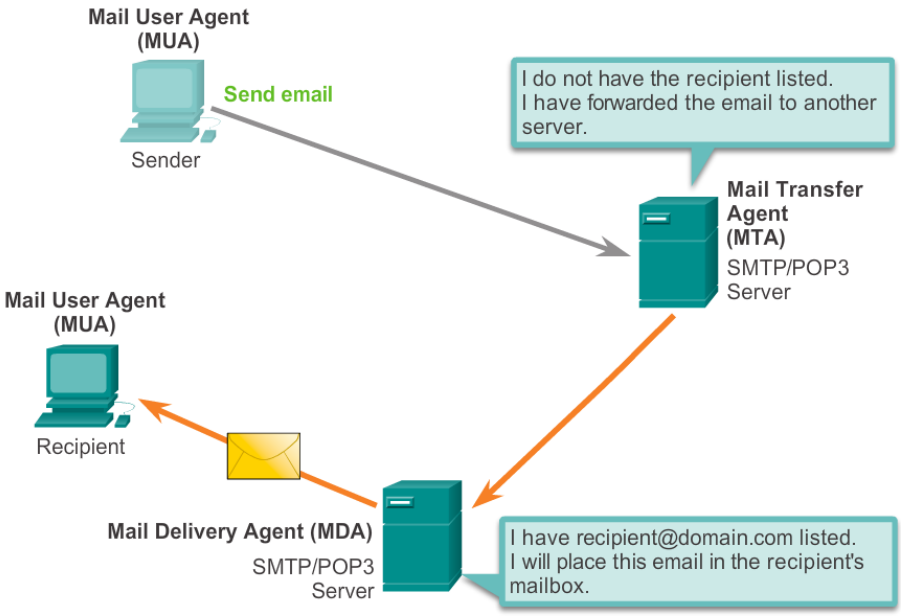
Πίνακας 2.2. Πιθανοί κώδικες κατάστασης (ή εντολές) ανάμεσα σε έναν SMTP εξυπηρετητή και έναν SMTP πελάτη

2.5.9 Post Ofice Protocol version 3 – POP3

Είναι ένα πρωτόκολλο ηλεκτρονικού ταχυδρομείου που χρησιμοποιείται από έναν πελάτη ηλεκτρονικού ταχυδρομείου (e-mail client) για την λήψη ηλεκτρονικών μηνυμάτων (e-mails) που βρίσκονται σε απομακρυσμένους εξυπηρετητές (servers). Το POP3 επιτρέπει την λήψη ηλεκτρονικών μηνυμάτων σε έναν τοπικό υπολογιστή επιτρέποντας παράλληλα και την ανάγνωση τους ακόμα κι αν δεν υπάρχει σύνδεση με το διαδίκτυο. Όταν ένας τοπικός υπολογιστής που χρησιμοποιεί το POP3 λάβει όλα τα ηλεκτρονικά μηνύματα θα διαγραφθούν από τους εξυπηρετητές (servers). Αυτό βέβαια δεν αποτελεί την καλύτερη λύση αν θέλουμε να βλέπουμε τα μηνύματα μας από διαφορετικές τοποθεσίες.

- Οι προκαθορισμένες θύρες επικοινωνίας που χρησιμοποιεί το POP3 είναι οι εξής:
- TCP θύρα 110 - χρησιμοποιείται όταν θέλουμε να χρησιμοποιήσουμε απλή επικοινωνία
- TCP θύρα 995 - χρησιμοποιείται όταν θέλουμε να χρησιμοποιήσουμε ασφαλή κρυπτογραφημένη επικοινωνία

Η διαδικασία λήψης των μηνυμάτων γίνεται από τον εξυπηρετητή που αναλαμβάνει τον ρόλο του Mail Delivery Agent (MDA) προς τον πελάτη που με την σειρά του αναλαμβάνει τον ρόλο του Mail User Agent (MUA).



Εικόνα 2.25. Παράδειγμα λειτουργίας του MDA και του MUA σε μία λήψη email

Ο εξυπηρετητής εκκινεί την υπηρεσία POP χρησιμοποιώντας την θύρα επικοινωνίας TCP 110 για τις αιτήσεις σύνδεσης του πελάτη. Όταν ένας POP πελάτης θέλει να κάνει χρήση της υπηρεσίας POP, στέλνει ένα αίτημα δημιουργίας TCP σύνδεσης με τον POP εξυπηρετητή. Όταν η σύνδεση αυτή πραγματοποιηθεί, ο εξυπηρετητή POP στέλνει ένα μήνυμα «hello». Ο πελάτης POP ανταλλάσει εντολές με τον εξυπηρετητή POP και λαμβάνει απαντήσεις από τον δεύτερο μέχρι τον τερματισμό της σύνδεσης ή τυχόν ακύρωσής της.

Επειδή τα ηλεκτρονικά μηνύματα (e-mails) αφαιρούνται από τον POP εξυπηρετητή όταν αυτά ληφθούν στο τοπικό υπολογιστή του POP πελάτη, δεν υπάρχει μια κεντρική τοποθεσία πέραν αυτού του τοπικού υπολογιστή γι αυτά τα ηλεκτρονικά μηνύματα. Για τον παραπάνω λόγο το POP δεν αποτελεί μια αποτελεσματική λύση για μια μικρή επιχείρηση που χρειάζεται έναν κεντρικό τόπο αποθήκευσης μηνυμάτων για λόγους εφεδρείας - ασφάλειας. Αντιθέτως, το POP είναι κατάλληλο για έναν πάροχο υπηρεσιών διαδικτύου διότι μειώνει τον όγκο των μηνυμάτων που αποθηκεύονται στους εξυπηρετητές του ηλεκτρονικού ταχυδρομείου τους.

2.5.10 Internet Message Access Protocol - IMAP

Το πρωτόκολλο αυτό δίνει την δυνατότητα πρόσβασης ενός τοπικού υπολογιστή (local client) σε ηλεκτρονικά μηνύματα (e-mails) που βρίσκονται σε κάποιον απομακρυσμένο web server. Γενικά το IMAP αλλά και το POP3 που αναφέραμε προηγουμένως είναι τα πιο διαδεδομένα πρωτόκολλα ηλεκτρονικού ταχυδρομείου και χρησιμοποιούνται μόνο για την λήψη ηλεκτρονικών μηνυμάτων. Τα δύο αυτά πρωτόκολλα υποστηρίζονται από όλους τους email clients και e-mail servers.
Ενώ το POP3 υποθέτει ότι τα ηλεκτρονικά μηνύματα (e-mails) είναι προσβάσιμα μόνο από μια εφαρμογή, το IMAP επιτρέπει την ταυτόχρονη πρόσβαση σε πολλαπλούς πελάτες (clients). Γι' αυτόν τον λόγο αποτελεί το κατάλληλο πρωτόκολλο σε περίπτωση που επιθυμούμε πρόσβαση από διαφορετικές τοποθεσίες ή ακόμα κι αν τα μηνύματα διαχειρίζονται από πολλαπλούς χρήστες.

Οι προκαθορισμένες θύρες επικοινωνίας που χρησιμοποιεί το IMAP είναι οι εξής:

- TCP Θύρα 143 - Χρησιμοποιείται για απλή επικοινωνία
- TCP Θύρα 993 - Χρησιμοποιείται για ασφαλή επικοινωνία

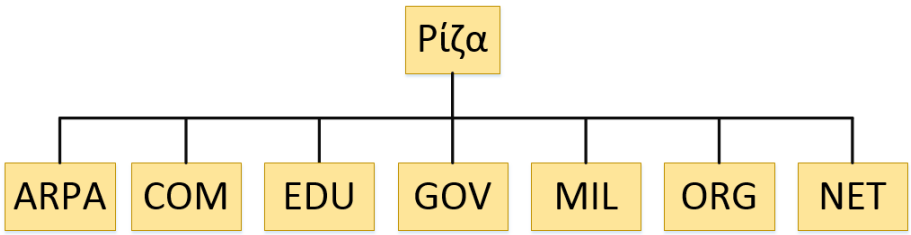
Σημαντική παρατήρηση

Ενώ το POP3 είναι ακαταστασιακό (stateless) από σύνοδο (session) σε σύνοδο, το IMAP διατηρεί την κατάσταση του χρήστη μεταξύ των συνόδων. Ο λόγος οφείλεται διότι το IMAP διατηρεί όλα τα μηνύματα στον εξυπηρετητή (server) και επιτρέπει στον χρήστη την οργάνωση των μηνυμάτων σε φακέλους.

2.5.11 Domain Name System – DNS

Επειδή οι IP διευθύνσεις είναι δύσκολο να αποτυπωθούν στο μυαλό μας υπήρχε η ανάγκη επίλυσης αυτού του προβλήματος. Φανταστείτε να θέλαμε να μπούμε σε μια συγκεκριμένη ιστοσελίδα και να πρέπει να θυμόμασταν μια IP διεύθυνση (π.χ. 140.15.89.8) θα ήταν κάτι πολύ κουραστικό καθότι υπάρχουν πολλές ιστοσελίδες στο διαδίκτυο όπου κάθε μια έχει την δική της IP διεύθυνση. Γι αυτούς τους λόγους αναπτύχθηκε το σύστημα ονοματοδοσίας περιοχών (Domain Name System - DNS) το οποίο αναλαμβάνει την διαδικασία αντιστοίχισης μιας IP διεύθυνσης σε ένα όνομα (domain) που είναι μοναδικό.
Το σύστημα ονομασίας περιοχών χρησιμοποιεί ιεραρχική αρχιτεκτονική. Δηλαδή οργανώνει τα ονόματα σε ιεραρχίες παρόμοιες με τις δομές καταλόγων σε ένα σύστημα αρχείων υπολογιστών. Τα ονόματα περιοχών συνήθως περιγράφουν οργανωτικές ή γεωγραφικές οντότητες. Δηλώνουν την χώρα που είναι συνδεδεμένο το δίκτυο, σε τι είδους οργανισμό ανήκει και σε μερικές περιπτώσεις τα ονόματα ορίζονται με ακόμη μεγαλύτερη λεπτομέρεια. Ένα όνομα περιοχής αποτελείται από λέξεις που χωρίζονται μεταξύ τους με τελείες. Το πλήθος των λέξεων μπορεί να ποικίλει. Συνήθως συναντάμε ονόματα με τρείς έως και πέντε λέξεις. Το πρώτο επίπεδο περιοχών ονομάζονται βασικές περιοχές και βρίσκονται στα δεξιά του ονόματος. Στις Η.Π.Α. υπάρχουν επτά τέτοιες περιοχές, στις οποίες κατατάσσονται τα δίκτυα ανάλογα με τις δραστηριότητες τους. Αυτές είναι οι εξής:

.arp:	Ειδικοί οργανισμοί διαδικτύου
.edu:	Εκπαιδευτικά ιδρύματα
.com:	Εμπορικές επιχειρήσεις
.gov:	Κρατικοί οργανισμοί
.mil:	Στρατιωτικοί οργανισμοί
.net:	Οργανισμοί διαχείρισης δικτύων
.org:	Οργανισμοί που δεν εντάσσονται στις παραπάνω κατηγορίες

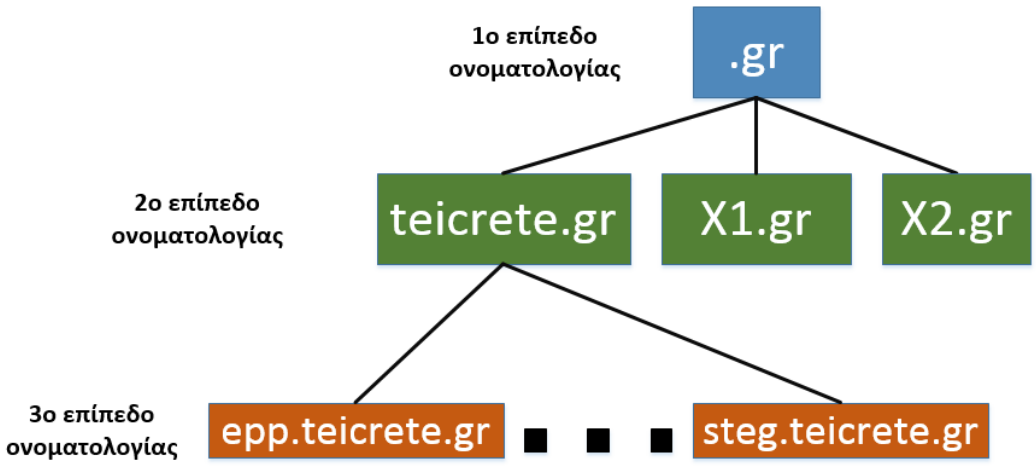


Εικόνα 2.26. Βασικές περιοχές ονομάτων DNS

Εκτός από τις παραπάνω βασικές περιοχές που αναφέρονται στις Η.Π.Α. υπάρχει επίσης μια βασική περιοχή για κάθε χώρα. Οι περιοχές αυτές συνήθως προσδιορίζονται από ένα μικρό τμήμα του ονόματος της χώρας στην οποία απευθύνεται. Παρακάτω ακολουθεί μια μικρή λίστα με χώρες και οι κωδικοί που αποδίδονται σε κάθε μία.

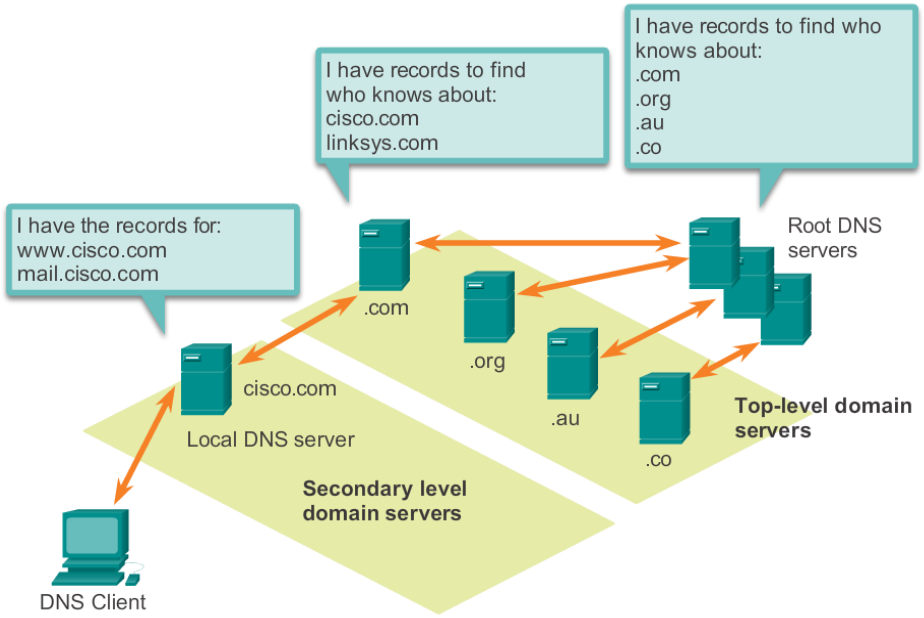
.us:	Ηνωμένες Πολιτείες Αμερικής
.ru:	Ρωσική Ομοσπονδία
.ca:	Καναδάς
.cn:	Λαϊκή Δημοκρατία της Κίνας
.uk:	Ηνωμένο Βασίλειο
.gr:	Ελλάδα
.rs:	Σερβία
.bg:	Βουλγαρία

Κάτω από κάθε βασική περιοχή υπάρχει ένα δεύτερο επίπεδο περιοχών που συνήθως προσδιορίζει τον οργανισμό στον οποίον ανήκει το δίκτυο. Οι περιοχές αυτές του δευτέρου επιπέδου ονομάζονται domains και κάθε μια είναι μοναδική. Συνήθως, τα ονόματα (domain names) που εκχωρούνται είναι αντιπροσωπευτικά και αντικατοπτρίζουν την εταιρία ή τον οργανισμό στον οποίον ανήκουν. Για παράδειγμα, το teicrete.gr ανήκει στην βασική περιοχή της Ελλάδας και το domain name teicrete αναφέρεται στην περιοχή που έχει παραχωρηθεί που είναι το ΤΕΙ Κρήτης.
Σε περίπτωση που ο εκάστοτε οργανισμός ή μια εταιρία που έχει παραχωρηθεί σε αυτήν ένα domain name διαχωρίσει το δίκτυο της σε μικρότερα υποδίκτυα θα επεκταθεί πάνω στην περιοχή ονομάτων του οργανισμού. Οπότε κάθε υποδίκτυο αντιστοιχείται σε μια περιοχή ονομάτων τρίτου επιπέδου που ονομάζεται subdomain. Για παράδειγμα το subdomain epp.teicrete.gr ανήκει στην βασική περιοχή της Ελλάδας στο domain name του teicrete.



Εικόνα 2.27. Ιεραρχική οργάνωση του χώρου ονομάτων DNS

Το δικαίωμα χρήσης ενός ονόματος DNS διαχειρίζεται από οργανισμούς μητρώου DNS. Για την Ελλάδα, ο οργανισμός αυτός είναι το Ινστιτούτο Τεχνολογίας και Έρευνας (ΙΤΕ) που εδρεύει στο Ηράκλειο, Κρήτης και είναι διαπιστευμένος ως οργανισμός μητρώου DNS από το ICANN (Internet Corporation for Assigned Names and Numbers). Το ICANN είναι μία μη κερδοσκοπική οργάνωση που είναι υπεύθυνη για το συντονισμό, της συντήρησης και της μεθοδολογίας των διαφόρων βάσεων δεδομένων (μεταξύ των οποίων και του DNS), που σχετίζονται με την καλή λειτουργία του διαδικτύου.



Εικόνα 2.28. Ιεραρχική οργάνωση της υπηρεσίας DNS στο Διαδίκτυο

Όπως αναφέραμε παραπάνω το πρωτόκολλο DNS χρησιμοποιεί ένα ιεραρχικό σύστημα για να δημιουργήσει μια βάση δεδομένων ώστε να παρέχεται η υπηρεσία DNS. Η ιεραρχία μοιάζει με ένα ανάποδο δένδρο με τη ρίζα στην κορυφή και τα κλαδιά κάτω (βλέπε Εικόνα 2.28). Το DNS χρησιμοποιεί τα ονόματα περιοχών για να σχηματίσουν την ιεραρχία. Οι διάφορες top-level domains αντιπροσωπεύουν είτε το είδος του οργανισμού ή τη χώρα προέλευσης. Το DNS βασίζεται σε αυτή την ιεραρχία των αποκεντρωμένων εξυπηρετητών για την αποθήκευση και τη διατήρηση των καταγραφών ονομάτων. Ο κατάλογος ονομάτων περιοχών περιέχει τα ονόματα που μπορεί να μεταφράσει ο συγκεκριμένος εξυπηρετητής καθώς και μία λίστα από εναλλακτικούς εξυπηρετητές που μπορούν να διεκπεραιώνουν αιτήματα DNS.

Ιστορικό σημείωμα

Ένα από τα πιο παράξενα στην ιστορία της ονοματοδοσίας περιοχών ανάμεσα σε χώρες αποτελεί το domain .su που ανήκε στην Σοβιετική Ένωση. Πριν δημιουργηθεί το domain .su υπήρχαν ελάχιστες ιστοσελίδες στην Σοβιετική Ένωση όπου οι περισσότερες ανήκαν σε πανεπιστημιακές κοινότητες. Από το 1989 και μετά μια ομάδα από νέα domains δημιουργήθηκαν στην Ευρώπη όπως το .pl (Πολωνία) .cs (Τσεχοσλοβακία) .yu (Γιουγκοσλάβια) και .dd (Ανατολική Γερμανία). Ανάμεσα όμως σε αυτά υπήρχε και το domain της Σοβιετικής Ένωσης το οποίο ήταν το .su και δημιουργήθηκε από τον τότε 19 χρόνο Φιλανδό φοιτητή Petri Ojala.

Όμως στις 26 Δεκεμβρίου του 1991 η χώρα διασπάστηκε με τις διάφορες λαϊκές δημοκρατίες να ζητούν επίσημα την ανεξαρτησία τους. Αυτό θα σήμαινε λογικά και την κατάργηση του domain .su όπως έγινε και με τα υπόλοιπα άλλα domains των πρώην Σοβιετικών δημοκρατιών όπως για παράδειγμα της ανατολικής Γερμανίας ή της Τσεχοσλοβακίας. Στην Ρωσία μέχρι και το 1993 δεν υπήρχε άλλο domain πέραν του .su που ήταν ακόμη σε χρήση και δεν είχε καταργηθεί. Όμως από το 1993 και μετά δημιουργήθηκε το domain .ru στην Ρωσία που υποτίθεται θα αντικαθιστούσε το παλιό .su domain.

Κανονικά θα έπρεπε να είχε αφαιρεθεί από τον οργανισμό ICANN παρόλα αυτά δεν πραγματοποιήθηκε κατόπιν αιτήματος της Ρωσικής ομοσπονδίας και των χρηστών του διαδικτύου. Το .su συνεχίζει να υπάρχει ακόμη και σήμερα και υπολογίζεται ότι 93,500 ιστοσελίδες έχουν καταχωρηθεί με αυτό το domain.

Οι ειδικοί στην ασφάλεια των δικτύων αναφέρουν ότι το domain .su αποτελεί τον διαδικτυακό παράδεισο των επίδοξων hackers που το χρησιμοποιούν για να στέλνουν spam μηνύματα και για υπεξαιρέσεις χρημάτων στο διαδίκτυο.
Ο Oren David που είναι ο διευθύνων της εταιρίας RSA anti-fraud unit, ανέφερε το εξής σε τηλεφωνική συνέντευξη που είχε. «Δεν νομίζω ότι το φαινόμενο αυτό αποτελεί στόχο για πολιτικές ιδεολογίες. Υπάρχουν και άλλα domains όπως το .tk το οποίο είναι καταχωρημένο για το νησί του Τόκελαου που βρίσκεται στην περιοχή του Νότιου Ειρηνικού και το οποίο με την σειρά του χρησιμοποιείται από επίδοξους hackers. Δηλαδή δεν είναι κάτι ιδεολογικό ή προσωπικό τα πάντα είναι για το όνομα του κέρδους. Όταν το 2011 οι όροι για το domain .ru έγιναν πιο αυστηροί οι περισσότεροι hackers άρχισαν να χρησιμοποιούν το παλιό domain .su»

2.5.12 Dynamic Host Configuration Protocol (DHCP)

Το πρωτόκολλο δυναμικής καταχώρησης IP διευθύνσεων επιτρέπει σε έναν πελάτη να αποκτήσει μια IP διεύθυνση αυτόματα και επίσης να μάθει επιπλέον πληροφορίες, όπως την IP διεύθυνση του δρομολογητή πρώτου άλματος (first hop router) καθώς και την διεύθυνση του DNS εξυπηρετητή του. Ένας DHCP πελάτης (DHCP client) βασίζεται όπως είναι λογικό στο μοντέλο επικοινωνίας TCP/IP που αναφέραμε προηγούμενος. Ένας λοιπόν DCHP πελάτης που βασίζεται στο μοντέλο TCP/IP δεν έχει ρυθμιστεί έτσι ώστε να διαθέτει την δική του IP διεύθυνση. Θα αναφερθούμε αργότερα τι είναι μια διεύθυνση IP προς το παρών ας συγκρατήσουμε ότι αυτή είναι η ταυτότητα του υπολογιστή στο διαδίκτυο (internet).

Όταν ένας DHCP πελάτης εκκινείτε (θέτεται δηλαδή σε λειτουργία) δεν είναι ικανός να στείλει ή να λάβει πληροφορία, διότι δεν έχει μια IP διεύθυνση για να επικοινωνήσει με άλλους υπολογιστές. Παρόλα αυτά μπορεί να συμμετέχει σε ανταλλαγή μηνυμάτων εκπομπής (broadcast). Ο DHCP πελάτης και ο DHCP εξυπηρετητής χρησιμοποιούν broadcast μηνύματα για να επικοινωνήσουν μεταξύ τους.

Τα broadcast μηνύματα είναι «ορατά» μόνο σε ένα τοπικό broadcast domain. Δηλαδή αυτά τα μηνύματα broadcast δεν πρόκειται ποτέ να φτάσουν σε ένα άλλο δίκτυο. Ο λόγος αυτός οφείλεται διότι οι δρομολογητές (routers) απορρίπτουν της περιορισμένες broadcast IP διευθύνσεις. Υπάρχουν δύο σημαντικές IP διευθύνσεις που χρησιμοποιούνται σε DHCP μηνύματα, αυτές είναι η 0.0.0.0 και η 255.255.255.255. Η 0.0.0.0 χρησιμοποιείται από μία συσκευή όταν δεν έχει χορηγηθεί σε αυτήν μια IP διεύθυνση. Όταν ένας DHCP πελάτης θέτεται σε λειτουργία δεν έχει μια έγκυρη IP διεύθυνση.

Η IP διεύθυνση 255.255.255.255 είναι γνωστή ως περιορισμένη broadcast IP διεύθυνση. Ένα αυτοδύναμο πακέτο IP (datagram) με την IP 255.255.255.255 θεωρείται σαν μήνυμα broadcast σε ένα τοπικό δίκτυο LAN. Τα μηνύματα DHCPDISCOVER και DHCPREQUEST στέλνονται από έναν DHCP πελάτη προς τον DHCP εξυπηρετητή. Τα δε μηνύματα DHCPOFFER και DHCPACK στέλνονται από τον DHCP εξυπηρετητή προς τον DHCP πελάτη.
Η διαδικασία σύμβασης ρυθμίσεως του TCP/IP από τον DHCP εξυπηρετητή περιλαμβάνει τα παρακάτω βήματα.

- DHCPDISCOVER: Ένας DHCP πελάτης στέλνει ένα μήνυμα εκπομπής (broadcast) τύπου DHCP discover στο δίκτυο που περιέχει την φυσική διεύθυνση MAC που προορίζεται στην UDP θύρα 68. Δηλαδή αυτό το αυτοδύναμο πακέτο (datagram) είναι στην ουσία μια αίτηση προς τον DHCP εξυπηρετητή ο οποίος με την σειρά του λαμβάνει αυτό το πακέτο για να λάβει πληροφορίες ως προς την ρύθμιση. Όπως λέει και το όνομα στην ουσία με αυτό το μήνυμα εντοπίζουμε τον DHCP εξυπηρετητή.

Εικόνα 2.29. Παράδειγμα αποστολής μηνύματος DHCPDISCOVER

Όπως βλέπουμε από την εικόνα 2.29 η φυσική διεύθυνση προορισμού MAC ενός DHCPDISCOVER μηνύματος είναι η FF-FF-FF-FF-FF-FF, η οποία είναι η broadcast MAC διεύθυνση. Ένα ethernet πλαίσιο (frame) με μια broadcast φυσική διεύθυνση MAC προορισμού κατευθύνεται προς όλες τις θύρες ενός τοπικού δικτύου (LAN). Το μήνυμα DHCPDISCOVER θα παραδοθεί σε κάθε συνδεμένο κόμβο του τοπικού δικτύου.

- DHCPOFFER: Σε περίπτωση που το μήνυμα DHCPDISCOVER μεταφερθεί επιτυχώς σε όλους τους διασυνδεδεμένους υπολογιστές του τοπικού δικτύου τότε ο κάθε DHCP εξυπηρετητής που θα λάβει αυτό το μήνυμα θα στείλει ένα απαντητικό μήνυμα τύπου DHCPOFFER πίσω στον DHCP πελάτη.

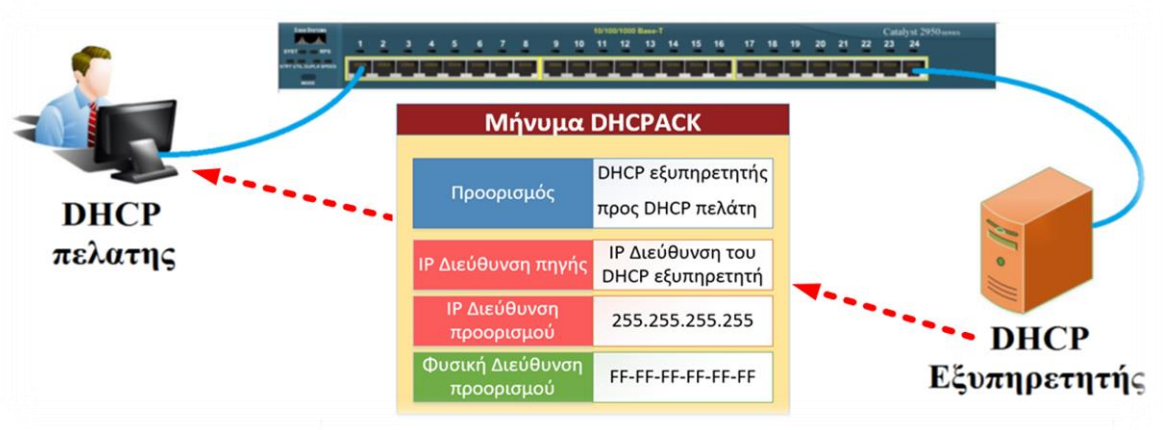
  Οι υπόλοιποι υπολογιστές που δεν είναι DHCP εξυπηρετητές θα παρακάμψουν αυτό το μήνυμα. Ένα μήνυμα DHCPOFFER περιέχει τα προσφερόμενα στοιχεία ρυθμίσεων TCP/IP όπως την IP διεύθυνση και την μάσκα υποδικτύου. Σε περίπτωση που για κάποιο λόγο ο DHCP πελάτης που έστειλε το μήνυμα DHCPDISCOVER λάβει παραπάνω από ένα μήνυμα DHCPOFFER τότε αποδέχεται το μήνυμα που θα φτάσει πρώτο. Οποιοδήποτε άλλο μήνυμα DHCPOFFER που θα έρθει αργότερα το απορρίπτει. Η εικόνα 2.30 δίνει ένα παράδειγμα DHCPOFFER.

Εικόνα 2.30. Παράδειγμα αποστολής μηνύματος DHCPOFFER

- DHCPREQUEST: Όταν ένας DCHP πελάτης αποδεχτεί το μήνυμα DHCPOFFER από τον DHCP εξυπηρετητή, θα πρέπει να στείλει με την σειρά του ένα αυτοδύναμο πακέτο broadcast το οποίο λέγεται DHCPREQUEST. Αυτό το πακέτο περιέχει την IP διεύθυνση του DHCP εξυπηρετητή που έστειλε το DHCPOFFER, και την φυσική διεύθυνση MAC του DHCP πελάτη (δηλαδή την φυσική διεύθυνση αυτού που στέλνει το DHCPREQUEST). Η εικόνα 2.31 δίνει ένα παράδειγμα DHCPREQUEST.

Εικόνα 2.31. Παράδειγμα αποστολής μηνύματος DHCPREQUEST

- DHCPACK: Όταν ο DHCP εξυπηρετητής απ' τον οποίο στάλθηκε το μήνυμα DHCPOFFER λάβει το αυτοδύναμο πακέτο DHCPREQUEST με την σειρά του δημιουργεί ένα αυτοδύναμο πακέτο DHCPACK (DHCP ACKNOWLEDGEMENT). Αυτό το πακέτο περιέχει την IP διεύθυνση και την μάσκα υποδικτύου για τον DHCP πελάτη. Μπορεί να περιέχει κι άλλες TCP/IP πληροφορίες ρυθμίσεων όπως προκαθορισμένη πύλη (default gateway), τις IP διευθύνσεις του DNS εξυπηρετητή κλπ. Όταν ο DHCP πελάτης λάβει το DHCPACK θα είναι σε θέση να χρησιμοποιήσει αυτήν την IP διεύθυνση. Η εικόνα 2.32 δίνει ένα παράδειγμα DHCPACK.



Εικόνα 2.32. Παράδειγμα αποστολής μηνύματος DHCPACK

Όπως είδαμε παραπάνω για να επικοινωνήσει ένας DHCP πελάτης και ένας DHCP εξυπηρετητής ανταλλάσουν μηνύματα. Σε αυτό το σημείο θα αναφερθούμε συνοπτικά στα πεδία αυτού μηνύματος. Όλα τα DHCP μηνύματα έχουν τον ίδιο ακριβώς σχεδιασμό. Το DHCP αναπτύχθηκε από το BOOTP (RFC 951) και όλα μηνύματα DHCP βασίζονται πάνω σε αυτό διότι το DHCP διαμοιράζετε με το BOOTP τις UDP θύρες 97 και 68. Το BOOTP και κατά συνέπεια το DHCP χρησιμοποιούν το UDP ως πρωτόκολλο μεταφοράς δεδομένων το οποίο δεν παρέχει αξιοπιστία. Οι DHCP πελάτες καλούνται να ξαναστείλουν τα μηνύματα τους αν δεν λάβουν απάντηση από τον DHCP εξυπηρετητή.
Για παράδειγμα αν ένας DHCP πελάτης στείλει ένα DHCPREQUEST μήνυμα και δεν απαντήσει σε αυτό ο DHCP εξυπηρετητής τότε ξαναστέλνει μηνύματα εκπομπής πάνω από τέσσερις φορές σε 2,4,8 και 16 δευτερόλεπτα. Αν παρόλα αυτά ο DHCP πελάτης εξακολουθεί να μην λαμβάνει απάντηση μέσα σε αυτό το χρονικό περιθώριο τότε ξαναστέλνει κάθε 5 λεπτά. Στην εικόνα 2.33 απεικονίζεται η δομή ενός DHCP μηνύματος.

Εικόνα 2.33. Δομή ενός DHCP μηνύματος

Αριθμός πεδίου	Περιγραφή
1	Καθορίζει τον τύπο του DHCP μηνύματος. Αν για παράδειγμα τεθεί σε 1 τότε είναι ένα DHCP μήνυμα αίτησης πελάτη (DHCP Request client) αν τεθεί σε 2 τότε είναι ένα μήνυμα απάντησης εξυπηρετητή (DHCP Response server).
2	Καθορίζει την αρχιτεκτονική υποδομή ενός τοπικού δικτύου (LAN). Για παράδειγμα, για να καθοριστεί ο τύπος του ehernet πρέπει το πεδίο αυτό να τεθεί σε 1.
3	Καθορίζεται το μήκος της φυσικής διεύθυνσης MAC (επιπέδου σύνδεσης δεδομένων) σε bytes. Στο Ethernet (που χρησιμοποιείται ευρέος σε LAN δίκτυα) η τιμή που θα πάρει αυτό το πεδίο θα είναι το 6.
4	Αριθμός hops που έγιναν για την προώθηση του μηνύματος
5	Χρησιμοποιείται από τους DHCP πελάτες για να «ταιριάξουν» τα απαντητικά μηνύματα του DHCP εξυπηρετητή με τις προηγούμενες αιτήσεις μηνυμάτων που μεταδόθηκαν.
6	Χρόνος που διήρκησε (σε δευτερόλεπτα) από την στιγμή που ο DHCP πελάτης εκκίνησε την διεργασία DHCP.
7	Το πεδίο αυτό αποκαλείται ως broadcast bit, και μπορεί να τεθεί σε 1 ως ένδειξη ότι τα μηνύματα ως προς τον DHCP πελάτη πρέπει να είναι broadcast.
8	Η IP διεύθυνση του DHCP πελάτη η οποία ορίζεται από τον ίδιο όταν έχει επιβεβαιώσει ότι η διεύθυνση του είναι έγκυρη.
9	Η IP διεύθυνση του DHCP πελάτη που έχει όμως οριστεί από τον DHCP εξυπηρετητή για να ενημερώσει τον πρώτο για την IP διεύθυνση που θα έχει.
10	Η IP διεύθυνση του επόμενου DHCP εξυπηρετητή που καλείται να επικοινωνήσει ο DHCP πελάτης προκειμένου να γίνει η διαδικασία ρύθμισης address.
11	Είναι η διεύθυνση του τοπικού gateway που λειτουργεί ως relay agent του DHCP.
12	Η φυσική διεύθυνση MAC του DHCP πελάτη.
13	Η φυσική διεύθυνση του DHCP εξυπηρετητή που θα επικοινωνήσει ο DHCP πελάτης για την διαδικασία ρύθμισης.
14	Το όνομα του αρχείου του DHCP πελάτη προκειμένου να κάνει αίτηση από τον επόμενο DHCP εξυπηρετητή. Για παράδειγμα το όνομα του αρχείου που περιέχει το λειτουργικό σύστημα του συγκεκριμένου DHCP πελάτη.

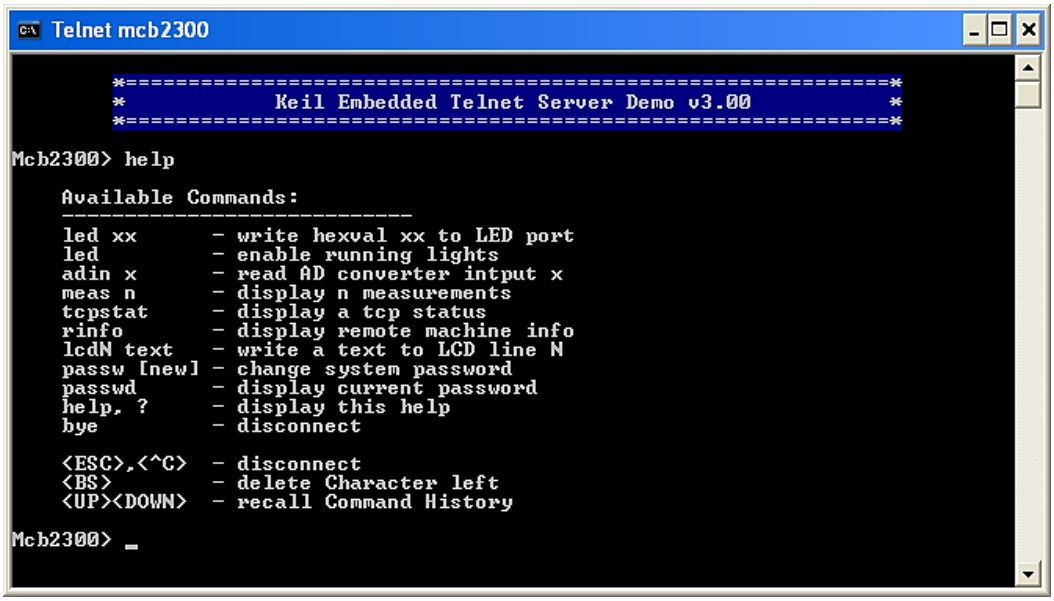
Πίνακας 2.3. Περιγραφή πεδίων του DHCP μηνύματος

2.5.13 Telnet

Το Telnet είναι μια από τις υπηρεσίες του διαδικτύου (Internet) που μας επιτρέπει να συνδεόμαστε με έναν απομακρυσμένο υπολογιστή και να δουλεύουμε αλληλεπιδραστικά σε αυτόν χρησιμοποιώντας τα προγράμματά του σαν να είμαστε δηλαδή άμεσα συνδεδεμένοι μαζί του.

Για παράδειγμα, το δικό μας τερματικό - προσωπικός υπολογιστής, workstation, τερματικό ενός UNIX συστήματος, κλπ. - μετατρέπεται σε τερματικό του απομακρυσμένου υπολογιστή ο οποίος ανταποκρίνεται στις εντολές μας.

Το Telnet βασίζεται κι αυτό με την σειρά του στην αρχιτεκτονική πελάτη – εξυπηρετητή (client/server). Για να το χρησιμοποιήσουμε, εκτελούμε στον υπολογιστή μας ένα πρόγραμμα Telnet πελάτη (Telnet client), ενώ στον απομακρυσμένο υπολογιστή εκτελείται ένα πρόγραμμα που ονομάζεται Telnet εξυπηρετητής (Telnet server). Ο Telnet εξυπηρετητής μπορεί να ανταποκριθεί σε πολλές αιτήσεις συγχρόνως, δημιουργώντας μια νέα διεργασία για κάθε νέα αίτηση.



Εικόνα 2.34. Παράδειγμα telnet session σε έναν telnet εξυπηρετητή (server)

2.5.14 Secure Shell - SSH

Το SSH είναι ένα πρωτόκολλο που παρέχει ασφαλή απομακρυσμένη σύνδεση σε δικτυακές επικοινωνίες. Είναι σχεδιασμένο ώστε να είναι απλό και φθηνό. Το SSH1 παρείχε ασφαλές remote logon με σκοπό την αντικατάσταση του TELNET και άλλων μη ασφαλών σχημάτων. Επίσης, έχει πιο γενική ικανότητα client/server. Το SSH2 διορθώνει έναν αριθμό σφαλμάτων ασφάλειας. Οι SSH πελάτες και οι SSH εξυπηρετητές είναι ευρέως διαθέσιμοι. Είναι ότι πρέπει για remote login και X tunnels. Το SSH αποτελείται από τρία βασικά στοιχεία:

- **Το πρωτόκολλο επιπέδου μεταφοράς SSH (SSH Transport layer protocol)** παρέχει πιστοποίηση ταυτότητας του εξυπηρετητή (server), ακεραιότητα των δεδομένων και εξασφάλιση του απόρρητου της συναλλαγής. Η πιστοποίηση της αυθεντικότητας του SSH εξυπηρετητή πραγματοποιείται στο επίπεδο μεταφοράς και βασίζεται στο ζεύγος κλειδιών που έχει ο SSH πελάτης (client) και ο SSH

εξυπηρετητής (server). Για να πραγματοποιηθεί η πιστοποίηση της αυθεντικότητας του SSH εξυπηρετητή είναι απαραίτητο οι SSH πελάτες να γνωρίζουν τα κλειδιά του host. Γίνεται ανταλλαγή πακέτων για αποκατάσταση της TCP σύνδεσης και για να μπορούν στην συνέχεια να ανταλλαγούν δεδομένα Χρησιμοποιεί συγκεκριμένη δομή πακέτου. Προαιρετικά μπορεί να εφαρμόσει και συμπίεση δεδομένων. Τυπικά τρέχει πάνω από μία TCP/IP σύνδεση.

- **Το πρωτόκολλο πιστοποίησης χρήστη SSH (SSH User Authentication protocol)** εγγυάται την αυθεντικότητα του SSH πελάτη στον SSH εξυπηρετητή και τρέχει πάνω από το πρωτόκολλο επιπέδου μεταφοράς. Υπάρχουν τρείς τύποι μηνυμάτων:

    - SSH_MSG_USERAUTH_REQUEST
    - SSH_MSG_USERAUTH_FAILURE
    - SSH_MSG_USERAUTH_SUCCESS

Χρησιμοποιούνται οι ακόλουθες μέθοδοι πιστοποίησης αυθεντικότητας: Δημόσιο κλειδί (public key), κωδικοί (passwords), hot-based

- **Το πρωτόκολλο σύνδεσης SSH (SSH Connection Protocol)** προϋποθέτει ασφαλή σύνδεση πιστοποίησης αυθεντικότητας και χρησιμοποιείται για πολλαπλά λογικά κανάλια όπου:

    - Οι SSH επικοινωνίες χρησιμοποιούν λογικά κανάλια
    - Η κάθε πλευρά μπορεί να τα ανοίξει με ένα μοναδικό αριθμό
    - Μηχανισμός ελέγχου ροής
    - Υπάρχουν τρία στάδια:
        - Άνοιγμα ενός καναλιού
        - Μεταφορά δεδομένων
        - Κλείσιμο καναλιού

<u>Ιδιωτικά Και Δημόσια Κλειδιά</u>

Κάθε SSH εξυπηρετητής και SSH πελάτης πρέπει να διαθέτουν ένα ζευγάρι ιδιωτικού και δημόσιου κλειδιού για να μπορέσουν να επαληθεύσουν την ταυτότητα τους μεταξύ τους.

Ο καθένας απ' τους δύο μπορεί να έχει στην κατοχή του παραπάνω από ένα ζευγάρι κλειδιών, όταν αυτά βέβαια χρησιμοποιούνται με διαφορετικούς αλγόριθμους, ενώ η από κοινού χρήση ενός ζεύγους από πολλούς εξυπηρετητές δεν είναι εφικτή.

Για να μπορεί με ευκολία ο SSH πελάτης (client) να επαληθεύει την ταυτότητα του SSH εξυπηρετητή (server) είναι απαραίτητο να γνωρίζει το δημόσιο κλειδί που αντιστοιχεί σε αυτόν. Υπάρχουν δυο διαφορετικά μοντέλα που εξασφαλίζουν την προηγούμενη προϋπόθεση:

- ✓ Πρώτον, ο client έχει αποθηκευμένα σε μια τοπική βάση δεδομένων τα ονόματα των server και τα σχετιζόμενα με αυτά δημόσια κλειδιά. Αυτή η μέθοδος δεν απαιτεί μια κεντρική διαχείριση των κλειδιών από τρίτους. Το μειονέκτημα είναι ότι το μέγεθος μιας τέτοιας βάσης δεδομένων μπορεί να εξελιχθεί σημαντικά και συνεπώς η συντήρηση της να γίνει δύσκολη.

- ✓ Στην δεύτερη περίπτωση, σχέση μεταξύ του ονόματος του server και του κλειδιού του πιστοποιείται από μια αξία εμπιστοσύνης Certification Authority. Το πρόγραμμα του πελάτη γνωρίζει μόνο το δημόσιο κλειδί της Certification

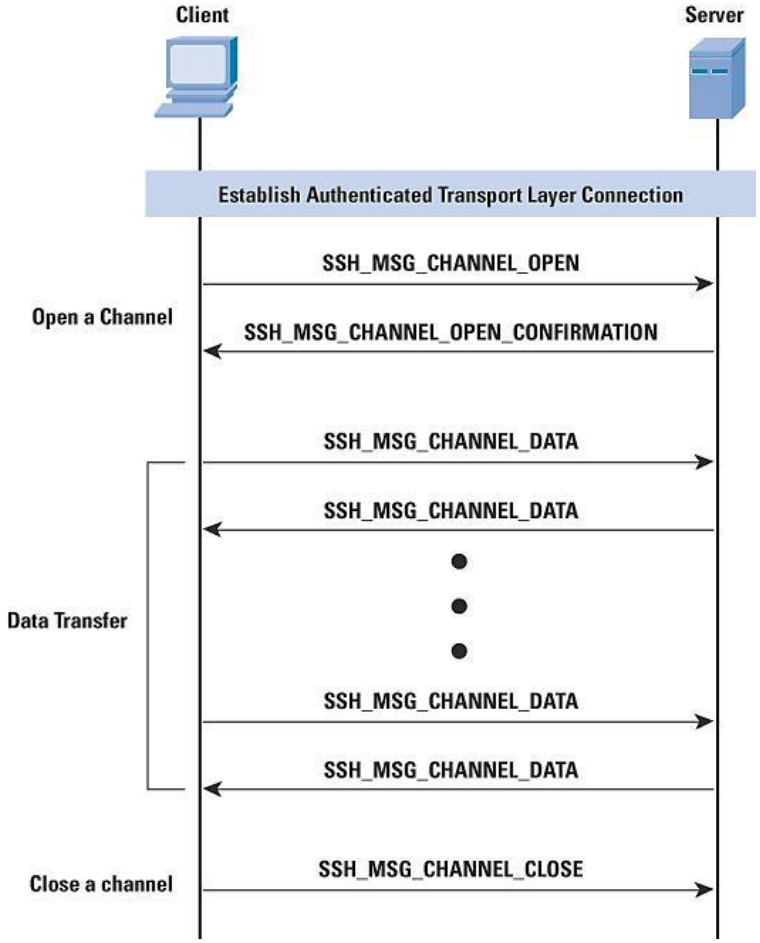
Authority και μπορεί να επιβεβαιώσει την εγκυρότητα των κλείδων που έχουν πιστοποιηθεί από την CA. Εδώ δεν υπάρχει το πρόβλημα της διατήρησης μεγάλων βάσεων δεδομένων από τα τοπικά συστήματα, αφού μόνο ένα κλειδί χρειάζεται να αποθηκεύει ο client. Επίσης, πιστοποίηση κάθε κλειδιού μπορεί να είναι μια χρονοβόρα και περίπλοκη διαδικασία.

Ο πρωταρχικός στόχος του SSH πρωτοκόλλου είναι η βελτίωση της ασφάλειας στο διαδίκτυο και ο τρόπος με τον οποίο προσπαθεί να το επιτύχει αυτό μιας και βασίζεται στο εξής σκεπτικό:

- Όλοι οι αλγόριθμοι κρυπτογράφησης, παροχής ακεραιότητας και ανταλλαγής κλειδιών έχουν δοκιμαστεί και οι αλγόριθμοι χρησιμοποιούν κλειδιά μεγέθους ικανού να παρέχει προστασία απέναντι στις ισχυρότερες επιθέσεις κρυπτοανάλυσης.

- Στην περίπτωση που κάποιος αλγόριθμος "σπάσει", είναι εύκολη η αντικατάσταση του από κάποιον άλλο χωρίς αλλαγές στις βάσεις του SSH.

- Για την ταχεία ανάπτυξη και υιοθέτηση του πρωτοκόλλου, κάποιες έχουν γίνει παραχωρήσεις. Σημαντικότερη από αυτές είναι η καθιέρωση της επαλήθευσης των κλείδων με υποχρεωτική, γεγονός όμως που δεν συνιστάται.



Εικόνα 2.35. Παράδειγμα επικοινωνίας SSH μεταξύ πελάτη (client) και εξυπηρετητή (server)

Το SSH μετατρέπει την μη ασφαλή σύνδεση TCP σε μια ασφαλή σύνδεση SSH και αυτό το κάνει με τους εξής τρόπους:

- ✓ Το πρωτόκολλο επιπέδου μεταφοράς SSH (SSH Transport Layer) αποκαθιστά μια σύνδεση TCP μεταξύ του SSH πελάτη και του SSH εξυπηρετητή.

- ✓ Υποστηρίζονται δύο είδη προώθησης θύρας:

  Τοπική προώθηση (local fowarding): Ανακατευθύνει συγκεκριμένο application layer traffic από μια μη ασφαλή σύνδεση TCP προς ένα ασφαλές SSH tunnel.

  Απομακρυσμένη προώθηση (remote forwading): Ο SSH πελάτης του χρήστη ενεργεί για λογαριασμό του SSH εξυπηρετητή. Ο SSH πελάτης λαμβάνει την κίνηση (traffic) με μια συγκεκριμένη θύρα προορισμού, προϋποθέτει την κίνηση στην σωστή θύρα και το στέλνει στον προορισμό που επιλέγει ο χρήστης.

2.6 Επίπεδο μεταφοράς (Transport layer – Layer 4)

Οι υπηρεσίες και τα πρωτόκολλα του επιπέδου μεταφοράς παρέχουν επικοινωνία (εικονική/ λογική σύνδεση) μεταξύ εφαρμογών που τρέχουν σε διαφορετικούς hosts. Όπως είχαμε αναφέρει στο επίπεδο εφαρμογής υπάρχουν δύο πρωτόκολλα μεταφοράς μηνυμάτων, το Transmission Control Protocol – TCP και το User Datagram Protocol – UDP. Το TCP όπως είχαμε αναφέρει παρέχει αξιόπιστη μεταφορά δεδομένων παρέχοντας μια συνδεσμική υπηρεσία στις εφαρμογές που το χρησιμοποιούν. Με τον όρο αξιόπιστη μεταφορά δεδομένων αναφερόμαστε στην εγγυημένη παράδοση μηνυμάτων στον προορισμό και τον έλεγχο ροής. Το TCP τεμαχίζει τα μηνύματα επιπέδου εφαρμογής σε μικρότερα τμήματα που ονομάζονται segments και παρέχει μηχανισμό ελέγχου συμφόρησης έτσι ώστε να ρυθμίζει τον ρυθμό μετάδοσης δεδομένων σε περίπτωση που ένα δίκτυο εμφανίσει συμφόρηση.
Το πρωτόκολλο UDP παρέχει στις εφαρμογές που το χρησιμοποιούν μια ασυνδεσμική υπηρεσία η οποία δεν παρέχει αξιοπιστία, έλεγχο ροής και έλεγχο συμφόρησης. Όταν αναφερόμαστε σε πακέτα UDP εννοούμε τα αυτοδύναμα πακέτα (datagrams). Τα πρωτόκολλα μεταφοράς δεδομένων TCP και UDP τρέχουν σε τερματικά συστήματα όπου:

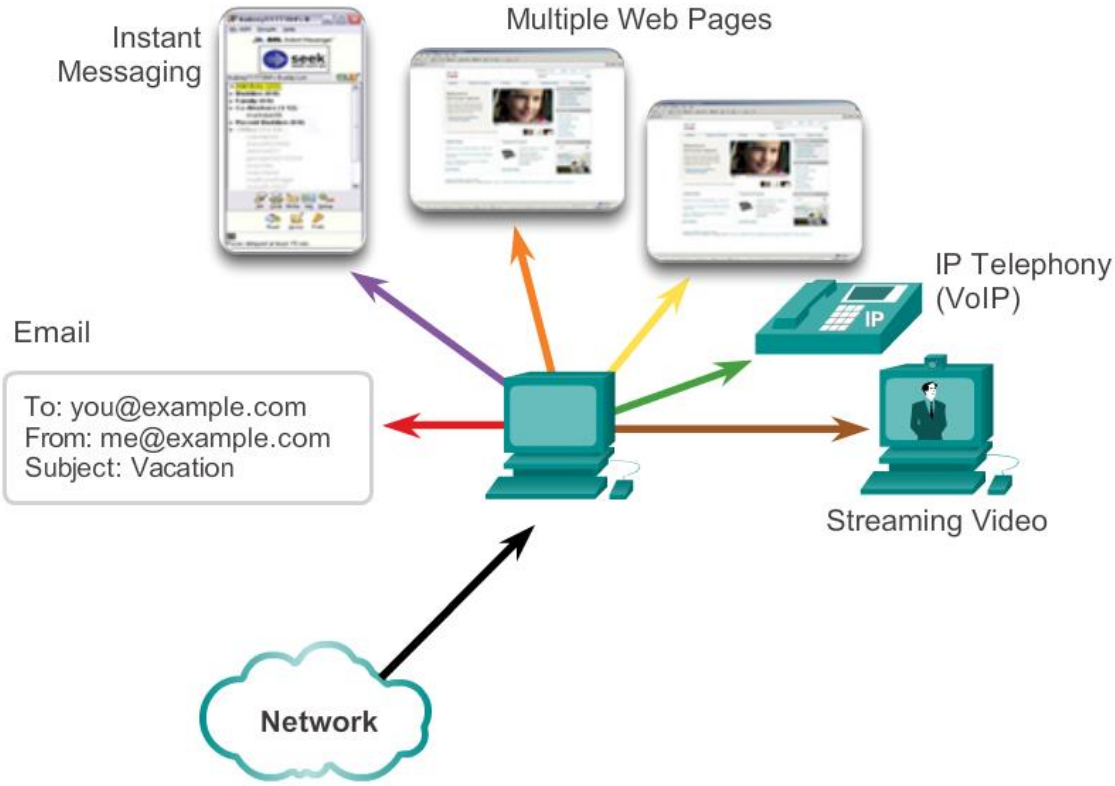
- Ο αποστολέας (δηλαδή η αποστέλλουσα πλευρά) χωρίζει τα μηνύματα είτε σε segments (αν η εφαρμογή του χρήστη χρησιμοποιεί το TCP) είτε σε datagrams (αν η εφαρμογή του χρήστη χρησιμοποιεί το UDP). Στην συνέχεια αφού τεμαχιστούν τα μηνύματα του επιπέδου εφαρμογής είτε σε segments είτε σε datagrams τα προωθεί στο επίπεδο δικτύου.

- Ο παραλήπτης (δηλαδή η λαμβάνουσα πλευρά) λαμβάνει αυτά τα πακέτα segment ή datagram, τα επανασυρναμολογεί και τα προωθεί στο επίπεδο εφαρμογής.

Τα πρωτόκολλα του επιπέδου μεταφοράς παρέχουν την δυνατότητα λογικής επικοινωνίας (logical communication) ανάμεσα σε διεργασίες εφαρμογών που εκτελούνται σε διαφορετικούς υπολογιστές. Οι διεργασίες εφαρμογών χρησιμοποιούν την λογική επικοινωνία που παρέχεται στο επίπεδο μεταφοράς για να ανταλλάξουν μηνύματα μεταξύ τους χωρίς να ασχολούνται με τις λεπτομέρειες της φυσικής υποδομής που χρησιμοποιείται για την μεταφορά αυτών των μηνυμάτων. Σε αυτό το σημείο ας κάνουμε μια μικρή παρατήρηση στο επίπεδο δικτύου. Το επίπεδο δικτύου επιτυγχάνει «επικοινωνία» μεταξύ hosts και το πρωτόκολλο IP δεν εγγυάται αξιόπιστη μεταφορά των πακέτων. Όταν αναφερόμαστε σε μη αξιόπιστη μετάδοση εννοούμε ότι δεν υπάρχει εγγύηση αν ο παραλήπτης θα λάβει τα πακέτα με την σειρά που στάλθηκαν ούτε ότι δεν θα υπάρξουν σφάλματα bits σε αυτά.

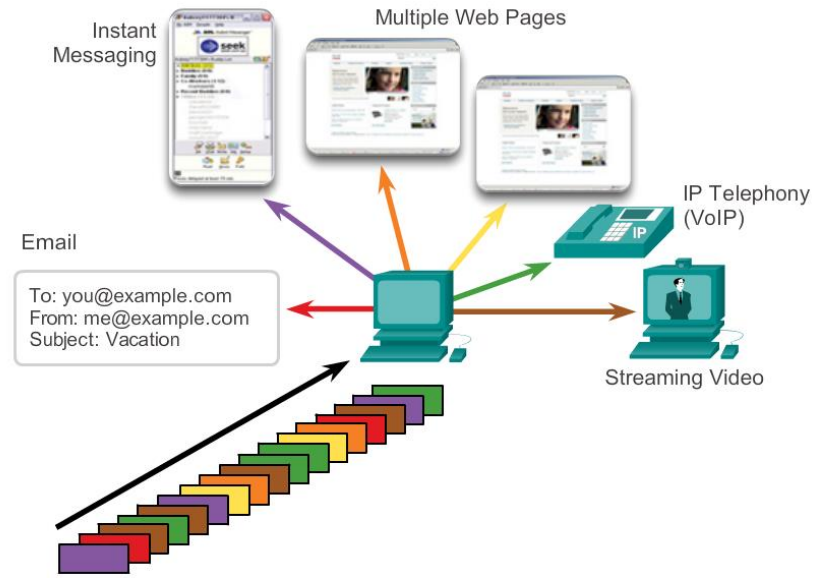
2.6.1 Διαχείριση πολλαπλών συνομιλιών: Πολύπλεξη και Αποπολύπλεξη

Στο επίπεδο μεταφοράς, το σύνολο των δεδομένων που μεταφέρονται μεταξύ μιας εφαρμογής πηγής και μιας εφαρμογής προορισμού είναι γνωστό ως σύνοδος (session). Δηλαδή ένας κόμβος μπορεί να χρησιμοποιεί πολλαπλές εφαρμογές που επικοινωνούν ταυτόχρονα μέσω του δικτύου (όπως στην εικόνα 2.36). Για παράδειγμα μια εφαρμογή Α στον τοπικό κόμβο επικοινωνεί με μια ή περισσότερες εφαρμογές που εκτελούνται σε έναν ή περισσότερους απομακρυσμένους υπολογιστές. Το επίπεδο μεταφοράς αναλαμβάνει την διαδικασία διατήρησης και παρακολούθησης των πολλαπλών αυτών συνόδων (sessions). Αυτή η μεταφορά πολλαπλής ροής δεδομένων ή σύνοδοι (sessions) μέσω το ίδιου μέσου δικτύου ονομάζεται πολύπλεξη συνόδων.



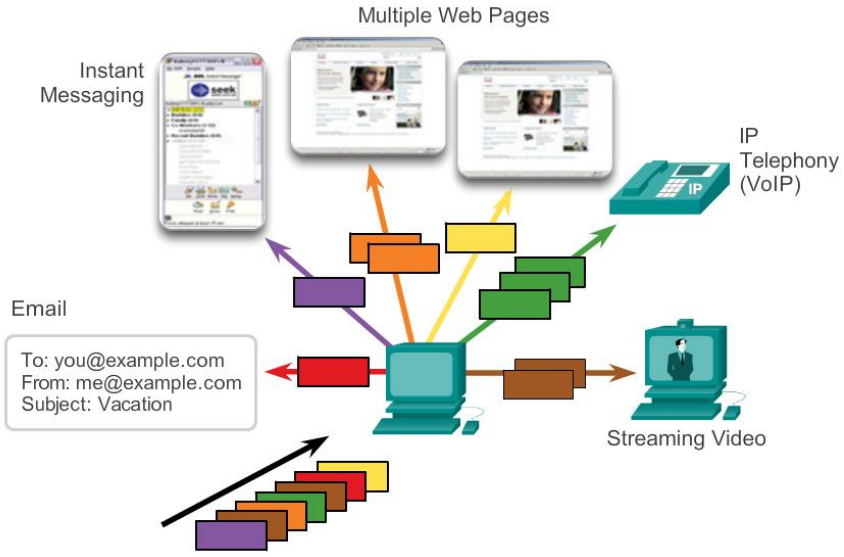
Εικόνα 2.36. Παράδειγμα επικοινωνίας SSH μεταξύ πελάτη (client) και εξυπηρετητή (server)

Τα δεδομένα πρέπει να διαμορφωθούν κατάλληλα ώστε να αποστέλλονται μέσω του δικτύου. Τα περισσότερα δίκτυα έχουν ένα περιορισμό σχετικά με την ποσότητα των δεδομένων που μπορούν να περιληφθούν σε ένα πακέτο. Τα πρωτόκολλα του στρώματος μεταφοράς έχουν υπηρεσίες που τεμαχίζουν τα δεδομένα της εφαρμογής σε κατάλληλου μεγέθους block δεδομένων (ένα τέτοιο παράδειγμα απεικονίζεται στην εικόνα 2.37). Αυτές οι υπηρεσίες περιλαμβάνουν την διαδικασία ενθυλάκωσης που απαιτείται για κάθε τμήμα (segment) δεδομένων. Η επικεφαλίδα προστίθεται σε κάθε τμήμα (segment) και χρησιμοποιείται για την επανασυναρμολόγηση τους. Αυτή η επικεφαλίδα χρησιμοποιείται και για την παρακολούθηση ροών δεδομένων. Αυτό συμβαίνει για διαχειριστεί ο όγκος των δεδομένων που διέρχονται σε κάθε σύνοδο.



Εικόνα 2.37. Παράδειγμα επικοινωνίας SSH μεταξύ πελάτη (client) και εξυπηρετητή (server)

Όταν φτάσει το τμήμα (segment) στον προορισμό, το επίπεδο μεταφοράς πρέπει να είναι σε θέση να επανασυναρμολογήσει τα κομμάτια των δεδομένων στην αρχική τους μορφή. Μπορεί να υπάρχουν πολλές εφαρμογές ή υπηρεσίες που εκτελούνται σε κάθε υπολογιστή στο δίκτυο. Για να περάσουν οι ροές δεδομένων με τις κατάλληλες εφαρμογές, το στρώμα μεταφοράς πρέπει να προσδιορίσει την εφαρμογή προορισμού. Ένα παράδειγμα είναι στην εικόνα 2.38.

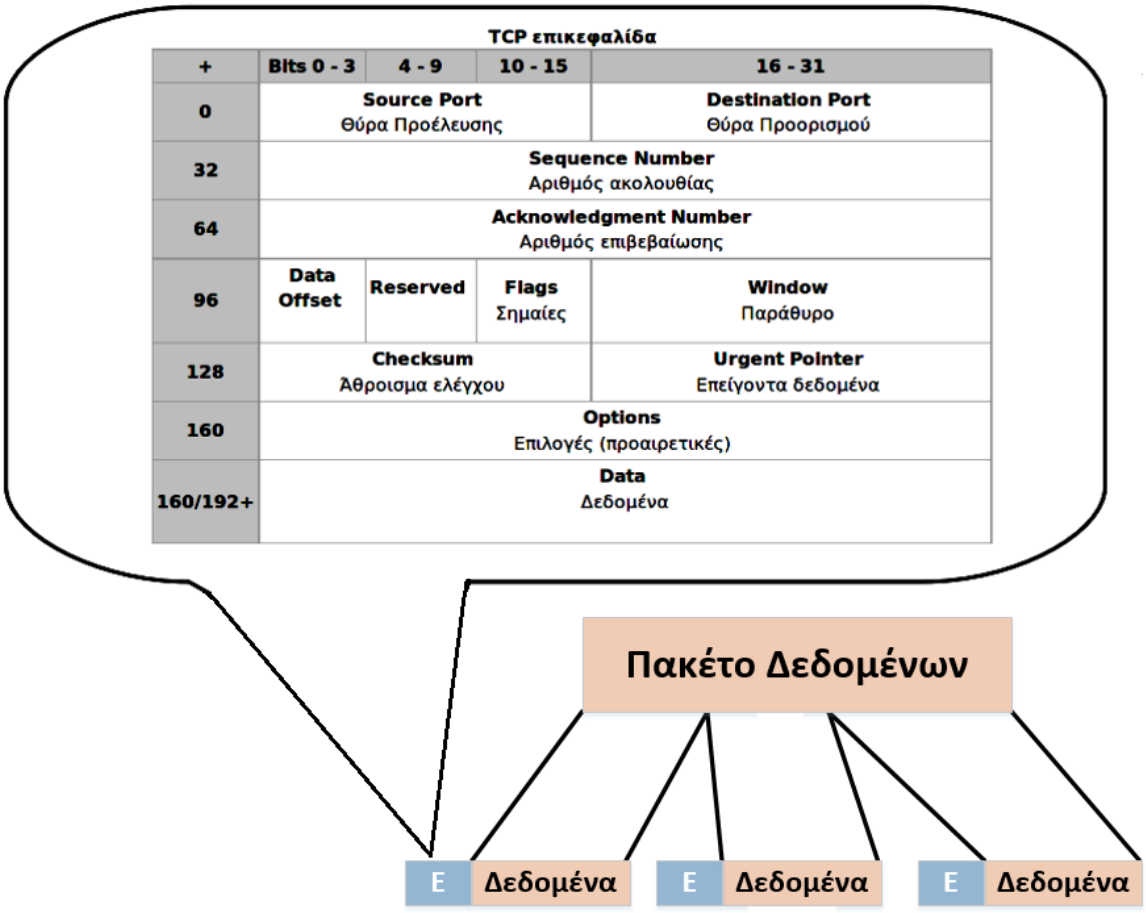


Εικόνα 2.38. Παράδειγμα επικοινωνίας SSH μεταξύ πελάτη (client) και εξυπηρετητή (server)

Για να επιτευχθεί αυτό, το στρώμα μεταφοράς αναθέτει σε κάθε εφαρμογή ένα αναγνωριστικό. Αυτό το αναγνωριστικό ονομάζεται ένας αριθμός θύρας (port number). Κάθε εφαρμογή που έχει πρόσβαση στο δίκτυο εκχωρείται σε αυτήν ένας αριθμός θύρας όπου μοναδικό στον συγκεκριμένο υπολογιστή. Το επίπεδο μεταφοράς χρησιμοποιεί τις θύρες για να προσδιορίσει την εφαρμογή ή την υπηρεσία στην οποία θα πρέπει να φτάσουν τα δεδομένα. Αυτός ο διαμοιρασμός των δεδομένων ονομάζεται αποπολύπλεξη συνόδων.

2.6.2 Transmission Control Protocol – TCP

Το πρωτόκολλο TCP (Transmission Control Protocol) είναι ένα βασικό πρωτόκολλο της τεχνολογίας TCP/IP. Περιέχει υπηρεσίες προσανατολισμένες σε σύνδεση και εξασφαλίζει την αξιόπιστη μεταφορά δεδομένων και την απ' άκρη σε άκρη επικοινωνία. Το TCP λαμβάνει απ' τα πρωτόκολλα του ανωτέρου επιπέδου τα προς μετάδοση δεδομένα και τα μεταδίδει μόνο όταν συμπληρωθεί πακέτο με μέγεθος ίσο με αυτό που έχει συμφωνηθεί κατά την εγκατάσταση της σύνδεσης. Αντίστοιχα όταν το TCP λαμβάνει μηνύματα με μέγεθος μεγαλύτερο από αυτό που συμφωνήθηκε το διασπά σε μικρότερα πακέτα τα οποία ονομάζονται segments.

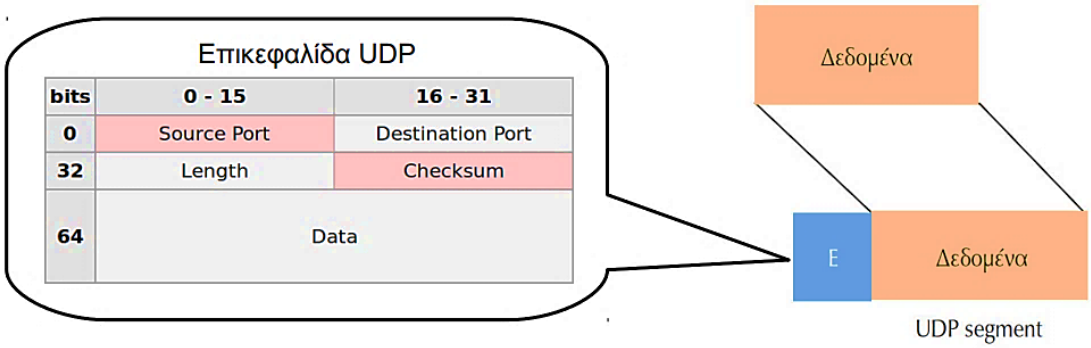


Εικόνα 2.39. Διάσπαση δεδομένων σε TCP τμήματα και η επικεφαλίδα

Όπως είπαμε το TCP προσφέρει αξιοπιστία. Εγγυάται δηλαδή ότι τα πακέτα θα παραδοθούν στον προορισμό τους, ότι θα φτάσουν με τη σωστή σειρά με την οποία στάλθηκαν και ότι τα περιεχόμενα των πακέτων θα φτάσουν στον προορισμό τους χωρίς να αλλοιωθούν (όπως δηλαδή στάλθηκαν). Το TCP δουλεύει ως εξής: το κάθε πακέτο δεδομένων αριθμείται. Μόνο ο παραλήπτης και ο αποστολέας μπορούν να παρακολουθούν τους αριθμούς των πακέτων και να ανταλλάσσουν μεταξύ τους πληροφορίες. Ο παραλήπτης λαμβάνει το πρώτο πακέτο, το δεύτερο, κλπ. Σε περίπτωση που παρουσιαστεί κάποιο πρόβλημα στο δίκτυο είτε χαθεί κάποιο πακέτο κατά τη διάρκεια της μετάδοσης, ο παραλήπτης ζητάει ξανά το πακέτο και ο αποστολέας είναι υπεύθυνος για την αναμετάδοση του. Ο παραλήπτης ελέγχει επίσης αν το περιεχόμενο των πακέτων φτάσει σωστά. Η μέθοδος αυτή εξασφαλίζει αξιοπιστία και ταχύτητα διότι οι ενδιάμεσοι υπολογιστές δεν εκτελούν ελέγχους.

2.6.3 User Datagram Protocol – UDP

Το πρωτόκολλο αυτοδύναμων πακέτων χρήστη (User Datagram Protocol – UDP) είναι ένα πρωτόκολλο χωρίς σύνδεση και ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο. Διάφορα προγράμματα χρησιμοποιούν το πρωτόκολλο UDP για την αποστολή σύντομων μηνυμάτων (γνωστών και ως UDP Segments) από τον έναν υπολογιστή στον άλλον μέσα σε ένα δίκτυο υπολογιστών. Ένα UDP segment αποτελείται από μια επικεφαλίδα των 8 byte (64 bit), ακολουθούμενη από δεδομένα. Στην εικόνα 2.37 απεικονίζεται η δομή ενός UDP αυτοδύναμου πακέτου.



Εικόνα 2.40. Δημιουργία UDP τμήματος και η επικεφαλίδα

Το UDP δεν εγγυάται αξιόπιστη επικοινωνία και αυτό διότι τα πακέτα UDP που λαμβάνει ο παραλήπτης μπορεί να τα παραλάβει με λάθος σειρά, διπλά ή να μην φτάσουν ποτέ εάν το δίκτυο έχει μεγάλο φόρτο. Παρόλο που όπως αναφέραμε παραπάνω το πρωτόκολλο TCP παρέχει όλους τους απαραίτητους μηχανισμούς ελέγχου και επιβολής της αξιοπιστίας. Το UDP δεν διαθέτει αυτές τις δυνατότητες.
Η έλλειψη των μηχανισμών αυτών καθιστά το πρωτόκολλο UDP αρκετά γρήγορο και αποτελεσματικό, τουλάχιστον για εφαρμογές που δεν απαιτούν αξιόπιστη επικοινωνία. Τέτοιες εφαρμογές μπορεί να θεωρηθούν το audio και video streaming οι οποίες χρησιμοποιούν κατά κόρον πακέτα UDP. Για τις εφαρμογές αυτές είναι πολύ σημαντικό τα πακέτα να παραδοθούν στον παραλήπτη σε σύντομο χρονικό διάστημα για να αποφευχθεί το ενδεχόμενο διακοπής στην ροή του ήχου ή της εικόνας. Συνεπώς το πρωτόκολλο UDP είναι αρκετά γρήγορο αλλά υπάρχει η πιθανότητα μερικά πακέτα UDP να χαθούν. Στην περίπτωση που χαθεί κάποιο πακέτο, οι εφαρμογές αυτές διαθέτουν ειδικούς μηχανισμούς διόρθωσης και παρεμβολής ώστε ο τελικός χρήστης να μην παρατηρεί καμία αλλοίωση ή διακοπή στην ροή του ήχου και της εικόνας.
Σε αντίθεση με το πρωτόκολλο TCP, το UDP υποστηρίζει τις τεχνικές broadcasting και multicasting δηλαδή:

- **Broadcasting:** Όπου η αποστολή ενός πακέτου λαμβάνεται απ' όλους τους υπολογιστές ενός δικτύου
- **Multicasting:** Όπου η αποστολή ενός πακέτου απευθύνεται σε συγκεκριμένους υπολογιστές ενός δικτύου.

Η τεχνική mlticasting χρησιμοποιείται πολύ συχνά στις εφαρμογές audio και video streaming ούτως ώστε μία ροή ήχου ή εικόνας να μεταδίδεται ταυτόχρονα σε πολλούς συνδρομητές. Μερικές σημαντικές εφαρμογές που χρησιμοποιούν πακέτα UDP είναι οι εξής: Domain Name System (DNS), IPTV, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) και τα διαδικτυακά παιχνίδια (online games).

2.6.4 Σύγκριση πρωτόκολλων μεταφοράς TCP και UDP

Υπηρεσίες	TCP	UDP
Αξιοπιστία	Μηχανισμούς που εξασφαλίζουν ότι τα πακέτα που μεταδίδονται από τον αποστολέα θα φτάσουν σίγουρα στον παραλήπτη και με την σωστή σειρά.	Είναι αναξιόπιστο καθότι κατά την μετάδοση ενός πακέτου, ο αποστολέας δεν είναι σε θέση να γνωρίζει εάν το πακέτο θα φτάσει σωστά στον προορισμό του ή εάν θα χαθεί μέσα στο δίκτυο.
Σειρά πακέτων	Εάν σταλούν πολλά πακέτα, τότε θα φτάσουν στον παραλήπτη με την ίδια σειρά με την οποία στάλθηκαν. Αν λείπει ένα πακέτο και έρθουν επόμενα πακέτα, τότε τα κρατάει στο buffer έως ότου φτάσει το πακέτο που λείπει. Τότε αναδιατάσσονται και εμφανίζονται με την σωστή σειρά στον παραλήπτη. Αν δεν έρθει ποτέ αυτό το πακέτο τότε ξαναστέλνεται.	Τα πακέτα UDP, σε αντίθεση με το TCP, δεν αριθμούνται και κατά συνέπεια δεν υπάρχει κάποια συγκεκριμένη σειρά με την οποία θα πρέπει να φτάσουν στον παραλήπτη.
Βαρύτητα	Ιδιαίτερα βαρύ, δεδομένου ότι χρειάζονται τουλάχιστον 3 πακέτα για την εγκαθίδρυση της σύνδεσης, πριν μεταδοθεί οποιοδήποτε πακέτο. Επίσης, οι μηχανισμοί αξιοπιστίας που υλοποιεί το κάνουν ακόμη πιο βαρύ, πράγμα που επηρεάζει την ταχύτητα μετάδοσης δεδομένων.	Το πρωτόκολλο αυτό καθ' αυτό είναι πολύ ελαφρύ σε σύγκριση με το TCP διότι δεν εφαρμόζει όλους τους μηχανισμούς αξιόπιστης επικοινωνίας που υπάρχουν στο δεύτερο. Αυτό έχει ως συνέπεια να είναι αρκετά πιο γρήγορο

Πίνακας 2.4. Σύγκριση πρωτοκόλλων μεταφοράς TCP και UDP

2.6.5 Πρωτόκολλο Μεταφοράς Πραγματικού-Χρόνου (RTP)

Αποτελεί το κύριο πρότυπο για τη μεταφορά ήχου / εικόνας σε δίκτυα IP. Το RTP στοχεύει στην παροχή χρήσιμων υπηρεσιών για τη μεταφορά πολυμέσων σε πραγματικό χρόνο, όπως ήχου ή εικόνας, πάνω από δίκτυα IP. Αυτές οι υπηρεσίες περιλαμβάνουν αναπλήρωση χρόνου, διαπίστωση και επιδιόρθωση απωλειών, αναγνώριση φορτίου και πηγής, ανατροφοδότηση σχετικά με την ποιότητα λήψης, συγχρονισμό πολυμέσων , και διαχείριση συμμετεχόντων. Το RTP σχεδιάστηκε αρχικά για χρήση σε πολυμερείς διασκέψεις (multicast conferences). Έκτοτε, έχει αποδειχθεί χρήσιμο σε μία γκάμα άλλων εφαρμογών: σε H.323 τηλεδιάσκεψη, εκπομπή μέσω δικτύου (web casting), και τηλεοπτική εκπομπή. Τόσο στη σταθερή, όσο και στην κινητή τηλεφωνία. Η χρήση του πρωτοκόλλου εκτείνεται από εφαρμογές σημείου – σε - σημείο (point-to-point), σε πολυδιάσκεψη με χιλιάδες χρηστών, και από χαμηλού εύρους ζώνης εφαρμογές κινητής τηλεφωνίας, στην μετάδοση ασυμπίεστων σημάτων Τηλεόρασης υψηλής ευκρίνειας σε ταχύτητες της τάξης των gigabit.
Το RTP αναπτύχθηκε από την ομάδα εργασίας του IETF για τη μεταφορά Ήχου / Εικόνας, και από τότε έχει υιοθετηθεί από το ITU και διάφορους άλλους οργανισμούς καθορισμών προτύπων. Η πρώτη έκδοση του RTP ολοκληρώθηκε το 1996. Χρειάζεται να διαμορφωθεί για εξειδικευμένες χρήσεις προτού θεωρηθεί πλήρες. Μια αρχική διαμόρφωση καθορίστηκε μαζί με το αρχικό πρότυπο του RTP, και αρκετές βρίσκονται υπό ανάπτυξη. Οι διαμορφώσεις συνοδεύονται από διάφορες προδιαγραφές για τη μορφή του φορτίου, περιγράφοντας τη μεταφορά μιας συγκεκριμένης μορφής πολυμέσων. Η ανάπτυξη του RTP συνεχίζεται και σήμερα, με επανακαθορισμό του πρωτοκόλλου σε τακτά χρονικά διαστήματα.

2.7 Επίπεδο δικτύου (Network layer – Layer 3)

Το επίπεδο δικτύου είναι υπεύθυνο για την μετακίνηση πακέτων επιπέδου δικτύου, που είναι γνωστά ως IP πακέτα (IP packets) από έναν υπολογιστή προς έναν άλλο. Το πρωτόκολλο επιπέδου μεταφοράς (TCP ή UDP) σε έναν υπολογιστή προέλευσης μεταβιβάζει ένα τμήμα (segment) επιπέδου μεταφοράς και μια διεύθυνση προορισμού στο επίπεδο δικτύου. Στην συνέχεια το επίπεδο δικτύου αναλαμβάνει την παράδοση του τμήματος (segment) στον παραλήπτη.
Το επίπεδο δικτύου περιλαμβάνει το πολύ γνωστό πρωτόκολλο IP (Internet protocol) το οποίο ορίζει τα πεδία ενός IP πακέτου (IP packet) καθώς και το πώς τα τερματικά συστήματα και οι δρομολογητές ενεργούν σε αυτά τα πεδία. Το επίπεδο δικτύου παρέχει επίσης πολλά πρωτόκολλα δρομολόγησης (π.χ. RIP, BGP, OSPF κλπ) τα οποία καθορίζουν δυναμικά τις διαδρομές που ακολουθούν τα IP πακέτα απ' την πηγή στον προορισμό.

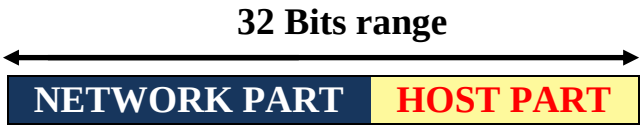
Με λίγα λόγια στο μοντέλο αναφοράς OSI το επίπεδο δικτύου είναι σε θέση να γνωρίζει τις διευθύνσεις των γειτονικών κόμβων σε ένα δίκτυο. Στα πακέτα αποδίδονται οι έγκυρες IP διευθύνσεις, επιλέγονται οι διαδρομές τους, η ποιότητα υπηρεσιών (QoS) και πραγματοποιείται η αναγνώριση και η προώθηση των εισερχόμενων μηνυμάτων (TCP ή UDP) του επιπέδου μεταφοράς.
Προτού όμως προχωρήσουμε στα πρωτόκολλα του επιπέδου δικτύου και στην λειτουργία του πρωτοκόλλου IP ας δούμε πρώτα τι είναι μια διεύθυνση IP.

2.7.1 Τι είναι μια διεύθυνση IP

Το διαδίκτυο (internet) είναι ένα δίκτυο δικτύων που αποτελείται από πολλά δίκτυα υπολογιστών όπου καθένα αποτελείται από κόμβους (π.χ. κόμβος μπορεί να θεωρηθεί ένας προσωπικός υπολογιστής). Για κάθε κόμβο που είναι συνδεδεμένος στο διαδίκτυο εκχωρείται ένας μοναδικός αριθμός που είναι γνωστός ως IP διεύθυνση και το κάθε IP πακέτο (IP packet) θα πρέπει να διαθέτει με την σειρά του μια μοναδική διεύθυνση προορισμού για να μπορέσει να δρομολογηθεί προς έναν άλλον υπολογιστή.
Η διεύθυνση αυτή αποτελείται από 4 ακέραιους αριθμούς χωρισμένους με τελεία και σε κάθε υπολογιστή αποδίδεται μια ξεχωριστή μοναδική IP διεύθυνση. Έτσι, ο κάθε υπολογιστής θα πρέπει να διαθέτει μια και μόνο μοναδική διεύθυνση. Σε αυτό το σημείο όμως πρέπει να αναφέρουμε ότι η IP διεύθυνση ακολουθεί ιεραρχική δομή. Δηλαδή μια IP διεύθυνση αλλάζει κάθε φορά που συνδεόμαστε στο διαδίκτυο και δεν παραμένει η ίδια. Οι πιθανοί αριθμοί μιας IP διεύθυνσης έχουν εύρος από 0 που είναι το ελάχιστο έως και το 255 που είναι το μέγιστο. Για παράδειγμα το σύνολο των αριθμών 193.106.1.51 αποτελεί μια IP διεύθυνση. Στο μοντέλο επικοινωνίας TCP/IP χρησιμοποιείται διευθυνσιοδότηση (addressing) μήκους 32 bits. Στους υπολογιστές, όπως γνωρίζουμε πολύ καλά ένα byte αντιστοιχείται με 8 bits οπότε το μοντέλο επικοινωνίας TCP/IP χρησιμοποιεί 4 bytes. Ένα byte μπορεί να περιέχει 256 διαφορετικές τιμές, που προκύπτουν από τις επαναληπτικές διατάξεις των 2 πραγμάτων ανά 8, δηλαδή το συνολικό πλήθος τιμών 28 = 256. Οι αριθμοί αυτοί είναι οι εξής:

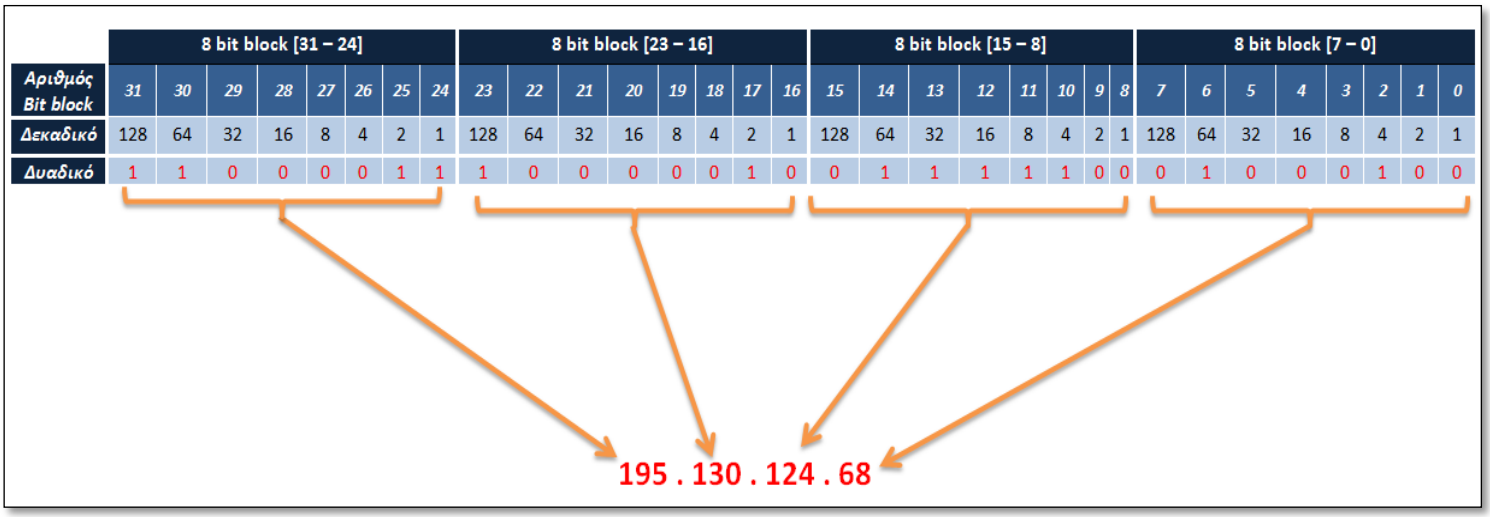
00000000
00000001
00000010
00000011
00000100
.
.
.
11111111

Όπως είχαμε αναφέρει στην υποπαράγραφο 2.5.11 οι IP διευθύνσεις αντιστοιχούνται με συμβολικά ονόματα τα οποία λέγονται domain names. Όπως είχαμε αναφέρει ο λόγος αυτός οφείλεται λόγω της δυσκολίας απομνημόνευσης μιας IP διεύθυνση. Σε αυτό το σημείο ας δούμε την δομή από την οποία αποτελούνται αυτές οι διευθύνσεις. Μια διεύθυνση IP χωρίζεται σε δύο κομμάτια το **network part** όπου είναι το μέρος που αφορά το δίκτυο και το **host part** όπου είναι το μέρος που αφορά των αριθμό των hosts σε ένα δίκτυο (δηλαδή το πόσες υπολογιστικές συσκευές μπορούν να συνδεθούν πάνω σε αυτό).



Σχήμα 2.1. Εύρος διεύθυνσης IP

Ο αριθμός δικτύου προσδιορίζει το δίκτυο, από τα πολλά που συνθέτουν το διαδίκτυο. Εκχωρείται από παγκόσμιους οργανισμούς (π.χ. RIPE,NIC,ARIN κλπ). Το host part προσδιορίζει τον κόμβο μέσα σε ένα δίκτυο και εκχωρείται από τον τοπικό διαχειριστή του δικτύου.



Εικόνα 2.41. Αναλυτική απεικόνιση δομής μιας IP διεύθυνσης

2.7.2 Διεύθυνση broadcast

Στα δίκτυα υπολογιστών το είδος εκπομπής broadcast αναφέρεται στη αποστολή ενός μηνύματος - πακέτου σε όλους τους δέκτες που ανήκουν στο υποδίκτυο. Η εκπομπή μηνυμάτων broadcast γίνεται με την αποστολή μηνύματος στη διεύθυνση broadcast του κάθε δικτύου.
Γενικά σε όλα τα δίκτυα υπάρχει μία διεύθυνση για εκπομπή μηνυμάτων broadcast. Όταν κάποιο μήνυμα απευθύνεται σε αυτήν τη διεύθυνση θεωρείται ότι αφορά όλους τους κόμβους του αντίστοιχου δικτύου. Με αυτόν τον τρόπο δεν είναι απαραίτητη η δημιουργία ξεχωριστού μηνύματος για κάθε κόμβο.

Η εκπομπή μηνυμάτων broadcast είναι χρήσιμη όταν κάποιος κόμβος του δικτύου θέλει να πάρει πληροφορίες από τους υπόλοιπους χωρίς να γνωρίζει ποιοι είναι. Όταν κάποιος κόμβος θέλει να πάρει πληροφορίες από έναν ή περισσότερους κόμβους του ίδιου δικτύου θα πρέπει να έχει έναν κατάλογο με τους γειτονικούς κόμβους ή να αρχίσει να στέλνει μηνύματα σε ένα-ένα από τα μέλη του δικτύου για να δει αν θα του απαντήσουν. Αυτή η διαδικασία είναι αρκετά χρονοβόρα και προκαλεί και άλλα προβλήματα.
Το καλύτερο είναι να αποστείλει ένα μήνυμα σε μία διεύθυνση που όποιος το παραλαμβάνει να γνωρίζει ότι πρόκειται για τέτοιου είδους μήνυμα. Πρακτικά αυτό σημαίνει ότι όταν κάποιος κόμβος παραλαμβάνει ένα πακέτο που έχει ως διεύθυνση παραλήπτη τη διεύθυνση broadcast θεωρεί ότι είναι και ο ίδιος παραλήπτης. Στις υπόλοιπες περιπτώσεις απλά απορρίπτει το πακέτο (με κάποιες εξαιρέσεις).

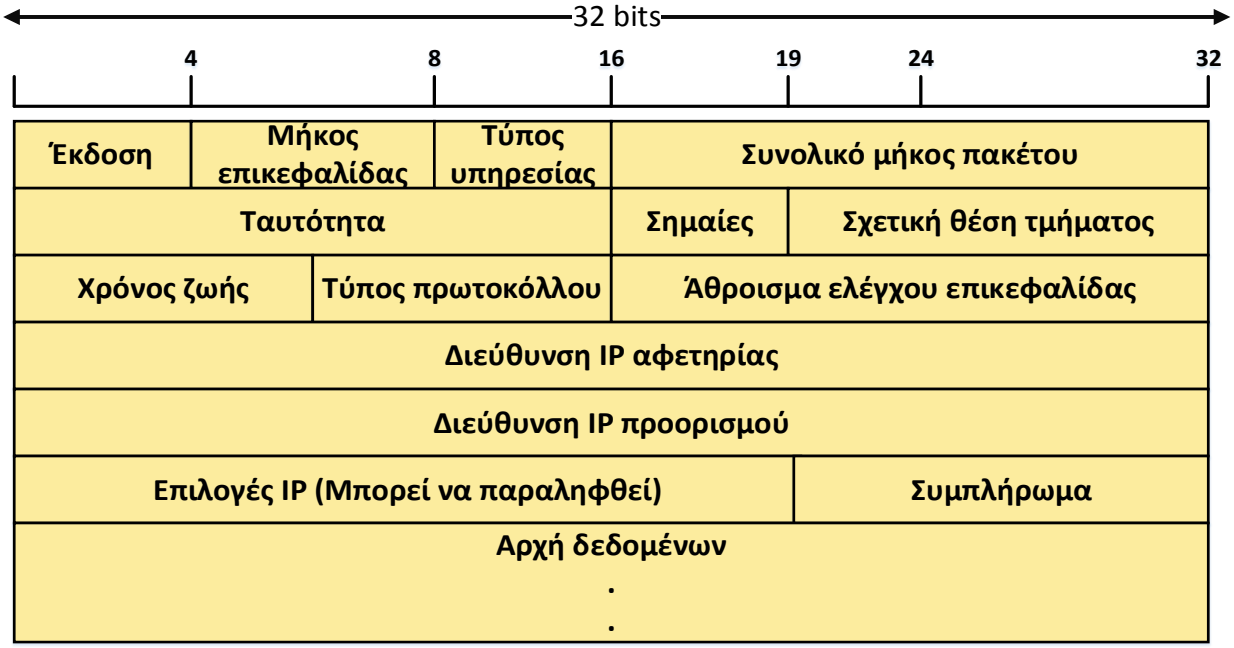
2.7.3 Δικτυακή Πύλη (Gateway)

Στα δίκτυα IP, η δικτυακή πύλη (gateway) χρησιμοποιείται για να συνδέσει δύο ή περισσότερα υποδίκτυα που χρησιμοποιούν το πρωτόκολλο IP. Για παράδειγμα, εάν μία gateway συνδέει το τοπικό δίκτυο με το διαδίκτυο, θα πρέπει από την πλευρά του τοπικού δικτύου να χρησιμοποιεί μία διεύθυνση όπως πχ 192.168.2.1, η οποία έχει δεσμευτεί από το πρωτόκολλο IP για τα τοπικά δίκτυα και στην οποία θα στέλνουν όλοι οι υπολογιστές του δικτύου τα πακέτα τους. Από την πλευρά του διαδικτύου θα πρέπει να χρησιμοποιεί μία άλλη IP διεύθυνση και συγκεκριμένα αυτή που έχει παραχωρήσει ο πάροχος διαδικτύου (ISP - Internet Service Provider).

Μία συσκευή gateway θα πρέπει να έχει όλους τους απαραίτητους μηχανισμούς ούτως ώστε να είναι σε θέση να χειριστεί τα πακέτα των δεκάδων ή εκατοντάδων υπολογιστών ενός τοπικού δικτύου. Τέτοιοι μηχανισμοί χρησιμοποιούνται παραδείγματος χάριν για την σωστή ταξινόμηση και διανομή των εισερχόμενων πακέτων στους διάφορους υπολογιστές του δικτύου και περιλαμβάνουν ανάμεσα σε άλλα και το NAT - Network Address Translation. Συνεπώς, κάθε δικτυακή συσκευή που θέλει να επικοινωνήσει με μία IP διεύθυνση που είναι εκτός του υποδικτύου του, θα πρέπει να επικοινωνήσει μέσω του τοπικού gateway το οποίο γνωρίζει τον τρόπο δρομολόγησης των πακέτων για να φτάσουν στον προορισμό τους.

2.7.4 Πρωτόκολλο διαδικτύου 4η έκδοση (IP v.4)

Το πρωτόκολλο διαδικτύου (Internet Protocol, IP) βασίζεται στην ιδέα των αυτοδύναμων πακέτων (datagrams), τα οποία μεταφέρονται ανεξάρτητα το ένα απ' το άλλο από την πηγή στον προορισμό, χωρίς να εξασφαλίζεται η αξιοπιστία στην μετάδοση τους. Όλοι οι έλεγχοι αξιόπιστης μετάδοσης δεδομένων έχουν τοποθετηθεί στο επίπεδο μεταφοράς και πραγματοποιούνται από το πρωτόκολλο TCP. Κάθε φορά που το πρωτόκολλο TCP ή UDP θέλει να μεταδώσει ένα τμήμα, το προωθεί στο πρωτόκολλο IP προσδιορίζοντας τη διεύθυνση του υπολογιστή προορισμού. Έτσι το IP δεν ενδιαφέρεται καθόλου για το τι περιέχει το τμήμα ή πως αυτό σχετίζεται με τα προηγούμενα ή επόμενα τμήματα που λαμβάνει από το πρωτόκολλο TCP ή UDP και τα οποία προωθήσει στον προορισμό τους. Κάθε φορά, που το IP λαμβάνει ένα TCP ή UDP τμήμα, προσθέτει σε αυτό τη δική του επικεφαλίδα και σχηματίζει με αυτό ένα IP αυτοδύναμο πακέτο με μήκος 64 kbytes. Από την στιγμή, που το πρωτόκολλο IP έχει σχηματίσει ένα IP αυτοδύναμο πακέτο, ο ρόλος του περιορίζεται στην εύρεση κατάλληλης διαδρομής.



Σχήμα 2.2. IP v.4 αυτοδύναμο πακέτο

Πεδία του πακέτου IP v.4

- *Έκδοση (Version):* Δείχνει την έκδοση του IP που χρησιμοποιείται
- *Μήκος Επικεφαλίδας (IP Header Length – IHL):* Δείχνει το μήκος της επικεφαλίδας σε λέξεις των 32-bit
- *Τύπος υπηρεσίας (Type-of-Service):* Αναθέτει στα πακέτα IP διαφορετικά επίπεδα σημαντικότητας
- *Συνολικό μήκος υπηρεσίας (Total Length):* Καθορίζει το μήκος σε bytes ολόκληρου του πακέτου IP, συμπεριλαμβανομένου των δεδομένων και της επικεφαλίδας

- *Ταυτότητα (Identification):* Περιέχει έναν ακέραιο που προσδιορίζει το τρέχον πακέτο. Αυτό το πεδίο χρησιμοποιείται για να βοηθήσει στη επανένωση των κατακερματισμένων πακέτων

- *Χρόνος ζωής (Time-to-Live):* Καθορίζει το χρονικό διάστημα (σε δευτερόλεπτα) που επιτρέπεται προκειμένου ένα αυτόνομο πακέτο να παραμείνει στο διαδίκτυο. Κάθε δρομολογητής που επεξεργάζεται το πακέτο πρέπει να μειώσει το χρόνο ζωής (TTL) το λιγότερο κατά ένα bit. Αυτό αποτρέπει τα πακέτα από το να κάνουν κύκλους συνέχεια.

- *Τύπος πρωτοκόλλου (Protocol type):* Προσδιορίζει το πρωτόκολλο ανωτέρου επιπέδου το οποίο θα λάβει το πεδίο δεδομένων στον προορισμό

- *Άθροισμα ελέγχου επικεφαλίδας (Header Checksum):* Εξασφαλίζει την ακεραιότητας της επικεφαλίδας IP. Επειδή πεδία της επικεφαλίδας μπορεί να αλλάξουν κατά τη μεταφορά, αυτή επαληθεύεται και επαναϋπολογίζεται σε κάθε δρομολογητή

- *Σημαίες (Flags):* Αποτελείται από ένα πεδίο των 3-bit από τα οποία τα 2 χαμηλότερης σημασίας bits ελέγχουν την κατάτμηση

    - Το χαμηλότερης σημασίας bit καθορίζει εάν το πακέτο μπορεί να κατατμηθεί
    - Το μεσαίο bit καθορίζει εάν το πακέτο είναι το τελευταίο πακέτο της κατάτμησης από μια σειρά από τεμαχισμένα πακέτα
    - Το τρίτο bit δεν χρησιμοποιείται

- *Σχετική θέση τμήματος (Fragment Offset):* Προσδιορίζει την θέση των δεδομένων των πακέτων κατάτμησης σχετικά με την αρχή των δεδομένων στο αρχικό datagram, και επιτρέπει στην διαδικασία IP προορισμού να επανενώσει σωστά το αρχικό πακέτο.

- *IP διεύθυνση αφετηρίας (Source Address):* Καθορίζει το δίκτυο και το τερματικό σύστημα που είναι συνδεδεμένο στο καθορισμένο δίκτυο και αποτελεί τον κόμβο αποστολέα

- *IP διεύθυνση προορισμού (Destination Address):* Προσδιορίζει τον κόμβο προορισμού

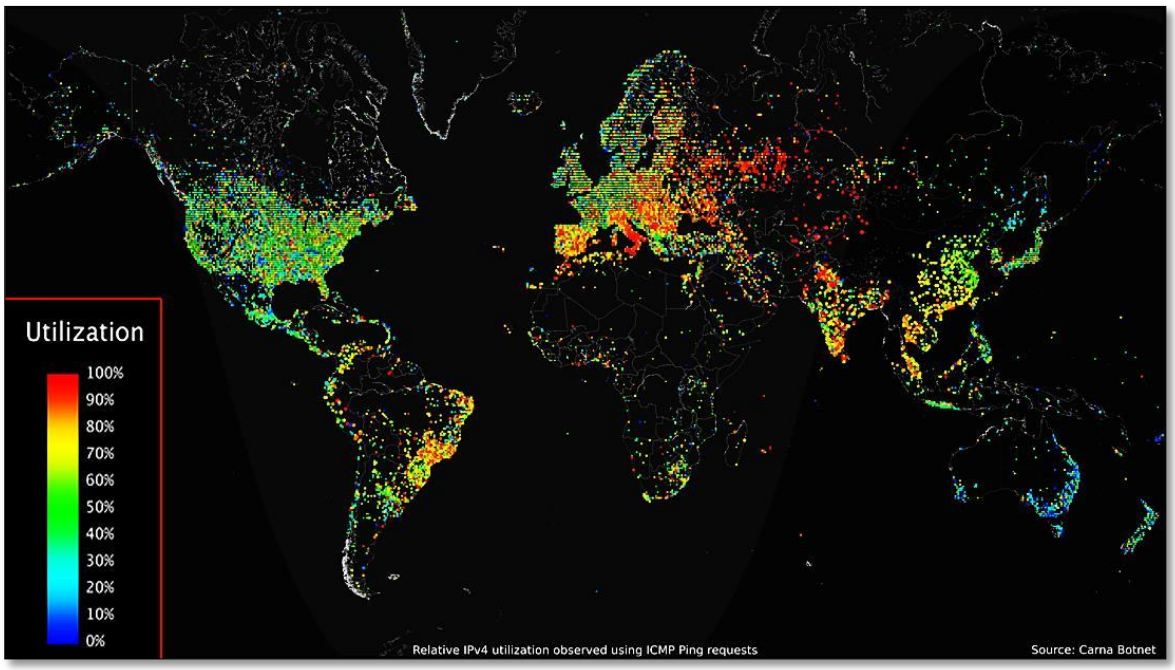
- *Επιλογές IP Options*: Επιτρέπει στο IP να υποστηρίζει διάφορες επιλογές, όπως ασφάλεια

- *Συμπλήρωμα (Padding):* Χρησιμοποιείται για να εξασφαλίσει πως το μήκος της επικεφαλίδας του αυτόνομου πακέτου είναι πολλαπλάσιο των 32 bit.

- *Αρχή δεδομένων (*Data): Περιέχει πληροφορία ανωτέρου επιπέδου.

2.7.5 Πρωτόκολλο διαδικτύου 6η έκδοση (IP v.6)

Το IPv6 (Internet Protocol version 6) είναι η πρόσφατη έκδοση του πρωτοκόλλου διαδικτύου (IP). Πρόκειται να αντικαταστήσει την παλιότερη έκδοση IPv4 που αναφέραμε στην υποπαράγραφο 2.7.4. Το IPv6 αναπτύχθηκε από το Internet Engineering Task Force – IETF, για να ασχοληθεί με το πρόβλημα εξάντλησης των IPv4 διευθύνσεων. Όπως αναφέραμε στην υποπαράγραφο 2.7.1 κάθε κόμβος ο οποίος διασυνδέεται στο διαδίκτυο πρέπει να αποδοθεί στον ίδιο μία IP διεύθυνση όπου αυτή αποτελεί και την ταυτότητα του στο διαδίκτυο. Το πρόβλημα με τις IP v.4 διευθύνσεις είναι ότι δεν επαρκεί για τις σημερινές ανάγκες καθότι η χρησιμοποίηση του διαδικτύου έχει αυξηθεί ραγδαία τα τελευταία χρόνια με αποτέλεσμα να υπάρχει η ανάγκη για περισσότερες IP διευθύνσεις.



Εικόνα 2.42. Παγκόσμιος χάρτης σχετικής χρήσης IPv.4 διευθύνσεων που παρατηρήθηκε με τη χρήση ICMP ping αιτημάτων.

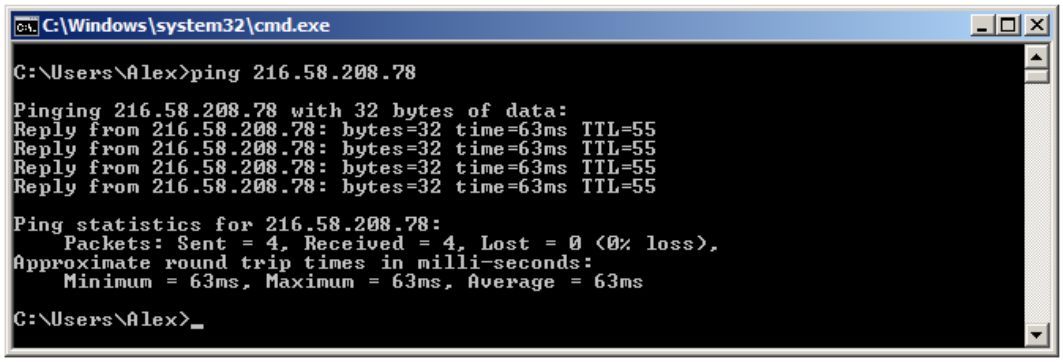
Όπως βλέπουμε από την εικόνα 2.42 απεικονίζεται η μέση χρήση των IPv.4 διευθύνσεων σε παγκόσμια κλίμακα. Η σχετική εικόνα είναι μέτρηση που πάρθηκε από έναν ανώνυμο hacker που ήθελε να παρατηρήσει την χρήση του διαδικτύου. Με κόκκινο χρώμα είναι περιοχές που κάνουν υψηλή χρήση του διαδικτύου και με μπλε σχεδόν καθόλου. Οπότε με την αυξανόμενη χρήση του διαδικτύου εμφανίζεται η ανάγκη περισσότερων διευθύνσεων απ' όσες μπορεί να παράσχει το IPv4.

Το IPv4 χρησιμοποιεί διευθύνσεις 32 bit, το οποίο επιτρέπει περίπου 4,3 δισεκατομμύρια διαφορετικές διευθύνσεις. Το IPv6 χρησιμοποιεί διευθύνσεις 128 bit, το οποίο επιτρέπει $3.4 * 10^{38}$ διαφορετικές διευθύνσεις. Τα δύο πρωτόκολλα δεν έχουν σχεδιαστεί ώστε να μπορούν να συνεργάζονται, δυσκολεύοντας έτσι την μετάβαση στο IPv6. Οι διευθύνσεις IP του πρωτοκόλλου IPv6, αποτελούνται από 8 ομάδες των τεσσάρων δεκαεξαδικών ψηφίων, χωρισμένων με άνω και κάτω τελεία, π.χ 2001:0db8:85a3:0042:1000:8a2e:0370:7334.

2.7.6 Internet Control Message Protocol – ICMP

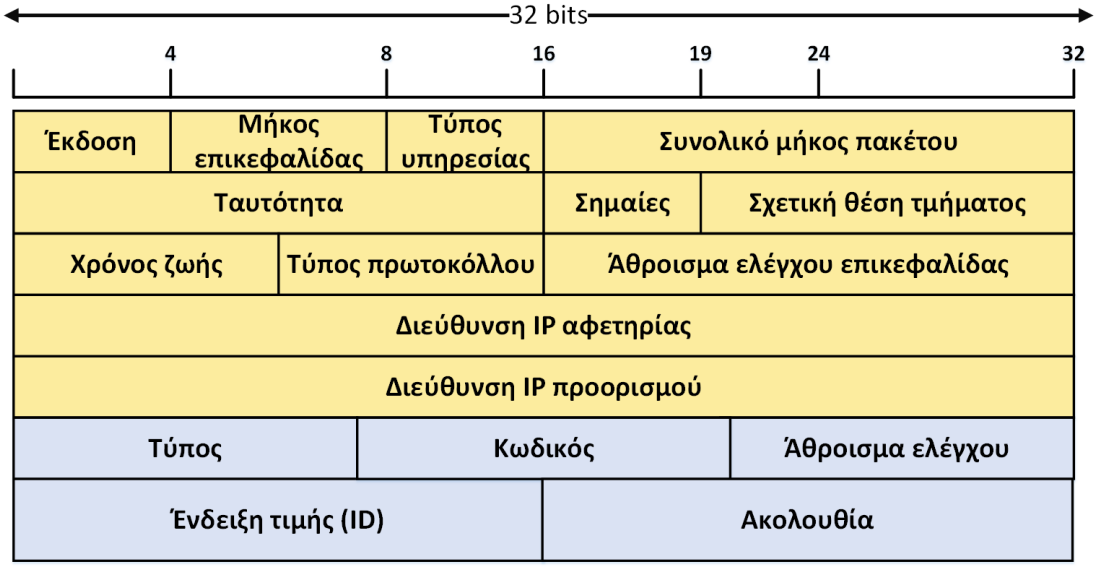
Το Internet Control Message Protocol (ICMP) είναι ένα από τα βασικά πρωτόκολλα του διαδικτύου. Η χρήση του εφαρμόζεται κυρίως από τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών ενός δικτύου για την ανταλλαγή μηνυμάτων λάθους, όπως για παράδειγμα την έλλειψη κάποιας υπηρεσίας από έναν server ή την απουσία ενός υπολογιστή από το δίκτυο.

Το πρωτόκολλο ICMP διαφέρει από τα πρωτόκολλα TCP και UDP που αναφέραμε στην παράγραφο 2.6 του επιπέδου μεταφοράς. Αυτό οφείλεται διότι δεν χρησιμοποιείται από τις εφαρμογές που εκτελούνται σε κάποιον υπολογιστή, αλλά από το λειτουργικό του σύστημα. Εξαίρεση σε αυτό τον κανόνα αποτελεί η εντολή ping, η οποία στέλνει μηνύματα ICMP Echo Request σε κάποιον υπολογιστή του δικτύου για να διαπιστώσει εάν ο υπολογιστής αυτός υπάρχει ή όχι και επίσης πόσο χρόνο χρειάζεται το μήνυμα να φτάσει σε αυτόν. Εάν ο υπολογιστής αυτός υπάρχει, θα απαντήσει με μηνύματα Echo Response.



Εικόνα 2.43. Παράδειγμα χρήσης εντολής ping στο cmd των windows.

Στην εικόνα 2.44 που ακολουθεί φαίνεται η επικεφαλίδα (header) ενός πακέτου ICMP. Με κίτρινο χρώμα απεικονίζεται η επικεφαλίδα που προκύπτει από το πρωτόκολλο IP και με ανοιχτό μπλε χρώμα η επικεφαλίδα που προκύπτει από το πρωτόκολλο ICMP. Στην παράγραφο 2.7.4 εξηγήσαμε τα πεδία ενός IP πακέτου ας κάνουμε σε αυτό το σημείο μια συνοπτική επεξήγηση των πεδίων της ICMP επικεφαλίδας.



Εικόνα 2.44. Δομή ICMP πακέτου.

Τύπος: Ο κωδικός του τύπου μηνύματος ICMP (π.χ. 0 - Echo Reply, 3 - Destination Unreachable κλπ)

Κωδικός: Το πεδίο αυτό χρησιμοποιείται ως επέκταση του προηγούμενου. Για παράδειγμα εάν το πεδίο τύπου περιέχει την τιμή 3 (Destination Unreachable), τότε το πεδίο αυτό μπορεί να περιέχει έναν κωδικό από το 1 έως το 15 που να δίνει τον λόγο για τον οποίο ο υπολογιστής που ψάχνουμε είναι εκτός δικτύου.

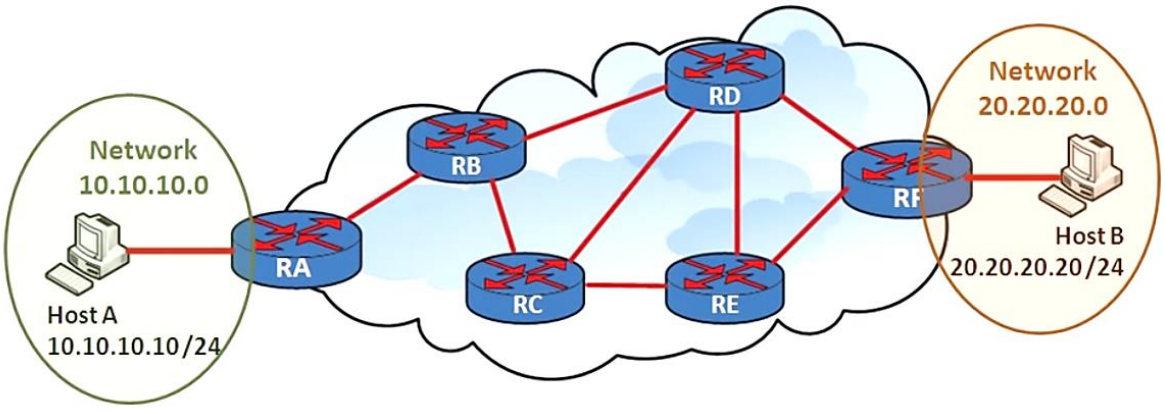
Άθροισμα ελέγχου: Το πεδίο αυτό χρησιμοποιείται για τον έλεγχο σφαλμάτων κατά την μετάδοση του πακέτου.

Ένδειξη τιμής (ID): Η τιμή ID του πακέτου, η οποία επιστρέφεται στον υπολογιστή που δημιούργησε το πακέτο στην περίπτωση που έχουμε απάντηση ECHO REPLY.

Ακολουθία: Αυτό το πεδίο περιέχει την τιμή σειράς του πακέτου και επιστρέφεται στον υπολογιστή που δημιούργησε το πακέτο στην περίπτωση που έχουμε απάντηση ECHO REPLY.

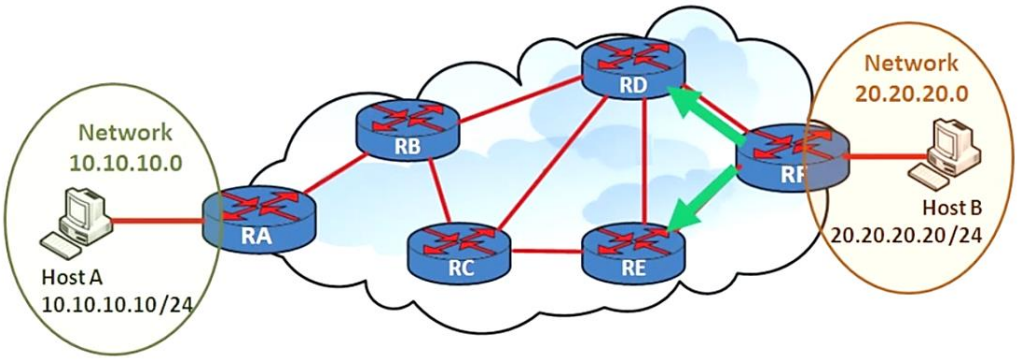
2.7.7 Πρωτόκολλα δρομολόγησης (routing protocols)

Γενικά οι δρομολογητές χρειάζονται πρωτόκολλά δρομολόγησης (routing protocols) για να δρομολογήσουν τα πακέτα δεδομένων από ένα δίκτυο σε ένα άλλο. Τα πρωτόκολλα δρομολόγησης αναλαμβάνουν την εύρεση και την επιλογή της βέλτιστης διαδρομής σε δίκτυα προορισμού. Για να επιτευχθεί αυτό εφαρμόζονται κατάλληλοι **αλγορίθμοι δρομολόγησης (routing algorithms)**. Αυτό που αναλαμβάνει να κάνει ένας αλγόριθμος δρομολόγησης είναι η δημιουργία ενός αριθμού ο οποίος ο ονομάζετε **τιμή κόστους (metric)**, για κάθε διαδρομή στο δίκτυο. Η διαδρομή η οποία διαθέτει το μικρότερο δυνατό κόστος για τον ίδιο προορισμό καταχωρείται στον πίνακα δρομολόγησης. Ανάλογα με την υλοποίηση, ως κόστος μπορεί να χρησιμοποιηθεί ο αριθμός των δρομολογητών (hop count) που περνά το μήνυμα μέχρι να φτάσει στον προορισμό του, το εύρος ζώνης της γραμμής (bandwidth), η καθυστέρηση (delay), το φορτίο της γραμμής (load) και μια σειρά άλλων παραμέτρων ή ένας συνδυασμός από αυτές.
Για παράδειγμα ας δούμε την εικόνα 2.45. Για να μπορέσουν οι δρομολογητές (routers) RF, RD και RB να ανταλλάξουν πακέτα με το δίκτυο LAN 10.10.10.0 απαιτείται η χρήση ενός αλγορίθμου δρομολόγησης.



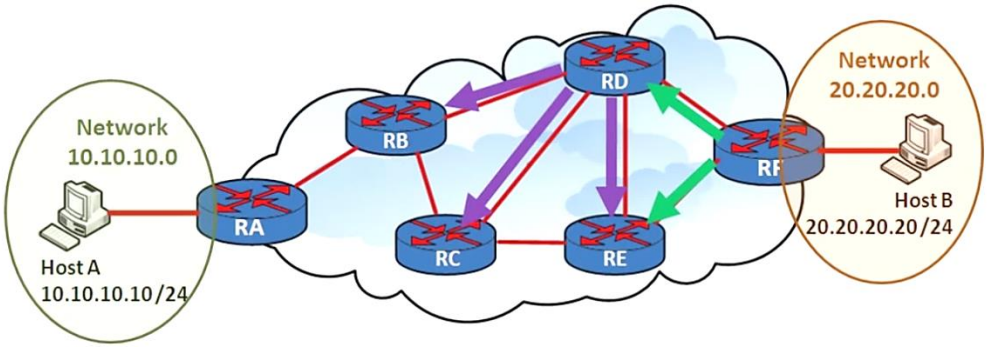
Εικόνα 2.45. Τοπολογία δικτύου με δύο διασυνδεδεμένα υποδίκτυα

Ο δρομολογητής RF στο παράδειγμα μας γνωρίζει πώς να δρομολογήσει τα πακέτα στο LAN δίκτυο με network IP 20.20.20.0 διότι συνδέεται άμεσα με αυτό. Με την εφαρμογή των δυναμικών πρωτόκολλων δρομολόγησης (dynamic routing protocols) ο router RF θα επικοινωνήσει με τον router RD και RE για τα routing updates (δηλαδή για να τους ενημερώσει ότι γνωρίζει την διαδρομή για το LAN δίκτυο με network IP 20.20.20.0).



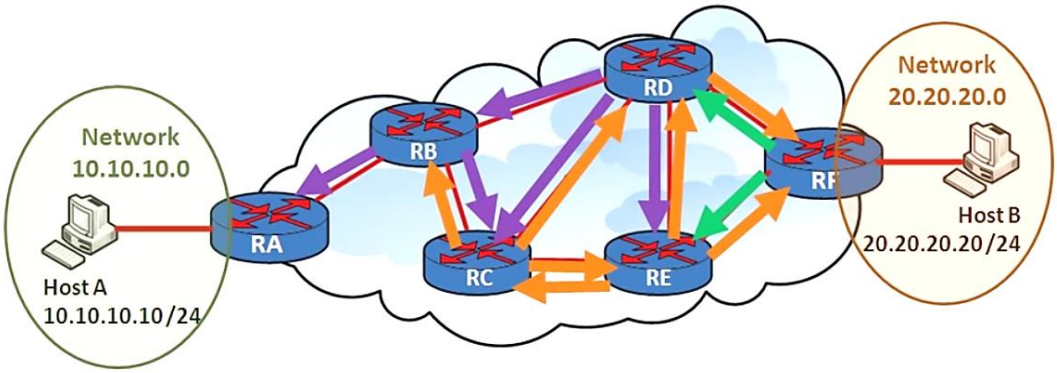
Εικόνα 2.46. Διαδικασία ενημέρωσης γειτονικών δρομολογητών του RF

Όταν λάβουν αυτά τα updates οι δρομολογητές RD και RE με την σειρά τους θα επικοινωνήσουν με τους αμέσους επόμενους γειτονικούς τους κόμβους για να τους ενημερώσουν ότι γνωρίζουν την διαδρομή για τον router RF που με την σειρά του ο ίδιος (δηλαδή ο RF) γνωρίζει την διαδρομή για το LAN δίκτυο με network IP 20.20.20.0.



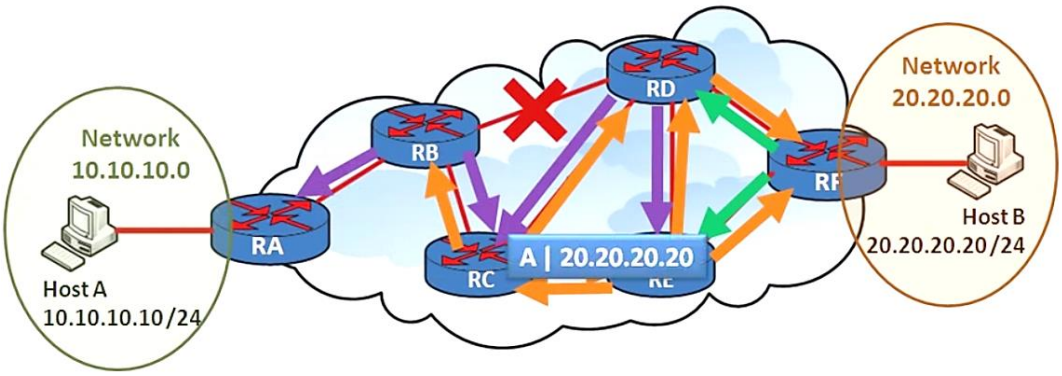
Εικόνα 2.47. Διαδικασία ενημέρωσης γειτονικών δρομολογητών του RD

Όταν λοιπόν με την σειρά του ο RB και ο RC λάβουν αυτό το update θα ακολουθήσουν την ίδια ακριβώς διαδικασία με αυτήν που αναφέραμε παραπάνω.



Εικόνα 2.48. Διαδικασία ενημέρωσης των υπολοίπων δρομολογητών του δικτύου

Στην ουσία κάθε δρομολογητής στέλνει routing updates στους άμεσα επόμενους γειτονικούς του. Αυτό είναι απαραίτητο για να εξερευνηθούν όλες οι πιθανές διαδρομές που διαθέτει ένα δίκτυο. Έστω ότι ο host A θέλει να στείλει ένα πακέτο στον host B και επιλέγεται η διαδρομή RA, RB, RD, RF διότι μπορεί να είναι αυτή με το μικρότερο κόστος. Αν για κάποιο λόγο η διαδρομή αυτή αποτύχει για κάποιον άγνωστο λόγο τότε θα στείλει αυτό το πακέτο από κάποια άλλη διαδρομή που στην περίπτωση μας για το παράδειγμα αυτό είναι η RA, RB, RC, RE, RF.



Εικόνα 2.49. Διαδικασία ενημέρωσης των υπολοίπων δρομολογητών του δικτύου

Σε αυτό το σημείο και αφού κάναμε μια μικρή εισαγωγή στην λειτουργία των δυναμικών πρωτοκόλλων δρομολόγησης ας δούμε τις κατηγορίες αυτών. Ο πρώτος τρόπος για να κατηγοριοποιήσουμε τους δυναμικούς αλγορίθμους δρομολόγησης βασίζεται στην απόδοση των λειτουργιών τους. Υπάρχουν δύο τύποι δυναμικών αλγορίθμων δρομολόγησης αυτές απεικονίζονται στον παρακάτω πίνακα.

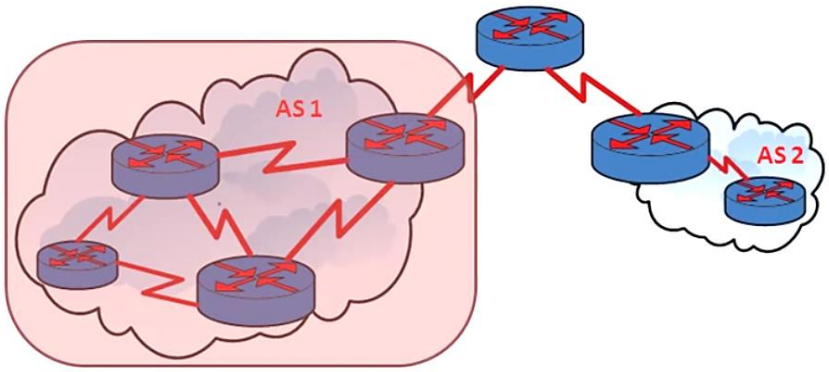
Βασισμένες κατηγορίες	Κατηγορία 1η	Κατηγορία 2η
Domain of operation	Interior (RIP, OSPF κλπ)	Exterior (BGP)
Routing Operation	Distance Vector (RIP, EIGRP)	Link State (OSPF)
IP Address Handling	Classful (RIP)	Classless (OSPF, EIGRP)

Πίνακας 2.5. Διαχωρισμός πρωτοκόλλων δρομολόγησης

Τα Interior gateway protocols λειτουργούν στα πλαίσια αυτόνομων συστημάτων (autonomous system).

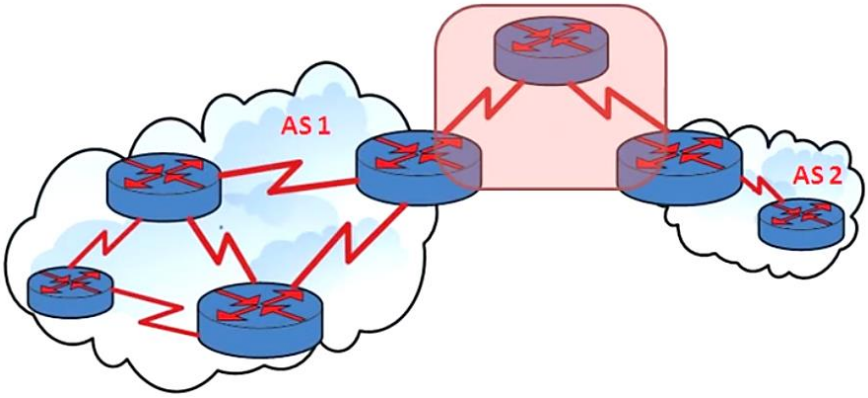
Εδώ τίθεται ένα ερώτημα τι είναι ένα αυτόνομο σύστημα ;

Με βάση απ' την οπτική της εταιρίας Cisco ένα αυτόνομο σύστημα είναι μια ομάδα από δρομολογητές (group of routers) που μπορεί να είναι σε μια εταιρία, σε έναν ISP κλπ. Οπότε το IGP λειτουργεί σε μόνο σε αυτό το domain.



Εικόνα 2.50. Domain operation του IGP

Ενώ το Exterior Gateway Protocol – EGP αναλαμβάνει την διασύνδεση δύο ή περισσοτέρων αυτόνομων συστημάτων. Δεν ασχολούνται με την δρομολόγηση που γίνεται στα αυτόνομα συστήματα. Βασικό τους καθήκον είναι να λάβουν την κίνηση πακέτων (traffic packet) από τα αυτόνομα συστήματα και να την δρομολογήσουν σε κάποιο άλλο αυτόνομο σύστημα το οποίο μπορεί να είναι κάποιος άλλος Internet Service Provider – ISP κλπ. Το πρωτόκολλο δρομολόγησης γι' αυτά είναι το BGP.



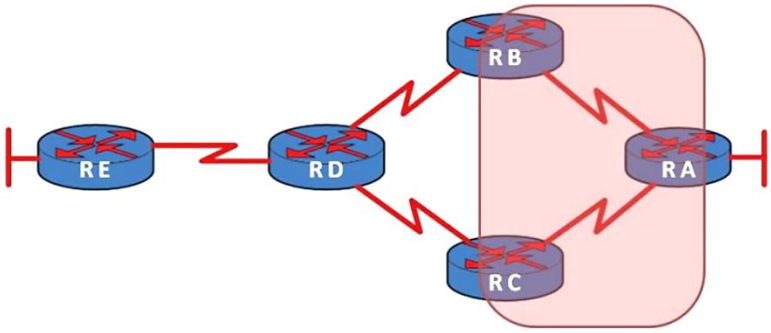
Εικόνα 2.51. Domain operation του EGP

Στην κατηγορία του routing operation υπάρχουν δύο τύποι οι οποίοι είναι οι αλγόριθμοι διανύσματος απόστασης (distance vector) και οι αλγόριθμοι κατάστασης της σύνδεσης (link state). Θα αναφερθούμε σε αυτά παρακάτω με περισσότερη λεπτομέρεια.

Η τελευταία κατηγορία στην οποία μπορούμε να κατατάξουμε τα διάφορα πρωτόκολλα δρομολόγησης είναι το IP Address handling όπου έχουμε τα classfull και τα classless.
Τα classfull πρωτόκολλα δρομολόγησης δεν υποστηρίζουν IP διευθύνσεις με CIDR πρόθεμα. Δηλαδή δεν υποστηρίζει διευθύνσεις με subnet masks διαφορετικές από αυτές που υποστηρίζουν οι κλάσεις διευθύνσεων IP. Ένα πρωτόκολλο δρομολόγησης που ανήκει σε αυτήν την κατηγορία είναι το RIP.
Τα classless πρωτόκολλα δρομολόγησης μπορούν να υποστηρίξουν δυνατότητες VLSM (Variable Length Subnet Masks). Δηλαδή υποστηρίζουν IP διευθύνσεις με CIDR πρόθεμα. Τα classless πρωτόκολλα δρομολόγησης είναι πιο αποδοτικά διότι με αυτά αποφεύγουμε την ανώφελη σπατάλη IP διευθύνσεων. Σε αυτό το σημείο ας αναλύσουμε τα distance vector protocols και τα link state protocols.

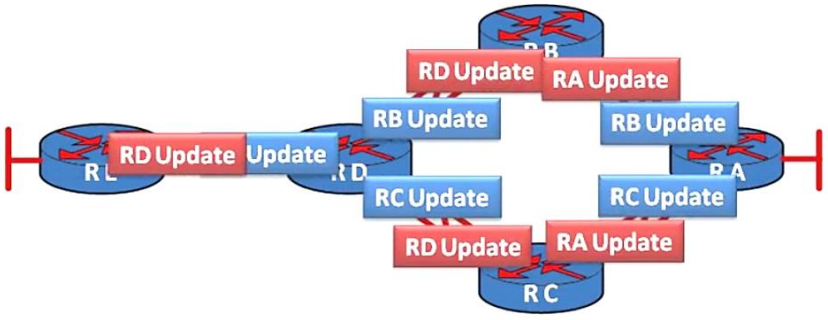
1. Αλγόριθμοι διανύσματος απόστασης (Distance Vector)

Τα πρωτόκολλα δρομολόγησης διανύσματος απόστασης είναι πρώτη γενιά πρωτοκόλλων δρομολόγησης. Είναι πιο απλά και δεν είναι σχεδιασμένα για τα σημερινά δεδομένα όπου έχουμε σύνθετες τοπολογίες δικτύων. Παρόλα αυτά χρησιμοποιούνται ακόμη και σήμερα για απλές τοπολογίες δικτύων. Τα πρωτόκολλα διανύσματος απόστασης έχουν περιορισμένη έκταση στον σχεδιασμό τοπολογιών. Αυτό σημαίνει ότι τα πρωτόκολλα που είναι distance vector (όπως το RIP) λειτουργούν έτσι ώστε οι routers να έχουν γνώση για τους κόμβους που είναι άμεσα συνδεδεμένοι μεταξύ τους. Για παράδειγμα ας δούμε την εικόνα 2.52 όπου ο δρομολογητής RA μπορεί να γνωρίζει μόνο για τους αντίστοιχους δρομολογητές RB και RC. Για τον RD και τον RE δεν είναι σε θέση να γνωρίζει κάτι γι αυτούς καθότι δεν είναι άμεσα συνδεδεμένοι.



Εικόνα 2.52. Τοπολογία δικτύου με πέντε δρομολογητές

Την ίδια ακριβώς λειτουργία επιτελεί κάθε δρομολογητής στην τοπολογία αυτή ή γενικά σε οποιαδήποτε τοπολογία που χρησιμοποιούνται πρωτόκολλα δρομολόγησης διανύσματος απόστασης (distance vector protocols). Αυτό βέβαια αποτελεί πρόβλημα διότι μπορεί να υπάρχουν πιθανά routing loops με βάση βέβαια τον σχεδιασμό της τοπολογία και οι δρομολογητές δεν θα είναι σε θέση να το γνωρίζουν. Για παράδειγμα στο δίκτυο της εικόνας ο RA δεν είναι σε θέση να γνωρίζει την έξοδο στην οποία συνδέεται ο RB ή ο RC.
Οι δρομολογητές που εκτελούν πρωτόκολλα τύπου distance vector στέλνουν κάθε 30 δευτερόλεπτα ενημερώσεις (updates) μεταξύ τους για να ενημερώσει έκαστος τον πίνακα δρομολόγησης του. Ας υποθέσουμε για παράδειγμα ότι έχει εφαρμοστεί το πρωτόκολλο RIP σε ένα δίκτυο (που όπως είπαμε το RIP είναι distance vector). Οι ενημερώσεις σχετικά με την δρομολόγηση θα στέλνονται από τους δρομολογητές κάθε 30 δευτερόλεπτα. Κάθε τέτοια ενημέρωση θα πρέπει να επεξεργαστεί από τον δρομολογητή κάτι που συνεισφέρει σε υψηλό overhead και υψηλή επεξεργαστική ισχύ καθώς και σε μεγάλη κατανάλωση του εύρους ζώνης.



Εικόνα 2.53. Διαδικασία διαμοιρασμού routing updates μεταξύ των γειτονικών δρομολογιτών

Τέλος τα πρωτόκολλα δρομολόγησης distance vector χρησιμοποιούν classfull IP διευθύνσεις. Δηλαδή δεν υποστηρίζουν IP διευθύνσεις με CIDR πρόθεμα.

2. Routing Information Protocol – RIP

Το πρωτόκολλο RIP χρησιμοποιεί τον αλγόριθμο διανύσματος απόστασης και είναι ένα κατάλληλο πρωτόκολλο για τη λειτουργία μικρών δικτύων. Στους πίνακες δρομολόγησης που προκύπτουν υπάρχουν πληροφορίες για το δρόμο και το κόστος της κάθε απόστασης μέχρι τον τελικό προορισμό. Με τον όρο κόστος αναφερόμαστε στον αριθμό των ενδιάμεσων δρομολογητών μέχρι να φτάσουμε στον τελικό προορισμό (hop count). Ο αριθμός των ενδιάμεσων δρομολογητών μέχρι το δίκτυο προορισμού μπορεί να είναι μέχρι 15. Στο πρωτόκολλο RIP οι δρομολογητές περιοδικά (συνήθως κάθε 30 δευτερόλεπτα), ανακοινώνουν ολόκληρο το περιεχόμενο του πίνακα δρομολόγησής τους, στους άμεσα γειτονικούς δρομολογητές. Ο πίνακας δρομολόγησης μπορεί να μεταδοθεί κι όταν υπάρξει κάποια αλλαγή στην τοπολογία του δικτύου. Έτσι επιτρέπεται στον κάθε δρομολογητή να βλέπει το δίκτυο του γειτονικού δρομολογητή και να προσθέτει το ανάλογο κόστος στην απόσταση που έχει ήδη προσθέσει ο δεύτερος. Το μειονέκτημα της προσέγγισης αυτής είναι ότι καθώς το δίκτυο μεγαλώνει, ανταλλάσσεται ένα μεγάλο ποσό πληροφορίας ανά τακτά χρονικά διαστήματα, ακόμα κι όταν η τοπολογία του δικτύου δεν έχει αλλάξει, με αποτέλεσμα να περιορίζεται το διαθέσιμο εύρος ζώνης και να αυξάνεται ο χρόνος σύγκλισης.

Με τον όρο **χρόνο σύγκλισης (convergence time)**, αναφερόμαστε στο χρόνο στον οποίο περνά μέχρι όλοι οι δρομολογητές να «συμφωνήσουν» σε κάποια περίπτωση που προκύψει μια οποιαδήποτε αλλαγή στην τοπολογία ενός δικτύου. Όταν αλλάζει η τοπολογία του δικτύου, εκτελείται ο αλγόριθμος δρομολόγησης και σταματά η κίνηση των δεδομένων που μεταφέρει ο δρομολογητής προς τις διάφορες διεπαφές (interfaces) του. Αυτό συμβαίνει διότι δεν είναι εφικτό να γνωρίζει αν το δίκτυο προορισμού είναι διαθέσιμο ή όχι. Συνεπώς, όσο πιο γρήγορα γίνεται η σύγκλιση τόσο πιο γρήγορα θα μεταφερθούν τελικά τα δεδομένα προς τον προορισμό.

Υπάρχουν δυο εκδόσεις:

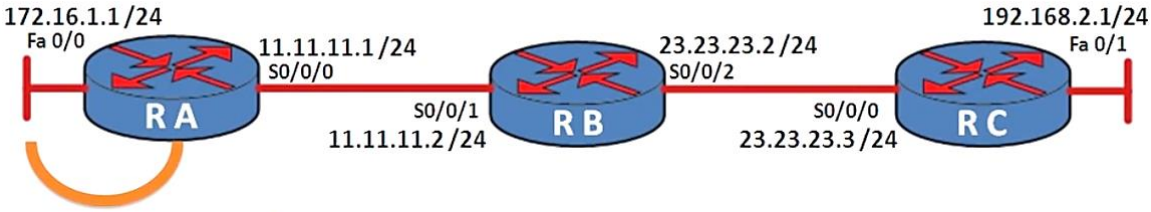
- RIP-1: Όπου είναι ένα απλό πρωτόκολλο τύπου Distance Vector
  - Αρχικοποίηση: Ο δρομολογητής στέλνει request σε κάθε διεπαφή και οι γείτονες απαντούν με όλη την πληροφορία δρομολόγησης που έχουν
  - Ενημέρωση: Περιοδικά, περίπου ανά 30’, ή όποτε γίνει κάποια αλλαγή γίνεται αναγγελία των πινάκων δρομολόγησης προς τους γείτονες. Για να αποφευχθεί κατάσταση ταλάντωσης, οι υπάρχουσες διαδρομές κρατούνται μέχρι μία καινούργια να ανακαλυφθεί με μικρότερο κόστος
  - Split horizon: Δεν γίνεται διαφήμιση μιας διαδρομής προς την κατεύθυνση από την οποία έγινε η εκμάθηση της, ώστε να αποφευχθούν βρόχοι
- RIP-2: Αφορά κάποιες βελτιώσεις στο RIPv1, όπως το VLSM, Variable Length Subnetting Mask, η αυθεντικοποίηση, η ενημέρωση με multicast μηνύματα. Γενικά δεν θεωρείται ιδιαίτερη βελτίωση σε σχέση με την πρώτη έκδοση, διότι διατηρεί τους περιορισμούς του RIP πρωτοκόλλου.

Εικόνα 2.54. Τοπολογία δικτύου με τρείς δρομολογητές

Σε αυτό το σημείο ας δούμε την δομή την οποία θα έχει ο πίνακας δρομολόγησης του δρομολογητή RA. Οι καταγραφές που θα έχει ο δρομολογητής RA θα είναι οι εξής:

Βήμα 1ο

Στην εικόνα 2.55 απεικονίζεται η πρώτη πληροφορία που θα καταχωρηθεί στο πίνακα δρομολόγησης του RA. Ο λόγος για τον οποίο το πεδίο hops έχει την τιμή μηδέν είναι διότι το πρώτο hop είναι απευθείας συνδεδεμένο στον δρομολογητή RA.



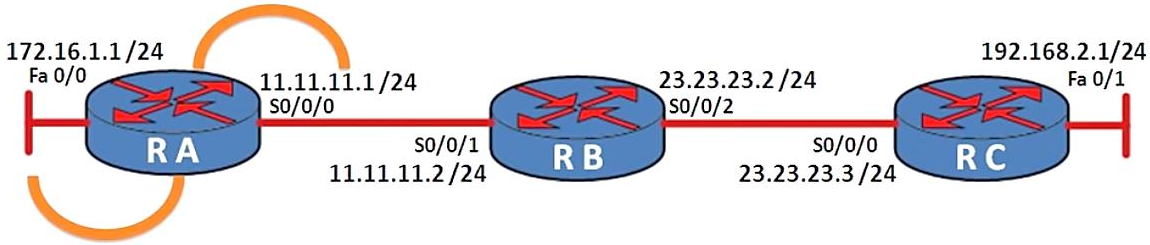
Πίνακας δρομολόγησης RA

Προορισμός	Hops	Θύρα
172.16.1.0	0	Fa0/0

Εικόνα 2.55. Η πρώτη πληροφορία που θα καταχωρηθεί στον πίνακα δρομολόγησης του RA

Βήμα 2ο

Στην εικόνα 2.56 απεικονίζεται η δεύτερη πληροφορία που θα καταχωρηθεί στο πίνακα δρομολόγησης του RA. Ο λόγος για τον οποίο το πεδίο hops έχει την τιμή μηδέν είναι ότι κι εδώ το δεύτερο hop είναι απευθείας συνδεδεμένο στον δρομολογητή RA.



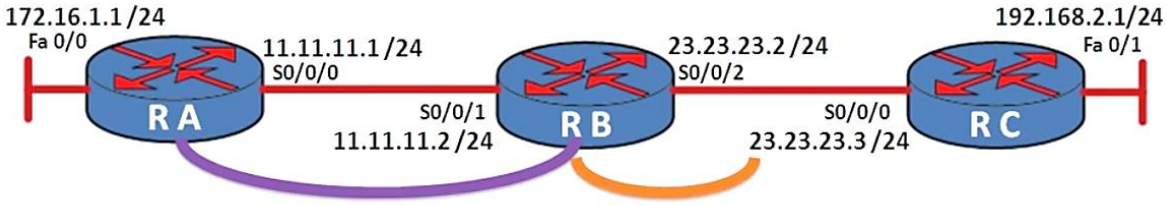
Πίνακας δρομολόγησης RA

Προορισμός	Hops	Θύρα
172.16.1.0	0	Fa0/0
11.11.11.0	0	S0/0/0

Εικόνα 2.56. Η δεύτερη πληροφορία που θα καταχωρηθεί στον πίνακα δρομολόγησης του RA

Βήμα 3ο

Στην εικόνα 2.57 απεικονίζεται η τρίτη πληροφορία που θα καταχωρηθεί στο πίνακα δρομολόγησης του δρομολογητή RA. Ο λόγος για τον οποίο το πεδίο hops έχει την τιμή 1 είναι διότι πρέπει το πακέτο να περάσει από τον δρομολογητή RB προκειμένου να φτάσει στον προορισμό του που είναι η θύρα S0/0/0.



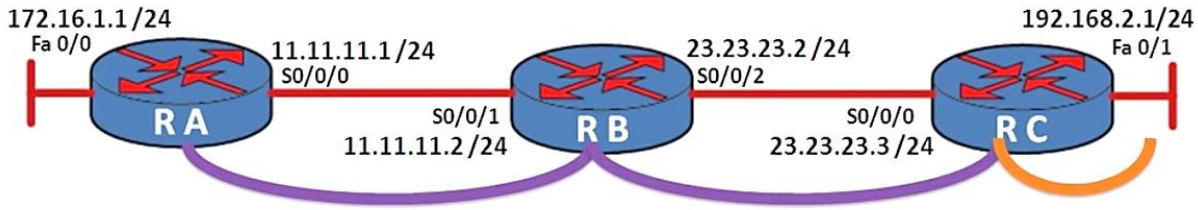
Πίνακας δρομολόγησης RA

Προορισμός	Hops	Θύρα
172.16.1.0	0	Fa0/0
11.11.11.0	0	S0/0/0
23.23.23.0	1	S0/0/0

Εικόνα 2.57. Η τρίτη πληροφορία που θα καταχωρηθεί στον πίνακα δρομολόγησης του RA

Βήμα 4ο

Τέλος το τελευταίο δίκτυο με το οποίο θα κάνει ενημέρωση ο RA στον πίνακα δρομολόγησης του θα είναι το 192.168.2.0 το οποίο είναι άμεσα συνδεδεμένο με τον δρομολογητή RC. Το πεδίο hops θα πάρει την τιμή 2 διότι θα εμπλακούν δύο ενδιάμεσοι δρομολογητές προκειμένου να φτάσει το πακέτο στον τελικό προορισμό του. Αυτοί οι δύο δρομολογητές στο παράδειγμα μας είναι οι RB και RC.



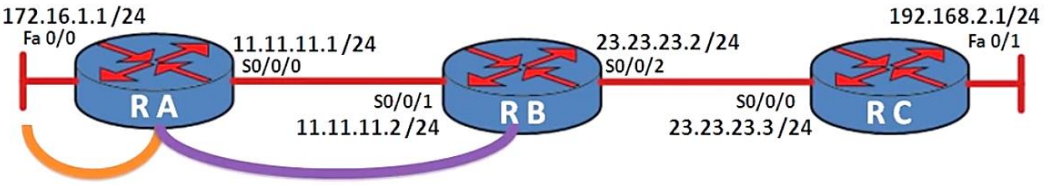
Πίνακας δρομολόγησης RA

Προορισμός	Hops	Θύρα
172.16.1.0	0	Fa0/0
11.11.11.0	0	S0/0/0
23.23.23.0	1	S0/0/0
192.168.2.0	2	S0/0/0

Εικόνα 2.58. Η τέταρτη πληροφορία που θα καταχωρηθεί στον πίνακα δρομολόγησης του RA

Σε αυτό το σημείο ολοκληρώθηκε η δομή του πίνακα δρομολόγησης του RA Με την ίδια φιλοσοφία μπορούμε να σχεδιάσουμε επίσης την δομή του πίνακα δρομολόγησης που θα έχει ο δρομολογητής RB. Ας δούμε την δομή του παρακάτω.

Βήμα 1ο
Όπως δείχνει η εικόνα 2.59 για τα δίκτυα 172.16.1.0 ο αριθμός των hops θα είναι 1 διότι αυτό το δίκτυο είναι συνδεδεμένο με τον δρομολογητή RA οπότε το πακέτο θα πρέπει να περάσει από τον ίδιο προκειμένου να φτάσει στο δίκτυο με network IP 172.16.1.0. Στο πεδίο θύρα θα πάρει την τιμή θύρας του δρομολογητή που έχει αυτόν τον πίνακα δρομολόγησης. Δηλαδή στο παράδειγμα μας θα καταχωρίσει στον πίνακα δρομολόγησης τον αριθμό θύρας εξόδου του RB που εδώ είναι η S0/0/1.

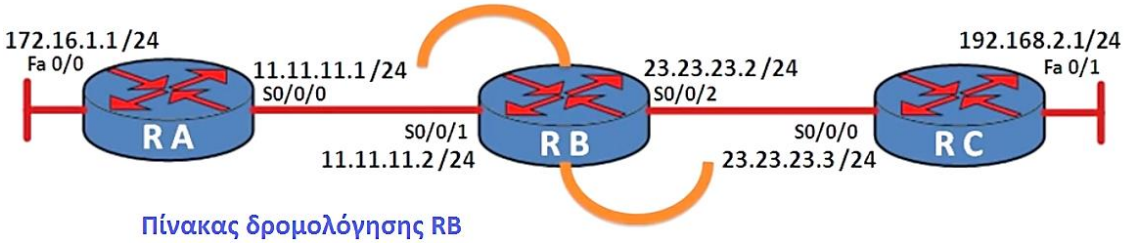


Πίνακας δρομολόγησης RB

Προορισμός	Hops	Θύρα
172.16.1.0	1	S0/0/1

Εικόνα 2.59. Η πρώτη πληροφορία που θα καταχωρηθεί στον πίνακα δρομολόγησης του RB

Βήμα 2ο
Όπως δείχνει η εικόνα για τα δίκτυα με network IP 11.11.11.0 και 23.23.23.0 ο αριθμός των hops θα είναι 0 διότι αυτό το δίκτυο είναι απευθείας συνδεδεμένο με τον δρομολογητή RB οπότε το πακέτο δεν θα περάσει από κάποιον ενδιάμεσο δρομολογητή. Στο πεδίο θύρα θα πάρει την τιμή θύρας του δρομολογητή που έχει αυτόν τον πίνακα δρομολόγησης. Δηλαδή στο παράδειγμα μας θα καταχωρίσει στον πίνακα δρομολόγησης τον αριθμό θύρας εξόδου του RB. Για το δίκτυο με network IP 11.11.11.0 η θύρα εξόδου από τον RB θα είναι η S0/0/1 ενώ για το δίκτυο με network IP 23.23.23.0 θα είναι η S0/0/2.

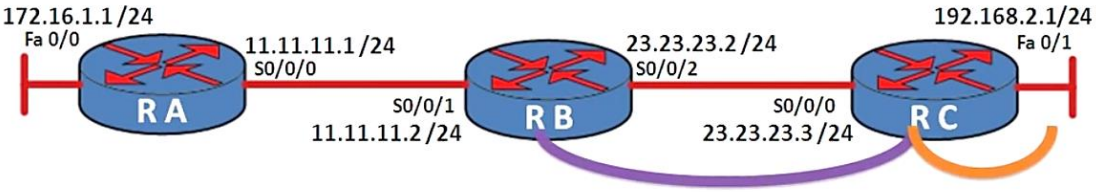


Πίνακας δρομολόγησης RB

Προορισμός	Hops	Θύρα
172.16.1.0	1	S0/0/1
11.11.11.0	0	S0/0/0
23.23.23.0	0	S0/0/2

Εικόνα 2.60.Η δεύτερη και η τρίτη πληροφορία που θα καταχωρηθεί στον πίνακα δρομολόγησης του RB

Βήμα 3ο
Όπως δείχνει η εικόνα 2.61 για το δίκτυο με network IP 192.168.2.1 ο αριθμός των hops θα είναι 1 θα είναι 1 διότι αυτό το δίκτυο είναι συνδεδεμένο με τον δρομολογητή RC οπότε το πακέτο θα πρέπει να περάσει από τον ίδιο προκειμένου να φτάσει στο δίκτυο με network IP 192.168.2.1. Στο πεδίο θύρα θα πάρει την τιμή θύρας του δρομολογητή που έχει αυτόν τον πίνακα δρομολόγησης. Δηλαδή στο παράδειγμα μας θα καταχωρίσει στον πίνακα δρομολόγησης τον αριθμό θύρας εξόδου του RB που εδώ είναι η S0/0/2.



Πίνακας δρομολόγησης RB

Προορισμός	Hops	Θύρα
172.16.1.0	1	S0/0/1
11.11.11.0	0	S0/0/0
23.23.23.0	0	S0/0/2
192.168.2.0	1	S0/0/2

Εικόνα 2.61. Η τέταρτη πληροφορία που θα καταχωρηθεί στον πίνακα δρομολόγησης του RB

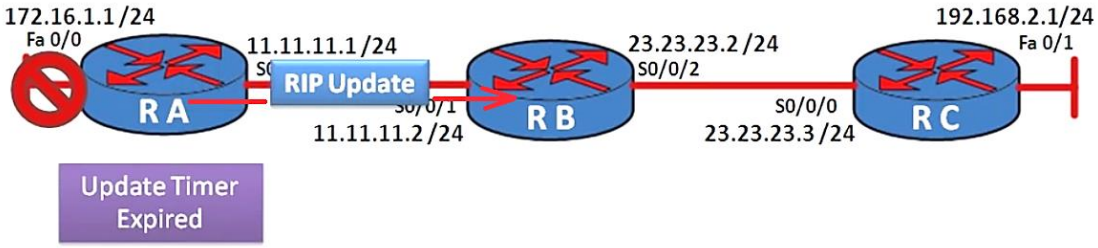
Με αυτόν τον τρόπο πραγματοποιούνται οι καταχωρίσεις στους πίνακες δρομολόγησης με το πρωτόκολλο RIP. Σε αυτό το σημείο ας δούμε με ποίον τρόπο το πρωτόκολλο δρομολόγησης RIP ενημερώνει ή διορθώνει τους πίνακες δρομολόγησης. Για να μπορέσουμε να κατανοήσουμε καλύτερα πως πραγματοποιείται αυτό θα βασιστούμε στην ίδια τοπολογία δικτύου με την παραπάνω που εξηγούσαμε τις καταχωρίσεις στους πίνακες δρομολόγησης.

Πίνακας δρομολόγησης RA

Προορισμός	Hops	Θύρα
172.16.1.0	X	Fa0/0
11.11.11.0	0	S0/0/0
23.23.23.0	1	S0/0/0
192.168.2.0	2	S0/0/0

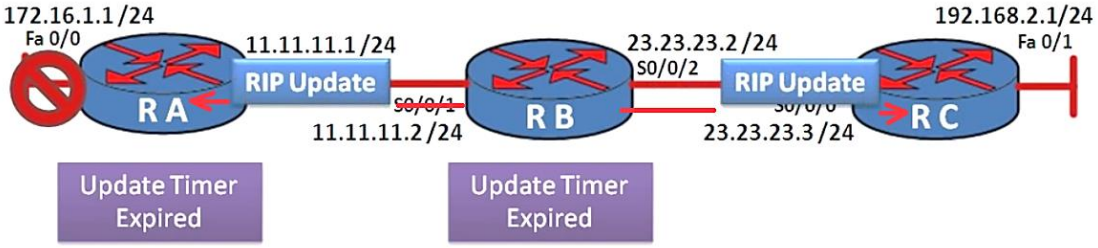
Εικόνα 2.62. Σφάλμα λειτουργίας στο υποδίκτυο με network IP 172.16.1.0

Ας υποθέσουμε στο δίκτυο της εικόνας 2.62 ότι για κάποιον λόγο η θύρα Fa0/0 αποτύχει για κάποιον λόγο ή αυτό το δίκτυο τεθεί εκτός λειτουργίας ο δρομολογητής RA θα μαρκάρει στον πίνακα δρομολόγησης το δίκτυο αυτό ως απρόσιτο (unreachable) στον πίνακα δρομολόγησης του αλλά δεν θα ενημερώσει τον δρομολογητή RB κατευθείαν γι αυτό το συμβάν. Σε αυτό το σημείο ο δρομολογητής RA θα πρέπει να περιμένει έως ότου αρχίσουν οι ενημερώσεις μεταξύ τους που εδώ ονομάζονται RIP ενημερώσεις (RIP updates). Η εικόνα δείχνει ένα παράδειγμα όπου ο δρομολογητής RA θα στείλει το δικό του RIP update για να ενημερώσει τον δρομολογητή RB αφού λήξει το update timer.



Εικόνα 2.63. Διαδικασία αποστολής RIP update από τον δρομολογητή RA προς τον RB

Στο σημείο αυτό όταν το RIP update που στάλθηκε από τον RA προς τον RB φτάσει στον δεύτερο τότε ο RB θα καταχωρίσει κι αυτός με την σειρά του στον πίνακα δρομολόγησης του ότι το δίκτυο με network IP 172.16.1.0 είναι unreachable. Στην συνέχεια θα περιμένει κι αυτός με την σειρά του για την λήξη του update timer ώστε να στείλει τα δικά του RIP updates στους δρομολογητές RA και RC.



Πίνακας δρομολόγησης RB

Προορισμός	Hops	Θύρα
172.16.1.0	X	S0/0/1
11.11.11.0	0	S0/0/1
23.23.23.0	0	S0/0/2
192.168.2.0	1	S0/0/2

Εικόνα 2.64. Διαδικασία αποστολής RIP update από τον δρομολογητή RB προς τους γειτονινκούς του RA και RC

Αυτό το φαινόμενο αποτελεί μείζον πρόβλημα στην διόρθωση σφαλμάτων ανάμεσα στους πίνακες δρομολόγησης των διαφόρων δρομολογητών που μπορεί να υπάρχουν σε ένα δίκτυο και επίσης στις δυνατότητες των δρομολογητών να επιτελέσουν τις διάφορες λειτουργίες τους όπως για παράδειγμα την δρομολόγηση των πακέτων.

Βέβαια σε πραγματικά δεδομένα οι πιθανότητες να αντιμετωπίσουμε τέτοια σφάλματα όπως αυτό που δείξαμε προηγουμένως είναι σχεδόν απίθανα.
Ας δούμε σε αυτό το σημείο ας πάμε ξανά στο παράδειγμα μας. Ας υποθέσουμε ότι ο δρομολογητής RA χάνει για κάποιο λόγο την σύνδεση με το δίκτυο που έχει network IP 172.16.1.0 και ενημερώνει τον πίνακα δρομολόγησης του ότι το δίκτυο αυτό είναι απλησίαστο (unreachable). Όπως είχαμε αναφέρει παραπάνω ο δρομολογητής RA θα πρέπει να περιμένει ένα συγκεκριμένο χρονικό διάστημα (30 δευτερόλεπτα) για να ενημερώσει με την σειρά του τον δρομολογητή RB ότι το δίκτυο με network IP 172.16.1.0 δεν είναι διαθέσιμο και ότι αυτή η σύνδεση δεν ισχύει πια. Έστω ότι ο δρομολογητής RA έχει εναπομένων χρόνο 20 δευτερολέπτων για την λήξη του δικού του update time expire και ότι ο RB έχει με την σειρά του έχει επίσης 5 δευτερόλεπτα για την λήξη του δικού του update timer. Αφού περάσουν τα 5 δευτερόλεπτα για την λήξη του update timer του RB με την σειρά του ο ίδιος θα στείλει στους δρομολογητές RA και RC τον δικό του πίνακα δρομολόγησης.

Πίνακας δρομολόγησης RA

Προορισμός	Hops	Θύρα
172.16.1.0	X	Fa0/0
11.11.11.0	0	S0/0/0
23.23.23.0	1	S0/0/0
192.168.2.0	2	S0/0/0

Πίνακας δρομολόγησης RB

Προορισμός	Hops	Θύρα
172.16.1.0	1	S0/0/1
11.11.11.0	0	S0/0/1
23.23.23.0	0	S0/0/2
192.168.2.0	1	S0/0/2

Εικόνα 2.65. Update timers σε έναν δρομολογητή και πως αυτά επιρεάζουν την ενημέρωση των πινάκων δρομολόγησης

Όταν λοιπόν ο δρομολογητής RA λάβει το RIP update που του έστειλε ο RB θα ενημερώσει με την σειρά του τον πίνακα δρομολόγησης του. Όπως είχαμε αναφέρει παραπάνω ο δρομολογητής RA έχει ήδη ενημερώσει τον πίνακα δρομολόγησης του και έχει σημειώσει ότι το δίκτυο με network IP 172.16.1.0 είναι unreachable. Όμως επειδή το timer update του RB έληξε πριν από αυτό του RA ο πρώτος (δηλαδή ο RB) στέλνει με την σειρά του RIP update που περιέχει τον πίνακα δρομολόγησης του. Οπότε ο δρομολογητής RA καλείται σε αυτό το σημείο να ξαναενημερώσει τον πίνακα δρομολόγησης του. Αυτό θα έχει σαν συνέπεια να αφαιρέσει την καταχώρηση που είχε προηγούμενος για το δίκτυο με network IP 172.16.1.0. Η εικόνα δίνει μια σαφή εξήγηση για την δομή του πίνακα δρομολόγησης του RA.

Πίνακας δρομολόγησης RA

Προορισμός	Hops	Θύρα
172.16.1.0	2	S0/0/0
11.11.11.0	0	S0/0/0
23.23.23.0	1	S0/0/0
192.168.2.0	2	S0/0/0

Πίνακας δρομολόγησης RB

Προορισμός	Hops	Θύρα
172.16.1.0	1	S0/0/1
11.11.11.0	0	S0/0/1
23.23.23.0	0	S0/0/2
192.168.2.0	1	S0/0/2

Εικόνα 2.66. Update timers σε έναν δρομολογητή και πως αυτά επιρεάζουν την ενημέρωση των πινάκων δρομολόγησης

Στην εικόνα αποτυπώνεται η αλλαγή που θα γίνει στον πίνακα δρομολόγησης του RA. Ο δρομολογητής RA όταν λάβει το RIP update που περιέχει τον πίνακα δρομολόγησης του RB θα αλλάξει την καταχώρηση που είχε για το δίκτυο με network IP 172.16.1.0 που είχε θέσει ως unreachable και θα βάλει μια καινούργια καταχώρηση. Αυτό συμβαίνει διότι ο δρομολογητής RA με το που λάβει το RIP update από τον δρομολογητή RB θα έχει την εντύπωση ότι πρόκειται για μια νέα διαδρομή οπότε ενημερώνει καταλλήλως τον πίνακα δρομολόγησης του.
Στο σημείο αυτό ας αναλύσουμε τι θα συμβεί αν το update timer του δρομολογητή RA λήξει. Όταν λοιπόν περάσουν τα 20 δευτερόλεπτα του update timer του δρομολογητή RA τότε ο ίδιος με την σειρά του θα στείλει ένα RIP update προς τον RB. Όταν λάβει αυτό το RIP update ο δρομολογητής RB δεν έχει επιλογή παρά από το να ενημερώσει τον πίνακα δρομολόγησης του με την λάθος καταχώρηση που περιέχεται στον RA. Έτσι στο πεδίο Hop του πίνακα δρομολόγησης RB για το δίκτυο με network IP 172.16.1.0 θα τεθεί σε 3. Αυτή η συνεχής διαδικασία ανταλλαγής RIP μηνυμάτων μεταξύ των δρομολογητών RA και RB θα συνεχίζεται επ' άπειρον και κατά συνέπεια θα αυξάνεται επίσης επ' άπειρον και το πεδίο hops για το δίκτυο με network IP 172.16.1.0 για τους δύο πίνακες δρομολόγησης των δρομολογητών RA και RB.

Πίνακας δρομολόγησης RA

Προορισμός	Hops	Θύρα
172.16.1.0	Inf.	S0/0/0
11.11.11.0	0	S0/0/0
23.23.23.0	1	S0/0/0
192.168.2.0	2	S0/0/0

Πίνακας δρομολόγησης RB

Προορισμός	Hops	Θύρα
172.16.1.0	Inf.	S0/0/1
11.11.11.0	0	S0/0/1
23.23.23.0	0	S0/0/2
192.168.2.0	1	S0/0/2

Εικόνα 2.67. Αλλαγή του πεδίου Hop για το υποδίκτυο με network IP 172.16.1.0 σε άπειρο

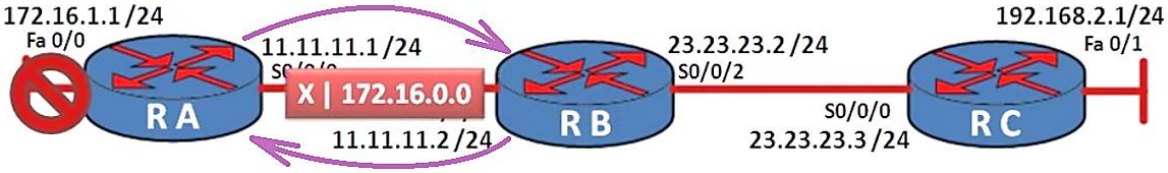
Προκειμένου να αποφευχθεί αυτό το φαινόμενο οι μηχανικοί δικτύων αποφάσισαν να τεθεί ένα maximum hop count σε διαδρομές, που αυτό είναι το 15. Αν λοιπόν συμβεί αυτό το φαινόμενο που περιγράψαμε παραπάνω τότε όταν το πεδίο hop τεθεί σε 16 ή ακόμα και αν μια διαδρομή έχει τιμή hop ίση με 16 τότε η διαδρομή θεωρείται μη προσιτή ή μη διαθέσιμη (unreachable) και κατά συνέπεια αφαιρείται από τον πίνακα δρομολόγησης.

Split Horizon

Ένα επίσης σημαντικό ζήτημα η επαναληπτική δρομολόγηση πακέτων (packet loop). Για να καταλάβουμε τι εννοούμε με αυτό ας παρατηρήσουμε το παρακάτω παράδειγμα της εικόνας. Έστω ότι κάποιος κόμβος από το υποδίκτυο 192.168.2.0 θέλει να στείλει δεδομένα προς έναν άλλο κόμβο που ανήκει στο υποδίκτυο 172.16.1.0 το οποίο όμως έχει τεθεί εκτός λειτουργίας.

Τότε το πακέτο θα περάσει από τους δρομολογητές RC και RB. Όταν φτάσει το πακέτο στον δρομολογητή RB τότε θα το στείλει προς την θύρα του S0/0/1 για να δρομολογηθεί στον RA. Όταν ο δρομολογητής RA λάβει αυτό το πακέτο θα κάνει ακριβώς την ίδια διαδικασία με αυτήν που έκανε ο RB. Δηλαδή ο RA θα εξετάσει τον πίνακα δρομολόγησης του και θα το στείλει στην outbound θύρα του δηλαδή στην S0/0/0.

Αυτό έχει σαν αποτέλεσμα το πακέτο να περιφέρεται συνέχεια από τον δρομολογητή RA προς τον RB και αντιστρόφως. Συνεπώς, δεν είναι δύσκολο να φανταστούμε ότι όλη η κίνηση των πακέτων θα κάνει μια συνεχή loop ανάμεσα στον RA και στον RB έως ότου λήξει το TTL των πακέτων. Αυτό βέβαια αποτελεί μείζον ζήτημα στην επεξεργαστική λειτουργία ενός δικτύου καθώς επίσης και στο bandwidth του.



Πίνακας δρομολόγησης RA

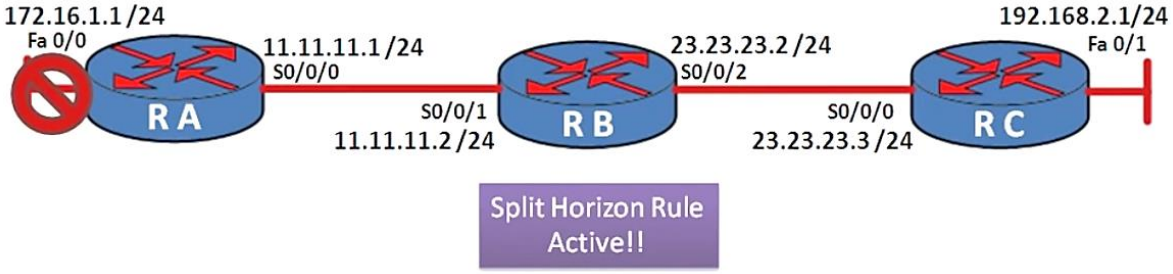
Προορισμός	Hops	Θύρα
172.16.1.0	4	S0/0/0
11.11.11.0	0	S0/0/0
23.23.23.0	1	S0/0/0
192.168.2.0	2	S0/0/0

Πίνακας δρομολόγησης RB

Προορισμός	Hops	Θύρα
172.16.1.0	5	S0/0/1
11.11.11.0	0	S0/0/1
23.23.23.0	0	S0/0/2
192.168.2.0	1	S0/0/2

Εικόνα 2.68. Συνεχείς ανταλλαγή του πακέτου από τον RA προς τον RB και αντιστρόφως

Οπότε εδώ λύνει το πρόβλημα ο κανόνας split horizon όπου σύμφωνα με τον οποίο ορίζεται ότι ποτέ δεν είναι χρήσιμο να σταλθεί κάποια πληροφορία σχετικά με ένα δίκτυο πίσω στην θύρα από την οποία προήλθε. Ας παρατηρήσουμε την εικόνα όπου το δίκτυο με network IP 172.16.1.0 αποτυγχάνει στην σύνδεση για κάποιον λόγο και ο δρομολογητής RA χάνει την διαδρομή του γι' αυτό το δίκτυο. Με τον κανόνα του split horizon ο δρομολογητής RB δεν θα στείλει στον RA κάποιο RIP update αλλά θα ενημερώσει τον RA ότι γνωρίζει την διαδρομή για το δίκτυο με network IP 172.16.1.0 από τον ίδιο τον δρομολογητή RA.



Πίνακας δρομολόγησης RA

Προορισμός	Hops	Θύρα
172.16.1.0	X	Fa0/1
11.11.11.0	0	S0/0/0
23.23.23.0	1	S0/0/0
192.168.2.0	2	S0/0/0

Πίνακας δρομολόγησης RB

Προορισμός	Hops	Θύρα
172.16.1.0	1	S0/0/1
11.11.11.0	0	S0/0/1
23.23.23.0	0	S0/0/2
192.168.2.0	1	S0/0/2

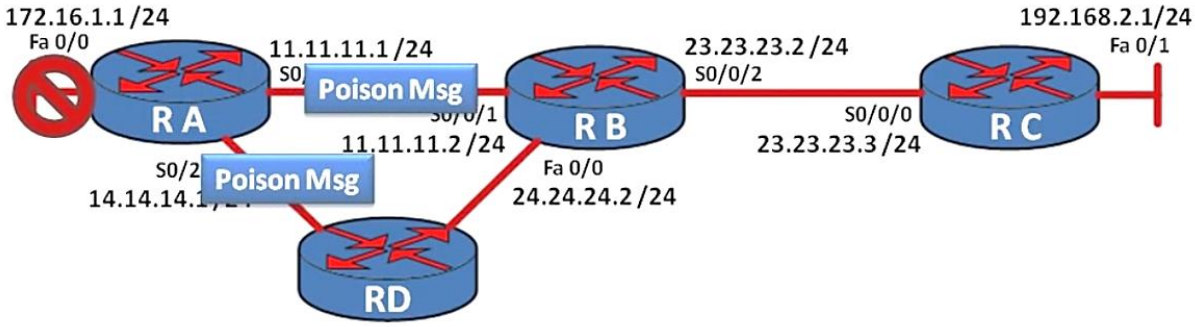
Εικόνα 2.69. Εφαρμογή κανόνα split Horizon

Δηλαδή ο RB θα έρθει σε επικοινωνία με τον RA για να του πει ότι «εγώ σαν RB έχω ακόμα την καταχώρηση που μου έδωσες για το δίκτυο με network IP 172.16.1.0 στον πίνακα δρομολόγησης μου και είμαι σε θέση να στη στείλω». Με αυτόν τον κανόνα μπορούμε να αποφύγουμε το παραπάνω πρόβλημα που είχαμε αναφέρει. Βέβαια ο

κανόνας split horizon μπορεί να εφαρμοστεί μόνο σε μικρά δίκτυα. Σε πιο σύνθετες δικτυακές τοπολογίες αποτυγχάνει παταγωδώς.

Route poisoning

Όπως είχαμε αναφέρει προηγουμένως ο κανόνας split horizon αποτυγχάνει να εφαρμοστεί σε μεγάλα δίκτυα. Το κενό αυτό έρχεται να καλύψει το route poisoning. Ας πάρουμε για παράδειγμα το δίκτυο της εικόνας 2.70 όπου κι εδώ το δίκτυο με network IP 172.16.1.0 έχει αποτύχει για κάποιο λόγο στην επικοινωνία του με τον δρομολογητή RA.



Πίνακας δρομολόγησης RA

Προορισμός	Hops	Θύρα
172.16.1.0	X	Fa0/1
11.11.11.0	0	S0/0/0
23.23.23.0	1	S0/0/0
192.168.2.0	2	S0/0/0

Εικόνα 2.70. Διαδικασία αποστολής poison μηνυμάτων από τον RA προς τους γειτονικούς του RB και RD

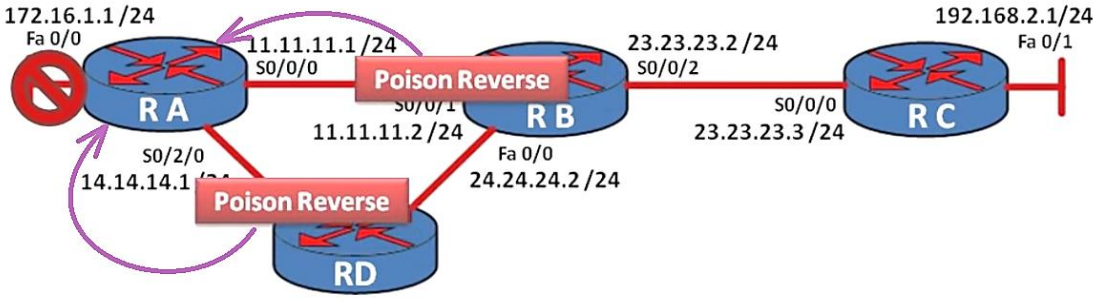
Όπως βλέπουμε και από την εικόνα 2.70 σε αυτήν την περίπτωση ο δρομολογητής RA θα στείλει μηνύματα poison στους RB και RD που είναι άμεσα συνδεδεμένοι με τον ίδιο για να τους ενημερώσει ότι το δίκτυο με network IP 172.16.1.0 έχει hop count 16 (δηλαδή ότι είναι άπειρο). Αφού λάβουν αυτά τα μηνύματα επιτυχώς οι δρομολογητές RB και RD θα κάνουν τα εξής:

- Θα σημειώσουν στους πίνακες δρομολόγησης τους ότι το δίκτυο με network IP 172.16.1.0 είναι πιθανών εκτός λειτουργίας διότι μπορεί να υπάρχει κάποιο άλλο μονοπάτι προς αυτό

- Μετά από αυτό θα στείλουν και οι δύο μηνύματα poison reverse στον δρομολογητή RA για να τον ενημερώσουν ότι έλαβαν το δικό του μήνυμα poison και ότι σημείωσαν ότι το δίκτυο με network IP 172.16.1.0 ως πιθανών εκτός λειτουργίας. Στην ουσία δεν πρόκειται άλλο παρά για επιβεβαιωτικά μηνύματα.

- Τέλος αφού το κάνουν οι RB και RD θα στείλουν μηνύματα poison προς όλους τους γειτονικούς τους κόμβους πλην του RA.

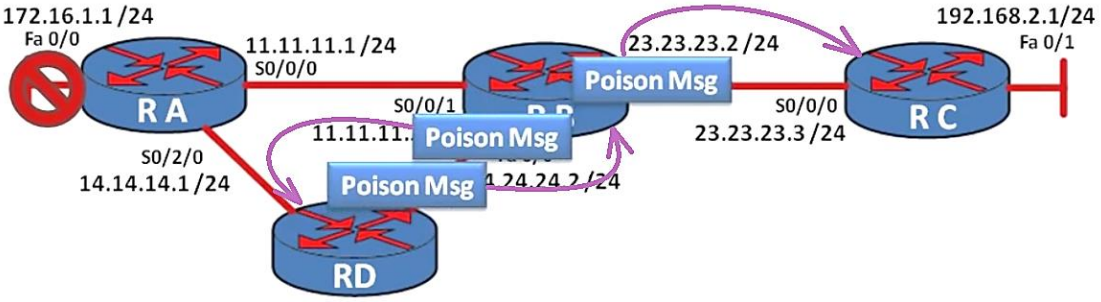
Η ίδια διαδικασία θα γίνεται κάθε φορά απ' όλους τους δρομολογητές του δικτύου ώστε να ενημερωθούν γι αυτήν την αλλαγή που έγινε στο δίκτυο και για την εύρεση των βέλτιστων διαδρομών που είναι βεβαίως σε λειτουργία.



Πίνακας δρομολόγησης RB

Προορισμός	Hops	Θύρα
172.16.1.0	X?	S0/0/1
11.11.11.0	0	S0/0/1
23.23.23.0	0	S0/0/2
192.168.2.0	1	S0/0/2
172.16.1.0	X?	Fa0/0

Εικόνα 2.71. Διαδικασία αποστολής poison reverse από τους δρομολογητες RB και RD προς τον RA



Πίνακας δρομολόγησης RB

Προορισμός	Hops	Θύρα
172.16.1.0	∞	S0/0/1
11.11.11.0	0	S0/0/1
23.23.23.0	0	S0/0/2
192.168.2.0	1	S0/0/2
172.16.1.0	∞	Fa0/0

Εικόνα 2.72. Αποσολή poison μηνυμάτων από τους δρομολογητές RB και RD προς όλους τους γειτονικούς τους κόμβους

Συνεπώς εφόσον δεν υπάρχει άλλη διαδρομή το δίκτυο με network IP 172.16.1.0 διαγράφεται από τον πίνακα δρομολόγησης του RB. Πέραν των poison μηνυμάτων

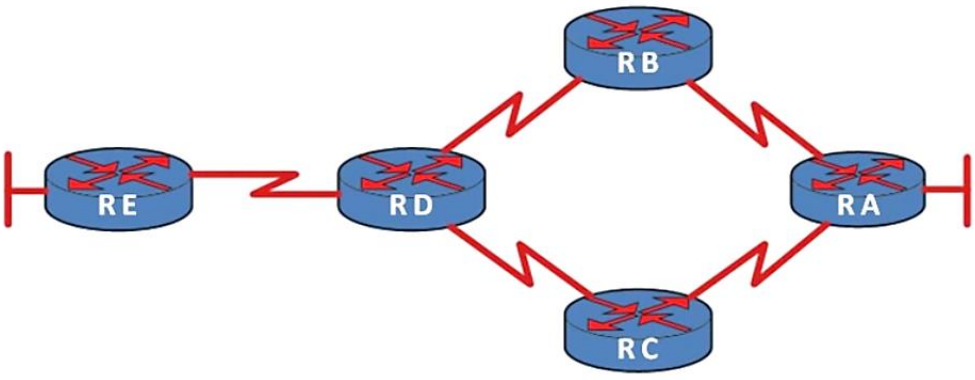
χρειαζόμαστε και άλλες μεθόδους προκειμένου να αποφύγουμε λάθος καταχωρήσεις στους πίνακες δρομολόγησης. Μια ακόμη μέθοδος είναι αυτή του holddown timers την οποία θα δούμε παρακάτω.

Holddown timers

Η μέθοδος του holddown timers είναι ένα πολύ απλή και χρήσιμη. Η βασική του λειτουργία είναι ότι κάθε δρομολογητής έχει έναν timer που αυτός τίθεται σε λειτουργία όταν λάβει μια πληροφορία για ένα δίκτυο το οποίο δεν είναι διαθέσιμο (unreachable). Μέχρι την λήξη αυτού του timer ο δρομολογητής θα απορρίψει οποιοδήποτε άλλες μεταγενέστερες ενημερώσεις που υποδεικνύουν ότι αυτή διαδρομή είναι στην ουσία διαθέσιμη.
Με άλλα λόγια, ένας holddown timer αποτρέπει έναν δρομολογητή από το να λάβει ενημερώσεις για διαδρομές έως ότου το δίκτυο σταθεροποιηθεί με την επαναφορά λειτουργίας της θύρας που συνδέεται το εκάστοτε δίκτυο ή όταν γίνει γνωστή κάποια διαφορετική διαδρομή προς αυτό το δίκτυο το οποίο είναι μη διαθέσιμο.
Αν ένας δρομολογητής εντοπίσει ένα δίκτυο το οποίο είναι μη διαθέσιμο τότε θα εκινήσει τον timer του. Ο δρομολογητής θα αναμένει για κάποιο χρονικό διάστημα έως ότου σταθεροποιηθεί το δίκτυο. Όταν ο timer λήξει τότε ο δρομολογητής θα μπορεί να λάβει ενημερώσεις για διαδρομές από άλλους δρομολογητές. Για παράδειγμα στο RIP το προκαθορισμένο holddown timer είναι ρυθμισμένο στα 180 δευτερόλεπτα.

3. Αλγόριθμοι κατάστασης της σύνδεσης (Link State)

Οι αλγόριθμοι δρομολόγησης κατάστασης της σύνδεσης (link state) βασίζονται σε αλγορίθμους όπου υπολογίζουν την βέλτιστη διαδρομή με διαφορετικό τρόπο απ' ότι οι αλγόριθμοι διανύσματος απόστασης (distance vector). Όπως περιγράψαμε παραπάνω στους αλγορίθμους διανύσματος απόστασης ένας δρομολογητής ενημερώνεται από τους γειτονικούς του δρομολογητές για τις διαθέσιμες διαδρομές. Όμως στους αλγορίθμους κατάστασης της σύνδεσης δημιουργείται εξ αρχής μια τοπολογία ολόκληρου του δικτύου και έπειτα υπολογίζονται οι βέλτιστες διαδρομές υπολογίζοντας την βέλτιστη με βάση αυτήν την τοπολογία.



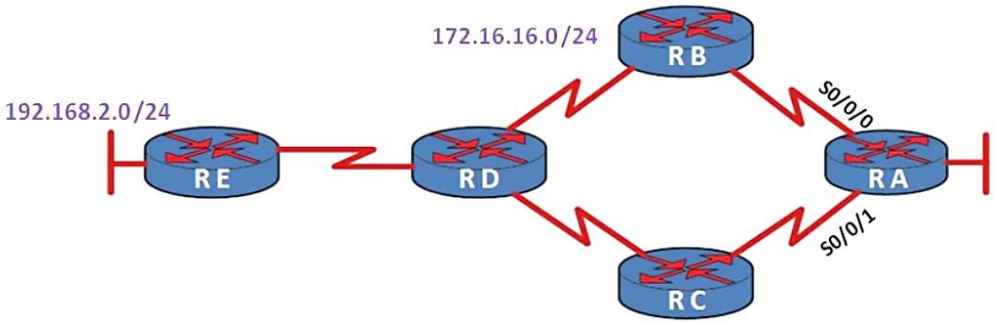
Εικόνα 2.73. Τοπολογία με πέντε δρομολογητές

Ας πάρουμε για παράδειγμα το δίκτυο της εικόνας. Ο δρομολογητής RA γνωρίζει εξ' αρχής όλους τους κόμβους του δικτύου χωρίς να έχει λάβει κάποιο ενημερωτικό μήνυμα από τους γειτονικούς του. Μια επίσης βελτίωση σε σχέση με τους αλγορίθμους διανύσματος απόστασης είναι ότι οι εδώ οι δρομολογητές δεν στέλνουν ενημερώσεις μεταξύ τους σχετικά με της ενδιάμεσες διαδρομές. Οι σχεδιαστές δικτύων όταν σχεδίαζαν τους αλγορίθμους κατάστασης της σύνδεσης κατάληξαν στο

συμπέρασμα ότι είναι ανώφελο να ενημερώνονται οι δρομολογητές μεταξύ τους κάθε 30 δευτερόλεπτα για τις διαθέσιμες διαδρομές που υπάρχουν σε ένα δίκτυο. Γι αυτόν τον απλό λόγο στους αλγορίθμους κατάστασης της σύνδεσης στέλνονται triggered updates δηλαδή ενημερώσεις προς όλους τους κόμβους ενός δικτύου σε περίπτωση που συμβεί κάποια αλλαγή σε αυτό και αυτές οι ενημερώσεις περιέχουν όλη την πληροφορία για την αλλαγή που συνέβη στο δίκτυο.
Επίσης οι αλγόριθμοι κατάστασης της σύνδεσης υποστηρίζουν classfull IP διευθύνσεις που αυτό σημαίνει ότι μπορούν να δρομολογήσουν πακέτα με διαφορετική subnet mask από αυτή των κλάσεων. Υπάρχουν τρείς αλγόριθμοι δρομολόγησης κατάστασης της σύνδεσης που είναι το OSPF, EIGRP (cisco) και ο IS-IS.

Link-state databases

Σε αυτό το σημείο ας δούμε πιο αναλυτικά την λειτουργία των αλγορίθμων κατάστασης της σύνδεσης. Η διαδικασία με την οποία επιτελούν την λειτουργία τους είναι με το να συλλέγουν και να αναλύουν περισσότερη πληροφορία από αυτήν των αλγορίθμων διανύσματος απόστασης. Όλη αυτή η πληροφορία αποθηκεύεται σε τρεις βάσεις δεδομένων ή αλλιώς και πίνακες δεδομένων. Ο πρώτος πίνακας δεδομένων ονομάζεται γειτονικός πίνακας ο οποίος περιέχει όλους τους άμεσα συνδεδεμένους κόμβους ενός δρομολογητή και όλες τις πιθανές θύρες τους.



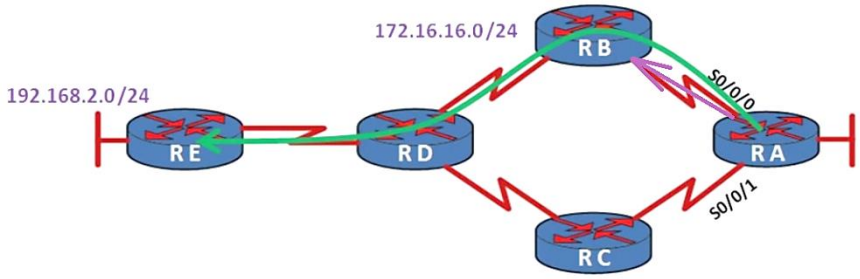
Γειτονικός πίνακας

Γείτονας	Θύρα
RB	S0/0/0
RC	S0/0/1

Εικόνα 2.74. Δομή γειτονικού πίνακα

Όπως βλέπουμε από την εικόνα ο γειτονικός πίνακας θα περιέχει τους γειτονικούς κόμβους του δρομολογητή RA που είναι ο RB και ο RC μαζί με τις αντίστοιχες θύρες τους. Υπάρχουν πολλοί λόγοι για τους οποίους ένας δρομολογητής κρατάει έναν πίνακα με τους γειτονικούς του κόμβους αλλά ο κυριότερος απ' όλους είναι ότι ο δρομολογητής αυτός προσδοκεί απ' όλους τους γειτονικούς του να τον ενημερώσουν για τις βέλτιστες διαδρομές προς όλους τους προορισμούς τους οποίος μπορούν να φτάσουν. Ο δρομολογητής αυτός συλλέγει όλες αυτές τις ενημερώσεις από τους γειτονικούς του και δημιουργεί έναν πίνακα τοπολογίας ή μια βάση δεδομένων της τοπολογίας του δικτύου. Αυτός ο πίνακας περιέχει όλες τις διαδρομές του δικτύου που αυτός ο δρομολογητής μπορεί να προσεγγίσει. Ο λόγος για τον οποίο ένας δρομολογητής κρατάει όλες τις πιθανές διαδρομές σε μια βάση δεδομένων είναι

προφανές ότι γίνεται για να επιλεγεί η βέλτιστη διαδρομή. Η διαφορά όμως από τους αλγόριθμους διανύσματος απόστασης είναι ότι εδώ επιλέγεται απλά η διαδρομή από τον πίνακα τοπολογίας. Πίσω πάλι στο παράδειγμα μας όταν ο δρομολογητής RA λάβει την βέλτιστη διαδρομή από τον δρομολογητή RB τότε θα καταγράψει αυτήν την διαδρομή στον πίνακα τοπολογίας που διαθέτει. Στην εικόνα αποτυπώνεται η διαδικασία αυτή καθώς και η καταχώρηση που θα γίνει στον πίνακα τοπολογίας του RA.



Γειτονικός πίνακας

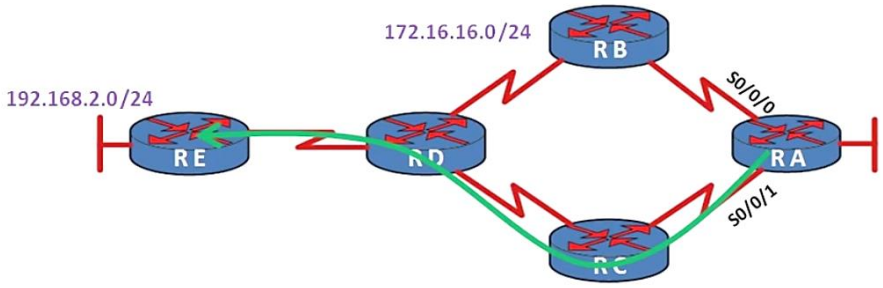
Γείτονας	Θύρα
RB	S0/0/0
RC	S0/0/1

Πίνακας τοπολογίας

Προορισμός	Κόστος	Θύρα
172.16.16.0	10	S0/0/0
192.168.2.0	55	S0/0/0

Εικόνα 2.75. Δομή πίνακα τοπολογίας και οι καταχωρήσεις του

Η πρώτη λοιπόν καταχώρηση που θα γίνει στον πίνακα τοπολογίας θα είναι για το δίκτυο 172.16.16.0 που το κόστος γι αυτό είναι 10 και η outbound θύρα που είναι η S0/0/0. Έπειτα η δεύτερη καταχώρηση θα γίνει για το δεύτερο δίκτυο το οποίο βρήκε και είναι το 192.16.2.0. Σημειώνουμε εδώ ότι όσο πιο χαμηλό είναι το κόστος της διαδρομής τόσο καλύτερη είναι αυτή. Σε αυτό το σημείο ο δρομολογητής RA λαμβάνει επίσης μια δεύτερη διαδρομή από τον δρομολογητή RC.



Γειτονικός πίνακας

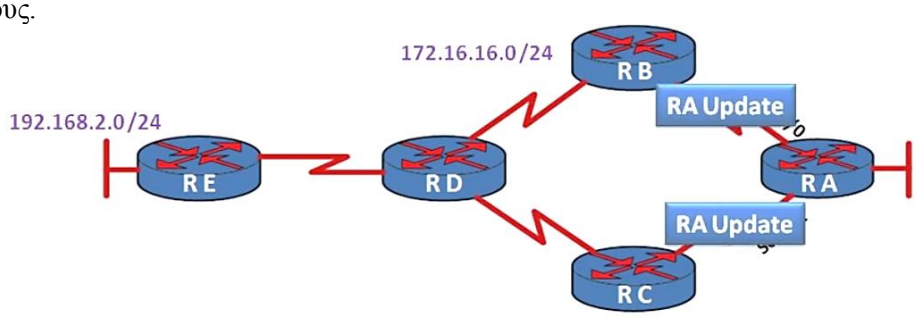
Γείτονας	Θύρα
RB	S0/0/0
RC	S0/0/1

Πίνακας τοπολογίας

Προορισμός	Κόστος	Θύρα
172.16.16.0	10	S0/0/0
192.168.2.0	55	S0/0/0
172.16.16.0	40	S0/0/1
192.168.2.0	55	S0/0/1

Εικόνα 2.76. Δομή πίνακα τοπολογίας και οι καταχωρήσεις του

Το κόστος για το δίκτυο 172.16.16.0 από τον δρομολογητή RC είναι 40 και για το δίκτυο 192.168.2.0 είναι 55. Με βάση λοιπόν τον αλγόριθμο Dijkstra ή τον αλγόριθμο σύντομου μονοπατιού ο δρομολογητής RA θα επιλέξει το βέλτιστο μονοπάτι από αυτές τις δύο διαδρομές και φτιάχνει τον πίνακα δρομολόγησης του.
Αφού ο δρομολογητής RA έχει φτιάξει τον πίνακα δρομολόγησης του θα στείλει προς τους γειτονικούς του δρομολογητές RB και RC routing updates που περιέχουν τα βέλτιστα μονοπάτια τα οποία επέλεξε έτσι ώστε αυτοί να ελέγξουν αν αυτές τις διαδρομές και να βρουν με την σειρά τους είναι οι βέλτιστες διαδρομές για τους ίδιους.



Γειτονικός πίνακας

Γείτονας	Θύρα
RB	S0/0/0
RC	S0/0/1

Πίνακας τοπολογίας

Προορισμός	Κόστος	Θύρα
172.16.16.0	10	S0/0/0
192.168.2.0	55	S0/0/0
172.16.16.0	40	S0/0/1
192.168.2.0	55	S0/0/1

Πίνακας δρομολόγησης RA

Προορισμός	Κόστος	Θύρα
172.16.16.0	10	S0/0/0
192.168.2.0	55	S0/0/0
192.168.2.0	55	S0/0/1

Εικόνα 2.77. Δομή πίνακα δρομολόγησης RA

4. OSPF (Open Shortest Path First)

Το OSPF είναι ένα link-state πρωτόκολλο δρομολόγησης IP δικτύων που είναι ανοικτά διαθέσιμο προς όλους. Με τον όρο «ανοικτά διαθέσιμο» εννοούμε ότι η προδιαγραφή αυτού του πρωτοκόλλου δρομολόγησης είναι δημόσια διαθέσιμη σε αντίθεση με το EIGRP που είναι ένα κλειστό πρωτόκολλο δρομολόγησης link-state της Cisco. Είναι πρωτόκολλο τύπου IGP, που αφορά τη διανομή πληροφορίας δρομολόγησης εντός ενός αυτόνομου συστήματος (intra-AS, interior gateway), παρότι μπορεί να στείλει και να λάβει διαδρομές και από άλλα. Αναπτύχθηκε από την ομάδα εργασίας IGP, Interior Gateway Protocol της IETF, Internet Engineering Task Force. Παρόμοια με το IGRP, Interior Gateway Routing Protocol το OSPF δημιουργήθηκε διότι στα μέσα 1980 το RIP φάνηκε αρκετά ανεπαρκές για να εξυπηρετήσει τα μεγάλα πλέον ανομοιογενή δίκτυα. Η πιο πρόσφατη έκδοση του

OSPF είναι η έκδοση 2 και ορίζεται στο RFC 2328. Στον πίνακα βρίσκονται όλες οι εκδόσεις του OSPF και πως αυτές έχουν οριστεί στο RFC.

Χρονολογία	Έκδοση	RFC
1989	OSPF Version 1	RFC 1131
1991	OSPF Version 2	RFC1247
1994	OSPF Version 2 (revised)	RFC 1583
1997	OSPF Version 2 (revised)	RFC 2178
1998	OSPF Version 2	RFC 2328

Πίνακας 2.6. Εκδόσεις του OSPF ανά χρονολογία

Το OSPF ξεκίνησε σαν διάδοχος του RIP και έτσι έχει αρκετά προχωρημένα χαρακτηριστικά. Βασίζεται στον αλγόριθμό SPF, Shortest Path First (αναφερόμενος και σαν αλγόριθμος του Dijkstra). Με το OSPF ένας δρομολογητής κατασκευάζει έναν πλήρη τοπολογικό χάρτη (δηλαδή έναν γράφο) ολόκληρου του αυτόνομου συστήματος. Ο δρομολογητής κατόπιν εκτελεί τοπικά τον αλγόριθμο ελάχιστου κόστους Dijkstra για να καθορίσει ένα δέντρο βραχύτερης διαδρομής προς όλα τα υποδίκτυα με τον εαυτό του ως ριζικό κόμβο. Μεμονωμένα στοιχεία κόστους ζεύξεων παραμετροποιούνται από τον διαχειριστή του δικτύου όπου ο ίδιος μπορεί να επιλέξει να θέσει το κόστος ζεύξεων σε 1 επιτυγχάνοντας με αυτό τον τρόπο δρομολόγηση ελάχιστου άλματος ή απλά μπορεί να επιλέξει να θέσει τα βάρη ζεύξεων να είναι αντιστρόφως ανάλογα με την χωρητικότητα της ζεύξης έτσι ώστε να αποθαρρύνει την κίνηση μέσω ζεύξεων που έχουν χαμηλό εύρους ζώνης. Το OSPF δεν επιβάλει κάποια πολιτική για το πώς θα τίθενται τα βάρη στις ζεύξεις. Αντ' αυτού παρέχει μηχανισμούς για τον καθορισμό της δρομολόγησης διαδρομής ελάχιστου κόστους για το δεδομένο σύνολο βαρών ζεύξεων. Στο OSPF δεν υπάρχει περιορισμός στον αριθμό των hop, ενώ το RIP περιορίζεται στα 15 hops.
Με το OSPF ένας δρομολογητής μπορεί να κάνει εκπομπή πληροφοριών δρομολόγησης σε όλους τους άλλους δρομολογητές μέσα στο αυτόνομο σύστημα και όχι μόνο προς τους γειτονικούς του δρομολογητές (όπως για παράδειγμα στο RIP). Ένας δρομολογητής κάνει εκπομπή πληροφοριών κατάστασης ζεύξης οπότε υπάρχει μια αλλαγή στην κατάσταση μιας ζεύξης. Επίσης κάνει περιοδικά εκπομπή της κατάστασης μιας ζεύξης (τουλάχιστον κάθε 30 λεπτά), ακόμη κι αν η κατάσταση ζεύξης δεν έχει αλλάξει.
Το πρωτόκολλο OSPF ελέγχει επίσης αν οι ζεύξεις είναι σε λειτουργία μέσω ενός μηνύματος HELLO που στέλνεται προς έναν συνδεδεμένο γειτονικό κόμβο επιτρέποντας έτσι να λάβει από αυτόν πληροφορίες για την κατάσταση των ζεύξεων σε όλο το δίκτυο.
Ορισμένα από τα νέα χαρακτηριστικά που έχουν ενσωματωθεί στο OSPF είναι τα εξής:

- **Ασφάλεια**: όλες οι ανταλλαγές των δρομολογητών (π.χ. ενημερώσεις για τις καταστάσεις των ζεύξεων σε ένα δίκτυο) αυθεντικοποιούνται. Αυτό σημαίνει ότι μόνο έμπιστοι δρομολογητές μπορούν να συμμετέχουν στο πρωτόκολλο OSPF μέσα σε ένα δίκτυο.

- **Πολλαπλές διαδρομές ίδιου κόστους:** Όταν πολλαπλές διαδρομές προς έναν προορισμό έχουν το ίδιο κόστος με την χρήση OSPF επιτρέπεται να χρησιμοποιηθούν πολλαπλές διαδρομές.

- **<u>Ολοκληρωμένη υποστήριξη για δρομολόγηση μονοεκπομπής και πολυεκπομπής:</u>** Το OSPF πολυεκπομπής παρέχει απλές επεκτάσεις στο OSPF για να παρέχει την δυνατότητα δρομολόγησης πολυεκπομπής.

- **<u>Ιεραρχική υποστήριξη μέσα σε έναν μόνο τομέα δρομολόγησης:</u>** Ίσως η σημαντικότερη εξέλιξη στο OSPF είναι η δυνατότητα ιεραρχικής δόμησης ενός συστήματος.

5. Σύγκριση OSPF και RIP

<table>
<tr><th colspan="2">Σύγκριση RIP και OSPF</th></tr>
<tr><td rowspan="2">Γενικά χαρακτηριστικά</td><td>Routing Information Protocol – RIP</td></tr>
<tr><td>• Το RIP συλλέγει μεγάλο ποσοστό άχρηστης πληροφορίας και δημιουργούνται λανθασμένες δρομολογήσεις λόγω της μεγάλης καθυστέρησης σύγκλησης.
• Οι ενημερώσεις στέλνονται περιοδικά ανά 30 sec, αφορούν όλη την πληροφορία δρομολόγησης και γίνονται με broadcast μετάδοση.
• Το γεγονός αυτό αυτόματα κάνει το RIP ακατάλληλο για χρήση σε ασύρματα δίκτυα.
• Ακατάλληλο πρωτόκολλο για μεγάλα δίκτυα ή δίκτυα που αλλάζουν αρκετά γρήγορα και συχνά.
• Η σύγκλιση μπορεί να πάρει αρκετά λεπτά, οι δρομολογητές κάνουν time-out πληροφορία που δεν έχει ληφθεί πρόσφατα</td></tr>
<tr><td rowspan="2"></td><td>Open Shortest Path First – OSPF</td></tr>
<tr><td>• Έχει καλύτερη - γρηγορότερη σύγκλιση, διότι οι αλλαγές προωθούνται άμεσα και όχι περιοδικά.
• Αλλαγές στη δρομολόγηση συμβαίνουν άμεσα και όχι περιοδικά
• Οι ενημερώσεις στέλνονται μόνο σε περίπτωση αλλαγής και γίνονται με ip multicast μετάδοση
• Λιγότερο overhead στο δίκτυο, ιδιότητα σημαντική για μεγάλα δίκτυα</td></tr>
<tr><td rowspan="2">Βέλτιστη διαδρομή</td><td>Routing Information Protocol – RIP</td></tr>
<tr><td>• Οι αποφάσεις δρομολόγησης λαμβάνονται με βάση μόνο των αριθμό των συνδέσεων και όχι το κόστος – εύρος της κάθε σύνδεσης.
• Έτσι προτιμάται μια κοντινή διαδρομή έστω και αν υπάρχει μακρύτερη με περισσότερο εύρος</td></tr>
<tr><td rowspan="2"></td><td>Open Shortest Path First – OSPF</td></tr>
<tr><td>• Οι αποφάσεις δρομολόγησης λαμβάνονται με βάση το κόστος των συνδέσεων και έτσι προτιμάται η αληθινά βέλτιστη διαδρομή</td></tr>
</table>

Ιεραρχία	**Routing Information Protocol – RIP**	
	• Τα RIP δίκτυα είναι επίπεδα, δεν έχουν τη δυνατότητα ιεράρχησης στη δρομολόγηση • Αυτό αποκλείει την εφαρμογή τεχνικών aggregation, summarization	
	Open Shortest Path First – OSPF	
	• Αντίθετα στο OSPF η δυνατότητα ορισμού ιεραρχίας στη δρομολόγηση, (με τον ορισμό περιοχών) περιορίζει τον αριθμό των ενημερώσεων σε μεγάλα δίκτυα και παρέχει το μηχανισμό για την συνένωση (aggregation) των διαδρομών και τον περιορισμό της μη χρήσιμης μετάδοσης πληροφορία σχετικά με τα υποδίκτυα	

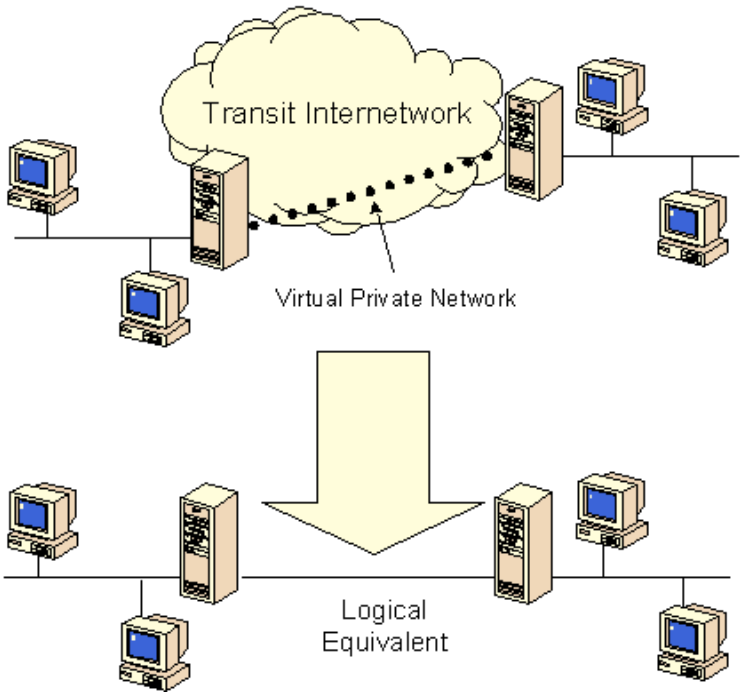
Πίνακας 2.7. Σύγκριση OSPF και RIP

6. Enhanced Interior Gateway Routing Protocol – EIGRP

Το EIGRP (Enhanced Interior Gateway Routing Protocol) είναι ένα πρωτόκολλο δρομολόγησης δικτύων υπολογιστών, αναπτυγμένο από την εταιρεία Cisco Systems, και είναι βασισμένο στο παλιότερο πρωτόκολλο IGRP (με το οποίο είναι προς τα πίσω συμβατό). Ανήκει στην κατηγορία των πρωτοκόλλων διανύσματος απόστασης (distance vector) και είναι βελτιστοποιημένο αφ' ενός προς την ελαχιστοποίηση της αστάθειας που συμβαίνει όταν αλλάξει η τοπολογία ενός δικτύου, και αφ' ετέρου προς την βέλτιστη αξιοποίηση του εύρους ζώνης και της επεξεργαστικής ισχύος του δρομολογητή. Οι περισσότερες από αυτές τις δυνατότητες αποτελούν μέρους του αλγόριθμου DUAL, ο οποίος αναπτύχθηκε από το ινστιτούτο SRI (Stanford Research Institute). Ο αλγόριθμος DUAL εγγυάται την αποτροπή βρόχων στη δρομολόγηση, και την ταχεία εύρεση εναλλακτικών δρομολογίων, τηρώντας αναπληρωματικά δρομολόγια για κάθε δίκτυο.

2.7.8 Ιδεατά ιδιωτικά δίκτυα (Virtual Private Network - VPN)

Με τον όρο ενός ιδεατού ιδιωτικού δικτύου (Virtual Private Network - VPN) αναφερόμαστε στην διασύνδεση των στοιχείων ενός δικτύου με αυτά ενός άλλου δικτύου. Τα VPNs υλοποιούν αυτή την διαδικασία σύνδεσης επιτρέποντας στον χρήστη να «διαπεράσει» (tunnel) το Internet ή άλλα δημόσια δίκτυα με την ίδια ασφάλεια και τα χαρακτηριστικά που θα είχε σε ένα αντίστοιχα ιδιωτικό δίκτυο LAN. Το VPN είναι ένα δίκτυο που έχει ως άμεσο σκοπό την αποκατάσταση της επικοινωνίας των δεδομένων μεταξύ δύο απομακρυσμένων παραρτημάτων που μπορεί να βρίσκονται σε μια εταιρία ή σε έναν οργανισμό.



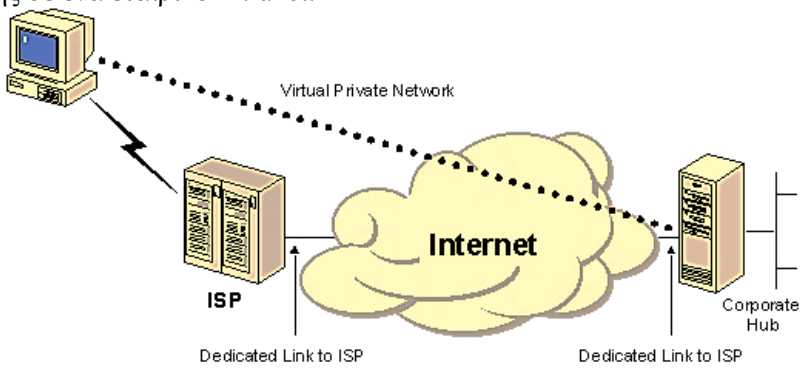
Εικόνα 2.78. Παράδειγμα λειτουργίας VPN

Όπως απεικονίζεται στην εικόνα 2.78, οι μηχανισμοί VPN επιτρέπουν σε έναν απομακρυσμένο κόμβο να συνδέετε σε ένα τοπικό δίκτυο (LAN) μέσω ενός εκ φύσεως μη ασφαλούς δικτύου όπως το Διαδίκτυο, και να απολαμβάνει τις υπηρεσίες, την πρόσβαση και την ασφάλεια που θα είχε εάν αυτός ο κόμβος βρισκόταν φυσικά στον ίδιο χώρο.

Το Virtual Private Network (VPN) εφαρμόζεται σε συνδέσεις από 9.6 Kbps έως 2 Mbps. Η διασύνδεση του γίνεται είτε με χρήση μισθωμένου κυκλώματος είτε μέσω απλού τηλεφωνικού δικτύου, ανάλογα βέβαια με τις απαιτήσεις της εφαρμογής. Το VPN χαρακτηρίζεται ως νοήμον δίκτυο. Με τον όρο Νοήμον Δίκτυο, αναφερόμαστε στην αρχιτεκτονική μιας πλατφόρμας που αποτελείται από υλικό και λογισμικό προστίθοντας «νοημοσύνη» στα τηλεπικοινωνιακά δίκτυα. Με τον τρόπο αυτόν, είναι δυνατόν πολύ εύκολα, γρήγορα και οικονομικά να αναπτύσσονται νέες τηλεπικοινωνιακές υπηρεσίες ανάλογα με τις διαμορφούμενες ανάγκες της τηλεπικοινωνιακής αγοράς. Μερικά από τα χαρακτηριστικά των νοήμον δικτύων είναι η ευελιξία στη δρομολόγηση της κίνησης (flexible routing), ταχεία ανάπτυξη και παροχή υπηρεσιών σύμφωνα με τις απαιτήσεις του πελάτη, σχεδιασμός νέων υπηρεσιών ανάλογα με τις απαιτήσεις της αγοράς κλπ. (αυτά είναι off)

1. **Απομακρυσμένη πρόσβαση μέσω Internet**

Τα VPNs παρέχουν την δυνατότητα πρόσβασης ενός απομακρυσμένου χρήστη στους πόρους ενός δικτύου μέσω βέβαια του διαδικτύου (Internet), διατηρώντας παράλληλα την ασφάλεια των πληροφοριών που διακινούνται. Η εικόνα 2.75 δείχνει πως χρησιμοποιείται ένα VPN για να συνδεθεί ένας απομακρυσμένος χρήστης σε ένα εταιρικό Intranet.

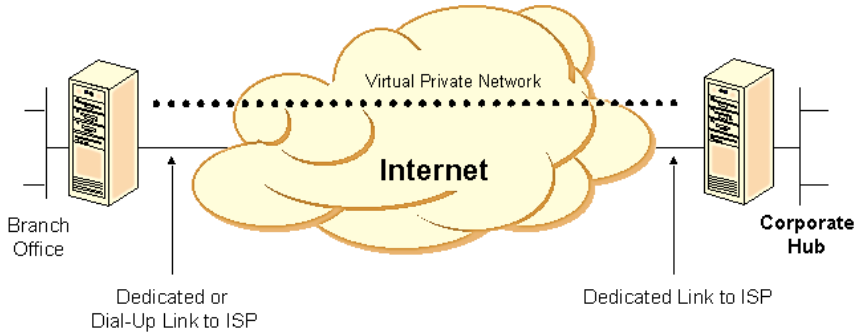


Εικόνα 2.79. Παράδειγμα λειτουργίας VPN σε ένα εταιρικό intranet

Αντί δηλαδή να καλούμε με υπεραστικό τηλεφώνημα έναν Network Access Server (NAS) καλούμε έναν τοπικό ISP. Χρησιμοποιώντας τη σύνδεση με τον τοπικό πάροχο Internet, το λογισμικό του VPN δημιουργεί ένα ιδεατό ιδιωτικό δίκτυο μεταξύ του υπολογιστή μας και του VPN server που βρίσκεται σε απομακρυσμένο σημείο.

2. **VLAN σύνδεση μεταξύ τοπικών δικτύων μέσω Internet**

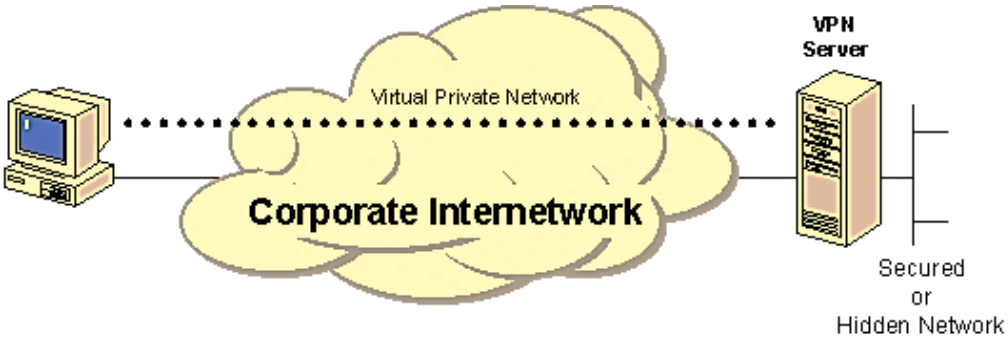
Οι μηχανισμοί VPN μπορούν να χρησιμοποιηθούν να συνδέσουν δύο απομακρυσμένα LAN μεταξύ τους με ασφάλεια μέσω του Διαδικτύου. Για να γίνει αυτό, κάθε LAN θα πρέπει να έχει μία σύνδεση στο Διαδίκτυο οποιουδήποτε τύπου (ADSL, Dialup κτλ). Φυσικά όσο πιο μεγάλο είναι το bandwidth, τόσο καλύτερη ποιότητα σύνδεσης μπορεί να επιτευχθεί. Κάθε ένα από τα απομακρυσμένα LAN θα πρέπει να διαθέτει δρομολογητές που να υποστηρίζουν μηχανισμούς VPN. Μεταξύ αυτών των δύο συσκευών, δημιουργείται η VPN tunnel, έτσι ώστε οι κόμβοι στο ένα LAN να μπορούν να επικοινωνούν με αυτούς στο δεύτερο LAN σαν να βρίσκονται στο ίδιο χώρο, δηλαδή στο ίδιο υποδίκτυο. Επισημαίνεται ότι σε αυτή τη περίπτωση, όλοι οι μηχανισμοί VPN βρίσκονται και λειτουργούν στους δύο δρομολογητές στις δύο άκρες της VPN σύνδεσης.



Εικόνα 2.80. Παράδειγμα λειτουργίας VPN μεταξύ δύο απομακρυσμένων LAN

3. VLAN Σύνδεση μεταξύ ενός Η/Υ και ενός VPN Server μέσω Intranet

Στην περίπτωση της σύνδεσης ενός μεμονωμένου υπολογιστή μέσω VPN σε ένα επιχειρησιακό δίκτυο, μπορεί να χρησιμοποιηθεί λογισμικό VPN Client στον υπολογιστή αυτό το οποίο μπορεί να συνδεθεί μέσω το Internet σε ένα VPN Server. Δημιουργείται μεταξύ των δύο ένα tunnel μέσω του οποίου μπορεί να επικοινωνεί ο υπολογιστής με το εσωτερικό δίκτυο της επιχείρησης σαν να βρίσκοταν στον ίδιο χώρο και στο ίδιο υποδίκτυο.



Εικόνα 2.81. Παράδειγμα λειτουργίας VPN μεταξύ μεμονωμένου Η/Υ και του εταιρικού δικτύου

Με τη χρήση του VPN ο χρήστης του δικτύου μπορεί να είναι σίγουρος ότι μόνο εκείνοι οι χρήστες της επιχείρησης που έχουν τα απαραίτητα δικαιώματα μπορούν να έχουν πρόσβαση στα ευαίσθητα δεδομένα. Π.χ. δε θα επιθυμούσε η γενική διεύθυνση μιας επιχείρησης την πρόσβαση όλων των χρηστών στις μισθολογικές καταστάσεις του προσωπικού για ευνόητους λόγους.

Τα κυριότερα πλεονεκτήματα του VPN είναι:

- Ουσιαστική, χωρίς όρια, αύξηση της χωρητικότητας
- Επέκταση δικτύου σε διαφορετικούς τόπους
- Πολλές νέες ευκολίες
- Ευελιξία και δημιουργία πακέτων ευκολιών επί παραγγελία
- Δεν υπάρχει ρίσκο λόγω απαρχαίωσης ή αχρηστίας
- Εξοικονόμηση (μείωση κόστους αφού δεν απαιτούνται επενδύσεις για την αγορά πρόσθετου εξοπλισμού)
- Τεχνική υποστήριξη από το διαχειριστή δικτύου
- Υψηλή αξιοπιστία

2.8 Επίπεδο σύνδεσης δεδομένων (Data link – Layer 2)

Το επίπεδο σύνδεσης δεδομένων ή αλλιώς και επίπεδο ζεύξης (Data Link Layer), είναι το δεύτερο επίπεδο συνολικά από τα επτά επίπεδα του μοντέλου αναφοράς OSI. Στόχος του είναι να παρέχει υπηρεσίες στο αμέσως επόμενο επίπεδο (δηλαδή προς το επίπεδο δικτύου), αξιοποιώντας τις υπηρεσίες του φυσικού επιπέδου.

Το επίπεδο σύνδεσης δεδομένων καθορίζεται από πρωτόκολλα τα οποία αναλαμβάνουν να ρυθμίσουν τη μετάδοση δεδομένων που διέρχεται από ένα φυσικό μέσο μετάδοσης (π.χ. οπτική ίνα, χάλκινα σύρματα κλπ). Ασχολείται με την τοπική παράδοση πλαισίων (frames) μεταξύ συσκευών στο ίδιο τοπικό δίκτυο.

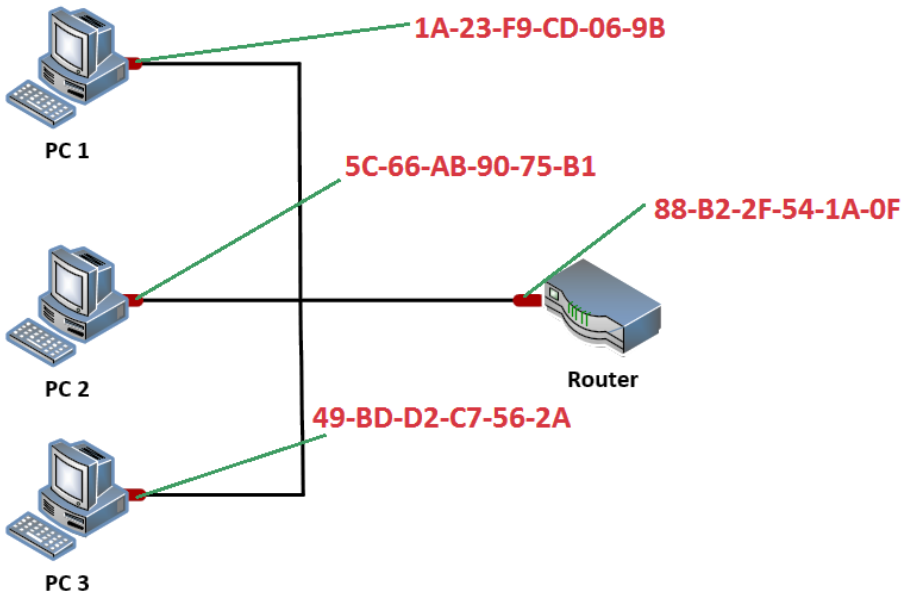
Τα πλαίσια του επιπέδου ζεύξης δεδομένων δεν διασχίζουν τα πλαίσια ενός τοπικού δικτύου. Τα ανώτερα επίπεδα που αναφέραμε παραπάνω αναλαμβάνουν την διαδικασία δρομολόγησης των μηνυμάτων ανάμεσα σε δίκτυα και γενικά στο διαδίκτυο (internet). Με αυτόν τον τρόπο δίνεται η δυνατότητα στα πρωτόκολλα του επίπεδου σύνδεσης δεδομένων να εστιάσουν στην τοπική παράδοση, διευθυνσιοδότηση και διαχείριση αυτών των μέσων.
Για παράδειγμα ας φανταστούμε έναν τροχονόμο ο οποίος είναι υπεύθυνος σε έναν δρόμο κυκλοφορίας οχημάτων.

Η δουλειά του είναι να διαιτητεύσει τα άτομα που αντιδικούν ώστε να γίνει αποσυμφόρηση του δρόμου και να ξεκινήσει ξανά και ομαλά η κυκλοφορία των οχημάτων. Την ίδια δουλειά λοιπόν αναλαμβάνει το επίπεδο σύνδεσης δεδομένων όταν συσκευές (π.χ. δύο υπολογιστές) επιχειρούν να χρησιμοποιούν το ίδιο μέσο μετάδοσης ταυτόχρονα με άμεσο σκοπό να προλάβει ή ακόμα και να αποφύγει τις συγκρούσεις πλαισίων. Τα πρωτόκολλα που ανήκουν σε αυτό το επίπεδο καθορίζουν πώς οι συσκευές ανιχνεύουν και ανακάμπτουν αυτές τις συγκρούσεις παρέχοντας επίσης μηχανισμούς για να την αποφυγή αυτών. Η παράδοση αυτών των πλαισίων (frames) από συσκευές δευτέρου επιπέδου (π.χ. μεταγωγείς επιπέδου ζεύξης), επιτυγχάνεται μέσω των φυσικών διευθύνσεων MAC. Θα αναφερθούμε σε αυτού του τύπου διευθύνσεων στην υποπαράγραφο 2.8.1. Σε αυτό το σημείο ας συζητήσουμε την δομή ενός πλαισίου (frame). Η επικεφαλίδα η οποία περιέχεται σε ένα πλαίσιο διαθέτει τις διευθύνσεις πηγής και προορισμού, οι οποίες δείχνουν τη συσκευή προέλευσης και προορισμού αντίστοιχα. Όπως είχαμε αναφέρει στην υποπαράγραφο 2.7.1 μια IP διεύθυνση ακολουθεί ιεραρχική δομή και αλλάζει κάθε φορά που συνδεόμαστε στο διαδίκτυο.

Όμως σε αντίθεση με τις IP διευθύνσεις, οι φυσικές διευθύνσεις MAC δεν ακολουθούν αυτήν την λογική. Αυτό σημαίνει ότι η φυσική διεύθυνση MAC δεν αλλάζει και παραμένει η ίδια προσδιορίζοντας μοναδικά τον κάθε κόμβο.
Με αυτόν τον τρόπο το επίπεδο σύνδεσης δεδομένων παρέχει την δυνατότητα μεταφοράς δεδομένων κατά μήκος της φυσικής ζεύξης. Η μεταφορά μπορεί να είναι αξιόπιστη ή αναξιόπιστη. Αρκετά πρωτόκολλα ζεύξης δεδομένων δεν έχουν επιβεβαίωση επιτυχούς λήψης των δεδομένων και μερικά πρωτόκολλα ζεύξης μπορεί να μην έχουν καμία μορφή checksum για τον έλεγχο λαθών μετάδοσης. Σε αυτές τις περιπτώσεις, τα πρωτόκολλα υψηλότερων επιπέδων πρέπει να παρέχουν έλεγχο ροής, έλεγχο λαθών, επιβεβαιώσεις λήψης και επανεκπομπή. Στο μοντέλο αναφοράς OSI, το επίπεδο σύνδεσης δεδομένων ανταποκρίνεται σε αιτήσεις εξυπηρέτησης του επιπέδου δικτύου και επιτελούν την λειτουργία τους κάνοντας αιτήσεις εξυπηρέτησης στο φυσικό επίπεδο.

2.8.1 Φυσικές διευθύνσεις MAC

Στην πραγματικότητα ένας κόμβος (δηλαδή ένας υπολογιστής ή ένας δρομολογητής) δεν έχει μια φυσική διεύθυνση MAC (επιπέδου σύνδεσης δεδομένων) αλλά ένας προσαρμογέας που λέγετε κάρτα δικτύου και είναι τοποθετημένη στην μητρική πλακέτα ενός κόμβου. Στην υποπαράγραφο 2.2.3 είχαμε κάνει μια επιγραμματική αναφορά στην λειτουργία της κάρτας δικτύου.
Μια φυσική διεύθυνση MAC έχει μήκος 6 byte, έτσι έχουμε 2^{48} πιθανές διευθύνσεις MAC. Όπως φαίνεται και στην εικόνα 2.82 αυτές οι διευθύνσεις εκφράζονται ως ένα ζεύγος δεκαεξαδικών αριθμών και κάθε προσαρμογέας έχει μια μοναδική MAC διεύθυνση.

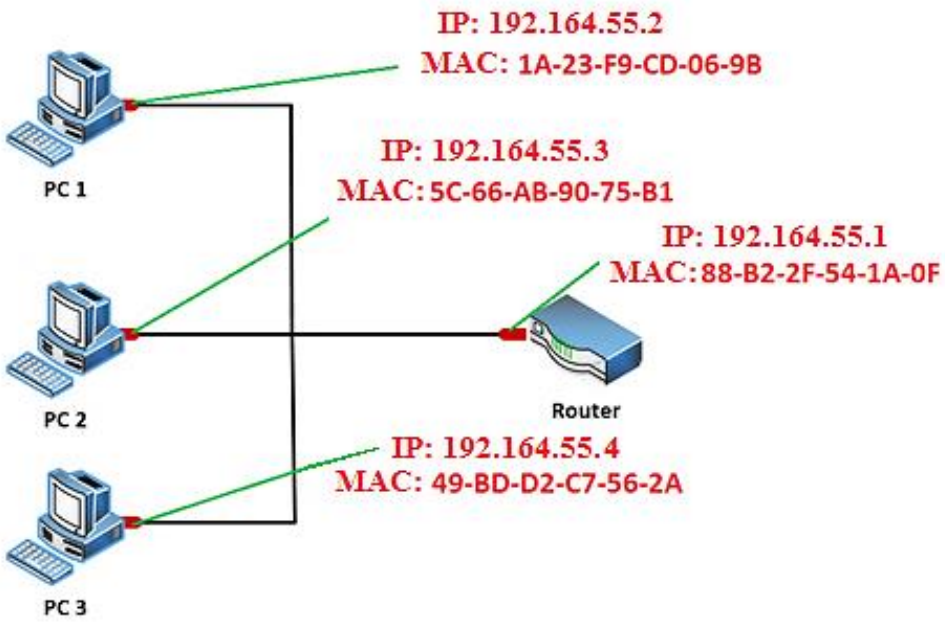


Εικόνα 2.82: Μορφή MAC διευθύνσεων

Το IEEE (Institute of Electrical and Electronic Engineers) διαχειρίζεται τον χώρο των φυσικών διευθύνσεων MAC. Συγκεκριμένα όταν μια εταιρία θέλει να κατασκευάσει προσαρμογείς αγοράζει έναντι ενός μικρού ποσού, μια ομάδα χώρου διευθύνσεων που αποτελείται από 2^{24} διευθύνσεις. Το IEEE δεσμεύει την ομάδα διευθύνσεων κρατώντας σταθερά τα πρώτα 24 bit μιας φυσικής διεύθυνσης επιτρέποντας έτσι στην εταιρία να δημιουργήσει μοναδικούς συνδυασμούς των τελευταίων 24 bit για κάθε προσαρμογέα. Η διεύθυνση MAC ενός προσαρμογέα έχει επίπεδη δομή (σε αντίθεση με την ιεραρχική δομή της IP διεύθυνσης) και δεν αλλάζει άσχετα με το που μεταφέρεται ο προσαρμογέας. Για παράδειγμα ένας φορητός υπολογιστής με μια κάρτα δικτύου έχει πάντα την ίδια φυσική διεύθυνση MAC ανεξάρτητα από το που πηγαίνει. Σε αντίθεση με την MAC η IP διεύθυνση έχει ιεραρχική δομή. Δηλαδή η IP διεύθυνση πάντα αλλάζει ακόμα κι όταν ο υπολογιστής δεν μετακινείται. Η MAC διεύθυνση σε κάθε hop αλλάζει ενώ η IP διεύθυνση παραμένει ίδια εκτός αν βρει NAT δρομολογητή.

2.8.2 Address Resolution Protocol (ARP)

Στην παράγραφο 2.8.1 αναλύσαμε την δομή των φυσικών διευθύνσεων. Σε αυτήν την παράγραφο θα δούμε πως μπορούμε να ανακτήσουμε την φυσική διεύθυνση MAC ενός κόμβου γνωρίζοντας μόνο την IP διεύθυνση του. Έστω ότι έχουμε το παρακάτω δίκτυο της εικόνας 2.83.



Εικόνα 2.83: Παράδειγμα δικτύου με MAC και IP διευθύνσεις

Ας υποθέσουμε ότι ο PC1 θέλει να στείλει ένα πακέτο στον PC2. Θα δημιουργήσει ένα πακέτο με τα δεδομένα και μέσα σε αυτό θα προστεθεί και η φυσική διεύθυνση MAC που διαθέτει. Μέσα όμως σε αυτό το πακέτο θα προσθέσει και η MAC διεύθυνση του προορισμού (δηλαδή του PC2). Εδώ τίθεται ένα ερώτημα, πως ο PC1 γνωρίζει την MAC διεύθυνση του PC2 ;
Για να το κάνει αυτό χρησιμοποιεί το πρωτόκολλο επίλυσης διευθύνσεων (Address Resolution Protocol – ARP) όπου σε κάθε κόμβο διαθέτει έναν πίνακα που ονομάζεται ARP table και περιέχει για κάθε IP διεύθυνση που υπάρχει στο δίκτυο, την αντίστοιχη φυσική διεύθυνση MAC. Με λίγα λόγια ο ARP table αντιστοιχεί όλες τις IP διευθύνσεις με τις φυσικές διευθύνσεις MAC των αντίστοιχων κόμβων. Κάθε κόμβος διατηρεί έναν ARP table όπου αποθηκεύονται οι αντιστοιχίσεις αυτές.

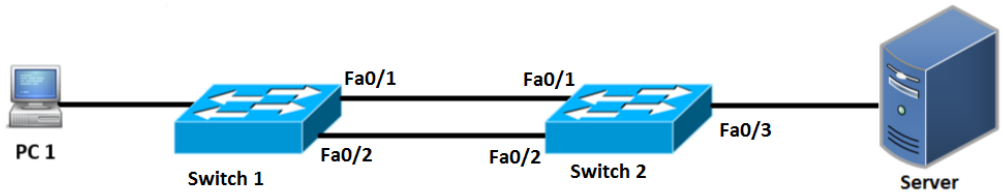
Διεύθυνση IP	Διεύθυνση MAC	TLL
192.164.55.2	1A-23-F9-CD-06-9B	13:45:00
192.164.55.4	49-BD-D2-C7-56-2A	13:52:00

Πίνακας 2.8. Παράδειγμα ενός πίνακα ARP

Έστω ότι στον ARP table δεν υπάρχει καταχώρηση μιας MAC διεύθυνσης ενός κόμβου του δικτύου. Αυτό που θα κάνει ο κόμβος είναι να στείλει ένα ARP request μήνυμα για να μάθει την MAC διεύθυνση του κόμβου και να την καταχωρίσει στο πίνακα. Ο κόμβος που έχει την IP διεύθυνση στέλνει ένα ARP reply με την MAC διεύθυνση.

2.8.3 Spanning Tree Protocol – STP

Το STP (Spanning Tree Protocol) είναι ένα δικτυακό πρωτόκολλο επιπέδου ζεύξης που εφαρμόζεται σε bridges και switches και έχει προτυποποιηθεί από την IEEE ως 802.1D. Ο βασικός σκοπός του STP είναι να αποτρέψει την ύπαρξη βρόχων (loops) σε δίκτυα που έχουν πλεονάζουσες διαδρομές.

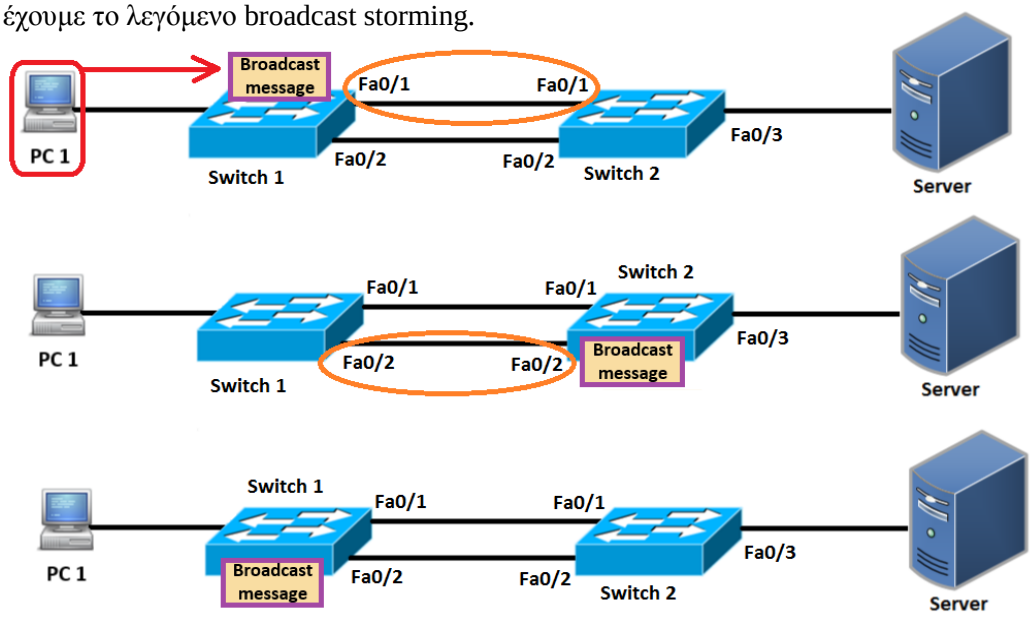


Εικόνα 2.84. Δίκτυο με πλεονάζουσες διαδρομές

Για να γίνει κατανοητό στην εικόνα 2.84 δίνεται ένα δίκτυο το οποίο έχει δύο μεταγωγείς (switches) με δύο διαδρομές την fast Ethernet 0/1 και την fast Ethernet 0/2. Το προβλήματα τα οποία παρουσιάζουν τέτοια δίκτυα είναι:

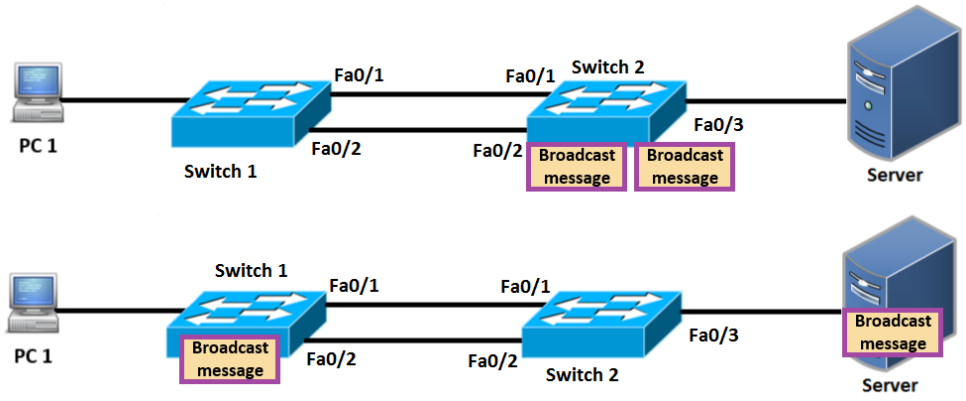
- Broadcast storms
- Multiple frame copies
- MAC table instabilities

Ας υποθέσουμε ότι ο PC1 θέλει να στείλει ένα broadcast μήνυμα. Ο μεταγωγέας (switch) μόλις λάβει ένα μήνυμα το στέλνει σε όλες τις υπόλοιπες θύρες εκτός από αυτήν από την οποία προήλθε. Ας υποθέσουμε λοιπόν ότι το broadcast μήνυμα του PC1 φτάνει στον switch 1 και εν συνεχεία ο μεταγωγέας αυτός στέλνει μέσω της γραμμής Fa0/1 (Fast Ethernet). Όταν λάβει λοιπόν ο switch 2 από την γραμμή fa0/1 το broadcast μήνυμα, είναι υποχρεωμένος να κάνει ότι έκανε και ο switch 1 (δηλαδή να στείλει το μήνυμα προς όλες τις θύρες πλην αυτήν από την οποία προήλθε το μήνυμα). Οπότε ο Switch 2 στέλνει το broadcast μήνυμα από την γραμμή fa0/2 και καταλήγει πάλι στον Switch 1. Όπως φαίνεται και στην εικόνα 2.85 αυτό αποτελεί πρόβλημα καθότι γίνεται μια συνεχόμενη επανάληψη αποστολής μεταξύ switch 1 και switch 2 με αποτέλεσμα να έχουμε το λεγόμενο broadcast storming.



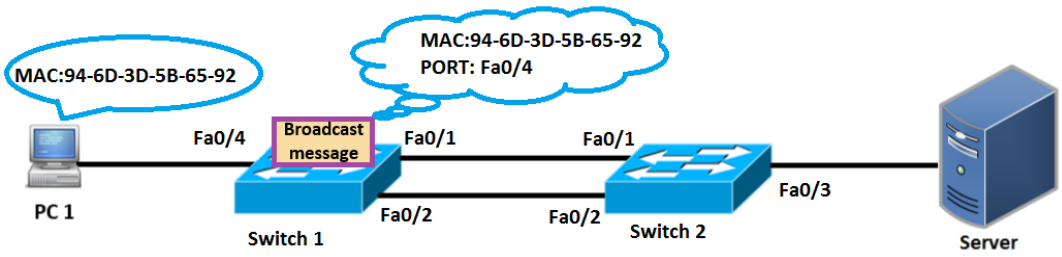
Εικόνα 2.85. Πρόβλημα broadcast storming σε ένα δίκτυο με πλεονάζουσες διαδρομές

Σε αυτό το σημείο στην εικόνα 2.85 κρατάμε την 2η περίπτωση όπου το broadcast μήνυμα έχει φτάσει στον Switch 2. Όπως παρατηρούμε ο switch 2 έχει δυο συνδέσεις διαθέσιμες την fa0/2 και την fa0/3 (η fa/0/1 δεν είναι διαθέσιμη διότι από εκεί προέρχεται το broadcast μήνυμα). Σε αυτήν την περίπτωση ο switch 1 θα στείλει δύο broadcast μηνύματα, ένα στην σύνδεση fa0/3 και ένα στην σύνδεση fa0/2. Αυτό είναι και το πρόβλημα των multiple frame copies.



Εικόνα 2.86. Πρόβλημα multiple frame copies σε ένα δίκτυο με πλεονάζουσες διαδρομές

Ας εξηγήσουμε και την τελευταία περίπτωση των MAC table instabilities. Έστω ότι ο PC 1 θέλει να στείλει πάλι ένα broadcast μήνυμα. Αυτό το μήνυμα περιέχει μια MAC διεύθυνση. Όταν φτάσει το μήνυμα στο switch 1 θα εξετάσει το μήνυμα αυτό και θα βρει την MAC διεύθυνση που περιέχει. Έτσι ο switch 1 θα ανανεώσει τον πίνακα από MAC διευθύνσεις που έχει (MAC address table) και θα προσθέσει την MAC διεύθυνση του broadcast μηνύματος στον πίνακα του μαζί με την θύρα από την οποία προήλθε που είναι η fa0/4. Η εικόνα 2.87 δίνει ένα παράδειγμα για το πώς θα φτάσει το πακέτο στον switch 1.



Εικόνα 2.87. Πληροφορία που περιέχει το broadcast μήνυμα όταν φτάσει στον switch 1

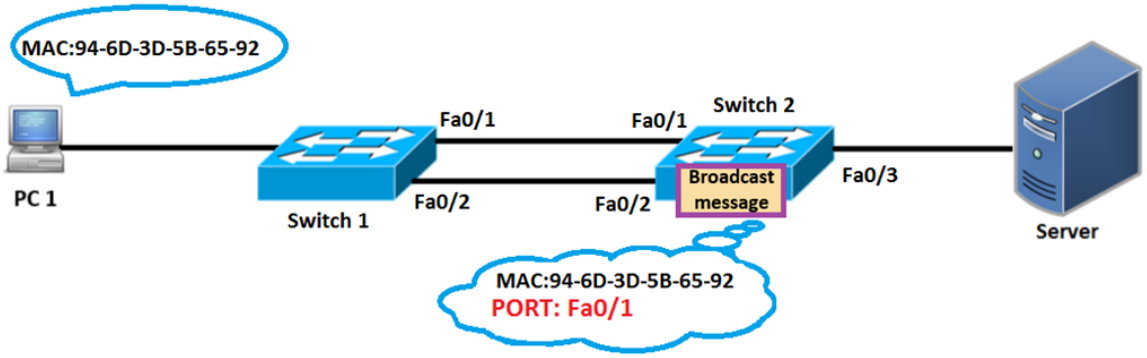
Στην εικόνα 2.87 δίνεται ένα παράδειγμα για το ποια πληροφορία θα περιέχει το broadcast μήνυμα όταν φτάσει στον switch 1. Όπως βλέπουμε ο PC1 έχει την MAC διεύθυνση 94-6D-3D-5B-65-92. Όταν λοιπόν ο PC1 στείλει ένα broadcast μήνυμα αυτό θα περιέχει την MAC διεύθυνση που έχει ο PC1 και την θύρα (port) από την οποία προήλθε δηλαδή την fa0/4. Στον πίνακα 2.9 δίνεται η ανανέωση που θα γίνει στον MAC πίνακα (MAC table) όταν αυτό φτάσει στο switch 1.

PORT	MAC ADDRESS
Fa0/4	**94-6D-3D-5B-65-92**

Πίνακας 2.9. Πληροφορία που θα καταχωρηθεί στον MAC address table του switch 1

Όταν λοιπόν φτάσει το μήνυμα στον switch τότε θα πάρει την πληροφορία από το broadcast μήνυμα και θα την καταχωρίσει στον πίνακα με τις MAC διευθύνσεις που περιέχει. Οπότε στην περίπτωση μας ο switch 1 θα πάρει την πληροφορία που έχει το broadcast μήνυμα (δηλαδή την θύρα από την οποία προήλθε και την MAC διεύθυνση του αποστολέα) και στην συνέχεια θα την καταχωρήσει στον πίνακα με τις MAC διευθύνσεις που διαθέτει. Στον πίνακα 2.9 δίνετε η πληροφορία που θα καταχωρηθεί στον MAC address table του switch 1.

Έπειτα ο switch 1 θα στείλει το broadcast μήνυμα στον switch 2 και όταν φτάσει το μήνυμα εκεί ο switch 2 θα κάνει ακριβώς την ίδια διαδικασία που έκανε και ο switch 1. Δηλαδή θα πάρει από το broadcast μήνυμα την πληροφορία και θα την καταχωρήσει στον αντίστοιχο MAC address table που διαθέτει. Η διαφορά με τον switch 1 είναι ότι εδώ θα αλλάξει η θύρα (port) και θα καταγραφεί αυτή από την οποία προήλθε το μήνυμα δηλαδή την fa0/1 και όχι την fa0/4. Στην εικόνα 2.88 δίνεται η πληροφορία η οποία περιέχεται στο broadcast μήνυμα.



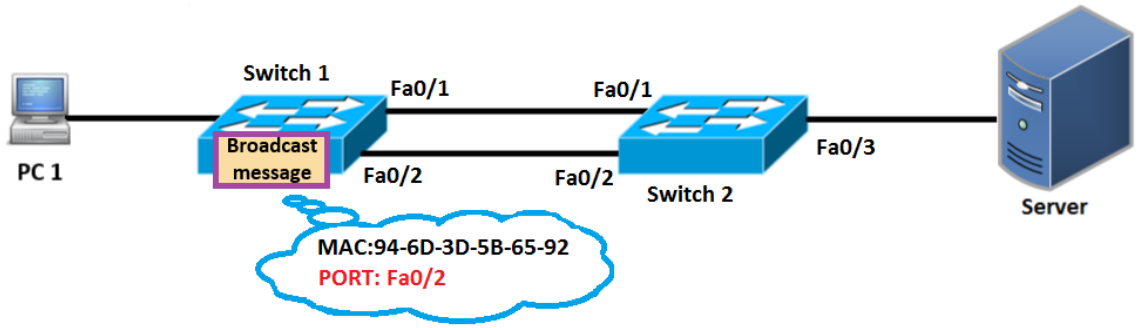
Εικόνα 2.88. Πληροφορία που περιέχει το broadcast μήνυμα όταν φτάσει στον switch 2

Οπότε η ανανέωση που θα γίνει στον MAC address table θα είναι διαφορετική από αυτήν του switch 1. Δηλαδή η θύρα θα είναι διαφορετική διότι καταχωρεί την θύρα από την οποία προήλθε το μήνυμα ενώ η MAC διεύθυνση δεν θα αλλάξει. Στον πίνακα 2.10 δίνεται η αντίστοιχη ανανέωση που θα γίνει στον πίνακα MAC address του switch 2.

PORT	MAC ADDRESS
Fa0/1	**94-6D-3D-5B-65-92**

Πίνακας 2.10. Πληροφορία που θα καταχωρηθεί στον MAC address table του switch 2

Όπως είχαμε αναφέρει προηγουμένως από την φύση του ο μεταγωγέας στέλνει σε όλες τις θύρες πλην αυτής από την οποία προήλθε το μήνυμα. Συνεπώς ο switch 2 θα ξαναστείλει το μήνυμα πίσω στον switch 1 μέσω της σύνδεσης fa0/2. Αυτό θα έχει σαν συνέπεια ο switch 1 να αλλάξει την προηγούμενη πληροφορία που καταχωρήθηκε στον MAC address table. Στον πίνακα 2.10 είχαμε πει ότι η θύρα είναι η fa0/4, επειδή όμως το μήνυμα τώρα έχει θύρα προορισμού την fa0/2 ο switch 1 θα αλλάξει την πληροφορία αυτή και θα καταχωρίσει την καινούργια που θα είναι η fa0/2. Στην εικόνα 2.88 δίνεται η πληροφορία η οποία περιέχεται στο broadcast μήνυμα.



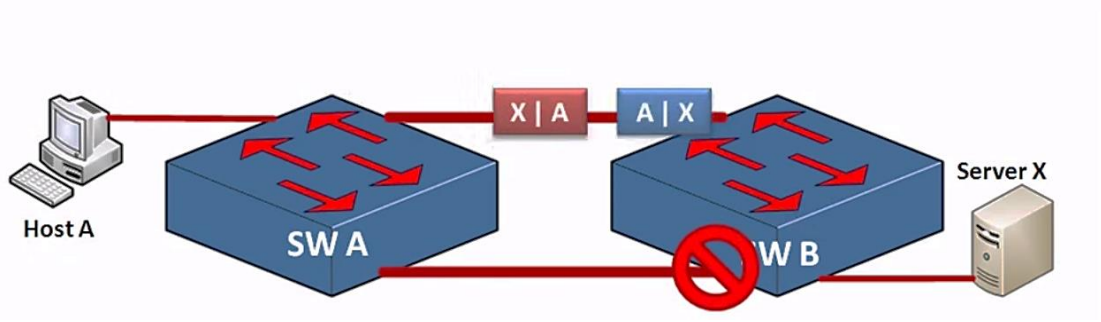
Εικόνα 2.89. Πληροφορία που περιέχει το broadcast μήνυμα όταν φτάσει ξανά στον switch 1

Οπότε η ανανέωση που θα γίνει στον MAC address table θα είναι και πάλι διαφορετική από αυτήν του switch 2. Δηλαδή η θύρα θα είναι διαφορετική διότι καταχωρεί την θύρα από την οποία προήλθε το μήνυμα ενώ η MAC διεύθυνση δεν θα αλλάξει. Στον πίνακα 2.11 δίνεται η αντίστοιχη ανανέωση που θα γίνει στον πίνακα MAC address του switch 1.

PORT	MAC ADDRESS
Fa0/1	**94-6D-3D-5B-65-92**

Πίνακας 2.11. Πληροφορία που θα καταχωρηθεί στον MAC address table του switch 1

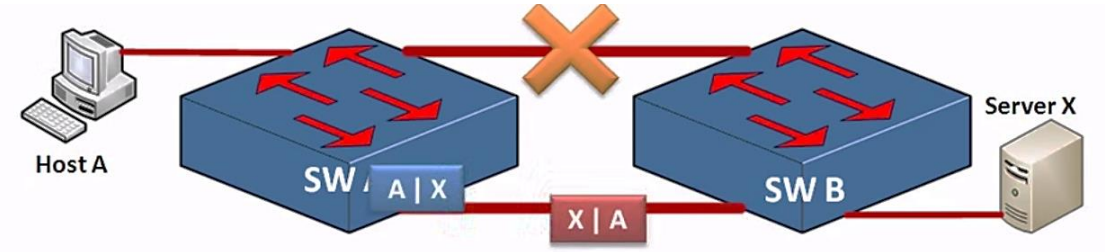
Όπως παρατηρούμε αυτό έχει σαν αποτέλεσμα την ασυνέπεια των MAC address tables σε ένα δίκτυο το οποίο διαθέτει πλεονάζουσες διαδρομές. Πρακτικά στα δίκτυα ο λόγος για τον οποίο χρησιμοποιούμε πλεονάζουσες διαδρομές είναι για εφεδρεία σε περίπτωση που η μια διαδρομή για κάποιο λόγο καταστραφεί ή παρουσιάσει κάποιο τεχνικό πρόβλημα με αποτέλεσμα να τεθεί εκτός λειτουργίας. Για να μην έχουμε λοιπόν τα παραπάνω προβλήματα εφαρμόζετε πάντα το spanning tree πρωτόκολλο που απλά μπλοκάρει τις πλεονάζουσες διαδρομές και αφήνει μόνο μια για επικοινωνία. Στην εικόνα 2.90 δίνεται ένα παράδειγμα για το πώς εφαρμόζεται το spanning tree protocol.



Εικόνα 2.90. Εφαρμογή του spanning tree protocol σε ένα δίκτυο με πλεονάζουσες διαδρομές

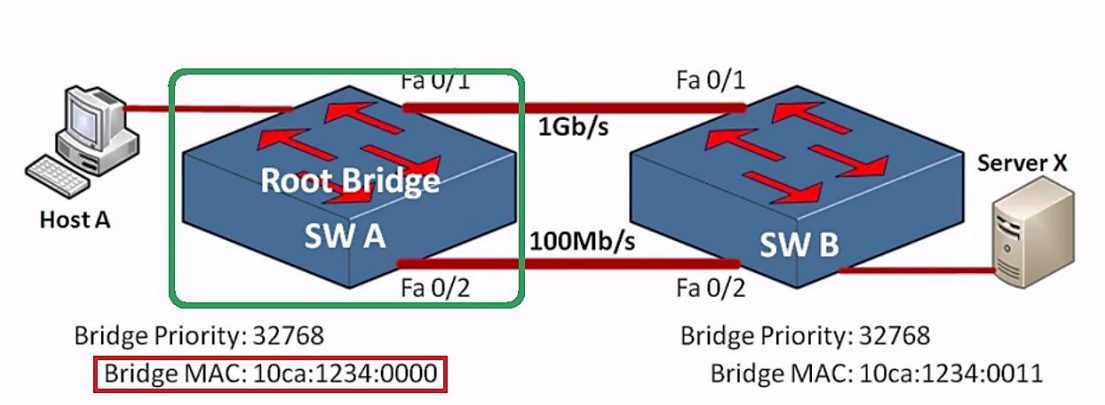
Όπως είπαμε το spanning tree protocol είναι ένα πρωτόκολλο ανοικτού προτύπου που δημιουργήθηκε προκειμένου να αποφευχθούν οι βρόγχοι (loops) σε δίκτυα με πλεονάζουσες διαδρομές. Όπως βλέπουμε στην εικόνα 2.90 αυτό που κάνει το spanning tree protocol είναι να μπλοκάρει τις πλεονάζουσες διαδρομές και να αφήνει μια από αυτές για την βασική επικοινωνία. Ενώ στην εικόνα 2.91 αν κατά την διάρκεια που οι συσκευές επικοινωνήσουν μεταξύ τους (δηλαδή οι δύο switch) και για κάποιο άγνωστο λόγο η επικοινωνία αποτύχει αυτό που θα κάνει το spanning tree protocol είναι να ξεμπλοκάρει

την ήδη μπλοκαρισμένη θύρα επικοινωνίας επιτρέποντας έτσι στις δύο αυτές συσκευές να επικοινωνήσουν μεταξύ τους από την εναλλακτική διαδρομή που ήταν πριν μπλοκαρισμένη.



Εικόνα 2.91. Εφαρμογή του spanning tree protocol σε περίπτωση που μια από τις δύο διαδρομές τεθεί εκτός λειτουργίας (π.χ. λόγω τεχνικών προβλημάτων)

Ας δούμε όμως πιο αναλυτικά με ποίον τρόπο το spanning tree protocol μπλοκάρει θύρες (ports) και επιτυγχάνει τα παραπάνω τα οποία είπαμε. Αυτό που κάνει το spanning tree protocol είναι να επιλέγει έναν switch ανάμεσα απ' όλους αυτούς που υπάρχουν στο δίκτυο για να λειτουργήσει ως σημείο αναφοράς. Η επιλογή αυτή γίνετε με βάση το priority bridge που διαθέτει ένας switch. Το ελάχιστο bridge priority είναι το 0 ενώ το μέγιστο είναι το 61440. Συνήθως είναι προεπιλεγμένο το 32768. Έστω για παράδειγμα ότι έχουμε δύο switches τον Α και τον Β αυτός που θα επιλεγεί για να λειτουργήσει ως σημείο αναφοράς θα είναι αυτός με το μικρότερο bridge priority και ονομάζεται ως root bridge.
Αλλά όπως δείχνει η εικόνα 2.91 υπάρχει και η περίπτωση να έχουμε switches όπου να διαθέτουν και οι δύο το χαμηλότερο bridge priority ανάμεσα απ' όλους τους switches που υπάρχουν στο δίκτυο. Σε αυτήν την περίπτωση εξετάζετε η φυσική MAC διεύθυνση που διαθέτουν αυτοί οι switches και θα επιλεχτεί αυτός με την μικρότερη MAC διεύθυνση. Αν για παράδειγμα έχουμε δύο switches A και B με το ίδιο bridge priority τότε θα επιλεχτεί αυτός με την μικρότερη MAC διεύθυνση. Όλες οι θύρες ενός root bridge είναι ανοιχτές για αποστολή και λήψη δεδομένων.



Εικόνα 2.92. Διαδικασία επιλογής ενός switch ως σημείο αναφοράς ανάμεσα σε δύο switches με το ίδιο bridge priority

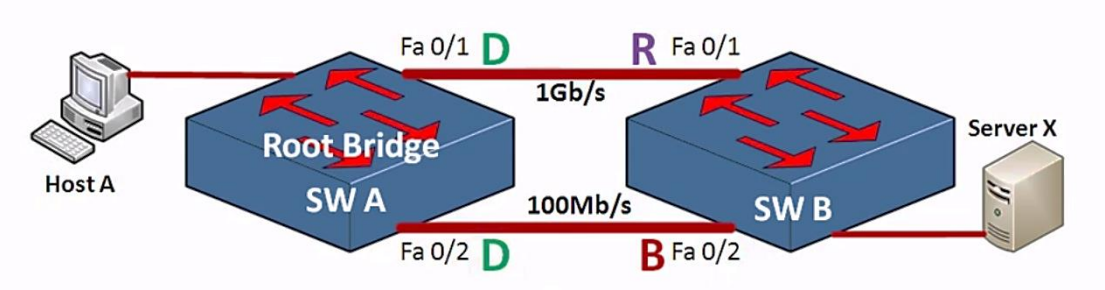
Αφού επιλεχθεί ένας switch ως σημείο αναφοράς δηλαδή αυτό που λέμε ως root bridge οποιαδήποτε άλλη διαδρομή που δεν είναι στον root bridge θα πρέπει να επιλέξει μια μοναδική διαδρομή για ανταλλαγή δεδομένων και να μπλοκάρει οποιαδήποτε άλλη διαδρομή. Για να επιλεγεί μια διαδρομή υπάρχει και ένα κόστος. Η διαδρομή με το χαμηλότερο κόστος είναι αυτή που επιλέγεται. Με τον όρο κόστος αναφερόμαστε σε

ένα πρότυπο που έχει ορίσει η IEEE. Ο πίνακας 2.12 δείχνει ενδεικτικά τα κόστη που υπάρχουν ανάλογα με την ταχύτητα που έχει μια σύνδεση.

Απόδοση ζεύξης (Bandwidth)	Κόστος που έχει οριστεί από την IEEE
10 Gbps	1
1 Gbps	2
100 Mbps	19
10 Mbps	100

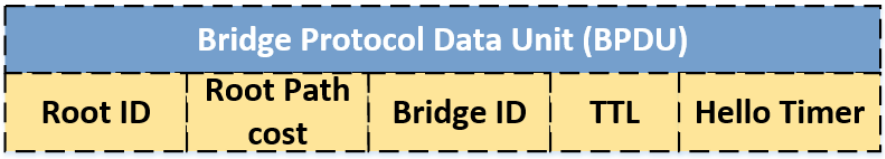
Πίνακας 2.12. Ενδεικτικά κόστη που έχουν οριστεί από τον οργανισμό IEEE

Όπως βλέπουμε από την εικόνα 2.92 η ζεύξη που θα επιλεγεί θα είναι η fa0/1 διότι με βάση τον πίνακα 2.12 είναι αυτή με το λιγότερο δυνατό κόστος. Οπότε από την ζεύξη fa0/1 μπορούν να στέλνονται και να λαμβάνονται δεδομένα για τον root bridge.



Εικόνα 2.93. Επιλογή διαδρομής με βάση το μικρότερο δυνατό κόστος

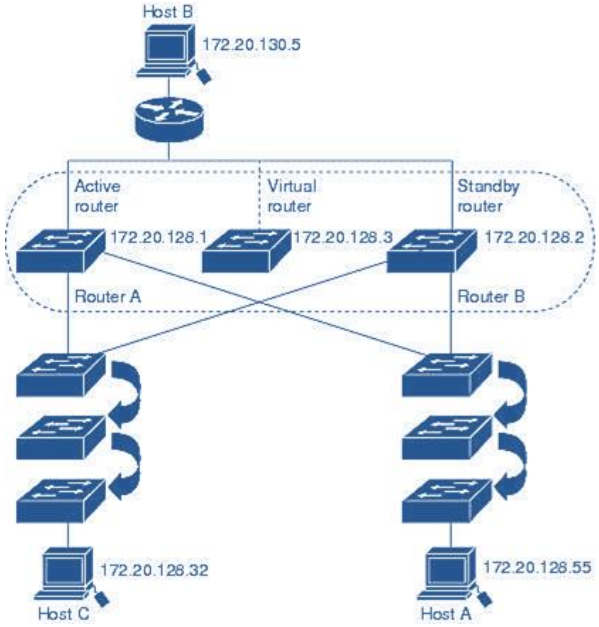
Όπως βλέπουμε στην εικόνα 2.93 στην ζεύξη fa0/1 έχουμε από την μία μεριά το D που σημαίνει ότι είναι σε θέση να στείλει δεδομένα και από την άλλη το R που σημαίνει ότι μπορεί να λάβει δεδομένα. Όμως στην ζεύξη fa0/2 έχουμε από την μια μεριά το D που όπως είπαμε είναι για αποστολή δεδομένων αλλά από την άλλη μεριά έχουμε το B που σημαίνει ότι η θύρα αυτή είναι μπλοκαρισμένη και δεν μπορεί να λάβει δεδομένα.
Για να μπορέσει το spanning tree protocol να επιβλέπει την σύνδεση και για να διαβεβαιώσει ότι δεν υπάρχει πρόβλημα στο δίκτυο χρησιμοποιεί μηνύματα BPDU (Bridge Protocol Data Unit). Ας πάρουμε για παράδειγμα το δίκτυο της εικόνας 2.93, όπου, ο switch A στέλνει ένα μήνυμα BPDU μέσω τις σύνδεσης που έχει επιλεγεί προς τον switch B και έπειτα με την σειρά του ο switch B στέλνει κι αυτός ένα επιβεβαιωτικό μήνυμα BPDU προς τον switch A. Με αυτόν τον τρόπο επιβλέπεται η σύνδεση. Τα μηνύματα BPDU στέλνονται κάθε 2 δευτερόλεπτα.



Εικόνα 2.94. Δομή ενός BPDU μηνύματος

2.8.4 Hot Standby Router Protocol – HSRP

Το πρωτόκολλο HSRP εξασφαλίζει υψηλή διαθεσιμότητα δικτύου, παρέχοντας εφεδρεία για δεδομένα IP σε δικτυακές συσκευές εντός αυτού. Δηλαδή επιτρέπει την χρήση ομάδων δύο ή περισσότερων δρομολογητών για να λειτουργήσουν ως τοπική δικτυακή πύλη (gateway). Σε μια τέτοια ομάδα, ο «ενεργός» (active) δρομολογητής είναι ένας και μοναδικός, ενώ αυτοί που είναι «σε αναμονή» (standby) αναλαμβάνουν τα καθήκοντα δρομολόγησης σε περίπτωση που ο ενεργός δρομολογητής τεθεί εκτός λειτουργίας για διάφορους λόγους (π.χ. λόγω τεχνικών προβλημάτων κλπ). Όταν το HSRP έχει ρυθμιστεί σε ένα τμήμα δικτύου, παρέχει μια φυσική εικονική MAC διεύθυνση και μια εικονική IP διεύθυνση. Αυτές τις διευθύνσεις τις μοιράζονται μεταξύ τους οι δρομολογητές που βρίσκονται στην ίδια ομάδα. Ο δρομολογητής που επιλέγεται από το πρωτόκολλο για να παίξει τον ρόλο του ενεργού δρομολογητή αναλαμβάνει να δρομολογήσει τα πακέτα που προορίζονται γι' αυτές τις διευθύνσεις MAC και IP.



Εικόνα 2.95. Παράδειγμα λειτουργίας HSRP

Το HSRP ανιχνεύει όταν ένας ενεργός δρομολογητής δυσλειτουργήσει. Σε αυτήν την περίπτωση ένας δρομολογητής που βρίσκεται σε αναμονή αναλαμβάνει τον έλεγχο της MAC και της IP διευθύνσεις της HSRP ομάδας. Οι συσκευές που χρησιμοποιούν το HSRP στέλνουν και λαμβάνουν UDP multicast πακέτα τύπου «hello» για την δρομολογητών που έχουν τεθεί εκτός λειτουργίας.

2.8.5 VLAN Trunking Protocol – VTP

Το ιδεατό τοπικό δίκτυο (virtual LAN – VLAN) είναι ένα κλειστό πρωτόκολλο της εταιρίας CISCO όπου καλύπτει την ανάγκη δημιουργίας πολλαπλών και ανεξάρτητων περιοχών καθολικής εκπομπής μεταξύ υπολογιστών, ανεξάρτητα από τη φυσική τους τοποθέτηση. Δηλαδή, πάνω στο ίδιο μέσο πολλαπλής πρόσβασης μπορούν να δημιουργηθούν πολλά VLANs ή ένα VLAN μπορεί να υπάρξει μεταξύ υπολογιστών που διασυνδέονται σε ανεξάρτητα και απομακρυσμένα φυσικά μέσα. Με τη δημιουργία VLANs επιτυγχάνουμε την ομαδοποίηση των χρηστών σε ομοειδή λειτουργικά σύνολα, ανεξάρτητα από το που βρίσκονται οι υπολογιστές τους. Το σημαντικό όφελος από αυτό το διαχωρισμό είναι η αυξημένη προστασία από κακόβουλη ή εσφαλμένη χρήση του δικτύου. Η σύσταση ενός VLAN πραγματοποιείται διαμέσου του λογισμικού των

δικτυακών συσκευών. Έτσι, είναι πολύ εύκολη η ανασύστασή του σε περιπτώσεις όπου π.χ. όταν ένας υπάλληλος αλλάζει γραφείο ή προστεθεί κάποιος νέος κόμβος.
Το πρωτόκολλο VTP χρησιμοποιείται για τη διανομή και το συγχρονισμό πληροφοριών αναγνώρισης σε VLANs τα οποία είναι διευθετημένα σε ένα δίκτυο μεταγωγής. Οι ρυθμίσεις που γίνονται σε ένα μεταγωγέα όπου βρίσκεται σε κατάσταση VTP Server διαδίδονται μέσω αυτού σε όλους τους συνδεδεμένους μεταγωγείς του δικτύου περιορίζοντας την ανάγκη διευθέτησης όλων των μεταγωγών. Το VTP μεταδίδει τα παρακάτω στοιχεία σε όλες τις trunk θύρες ενός μεταγωγέα (switch):

- Domain
- Αριθμός αναθεώρησης (Configuration revision number)
- Τις ρυθμίσεις των ιδεατών τοπικών δικτύων VLANs
- Έκδοση VTP που χρησιμοποιείται (version 1, version 2, version 3).

Το VTP βασίζεται κι αυτό στο μοντέλο του πελάτη – εξυπηρετητή (client –server) όπου ένας μεταγωγέας (switch) αναλαμβάνει τον ρόλο του εξυπηρετητή και οι υπόλοιποι μεταγωγείς (switches) αναλαμβάνουν τον ρόλο των πελατών. Οι πελάτες που βρίσκονται στο VTP domain του εξυπηρετητή ενημερώνονται από αυτόν για τα VLAN και για τυχόν αλλαγές που θα συμβούν.

Trunking και access port: Μια θύρα πρόσβασης (access port) ανήκει μονάχα σε ένα VLAN και τα πλαίσια (frames) που λαμβάνει τα τοποθετεί στο συγκεκριμένο VLAN. Από την άλλη ένα trunk, επιτρέπει μαρκαρισμένα πλαίσια (tagged frames) που έχουν πολλαπλά VLAN ID. Γενικά, μία θύρα πρόσβασης εξυπηρετεί κάποιον κόμβο του δικτύου, ενώ μία trunk εξυπηρετεί ένα uplink σε κάποιο άλλο μεταγωγέα (switch) ή ένα inter-VLAN routing interface.

2.8.6 Cisco Discovery Protocol – CDP

Το Cisco Discovery Protocol είναι ένα πρωτόκολλο του επίπεδου σύνδεσης δεδομένων το οποίο είναι ανεξάρτητο από το μέσο μεταφοράς. Χρησιμοποιείται από εφαρμογές δικτύου για να ενημερωθούν για τους γειτονικούς τους κόμβους. Κάθε συσκευή που χρησιμοποιεί το πρωτόκολλο αυτό δημοσιεύει στις γειτονικές συσκευές μια διεύθυνση στην οποία μπορεί να δεχθεί μηνύματα CDP και στέλνει περιοδικά, ενημερώσεις προς την γνωστή multicast διεύθυνση η οποία είναι 01-00-0C-CC-CC-CC. Οι συσκευές ανιχνεύουν η μία την άλλη «ακούγοντας» μηνύματα που στέλνονται σε αυτήν την διεύθυνση. Επίσης επιβλέπουν τα μηνύματα αυτά ώστε να ενημερωθούν όταν κάποιες θύρες σε γειτονικές συσκευές αλλάξουν κατάσταση. Τα μηνύματα CDP περιέχουν πληροφορίες όπως το χρονικό διάστημα στο οποίο μια συσκευή θα θεωρήσει τα στοιχεία CDP έγκυρα (Time –to –Live – TTL). Η πληροφορία που περιέχεται σε ένα μήνυμα CDP διαφέρει ανάλογα με την συσκευή και με την έκδοση CDP που χρησιμοποιείται. Ενδεικτικά, κάποιες πληροφορίες που στέλνονται είναι:

- Έκδοση IOS που χρησιμοποιείται σε Cisco συσκευές
- Υλικό-πλατφόρμα (Hardware platform) των συσκευών
- Διευθύνσεις IP σε διεπαφές των συσκευών
- Τοπικά συνδεμένες συσκευές που εφαρμόζουν το πρωτόκολλο CDP
- Ενεργές διεπαφές που υπάρχουν σε μια συσκευή cisco, περιλαμβάνοντας και τον τύπο ενθυλάκωσης
- Hostname
- Duplex setting
- VTP domain
- Native VLAN

2.9 Συμπέρασμα

Τα πρωτόκολλα αυτά λειτουργούν για την επιτυχή μετάδοση δεδομένων από ένα σημείο του δικτύου στο άλλο. Η διαδικασία μετάδοσης δεδομένων σε ένα δίκτυο περιλαμβάνει:

- ✓ Τον υπολογιστή – αφετηρία:
  Όπου μπορεί να είναι οποιοσδήποτε υπολογιστής του δικτύου.

- ✓ Το πρωτόκολλο επικοινωνίας: Όπου αποτελείται από ολοκληρωμένα κυκλώματα καθώς και από τα προγράμματα της κάρτας διασύνδεσης του δικτύου και είναι υπεύθυνο για τη λογική της επικοινωνίας του δικτύου.

- ✓ Τον μεταδότη: Όπου στέλνει ηλεκτρικά σήματα μέσα από το καλώδιο.

- ✓ Το καλώδιο μεταφοράς

- ✓ Τον δέκτη: Όπου λαμβάνει τα σήματα και τα αποκωδικοποιεί για το μηχανισμό πρωτοκόλλου.

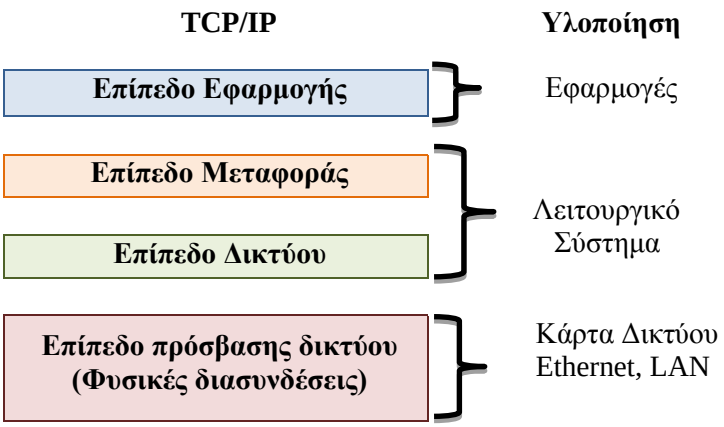
- ✓ Τον υπολογιστή – προορισμό

Η μετάδοση ξεκινά με τον υπολογιστή που στέλνει bits (δηλαδή 0 και 1) στο μηχανισμό πρωτοκόλλου. Αυτός αναλαμβάνει να δημιουργήσει πλαίσια δεδομένων που περιέχουν πεδία δεδομένων, ελέγχου και της διεύθυνσης όπου θα αποσταλούν. Στη συνέχεια, μετατρέπονται σε ηλεκτρικά σήματα και προωθούνται στο δέκτη όπου πάλι ο μηχανισμός πρωτοκόλλου αναλαμβάνει να μεταβιβάσει τα δεδομένα στον υπολογιστή - προορισμό, αφού προηγουμένως ανιχνεύσει λάθη μετάδοσης και επιβεβαιώσει την ορθή λήψη, μέσω των πεδίων ελέγχου. Από την όλη διαδικασία, γίνεται φανερό, ότι το πρωτόκολλο επικοινωνίας ελέγχει τη λογική της επικοινωνίας του δικτύου. Κάθε τύπος πρωτοκόλλου έχει πλεονεκτήματα και μειονεκτήματα, ανάλογα με τον τρόπο εγκατάστασης του δικτύου, το πλήθος των δεδομένων που μεταφέρονται, τον αριθμό των σταθμών εργασίας κλπ. Επιπλέον, το πρωτόκολλο που επιλέγεται επηρεάζει και το είδος της καλωδίωσης που μπορεί να χρησιμοποιηθεί.

2.10 Εισαγωγή στην τεχνολογία TCP/IP

Στην παράγραφο 2.4 αναφέραμε επιγραμματικά το μοντέλο επικοινωνίας TCP/IP ας δούμε όμως συνοπτικά πως αυτό λειτουργεί. Οι διαφορές δεν είναι τεράστιες καθότι το TCP/IP αναπτύχθηκε συγχρόνως με το μοντέλο αναφοράς OSI. Εδώ όμως δημιουργείται ένα ερώτημα, αφού λοιπόν το TCP/IP αναπτύχθηκε συγχρόνως με το OSI ποίος ο λόγος να το αναφέρουμε;
Ας πάρουμε για παράδειγμα ένα τοπικό δίκτυο LAN. Ένα τέτοιο δίκτυο μπορεί να αποτελείται από πολλές συσκευές που όλες αυτές βασίζονται πάνω στο μοντέλο επικοινωνίας TCP/IP. Στην παράγραφο 2.4 είδαμε ότι το TCP/IP αποτελείται μια στοίβα τεσσάρων επιπέδων (και όχι 7 όπως το OSI) όπου το κάθε επίπεδο περιέχει τα δικά του πρωτόκολλα επικοινωνίας. Στην παράγραφο 2.4 είδαμε κάποια από αυτά τα πρωτόκολλα και πως αυτά ορίζουν τους κανόνες επικοινωνίας. Οπότε σκοπός της στοίβας TCP/IP είναι η επίτευξη μεταφοράς δεδομένων στο μέσο μετάδοσης. Στην ουσία δεν εφαρμόζει ένα συνδυασμό των δύο πρωτόκολλων (TCP και IP) αλλά αποτελεί ένα σύνολο πολλών πρωτοκόλλων. Ο όρος αυτός δεν περιορίζεται μόνο εκεί αλλά και για την αναφορά σε ομάδες που κάνουν χρήση παρόμοιων πρωτοκόλλων για την επίτευξη επικοινωνίας μεταξύ υπολογιστών.
Η ονομασία αυτή προέκυψε εξαιτίας του ότι τα πρωτόκολλα TCP και IP είναι αρκετά δημοφιλή. Χάρης την επαρκή διαθεσιμότητα των εν λόγω πρωτοκόλλων αλλά για την ανάγκη επικράτησης ενός και μόνο κοινού επικοινωνιακού προτύπου οδήγησαν στους παράγοντες που συνέβαλλαν στην επιτυχία τους. Αυτό είχε ως αποτέλεσμα την υιοθέτηση των πρωτοκόλλων TCP/IP από την

πλειοψηφία των κατασκευαστών με άμεσο σκοπό την επίτευξη διαλειτουργικότητας μεταξύ συσκευών που προέρχονται από διαφορετικούς κατασκευαστές. Συνεπώς, ένα δίκτυο που αποτελείται από υλικό (hardware) διαφορετικών κατασκευαστών, χαρακτηριστικών αλλά και λειτουργικών συστημάτων μπορούν κάλλιστα να επικοινωνήσουν και να λειτουργήσουν με τα ιδία πρωτόκολλα δικτύου.



Σχήμα 2.3: Απεικόνιση του μοντέλου TCP/IP.

Επίπεδο		Λειτουργία	Πρωτόκολλα
L4	Εφαρμογής	Υποστηρίζει δικτυακές εφαρμογές **Μήνυμα (message)**	HTTP, HTTPS, SMTP, POP3, IMAP, DNS, DHCP, SSH,TELNET
L3	Μεταφοράς	Μεταφορά δεδομένων μεταξύ τερματικών **Τμήμα (Segment)**	TCP, UDP. RTP
L2	Δικτύου	Δρομολόγηση datagrams απ' την πηγή στον προορισμό. **Πακέτο (Datagram)**	IPv.4, IPv.6, ICMP, ARP
L1	Επίπεδο πρόσβασης δικτύου (Φυσικές διασυνδέσεις)	Μεταφορά δεδομένων και bits μεταξύ γειτονικών κόμβων. **Πλαίσιο (Frame)**	Ethernet, STP, HSRP, VLAN, VTP, CDP, PPP, DSL

Σχήμα 2.4: Στοίβα πρωτοκόλλων του μοντέλου TCP/IP.

2.10.1 Επίπεδο Εφαρμογής

Παρέχει εφαρμογές, που χρησιμοποιούν τα πρωτόκολλα του επιπέδου μεταφοράς, όπως μεταφορά αρχείων, απομακρυσμένη σύνδεση και ηλεκτρονικού ταχυδρομείου. Αυτό το επίπεδο αποτελεί το σημείο διεπαφής του χρήστη με τη στοίβα πρωτοκόλλων της τεχνολογίας TCP/IP

2.10.2 Επίπεδο Μεταφοράς

Υλοποιεί τις συνδέσεις μεταξύ των υπολογιστών συσκευών σε ένα δίκτυο. Το βασικό πρωτόκολλο του είναι το TCP, που:

- ✓ φροντίζει για την αποκατάσταση πιθανών σφαλμάτων (αξιόπιστες συνδέσεις)
- ✓ επιτρέπει την ταυτόχρονη εγκατάσταση συνδέσεων και στέλνει τα δεδομένα της κάθε σύνδεσης ταυτόχρονα, αλλά ανεξάρτητα από τις άλλες συνδέσεις (ταυτόχρονες συνδέσεις). Κάθε σύνδεση μπορεί να στέλνει, αλλά και να λαμβάνει δεδομένα (δικατευθυντήριες συνδέσεις)

Επίσης υπάρχει και το πρωτόκολλο UDP όπου είναι πρωτόκολλο χωρίς σύνδεση, χρησιμοποιείται για ειδικούς σκοπούς, για εφαρμογές που δεν απαιτούν αξιοπιστία.

2.10.3 Επίπεδο Δικτύου

Αναλαμβάνει την μετάδοση και δρομολόγηση των πακέτων TCP (segment) ή UDP (datagram) στο δίκτυο. Το βασικό πρωτόκολλο του είναι το IP, που:

- ✓ εξασφαλίζει στο σύστημα την παγκόσμια συνδεσιμότητα
- ✓ φροντίζει για την παροχή λογικών διευθύνσεων στα σημεία διεπαφής του με το φυσικό δίκτυο

Υπάρχει επίσης και το πρωτόκολλο ICMP που είναι υπεύθυνο για τον έλεγχο και τη δημιουργία μηνυμάτων, που δηλώνουν την κατάσταση των συσκευών σε ένα δίκτυο.

2.10.4 Επίπεδο πρόσβασης δικτύου (Φυσικές διασυνδέσεις)

Παρέχει πρόσβαση στο φυσικό μέσο, στο οποίο διαδίδεται η πληροφορία με μορφή πακέτων Αποτελεί το χαμηλότερο λογικό επίπεδο λειτουργικότητας, που απαιτείται από ένα δίκτυο και περιλαμβάνει στοιχεία των φυσικών συνδέσεων, όπως:

- ✓ καλώδια,
- ✓ αναμεταδότες,
- ✓ κάρτες δικτύου,
- ✓ πρωτόκολλα πρόσβασης τοπικών δικτύων

Προσφέρει τις υπηρεσίες του στο ανώτερο επίπεδο, το επίπεδο δικτύου. Παρέχει τις φυσικές διευθύνσεις (Physical Address) τις οποίες αντιστοιχεί με λογικές διευθύνσεις (διευθύνσεις internet, IP), χρησιμοποιώντας τα πρωτόκολλα Μετατροπής διευθύνσεων (ARP, Address Resolution Protocol) και Ανάστροφης Μετατροπής διευθύνσεων (RARP, Reverse Address Resolution Protocol) – Επίπεδο MAC, Media Access Control του OSI.

2.11 Παράμετροι επικοινωνίας TCP/IP

Υπάρχουν τέσσερις παράμετροι για να επιτευχθεί μια TCP/IP επικοινωνία:

1) Διεύθυνση IP (IP Address)
2) Μάσκα υποδικτύου (subnet mask)
3) DNS Server
4) IP gateway

2.11.1 Διευθυνσιοδότηση IP

Είναι η δημιουργία ενός δικτύου ή ακόμα και η σύνδεση σε ήδη υπάρχοντα δίκτυα που απαιτούν την ύπαρξη κάποιου τρόπου διαχωρισμού των υπολογιστών μεταξύ τους. Αυτό λοιπόν πραγματοποιείτε με έναν μοναδικό αριθμό που ονομάζεται IP διεύθυνση. Οι αριθμοί αυτοί ονομάζονται διευθύνσεις και έχουν μήκος 32 bits.
Συχνά παρουσιάζεται με τη μορφή 4 δεκαδικών αριθμών (ένας για κάθε 8 bit) χωρισμένους με τελείες.

Η **διεπαφή (interface)** είναι το σημείο εφαρμογής μεταξύ του τερματικού/ δρομολογητή και της ζεύξης.

- Κάθε διεπαφή έχει μια διεύθυνση IP
- Οι δρομολογητές έχουν συνήθως πολλές διεπαφές
- Ένα τερματικό έχει συνήθως μια διεπαφή

Από το 1981 έως και το 1993 οι IP διευθύνσεις ήταν χωρισμένες σε κλάσεις (τάξεις διευθύνσεων IP). Από το 1993 και μετά δημιουργήθηκε η αταξική δρομολόγηση δικτυακών περιοχών (Classless Inter-Domain Routing, CIDR).

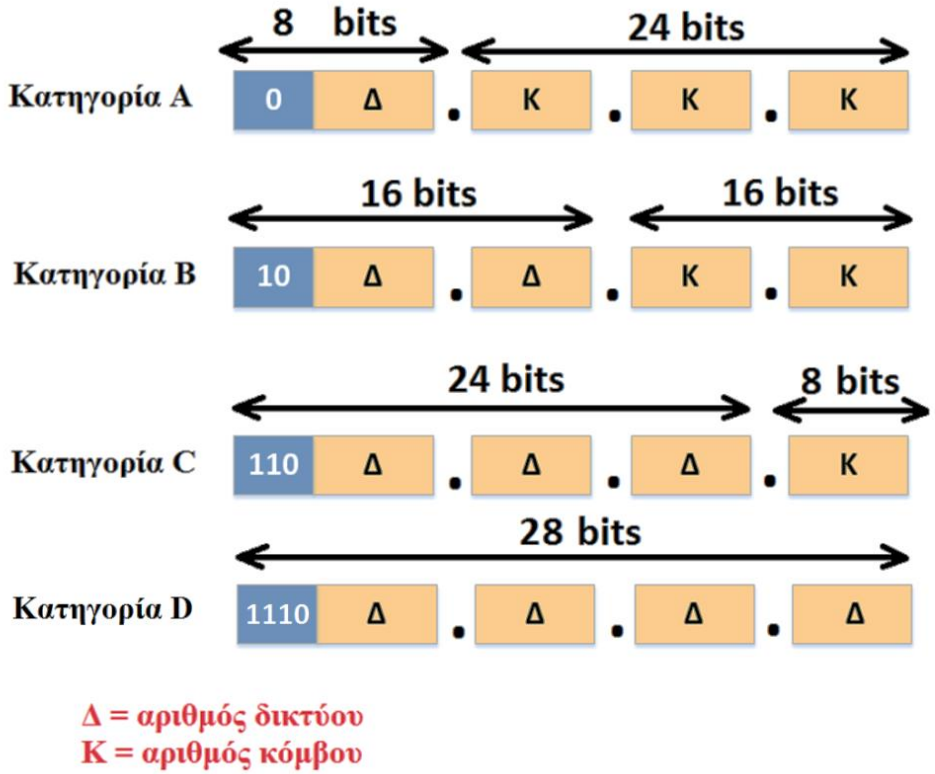
2.11.2 Τάξεις διευθύνσεων IP (1981 – 1993)

Όπως είπαμε, στην υποπαράγραφο 2.7.1 όταν αναφερόμαστε σε τάξεις διευθύνσεων IP μιλάμε για δίκτυα τα οποία χωρίζονται σε τάξεις με βάση τον τρόπο με τον οποίο κατανέμουν τα bits μιας IP διεύθυνσης σε κάθε πεδίο.
Έχουμε λοιπόν πέντε κατηγορίες διευθύνσεων την A, B, C, D και E. Οι A, B και C είναι διαθέσιμες για διανομή και εμπορική χρήση. Η κατηγορία D χρησιμοποιείται για την υλοποίηση ενός αποδοτικού συστήματος αποστολής των ίδιων δεδομένων σε πολλαπλούς παραλήπτες (multicasting). Η κατηγορία E έχει δεσμευτεί για πειραματικές προσπάθειες. Τα πρώτα bits της κάθε διεύθυνσης υποδεικνύουν την κατηγορία στην οποία ανήκει.

- Η κατηγορία A, έχει το πρώτο της bit ίσο με 0, ο αριθμός του δικτύου έχει εύρος 8 bits και ο αριθμός κόμβου 24 bits.

- Η κατηγόρια B, ξεκινάει με 10, ενώ τόσο ο αριθμός δικτύου όσο και ο αριθμός κόμβου της έχουν εύρος 16 bits.

- Η κατηγορία C, ξεκινάει με 110 με εύρος αριθμού δικτύου 24 bits και εύρος αριθμού κόμβου 8 bits



Εικόνα 2.96: Κλάσεις IP διευθύνσεων

Κατηγορία	Τιμές των πρώτων bits	Περιοχή διευθύνσεων	Πλήθος bits δικτύου/κομβου	Μέγιστο πλήθος δικτύων	Μέγιστο πλήθος κόμβων ανά δίκτυο
A	0	1.0.0.0 – 127.255.255.255	7/24	126 (2^7 - 2)	16.777.214 (2^{24}-2)
B	10	128.0.0.0 – 191.255.255.255	14/16	16384 (2^{14})	65.534 (2^8 - 2)
C	110	192.0.0.0 – 223.255.255.255	21/8	2.097.152 (2^{21})	254 (2^8 - 2)
D	1110	224.0.0.0 – 239.255.255.255	–	–	–
E	1111	240.0.0.0 – 254.255.255.255	–	–	–

Πίνακας 2.13. Αναλυτικός πίνακας από κλάσεις IP διευθύνσεων

Παρατήρηση: Στο μέγιστο πλήθος κόμβων ανά δίκτυο αφαιρείται ο αριθμός 2, αυτό συμβαίνει διότι η διεύθυνση με 0 σε όλο το τμήμα του κόμβου (host) είναι δεσμευμένη σαν Network address αλλά και η διεύθυνση με 1 σε όλο το τμήμα του κόμβου (host) είναι δεσμευμένη σαν broadcast address.

Υπάρχουν 3 σύνολα IP διευθύνσεων δεσμευμένα για ιδιωτική χρήση:

- Class A: 10.0.0.0 - 10.255.255.255
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0 – 192.168.255.255

Επίσης το δίκτυο 127.0.0.0 είναι δεσμευμένο για δοκιμές και διαδικασίες loopback. Με αυτό τον τρόπο διευθυνσιοδότησης έχουμε το εξής μειονέκτημα:
Αν για παράδειγμα κάποιο δίκτυο θέλει να καλύψει 254 κόμβους, τότε θα του δοθεί διεύθυνση κατηγορίας C. Αν θελήσει όμως να καλύψει 270 κόμβους θα του δοθεί διεύθυνση κατηγορίας B (η οποία καλύπτει μέχρι 65534 κόμβους). Άρα 65534-270 =65264 διευθύνσεις θα μείνουν ανεκμετάλλευτες πράγμα που οδηγεί σε ανώφελη σπατάλη διευθύνσεων.

2.11.3 Αταξική δρομολόγηση δικτυακών περιοχών (Classless Inter-Domain Routing – CIDR)

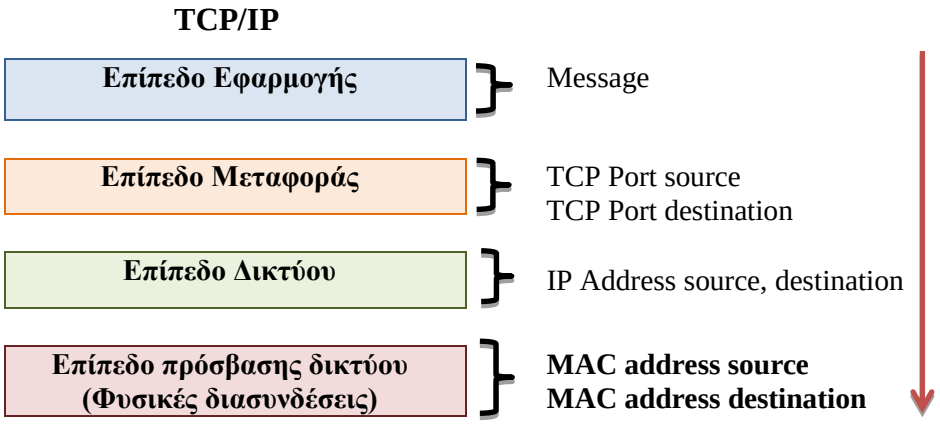
Η ραγδαία ανάπτυξη του διαδικτύου που σημειώθηκε τα τελευταία χρόνια είχε ως αποτέλεσμα ως αποτέλεσμα να προκύψουν τα πρώτα προβλήματα λόγω του πεπερασμένου χώρου διευθύνσεων. Η εκθετική αύξηση των διασυνδεδεμένων δικτύων στο διαδίκτυο συντέλεσε αφενός στην μείωση του ελεύθερου διαθέσιμου χώρου διευθύνσεων και αφετέρου στην αύξηση του μεγέθους των πινάκων δρομολόγησης. Το σημαντικότερο όμως πρόβλημα ήταν η υπερβολική σπατάλη IP διευθύνσεων δηλαδή αν για παράδειγμα ένας οργανισμός ήθελε περισσότερες από 256 IP διευθύνσεις τότε έπρεπε να πάρει διεύθυνση κλάσης B που υποστήριζε 65,536 διευθύνσεις. Προκειμένου λοιπόν να αντιμετωπιστούν αυτά τα προβλήματα προτάθηκε η **αταξική δρομολόγηση δικτυακών περιοχών (Classless Inter-Domain Routing – CIDR)**.
Το σύστημα CIDR καταργεί τις κλάσεις διευθύνσεων, με αποτέλεσμα τα τμήματα δικτύου και υπολογιστή κάθε διεύθυνσης να καθορίζονται κατά περίπτωση με βάση των αναγκών που έχει ο εκάστοτε οργανισμός. Το μέγεθος των τμημάτων δικτύου και υπολογιστή προσδιορίζονται από έναν αριθμό που ονομάζεται πρόθεμα. Για παράδειγμα έστω ότι έχουμε την διεύθυνση 192.168.30.4 /24 το /24 είναι το πρόθεμα του δικτύου και σημαίνει ότι τα πρώτα 24 bits της διεύθυνσης χρησιμοποιούνται για τον προσδιορισμό του δικτύου ενώ τα υπόλοιπα 8 bits για τον προσδιορισμό του υπολογιστή.

Εικόνα 2.97: Παράδειγμα εύρεσης προθέματος – CIDR σε μια IP διεύθυνση

Το σύστημα CIDR επιτρέπει την ανάθεση μεγάλων και συνεχόμενων περιοχών αριθμών σε αυτούς που παρέχουν υπηρεσίες διαδικτύου (Internet Service Providers – ISPs) οι οποίοι είναι υπεύθυνοι για την ανάθεση μικρότερων υποσυνόλων αριθμών στους πελάτες τους, ανάλογα με τις ανάγκες του καθενός Με αυτόν τον τρόπο, επιτυγχάνεται η ομαδοποίηση των διευθύνσεων, που εξυπηρετούνται από τον ίδιο τον ISP. Η ομαδοποίηση αυτή επιτρέπει την δρομολόγηση της κίνησης προς τον σωστό προορισμό, διατηρώντας μόνο μια εγγραφή για όλους τους προορισμούς/διευθύνσεις, ποτ εξυπηρετούνται από τον ίδιο τον ISP.

2.12 Ενθυλάκωση/ Αποθυλάκωση Πακέτου

Όπως αναφέραμε το TCP/IP χωρίζει την πληροφορία ανά επίπεδα όπου το κάθε επίπεδο επιτελεί την δική του λειτουργία και επικοινωνεί με το αμέσως επόμενο. Κάθε επίπεδο περιέχει την δική του πληροφορία που είναι:



Σχήμα 2.5: Πληροφορία ανά επίπεδο στο μοντέλο TCP/IP

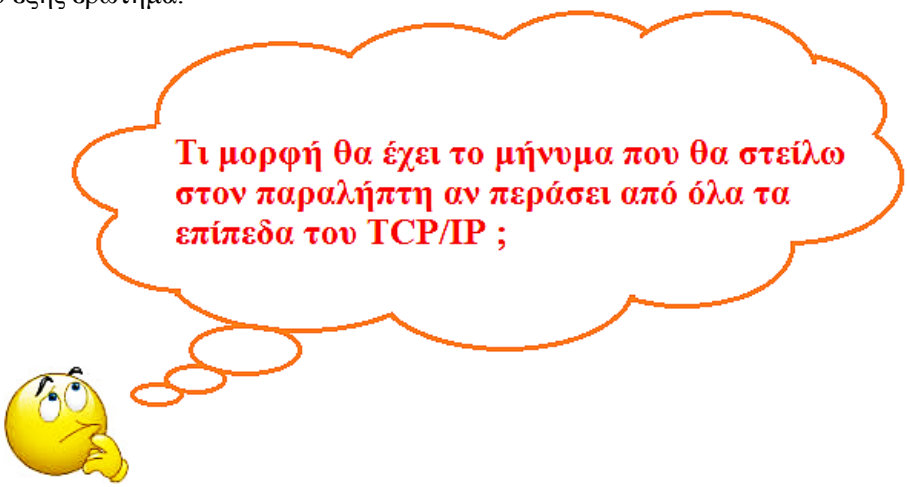
Όπως είδαμε παραπάνω το TCP/IP έχει 4 επίπεδα όπου κάθε επίπεδο προσθέτει και από μια επικεφαλίδα (header) στο πακέτο. Για παράδειγμα έστω ότι έχουμε ένα μήνυμα το οποίο θέλουμε να σταλεί στην άλλη πλευρά του δικτύου. Για να στείλουμε λοιπόν το μήνυμα αυτό θα πρέπει να βάλουμε τα στοιχεία του παραλήπτη και του αποστολέα.

Αναγνωριστικά
Αποστολέα
Παραλήπτη

Συνεπώς χρειαζόμαστε δύο χαρακτηριστικά:

- Του δικτύου (TCP Ports)
- Του κόμβου (IP Διεύθυνση)

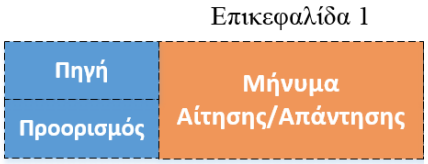
Με βάση λοιπόν τα προηγούμενα που είπαμε για την διαδικασία ενθυλάκωσης μπορούμε να θέσουμε το εξής ερώτημα.



Ας δούμε αυτό το βήμα αναλυτικά σε κάθε επίπεδο.

2.12.1 Επίπεδο Εφαρμογής

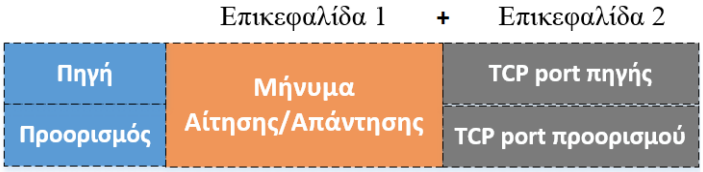
Στο επίπεδο εφαρμογής το πακέτο θα βρίσκεται στο αρχικό στάδιο στο οποίο θα έχει μόνο την πρώτη επικεφαλίδα (header 1). Οπότε το πακέτο θα έχει την παρακάτω μορφή:



Σχήμα 2.6: Δομή πακέτου στο επίπεδο εφαρμογής

2.12.2 Επίπεδο Μεταφοράς

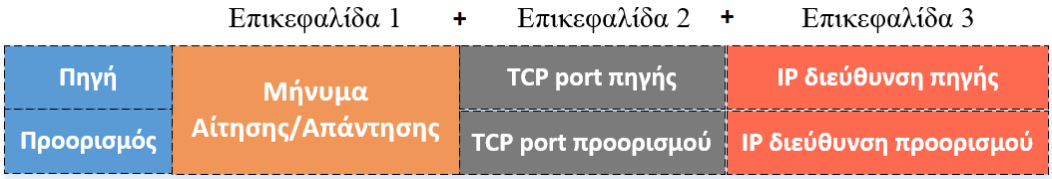
Στο επίπεδο μεταφοράς θα προστεθεί σε αυτό το η δεύτερη επικεφαλίδα που έχει να κάνει με τις θύρες (TCP Ports) στις οποίες απευθύνεται το πακέτο. Οπότε το πακέτο θα έχει την παρακάτω μορφή:



Σχήμα 2.7: Δομή πακέτου στο επίπεδο μεταφοράς

2.12.3 Επίπεδο Δικτύου

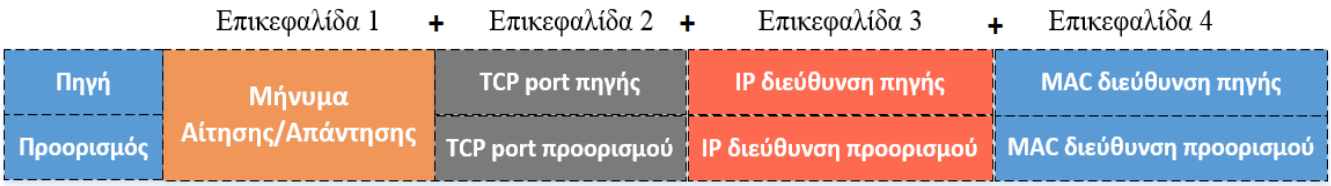
Στο επίπεδο δικτύου θα έχει προστεθεί στο πακέτο και η επικεφαλίδα 3 που περιέχει το επίπεδο δικτύου που αφορά τις IP διευθύνσεις πηγής και προορισμού.



Σχήμα 2.8: Δομή πακέτου στο επίπεδο δικτύου

2.12.4 Επίπεδο πρόσβασης δικτύου (Φυσικές διασυνδέσεις)

Στο επίπεδο αυτό θα προστεθεί στο πακέτο και η τελική επικεφαλίδα που περιέχει την MAC διεύθυνση πηγής και προορισμού.

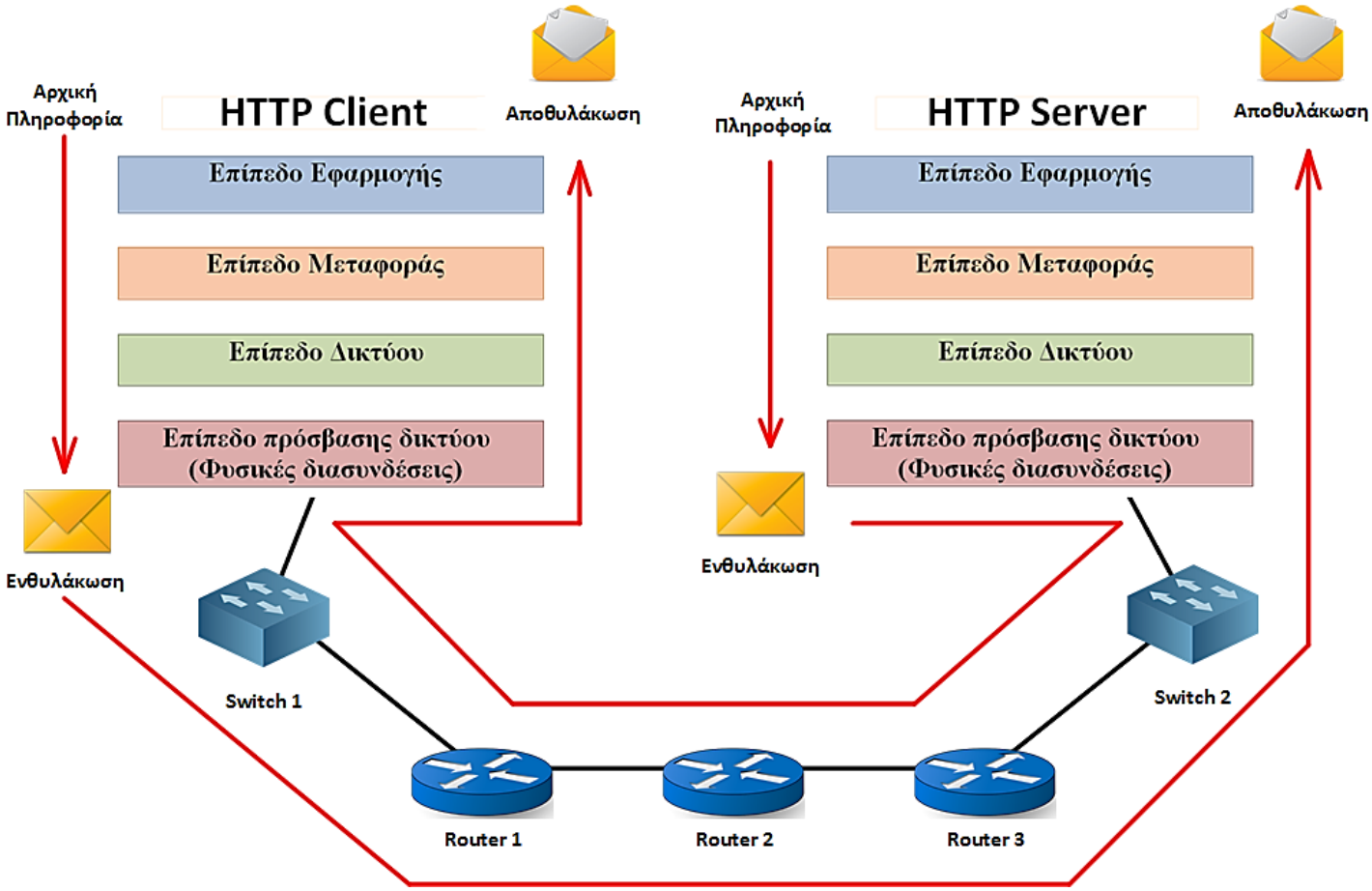


Σχήμα 2.9: Δομή πακέτου στο επίπεδο πρόσβασης δικτύου (Φυσικές διασυνδέσεις)

Οπότε το μήνυμα που θέλουμε να στείλουμε στον παραλήπτη έχει περάσει απ' όλα τα επίπεδα του TCP/IP. Αυτό ονομάζεται **Ενθυλάκωση** και η αντίστροφη διαδικασία (δηλαδή η αφαίρεση όλων των headers) ονομάζεται **Αποθυλάκωση**

Ας πάρουμε τώρα ένα παράδειγμα δικτύου που έχει έναν client και έναν server. Πως εφαρμόζεται το μοντέλο αυτό στο TCP/IP ;

Στην εικόνα 2.98 απεικονίζεται η διαδικασία που στέλνεται η πληροφορία μεταξύ δύο τερματικών (hosts) client – server. Η πληροφορία περνάει απ' όλα τα επίπεδα του TCP/IP (από το χαμηλότερο προς το ανώτερο) ώστε να γίνει η ενθυλάκωση του μηνύματος και να σταλθεί στον παραλήπτη. Την ίδια διαδικασία αναλαμβάνει και ο παραλήπτης όταν θα στείλει κι αυτός με την σειρά του ένα μήνυμα.



Εικόνα 2.98: Διαδικασία αποστολής πληροφορίας σε εφαρμογή client – server

2.13 Μέσα Μετάδοσης (Φυσικές ζεύξεις)

Εισαγωγή

Με τον όρο ενός φυσικού μέσου μετάδοσης αναφερόμαστε στην φυσική σύνδεση που δημιουργείται μεταξύ του αποστολέα και του παραλήπτη σε ένα οποιοδήποτε σύστημα επικοινωνίας. Με λίγα λόγια μπορούμε να θεωρήσουμε ότι είναι ο δρόμος μέσα απ' τον οποίο περνάει το σήμα, που στέλνει ο πομπός, έως ότου το λάβει ο δέκτης. Ο καπνός, η φωτιά, οι συνθηματικές τυμπανοκρουσίες και η ανάκλαση ηλιακών ακτινών πάνω σε γυάλινες επιφάνειες είναι μερικά από τα μέσα μετάδοσης, που χρησιμοποιήθηκαν από τους αρχαίους λαούς για τη μεταβίβαση προσυμφωνημένων μηνυμάτων.

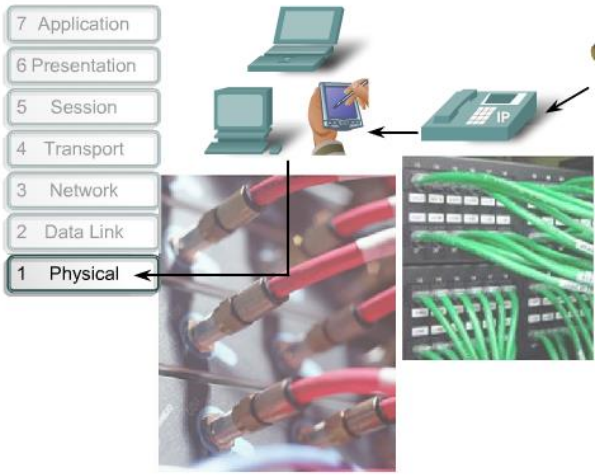
Ιστορικό σημείωμα

Στην τραγωδία «Αγαμέμνων» του Αισχύλου αναφέρετε, ότι η άλωση της Τροίας έγινε γνωστή στις Μυκήνες με σειρές από φωτιές, που άναβαν διαδοχικά στις βουνοκορφές της Λήμνου, του Άγιου Όρους, της Εύβοιας και της Στερεάς Ελλάδας έως την Πελοπόννησο. Η μετάδοση μηνυμάτων με φωτιές είχε συστηματοποιηθεί για κυρίως στρατιωτικούς σκοπούς. Οι φρυκτωρίες αποτελούν ένα τέτοιο παράδειγμα όπου ήταν το βασικό μέσο επικοινωνίας στις στρατιωτικές επιχειρήσεις όπως για παράδειγμα στις εκστρατείες του μέγα Αλέξανδρου.

Τα φυσικά μέσα μετάδοσης χωρίζονται σε **ενσύρματα** όπου εδώ το μέσο μετάδοσης είναι το καλώδιο και τα **ασύρματα** όπου εδώ το μέσο μετάδοσης είναι ο αέρας. Στα ενσύρματα μέσα μετάδοσης έχουμε τα εξής καλώδια: τα **χάλκινα**, τα **ομοαξονικά καλώδια** και τις **οπτικές ίνες** και στα ασύρματα έχουμε τις εξής τεχνικές διάδοσης: οι **επίγειες** και **δορυφορικές μικροκυματικές ζεύξεις**. Τα τελευταία χρόνια με την εξέλιξη της τεχνολογίας χρησιμοποιούνται για τη μετάδοση δεδομένων και τα συστήματα κυψελοειδούς τηλεφωνίας.

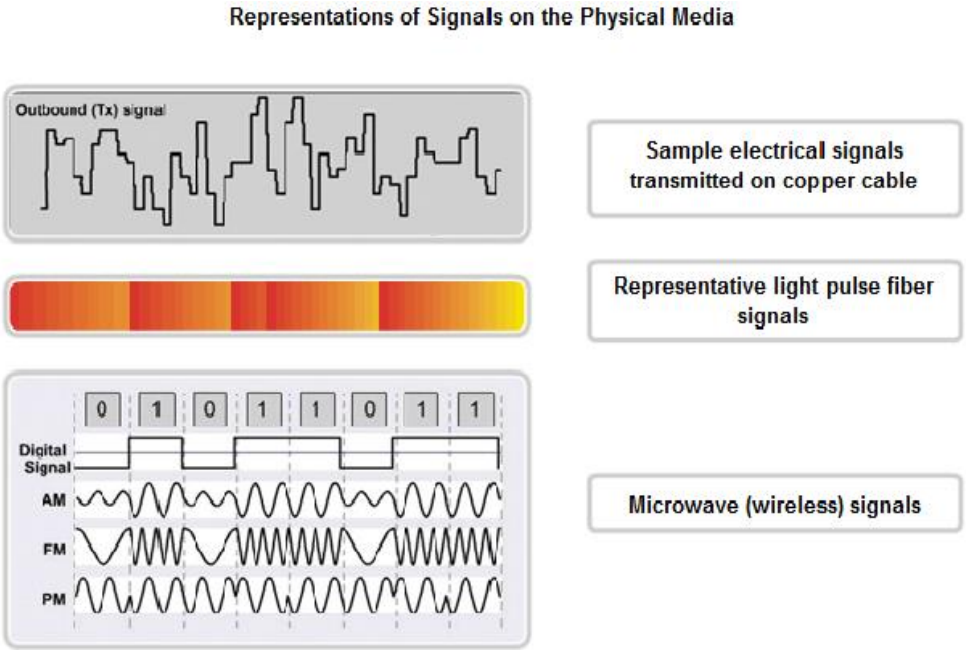
2.13.1 Το bit και η μορφή του

Τα bits είναι ηλεκτρικοί παλμοί οι οποίοι αναπαρίστανται με 0 και 1, είναι δηλαδή η γλώσσα με την οποία επικοινωνούν οι υπολογιστές. Ανήκουν στο φυσικό επίπεδο και κατά συνέπεια και στην κάρτα δικτύου.



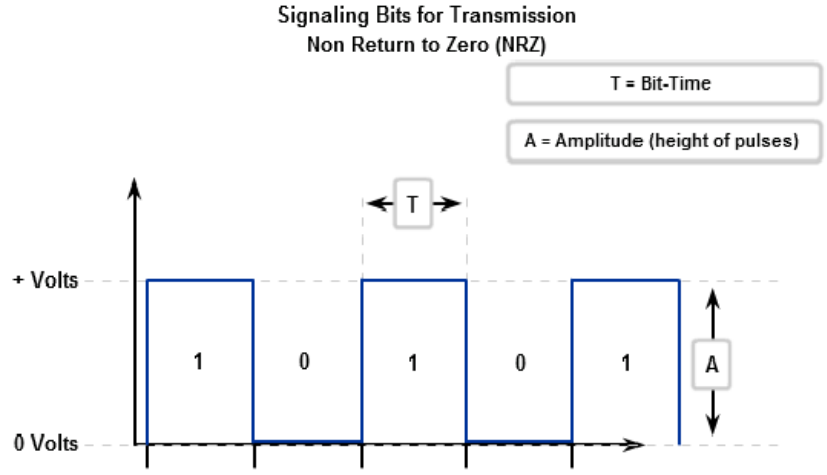
Εικόνα 2.99: Αναπαράσταση του φυσικού επιπέδου του μοντέλου OSI

Για να κατανοήσουμε καλύτερα πως αναπαρίστανται τα bits μπορούμε να παρατηρήσουμε την εικόνα 2.100. Στο πρώτο πλαίσιο απεικονίζονται τα bits τα οποία μεταδίδονται σε ένα καλώδιο όπως θα τα βλέπαμε σε ένα παλμογράφο. Στο δεύτερο πλαίσιο έχουμε τους παλμούς φωτός πάνω σε μια οπτική ίνα και στο τρίτο πλαίσιο παρατηρούμε τις διάφορες αναπαραστάσεις για το 0 και το 1 σε μικροκύματα. Τα μικροκύματα τα βρίσκουμε στη μετάδοση μιας ασύρματης κάρτας δικτύου ή ενός ασύρματου router. Στο φυσικό επίπεδο , πάνω δηλαδή στη κάρτα δικτύου διαμορφώνεται το bit. Και λέγοντας διαμόρφωση εννοούμε, το πλάτος σε βολτ τη διάρκειά του κλπ.



Εικόνα 2.100: Απεικόνιση των bits με την βοήθεια ψηφιακών μέσων

Επίσης ένα πιο κατανοητό γράφημα για την μορφή με την οποία απεικονίζονται το 0 και το 1 (δηλαδή τα bits) είναι η εικόνα 2.101 όπου παρατηρούμε ότι όταν πλάτος ισούται με 1 τότε η τάση των volts αυξάνεται και κατά συνέπεια το πλάτος (amplitude) ενώ όταν είναι ίσο με μηδέν τότε έχουμε μηδενική τάση άρα και μηδενικό πλάτος.



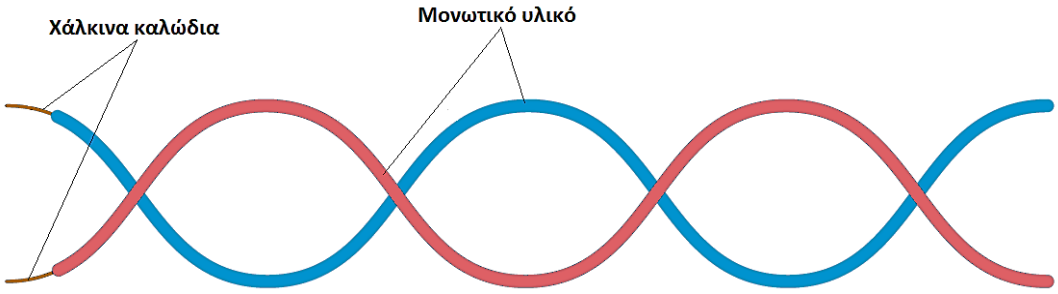
Εικόνα 2.101: Απεικόνιση των bits με τετραγωνικό παλμό

2.13.2 Ενσύρματα μέσα μετάδοσης

Τα ενσύρματα μέσα μετάδοσης είχαν ευρεία εφαρμογή στον τομέα των τηλεπικοινωνιακών δικτύων, μέχρι που έκαναν την εμφάνιση τους τα επίγεια και δορυφορικά μικροκυματικά συστήματα μετάδοσης. Παλαιότερα, το δισύρματο καλώδιο ήταν το μοναδικό μέσο για τη μετάδοση πληροφορίας. Αυτό είχε σαν αποτέλεσμα οι πρώτες γραμμές μεταφοράς να ήταν απλά χάλκινα σύρματα χωρίς μόνωση, στηριγμένα σε μονωτήρες πορσελάνης πάνω σε ξύλινους στύλους. Με την ραγδαία αύξηση των γραμμών, ήταν απαραίτητη η συγκέντρωση τούς σε δέσμες με συνέπεια τη δημιουργία των καλωδίων. Στα καλώδια οι γραμμές είναι κατάλληλα διαμορφωμένες (πλεγμένες μεταξύ τους), για να αποφεύγονται οι συνακροάσεις και προστατεύονται από εξωτερικές κακώσεις από ένα σκληρό, πλαστικό συνήθως, μανδύα. Ο μανδύας αυτός παρέχει και εξωτερική μόνωση. Τα καλώδια, όταν τοποθετούνται υπόγεια, προστατεύονται είτε μέσα σε σωλήνες, είτε οπλίζονται με χαλύβδινο περίβλημα. Στις αρτηρίες με πολύ μεγάλη κίνηση και στις υποβρύχιες ζεύξεις, παλαιότερα, χρησιμοποιήθηκαν σχεδόν αποκλειστικά ομοαξονικά καλώδια, ενώ τα τελευταία χρόνια αντικαταστήθηκαν από καλώδια οπτικών ινών.

2.13.3 Χάλκινο Καλώδιο

Τα χάλκινα καλώδια αποτελούνται από ένα συνεστραμμένο ζεύγος καλωδίων το οποίο είναι είτε συμπαγές χάλκινο σύρμα, είτε από νήματα χάλκινου σύρματος, τα οποία καλύπτονται από πλαστικό περίβλημα. Παλαιότερα, το πλέξιμο των ζευγών του χάλκινου σύρματος στο καλώδιο γίνονταν, έτσι ώστε να αναγνωρίζεται πιο καλώδιο ανήκει σε πιο ζεύγος και όχι για να αντιμετωπισθούν προβλήματα μετάδοσης. Παρόλα αυτά, για τη μετάδοση φωνής το χάλκινο καλώδιο ήταν αρκετά αξιόπιστο μέσο. Αποτέλεσμα αυτού είναι να υπάρχουν, σήμερα, χιλιάδες χιλιόμετρα χάλκινου καλωδίου στο τηλεφωνικό δίκτυο και να αποτελεί το πιο διαδεδομένο μέσο μετάδοσης. Τα χάλκινα καλώδια, που έχουν εγκατασταθεί στο τηλεφωνικό δίκτυο, ήταν σχεδιασμένα, έτσι ώστε να περνούν, χωρίς εξασθένηση όλες οι συχνότητες φωνής, αλλά παράλληλα να εμποδίζεται και η διέλευση συχνοτήτων έξω από τη ζώνη των φωνητικών (χαμηλοπερατά φίλτρα). Αυτό είχε καταστροφικά αποτελέσματα για τη μετάδοση δεδομένων.

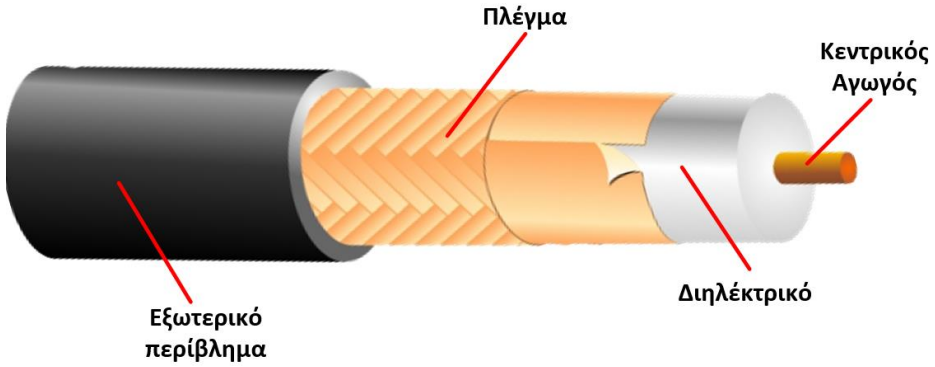


Εικόνα 2.102: Απεικόνιση χάλκινων καλωδίων

Οπότε όταν αναφερόμαστε σε καλώδια UTP, αναφερόμαστε σε αθωράκιστα συνεστραμμένα ζεύγη (Unshielded Twisted Pair) τα οποία αποτελούνται από τέσσερα ζευγάρια συνεστραμμένων αγωγών (σύνολο 8 αγωγοί λοιπόν). Η συστροφή ζευγών γίνεται για μείωση του θορύβου αλλά και για φαινόμενα όπως για παράδειγμα παραδιαφωνίας (cross talk) με το εύρος ζώνης τους να φτάνει τα 100MHz. Αυτό που κυκλοφορεί στην αγορά σήμερα έχει τη τυποποίηση cat6 (κατηγορία 6). Υπάρχουν και άλλες κατηγορίες όπως πχ οι κατηγορίες 1,2,3,4,5 κλπ οι οποίες είναι χειρότερες σε σχέση με την cat6. Το δισύρματο του ΟΤΕ που έχουμε όλοι σπίτι μας είναι κατηγορίας 3.

2.13.4 Ομοαξονικά καλώδια

Το ομοαξονικό καλώδιο ήταν από τα πρώτα καλώδια τα οποία είχαν ευρεία χρήση σε τοπικά δίκτυα. Σήμερα, η χρήση τους στα τοπικά δίκτυα έχει εκλείψει καθότι πλέον χρησιμοποιείται η ethernet τεχνολογία. Το ομοαξονικό καλώδιο έχει πάρει την ονομασία αυτή λόγο της κατασκευής του. Αποτελείται δηλαδή από έναν κεντρικό χάλκινο αγωγό, ο οποίος γύρω του περιέχει ένα πλαστικό περίβλημα το οποίο ονομάζεται διηλεκτρικό. Γύρω από το διηλεκτρικό και ομοαξονικά τοποθετημένο ως προς τον κεντρικό αγωγό υπάρχει μια θωράκιση από μεταλλικό πλέγμα και τέλος όλο αυτό καλύπτεται από ένα πλαστικό εξωτερικό μονωτικό περίβλημα.
Το ομοαξονικό καλώδιο προσφέρει υψηλό εύρος ζώνης (bandwidth), με αποτέλεσμα να επιτυγχάνονται ταχύτητες μετάδοσης υψηλότερες από ότι στα χάλκινα καλώδια. Το γεγονός αυτό δικαιολογεί, την ευρεία χρησιμοποίηση του στην καλωδιακή τηλεόραση και στις υπεραστικές συνδέσεις των τηλεφωνικών δικτύων.

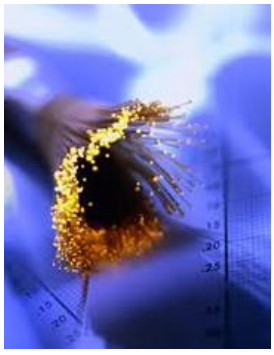


Εικόνα 2.103: Απεικόνιση ενός ομοαξονικού καλωδίου

Στην αγορά μπορούμε να το βρούμε σαν RG-59 και χρησιμοποιείται κυρίως για τη μετάδοση του τηλεοπτικού σήματος στη σύνδεση κεραίας-TV. Όταν χρησιμοποιήθηκε στα δίκτυα ήταν αρκετά αποτελεσματικό. Το εύρος ζώνης του είναι αρκετά μεγάλο έως και 100MHz. Αυτό σημαίνει ότι μπορεί να μεταδοθεί παλμός-bit μέσα από αυτό χωρίς να αλλοιωθεί το πλάτος ή το σχήμα παλμού. Έτσι μπορεί να υποστηρίξει ταχύτητες έως και 600 Mbps.

2.13.5 Οπτικές ίνες

Οι οπτικές ίνες, είναι πολύ λεπτά νήματα από πλαστικό ή γυαλί, όπου η πληροφορία (που περνάει μέσα απ' αυτήν) μεταδίδεται υπό μορφή παλμών φωτός διαφόρων μηκών κύματος. Ένα καλώδιο οπτικών ινών μπορεί να περιέχει μέσα του δεκάδες ή ακόμη και εκατοντάδες πολύ λεπτές τέτοιες οπτικές ίνες, σε διάμετρο, μικρότερη και από μίας τρίχα.



Εικόνα 2.104: Παράδειγμα οπτικής ίνας

Οι οπτικές ίνες έχουν δύο σημαντικά πλεονεκτήματα σε σχέση με άλλα μέσα μετάδοσης δεδομένων: οι μεγάλοι ρυθμοί μετάδοσης δεδομένων και η μεταφορά δεδομένων σε μεγάλες αποστάσεις.

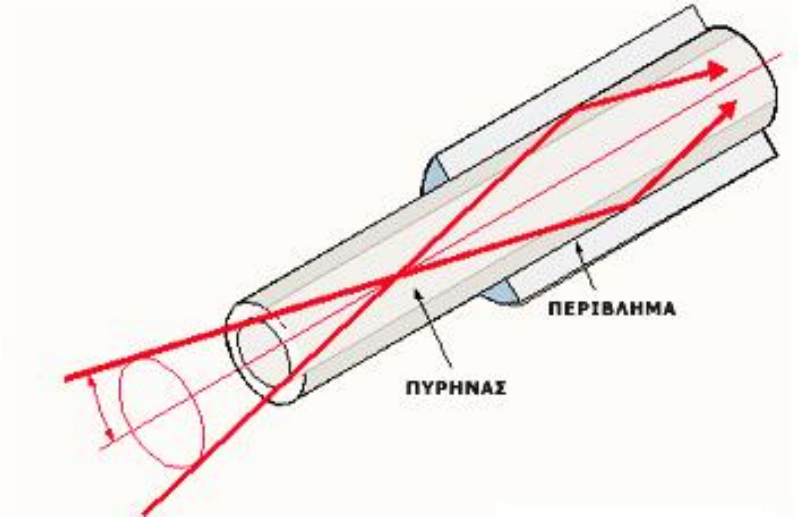
Οι οπτικές ίνες μεταφέρουν πληροφορίες σε πολύ μεγάλες ταχύτητες όχι λόγω της μεγάλης ταχύτητας του φωτός όπως αναφέρεται συχνά. Οι μεγάλοι ρυθμοί μεταφοράς δεδομένων των οπτικών ινών οφείλονται σε δύο βασικούς λόγους:

3. Στις μεγάλες συχνότητες με τις οποίες μπορούν να αναβοσβήνουν τα LED (Light Emitting Diodes) ή τα Laser που είναι οι πομποί των παλμών φωτός και

4. Στην δυνατότητα της ταυτόχρονης αποστολής πολλών ακτινών φωτός σε διαφορετικούς μήκους κύματος μέσα από την ίδια ίνα χωρίς αυτές να επηρεάζουν η μία την άλλη. Έτσι στέλνονται πολλαπλές ταυτόχρονες ροές πληροφοριών μέσω της ίδιας ίνας αυξάνοντας τον συνολικό ρυθμό μεταφοράς δεδομένων.

2.13.6 Πως λειτουργούν οι οπτικές ίνες

Μια οπτική ίνα έχει δύο άκρα όπου στο ένα υπάρχει ο πομπός και στο άλλο, ο δέκτης. Ο πομπός, έχει την δυνατότητα να μετατρέπει δεδομένα σε μορφή παλμών φωτός. Με την σειρά του ο δέκτης αποκωδικοποιεί αυτούς τους παλμούς και τα μετατρέπει ξανά σε ψηφιακά δεδομένα. Για να πραγματοποιηθεί αμφίδρομη επικοινωνία είναι απαραίτητη η χρήση ενός ζευγαριού ινών.
Οι παλμοί φωτός, ταξιδεύουν με την ταχύτητα του φωτός μέσα από την οπτική ίνα, με διαδοχικές ανακλάσεις στα τοιχώματα της οπτικής ίνας. Οι ανακλάσεις αυτές, γίνονται στα τοιχώματα, σε γωνία μικρότερη των 42 μοιρών, με αποτέλεσμα να λειτουργούν τα τοιχώματα σαν καθρέφτες. Το φαινόμενο αυτό ονομάζεται ολική ανάκλαση και είναι η αιτία που τα κύματα φωτός μένουνε μέσα στην οπτική ίνα και διατηρούν την ισχύ τους, συνεχίζοντας το ταξίδι τους μέχρι το άλλο άκρο, χωρίς να βγαίνουν-χάνονται έξω από την ίνα.
Σε αυτό συνεισφέρει και η δομή της. Το εσωτερικό μέρος της οπτικής ίνας, ονομάζεται πυρήνας και μέσω αυτού, ταξιδεύουν τα κύματα φωτός. Ο πυρήνας, είναι περιτυλιγμένος από μία άλλη στρώση πλαστικού - γυαλιού που ονομάζεται περίβλημα.



Εικόνα 2.105: Απεικόνιση ενός καλωδίου οπτικής ίνας

2.13.7 Τρόποι εκπομπής και μετάδοσης στις οπτικές ίνες

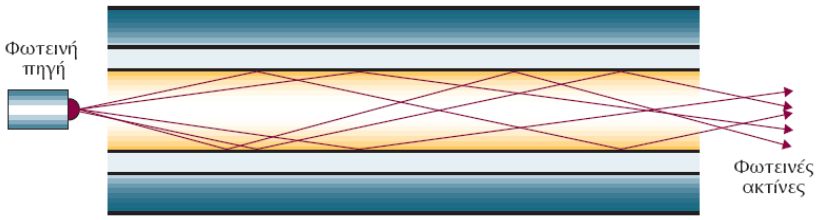
Η εκπομπή του οπτικού σήματος σε οπτική ίνα γίνεται από δύο ειδών πηγών: **LED (light Emmiting Diode) ή LASER (Light Amplification by Stimulated Emission off Radiation),** και τα μήκη κύματος του φωτός, που η οπτική ίνα είναι σχεδιασμένη να μεταφέρει, ποικίλουν από 800nm μέχρι 1500nm. Οι οπτικές ίνες διαφοροποιούνται, καταρχήν, από τον τρόπο μετάδοσης του σήματος σε αυτές. Η πρώτη βασική διάκριση είναι μεταξύ των πολύτροπων και μονότροπων οπτικών ινών.

1. **Πολύτροπες οπτικές ίνες (Multimode fiber optics)**

Ο τρόπος αναφοράς των μεγεθών για τις οπτικές ίνες είναι να αναφέρουμε πρώτα τη διάμετρο του πυρήνα (γυαλιού) και στη συνέχεια τη διάμετρο της επίστρωσης (cladding). Οι μετρήσεις των παραπάνω μεγεθών γίνονται σε 10-6 μέτρα. Οι πολύτροπες οπτικές ίνες έχουν τυπικά μεγέθη 50μm/ 125μm, 62,5/125, 85/125 ή 100/140. Ο συνηθέστερος τύπος, ο οποίος κυκλοφορεί, είναι ο 62,5/125. Η ολική διάμετρος της οπτικής ίνας συμπεριλαμβανομένων των ενισχυτικών συνθετικών ινών και του εξωτερικού περιβλήματος φτάνει τα 900μm. Η αρχή μετάδοσης σε πολύτροπη οπτική ίνα είναι ότι οι διάφορες ακτίνες του οπτικού σήματος ανάλογα με την είσοδο τους στην οπτική ίνα ταξιδεύουν ανακλώμενες υπό διαφορετικές γωνίες, όπως φαίνεται στις εικόνας 2.106 και 2.107. Αυτός ο τρόπος μετάδοσης ονομάζεται πολύτροπος (multimode), επειδή έχουμε πολλούς δρόμους μετάδοσης, που αντιστοιχούν στις διαφορετικές γωνίες ανάκλασης. Οι πολύτροπες οπτικές ίνες διακρίνονται σε δυο κατηγορίες: τις **διακριτού βήματος (step index)** και **τις βαθμιαίου βήματος (graded index)**.

I. Οπτική ίνα διακριτού δείκτη (step index)

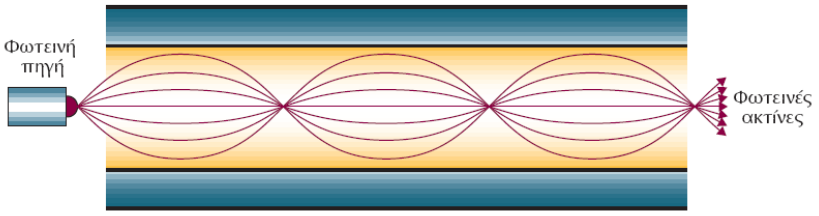
Στις ίνες αυτές συμβαίνει απότομη μεταβολή του δείκτη διάθλασης μεταξύ της κεντρικής ίνας και του υλικού επίστρωσης. Στην περίπτωση αυτή, η πορεία των ακτινών εμφανίζεται στην εικόνα 2.106.



Εικόνα 2.106. Οπτική ίνα διακριτού δείκτη

II. Οπτική ίνα βαθμιαίου δείκτη (graded index)

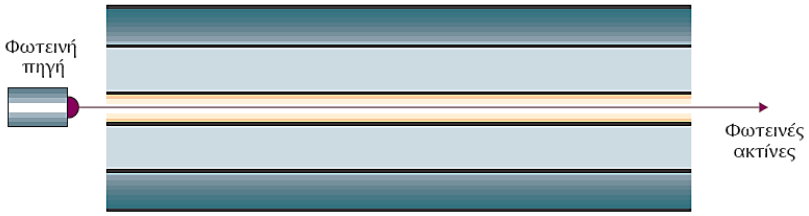
Οι ίνες αυτές χαρακτηρίζονται από βαθμιαία μεταβολή του δείκτη διάθλασης του υλικού της κεντρικής ίνας. Συμβαίνει βαθμιαία μείωση όσο απομακρυνόμαστε από το κέντρο προς την εξωτερική επιφάνεια του γυαλιού. Η πορεία των ακτινών σε μια τέτοια ίνα είναι αυτή, που φαίνεται στην εικόνα 2.107.



Εικόνα 2.107. Οπτική ίνα βαθμιαίου δείκτη

2. **Μονότροπες οπτικές ίνες (Single mode fiber optics)**

Στις μονότροπες οπτικές ίνες η διάμετρος της κεντρικής ίνας είναι πολύ μικρή και πλησιάζει περίπου το επίπεδο του μήκους κύματος του εκπεμπόμενου σήματος. Στην περίπτωση αυτή, έχουμε έναν μόνο δυνατό τρόπο μετάδοσης του οπτικού σήματος, τον αξονικό. Η πορεία των ακτινών σε μια τέτοια οπτική ίνα φαίνεται στην εικόνα 2.108. Η κεντρική ίνα στις μονότροπες οπτικές ίνες έχει διάμετρο από 5μm έως 10μm με συνηθέστερη τιμή τα 8,3 μm.

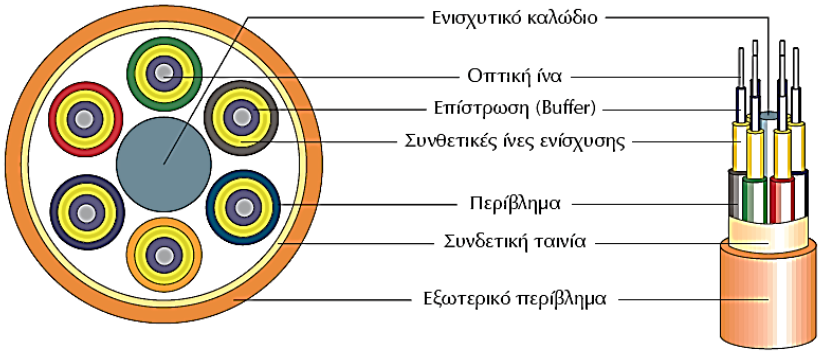


Εικόνα 2.108. Μονότροπη οπτική ίνα

2.13.8 Τύποι καλωδίων οπτικών ινών

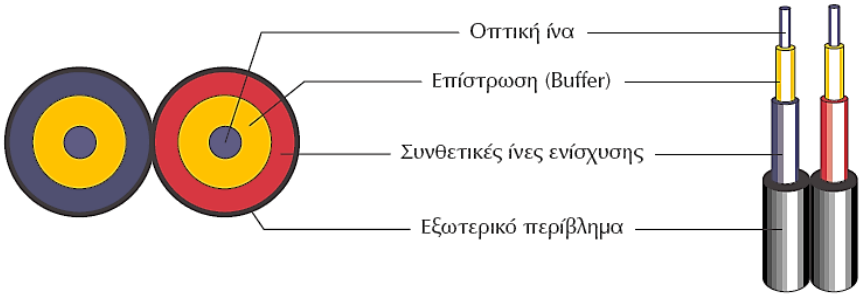
Τα καλώδια οπτικών ινών περιέχουν από 1 έως 36 οπτικές ίνες. Τα πιο συνηθισμένα είναι τα καλώδια με ζυγό αριθμό οπτικών ινών για την επικοινωνία των full-duplex κυκλωμάτων. Θα ξεχωρίσουμε δυο τύπους οπτικών ινών ως προς την κατασκευή τους.

Στην πρώτη περίπτωση, έχουμε σε κάθε οπτική ίνα και εξωτερικά από την επίστρωση συνθετικές ίνες και εξωτερικό μονωτικό περίβλημα. Μέσα στο καλώδιο υπάρχουν πολλές τέτοιες ίνες, όπου η κάθε ίνα αποτελεί και ένα ξεχωριστό καλώδιο. Μέσα στο καλώδιο περιέχονται εκτός από καλώδια οπτικών ινών και καλώδια, τα οποία χρησιμεύουν για ενίσχυση και στρογγυλοποίηση του όλου σχήματος. Όλα αυτά τα καλώδια, τέλος, περικλείονται από εξωτερικό περίβλημα. Αυτή η κατασκευή είναι γνωστή σαν Tight Buffer. Στην εικόνα 2.109 εμφανίζεται ανάλογη κατασκευή καλωδίου οπτικών ινών.



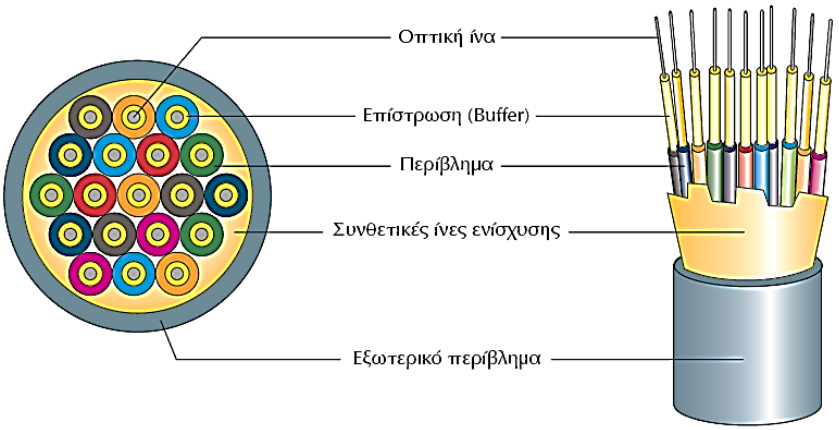
Εικόνα 2.109. Καλώδιο οπτικών ινών (Tight Buffer)

Παρόμοιας κατασκευής είναι τα εύκαμπτα καλώδια, που χρησιμοποιούμε για τη σύνδεση με τον ενεργό εξοπλισμό (Optical patch cords). Αυτά αποτελούνται από δυο καλώδια ενωμένα στο εξωτερικό τους, το κάθε ένα από τα οποία περιέχει οπτική ίνα από πλαστικό. Στην εικόνα 2.110 εμφανίζεται ένα οπτικό καλώδιο σύνδεσης.



Εικόνα 2.110. Οπτικό Patch cord

Στην δεύτερη περίπτωση, έχουμε τις οπτικές ίνες με την επίστρωση τους να είναι τοποθετημένες ελεύθερα μέσα στο καλώδιο και περικλείονται από εξωτερικό περίβλημα, αφού πρώτα τοποθετηθεί μέσα στο καλώδιο επίστρωση από συνθετικές ίνες για την ανθεκτικότητα του καλωδίου. Αυτή η κατασκευή είναι γνωστή σαν Loose Buffer. Στην εικόνα 2.111 εμφανίζεται ανάλογη κατασκευή καλωδίου οπτικών ινών.



Εικόνα 2.111. Καλώδιο οπτικών ινών (loose buffer)

2.13.9 Τύποι βυσμάτων και υποδοχών οπτικών ινών

Πέρα από τους τύπους των καλωδίων είναι και οι τύποι των βυσμάτων και των υποδοχών των οπτικών ινών. Παρακάτω θα δείτε τους πιο δημοφιλές τύπους που χρησιμοποιούνται στην αγορά σήμερα. Τα βύσματα και οι υποδοχές αυτές μπορούν να χρησιμοποιηθούν σε μονότροπες καθώς και σε πολύτροπες οπτικές ίνες.

Εικόνα 2.112. Βύσματα οπτικών ινών, από αριστερά προς δεξιά: SC, ST, LC

2.14 Ασύρματη Μετάδοση

Ασύρματη μετάδοση είναι η ζεύξη όπου δεν χρησιμοποιείται κάποιο είδος καλωδίου και χρησιμοποιεί ως μέσο διάδοσης τον αέρα ή το κενό. Αυτό γίνεται με τη διάδοση σημάτων στην ατμόσφαιρα μέσω κατάλληλων κεραιών (μεταξύ πομπού και δέκτη μεταδίδοντας την πληροφορία κωδικοποιημένη). Ένα σύστημα ασύρματης επικοινωνίας εξαρτάται από:

- Τον πομπό (transmitter)
- Τη γραμμή τροφοδοσίας (feeder) του πομπού με την κεραία εκπομπής
- Την κεραία εκπομπής (transmitting antenna)
- Το χώρο διαδόσεως ηλεκτρομαγνητικών κυμάτων (path)
- Την κεραία λήψεως (receiving antenna)
- Τη γραμμή σύνδεσης (feeder) της κεραίας λήψεως με το δέκτη
- Το δέκτη (receiver)
- Τους πύργους εγκατάστασης (tower) των κεραιών (όπου κρίνεται απαραίτητο)

Ιδιότητες κεραιών (με βάση τη λειτουργία τους)

- ✓ Το σχήμα (το σχήμα καθορίζει την κατεύθυνση όπου θα ακτινοβολούνται τα κύματα, αν είναι κεραία εκπομπής, ή την κατεύθυνση από την οποία θα λαμβάνονται τα κύματα, αν είναι κεραία λήψης)
- ✓ Το σημείο που ανατροφοδοτείται από τον πομπό

Πλεονεκτήματα	**Μειονεκτήματα**
Ανεξαρτησία από υλικά μέσα διάδοσης (π.χ καλώδιο)	Απαιτείται μεγάλη ισχύς
Χαμηλότερο κόστος επέκτασης	Ευάλωτα σε παρεμβολές
Γρήγορη εγκατάσταση και τοποθέτηση	Ευάλωτα σε επιθέσεις
Διευκόλυνση μεγάλων αποστάσεων	Δυνατότητες μετάδοσης περιορίζονται από τον νόμο

Πίνακας 2.14. Πλεονεκτήματα και μειονεκτήματα της ασύρματης μετάδοσης

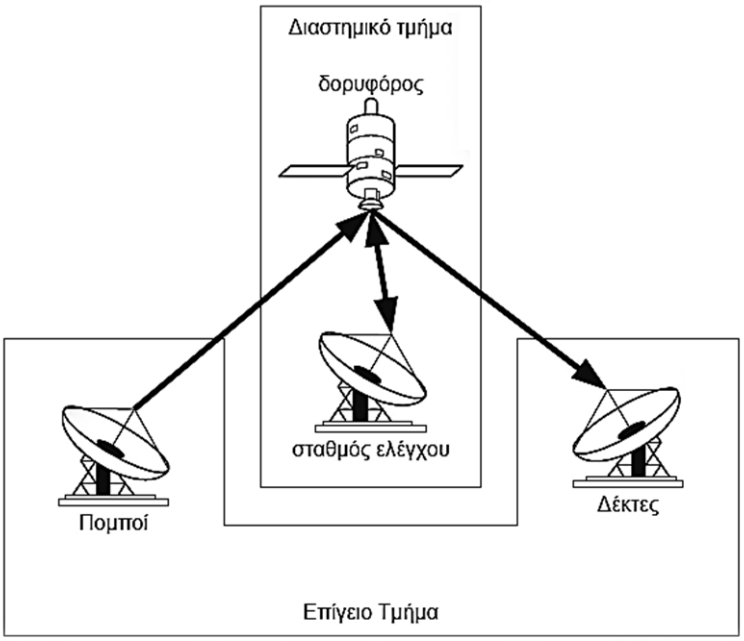
Στα **ασύρματα μέσα μετάδοσης** ανήκουν οι επίγειες και **δορυφορικές μικροκυματικές ζεύξεις**, και τα **συστήματα κυψελοειδούς τηλεφωνίας**.

2.14.1 Επίγειες μικροκυματικές ζεύξεις

Οι επίγειες μικροκυματικές ζεύξεις στηρίζονται στην κατευθυντική μετάδοση μικροκυμάτων στην περιοχή πολύ υψηλών συχνοτήτων (από 2-40 GHz). Για να είναι δυνατή η μεταφορά δεδομένων πρέπει να έχουν οπτική επαφή μεταξύ τους και λόγω της καμπυλότητας της γης απαιτούνται σταθμοί αναμετάδοσης 40-50 χιλιόμετρα περίπου. Χρησιμοποιούνται για μετάδοση τηλεοπτικού σήματος και φωνής, για μικρές συνδέσεις, μεταξύ κτιρίων για κλειστό κύκλωμα τηλεόρασης ή για συνδέσεις δεδομένων μεταξύ τοπικών δικτύων.

2.14.2 Δορυφορικές μικροκυματικές ζεύξεις

Οι δορυφορικές μικροκυματικές ζεύξεις χρησιμοποιούν δορυφόρους οι οποίοι μπορούν να αναμεταδίδουν σήμα σε πολύ μεγάλες αποστάσεις. Οι δορυφορικές ζεύξεις χωρίζονται σε δυο κατηγορίες, στις **ανοδικές (uplink)** και **καθοδικές (downlink)**. Ανοδικές ζεύξεις χρησιμοποιούνται για την αποστολή των σημάτων από τους επίγειους σταθμούς στους δορυφόρους και οι δορυφόροι αναμεταδίδουν τα σήματα στις καθοδικές ζεύξεις.



Εικόνα 2.113. Παράδειγμα επικοινωνίας μεταξύ επίγειων σταθμών και ενός δορυφόρου

Τα βασικά μέρη ενός δορυφόρου είναι:

1) Το ωφέλιμο φορτίο (payload) το οποίο περιλαμβάνει:
   - Κεραίες
   - Ηλεκτρονικό εξοπλισμό μετάδοσης και λήψης

2) Η πλατφόρμα η οποία περιλαμβάνει:
   - Μηχανική κατασκευή
   - Παροχή ηλεκτρικής ενέργειας
   - Έλεγχος θερμοκρασίας
   - Έλεγχος θέσης και τροχιάς
   - Εξοπλισμός πρόωσης
   - Εξοπλισμός παρακολούθησης και τηλεμετρίας ελέγχου

Ο ρόλος που αναλαμβάνει ένας δορυφόρος είναι να ενισχύει τα σήματα που λαμβάνει (uplink) και να τα επανεκπέμπει (downlink) σε προκαθορισμένες συχνότητες

Μετατροπή συχνότητας:

α) Με μετατροπέα συχνότητας
β) Με χρήση αποδιαμορφωτών

Το επίγειο τμήμα το αποτελούν ο πομπός και ο δέκτης. Οι επίγειοι σταθμοί χωρίζονται σε δύο κατηγορίες τους σταθερούς και τους κινητούς. Οι σταθεροί επίγειοι σταθμοί περιλαμβάνουν:

α) Σταθμούς δρομολόγησης της τηλεπικοινωνιακής κίνησης που συλλέγεται από επίγεια τμήματα

β) Σταθμούς στις εγκαταστάσεις του χρήστη

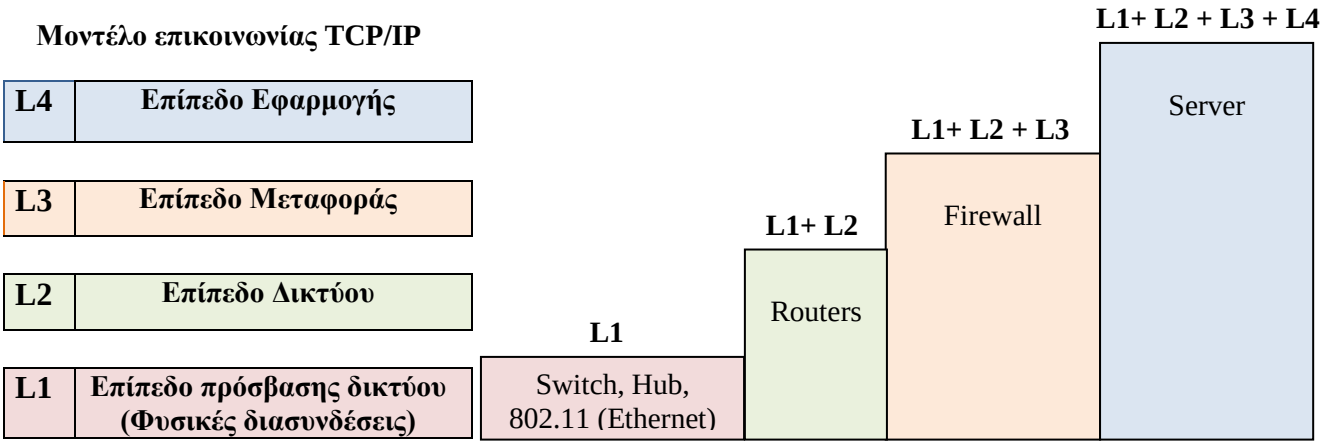
Οι κινητοί σταθμοί περιλαμβάνουν σταθμούς σε ξηρά, θάλασσα και αέρα

2.14.3 Συστήματα κυψελοειδούς τηλεφωνίας

Τα συστήματα κυψελοειδούς τηλεφωνίας είναι συστήματα τα οποία χρησιμοποιούνται στην κινητή ραδιοτηλεφωνία. Η κινητή ραδιοτηλεφωνία εξυπηρετεί την επικοινωνία μεταξύ κινούμενων και σταθερών σταθμών αλλά και μεταξύ κινούμενων σταθμών σε μικρές και μεσαίες αποστάσεις. Χρησιμοποιούνται για την επικοινωνία μέσα σε πόλεις όπως η Αστυνομία, Πυροσβεστική κ.ο.κ (30-900 MHz οι συχνότητες που χρησιμοποιούνται)

2.15 Δικτυακές συσκευές στο μοντέλο επικοινωνίας TCP/IP

Αφού περιγράψαμε πως λειτουργεί το TCP/IP και την λειτουργία των φυσικών μέσων μετάδοσης και των δικτυακών συσκευών όπως μεταγωγείς, συσκευές NAT κλπ ας αποτυπώσουμε στο μυαλό μας κάτι τελευταίο που είναι και το πιο σημαντικό για την ολική κατανόηση του 2ου κεφαλαίου. Όπως είπαμε το TCP/IP διαχωρίζει την πληροφορία σε επίπεδα ώστε να επιτυγχάνεται μια ιεραρχική επικοινωνία όπου όλα τα επίπεδα επικοινωνούν με τα αμέσως επόμενα κοκ. Το ίδιο λοιπόν μπορούμε να πούμε και για όλες τις δικτυακές συσκευές που περιγράψαμε. Κάθε συσκευή «σκέφτεται» σε κάποιο συγκεκριμένο επίπεδο του TCP/IP. Στο σχήμα 2.10 ακολουθεί μα αναλυτική δομή για όλες τις δικτυακές συσκευές στο μοντέλο TCP/IP.



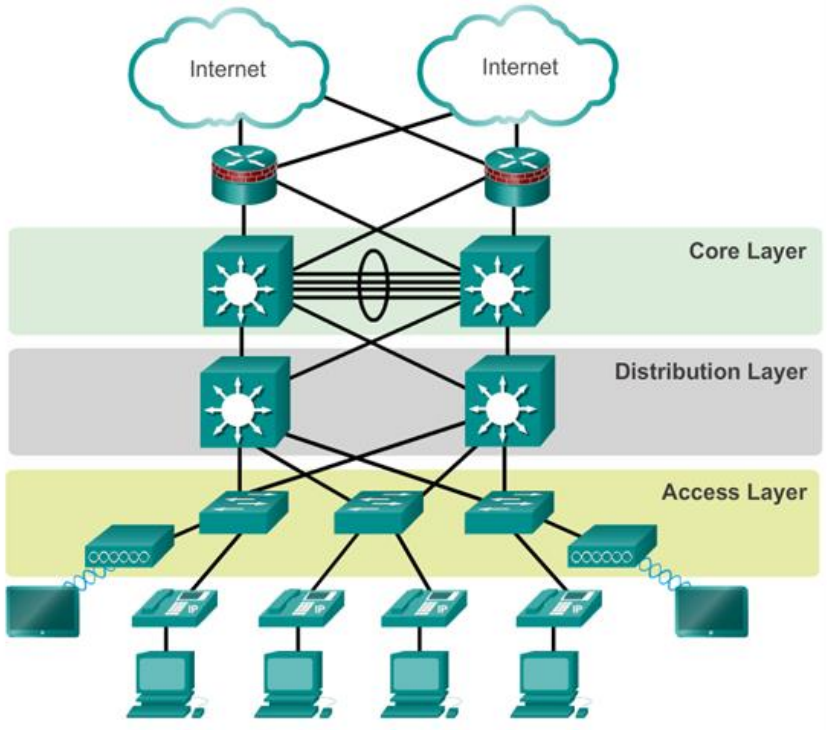
Σχήμα 2.10:Δικτυακές συσκευές που χρησιμοποιούν τα επίπεδα του TCP/IP

3.1 Εταιρικά και Επιχειρησιακά Δίκτυα Υπολογιστών

Οι τηλεπικοινωνίες είναι πλέων ένα αναπόσπαστο κομμάτι της σημερινής επιχειρησιακής πραγματικότητας. Για τις επιχειρήσεις, οι τηλεπικοινωνίες είναι όσο απαραίτητες όσο το ρεύμα και το τρεχούμενο νερό. Επιπλέον, οι τηλεπικοινωνίες είναι ένας τεχνολογικός τομέας που αναπτύσσεται ραγδαία και επιτρέπει την άμεση εφαρμογή νέων τεχνολογιών για την εξυπηρέτηση των επιχειρησιακών στόχων. Η εταιρία για την οποία σχεδιάζουμε το δίκτυο αυτό έχει ανάγκη από ένα δίκτυο το οποίο είναι σύγχρονο, ασφαλές και οικονομικό. Όλα αυτά τα στοιχεία είναι απαραίτητα για να παραμείνει ανταγωνιστική και αποτελεσματική.
Αντίθετα με την παραδοσιακή αντίληψη των δικτύων, τα σύγχρονα δίκτυα προσφέρουν πολύ περισσότερο από μια απλή διασύνδεση υπολογιστών και μοίρασμα υπηρεσιών. Είναι αγωγοί που φέρουν χρήσιμες και προηγμένες υπηρεσίες στο σταθμό εργασίας του εργαζόμενου καθώς και στην φορητή συσκευή του κινούμενου χρήστη. Η εταιρία μας θέλει να αξιοποιήσει όλες αυτές τις δυνατότητες που προσφέρουν τα σύγχρονα δίκτυα τώρα, αλλά και στο μέλλον. Γι' αυτό ο σχεδιασμός θα πρέπει να περιλαμβάνει τα παρακάτω χαρακτηριστικά:

3.1.1 Ιεραρχικός σχεδιασμός

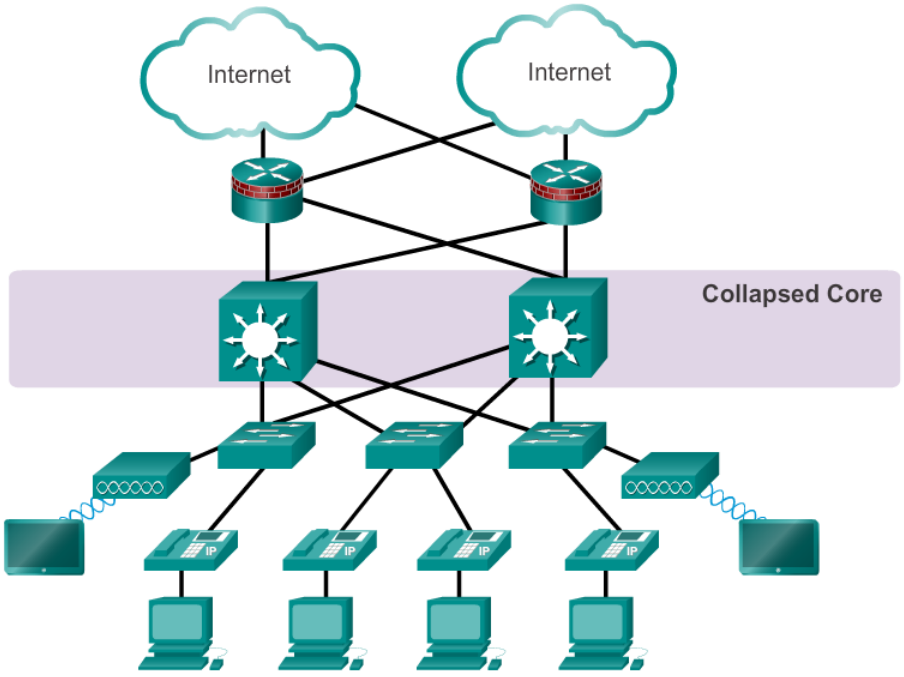
Για την βελτιστοποίηση της χρήσης των ευρυζωνικών συνδέσεων, σε ένα εταιρικό δίκτυο, το δίκτυο θα πρέπει να οργανωθεί έτσι ώστε η κυκλοφορία να παραμένει τοπική και να μην διαδίδεται άσκοπα σε άλλα τμήματα του δικτύου. Γι αυτόν τον λόγο χρησιμοποιούμε το ιεραρχικό μοντέλο σχεδίασης τριών επιπέδων που βοηθάει στην οργάνωση των δικτύων. Αυτό το μοντέλο χωρίζει τη λειτουργία του δικτύου σε τρεις διακριτές στρώσεις, όπως φαίνεται στην εικόνα 3.1.



Εικόνα 3.1.Ιεραρχικός σχεδιασμός δικτύου δεδομένων

- Επίπεδο Πρόσβασης (Access)
- Επίπεδο Διανομής (Distribution)
- Επίπεδο Κορμού (Core)

Το στρώμα πρόσβασης παρέχει την διασυνδεσιμότητα στους χρήστες. Το επίπεδο διανομής χρησιμοποιείται για να διαβιβάσει κίνηση από ένα τοπικό δίκτυο σε ένα άλλο. Τέλος, το επίπεδο κορμού προσφέρει υψηλή ταχύτητα μεταξύ διασκορπισμένων δικτύων. Παρόλο που το ιεραρχικό μοντέλο αποτελείται από τρία επίπεδα, σε δίκτυα τα οποία είναι μικρά σε μέγεθος μπορεί επίσης να εφαρμοστεί μία σχεδίαση με δύο επίπεδα. Σε μία τέτοια σχεδίαση, τα επίπεδα κορμού και διανομής ενώνονται σε ένα ενιαίο επίπεδο, μειώνοντας το κόστος και την πολυπλοκότητα. Κάτι τέτοιο αποτυπώνεται στην εικόνα 3.2. Στην περίπτωση της εταιρίας μας, λόγω του μεγέθους της, επιλέγουμε αυτό το σχήμα δύο επιπέδων.



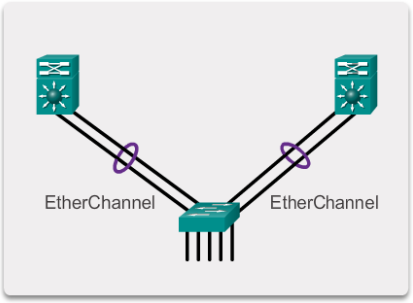
Εικόνα 3.2.Ενοποιημένος ιεραρχικός σχεδιασμός δικτύου

3.1.2 Επεκτασιμότητα (Scalability)

Για την υποστήριξη ενός επιχειρησιακού δικτύου, ο σχεδιαστής αυτού θα πρέπει να αναπτύξει και να καταγράψει μια στρατηγική με άμεσο σκοπό την αποτελεσματικότητα και την επεκτασιμότητα του δικτύου. Για να πραγματοποιηθεί αυτό, εφαρμόζουμε μια καταγραφή βασικής στρατηγικής όσον αφορά τον σχεδιασμό των δικτύων. Αυτές οι ακόλουθες καταγραφές στρατηγικής είναι οι εξής:

- Χρήση επεκτάσιμου και τμηματικού (modular) εξοπλισμού ή ακόμα και συσκευές που λειτουργούν σε ομάδες για την εύκολη επέκταση και αναβάθμιση μελλοντικών αναγκών.
- Διευθυνσιοδότηση σε IPv4 ή IPv6, που είναι ιεραρχική. Στην περίπτωση του IPv4 ο σχεδιασμός πρέπει να γίνει με προσεκτικά βήματα ώστε να μην υπάρχει η μελλοντική ανάγκη για εξ' αρχής νέα διευθυνσιοδότηση για την υποστήριξη περισσοτέρων χρηστών ή υπηρεσιών.

- Επιλογή δρομολογητών (routers) ή μεταγωγών (switches) πολλαπλών στρωμάτων για τον περιορισμό των εκπομπών και ο φιλτρατισμός ανεπιθύμητης κυκλοφορίας από το δίκτυο. Συνήθως το φιλτράρισμά ανεπιθύμητης κυκλοφορίας δεδομένων επιτυγχάνεται με firewalls. Χρήση συσκευών 3ου επιπέδου ώστε να φιλτράρουμε την μείωση της κίνησης (traffic) με το κεντρικό δίκτυο.
- Χρήση συσκευών που υποστηρίζουν πολλαπλές συνδέσεις μεταξύ του εξοπλισμού με τεχνολογίες EtherChannel ή με την εξισορρόπηση φορτίου σε εφεδρικές συνδέσεις.
- Εφαρμογή ασύρματων υπηρεσιών για να επιτραπεί η μεταφερσιμότητα (scalability) και η εύκολη και οικονομική επέκταση.
- Χρήση επεκτάσιμων πρωτοκόλλων δρομολόγησης και εφαρμογή των χαρακτηριστικών τους για την απομόνωση των ενημερώσεων δρομολόγησης. Αυτό θα έχει ως αποτέλεσμα την ελαχιστοποίηση του μεγέθους στους πίνακες δρομολόγησης.

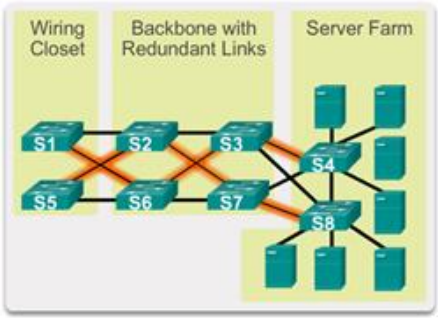


Εικόνα 3.3. Παράδειγμα χρήσης EtherChannel

3.1.3 Εφεδρεία (Redundancy)

Σε πολλές εταιρίες ή οργανισμούς, η διαθεσιμότητα ενός δικτύου είναι απαραίτητη για την υποστήριξη των επιχειρηματικών αναγκών. Η εφεδρεία (backup) είναι ένα πολύ σημαντικό κομμάτι του σχεδιασμού ενός δικτύου για την πρόληψη της διατάραξης των υπηρεσιών του, ελαχιστοποιώντας έτσι την πιθανότητα ενός ενιαίου σημείου αποτυχίας. Μία μέθοδος εφαρμογής εφεδρείας είναι η εγκατάσταση ενός διπλού εξοπλισμού και η παροχή υπηρεσιών ανακατεύθυνσης για τις κύριες συσκευές (backbone devices).

Μία άλλη μέθοδος εφαρμογής εφεδρικότητας είναι οι πολλαπλές διαδρομές όπως αυτό αποτυπώνεται στην εικόνα 3.4. Οι πολλαπλές διαδρομές προσφέρουν εναλλακτικές φυσικές διαδρομές που μπορούν να διασχίσουν τα πακέτα δεδομένων. Βέβαια οι πολλαπλές διαδρομές δημιουργούν loops σε μεταγωγείς (switches) κάτι που είχαμε εξηγήσει στο δεύτερο κεφάλαιο και την επίλυση αυτού του προβλήματος καλείται να διορθώσει το πρωτόκολλο STP.



Εικόνα 3.4. Παράδειγμα εφεδρικών διασυνδέσων σε ένα δίκτυο δεδομένων

3.1.4 Σύγκληση δικτύων (Network Convergence)

Με τον όρο σύγκληση δικτύων (network convergence) αναφερόμαστε στην παροχή υπηρεσιών τηλεφώνου, βίντεο και δεδομένων τα οποία ενσωματώνονται σε ένα ενιαίο δίκτυο. Με άλλα λόγια, ένας «σωλήνας» χρησιμοποιείται για να παραδώσει όλες τις μορφές των υπηρεσιών επικοινωνίας. Η διαδικασία της σύγκλησης δικτύου καθοδηγείται κυρίως από την ανάπτυξη της τεχνολογίας και ζήτησης. Ένας κύριος στόχος αυτής της ενοποίησης είναι η παροχή καλύτερων υπηρεσιών σε χαμηλότερες τιμές για τους καταναλωτές. Οι χρήστες είναι σε θέση να έχουν πρόσβαση σε ένα ευρύτερο φάσμα υπηρεσιών και να επιλέξουν ανάμεσα σε περισσότερους παρόχους υπηρεσιών. Από την άλλη πλευρά, η σύγκλιση επιτρέπει στους παρόχους υπηρεσιών να υιοθετήσουν τα νέα επιχειρηματικά μοντέλα, προσφέρει καινοτόμες υπηρεσίες, και να εισέλθουν σε νέες αγορές. Το δίκτυο της εταιρίας μας θα σχεδιαστεί έχοντας υπόψη και την σύγκληση δικτύων.

3.1.5 Προηγμένες Υπηρεσίες

Ένα δίκτυο μπορεί να προετοιμαστεί για την σημερινή ή την μελλοντική αξιοποίηση νέων τηλεπικοινωνιακών τεχνολογιών και υπηρεσιών, VoIP, IPTV, εφαρμογές σύννεφου (cloud) βασισμένες σε παρουσία (presence based) και σε τοποθεσία (location based). Για παράδειγμα όλες αυτές οι υπηρεσίες αναπτύσσονται και χρησιμοποιούνται στο διαδίκτυο ή σε ιδιωτικά δίκτυα IP.

3.1.6 Οικονομικό κόστος

Μια εταιρία προκειμένου να μπορέσει να ανταποκριθεί στην σύγχρονη αγορά θα πρέπει να υπολογίσει το κόστος για τα παραπάνω που αναφέραμε αλλά και για περεταίρω δευτερεύοντες υπηρεσίες όπως για παράδειγμα online εξυπηρέτηση πελατών, αγορά επιπλέων ηλεκτρονικών συσκευών (π.χ. εκτυπωτές, υπολογιστές, κόστος διαφημίσεων κλπ). Κύριος στόχος στο αρχικό ξεκίνημα της εταιρίας είναι να υπολογίσουμε το κόστος που θα χρειαστεί προκειμένου να ανταποκριθεί στις βασικές της ανάγκες (π.χ. το ποσοστό εργαζομένων που θα μπορέσει να απασχολήσει η εταιρία, την κάλυψη μισθοδοσίας αυτών, την σωστή και γρήγορη εξυπηρέτηση των πελατών, το κέρδος κλπ) αλλά κυρίως τον εργονομικό και ασφαλή σχεδιασμό του δικτύου τόσο σε φυσικό επίπεδο (δηλαδή την πρόβλεψη για φυσικές καταστροφές που μπορεί να συμβούν στο δίκτυο μας) όσο και σε επίπεδο exploit (δηλαδή την κάλυψη κενών ασφάλειας για να αποφύγουμε επιθέσεις από τρίτους). Για την αρχική κάλυψη αναγκών μια εταιρία θα αναγκαστεί να δανειστεί από την τραπεζική αγορά ένα λογικό ποσό προκειμένου να μπορέσει να αποκτήσει ένα αρχικό κεφάλαιο ώστε να καταφέρει να καλύψει τις όποιες ανάγκες προκύψουν. Αυτό για να γίνει θα πρέπει η εταιρία να μπορέσει να ανταποκριθεί στο δάνειο στο οποίο θα λάβει ώστε να αποκτήσει την εμπιστοσύνη των τραπεζικών αγορών.

3.2 Σχεδιασμός δικτύου στα μέτρα της εταιρίας

Το δίκτυο που θα σχεδιάσουμε θα αφορά μια τοπική επιχείρηση τηλεπικοινωνιακού φορέα η οποία θα εδρεύει στα πλαίσια της πόλης του Ηρακλείου. Θα διαθέτει ένα κεντρικό κατάστημα και ένα υποκατάστημα. Η επιχείρηση αυτή θα διαθέτει τα παρακάτω τμήματα εργασίας:

Τμήματα Δικτύου	Σταθμοί Εργασίας	Συσκευές ανά σταθμό εργασίας	Σύνολο τερματικών σταθμών
Πώλησης	8	1,5	12
Διοίκησης	4	2,0	8
Λογιστηρίου	6	1,5	9
Marketing	7	1,5	11
Τμήμα πληροφοριών	1	4,0	4
Wireless LAN	40	1,0	40
Management LAN	10	1,5	15
Server LAN	4	1,0	4
Υποκατάστημα	10	1,5	15

Πίνακας 3.1. Ενδεικτικός αριθμός συσκευών ανά τμήμα

- Οι σταθμοί εργασίας μας λένε τον αριθμό των ηλεκτρονικών υπολογιστών που υπάρχουν σε κάθε τμήμα. Στην περίπτωση των τμημάτων Management LAN και Wireless LAN, αυτός ο αριθμός μας δίνει τον αριθμό των εν λόγω συσκευών.

- Οι συσκευές ανά σταθμό εργασίας μας επιτρέπουν να υπολογίσουμε πόσοι περισσότεροι τερματικοί σταθμοί θα υπάρχουν σε κάθε τμήμα όπως εκτυπωτές, φωτοτυπικά και άλλες δικτυακές συσκευές. Μία τιμή των 1 σημαίνει ότι δεν θα υπάρχουν άλλες δικτυακές συσκευές εκτός από τους ηλεκτρονικούς υπολογιστές. Μία τιμή πάνω από το 1 σημαίνει ότι θα υπάρχουν περισσότερες συσκευές πέρα από τους υπολογιστές.

- Το σύνολο των τερματικών σταθμών είναι το αποτέλεσμα του πολλαπλασιασμού των σταθμών εργασίας με τις συσκευές ανά σταθμό εργασίας. Αυτός είναι ο τελικός αριθμός των δικτυακών συσκευών που θα πρέπει να εξυπηρετηθούν.

Οι εξυπηρετητές (servers) που θα διαθέτει η εταιρεία θα είναι:

Servers	**Αριθμός**
Database server	1
Communication server	1
Backup server	1
Print server	1
Σύνολο	4

Πίνακας 3.2. Ενδεικτικός αριθμός εξυπηρετητών (servers)

3.2.1 Ποιες είναι οι ανάγκες της εταιρίας

Για να σχεδιαστεί το δίκτυο θα χρειαστεί πρώτα να γνωρίσουμε την διάταξη της εταιρίας στο κτίριο. Στον παρακάτω πίνακα θα βρείτε την απεικόνιση του κτιρίου και τους ορόφους του καθώς και τον αριθμό των ενεργών πορτών που θα χρειαστούν για κάθε τμήμα.

Όροφος	**Τμήμα**
3ος	Διοίκηση 10 Ασύρματο σημείο πρόσβασης 1
2ος	Marketing 8 Πωλήσεις 6 Ασύρματο σημείο πρόσβασης 1
1ος	Λογιστήριο 9 Πωλήσεις 6 Ασύρματο σημείο πρόσβασης 1
Ισόγειο	Διοίκηση 1 Τμήμα Πληροφορικής 4 Server LAN 4 Ασύρματο σημείο πρόσβασης 1

Πίνακας 3.3. Διανομή των VLANs ανά όροφο

Οι απαραίτητες προδιαγραφές του δικτύου περιλαμβάνουν τα παρακάτω στοιχεία:

- Να ληφθεί υπόψη ότι μπορεί να υπάρχει αύξηση του προσωπικού μέχρι και 20% τα επόμενα 5 χρόνια.
- Να υπάρχει εφεδρεία στις διασυνδέσεις του δικτύου (STP)
- Οι κάθετες διασυνδέσεις να μην επηρεάζονται από πιθανά ηλεκτρομαγνητικά παιδία (από καλώδια ρεύματος κτλ)
- Να εφαρμοστεί ασφάλεια στο δίκτυο της εταιρίας
    - Φυσική ασφάλεια χώρων των servers
    - Εφαρμογή ενός ASA Firewall
    - VPN/IPSec στις επικοινωνίες με το υποκατάστημα
    - Ασφάλεια στο 2^{ο} επίπεδο (Port security, MAC Address Spoofing κτλ)
    - Ασφάλεια στο ασύρματο δίκτυο
    - Πρόσβαση στον database server μόνο από χρήστες του Λογιστηρίου
    - Χρήση DHCP για τους χρήστες και στατικές IP για εκτυπωτές, access points και εξυπηρετητές.
    - Χρήση VTP για την λειτουργία των VLANs
- Να δημιουργηθεί και να ακολουθηθεί μία πολιτική ασφάλειας π.χ.
    - Χρήστες στα pc δεν θα είναι administrators
    - Θα υπάρχει χρήση μόνο ssh και όχι telnet για τις συνδέσεις στον ενεργό εξοπλισμό
    - Θα υπάρχει κωδικός πρόσβασης με κατάλληλες προδιαγραφές για την πρόσβαση στον ενεργό εξοπλισμό
    - Θα απενεργοποιηθεί το http access στον ενεργό εξοπλισμό

3.2.2 Σχεδιασμός υποδικτύων

Για να υπολογίσουμε τα μεγέθη των υποδικτύων, χρησιμοποιούμε τον παρακάτω πίνακα.

Subnet Mask	Μέγεθος Υποδικτύου	Χρήσιμες διευθύνσεις
255.255.255.0	256	254
255.255.255.128	128	126
255.255.255.192	64	62
255.255.255.224	32	30
255.255.255.240	16	14
255.255.255.248	8	6
255.255.255.252	4	2

Πίνακας 3.4. Πιθανοί συνδυασμοί subnet masks

Γνωρίζουμε ότι τα μεγέθη κάθε υποδικτύου είναι συγκεκριμένα. Επειδή κάθε υποδίκτυο περιέχει την Network Διεύθυνση και την Broadcast Διεύθυνση, δύο διευθύνσεις που δεν χρησιμοποιούνται για hosts, οι χρήσιμες διευθύνσεις για κάθε υποδίκτυο είναι δύο λιγότερες. Βλέποντας τον παραπάνω πίνακα και το σύνολο τερματικών σταθμών ανά τμήμα, μπορούμε να βρούμε το μέγεθος των υποδικτύων για κάθε τμήμα και συνεπώς το subnet mask του καθενός. Σημειώνεται ότι τα μεγέθη

επιλέγονται έτσι ώστε να εκπληρώνουμε και την απαίτηση της πρόβλεψης για 20% αύξηση στον αριθμό των εργαζομένων.

Τμήματα Δικτύου	**Σύνολο τερματικών σταθμών**	**Μέγεθος Υποδικτύου**	**Subnet Mask**
Πώλησης	12	30*	255.255.255.224
Marketing	8	14	255.255.255.240
Λογιστηρίου	9	14	255.255.255.240
Διοίκησης	11	14	255.255.255.240
Τμήμα Πληροφορικής	4	6	255.255.255.248
Wireless LAN	40	62	255.255.255.192
Management LAN	15	30*	255.255.255.224
Server LAN	4	14	255.255.255.240
Υποκατάστημα	9	14	255.255.255.240

Πίνακας 3.5. Μεγέθη των VLANs που θα χρησιμοποιήσει η εταιρία

*Σημειώνεται ότι παρ' όλο που το Σύνολο Τερματικών Σταθμών χωράει οριακά και σε μικρότερο υποδίκτυο, επιλέχθηκε το μεγαλύτερο μέγεθος υποδικτύου για ευκολότερη μελλοντική επέκταση.

Για να έχω επιθυμητό subneting πρέπει να ξεκινήσω με το μεγαλύτερο τμήμα και να πάω στο μικρότερο:

1. **Τμήμα wireless LAN**

Network IP: 172.16.0.0/23
Subnet Mask: 1111 1111. 1111 1111. 1111 1110.0000 0000

Το τμήμα αυτό ζητάει 40 hosts οπότε:

64	32	16	8	4	2	1
-----	2^5	2^4	2^3	2^2	2^1	2^0

Οπότε το νέο subnet mask θα είναι:

1111 1111. 1111 1111. 1111 11111.11 00 0000

Ελεύθερα bits για το τμήμα

Στο δεκαδικό: 255.255.255.192 → CIDR /26

Άρα παίρνω τα 8 bit block [0 – 7]

8 bit block [0 – 7]								
Bit #	7	6	5	4	3	2	1	0
Δεκαδικό	128	64	32	16	8	4	2	1
Δυαδικό	0	0	0	0	0	0	0	0

Κανένα δεν χωράει στο 0 οπότε όλα 0

	255	.	255	.	255	.	11	00 0000
AND	172	.	16	.	0	.	00	00 0000
	172	.	16	.	0	.	00	00 0000

Host Part

Αρχική διεύθυνση: 172.16.0.1/26

Για να βρω την broadcast διεύθυνση παίρνω το host part και όπου 0 βάζω 1

11 1111 → 32+16+8+4+2+1=63

Άρα το εύρος διευθύνσεων είναι:

172.16.0.1/26

.
.
.

172.16.0.62/26

Και broadcast διεύθυνση: **172.16.0.63/26**

2. **Τμήμα πωλήσεως**

Network IP: 172.16.0.64

Το τμήμα αυτό ζητάει 30 hosts οπότε:

32	16	8	4	2	1
-----	2^4	2^3	2^2	2^1	2^0

Οπότε το νέο subnet mask θα είναι:

1111 1111. 1111 1111. 1111 11111.111 00000

Ελεύθερα bits για το τμήμα

Στο δεκαδικό: 255.255.255.224 → CIDR /27

Άρα παίρνω τα 8 bit block [0 – 7]

8 bit block [0 – 7]								
Bit #	7	6	5	4	3	2	1	0
Δεκαδικό	128	64	32	16	8	4	2	1
Δυαδικό	0	1	0	0	0	0	0	0

Το 128 δεν χωράει στο 64 οπότε 0
Το 64 στο 64 χωράει άρα 1
Τα υπόλοιπα μηδέν

	255	.	255	.	255	.	111	00000
AND	172	.	16	.	0	.	010	00000
	172	.	16	.	0	.	010	00000

Host Part

Αρχική διεύθυνση: 172.16.0.65/27

Για να βρω την broadcast διεύθυνση παίρνω το host part και όπου 0 βάζω 1

11 111 → 16+8+4+2+1= 31→ 31+64=95

Άρα η broadcast διεύθυνση είναι η: **172.16.0.95/27**

Άρα το εύρος διευθύνσεων είναι:

172.16.0.65/27

.

.

.

172.16.0.94/27

3. **Τμήμα Management VLAN**

Network IP: 172.16.0.96

Το τμήμα αυτό ζητάει 30 hosts οπότε:

32	16	8	4	2	1
-----	2^4	2^3	2^2	2^1	2^0

Οπότε το νέο subnet mask θα είναι:

1111 1111. 1111 1111. 1111 11111.111 00000

Ελεύθερα bits για το τμήμα

Στο δεκαδικό: 255.255.255.224 → CIDR /27

Άρα παίρνω τα 8 bit block [0 – 7]

8 bit block [0 – 7]								
Bit #	7	6	5	4	3	2	1	0
Δεκαδικό	128	64	32	16	8	4	2	1
Δυαδικό	0	1	1	0	0	0	0	0

Το 128 δεν χωράει στο 96 οπότε 0
Το 64 στο 96 χωράει άρα 1 → 96-64 =32
Το 32 στο 32 χωράει άρα 1 → 32 -32 =0
Όλα τα υπόλοιπα μηδέν

	255	.	255	.	255	.	111	00000
AND	172	.	16	.	0	.	011	00000
	172	.	16	.	0	.	011	00000

Host Part

Αρχική διεύθυνση: 172.16.0.97/27

Για να βρω την broadcast διεύθυνση παίρνω το host part και όπου 0 βάζω 1

11 111 → 16+8+4+2+1= 31→ 31+96= 127

Άρα η broadcast διεύθυνση είναι η: **172.16.0.127/27**

Άρα το εύρος διευθύνσεων είναι:

172.16.0.97/27
.
.
.
172.16.0.126/27

4. **Τμήμα Λογιστηρίου**

Network IP: 172.16.0.128

Το τμήμα αυτό ζητάει 14 hosts οπότε:

16	8	4	2	1
-----	2^3	2^2	2^1	2^0

Οπότε το νέο subnet mask θα είναι:

1111 1111. 1111 1111. 1111 11111.1111 0000

Ελεύθερα bits για το τμήμα

Στο δεκαδικό: 255.255.255.240 → CIDR /28

Άρα παίρνω τα 8 bit block [0 – 7]

8 bit block [0 – 7]								
Bit #	7	6	5	4	3	2	1	0
Δεκαδικό	128	64	32	16	8	4	2	1
Δυαδικό	1	0	0	0	0	0	0	0

Το 128 στο 128 χωράει άρα 1 → 128-128 =0
Όλα τα υπόλοιπα μηδέν

	255	.	255	.	255	.	1111	0000
AND	172	.	16	.	0	.	1000	0000
	172	.	16	.	0	.	1000	0000

Host Part

Αρχική διεύθυνση: 172.16.0.129/28

Για να βρω την broadcast διεύθυνση παίρνω το host part και όπου 0 βάζω 1

1111 → 8+4+2+1= 15→ 15+128=143

Άρα η broadcast διεύθυνση είναι η: **172.16.0.143/28**

Άρα το εύρος διευθύνσεων είναι:

172.16.0.129/28
.
.
.
172.16.0.142/28

5. **Τμήμα Διοίκησης**

Network IP: 172.16.0.144

Το τμήμα αυτό ζητάει 14 hosts οπότε:

16	8	4	2	1
-----	2^3	2^2	2^1	2^0

Οπότε το νέο subnet mask θα είναι:

1111 1111. 1111 1111. 1111 11111.1111 0000

Ελεύθερα bits για το τμήμα

Στο δεκαδικό: 255.255.255.240 → CIDR /28

Άρα παίρνω τα 8 bit block [0 – 7]

8 bit block [0 – 7]								
Bit #	7	6	5	4	3	2	1	0
Δεκαδικό	128	64	32	16	8	4	2	1
Δυαδικό	1	0	0	1	0	0	0	0

Το 128 στο 144 χωράει άρα 1 → 144-128 =16
Το 64 στο 16 δεν χωράει άρα 0
Το 32 στο 16 δεν χωράει άρα 0
Το 16 στο 16 χωράει άρα 1 → 16-16 =0
Όλα τα υπόλοιπα μηδέν

	255	.	255	.	255	.	1111	0000
AND	172	.	16	.	0	.	1001	0000
	172	.	16	.	0	.	1001	0000

Host Part

Αρχική διεύθυνση: 172.16.0.145/28

Για να βρω την broadcast διεύθυνση παίρνω το host part και όπου 0 βάζω 1

1111 → 8+4+2+1= 15→ 15+144=159

Άρα η broadcast διεύθυνση είναι η: **172.16.0.159/28**

Άρα το εύρος διευθύνσεων είναι:

172.16.0.145/28
.
.
.
172.16.0.158/28

6. **Τμήμα Marketing**

Network IP: 172.16.0.160

Το τμήμα αυτό ζητάει 14 hosts οπότε:

16	8	4	2	1
-----	2^3	2^2	2^1	2^0

Οπότε το νέο subnet mask θα είναι:

1111 1111. 1111 1111. 1111 11111.1111 0000

Ελεύθερα bits για το τμήμα

Στο δεκαδικό: 255.255.255.240 → CIDR /28

Άρα παίρνω τα 8 bit block [0 – 7]

8 bit block [0 – 7]								
Bit #	7	6	5	4	3	2	1	0
Δεκαδικό	128	64	32	16	8	4	2	1
Δυαδικό	1	0	1	0	0	0	0	0

Το 128 στο 160 χωράει άρα 1 → 160-128 =32
Το 64 στο 32 δεν χωράει άρα 0
Το 32 στο 32 χωράει άρα 1 → 32-32 =0
Όλα τα υπόλοιπα μηδέν

	255	.	255	.	255	.	1111	0000
AND	172	.	16	.	0	.	1010	0000
	172	.	16	.	0	.	1010	0000

Host Part

Αρχική διεύθυνση: 172.16.0.161/28

Για να βρω την broadcast διεύθυνση παίρνω το host part και όπου 0 βάζω 1

1111 → 8+4+2+1= 15→ 15+160=175

Άρα η broadcast διεύθυνση είναι η: **172.16.0.175/28**

Άρα το εύρος διευθύνσεων είναι:

172.16.0.161/28

.
.
.

172.16.0.174/28

7. **Τμήμα Server LAN**

Network IP: 172.16.0.176

Το τμήμα αυτό ζητάει 14 hosts οπότε:

16	8	4	2	1
-----	2^3	2^2	2^1	2^0

Οπότε το νέο subnet mask θα είναι:

1111 1111. 1111 1111. 1111 11111.1111 0000

Ελεύθερα bits για το τμήμα

Στο δεκαδικό: 255.255.255.240 → CIDR /28

Άρα παίρνω τα 8 bit block [0 – 7]

8 bit block [0 – 7]								
Bit #	7	6	5	4	3	2	1	0
Δεκαδικό	128	64	32	16	8	4	2	1
Δυαδικό	1	0	1	1	0	0	0	0

Το 128 στο 176 χωράει άρα 1 → 176-128 =48
Το 64 στο 48 δεν χωράει άρα 0
Το 32 στο 48 χωράει άρα 1 → 48-32 =16
Το 16 στο 16 χωράει άρα 1 → 16-16 =0
Όλα τα υπόλοιπα μηδέν

	255	.	255	.	255	.	1111	0000
AND	172	.	16	.	0	.	1011	0000
	172	.	16	.	0	.	1011	0000

Host Part

Αρχική διεύθυνση: 172.16.0.177/28

Για να βρω την broadcast διεύθυνση παίρνω το host part και όπου 0 βάζω 1

1111 → 8+4+2+1= 15→ 15+176=191

Άρα η broadcast διεύθυνση είναι η: **172.16.0.191/28**

Άρα το εύρος διευθύνσεων είναι:

172.16.0.177/28

.
.
.

172.16.0.190/28

8. **Τμήμα Πληροφορικής**

Network IP: 172.16.0.192

Το τμήμα αυτό ζητάει 6 hosts οπότε:

8	4	2	1
-----	2^2	2^1	2^0

Οπότε το νέο subnet mask θα είναι:

1111 1111. 1111 1111. 1111 11111.11111 000

Ελεύθερα bits για το τμήμα

Στο δεκαδικό: 255.255.255.248 → CIDR /29

Άρα παίρνω τα 8 bit block [0 – 7]

8 bit block [0 – 7]								
Bit #	7	6	5	4	3	2	1	0
Δεκαδικό	128	64	32	16	8	4	2	1
Δυαδικό	1	1	0	0	0	0	0	0

Το 128 στο 192 χωράει άρα 1 → 192 - 128 =64
Το 64 στο 64 χωράει άρα 1 → 64 - 64 =0
Όλα τα υπόλοιπα μηδέν

	255	.	255	.	255	.	11111	000
AND	172	.	16	.	0	.	11000	000
	172	.	16	.	0	.	11000	000

Host Part

Αρχική διεύθυνση: 172.16.0.193/29

Για να βρω την broadcast διεύθυνση παίρνω το host part και όπου 0 βάζω 1

111 → 4+2+1= 7→ 7+193=200

Άρα η broadcast διεύθυνση είναι η: **172.16.0.200/29**

Άρα το εύρος διευθύνσεων είναι:

172.16.0.193/29

.

.

.

172.16.0.199/29

9. **Υποκατάστημα**

Για το υποκατάστημα η διευθυνσιοδότηση γίνετε με τέτοιο τρόπο ώστε να μπορούν να προστεθούν κι άλλα υποκαταστήματα στο μέλλον. Ξεκινάμε με διεύθυνση δικτύου 172.16.1.0 οπότε:

Network IP: 172.16.1.0

Το υποκατάστημα ζητάει 14 hosts οπότε:

16	**8**	**4**	**2**	**1**
------	2^3	2^2	2^1	2^0

Οπότε το νέο subnet mask θα είναι:

1111 1111. 1111 1111. 1111 11111.1111 0000

Ελεύθερα bits για το υποκατάστημα

Στο δεκαδικό: 255.255.255.240 → CIDR /28

Άρα παίρνω τα 8 bit block [0 – 7]

8 bit block [0 – 7]								
Bit #	7	6	5	4	3	2	1	0
Δεκαδικό	128	64	32	16	8	4	2	1
Δυαδικό	0	0	0	0	0	0	0	0

Κανένα δεν χωράει στο 0 οπότε όλα 0

	255	.	255	.	255	.	1111	0000
AND	172	.	16	.	0	.	0000	0000
	172	.	16	.	0	.	0000	0000

Host Part

Αρχική διεύθυνση: 172.16.1.1/28

Για να βρω την broadcast διεύθυνση παίρνω το host part και όπου 0 βάζω 1

1111 → 8+4+2+1=15

Άρα το εύρος διευθύνσεων είναι:

172.16.1.1/28

.

.

.

172.16.1.14/28

Και broadcast διεύθυνση: **172.16.1.15/28**

Συγκεντρωτικός πίνακας IP υποδικτύων						
A/A	Τμήμα	Network Διεύθυνση	First host διεύθυνση	Last host διεύθυνση	Broadcast διεύθυνση	Subnet Mask
1	Wireless LAN	172.16.0.0	172.16.0.1	172.16.0.62	172.16.0.63	255.255.255.192
2	Πωλήσεως	172.16.0.64	172.16.0.65	172.126.0.94	172.16.0.95	255.255.255.224
3	Management VLAN	172.16.0.96	172.16.0.97	172.16.0.126	172.16.0.127	255.255.255.224
4	Λογιστηρίου	172.16.0.128	172.16.0.129	172.16.0.142	172.16.0.143	255.255.255.240
5	Διοίκησης	172.16.0.144	172.16.0.145	172.16.0.158	172.16.0.159	255.255.255.240
6	Marketing	172.16.0.160	172.16.0.161	172.16.0.174	172.16.0.175	255.255.255.240
7	Server LAN	172.16.0.176	172.16.0.177	172.16.0.190	172.16.0.191	255.255.255.240
8	Πληροφορικής	172.16.0.192	172.16.0.193	172.16.0.199	172.16.0.200	255.255.255.248
9	Υποκατάστημα	172.16.1.0	172.16.1.1	172.16.1.14	172.16.1.15	255.255.255.240

Πίνακας 3.6: Εύρη IP διευθύνσεων που έχουμε εκχωρήσει σε κάθε τμήμα

A/A	Περιγραφή	IP Διεύθυνση	Στατική ή Δυναμική	VLAN #	VLAN Όνομα	Μάσκα υποδικτύου
1	Network	172.16.0.0	-	100	wireless	255.255.255.192
2	Gateway	172.16.0.1	Στατική	100	wireless	255.255.255.192
3	Core A	172.16.0.2	Στατική	100	wireless	255.255.255.192
4	Core B	172.16.0.3	Στατική	100	wireless	255.255.255.192
5	Host	172.16.0.4	Δυναμική	100	wireless	255.255.255.192
6	Host	172.16.0.5	Δυναμική	100	wireless	255.255.255.192
7	Host	172.16.0.6	Δυναμική	100	wireless	255.255.255.192
8	Host	172.16.0.7	Δυναμική	100	wireless	255.255.255.192
9	Host	172.16.0.8	Δυναμική	100	wireless	255.255.255.192
10	Host	172.16.0.9	Δυναμική	100	wireless	255.255.255.192
11	Host	172.16.0.10	Δυναμική	100	wireless	255.255.255.192
12	Host	172.16.0.11	Δυναμική	100	wireless	255.255.255.192
13	Host	172.16.0.12	Δυναμική	100	wireless	255.255.255.192
14	Host	172.16.0.13	Δυναμική	100	wireless	255.255.255.192
15	Host	172.16.0.14	Δυναμική	100	wireless	255.255.255.192
16	Host	172.16.0.15	Δυναμική	100	wireless	255.255.255.192
17	Host	172.16.0.16	Δυναμική	100	wireless	255.255.255.192
18	Host	172.16.0.17	Δυναμική	100	wireless	255.255.255.192
19	Host	172.16.0.18	Δυναμική	100	wireless	255.255.255.192
20	Host	172.16.0.19	Δυναμική	100	wireless	255.255.255.192
21	Host	172.16.0.20	Δυναμική	100	wireless	255.255.255.192
22	Host	172.16.0.21	Δυναμική	100	wireless	255.255.255.192
23	Host	172.16.0.22	Δυναμική	100	wireless	255.255.255.192
24	Host	172.16.0.23	Δυναμική	100	wireless	255.255.255.192
25	Host	172.16.0.24	Δυναμική	100	wireless	255.255.255.192
26	Host	172.16.0.25	Δυναμική	100	wireless	255.255.255.192
27	Host	172.16.0.26	Δυναμική	100	wireless	255.255.255.192

28	Host	172.16.0.27	Δυναμική	100	wireless	255.255.255.192
29	Host	172.16.0.28	Δυναμική	100	wireless	255.255.255.192
30	Host	172.16.0.29	Δυναμική	100	wireless	255.255.255.192
31	Host	172.16.0.30	Δυναμική	100	wireless	255.255.255.192
32	Host	172.16.0.31	Δυναμική	100	wireless	255.255.255.192
33	Host	172.16.0.32	Δυναμική	100	wireless	255.255.255.192
34	Host	172.16.0.33	Δυναμική	100	wireless	255.255.255.192
35	Host	172.16.0.34	Δυναμική	100	wireless	255.255.255.192
36	Host	172.16.0.35	Δυναμική	100	wireless	255.255.255.192
37	Host	172.16.0.36	Δυναμική	100	wireless	255.255.255.192
38	Host	172.16.0.37	Δυναμική	100	wireless	255.255.255.192
39	Host	172.16.0.38	Δυναμική	100	wireless	255.255.255.192
40	Host	172.16.0.39	Δυναμική	100	wireless	255.255.255.192
41	Host	172.16.0.40	Δυναμική	100	wireless	255.255.255.192
42	Host	172.16.0.41	Δυναμική	100	wireless	255.255.255.192
43	Host	172.16.0.42	Δυναμική	100	wireless	255.255.255.192
44	Host	172.16.0.43	Δυναμική	100	wireless	255.255.255.192
45	Host	172.16.0.44	Δυναμική	100	wireless	255.255.255.192
46	Host	172.16.0.45	Δυναμική	100	wireless	255.255.255.192
47	Host	172.16.0.46	Δυναμική	100	wireless	255.255.255.192
48	Host	172.16.0.47	Δυναμική	100	wireless	255.255.255.192
49	Host	172.16.0.48	Δυναμική	100	wireless	255.255.255.192
50	Host	172.16.0.49	Δυναμική	100	wireless	255.255.255.192
51	Host	172.16.0.50	Δυναμική	100	wireless	255.255.255.192
52	Host	172.16.0.51	Δυναμική	100	wireless	255.255.255.192
53	Host	172.16.0.52	Δυναμική	100	wireless	255.255.255.192
54	Host	172.16.0.53	Δυναμική	100	wireless	255.255.255.192
55	Host	172.16.0.54	Δυναμική	100	wireless	255.255.255.192
56	Host	172.16.0.55	Δυναμική	100	wireless	255.255.255.192
57	Host	172.16.0.56	Δυναμική	100	wireless	255.255.255.192
58	Host	172.16.0.57	Δυναμική	100	wireless	255.255.255.192
59	Host	172.16.0.58	Δυναμική	100	wireless	255.255.255.192
60	Host	172.16.0.59	Δυναμική	100	wireless	255.255.255.192
61	Host	172.16.0.60	Δυναμική	100	wireless	255.255.255.192
62	Host	172.16.0.61	Δυναμική	100	wireless	255.255.255.192
63	Host	172.16.0.62	Δυναμική	100	wireless	255.255.255.192
64	Broadcast	172.16.0.63	-	100	wireless	255.255.255.192
65	Network	172.16.0.64	-	110	sales	255.255.255.224
66	Gateway	172.16.0.65	Στατική	110	sales	255.255.255.224
67	Core A	172.16.0.66	Στατική	110	sales	255.255.255.224
68	Core B	172.16.0.67	Στατική	110	sales	255.255.255.224
69	Host	172.16.0.68	Στατική	110	sales	255.255.255.224
70	Host	172.16.0.69	Στατική	110	sales	255.255.255.224
71	Host	172.16.0.70	Στατική	110	sales	255.255.255.224
72	Host	172.16.0.71	Στατική	110	sales	255.255.255.224
73	Host	172.16.0.72	Δυναμική	110	sales	255.255.255.224

74	Host	172.16.0.73	Δυναμική	110	sales	255.255.255.224
75	Host	172.16.0.74	Δυναμική	110	sales	255.255.255.224
76	Host	172.16.0.75	Δυναμική	110	sales	255.255.255.224
77	Host	172.16.0.76	Δυναμική	110	sales	255.255.255.224
78	Host	172.16.0.77	Δυναμική	110	sales	255.255.255.224
79	Host	172.16.0.78	Δυναμική	110	sales	255.255.255.224
80	Host	172.16.0.79	Δυναμική	110	sales	255.255.255.224
81	Host	172.16.0.80	Δυναμική	110	sales	255.255.255.224
82	Host	172.16.0.81	Δυναμική	110	sales	255.255.255.224
83	Host	172.16.0.82	Δυναμική	110	sales	255.255.255.224
84	Host	172.16.0.83	Δυναμική	110	sales	255.255.255.224
85	Host	172.16.0.84	Δυναμική	110	sales	255.255.255.224
86	Host	172.16.0.85	Δυναμική	110	sales	255.255.255.224
87	Host	172.16.0.86	Δυναμική	110	sales	255.255.255.224
88	Host	172.16.0.87	Δυναμική	110	sales	255.255.255.224
89	Host	172.16.0.88	Δυναμική	110	sales	255.255.255.224
90	Host	172.16.0.89	Δυναμική	110	sales	255.255.255.224
91	Host	172.16.0.90	Δυναμική	110	sales	255.255.255.224
92	Host	172.16.0.91	Δυναμική	110	sales	255.255.255.224
93	Host	172.16.0.92	Δυναμική	110	sales	255.255.255.224
94	Host	172.16.0.93	Δυναμική	110	sales	255.255.255.224
95	Host	172.16.0.94	Δυναμική	110	sales	255.255.255.224
96	Broadcast	172.16.0.95	-	110	sales	255.255.255.224
97	Network	172.16.0.96	-	120	ManagementVlan	255.255.255.224
98	Gateway	172.16.0.97	Στατική	120	ManagementVlan	255.255.255.224
99	Core A	172.16.0.98	Στατική	120	ManagementVlan	255.255.255.224
100	Core B Server	172.16.0.99	Στατική	120	ManagementVlan	255.255.255.224
101	Switch A Server	172.16.0.100	Στατική	120	ManagementVlan	255.255.255.224
102	Switch B	172.16.0.101	Στατική	120	ManagementVlan	255.255.255.224
103	Host	172.16.0.102	Στατική	120	ManagementVlan	255.255.255.224
104	Host	172.16.0.103	Στατική	120	ManagementVlan	255.255.255.224
105	Host	172.16.0.104	Στατική	120	ManagementVlan	255.255.255.224
106	Host	172.16.0.105	Στατική	120	ManagementVlan	255.255.255.224
107	Host	172.16.0.106	Στατική	120	ManagementVlan	255.255.255.224
108	Host	172.16.0.107	Στατική	120	ManagementVlan	255.255.255.224
109	Host	172.16.0.108	Στατική	120	ManagementVlan	255.255.255.224
110	Host	172.16.0.109	Στατική	120	ManagementVlan	255.255.255.224
111	Host	172.16.0.110	Στατική	120	ManagementVlan	255.255.255.224
112	Host	172.16.0.111	Στατική	120	ManagementVlan	255.255.255.224
113	Host	172.16.0.112	Στατική	120	ManagementVlan	255.255.255.224
114	Host	172.16.0.113	Στατική	120	ManagementVlan	255.255.255.224
115	Host	172.16.0.114	Στατική	120	ManagementVlan	255.255.255.224
116	Host	172.16.0.115	Στατική	120	ManagementVlan	255.255.255.224
117	Host	172.16.0.116	Στατική	120	ManagementVlan	255.255.255.224
118	Host	172.16.0.117	Στατική	120	ManagementVlan	255.255.255.224

119	Host	172.16.0.118	Στατική	120	ManagementVlan	255.255.255.224
120	Host	172.16.0.119	Στατική	120	ManagementVlan	255.255.255.224
121	Host	172.16.0.120	Στατική	120	ManagementVlan	255.255.255.224
122	Host	172.16.0.121	Στατική	120	ManagementVlan	255.255.255.224
123	Host	172.16.0.122	Στατική	120	ManagementVlan	255.255.255.224
124	Host	172.16.0.123	Στατική	120	ManagementVlan	255.255.255.224
125	Host	172.16.0.124	Στατική	120	ManagementVlan	255.255.255.224
126	Host	172.16.0.125	Στατική	120	ManagementVlan	255.255.255.224
127	Host	172.16.0.126	Στατική	120	ManagementVlan	255.255.255.224
128	Broadcast	172.16.0.127	-	120	ManagementVlan	255.255.255.224
129	Network	172.16.0.128	-	130	Accounting office	255.255.255.240
130	Gateway	172.16.0.129	Στατική	130	Accounting office	255.255.255.240
131	Core A	172.16.0.130	Στατική	130	Accounting office	255.255.255.240
132	Core B	172.16.0.131	Στατική	130	Accounting office	255.255.255.240
133	Host	172.16.0.132	Στατική	130	Accounting office	255.255.255.240
134	Host	172.16.0.133	Στατική	130	Accounting office	255.255.255.240
135	Host	172.16.0.134	Στατική	130	Accounting office	255.255.255.240
136	Host	172.16.0.135	Δυναμική	130	Accounting office	255.255.255.240
137	Host	172.16.0.136	Δυναμική	130	Accounting office	255.255.255.240
138	Host	172.16.0.137	Δυναμική	130	Accounting office	255.255.255.240
139	Host	172.16.0.138	Δυναμική	130	Accounting office	255.255.255.240
140	Host	172.16.0.139	Δυναμική	130	Accounting office	255.255.255.240
141	Host	172.16.0.140	Δυναμική	130	Accounting office	255.255.255.240
142	Host	172.16.0.141	Δυναμική	130	Accounting office	255.255.255.240
143	Host	172.16.0.142	Δυναμική	130	Accounting office	255.255.255.240
144	Broadcast	172.16.0.143	-	130	Accounting office	255.255.255.240
145	Network	172.16.0.144	-	140	Administration	255.255.255.240
146	Gateway	172.16.0.145	Στατική	140	Administration	255.255.255.240
147	Core A	172.16.0.146	Στατική	140	Administration	255.255.255.240
148	Core B	172.16.0.147	Στατική	140	Administration	255.255.255.240
149	Host	172.16.0.148	Στατική	140	Administration	255.255.255.240
150	Host	172.16.0.149	Στατική	140	Administration	255.255.255.240
151	Host	172.16.0.150	Στατική	140	Administration	255.255.255.240
152	Host	172.16.0.151	Δυναμική	140	Administration	255.255.255.240
153	Host	172.16.0.152	Δυναμική	140	Administration	255.255.255.240

154	Host	172.16.0.153	Δυναμική	140	Administration	255.255.255.240
155	Host	172.16.0.154	Δυναμική	140	Administration	255.255.255.240
156	Host	172.16.0.155	Δυναμική	140	Administration	255.255.255.240
157	Host	172.16.0.156	Δυναμική	140	Administration	255.255.255.240
158	Host	172.16.0.157	Δυναμική	140	Administration	255.255.255.240
159	Host	172.16.0.158	Δυναμική	140	Administration	255.255.255.240
160	Broadcast	172.16.0.159	-	140	Administration	255.255.255.240
161	Network	172.16.0.160	-	150	Marketing	255.255.255.240
162	Gateway	172.16.0.161	Στατική	150	Marketing	255.255.255.240
163	Core A	172.16.0.162	Στατική	150	Marketing	255.255.255.240
164	Core B	172.16.0.163	Στατική	150	Marketing	255.255.255.240
165	Host	172.16.0.164	Στατική	150	Marketing	255.255.255.240
166	Host	172.16.0.165	Στατική	150	Marketing	255.255.255.240
167	Host	172.16.0.166	Στατική	150	Marketing	255.255.255.240
168	Host	172.16.0.167	Δυναμική	150	Marketing	255.255.255.240
169	Host	172.16.0.168	Δυναμική	150	Marketing	255.255.255.240
170	Host	172.16.0.169	Δυναμική	150	Marketing	255.255.255.240
171	Host	172.16.0.170	Δυναμική	150	Marketing	255.255.255.240
172	Host	172.16.0.171	Δυναμική	150	Marketing	255.255.255.240
173	Host	172.16.0.172	Δυναμική	150	Marketing	255.255.255.240
174	Host	172.16.0.173	Δυναμική	150	Marketing	255.255.255.240
175	Host	172.16.0.174	Δυναμική	150	Marketing	255.255.255.240
176	Broadcast	172.16.0.175	-	150	Marketing	255.255.255.240
177	Network	172.16.0.176	-	160	Server LAN	255.255.255.240
178	Gateway	172.16.0.177	Στατική	160	Server LAN	255.255.255.240
179	Core A	172.16.0.178	Στατική	160	Server LAN	255.255.255.240
180	Core B	172.16.0.179	Στατική	160	Server LAN	255.255.255.240
181	Host	172.16.0.180	Στατική	160	Server LAN	255.255.255.240
182	Host	172.16.0.181	Στατική	160	Server LAN	255.255.255.240
183	Host	172.16.0.182	Στατική	160	Server LAN	255.255.255.240
184	Host	172.16.0.183	Στατική	160	Server LAN	255.255.255.240
185	Host	172.16.0.184	Στατική	160	Server LAN	255.255.255.240
186	Host	172.16.0.185	Στατική	160	Server LAN	255.255.255.240
187	Host	172.16.0.186	Στατική	160	Server LAN	255.255.255.240
188	Host	172.16.0.187	Στατική	160	Server LAN	255.255.255.240
189	Host	172.16.0.188	Στατική	160	Server LAN	255.255.255.240
190	Host	172.16.0.189	Στατική	160	Server LAN	255.255.255.240
191	Host	172.16.0.190	Στατική	160	Server LAN	255.255.255.240
192	Broadcast	172.16.0.191	-	160	Server LAN	255.255.255.240
193	Network	172.16.0.192	-	170	IT dep	255.255.255.248
194	Gateway	172.16.0.193	Στατική	170	IT dep	255.255.255.248
195	Core A	172.16.0.194	Στατική	170	IT dep	255.255.255.248
196	Core B	172.16.0.195	Στατική	170	IT dep	255.255.255.248
197	Host	172.16.0.196	Στατική	170	IT dep	255.255.255.248
198	Host	172.16.0.197	Στατική	170	IT dep	255.255.255.248
199	Host	172.16.0.198	Στατική	170	IT dep	255.255.255.248

200	Broadcast	172.16.0.199	-	170	IT dep	255.255.255.248
201	Network	172.16.0.200	-			255.255.255.248
202	Core A	172.16.0.201	Στατική			255.255.255.248
203	ASA	172.16.0.202	Στατική			255.255.255.248
204	Host	172.16.0.203	Στατική	Δίκτυο Σύνδεσης Core A - ASA		255.255.255.248
205	Host	172.16.0.204	Στατική			255.255.255.248
206	Host	172.16.0.205	Στατική			255.255.255.248
207	Host	172.16.0.206	Στατική			255.255.255.248
208	Broadcast	172.16.0.207	-			255.255.255.248
209	Network	172.16.0.208	-			255.255.255.248
210	Core B	172.16.0.209	Στατική			255.255.255.248
211	ASA	172.16.0.210	Στατική			255.255.255.248
212	Host	172.16.0.211	Στατική	Δίκτυο Σύνδεσης Core B - ASA		255.255.255.248
213	Host	172.16.0.212	Στατική			255.255.255.248
214	Host	172.16.0.213	Στατική			255.255.255.248
215	Host	172.16.0.214	Στατική			255.255.255.248
216	Broadcast	172.16.0.215	-			255.255.255.248
217	Network ADSL	172.16.0.216	-			255.255.255.248
218	Router	172.16.0.217	Στατική			255.255.255.248
219	ASA	172.16.0.218	Στατική			255.255.255.248
220	Host	172.16.0.219	Στατική	Δίκτυο Σύνδεσης ASA - ADSL Rouer (techcom)		255.255.255.248
221	Host	172.16.0.220	Στατική			255.255.255.248
222	Host	172.16.0.221	Στατική			255.255.255.248
223	Host	172.16.0.222	Στατική			255.255.255.248
224	Broadcast	172.16.0.223	-			255.255.255.248
225		172.16.0.224	NOT USED			
226		172.16.0.225	NOT USED			
227		172.16.0.226	NOT USED			
228		172.16.0.227	NOT USED			
229		172.16.0.228	NOT USED			
230		172.16.0.229	NOT USED			
231		172.16.0.230	NOT USED			
232		172.16.0.231	NOT USED			
233		172.16.0.232	NOT USED			
234		172.16.0.233	NOT USED			
235		172.16.0.234	NOT USED			
236		172.16.0.235	NOT USED			
237		172.16.0.236	NOT USED			
238		172.16.0.237	NOT USED			
239		172.16.0.238	NOT USED			
240		172.16.0.239	NOT USED			
241		172.16.0.240	NOT USED			
242		172.16.0.241	NOT USED			
243		172.16.0.242	NOT USED			
244		172.16.0.243	NOT USED			

245		172.16.0.244	NOT USED		
246		172.16.0.245	NOT USED		
247		172.16.0.246	NOT USED		
248		172.16.0.247	NOT USED		
249		172.16.0.248	NOT USED		
250		172.16.0.249	NOT USED		
251		172.16.0.250	NOT USED		
252		172.16.0.251	NOT USED		
253		172.16.0.252	NOT USED		
254		172.16.0.253	NOT USED		
255		172.16.0.254	NOT USED		
256		172.16.0.255	NOT USED		
257	Network	172.16.1.0	-	Δίκτυο Υποκαταστήματος	255.255.255.240
258	ASA_2	172.16.1.1	Στατική		255.255.255.240
259	Branch	172.16.1.2	Στατική		255.255.255.240
260	Host	172.16.1.3	Στατική		255.255.255.240
261	Host	172.16.1.4	Στατική		255.255.255.240
262	Host	172.16.1.5	Στατική		255.255.255.240
263	Host	172.16.1.6	Στατική		255.255.255.240
264	Host	172.16.1.7	Δυναμική		255.255.255.240
265	Host	172.16.1.8	Δυναμική		255.255.255.240
266	Host	172.16.1.9	Δυναμική		255.255.255.240
267	Host	172.16.1.10	Δυναμική		255.255.255.240
268	Host	172.16.1.11	Δυναμική		255.255.255.240
269	Host	172.16.1.12	Δυναμική		255.255.255.240
270	Host	172.16.1.13	Δυναμική		255.255.255.240
271	Host	172.16.1.14	Δυναμική		255.255.255.240
272	Broadcast	172.16.1.15	-		255.255.255.240
273		172.16.1.16	NOT USED		
274		172.16.1.17	NOT USED		
275		172.16.1.18	NOT USED		
276		172.16.1.19	NOT USED		
277		172.16.1.20	NOT USED		
278		172.16.1.21	NOT USED		
279		172.16.1.22	NOT USED		
280		172.16.1.23	NOT USED		
281		172.16.1.24	NOT USED		
282		172.16.1.25	NOT USED		
283		172.16.1.26	NOT USED		
284		172.16.1.27	NOT USED		
285		172.16.1.28	NOT USED		
286		172.16.1.29	NOT USED		
287		172.16.1.30	NOT USED		
288		172.16.1.31	NOT USED		
289		172.16.1.32	NOT USED		
290		172.16.1.33	NOT USED		

291	172.16.1.34	NOT USED
292	172.16.1.35	NOT USED
293	172.16.1.36	NOT USED
	•	
	•	
	•	
	•	
294	172.16.1.37	NOT USED
295	172.16.1.38	NOT USED
510	172.16.1.253	NOT USED
511	172.16.1.254	NOT USED
512	172.16.1.255	NOT USED

Πίνακας 3.7: Συγκεντρωτικός πίνακας για κάθε IP διεύθυνση και σε ποιο τμήμα ανήκει η κάθε μια

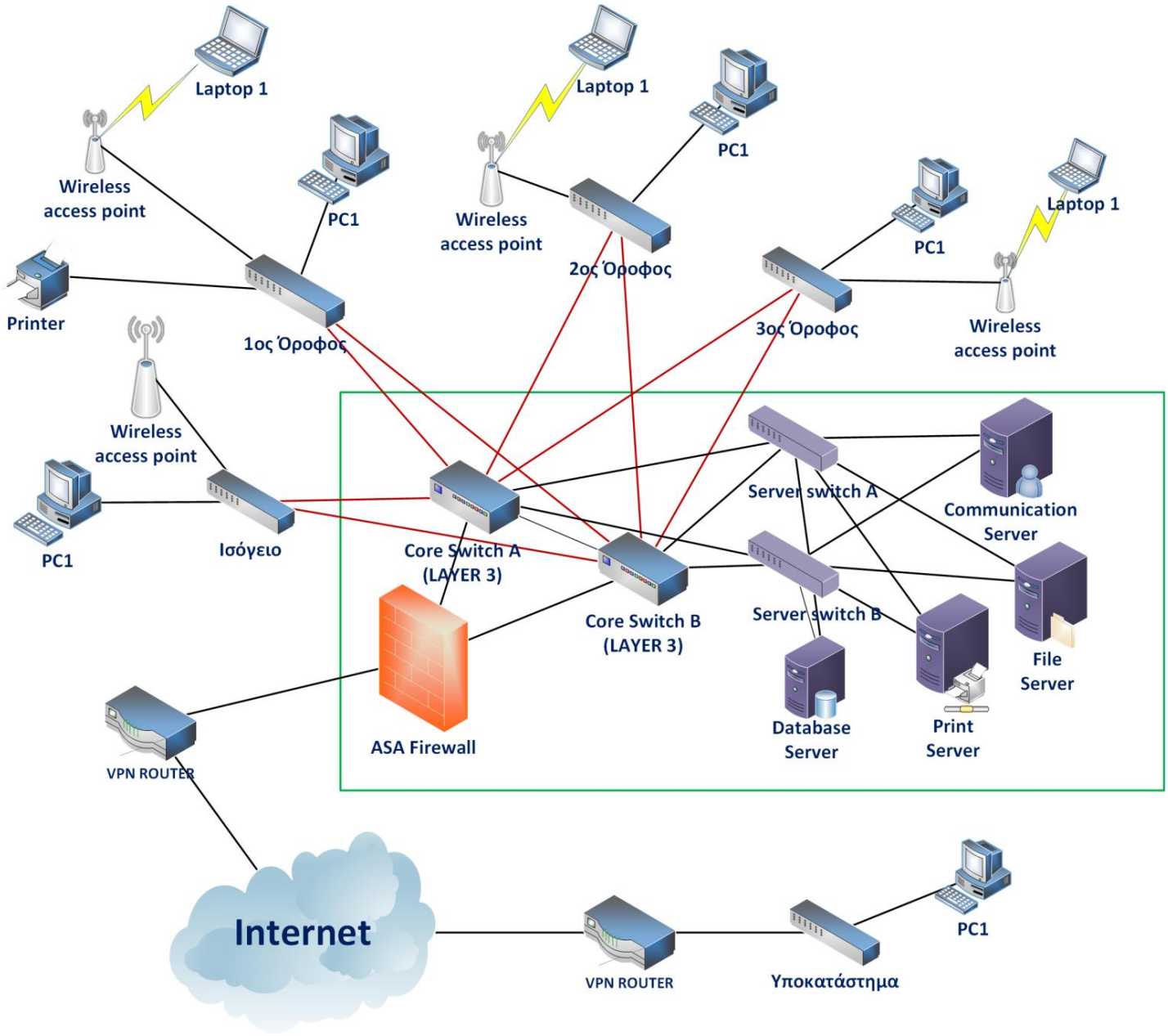
3.2.3 Βασικός σχεδιασμός δικτύου

Με βάση τις προδιαγραφές και τις απαιτήσεις της εταιρίας θα σχεδιάσουμε το παρακάτω την βασική υλοποίηση του δικτύου.
Στο κεντρικό μας κατάστημα έχουμε ένα τριώροφο κτήριο το οποίο θα στεγάζει τα διάφορα τμήματα εργασίας που έχουμε συμπεριλάβει στο επιχειρησιακό μας δίκτυο. Στο ισόγειο βρίσκεται ένα άτομο του τμήματος διοίκησης στην υποδοχή καθώς και το τμήμα πληροφορικής, στον $1^{ο}$ όροφο έχουμε το τμήμα Λογιστηρίου και το τμήμα πωλήσεων, στον $2^{ο}$ όροφο έχουμε το τμήμα Marketing και το υπόλοιπο κομμάτι του τμήματος πωλήσεων που δεν χώρεσε στον $1^{ο}$ όροφο και τέλος στον $3^{ο}$ όροφο έχουμε το τμήμα διοίκησης. Να σημειωθεί ότι σε κάθε όροφο υπάρχουν ασύρματα σημεία πρόσβασης (wireless access points).
Σημαντικό είναι ότι ο κάθε όροφος θα διαθέτει έναν μεταγωγέα (switch) επιπέδου 2 (layer 2) όπου πάνω σε αυτόν θα συνδέονται όλες οι τερματικές συσκευές του. Αυτοί οι μεταγωγοί αποτελούν το δίκτυο πρόσβασης.
Το δίκτυο κορμού (core network) αποτελείται από δύο μεταγωγείς (switches) επιπέδου 3 (layer 3) όπου σε περίπτωση που ο πρώτος μεταγωγέας καταστραφεί ή πάθει μια βλάβη να υπάρχει κι ένας δεύτερος ως εφεδρικός για ασφάλεια.
Μετά τους μεταγωγείς (switches) θα ακολουθήσει κι ένα ASA Firewall ώστε να μας παρέχει προστασία από τρίτους που θα θελήσουν να αποκτήσουν πρόσβαση στα δεδομένα της εταιρίας μας. Αυτό το firewall με τη σειρά του θα παρέχει την έξοδο μας στο διαδίκτυο. Για να επικοινωνήσουμε με το υποκατάστημα από την μεριά του υποκαταστήματος θα υπάρχει επίσης ένα ASA firewall ώστε να προστατεύει και αυτό το δίκτυο. Οι servers που θα χρησιμοποιήσουμε θα είναι τέσσερις και είναι οι εξής:

- communication server
- Database server
- Print server
- file server

Κι εδώ η μεταξύ τους σύνδεση με το δίκτυο θα γίνετε με δύο switches (Layer 2) για τον ίδιο λόγο ασφάλειας και εφεδρείας που αναφέραμε και παραπάνω.

Σύμφωνα με τις απαιτήσεις της εταιρίας, τα φυσικά μέσα σύνδεσης που θα χρησιμοποιηθούν για την διασύνδεση των τερματικών συσκευών στον κάθε όροφο του κεντρικού καταστήματος θα γίνετε με χάλκινο καλώδιο, η διασύνδεση των ορόφων μεταξύ των Core switch A και Core switch B θα γίνετε με οπτική ίνα όπου και οι δύο θα συνδέονται μεταξύ τους με χάλκινο καλώδιο και η διασύνδεση των server και του υποκαταστήματος θα γίνετε κι αυτή με χάλκινο καλώδιο.



Εικόνα 3.5: Προσχέδιο του εταιρικού δικτύου

3.2.4 Απαραίτητες ρυθμίσεις για την εφαρμογή απαιτήσεων της εταιρίας

A/A	Ρύθμιση	Τιμή	Σημειώσεις
1	enable password	cisco123	Χρησιμοποιείται η κρυπτογραφημένη μορφή του password
2	vty password	cisco123	
3	console password	cisco123	
4	ssh	Ενεργοποιημένο	
5	dhcp	Ενεργοποιημένο	Εκτός από τα VLAN Servers και Management

1. **Πρωτόκολλα που θα χρησιμοποιηθούν**

   - HSRP – Hot Standby Router Protocol – για την εφεδρεία των δύο κεντρικών μεταγωγών επίπεδου 3
   - STP – Spanning Tree Protocol – για την λειτουργία των εφεδρικών συνδέσεων 2^{ου} επιπέδου
   - VTP – VLAN Trunking Protocol – για την δημιουργία και διαχείριση των VLANs
   - DHCP – Dynamic Host Configuration Protocol – για την διαχείριση των IP διευθύνσεων
   - VPN/IPSec – Virtual Private Network/IP Security – για την ασφαλή διασύνδεση του υποκαταστήματος
   - SSH – Secure Shell – για την ασφαλή σύνδεση και ρύθμιση των ενεργών στοιχείων
   - Access Lists – Εφαρμογή access lists για περιορισμό πρόσβασης σε συγκεκριμένους servers ή υπηρεσίες
   - ASA Firewall – Adaptive Security Appliance Firewall

2. **Άλλες ενέργειες ασφάλειας**

   - Εφαρμογή φυσικής ασφάλειας στο datacenter και στους κατανεμητές
     - Πυρασφάλεια, κλιματισμός, περιορισμένη πρόσβαση στους χώρους, προστασία ρεύματος (UPS, γεννήτρια κτλ)
   - Χρήστες στα PC δεν θα είναι administrators
   - Θα υπάρχει κωδικός πρόσβασης με κατάλληλες προδιαγραφές για την πρόσβαση στον ενεργό εξοπλισμό
   - Θα απενεργοποιηθεί το http access στον ενεργό εξοπλισμό

3.2.5 Καταγραφή ρυθμίσεων ενεργών στοιχείων

A/A	Περιγραφή	Τιμή
1	VTP Server	Core Switch A
2	VTP Domain	techcom.gr
3	VTP Password	cisco123
4	VTP Version	2

Πίνακας 3.8: Ρυθμίσεις VTP

A/A	Περιγραφή	Τιμή
1	enable secret	cisco123
2	telnet	Disabled
3	SSH password	cisco123
4	Console password	cisco123

Πίνακας 3.9: Ρυθμίσεις ασφάλειας (ίδιες ρυθμίσεις σε όλα τα ενεργά)

A/A	VLAN	Active Core Switch	Priority
1	100	Core Switch A	A=255 B=1
2	110	Core Switch A	A=255 B=1
3	120	Core Switch A	A=255 B=1
4	130	Core Switch A	A=255 B=1
5	140	Core Switch B	A=1 B=255
6	150	Core Switch B	A=1 B=255
7	160	Core Switch B	A=1 B=255
8	170	Core Switch B	A=1 B=255

Πίνακας 3.10: Ρυθμίσεις HSRP

A/A	Περιγραφή	Ενεργό	Priority
1	Root Bridge	Core Switch A	Primary
2	Backup Root Bridge	Core Switch B	Secondary
3	Non Root Bridge	Server Switch A	61440
4	Non Root Bridge	Server Switch B	61440
5	Non Root Bridge	Switch Ισόγειο	61440
6	Non Root Bridge	Switch 1ος	61440
7	Non Root Bridge	Switch 2ος	61440
8	Non Root Bridge	Switch 3ος	61440

Πίνακας 3.11: Ρυθμίσεις STP

3.2.6 Επιλογή εξοπλισμού (μοντέλα κτλ) με βάση της δυνατότητες αυτών

Στον παρακάτω πίνακα θα βρείτε την επιλογή των μοντέλων των ενεργών στοιχείων που θα επιλεχθούν για κάθε τοποθεσία. Η επιλογή αυτή γίνεται με βάση της απαραίτητες προδιαγραφές και ανάγκες.

Α/Α	Συσκευή	Μοντέλο	Αριθμός	Λειτουργίες
1	Core Switch	Cisco Catalyst 3850	2	24 port, HSRP, Layer 3 Routing, STP, VTP, DHCP, SSH, Port Security, Gigabit, Fibre Optic ports
2	Access Switch	Cisco Catalyst 2960	4	24 port, STP, VTP, DHCP, SSH, Port Security, Gigabit, Fibre Optic ports
3	Server Switch	Cisco Catalyst 3750	2	24 port, STP, VTP, DHCP, SSH, Port Security, Gigabit, Fibre Optic ports
4	ADSL Router	Cisco 887V	2	VDSL Router, VPN, IPSec, 3DES, AES
5	Wireless AP	Cisco Aeronet 700	4	802.11n, 2,4 GHz & 5 GHz, WPA2, AES, TKIP
6	Access Switch Υποκατάστημα	Cisco Catalyst 2960-C	1	STP, VTP, SSH, Port Security, Compact 12 πόρτες

Πίνακας 3.12: Συγκεντρωτικός πίνακας με τις αντίστοιχες συσκευές που θα χρησιμοποιηθούν στο δίκτυο και λειτουργίες που παρέχουν η κάθε μία

3.2.7 Προϋπολογισμός κόστος δικτύου

Ένα σημαντικό κομμάτι στον σχεδιασμό έχει να κάνει με το κόστος του εξοπλισμού. Όταν σχεδιάζεται ένα δίκτυο, πρέπει πάντα να διατηρείται μία ισορροπούσα μεταξύ της αποτελεσματικότητας του δικτύου και του κόστους. Με αποτελεσματικότητα εννοούμε την εφαρμογή εφεδρείας, μέτρα ασφάλειας δικτύου καθώς και υποστηριζόμενες υπηρεσίες όλα τα οποία έχουν κάποιο κόστος. Στον παρακάτω πίνακα θα βρείτε τις ενδεικτικές τιμές στις οποίες προσφέρει η cisco τον παραπάνω εξοπλισμό:

Α/Α	Συσκευή	Μοντέλο	Τεμάχιο	Κόστος/τεμάχιο	Συνολικό κόστος
1	Core Switch	Cisco Catalyst 3850 (WS-C3850-24T-S)	2	6.077,31 €	12.154,61 €
2	Access Switch	Cisco Catalyst 2960 (WS-C2960S-24TS-L)	4	2.426,25 €	9.704,99 €
3	Server Switch	Cisco Catalyst 3750 (WS-C3750-24FS-S)	2	4.350,42 €	8.700,83 €
4	ADSL Router	Cisco 887V (C886VA-W-E-K9)	2	977,04 €	1.954,09 €
5	Wireless AP	Cisco Aeronet 700 (AIR-CAP702I-R-K9)	4	462,81 €	1.851,24 €
6	Access Switch Υποκατάστημα	Cisco Catalyst 2960 (WS-C2960S-24TS-L)	1	2.426,25 €	2.426,25 €
7	Firewall	ASA FIREWALL 8.4(2)	1	1.405,00 €	1.405,00 €
				Σύνολο	**38.197,01 €**

Πίνακας 3.13: Οι αντίστοιχες τιμές για κάθε συσκευή που θα χρησιμοποιήσουμε στο δίκτυο μας

Σημειώνεται ότι οι παραπάνω τιμές είναι οι list price τιμές της Cisco. Συνηθίζεται να υπάρχει κάποια έκπτωση της τάξης των 10% για επιχειρήσεις και άνω των 25% για εκπαιδευτικά ιδρύματα και δημόσιους φορείς. Εκτός από το κόστος εξοπλισμού, υπάρχουν κι άλλα κόστη που πρέπει να λαμβάνονται υπόψη:

- Το κόστος εγκατάστασης και ρυθμίσεις του δικτύου. Αυτό στην Ελληνική αγορά βρίσκεται στο περίπου 10% με 20% του κόστους του εξοπλισμού.

- Το κόστος συντήρησης το οποίο το οποίο ορίζεται σε ένα ετήσιο συμβόλαιο συντήρησης και κοστολογείται ανάλογα με το μέγεθος του δικτύου και με τους όρους του συμβολαίου όπως χρόνος ανταπόκρισης και βλάβες που καλύπτονται. Τέτοιου είδους συμβόλαια εφαρμόζονται όταν κάποια εταιρία δεν έχει προσωπικό ή τεχνογνωσία για να υποστηρίξει ένα δίκτυο.

Η ενδεικτική κοστολόγηση αυτού του έργου υπολογίζεται ως εξής:

Εξοπλισμός = 38.197,01 € - 10% = 34.377,31€

Εγκατάσταση = 15% * 34.377,31€ = 5.156,60€

Υποσύνολο = 5.156,60€ + 34.377,31€ = 39.533,91€
ΦΠΑ = 23% * 39.533,91€ = 9.092,80 €

Σύνολο = 9.092,80 € + 39.533,91 € = 48.626,70 €

3.2.8 Επιλογή εξοπλισμού (μοντέλα κτλ) στο GNS3

Επειδή το GNS3 είναι κυρίως προσομοιωτής δρομολογητών, είναι περιορισμένη η λειτουργία των μεταγωγέων (switch). Γι' αυτό δεν είναι δυνατόν να προσομοιώσουμε ακριβός τα μοντέλα που επιλέχθηκαν παραπάνω. Γι' αυτό, για να λειτουργήσει το GNS3 στην τοπολογία που θέλουμε, θα χρησιμοποιήσουμε την παρακάτω αντιστοίχηση συσκευών:

Α/Α	Συσκευή	Μοντέλο	Αντίστοιχο μοντέλο GNS3	Επιπλέον Modules
1	Core Switch	Cisco Catalyst 3850	Cisco Router 3745	NM-16ESW
2	Access Switch	Cisco Catalyst 2960	Cisco Router 3745	NM-16ESW
3	Server Switch	Cisco Catalyst 3750	Cisco Router 3745	NM-16ESW
4	ADSL Router	Cisco 887V	Cisco Router 3745	
5	Wireless AP	Cisco Aeronet 700		
6	Access Switch Υποκατάστημα	Cisco Catalyst 2960-C	Cisco Router 3745	NM-16ESW
7	ASA Firewall	ASA 8.4(2)	ASA 8.4(2)	-

Πίνακας 3.14: Αντίστοιχα μοντέλα των συσκευών που επιλέξαμε με τα κατάλληλα modules για να τα προσομοιώσουμε στο GNS3

Με την χρήση ενός Cisco Router 3600 μαζί με ένα module NM-16ESW, μπορούμε να προσομοιώσουμε πλήρως όλες τις λειτουργίες των μοντέλων των switch που χρησιμοποιούμε πλην το Port Security. Ωστόσο, για το Port Security, θα καταγράψουμε τις απαραίτητες ρυθμίσεις και λειτουργίες που θα θέλαμε να υπάρχουν στην εταιρία μας.

4.1 Τι είναι το Graphical Network Simulator (GNS3)

Το GNS3 είναι ένας εικονικός γραφικός προσομοιωτής δικτύων που επιτρέπει την προσομοίωση πολύπλοκων δικτυακών αρχιτεκτονικών. Είναι απαιτούμενη η γνώση του VMWare ή του VirtualBox διότι χρησιμοποιούνται για να προσομοιώσουν ποικίλα λειτουργικά συστήματα σε ένα εικονικό υπολογιστικό τερματικό. Αυτά τα προγράμματα επιτρέπουν την χρήση λειτουργικών συστημάτων όπως τα Windows XP, Windows 7 ή διάφορες διανομές Linux όπως mint, ubuntu κλπ. Το σημαντικότερο απ' όλα είναι ότι το GNS3 επιτρέπει την προσομοίωση διαδικτυακών λειτουργικών συστημάτων της CISCO. Δηλαδή επιτρέπει την προσομοίωση του IOS που χρησιμοποιεί η κατασκευάστρια εταιρία CISCO στις διάφορες διαδικτυακές συσκευές τις (δρομολογητές, μεταγωγείς κλπ) σε εικονικό περιβάλλον. Αυτό το επιτυγχάνει με την χρήση του dynamips, όπου είναι ένας γνωστός εξομοιωτής IOS της CISCO.
Το GNS3 επιτρέπει την εξομοίωση του IOS της CISCO σε windows και linux λειτουργικά συστήματα. Επιτρέπει επίσης την προσομοίωση πολλών διαδικτυακών συσκευών της CISCO όπως για παράδειγμα routers, firewalls κλπ. Το GNS3 αποτελεί ένα χρήσιμο εργαλείο για την προετοιμασία πιστοποιητικών της CISCO όπως το CCNA, CCNP και το CCIE.
Για να παρέχει ολοκληρωμένες και ακριβείς προσομοιώσεις το GNS3 χρησιμοποιεί τους ακόλουθους εξομοιωτές emulators για να τρέξει τα ίδια λειτουργικά συστήματα, όπως γίνετε σε ένα πραγματικό δίκτυο υπολογιστών:

1. Dynamips, γνωστός εξομοιωτής της Cisco IOS. Ακολουθεί και σχετική λίστα με τα μοντέλα δρομολογητών Cisco που υποστηρίζει:

   - 1710
   - 1720
   - 1721
   - 1750
   - 1751
   - 1760
   - 2610
   - 2610XM
   - 2611
   - 2611XM
   - 2620
   - 2620XM
   - 2621
   - 2621XM
   - 2650XM
   - 2651XM
   - 2691
   - 3620
   - 3640
   - 3660
   - 3725
   - 3745
   - 7200
   - 7600

2. VirtualBox, τρέχει λειτουργικά συστήματα με χρήση desktop και server όπως και το JunOS

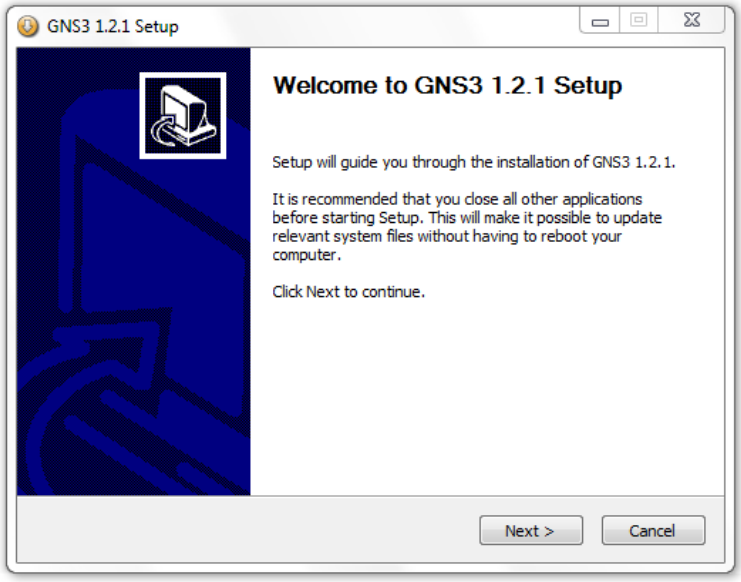
3. QUEMU, εξομοιωτής μηχανής ανοιχτού κώδικα που τρέχει, Cisco ASA, PIX και IPS.

Οι δυνατότητες του λογισμικού ως προς την απόδοση του σε εικονικό περιβάλλον είναι 1000 πακέτα ανά δευτερόλεπτο. Η πρώτη του έκδοση κυκλοφόρησε το 2007.

4.2 Εγκατάσταση του GNS3

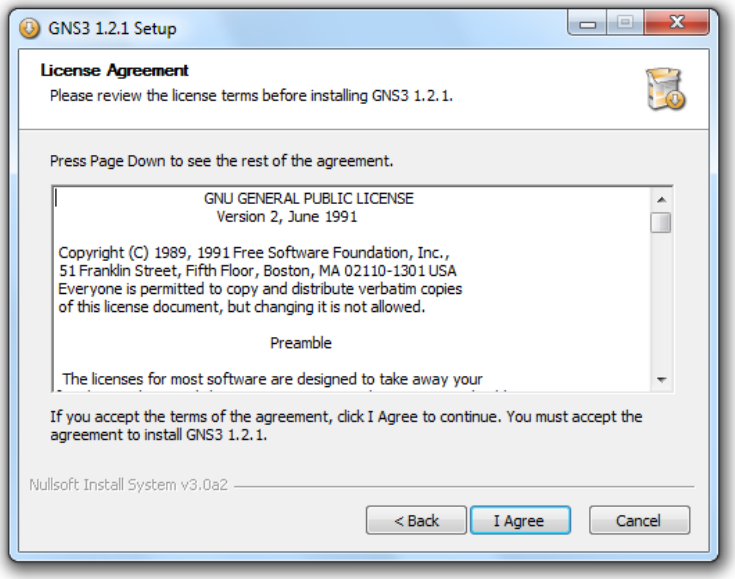
Το GNS3 μπορούμε να το κατεβάσουμε από το http://www.gns3.net/download/. Εμείς θα χρησιμοποιήσουμε την έκδοση GNS3-1.2.1-all-in-one. Η συγκεκριμένη έκδοση περιέχει τον εξομοιωτή Dynamips καθώς και την κονσόλα διαχείρισης Super Putty.

Βήμα 1ο
Είμαστε στην αρχή του οδηγού εγκατάστασης πατάμε το κουμπί next.



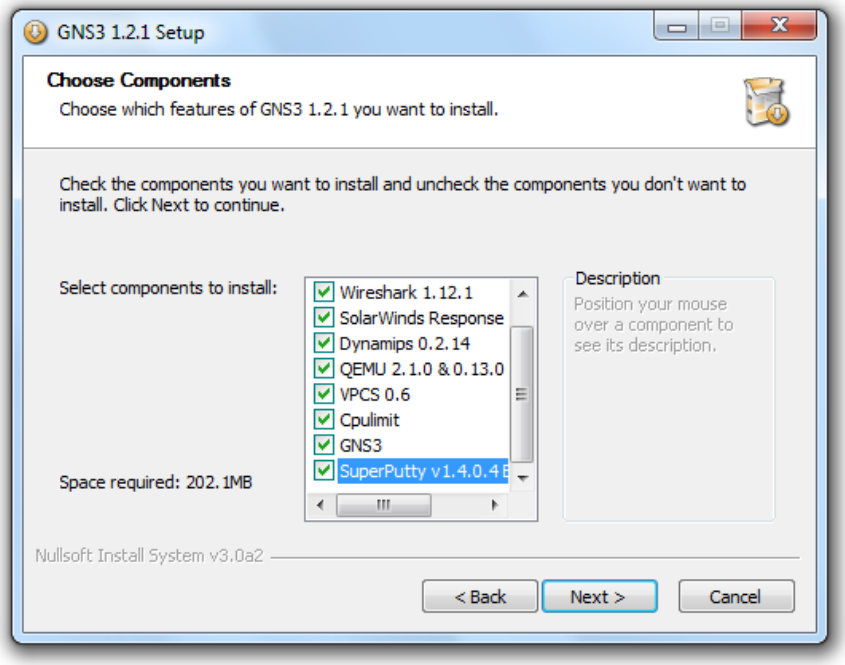
Εικόνα 4.1: Αρχικό μενού του οδηγού εγκατάστασης

Βήμα 2ο
Στο παρακάτω παράθυρο εμφανίζει το παράθυρο με τους όρους εγκατάστασης τους διαβάζουμε και πατάμε το κουμπί I agree



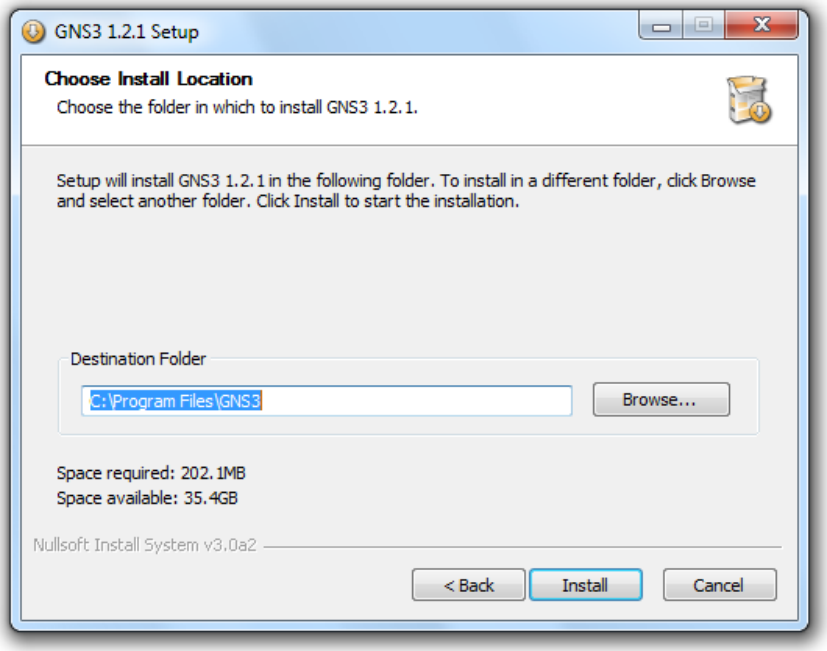
Εικόνα 4.2: Όροι εγκατάστασης του GNS3

Βήμα 3ο
Στο παρακάτω παράθυρο εμφανίζει τα components που περιέχει το πρόγραμμα. Τα επιλέγουμε όλα και πατάμε το κουμπί next.



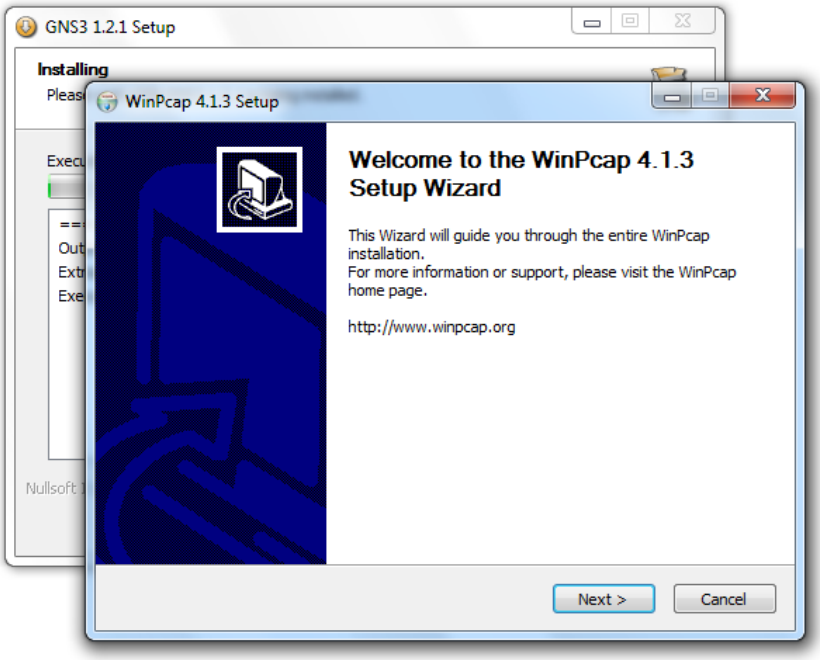
Εικόνα 4.3: Περιεχόμενα εγκατάστασης του GNS3

Βήμα 4ο
Επιλέγουμε το path στο οποίο θέλουμε να εγκατασταθεί το πρόγραμμα και πατάμε το κουμπί install για να ξεκινήσει η εγκατάσταση του προγράμματος.



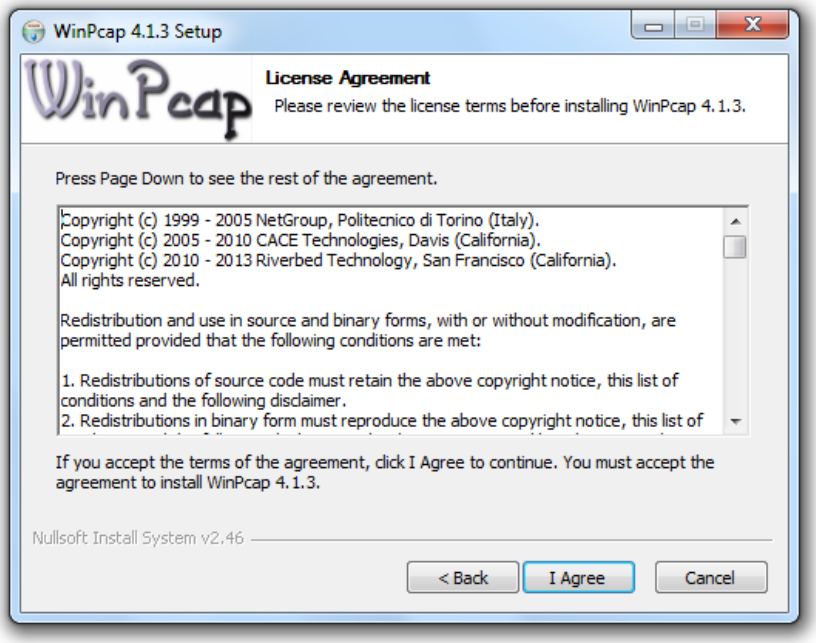
Εικόνα 4.4: Μονοπάτι (path) εγκατάστασης του GNS3

Βήμα 5ο
Στην συνέχεια θα εμφανιστεί το παρακάτω αναδυόμενο παράθυρο το οποίο είναι ο οδηγός εγκατάστασης του WinPcap 4.1.3 πατάμε το κουμπί next.



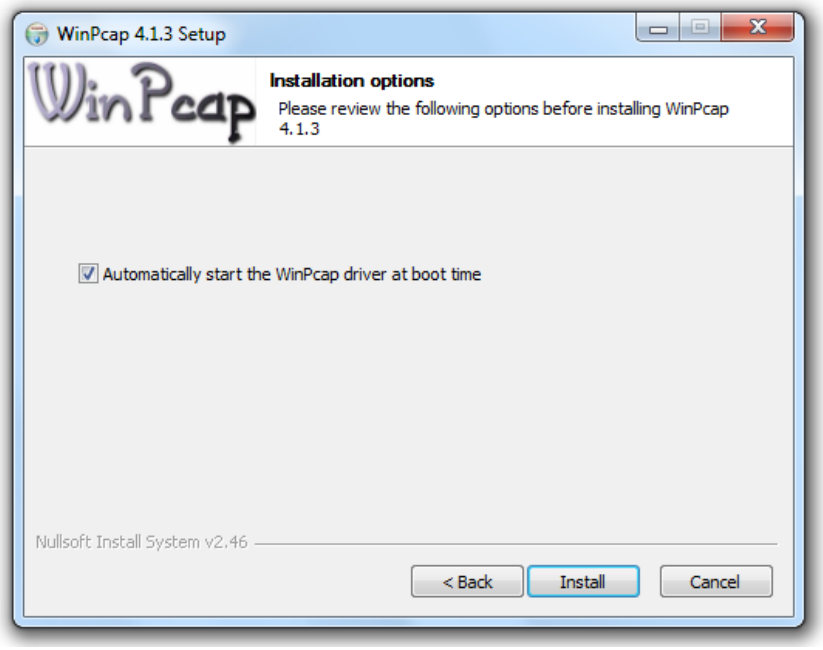
Εικόνα 4.5: Αρχικό μενού εγκατάστασης του WinPcap

Βήμα 6ο
Διαβάζουμε τους όρους εγκατάστασης και πατάμε το κουμπί I aggre.



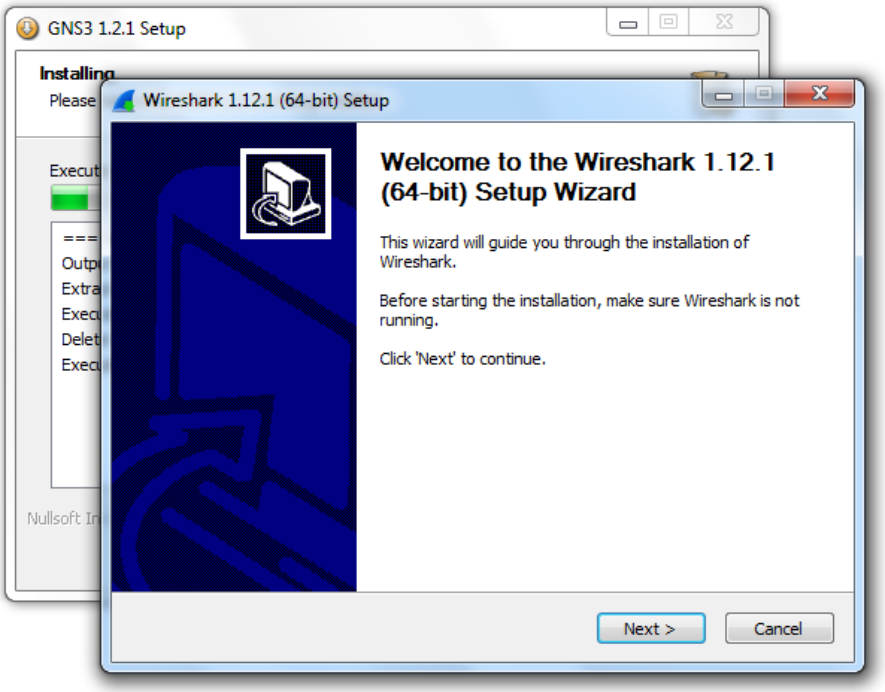
Εικόνα 4.6: Όροι εγκατάστασης του WinPcap

Βήμα 7ο
Πατάμε το κουμπί Install.



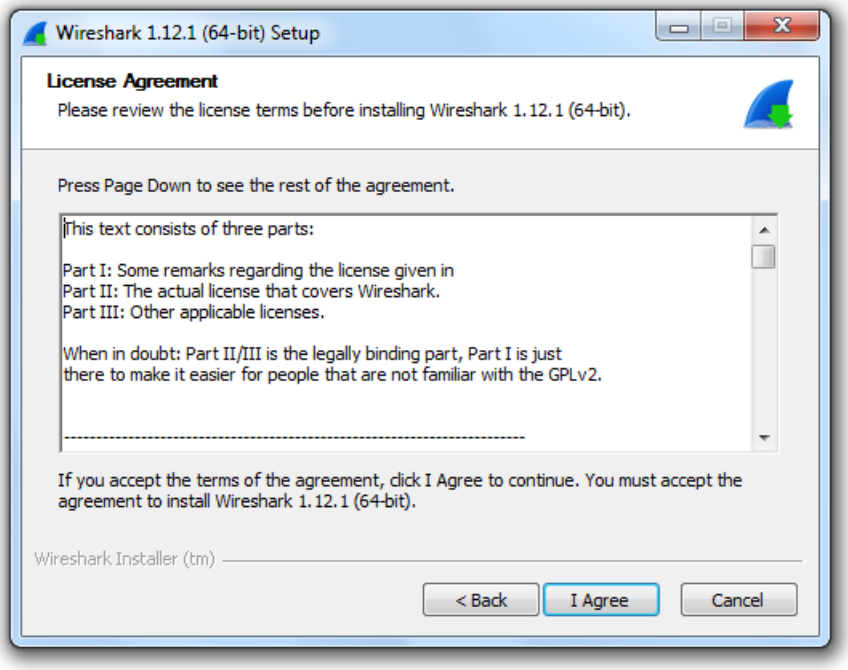
Εικόνα 4.7: Τελικό μενού εγκατάστασης του WinPcap

Βήμα 8ο
Μετά την εγκατάσταση του WinPcap θα εμφανιστεί το παρακάτω αναδυόμενο παράθυρο που είναι ο οδηγός εγκατάστασης του Wireshark 1.10.2 πατάμε το κουμπί next.



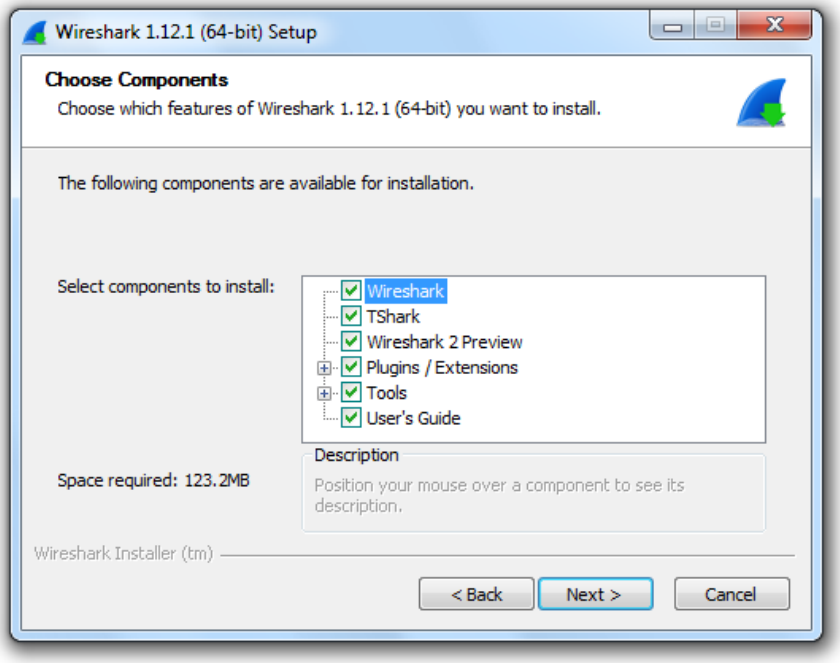
Εικόνα 4.8: Οδηγός εγκατάστασης του wireshark

Βήμα 9ο
Διαβάζουμε τους όρους εγκατάστασης και πατάμε το κουμπί I Aggre.



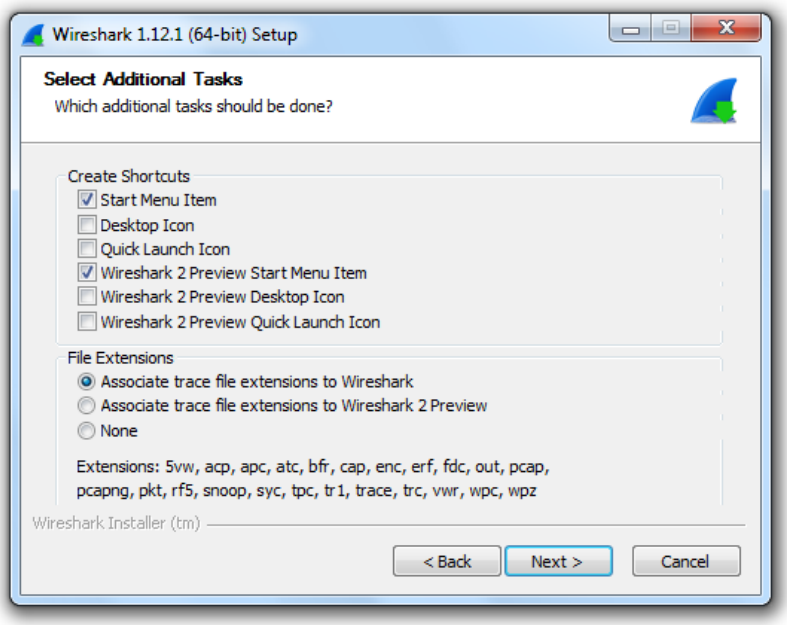
Εικόνα 4.9: Όροι εγκατάστασης του wireshark

Βήμα 10ο
Στο παρακάτω παράθυρο εμφανίζει τα components που περιέχει το πρόγραμμα. Τα επιλέγουμε όλα και πατάμε το κουμπί next.



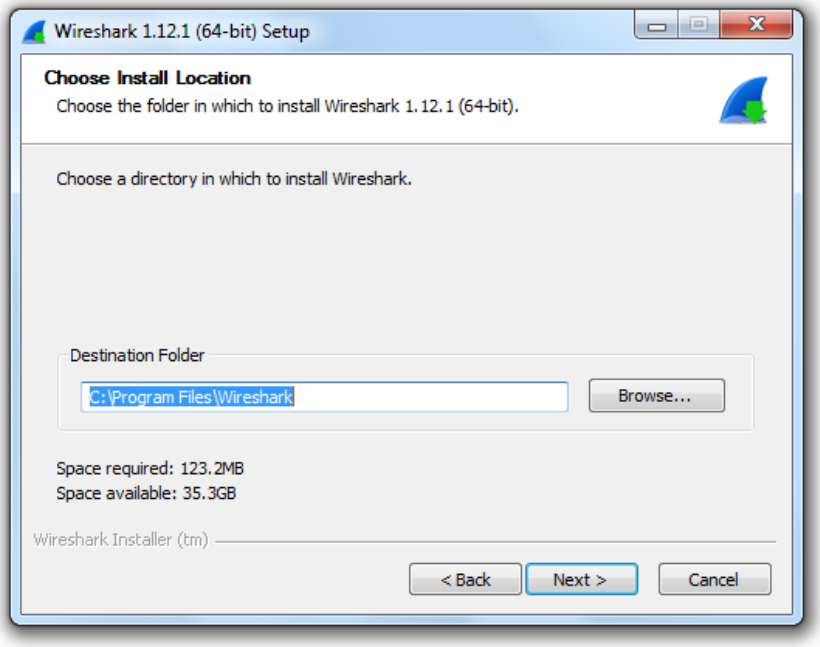
Εικόνα 4.10: Περιεχόμενα εγκατάστασης του wireshark

Βήμα 11ο
Πατάμε το κουμπί Next.



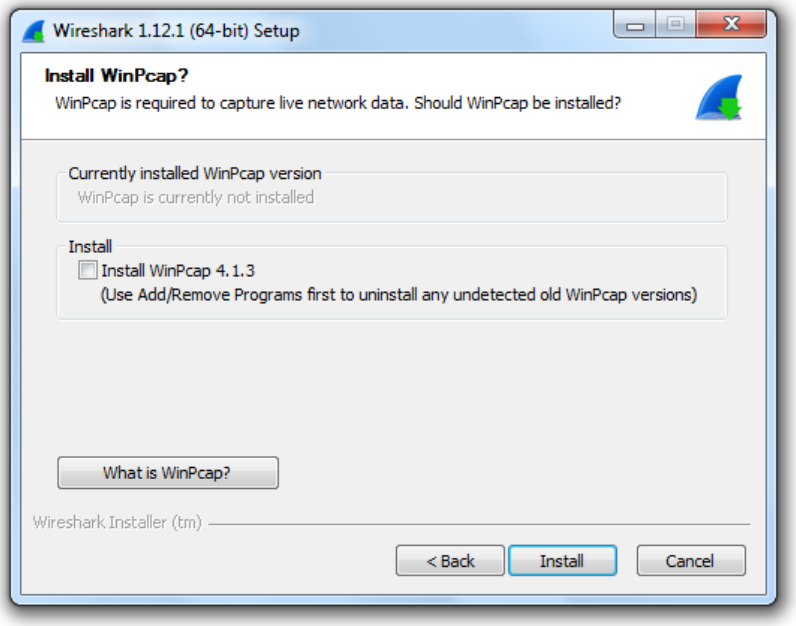
Εικόνα 4.11: Επιλογές συντομεύσεων και επεκτάσεων αρχειων της εγκατάστασης του wireshark

Βήμα 12ο
Επιλέγουμε το path στο οποίο θέλουμε να εγκατασταθεί το πρόγραμμα και πατάμε το κουμπί next για να ξεκινήσει η εγκατάσταση του προγράμματος.



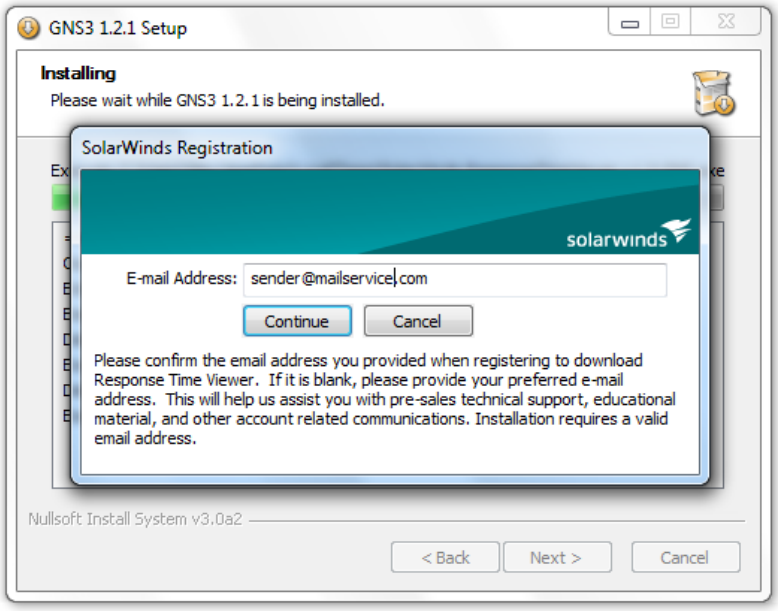
Εικόνα 4.12: Μονοπάτι (path) εγκατάστασης του wireshark

Βήμα 13ο
Δεν επιλέγουμε το checkbox Install WinPcap 4.1.3 διότι το έχουμε ήδη εγκαταστήσει και πατάμε το κουμπί Install



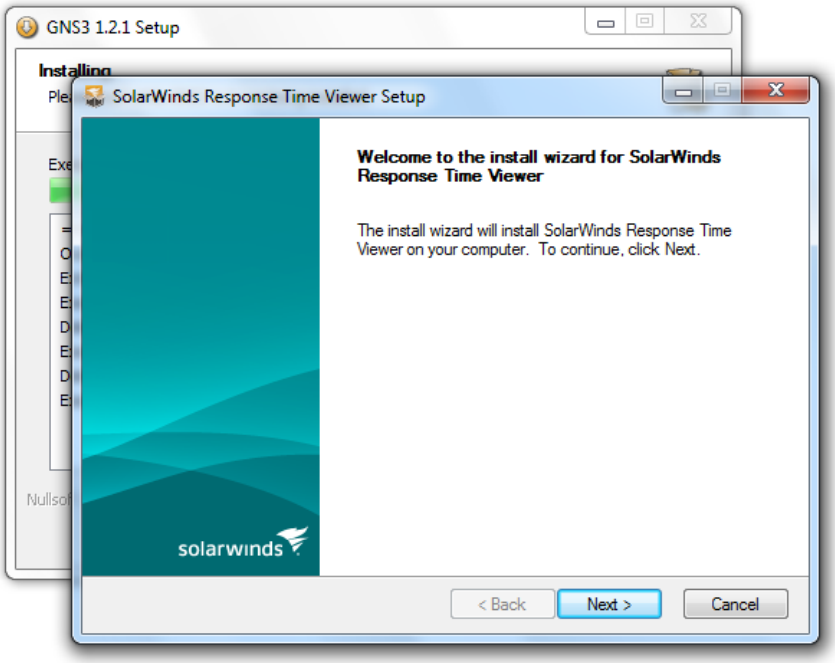
Εικόνα 4.13: Τελικό μενού εγκατάστασης του wireshark

Βήμα 14ο
Όταν τελειώσει η εγκατάσταση του Wireshark θα εμφανιστεί ένα νέο αναδυόμενο παράθυρο που θα αφορά την εγκατάσταση του SolarWinds. Στο επόμενο παράθυρο που θα εμφανιστεί στο πεδίο Email address πληκτρολογούμε την προσωπική διεύθυνση του ηλεκτρονικού μας ταχυδρομείου για να λαμβάνουμε πληροφορίες και news feeds σχετικά με το πρόγραμμα.



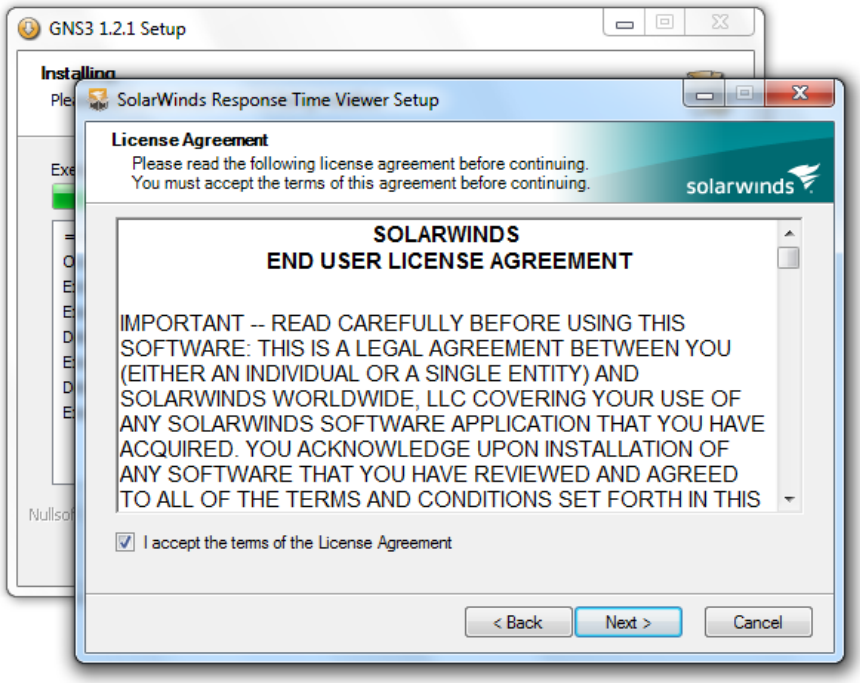
Εικόνα 4.14: Φόρμα συμπλήρωσης e-mail του solar-winds

Βήμα 15ο
Αυτός είναι ο οδηγός εγκατάστασης του SolarWinds. Πατάμε το κουμπί next.



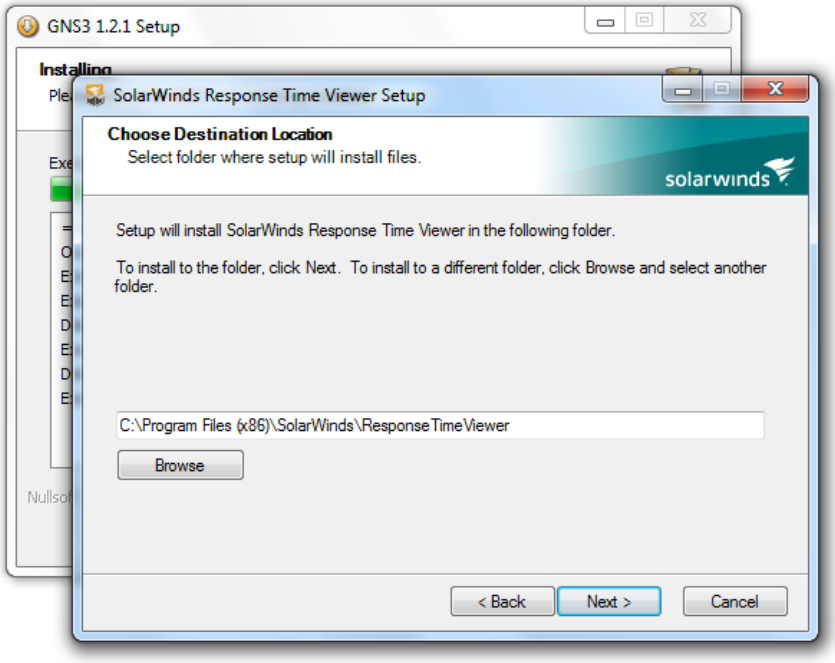
Εικόνα 4.15: Αρχικό μενού εγκατάστασης του solar-winds

Βήμα 16ο
Αποδεχόμαστε τους όρους εγκατάστασης του προγράμματος και πατάμε το κουμπί next.



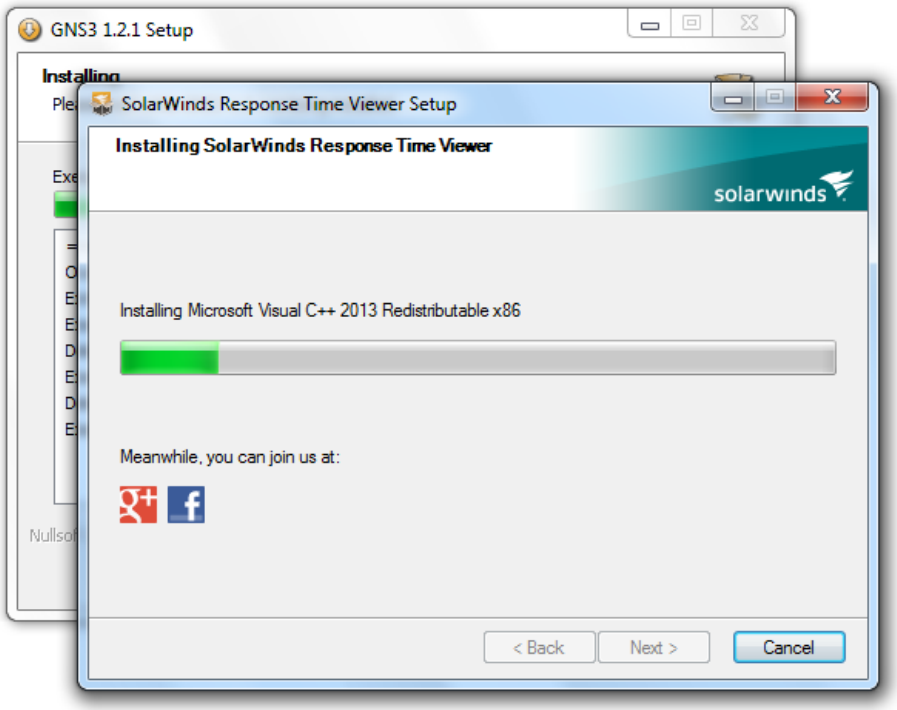
Εικόνα 4.16: Όροι εγκατάστασης του solar-winds

Βήμα 17ο
Επιλέγουμε το path στο οποίο θέλουμε να εγκατασταθεί το πρόγραμμα και πατάμε το κουμπί next για να ξεκινήσει η εγκατάσταση του προγράμματος.



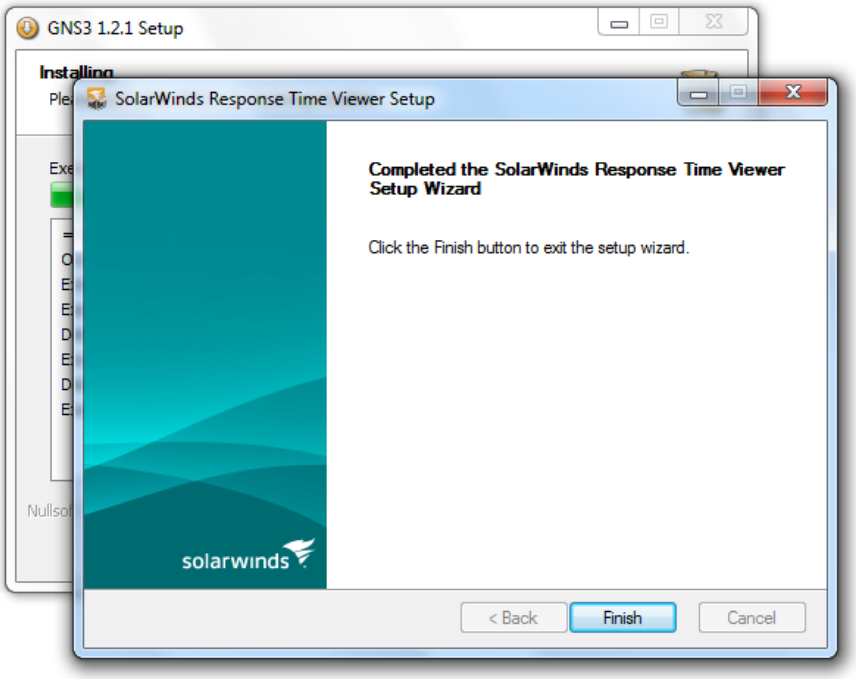
Εικόνα 4.17: Μονοπάτι (path) εγκατάστασης του solar-winds

Βήμα 18ο
Περιμένουμε μέχρι να ολοκληρωθεί η εγκατάσταση του προγράμματος.



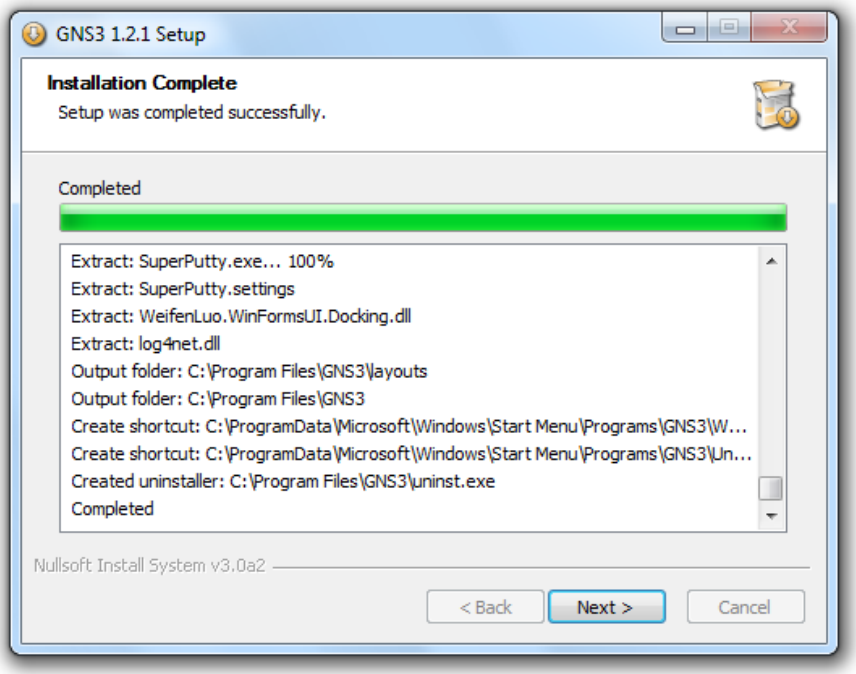
Εικόνα 4.18: Εγκατάσταση του solar-winds

Βήμα 19ο
Η εγκατάσταση του SolarWinds ολοκληρώθηκε.



Εικόνα 4.19: Τελικό μενού εγκατάστασης του solar-winds

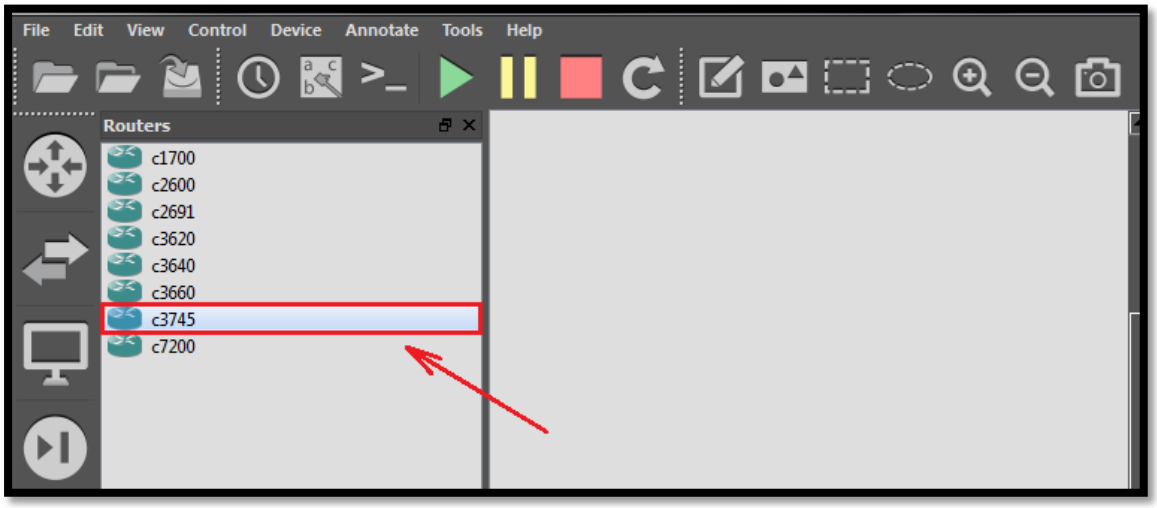
Βήμα 20ο
Η εγκατάσταση του GNS3 ολοκληρώθηκε πατάμε το κουμπί Next και στο επόμενο παράθυρο το κουμπί finish.



Εικόνα 4.20: Τελικό μενού εγκατάστασης του GNS3

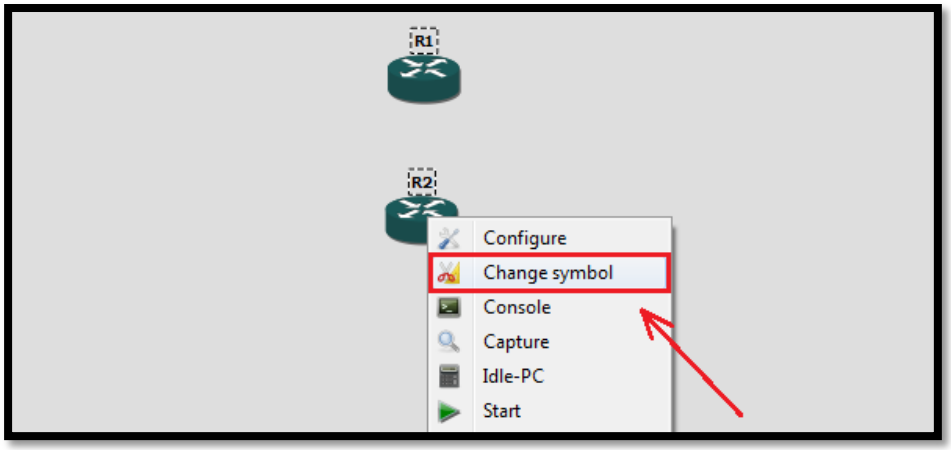
5.1 Ρυθμίσεις core switches A και B

Ξεκινώντας την δημιουργία του δικτύου μας θα δημιουργήσουμε πρώτα τους core switch A και core switch B η οποίοι είναι μεταγωγείς επιπέδου 3 (ανήκουν δηλαδή στο επίπεδο δικτύου). Για να το κάνουμε αυτό θα χρησιμοποιήσουμε έναν router c3745.



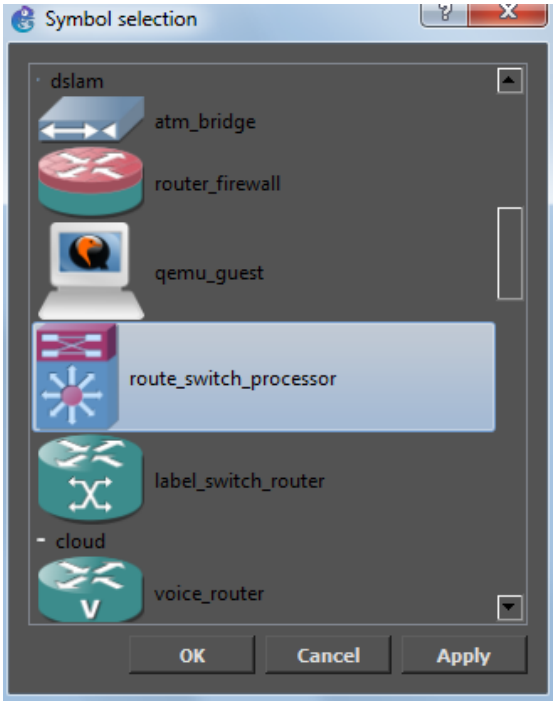
Εικόνα 5.1: Επιλογή εξοπλισμού

Επιλέγουμε και τους δύο routers → δεξί κλίκ →change symbol ώστε να έχει το σύμβολο με το οποίο συμβολίζεται ένα switch (layer 3).



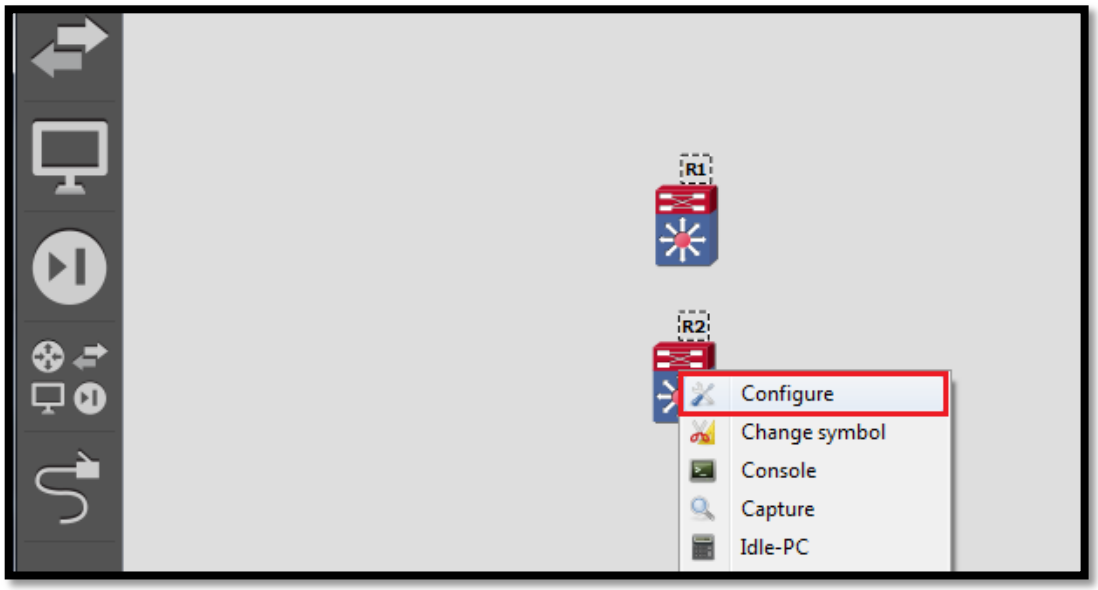
Εικόνα 5.2: Αλλαγή συμβόλου εξοπλισμού

Επιλέγουμε το route_switch_processor και πατάμε το κουμπί οκ.



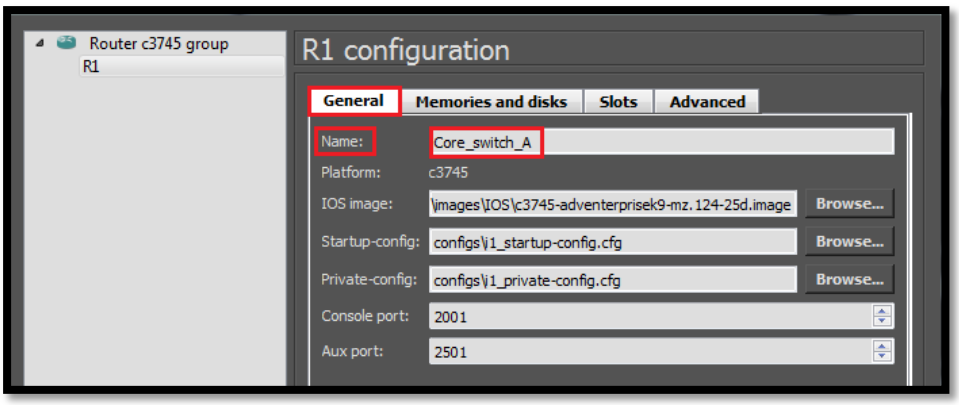
Εικόνα 5.3: Επιλογή συμβόλου εξοπλισμού

Πατάμε δεξί κλικ και επιλέγουμε το Configure για να αλλάξουμε το όνομα των κόμβων και να αποδώσουμε σε αυτούς τα κατάλληλα slots.



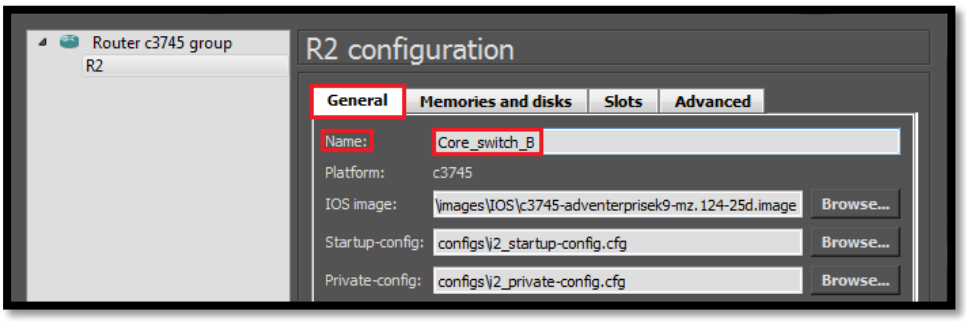
Εικόνα 5.4: Είσοδος στις ρυθμίσεις της συσκευής

Πηγαίνουμε στην καρτέλα general name και το ονομάζουμε Core_switch_A.



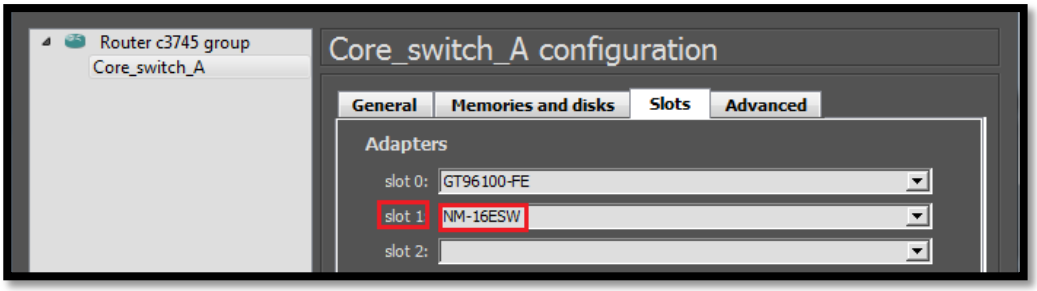
Εικόνα 5.5: Ρύθμιση ονόματος Core switch A

Το ίδιο κάνουμε και για το Core_switch_B.



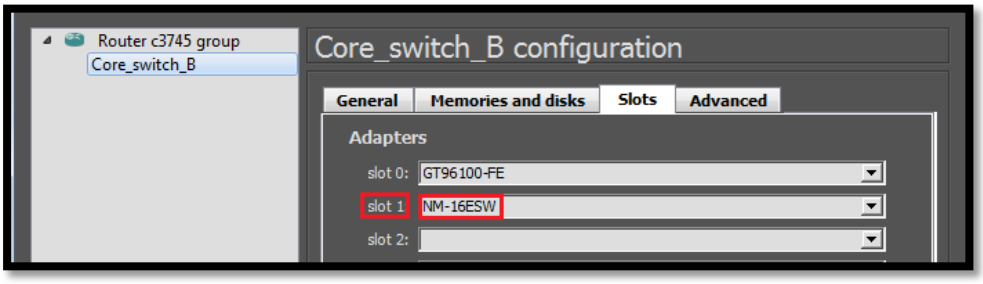
Εικόνα 5.6: Ρύθμιση ονόματος Core switch B

Έπειτα στην καρτέλα Slots για να ρυθμίσουμε



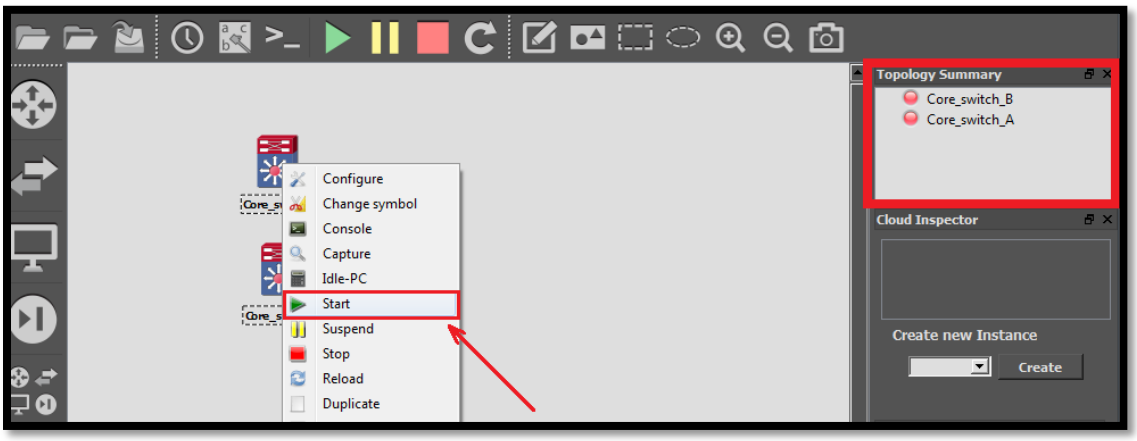
Εικόνα 5.7: Ρύθμιση slots του Core switch A

Το ίδιο και στο Core_switch_B



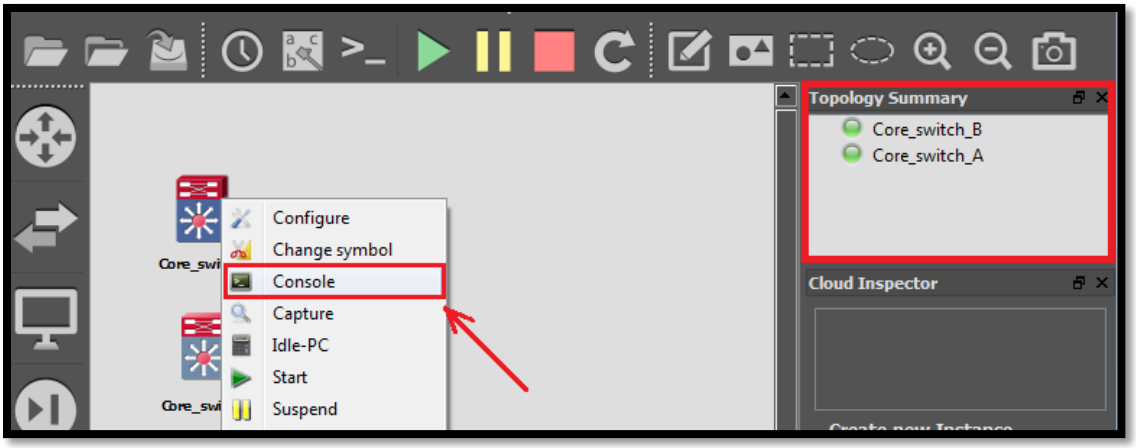
Εικόνα 5.8: Ρύθμιση slots του Core switch B

Παρατηρούμε ότι στο topology summary τα core switch A και B είναι με κόκκινη σήμανση. Αυτό σημαίνει ότι τα switches που έχουμε στο δίκτυο είναι κλειστά. Για να τα ενεργοποιήσουμε ώστε να ρυθμίσουμε παραμέτρους επιλέγουμε το core_switch_A και core_switch_B κάνουμε δεξί κλικ και start.

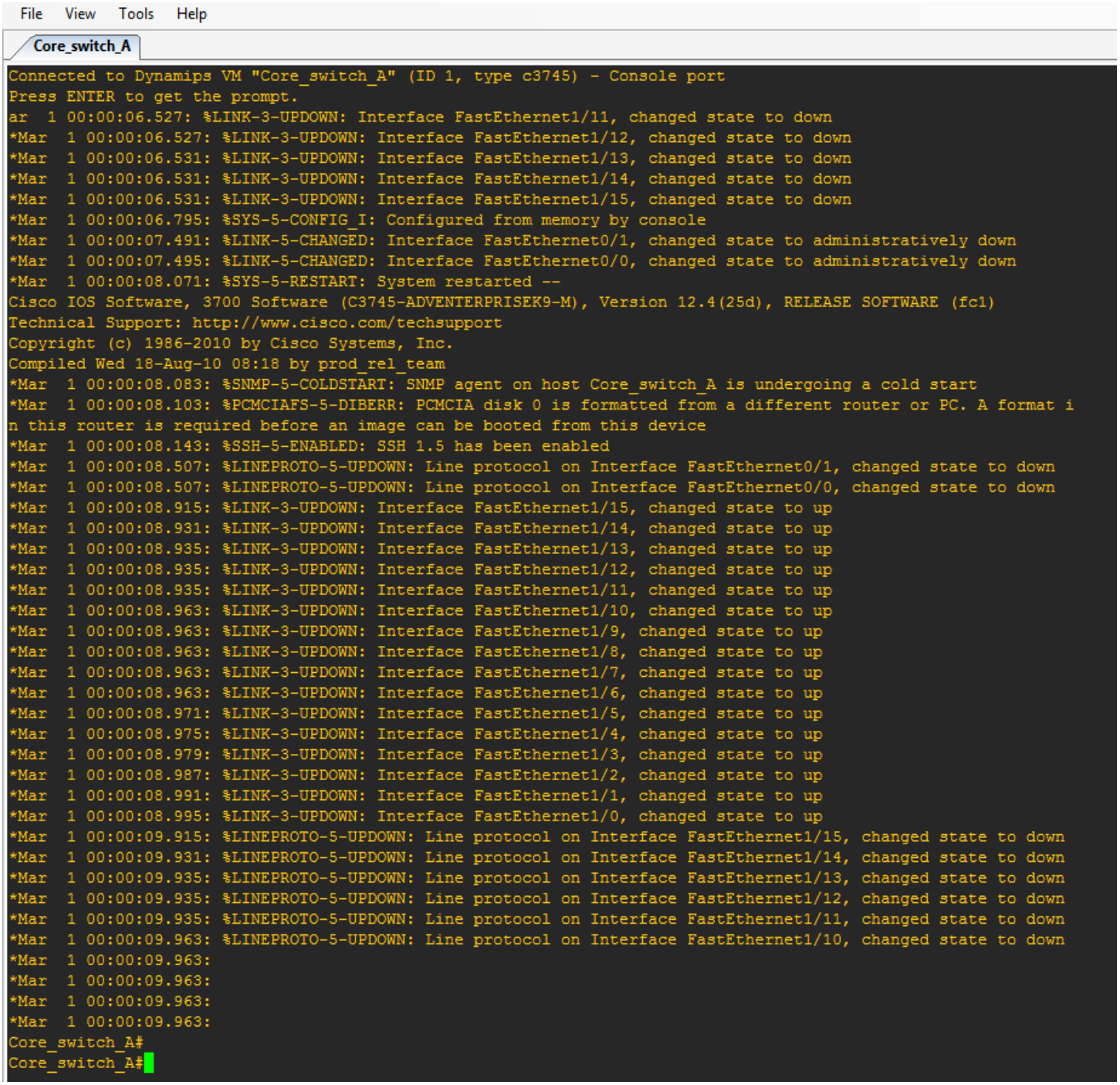


Εικόνα 5.9: Εκίνηση συσκευών Core switch A και Core switch B

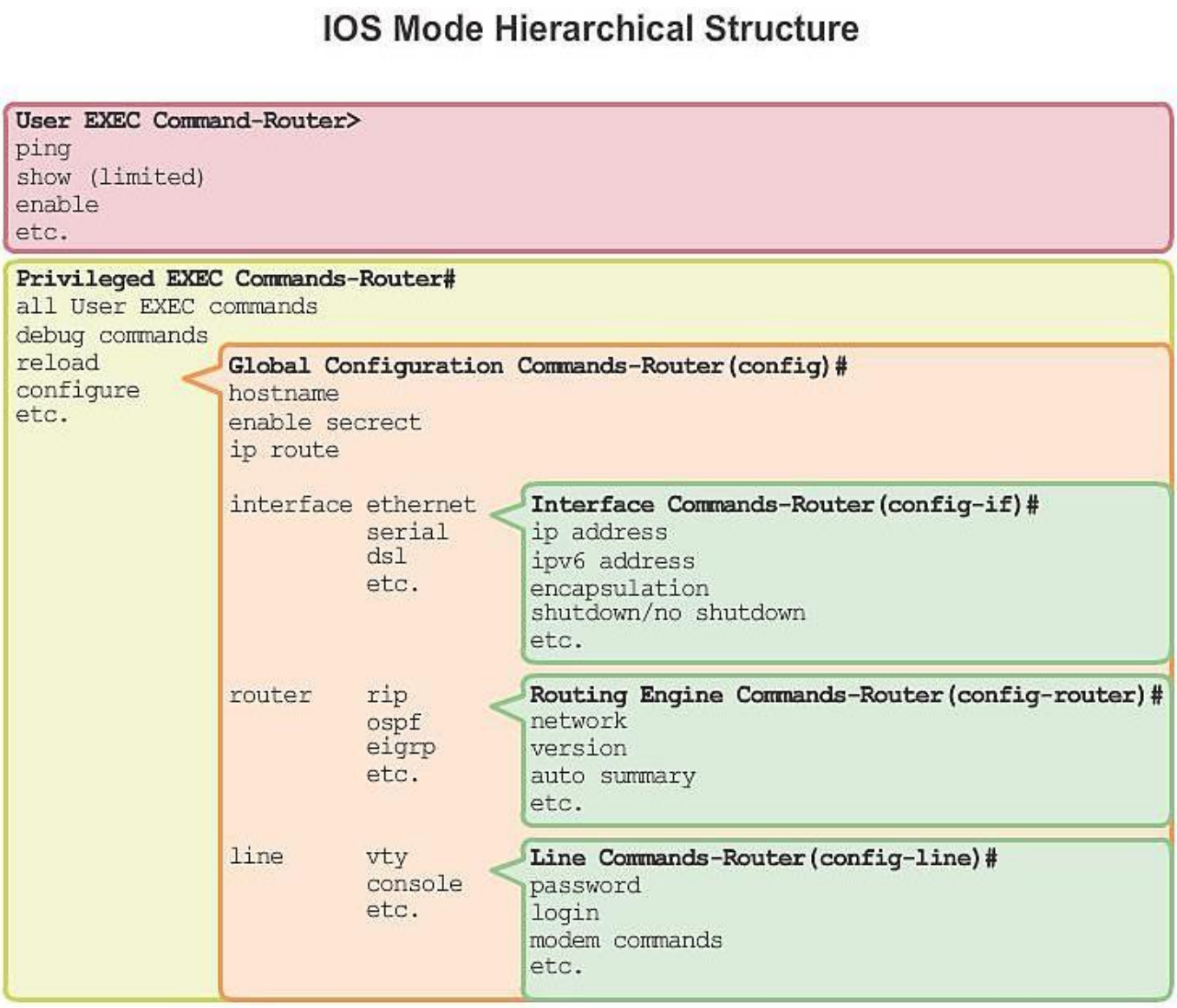
Όπως βλέπουμε στο topology summary μετά που πατήσουμε start η σήμανση για core switch A και B είναι πράσινη που σημαίνει ότι είναι ενεργοποιημένα. Οπότε τώρα μπορούμε να θέσουμε παραμέτρους μέσω του Console. Το Console δέχεται εντολές του CLI της Cisco και στην ουσία είναι ένας προσομοιωτής ενός κανονικού router της Cisco.



Εικόνα 5.10: Εκίνηση κονσόλας εντολών



Εικόνα 5.11:Δομή κόνσόλας εντολών στο GNS3



Εικόνα 5.12: Ιεραρχική δομή IOS mode

Περιγραφή operation modes	Συμβολισμός
Με ανοικτό κόκκινο είναι USER EXEC MODE	**>**
Με ανοικτό κίτρινο είναι PRIVILEGED EXEC MODE	**#**
Με ανοικτό πορτοκαλί είναι GLOBAL CONFIGURATION MODE	**(config)#**
Με ανοικτό πράσινο είναι CONFIG MODE	**Config-if #** **Config- router #** **Config-line #** **(vlan)#**

Πίνακας 5.1: Ενδεικτικά operation modes του IOS της CISCO

Παρακάτω θα προχωρήσουμε στην ρύθμιση των συσκευών που θα βάλουμε. Κανονικά στο IOS περιβάλλον ο χρωματισμός για εντολές προειδοποιητικό κείμενο κλπ είναι ενιαίος. Για να γίνει όμως κατανοητό και για να ξεχωρίσουμε τις καθαρές εντολές από το κύριο κείμενο του IOS περιβάλλοντος έχει γίνει διαχωρισμός με τον εξής τρόπο.

Περιγραφή	Ένδειξη
Με ανοικτό κίτρινο είναι τα διάφορα **operation modes**	
Με γαλάζιο είναι οι **εντολές** που δίνουμε	
Με ανοικτό μπλε είναι το **κείμενο που εμφανίζεται όταν πληκτρολογήσουμε μια εντολή**	
Με πράσινο είναι τα **σχόλια επεξήγησης της κάθε εντολής.** *Εδώ αξίζει να σημειώσουμε ότι στο IOS περιβάλλον δεν μπορούμε να βάλουμε σχόλια!! Αυτό το χρησιμοποιούμε για να καταλάβουμε τι κάνει η κάθε εντολή.	

Πίνακας 5.2: Χρωματική ένδειξη κειμένου

Πρώτο μας βήμα είναι να διαγράψουμε ότι έχει στην μνήμη το Core switch A και αυτό το κάνουμε με τις εξής εντολές.

```
Core_switch_A# erase nvram:    /*διαγραφή μνήμης*/
Core_switch_A# reload      /*Επανεκκίνηση συσκευής*/
```

Με την εντολή Erase nvram: του λέω να διαγράψει όλες τις ρυθμίσεις που έχει και με την εντολή reload κάνω επανεκκίνηση την συσκευή.

Για να ρυθμίσουμε παραμέτρους

```
                          /*Ρυθμίσεις παραμέτρων*/


core_switch_A# config t          /*Είσοδος σε configuration mode*/
core_switch_A(config)# hostname core_switch_A  /*Θέτουμε το hostname core switch B
                                                στον κόμβο*/
core_switch_A(config)# enable secret cisco123   /*Θέτουμε κωδικό για να μπούμε σε
                                              privileged user exec (enable) mode*/
core_switch_A(config)# line vty 0 1340      /*Ρυθμίζουμε εικονικά τερματικά από 0
                                            έως 1340 που είναι το μέγιστο */

core_switch_A(config-line)# password cisco123   /* Θέτουμε κωδικό για config-line
core_switch_A(config-line)# login         /*Υποχρέωσε τον χρήστη να κάνει login*/
core_switch_A(config-line)# transport input ssh    /* Εισήγαγε SSH, και
                                                    απενεργοποίησε το telnet*/
core_switch_A(config-line)# exit         /*Εξοδος από configure line mode*/

core_switch_A(config)# line con 0
core_switch_A(config-line)# password cisco123       /*Θέτουμε κωδικό στην κονσόλα
                                                   σε cisco123*/
core_switch_A(config-line)# login     /*Υποχρέωσε τον χρήστη να κάνει login*/
core_switch_A(config-line)# exit      /*Exit from configure line mode*/
core_switch_A(config)# exit          /*Εξοδος από configure mode*/

core_switch_A# show run          /*Εμφάνισε τις ρυθμίσεις που είναι στην DRAM*/
core_switch_A# config t          /*Είσοδος σε configuration mode*/
core_switch_A(config)# service password-encryption     /*Κρυπτογράφηση κωδικών
                                                        συστήματος */
core_switch_A(config)# exit     /*Εξοδος από configure mode*/

core_switch_A# write  /*Αποθήκευσε όλες τις ρυθμίσεις στην non-volatile RAM*/
```

```
core_switch_A# config t          /*Είσοδος σε configuration mode*/
core_switch_A# no ip http server
core_switch_A# no ip http secure-server
core_switch_A# exit         /*Έξοδος από configure mode*/

/*Για να θέσω VLAN ονόματα και id για το κάθε τμήμα. Πρέπει να είμαι σε user exec
                                    mode*/

core_switch_A# vlan database           /*Είσοδος για ρύθμιση vlan*/

core_switch_A(vlan)# vlan 100 name wireless
core_switch_A(vlan)# vlan 110 name sales
core_switch_A(vlan)# vlan 120 name ManagementVlan     /*Εδώ δίνουμε ονόματα για
core_switch_A(vlan)# vlan 130 name AccountingOffice   κάθε τμήμα της εταιρίας μας
core_switch_A(vlan)# vlan 140 name Administration     και id για το καθένα.*/
core_switch_A(vlan)# vlan 150 name Marketing
core_switch_A(vlan)# vlan 160 name ServerLAN
core_switch_A(vlan)# vlan 170 name ITdep
core_switch_A(vlan)# vlan 200 name 2ndStore

core_switch_A(vlan)# exit         /*Έξοδος από ρύθμιση vlan*/
core_switch_A# show vlan-switch  /*Δείχνει πληροφορίες για vlan*/

           /*Δημιουργία VLANs και ανάθεση IP διευθύνσεων στο καθένα*/

core_switch_A# config t

/*Δίνουμε στο υποκατάστημα με vlan name wireless και id 100 network ip 172.16.0.2
και μάσκα υποδικτύου 255.255.255.192*/

core_switch_A(config)# interface vlan 100
core_switch_A(config-if)# ip address 172.16.0.2 255.255.255.192
core_switch_A(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name sales και id 110 network ip 172.16.0.66
και μάσκα υποδικτύου 255.255.255.224*/

core_switch_A(config-if)# interface vlan 110
core_switch_A(config-if)# ip address 172.16.0.66 255.255.255.224
core_switch_A(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name ManagementVlan και id 120 network ip
172.16.0.98 και μάσκα υποδικτύου 255.255.255.224*/

core_switch_A(config-if)# interface vlan 120
core_switch_A(config-if)# ip address 172.16.0.98 255.255.255.224
core_switch_A(config-if)# no shutdown
```

```
/*Δίνουμε στο υποκατάστημα με vlan name AccountingOffice και id 130 network ip
172.16.0.130 και μάσκα υποδικτύου 255.255.255.240*/

core_switch_A(config-if)# interface vlan 130
core_switch_A(config-if)# ip address 172.16.0.130 255.255.255.240
core_switch_A(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name Administration και id 140 network ip
172.16.0.140 και μάσκα υποδικτύου 255.255.255.240*/

core_switch_A(config-if)# interface vlan 140
core_switch_A(config-if)# ip address 172.16.0.146 255.255.255.240
core_switch_A(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name Marketing και id 150 network ip
172.16.0.162 και μάσκα υποδικτύου 255.255.255.240*/

core_switch_A(config-if)# interface vlan 150
core_switch_A(config-if)# ip address 172.16.0.162 255.255.255.240
core_switch_A(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name ServerLAN και id 160 network ip
172.16.0.178 και μάσκα υποδικτύου 255.255.255.240*/

core_switch_A(config-if)# interface vlan 160
core_switch_A(config-if)# ip address 172.16.0.178 255.255.255.240
core_switch_A(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name ITdep και id 170 network ip 172.16.0.194
και μάσκα υποδικτύου 255.255.255.248*/

core_switch_A(config-if)# interface vlan 170
core_switch_A(config-if)# ip address 172.16.0.194 255.255.255.248
core_switch_A(config-if)# no shutdown

core_switch_A(config-if)# exit   /*Έξοδος από configure interface mode*/
core_switch_A(config)# exit     /*Έξοδος από configure mode*/

core_switch_A# write  /*Αποθήκευσε όλες τις ρυθμίσεις στην non-volatile RAM*/
```

```
core_switch_A# vlan database     /*Είσοδος στην βάση που έχει αποθηκευμένα
                                 όλα τα στοιχεία που ρυθμίσαμε για τα vlan
                                 μας*/
core_switch_A(vlan)# show current        /*Προβολή στοιχείων vlans*/
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 100
    Name: wireless
    Media Type: Ethernet
    VLAN 802.10 Id: 100100
    State: Operational
    MTU: 1500

  VLAN ISL Id: 110
    Name: sales
    Media Type: Ethernet
    VLAN 802.10 Id: 100110
    State: Operational
    MTU: 1500

  VLAN ISL Id: 120
    Name: ManagementVlan
    Media Type: Ethernet
    VLAN 802.10 Id: 100120
    State: Operational
    MTU: 1500

  VLAN ISL Id: 130
    Name: AccountingOffice
    Media Type: Ethernet
    VLAN 802.10 Id: 100130
    State: Operational
    MTU: 1500

  VLAN ISL Id: 140
    Name: Administration
    Media Type: Ethernet
    VLAN 802.10 Id: 100140
    State: Operational
    MTU: 1500

  VLAN ISL Id: 150
    Name: Marketing
    Media Type: Ethernet
    VLAN 802.10 Id: 100150
    State: Operational
    MTU: 1500
```

/* Όλες οι θύρες ενός switch πρέπει να ανήκουν σε κάποιο vlan. Το VLAN με id 1 είναι το default vlan όπου όλες οι πόρτες (ports) ανήκουν σε αυτό. */

/* Εδώ μας δείχνει πληροφορίες για τα διάφορα vlan τμήματα που δημιουργήσαμε προηγούμενος. Οι πληροφορίες αυτές είναι το όνομα του VLAN (π.χ. wireless, ManagementVlan, Accounting Office κλπ), επίσης περιέχει το id που θέσαμε για κάθε τμήμα. Το πρωτόκολλο του data link layer που περνάει από το κάθε VLAN τμήμα στην συγκεκριμένη περίπτωση είναι το Ethernet (Media Type). Το πρότυπο 802.10 του οργανισμού IEEE καθορίζει τον τρόπο με τον οποίο θα μαρκάρονται τα πλαίσια (frames) με το κατάλληλο VLAN id κατά την διάρκεια της αποστολής. Δηλαδή έστω ένα πλαίσιο το οποίο μεταδίδεται από ένα VLAN με id 120 όπου είναι το ManagementVlan. Το πλαίσιο αυτό μαρκάρεται με το id 100120. Το MTU – Maximum Transmission Unit είναι το μέγιστο μέγεθος σε bytes που μπορεί να έχει ένα πλαίσιο σε αυτό το VLAN. By default παραμένει στα 1500 bytes */

```
VLAN ISL Id: 160
  Name: ServerLAN
  Media Type: Ethernet
  VLAN 802.10 Id: 100160
  State: Operational
  MTU: 1500

VLAN ISL Id: 170
  Name: ITdep
  Media Type: Ethernet
  VLAN 802.10 Id: 100170
  State: Operational
  MTU: 1500

VLAN ISL Id: 200
  Name: 2ndStore
  Media Type: Ethernet
  VLAN 802.10 Id: 100200
  State: Operational
  MTU: 1500

VLAN ISL Id: 1002
  Name: fddi-default
  Media Type: FDDI
  VLAN 802.10 Id: 101002
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Translational Bridged VLAN: 1
  Translational Bridged VLAN: 1003

VLAN ISL Id: 1003
  Name: token-ring-default
  Media Type: Token Ring
  VLAN 802.10 Id: 101003
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Ring Number: 0
  Bridge Number: 1
  Parent VLAN: 1005
  Maximum ARE Hop Count: 7
  Maximum STE Hop Count: 7
  Backup CRF Mode: Disabled
  Translational Bridged VLAN: 1
  Translational Bridged VLAN: 1002

  VLAN ISL Id: 1004
  Name: fddinet-default
  Media Type: FDDI Net
  VLAN 802.10 Id: 101004
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Bridge Number: 1
  STP Type: IBM
```

```
/* Αυτά τα VLAN εξυπηρετούν παλιά πρότυπα. Στην ουσία δεν χρησιμοποιούνται και ο σκοπός τους είναι να υπάρχουν για να εξυπηρετούν παλιά δίκτυα. Αυτά τα πρότυπα δεν μπορούν να σβηστούν. */
```

```
    VLAN ISL Id: 1005
    Name: trnet-default
    Media Type: Token Ring Net
    VLAN 802.10 Id: 101005
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM
```

Απ' ότι παρατηρούμε με την εντολή show current μας εμφάνισε όλα τα στοιχεία των vlans που δημιουργήσαμε στον Core switch A και

```
core_switch_A(vlan)# vtp server    /*Θέτουμε την λειτουργία VTP στον Core
Device mode already VTP SERVER.     switch B */

/* Θέλουμε να δώσουμε ένα vtp domain για να το κάνουμε αυτό χρησιμοποιούμε
την εντολή domain και δίνουμε ένα κατάλληλο όνομα που στην περίπτωση μας
είναι το techcom.gr. Όσοι clients είναι σε αυτό το domain θα μπορούν να
επικοινωνούν με τον VTP Server. */

core_switch_A(vlan)# vtp domain ?
  WORD  The ascii name for the VTP administrative domain.

core_switch_A(vlan)# vtp domain techcom.gr
     Changing VTP domain name from NULL to techcom.gr
     core_switch_A(vlan)#vtp password cisco123
     Setting device VLAN database password to cisco123.

/* Χρησιμοποιούμε το vtp v2-mode. Αυτή η έκδοση είναι η πιο καινούργια του
πρωτοκόλλου του VTP. */

core_switch_A(vlan)# vtp v2-mode
     V2 mode enabled.

core_switch_A(vlan)# apply
     APPLY completed.

core_switch_A(vlan)# exit
     APPLY completed.
     Exiting....
```

/* Χρησιμοποιούμε την apply για να αποθηκευτούν οι αλλαγές στην μνήμη του core switch A και exit για να πάμε σε user exec mode */

```
/* Με την παρακάτω εντολή μας εμφανίζει την κατάσταση διεπαφών του core
switch_A. Όπως βλέπουμε η θύρα Fa1/0 δεν είναι συνδεδεμένη. */

core_switch_A# show inter status

      Port     Name               Status       Vlan     Duplex       Speed Type
      Fa1/0                       notconnect    1         auto     auto 10/100BaseTX
      Fa1/1                       notconnect    1         auto     auto 10/100BaseTX
      Fa1/2                       notconnect    1         auto     auto 10/100BaseTX
      Fa1/3                       notconnect    1         auto     auto 10/100BaseTX
                                                .
                                                .
                                                .
      Fa1/14                      notconnect    1         auto     auto 10/100BaseTX
      Fa1/15                      notconnect    1         auto     auto 10/100BaseTX

core_switch_A# config t
      Enter configuration commands, one per line.  End with CNTL/Z.

/* Με την παρακάτω εντολή ρυθμίζουμε την διεπαφή Fa1/0. */

core_switch_A(config)# interface fastEthernet 1/0

/* Με την παρακάτω εντολή θέτουμε την διεπαφή Fa1/0 σε trunk mode. Δηλαδή
μεταφέρει πολλαπλά VLANs πάνω από μια σύνδεση. By default περνάνε όλα τα
υφιστάμενα vlan από το trunk. */

core_switch_A(config-if)# switchport mode trunk

/* Με την παρακάτω εντολή ορίζουμε το πρωτόκολλο του trunk encapsulation στο
IEEE 802.1q. */

core_switch_A(config-if)# switchport trunk encapsulation dot1q

/* Με την παρακάτω εντολή ενεργοποιούμε την Fa1/0. */
core_switch_A(config-if)# no shutdown

/* Δίνουμε περιγραφή. */
Core_switch_A(config-if)# description CONN WITH CORE B

/* Εξοδος από interface config-mode. */
core_switch_A(config-if)# exit

/* Εξοδος από global config-mode. */
core_switch_A(config)# exit

/*Αποθήκευσε όλες τις ρυθμίσεις στην non-volatile RAM*/
core_switch_A# write
Building configuration...
[OK]
```

```
/* Με την παρακάτω εντολή μας εμφανίζει την κατάσταση διεπαφών του core
switch_A. Όπως βλέπουμε η θύρα Fa1/0 έχει πλέον την περιγραφή που της δώσαμε
αλλά είναι ακόμα notconnect αφού δεν έχει συνδεθεί ακόμα με το core
switch_B. */

Core_switch_A# show interface status

      Port    Name               Status    Vlan     Duplex      Speed Type
      Fa1/0 CONN WITH CORE B notconnect   1        auto    auto 10/100BaseTX
      Fa1/1                  notconnect   1        auto    auto 10/100BaseTX
      Fa1/2                  notconnect   1        auto    auto 10/100BaseTX
      Fa1/3                  notconnect   1        auto    auto 10/100BaseTX
                                        .
                                        .
                                        .
      Fa1/14                notconnect    1        auto    auto 10/100BaseTX
      Fa1/15                notconnect    1        auto    auto 10/100BaseTX
```

Στο Core switch B

Πρώτο μας βήμα είναι να διαγράψουμε ότι έχει στην μνήμη το Core switch B και αυτό το κάνουμε με τις εξής εντολές.

```
Core_switch_B# erase nvram:    /*διαγραφή μνήμης*/
Core_switch_B# reload   /*Επανεκκίνηση συσκευής*/
```

Με την εντολή Erase nvram: του λέω να διαγράψει όλες τις ρυθμίσεις που έχει και με την εντολή reload κάνω επανεκκίνηση την συσκευή.
Για να ρυθμίσουμε παραμέτρους

```
                          /*Ρυθμίσεις παραμέτρων*/


core_switch_B# config t          /*Είσοδος σε configuration mode*/
core_switch_B(config)# hostname core_switch_B  /*Θέτουμε το hostname core switch B
                                                στον κόμβο*/
core_switch_B(config)# enable secret cisco123   /*Θέτουμε κωδικό για να μπούμε σε
                                               privileged user exec (enable) mode*/
core_switch_B(config)# line vty 0 1340   /*Ρυθμίζουμε εικονικά τερματικά από 0 έως
                                           1340 που είναι το μέγιστο */

core_switch_B(config-line)# password cisco123 /* Θέτουμε κωδικό για config-line*/
core_switch_B(config-line)# login          /*Υποχρέωσε τον χρήστη να κάνει login*/
core_switch_B(config-line)# transport input ssh    /* Ενεργοποίησε το SSH, και
                                                    απενεργοποίησε το telnet*/
core_switch_B(config-line)# exit      /*Έξοδος από configure line mode*/

core_switch_B(config)# line con 0
core_switch_B(config-line)# password cisco123  /*Θέτουμε κωδικό στην κονσόλα
                                                σε cisco123*/
core_switch_B(config-line)# login     /*Υποχρέωσε τον χρήστη να κάνει login*/
core_switch_B(config-line)# exit      /*Exit from configure line mode*/
core_switch_B(config)# exit          /*Έξοδος από configure mode*/
```

```
core_switch_B# show run          /*Εμφάνισε τις ρυθμίσεις που είναι στην DRAM*/
core_switch_B# config t          /*Είσοδος σε configuration mode*/
core_switch_B(config)# service password-encryption     /*Κρυπτογράφηση κωδικών
                                                        συστήματος */
core_switch_B(config)# exit     /*Έξοδος από configure mode*/

core_switch_B# write    /*Αποθήκευσε όλες τις ρυθμίσεις στην non-volatile RAM*/
```

Σε αυτό το σημείο ρυθμίζουμε το core_switch_B για να λειτουργήσει ως VTP client του Core switch_A. Με αυτόν τον τρόπο το Core_switch_B θα ενημερωθεί αυτόματα για όλα τα VLAN που έχουν ρυθμιστεί ήδη στο core_switch_A.

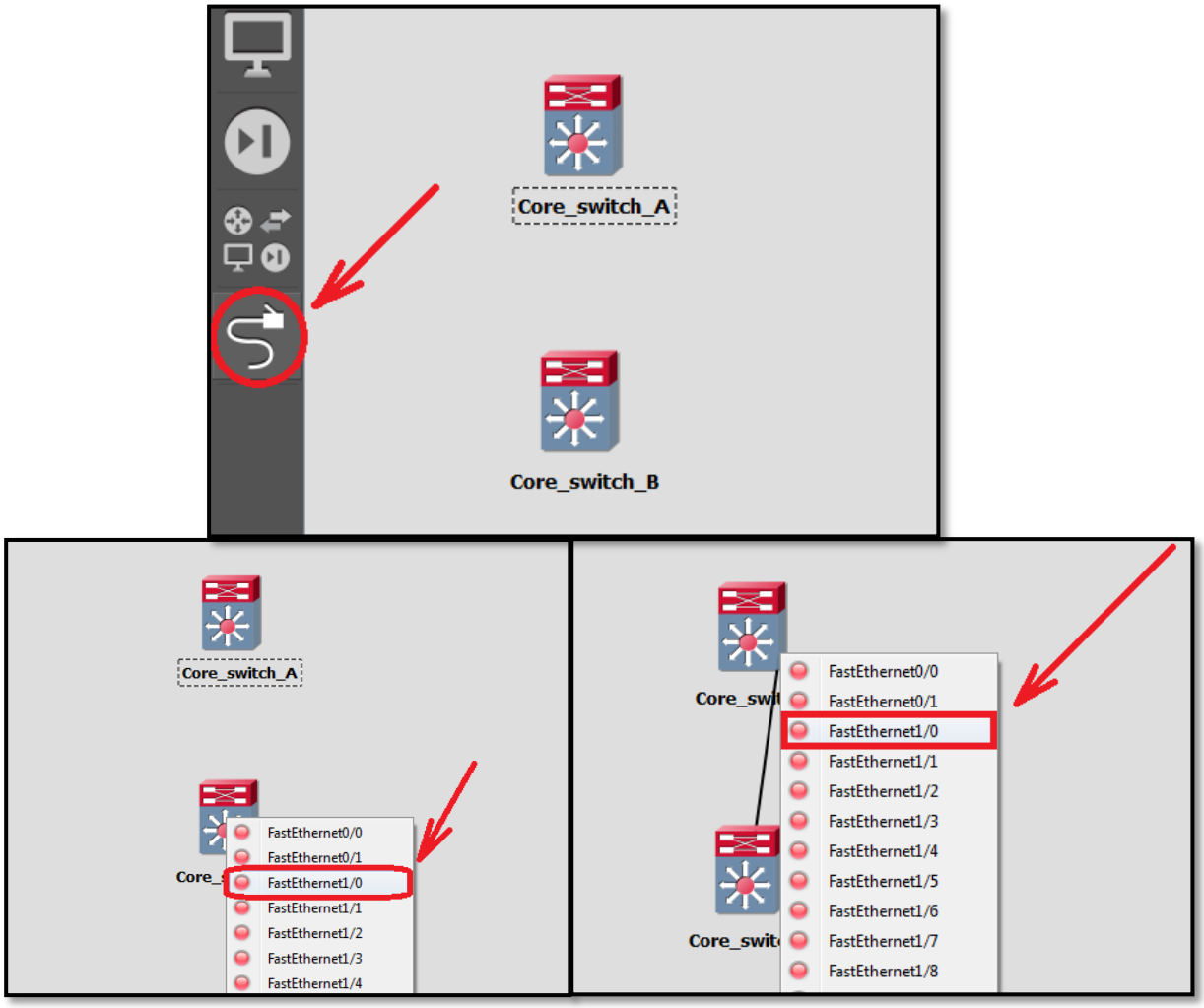
```
Core_switch_B# vlan database

/*Αρχικά κάνουμε το Core_switch_B ως server για να αλλάξουμε τις VTP ρυθμίσεις
του*/
Core_switch_B(vlan)# vtp server
Setting device to VTP SERVER mode.

Core_switch_B(vlan)# vtp v2-mode
V2 mode enabled.

Core_switch_B(vlan)# vtp password cisco123
Password already set to cisco123.

Core_switch_B(vlan)# vtp domain techcom.gr
Changing VTP domain name from NULL to techcom.gr

Core_switch_B(vlan)# apply       /*Αποθήκευση ρυθμίσεων*/
APPLY completed.

/*Η παρακάτω εντολή ρυθμίζει το Core_switch_B ως VTP client */

Core_switch_B(vlan)# vtp client
Setting device to VTP CLIENT mode.

Core_switch_B(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....
```

/* Αλλάζουμε τις ρυθμίσεις VTP για να είναι ίδιες με το VTP Server δηλαδή το core_switch_A */

Με τις παρακάτω εντολές ρυθμίζουμε την άλλη άκρη της σύνδεσης μεταξύ του core_switch_A και του core_switch_B.

```
Core_switch_B# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/* Με την παρακάτω εντολή ρυθμίζουμε την διεπαφή Fa1/0. */
Core_switch_B(config)# interface fastEthernet 1/0

/* Με την παρακάτω εντολή θέτουμε την διεπαφή Fa1/0 σε trunk mode. Δηλαδή μεταφέρει πολλαπλά VLANs πάνω από μια σύνδεση. By default περνάνε όλα τα υφιστάμενα vlan από το trunk. */
Core_switch_B(config-if)# switchport mode trunk

/* Με την παρακάτω εντολή ορίζουμε το πρωτόκολλο του trunk encapsulation στο IEEE 802.1q. */
Core_switch_B(config-if)# switchport trunk encapsulation dot1q

/* Με την παρακάτω εντολή ενεργοποιούμε την Fa1/0. */
Core_switch_B(config-if)# no shutdown

/* Δίνουμε περιγραφή. */
Core_switch_B(config-if)# description CONN WITH CORE A

/* Έξοδος από interface config-mode. */
Core_switch_B(config-if)# exit

/* Έξοδος από global config-mode. */
Core_switch_B(config)# exit

/*Αποθήκευσε όλες τις ρυθμίσεις στην non-volatile RAM*/
core_switch_B# write

Building configuration...
[OK]

/* Με την παρακάτω εντολή μας εμφανίζει την κατάσταση διεπαφών του core switch_B. Όπως βλέπουμε η θύρα Fa1/0 έχει πλέον την περιγραφή που της δώσαμε αλλά είναι ακόμα notconnect αφού δεν έχει συνδεθεί ακόμα με το core switch_A. */

Core_switch_B# show interface status
      Port     Name               Status     Vlan      Duplex      Speed Type
      Fa1/0 CONN WITH CORE A notconnect    1         auto     auto 10/100BaseTX
      Fa1/1                  notconnect    1         auto     auto 10/100BaseTX
      Fa1/2                  notconnect    1         auto     auto 10/100BaseTX
      Fa1/3                  notconnect    1         auto     auto 10/100BaseTX
                                          .
                                          .
                                          .
      Fa1/14                 notconnect    1         auto     auto 10/100BaseTX
      Fa1/15                 notconnect    1         auto     auto 10/100BaseTX
```

Συνδέουμε την fastEthernet θύρα 1/0 του Core Switch A με αυτήν του Core Switch B. Για να συνδέσουμε τους δύο αυτούς κόμβους πηγαίνοντας αριστερά στο tool box το κουμπί που είναι κυκλωμένο.



Εικόνα 5.13: Διασύνδεση μεταξύ των Core switches A και B

```
/* Με την παρακάτω εντολή μας εμφανίζει την κατάσταση διεπαφών του core
switch_B. Όπως βλέπουμε η θύρα Fa1/0 είναι πλέον συνδεδεμένη και ορίζεται ως
trunk. */

Core_switch_B# show interface status

Port     Name               Status       Vlan       Duplex Speed Type
Fa1/0    CONN WITH CORE A   connected    trunk      a-full   a-100 10/100BaseTX
Fa1/1                       notconnect   1            auto    auto 10/100BaseTX
Fa1/2                       notconnect   1            auto    auto 10/100BaseTX
                                         .
                                         .
                                         .
Fa1/15                      notconnect   1            auto    auto 10/100BaseTX
```

Ομοίως πράττουμε και στο Core Switch A για να δούμε αν συνδέθηκαν μεταξύ τους

```
Core_switch_A# show interface status

Port     Name               Status       Vlan       Duplex Speed Type
Fa1/0    CONN WITH CORE B   connected    trunk      a-full   a-100 10/100BaseTX
Fa1/1                       notconnect   1            auto    auto 10/100BaseTX
Fa1/2                       notconnect   1            auto    auto 10/100BaseTX
                                        .
                                        .
                                        .
Fa1/15                      notconnect   1            auto    auto 10/100BaseTX
```

Όπως παρατηρούμε η σύνδεση μεταξύ του core_switch_A και core_switch_B είναι ενεργή μεταξύ τους.

```
core_switch_B# vlan database      /*Είσοδος στην βάση που έχει αποθηκευμένα
                                  όλα τα στοιχεία που ρυθμίσαμε για τα vlan
                                  μας*/
core_switch_B(vlan)# show current       /*Προβολή στοιχείων vlans*/
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 100
    Name: wireless
    Media Type: Ethernet
    VLAN 802.10 Id: 100100
    State: Operational
    MTU: 1500

  VLAN ISL Id: 110
    Name: sales
    Media Type: Ethernet
    VLAN 802.10 Id: 100110
    State: Operational
    MTU: 1500

  VLAN ISL Id: 120
    Name: ManagementVlan
    Media Type: Ethernet
    VLAN 802.10 Id: 100120
    State: Operational
    MTU: 1500
```

/* Όλες οι θύρες ενός switch πρέπει να ανήκουν σε κάποιο vlan. Το VLAN με id 1 είναι το default vlan όπου όλες οι πόρτες (ports) ανήκουν σε αυτό. */

/* Εδώ μας δείχνει πληροφορίες για τα διάφορα vlan τμήματα που δημιουργήσαμε προηγούμενος. Οι πληροφορίες αυτές είναι το όνομα του VLAN (π.χ. wireless, ManagementVlan, Accounting Office κλπ), επίσης περιέχει το id που θέσαμε για κάθε τμήμα. Το πρωτόκολλο του data link layer που περνάει από το κάθε VLAN τμήμα στην συγκεκριμένη περίπτωση είναι το Ethernet (Media Type). Το πρότυπο 802.10 του οργανισμού IEEE καθορίζει τον τρόπο με τον οποίο θα μαρκάρονται τα πλαίσια (frames) με το κατάλληλο VLAN id κατά την διάρκεια της αποστολής. Δηλαδή έστω ένα πλαίσιο το οποίο μεταδίδεται από ένα VLAN με id 120 όπου είναι το ManagementVlan. Το πλαίσιο αυτό μαρκάρεται με το id 100120. Το MTU – Maximum Transmission Unit είναι το μέγιστο μέγεθος σε bytes που μπορεί να έχει ένα πλαίσιο σε αυτό το VLAN. By default παραμένει στα 1500 bytes */

```
VLAN ISL Id: 130
    Name: AccountingOffice
    Media Type: Ethernet
    VLAN 802.10 Id: 100130
    State: Operational
    MTU: 1500

  VLAN ISL Id: 140
    Name: Administration
    Media Type: Ethernet
    VLAN 802.10 Id: 100140
    State: Operational
    MTU: 1500

  VLAN ISL Id: 150
    Name: Marketing
    Media Type: Ethernet
    VLAN 802.10 Id: 100150
    State: Operational
    MTU: 1500

    VLAN ISL Id: 160
    Name: ServerLAN
    Media Type: Ethernet
    VLAN 802.10 Id: 100160
    State: Operational
    MTU: 1500

  VLAN ISL Id: 170
    Name: ITdep
    Media Type: Ethernet
    VLAN 802.10 Id: 100170
    State: Operational
    MTU: 1500

  VLAN ISL Id: 200
    Name: 2ndStore
    Media Type: Ethernet
    VLAN 802.10 Id: 100200
    State: Operational
    MTU: 1500
```

```
VLAN ISL Id: 1002
  Name: fddi-default
  Media Type: FDDI
  VLAN 802.10 Id: 101002
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Translational Bridged VLAN: 1
  Translational Bridged VLAN: 1003

VLAN ISL Id: 1003
  Name: token-ring-default
  Media Type: Token Ring
  VLAN 802.10 Id: 101003
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Ring Number: 0
  Bridge Number: 1
  Parent VLAN: 1005
  Maximum ARE Hop Count: 7
  Maximum STE Hop Count: 7
  Backup CRF Mode: Disabled
  Translational Bridged VLAN: 1
  Translational Bridged VLAN: 1002

  VLAN ISL Id: 1004
  Name: fddinet-default
  Media Type: FDDI Net
  VLAN 802.10 Id: 101004
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Bridge Number: 1
  STP Type: IBM

  VLAN ISL Id: 1005
  Name: trnet-default
  Media Type: Token Ring Net
  VLAN 802.10 Id: 101005
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Bridge Number: 1
  STP Type: IBM
```

```
/* Αυτά τα VLAN εξυπηρετούν παλιά πρότυπα. Στην ουσία δεν χρησιμοποιούνται και ο σκοπός τους είναι να υπάρχουν για να εξυπηρετούν παλιά δίκτυα. Αυτά τα πρότυπα δεν μπορούν να σβηστούν. */
```

Παρατηρούμε ότι εκτελόντας την εντολή show current στον core switch B τα VLAN που δημιουργήθηκαν στο Core Switch A αυτομάτως περάστηκαν στο Core switch B μέσω του πρωτόκολλου VTP.

```
Core_switch_B# show vtp status
VTP Version                     : 2
Configuration Revision          : 4
Maximum VLANs supported locally : 68
Number of existing VLANs        : 14
VTP Operating Mode              : Client
VTP Domain Name                 : techcom.gr
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x29 0x67 0xF4 0x00 0x28 0x8A 0xF2 0xEB
Configuration last modified by 172.16.0.2 at 3-1-02 00:08:36

Core_switch_B# config t
Enter configuration commands, one per line.  End with CNTL/Z.

          /*Δημιουργία VLANs και ανάθεση IP διευθύνσεων στο καθένα*/

/*Δίνουμε στο υποκατάστημα με vlan name wireless και id 100 network ip
172.16.0.3 και μάσκα υποδικτύου 255.255.255.192*/

Core_switch_B(config)# interface vlan 100
Core_switch_B(config-if)# ip address 172.16.0.3 255.255.255.192
Core_switch_B(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name sales και id 110 network ip
172.16.0.67 και μάσκα υποδικτύου 255.255.255.224*/

Core_switch_B(config)# interface vlan 110
Core_switch_B(config-if)# ip address 172.16.0.67 255.255.255.224
Core_switch_B(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name ManagementVlan και id 120 network ip
172.16.0.99 και μάσκα υποδικτύου 255.255.255.224*/

Core_switch_B(config-if)# interface vlan 120
Core_switch_B(config-if)# ip address 172.16.0.99 255.255.255.224
Core_switch_B(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name AccountingOffice και id 130 network ip
172.16.0.131 και μάσκα υποδικτύου 255.255.255.240*/

Core_switch_B(config-if)# interface vlan 130
Core_switch_B(config-if)# ip address 172.16.0.131 255.255.255.240
Core_switch_B(config-if)# no shutdown
```

```
/*Δίνουμε στο υποκατάστημα με vlan name Administration και id 140 network ip
172.16.0.140 και μάσκα υποδικτύου 255.255.255.240*/

Core_switch_B(config-if)# interface vlan 140
Core_switch_B(config-if)# ip address 172.16.0.147 255.255.255.240
core_switch_B(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name Marketing και id 150 network ip
172.16.0.163 και μάσκα υποδικτύου 255.255.255.240*/

Core_switch_B(config)# interface vlan 150
Core_switch_B(config-if)# ip address 172.16.0.163 255.255.255.240
core_switch_B(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name ServerLAN και id 160 network ip
172.16.0.179 και μάσκα υποδικτύου 255.255.255.240*/

Core_switch_B(config-if)# interface vlan 160
Core_switch_B(config-if)# ip address 172.16.0.179 255.255.255.240
core_switch_B(config-if)# no shutdown

/*Δίνουμε στο υποκατάστημα με vlan name ITdep και id 170 network ip
172.16.0.194 και μάσκα υποδικτύου 255.255.255.248*/

Core_switch_B(config-if)# interface vlan 170
Core_switch_B(config-if)# ip address 172.16.0.195 255.255.255.248
core_switch_B(config-if)# no shutdown

core_switch_B(config-if)# exit   /*Εξοδος από configure interface mode*/
core_switch_B(config)# exit/*Εξοδος από configure mode*/

Core_switch_B# write /*Αποθήκευσε όλες τις ρυθμίσεις στην non-volatile RAM*/
```

Παρακάτω ελέγχουμε την διασυνδεσιμότητα των VLANs μεταξύ των core switches πραγματοποιώντας κάποια ping απ'το core switch B προς τις IP διευθύνσεις όλων των VLAN θυρών στο core switch A. Παρατηρούμε στις περισσότερες περιπτώσεις το πρώτο πακέτο ping αποτυγχάνει ενώ τα υπόλοιπα επιτυγχάνουν. Ο λόγος που συμβαίνει αυτό είναι διότι στέλνεται στην αρχή ένα broadcast μήνυμα ARP αίτησης που ζητάει την MAC διεύθυνση που αντιστοιχεί στην συγκεκριμένη IP διεύθυνση ώστε να μπορέσει να το καταχωρίσει στον πινακα φυσικών διευθύνσεων MAC που διαθέτει.

```
/* Έλεγχος επικοινωνίας μεταξύ των VLANs στα δύο switches */

Core_switch_B# ping 172.16.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/27/56 ms

Core_switch_B# ping 172.16.0.66

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.66, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 16/29/48 ms
```

```
Core_switch_B# ping 172.16.0.98

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.98, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/31/48 ms

Core_switch_B# ping 172.16.0.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.130, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/27/36 ms

Core_switch_B# ping 172.16.0.146

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.146, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 32/58/124 ms

Core_switch_B# ping 172.16.0.162

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.162, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/39/92 ms

Core_switch_B# ping 172.16.0.178

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.178, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 16/27/52 ms

Core_switch_B# ping 172.16.0.194

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.194, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/27/52 m
```

```
/* Ρύθμιση HSRP στον Core Switch A */


/* Μπαίνουμε στις ρυθμίσεις του vlan 100 και ενεργοποιούμε το HSRP με την
εντολή standby. Με την εντολή standby 100 ip 172.16.0.1 ορίζουμε την εικονική
IP για το vlan 100 και ονομάζουμε την ομάδα HSRP με το όνομα 100. Αυτό το
κάνουμε για να μπορέσει το core switch A να συνεργαστεί με το core switch B.
Με την εντολή standby 100 priority 255 ορίζουμε την προτεραιότητα του core
switch A έτσι ώστε να είναι πάντα το active switch για το vlan 100. Με αυτόν
τον τρόπο η εικονική ip διεύθυνση αντιστοιχεί στο core switch A. Η εντολή
standby 100 preempt υποχρεώνει το core switch A να αναλάβει ξανά τον ενεργό
ρόλο αφού διορθωθεί κάποια τυχόν βλάβη.
Παρατηρούμε ότι μετά την ενεργοποίηση του HSRP (δηλαδή με την εντολή standby)
η κατάσταση του core switch A αλλάζει από standby σε active. */

core_switch_A(config)# interface vlan 100
core_switch_A(config-if)# standby 100 ip 172.16.0.1

*Mar  1 00:40:45.983: %HSRP-5-STATECHANGE: Vlan100 Grp 100 state Speak ->
Standby
*Mar  1 00:40:46.483: %HSRP-5-STATECHANGE: Vlan100 Grp 100 state Standby ->
Active
core_switch_A(config-if)# standby 100 priority 255
core_switch_A(config-if)# standby 100 preempt


/* Παρομοίως ρυθμίστηκαν τα interfaces των vlan 110, 120 και 130. */

core_switch_A(config)# interface vlan 110
core_switch_A(config-if)# standby 110 ip 172.16.0.65
*Mar  1 00:40:45.983: %HSRP-5-STATECHANGE: Vlan110 Grp 110 state Speak ->
Standby
*Mar  1 00:40:46.483: %HSRP-5-STATECHANGE: Vlan110 Grp 110 state Standby ->
Active
core_switch_A(config-if)# standby 110 priority 255
core_switch_A(config-if)# standby 110 preempt

core_switch_A(config-if)# interface vlan 120
core_switch_A(config-if)# standby 120 ip 172.16.0.97
*Mar  1 00:43:29.779: %HSRP-5-STATECHANGE: Vlan120 Grp 120 state Speak ->
Standby
*Mar  1 00:43:30.279: %HSRP-5-STATECHANGE: Vlan120 Grp 120 state Standby ->
Active

core_switch_A(config-if)# standby 120 priority 255
core_switch_A(config-if)# standby 120 preempt

core_switch_A(config-if)# interface vlan 130
core_switch_A(config-if)# standby 130 ip 172.16.0.129
*Mar  1 00:45:28.943: %HSRP-5-STATECHANGE: Vlan130 Grp 130 state Speak ->
Standby
*Mar  1 00:45:29.443: %HSRP-5-STATECHANGE: Vlan130 Grp 130 state Standby ->
Active
core_switch_A(config-if)# standby 130 preempt
core_switch_A(config-if)# standby 130 priority 255
```

```
/* Τα vlan 140, 150, 160 και 170 θα έχουν ως active switch το core switch B.
Γι αυτό οι ρυθμίσεις των προτεραιοτήτων διαφέρουν. Μπαίνουμε στις ρυθμίσεις
του vlan 140 και ενεργοποιούμε το HSRP με την εντολή standby. Με την εντολή
standby 140 ip ip 172.16.0.145 ορίζουμε την εικονική IP για το vlan 140 και
ονομάζουμε την ομάδα HSRP με το όνομα 140. Αυτό το κάνουμε για να μπορέσει το
core switch B να συνεργαστεί με το core switch A. Με την εντολή standby 140
priority 1 ορίζουμε την προτεραιότητα του core switch A έτσι ώστε να μην είναι
το active switch για το vlan 140. Το core switch B θα ρυθμιστεί με την
κατάλληλη προτεραιότητα για να γίνει αυτό. Με αυτόν τον τρόπο η εικονική ip
διεύθυνση αντιστοιχεί στο core switch B.
Παρατηρούμε ότι μετά την ενεργοποίηση του HSRP (δηλαδή με την εντολή standby)
η κατάσταση του core switch A αλλάζει από standby σε active. Αυτό συμβαίνει
επειδή το core switch B δεν έχει ρυθμιστεί ακόμα. Όταν ρυθμιστεί το core
switch B θα γίνει active και το core switch A θα γίνει standby. */

core_switch_A(config-if)# interface vlan 140
core_switch_A(config-if)# standby 140 ip 172.16.0.145
core_switch_A(config-if)# standby 140 priority 1

*Mar  1 00:46:31.071: %HSRP-5-STATECHANGE: Vlan140 Grp 140 state Speak ->
Standby
*Mar  1 00:46:31.571: %HSRP-5-STATECHANGE: Vlan140 Grp 140 state Standby ->
Active

/* Παρομοίως ρυθμίστηκαν τα interfaces των vlan 150, 160 και 170. */

core_switch_A(config-if)# interface vlan 150
core_switch_A(config-if)# standby 150 ip 172.16.0.161
core_switch_A(config-if)# standby 150 priority 1

*Mar  1 00:47:26.979: %HSRP-5-STATECHANGE: Vlan150 Grp 150 state Speak ->
Standby
*Mar  1 00:47:27.479: %HSRP-5-STATECHANGE: Vlan150 Grp 150 state Standby ->
Active

core_switch_A(config-if)# interface vlan 160
core_switch_A(config-if)# standby 160 ip 172.16.0.177
core_switch_A(config-if)# standby 160 priority 1

*Mar  1 00:48:15.627: %HSRP-5-STATECHANGE: Vlan160 Grp 160 state Speak ->
Standby
*Mar  1 00:48:16.127: %HSRP-5-STATECHANGE: Vlan160 Grp 160 state Standby ->
Active

core_switch_A(config-if)# interface vlan 150
core_switch_A(config-if)# standby 170 ip 172.16.0.193
core_switch_A(config-if)# standby 170 priority 1

*Mar  1 00:48:15.627: %HSRP-5-STATECHANGE: Vlan170 Grp 170 state Speak ->
Standby
*Mar  1 00:48:16.127: %HSRP-5-STATECHANGE: Vlan170 Grp 170 state Standby ->
Active
```

```
/* Ρύθμιση HSRP στον Core Switch B */


/* Μπαίνουμε στις ρυθμίσεις του vlan 100 και ενεργοποιούμε το HSRP με την εντολή standby. Με την εντολή standby 100 ip 172.16.0.1 ορίζουμε την εικονική IP για το vlan 100 και ονομάζουμε την ομάδα HSRP με το όνομα 100 όπως κάναμε και στο core switch A. Με την εντολή standby 100 priority 1 ορίζουμε την προτεραιότητα του core switch B έτσι ώστε να είναι πάντα το standby switch για το vlan 100. Με αυτόν τον τρόπο η εικονική ip διεύθυνση αντιστοιχεί στο core switch A που έχει υψηλότερη προτεραιότητα.
Παρατηρούμε ότι μετά την ενεργοποίηση του HSRP (δηλαδή με την εντολή standby) η κατάσταση του core switch B παραμένει σε standby. */

Core_switch_B(config)# interface vlan 100
Core_switch_B(config-if)# standby 100 ip 172.16.0.1
Core_switch_B(config-if)# standby 100 priority 1

*Mar  1 00:34:50.143: %HSRP-5-STATECHANGE: Vlan100 Grp 100 state Speak ->
Standby

/* Παρομοίως ρυθμίστηκαν τα interfaces των vlan 110, 120 και 130. Παρατηρούμε στις παρακάτω εντολές ότι το αποτέλεσμα είναι η κατάσταση του core switch B να είναι standby. */

Core_switch_B(config-if)# interface vlan 110
Core_switch_B(config-if)# standby 110 ip 172.16.0.65
Core_switch_B(config-if)# standby 110 priority 1

*Mar  1 00:52:28.679: %HSRP-5-STATECHANGE: Vlan110 Grp 110 state Speak ->
Standby

Core_switch_B(config-if)#interface vlan 120
Core_switch_B(config-if)#standby 120 ip 172.16.0.97
Core_switch_B(config-if)#standby 120 priority 1

*Mar  1 00:53:41.539: %HSRP-5-STATECHANGE: Vlan120 Grp 120 state Speak ->
Standby

Core_switch_B(config-if)# interface vlan 130
Core_switch_B(config-if)# standby 130 ip 172.16.0.129
Core_switch_B(config-if)# standby 130 priority 1

*Mar  1 00:54:09.975: %HSRP-5-STATECHANGE: Vlan130 Grp 130 state Speak ->
Standby
```

```
/* Τα vlan 140, 150, 160 και 170 θα έχουν ως active switch το core switch B.
Γι αυτό οι ρυθμίσεις των προτεραιοτήτων διαφέρουν. Μπαίνουμε στις ρυθμίσεις
του vlan 140 και ενεργοποιούμε το HSRP με την εντολή standby. Με την εντολή
standby 140 ip ip 172.16.0.145 ορίζουμε την εικονική IP για το vlan 140 και
ονομάζουμε την ομάδα HSRP με το όνομα 140. Αυτό το κάνουμε για να μπορέσει το
core switch A να συνεργαστεί με το core switch B. Με την εντολή standby 140
priority 255 ορίζουμε την προτεραιότητα του core switch B έτσι ώστε να
αναλαμβάνει τον ρόλο του active switch για το vlan 140. Το core switch A έχει
ρυθμιστεί με την κατάλληλη προτεραιότητα για να γίνει αυτό. Με αυτόν τον τρόπο
η εικονική ip διεύθυνση αντιστοιχεί στο core switch B. Η εντολή standby 140
preempt υποχρεώνει το core switch B να αναλάβει ξανά τον ενεργό ρόλο αφού
διορθωθεί κάποια τυχόν βλάβη.
Παρατηρούμε ότι μετά την ενεργοποίηση του HSRP (δηλαδή με την εντολή standby)
η κατάσταση του core switch B αλλάζει από standby σε active. Αυτό συμβαίνει
επειδή το core switch B δεν έχει ρυθμιστεί ακόμα. Όταν ρυθμιστεί το core
switch B θα γίνει active και το core switch A θα γίνει standby. */

Core_switch_B(config-if)# interface vlan 140
Core_switch_B(config-if)# standby 140 ip 172.16.0.145
Core_switch_B(config-if)# standby 140 priority 255
Core_switch_B(config-if)# standby 140 preempt

*Mar  1 00:55:01.419: %HSRP-5-STATECHANGE: Vlan140 Grp 140 state Speak ->
Active

/* Παρομοίως ρυθμίστηκαν τα interfaces των vlan 150, 160 και 170. Παρατηρούμε
στις παρακάτω εντολές ότι το αποτέλεσμα είναι η κατάσταση του core switch B να
είναι active. */

Core_switch_B(config-if)# interface vlan 150
Core_switch_B(config-if)# standby 150 ip 172.16.0.161
Core_switch_B(config-if)# standby 150 priority 255
Core_switch_B(config-if)# standby 150 preempt

*Mar  1 00:55:40.351: %HSRP-5-STATECHANGE: Vlan150 Grp 150 state Speak ->
Active

Core_switch_B(config-if)# interface vlan 160
Core_switch_B(config-if)# standby 160 ip 172.16.0.177
Core_switch_B(config-if)# standby 160 preempt
Core_switch_B(config-if)# standby 160 priority 255

*Mar  1 00:56:55.267: %HSRP-5-STATECHANGE: Vlan160 Grp 160 state Listen ->
Active
Core_switch_B(config-if)# interface vlan 170
Core_switch_B(config-if)# standby 170 priority 255
Core_switch_B(config-if)# standby 170 preempt
Core_switch_B(config-if)# standby 170 ip 172.16.0.193

*Mar  1 00:57:34.399: %HSRP-5-STATECHANGE: Vlan170 Grp 170 state Listen ->
Active
Core_switch_B(config-if)# exit
Core_switch_B(config)# exit
*Mar  1 00:57:43.515: %SYS-5-CONFIG_I: Configured from console by console
```

Όπως παρατηρούμε παρακάτω εκτελώντας την εντολή show standby brief σε privileged exec mode μας εμφανίζει την κατάσταση του HSRP. Για τα VLANs 100 έως 130 το local switch δηλαδή το core switch A είναι active. Παρατηρούμε ότι για τα ίδια VLAN το standby switch είναι το core switch B που αντιστοιχεί στις τέσσερις IP διευθύνσεις που βρίσκονται στην στήλη standby. Για τα VLAN 140 έως 170 το local switch είναι standby. Παρατηρούμε ότι για τα ίδια VLAN το active switch είναι το core switch B που αντιστοιχεί στις 4 IP διευθύνσεις που βρίσκονται στην στήλη active.

```
core_switch_A# show standby brief

                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl100       100 255  P Active   local           172.16.0.3      172.16.0.1
Vl110       110 255  P Active   local           172.16.0.67     172.16.0.65
Vl120       120 255  P Active   local           172.16.0.99     172.16.0.97
Vl130       130 255  P Active   local           172.16.0.131    172.16.0.129
Vl140       140 1      Standby  172.16.0.147    local           172.16.0.145
Vl150       150 1      Standby  172.16.0.163    local           172.16.0.161
Vl160       160 1      Standby  172.16.0.179    local           172.16.0.177
Vl170       170 1      Standby  172.16.0.195    local           172.16.0.193
```

Όπως παρατηρούμε παρακάτω εκτελώντας την εντολή show standby brief σε privileged exec mode στο core switch B φαίνονται οι αντίστοιχες πληροφορίες ανάστροφα.

```
Core_switch_B# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Vl100       100 1      Standby  172.16.0.2      local           172.16.0.1
Vl110       110 1      Standby  172.16.0.66     local           172.16.0.65
Vl120       120 1      Standby  172.16.0.98     local           172.16.0.97
Vl130       130 1      Standby  172.16.0.130    local           172.16.0.129
Vl140       140 255  P Active   local           172.16.0.146    172.16.0.145
Vl150       150 255  P Active   local           172.16.0.162    172.16.0.161
Vl160       160 255  P Active   local           172.16.0.178    172.16.0.177
Vl170       170 255  P Active   local           172.16.0.194    172.16.0.193
```

Συμπεράνουμε από τα παραπάνω ότι το πρωτόκολλο HSRP έχει ρυθμιστεί και στους δύο core switches με επιτυχία.

Παρακάτω το core switch A ώστε να λειτουργεί ως DHCP server των υποδικτύων της εταιρίας.

```
/* Με την εντολή ip dhcp pool wireless δημιουργούμε ένα DHCP pool που είναι
ένα σύνολο IP διευθύνσεων που θα εκχωρούνται στους hosts του ασύρματου
υποδικτύου. Με την εντολή network ορίζουμε το φάσμα των ip διευθύνσεων που θα
εκχωρούνται στους hosts. Με την εντολή default-router ορίζουμε το default
gateway που θα δωθεί στους hosts σε αυτό το υποδίκτυο.  Τέλος η εντολή ip dhcp
excluded-address ορίζει ποίες διευθύνσεις του φάσματος εξαιρούνται από αυτήν
την εκχώρηση*/

core_switch_A(config)# ip dhcp pool wireless
core_switch_A(dhcp-config)# network 172.16.0.0 255.255.255.192
core_switch_A(dhcp-config)# default-router 172.16.0.1
core_switch_A(dhcp-config)# exit
core_switch_A(config)# ip dhcp excluded-address 172.16.0.1 172.16.0.3

/* Παρομοίως ρυθμίζουμε τα DHCP pools για τα υπόλοιπα υποδίκτυα της εταιρίας.

core_switch_A(config)# ip dhcp pool sales
core_switch_A(dhcp-config)# network 172.16.0.64 255.255.255.224
core_switch_A(dhcp-config)# default-router 172.16.0.65
core_switch_A(dhcp-config)# exit
core_switch_A(config)# ip dhcp excluded-address 172.16.0.65 172.16.0.71

core_switch_A(config)# ip dhcp pool accountingoffice
core_switch_A(dhcp-config)# network 172.16.0.128 255.255.255.240
core_switch_A(dhcp-config)# default-router 172.16.0.129
core_switch_A(dhcp-config)# exit
core_switch_A(config)# ip dhcp excluded-address 172.16.0.129 172.16.0.134

core_switch_A(config)# ip dhcp pool administration
core_switch_A(dhcp-config)# network 172.16.0.144 255.255.255.240
core_switch_A(dhcp-config)# default-router 172.16.0.145
core_switch_A(dhcp-config)# exit
core_switch_A(config)# ip dhcp excluded-address 172.16.0.145 172.16.0.150

core_switch_A(config)# ip dhcp pool marketing
core_switch_A(dhcp-config)# network 172.16.0.160 255.255.255.240
core_switch_A(dhcp-config)# default-router 172.16.0.161
core_switch_A(dhcp-config)# exit
core_switch_A(config)# ip dhcp excluded-address 172.16.0.161 172.16.0.166

core_switch_A(dhcp-config)# write
```

Επειδή το core switch A και το core switch B αναλαμβάνουν την διαδικασία εφεδρείας σε περίπτωση που κάποιος από τους δύο τεθεί εκτός λειτουργίας (π.χ. λόγο βλάβης) οι ρυθμίσεις που γίνονται στον έναν απ' τους δύο απαραίτητα πρέπει να γίνουν και στον άλλο. Οπότε με τις ίδιες εντολές που ρυθμίσαμε για το DHCP pool στον core switch A θα κάνουμε και για τον core switch B.

```
core_switch_B(config)# ip dhcp pool wireless
core_switch_B(dhcp-config)# network 172.16.0.0 255.255.255.192
core_switch_A(dhcp-config)# default-router 172.16.0.1
core_switch_B(dhcp-config)# exit
core_switch_B(config)# ip dhcp excluded-address 172.16.0.1 172.16.0.3

core_switch_B(config)# ip dhcp pool sales
core_switch_B(dhcp-config)# network 172.16.0.64 255.255.255.224
core_switch_A(dhcp-config)# default-router 172.16.0.65
core_switch_B(dhcp-config)# exit
core_switch_B(config)# ip dhcp excluded-address 172.16.0.65 172.16.0.71

core_switch_B(config)# ip dhcp pool accountingoffice
core_switch_B(dhcp-config)# network 172.16.0.128 255.255.255.240
core_switch_A(dhcp-config)# default-router 172.16.0.129
core_switch_B(dhcp-config)# exit
core_switch_B(config)# ip dhcp excluded-address 172.16.0.129 172.16.0.134

core_switch_B(config)# ip dhcp pool administration
core_switch_B(dhcp-config)# network 172.16.0.144 255.255.255.240
core_switch_A(dhcp-config)# default-router 172.16.0.145
core_switch_B(dhcp-config)# exit
core_switch_A(config)# ip dhcp excluded-address 172.16.0.145 172.16.0.150

core_switch_B(config)# ip dhcp pool marketing
core_switch_B(dhcp-config)# network 172.16.0.160 255.255.255.240
core_switch_A(dhcp-config)# default-router 172.16.0.129
core_switch_B(dhcp-config)# exit
core_switch_B(config)# ip dhcp excluded-address 172.16.0.161 172.16.0.166

core_switch_B(dhcp-config)#write
```

5.2 Ρυθμίσεις server switches A και B

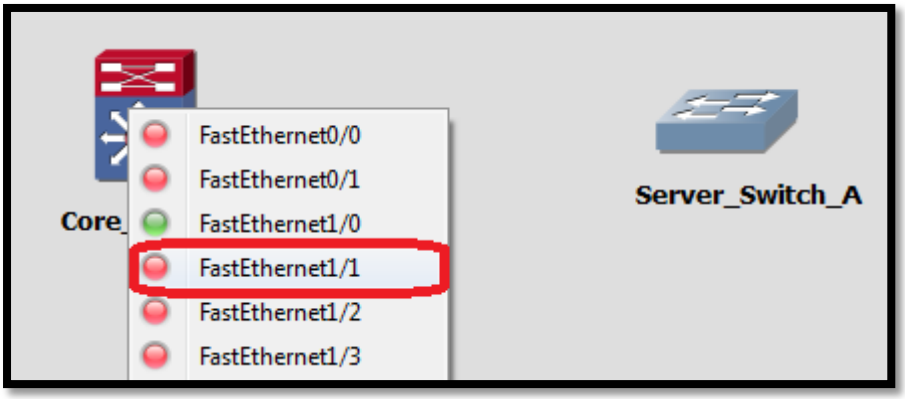
Για να τοποθετήσουμε τα server switches ακολουθήσαμε την ίδια ακριβώς διαδικασία με αυτήν που κάναμε στην παράγραφο 5.1. Δηλαδή θα πάρουμε από το toolbox των routers την συσκευή c3745. Στο menu → change symbol για επιλογή εικονιδίου (icon) διαλέγουμε το switch.

```
                              /*Ρυθμίσεις παραμέτρων*/

Server_Switch_A# config t        /*Είσοδος σε configuration mode*/
Enter configuration commands, one per line.  End with CNTL/Z.
Server_Switch_A(config)# hostname server_switch_A  /*Θέτουμε το hostname
                                                     server switch A*/
server_switch_A(config)# enable secret cisco123 /*Θέτουμε κωδικό για να μπούμε σε
                                                 privileged user exec (enable) mode*/
server_switch_A(config)# line con 0
server_switch_A(config-line)# password cisco123  /*Θέτουμε κωδικό στην κονσόλα σε
                                                   cisco123*/
server_switch_A(config-line)# login   /*Υποχρέωσε τον χρήστη να κάνει login*/
server_switch_A(config-line)# exit   /*Εξοδος από configure line mode*/
server_switch_A(config)# line vty 0 1340  /*Ρυθμίζουμε εικονικά τερματικά από 0
                                            έως 1340 που είναι το μέγιστο */
server_switch_A(config-line)# password cisco123 /* Θέτουμε κωδικό για config-line
server_switch_A(config-line)# transport input ssh /* Εισήγαγε SSH, και
                                                    απενεργοποίησε το telnet*/
server_switch_A(config-line)# login /*Υποχρέωσε τον χρήστη να κάνει login*/
server_switch_A(config-line)# exit
server_switch_A(config)# service password-encryption /*Κρυπτογράφηση κωδικών
                                                       συστήματος */
server_switch_A(config)# exit
server_switch_A# write
Building configuration...
[OK]

server_switch_A# config t        /*Είσοδος σε configuration mode*/
server_switch_A# no ip http server
server_switch_A# no ip http secure-server
server_switch_A# exit      /*Εξοδος από configure mode*/

 /*Για να θέσω VLAN ονόματα και id για το κάθε τμήμα. Πρέπει να είμαι σε user exec
mode.  Εδώ χρειάζεται μόνο ένα VLAN να φτιάξουμε για την αρχική επικοινωνία μεταξύ
        του server_switch A και του VTP server, δηλαδή το Core Switch A.*/

server_switch_A# vlan database
 server_switch_A(vlan)# vlan 120 name ManagementVlan /*εδώ προσθέτουμε το vlan 120
                                                       για να επιτύχουμε την αρχική
                                                      επικοινωνία με το VTP server.*/
VLAN 120 added:
    Name: ManagementVlan

server_switch_A(vlan)# vlan 120 state active
VLAN 120 modified:
    State ACTIVE
```

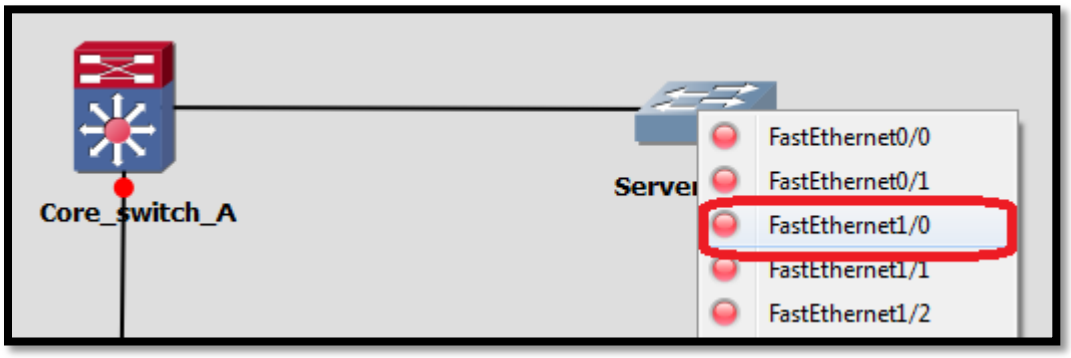
```
server_switch_A(vlan)# show current  /* Ελέγχουμε την κατάσταση των VLANs*/
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 120
    Name: ManagementVlan
    Media Type: Ethernet
    VLAN 802.10 Id: 100120
    State: Operational
    MTU: 1500
    .
    .
    .
    .
server_switch_A(vlan)# exit
APPLY completed.
Exiting....

server_switch_A# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/*Δίνουμε στο υποκατάστημα με vlan name ManagementVlan και id 120 network ip
172.16.0.100 και μάσκα υποδικτύου 255.255.255.224*/

server_switch_A(config)# interface vlan 120
server_switch_A(config-if)# ip address 172.16.0.100 255.255.255.224
server_switch_A(config-if)# no shutdown
server_switch_A(config-if)# exit
server_switch_A(config)# exit

server_switch_A# vlan database   /*Είσοδος στην βάση που έχει αποθηκευμένα όλα
                                 τα στοιχεία που ρυθμίσαμε για τα vlan μας*/

/* Θέλουμε να δώσουμε ένα vtp domain για να το κάνουμε αυτό χρησιμοποιούμε την
εντολή domain και δίνουμε ένα κατάλληλο όνομα που στην περίπτωση μας είναι το
techcom.gr. */

server_switch_A(vlan)# vtp domain techcom.gr
Changing VTP domain name from NULL to techcom.gr

server_switch_A(vlan)# vtp password cisco123
Setting device VLAN database password to cisco123.

/* Χρησιμοποιούμε το vtp v2-mode. Αυτή η έκδοση είναι η πιο καινούργια του
πρωτοκόλλου του VTP. */

server_switch_A(vlan)# vtp v2-mode
V2 mode enabled.
```

```
server_switch_A(vlan)# apply     /* Χρησιμοποιούμε την apply για να αποθηκευτούν
APPLY completed.                 οι αλλαγές στην μνήμη */

server_switch_A(vlan)# vtp client      /*Ενεργοποιούμε το client mode για να
Setting device to VTP CLIENT mode.     λάβει όλες τις πληροφορίες των VLAN από
server_switch_A(vlan)# exit            τον VTP server. */
In CLIENT state, no apply attempted.
Exiting....

/* Βλέπουμε την κατάσταση των interfaces με εντολή show ip interface brief */

server_switch_A# show ip interface brief
Interface        IP-Address      OK? Method Status                Protocol
FastEthernet0/0  unassigned      YES unset  administratively down down
FastEthernet0/1  unassigned      YES unset  administratively down down
FastEthernet1/0  unassigned      YES unset  up                    down
FastEthernet1/1  unassigned      YES unset  up                    down
                                     .
                                     .
                                     .
                                     .
FastEthernet1/15 unassigned      YES unset  up                    down
Vlan1            unassigned      YES unset  up                    down
Vlan120          172.16.0.100    YES manual up                    down

server_switch_A# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/* Με την παρακάτω εντολή ρυθμίζουμε την διεπαφή Fa1/0. */
server_switch_A(config)# interface fa1/0
server_switch_A(config-if)# description CONN WITH CORE_A

/* Με την παρακάτω εντολή θέτουμε την διεπαφή Fa1/0 σε trunk mode. Δηλαδή
μεταφέρει πολλαπλά VLANs πάνω από μια σύνδεση. By default περνάνε όλα τα
υφιστάμενα vlan από το trunk. */

server_switch_A(config-if)# switchport mode trunk
*Mar  1 00:14:29.739: %DTP-5-TRUNKPORTON: Port Fa1/0 has become dot1q trunk
*Mar  1 00:14:30.207: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan120,
changed state to down
*Mar  1 00:15:00.315: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
*Mar  1 00:15:00.339: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan120,
changed state to up

server_switch_A(config-if)# no shutdown

server_switch_A(config-if)# exit
server_switch_A(config)# exit                        ^
*Mar  1 00:15:20.987: %SYS-5-CONFIG_I: Configured from console by console
```

```
core_switch_A# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/* Με την παρακάτω εντολή θέτουμε την διεπαφή Fa1/1 σε trunk mode. Δηλαδή
μεταφέρει πολλαπλά VLANs πάνω από μια σύνδεση. By default περνάνε όλα τα
υφιστάμενα vlan από το trunk. */

core_switch_A(config)# interface fa1/1
core_switch_A(config-if)# description CONN WITH SERVER_SW_A
core_switch_A(config-if)# switchport mode trunk
Core_switch_A(config-if)# no shutdown
core_switch_A(config-if)# exit
core_switch_A(config)# exit
*Mar  1 00:07:21.007: %DTP-5-TRUNKPORTON: Port Fa1/1 has become dot1q trunk

core_switch_A# write
Building configuration...
[OK]
```



Εικόνα 5.14: Διασύνδεση μεταξύ του Core switch A και του Server switch A



Εικόνα 5.15: Διασύνδεση μεταξύ του Core switch A και του Server switch A

```
server_switch_A# vlan database  /*Είσοδος στην βάση που έχει αποθηκευμένα όλα
                                 τα στοιχεία που ρυθμίσαμε για τα vlan μας*/
server_switch_A(vlan)# show current   /*Προβολή στοιχείων vlans*/
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 100
    Name: wireless
    Media Type: Ethernet
    VLAN 802.10 Id: 100100
    State: Operational
    MTU: 1500

  VLAN ISL Id: 110
    Name: sales
    Media Type: Ethernet
    VLAN 802.10 Id: 100110
    State: Operational
    MTU: 1500

  VLAN ISL Id: 120
    Name: ManagementVlan
    Media Type: Ethernet
    VLAN 802.10 Id: 100120
    State: Operational
    MTU: 1500
        .
        .
        .
        .
  VLAN ISL Id: 1005
    Name: trbrf-default
    Media Type: TRBRF
    VLAN 802.10 Id: 101005
    State: Operational
    MTU: 4472
    Bridge Type: SRB
    Bridge Number: 15
    STP Type: IBM

server_switch_A(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....
```

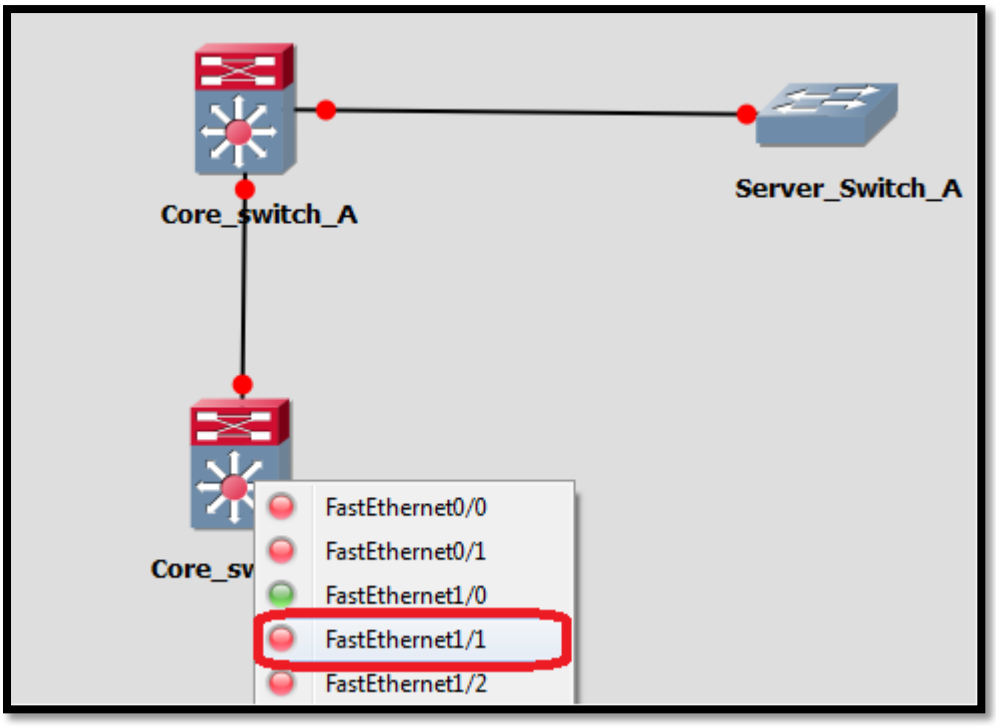
/* Όλες οι θύρες ενός switch πρέπει να ανήκουν σε κάποιο vlan. Το VLAN με id 1 είναι το default vlan όπου όλες οι πόρτες (ports) ανήκουν σε αυτό. */

/* Εδώ μας δείχνει πληροφορίες για τα διάφορα vlan τμήματα που δημιουργήσαμε προηγούμενος. Οι πληροφορίες αυτές είναι το όνομα του VLAN (π.χ. wireless, ManagementVlan, Accounting Office κλπ), επίσης περιέχει το id που θέσαμε για κάθε τμήμα. Το πρωτόκολλο του data link layer που περνάει από το κάθε VLAN τμήμα στην συγκεκριμένη περίπτωση είναι το Ethernet (Media Type). Το πρότυπο 802.10 του οργανισμού IEEE καθορίζει τον τρόπο με τον οποίο θα μαρκάρονται τα πλαίσια (frames) με το κατάλληλο VLAN id κατά την διάρκεια της αποστολής. Δηλαδή έστω ένα πλαίσιο το οποίο μεταδίδεται από ένα VLAN με id 120 όπου είναι το ManagementVlan. Το πλαίσιο αυτό μαρκάρεται με το id 100120. Το MTU – Maximum Transmission Unit είναι το μέγιστο μέγεθος σε bytes που μπορεί να έχει ένα πλαίσιο σε αυτό το VLAN. By default παραμένει στα 1500 bytes */

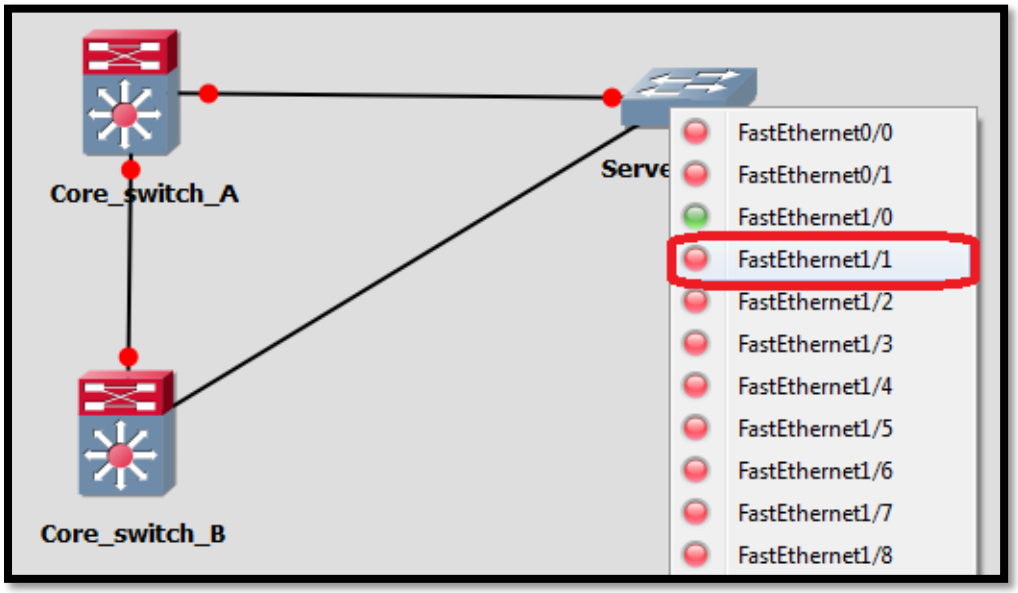
```
server_switch_A# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/*Εδώ ρυθμίζουμε την θύρα fastethernet 1/1 για να συνδεθεί με το Core Switch
B, δηλαδή με την εφεδρική σύνδεση του sever switch A.*/

server_switch_A(config)# interface fa1/1
server_switch_A(config-if)# description CONN WITH CORE_B
server_switch_A(config-if)# switchport mode trunk
server_switch_A(config-if)# no shutdown
server_switch_A(config-if)# exit
server_switch_A(config)# exit
*Mar  1 00:22:28.135: %SYS-5-CONFIG_I: Configured from console by console

server_switch_A# write
Building configuration...
[OK]
```

Στην συνέχεια πηγαίνουμε στο core switch B για να ρυθμίσουμε την θύρα επικοινωνίας όπου θα συνδεθεί η εφεδρική σύνδεση του server switch A.

```
Core_switch_B# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/*Ρυθμίζουμε την θύρα fastethernet 1/1 για να συνδεθεί με το server Switch A.

Core_switch_B(config)# interface fa1/1
Core_switch_B(config-if)# description CONN WITH SERVER_SW_A
Core_switch_B(config-if)# switchport mode trunk
Core_switch_B(config-if)# no shutdown
Core_switch_B(config-if)# exit
Core_switch_B(config)# exit
*Mar  1 00:14:40.855: %SYS-5-CONFIG_I: Configured from console by console

Core_switch_B# write
Building configuration...
[OK]
```



Εικόνα 5.16: Διασύνδεση μεταξύ του Core switch B και του Server switch A



Εικόνα 5.17: Διασύνδεση μεταξύ του Core switch B και του Server switch A

Μπαίνοντας στο server switch A μπορούμε να δούμε την λειτουργία του spanning tree protocol το οποίο είναι ενεργοποιημένο εξ αρχής χωρίς να δώσουμε ρυθμίσεις γι αυτό.

```
/*Με την παρακάτω εντολή, ελέγχετε η κατάσταση του spanning-tree πρωτοκόλλου.
Βλέπουμε εδώ την ταυτότητα του route bridge και την κατάσταση των πορτών του
τοπικού switch (Blocked ή Forwarding) */


server_switch_A# show spanning-tree brief

VLAN1
                                .
                                .
                                .

VLAN100
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     c401.08e8.0001
              Cost        19
              Port        41 (FastEthernet1/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     c403.0f30.0001
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                    Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0      128.41   128    19 FWD     0 32768 c401.08e8.0001 128.42
FastEthernet1/1      128.42   128    19 BLK    19 32768 c402.07a8.0001 128.42

                                .
                                .
                                .
                                .
                                .
                                .
```

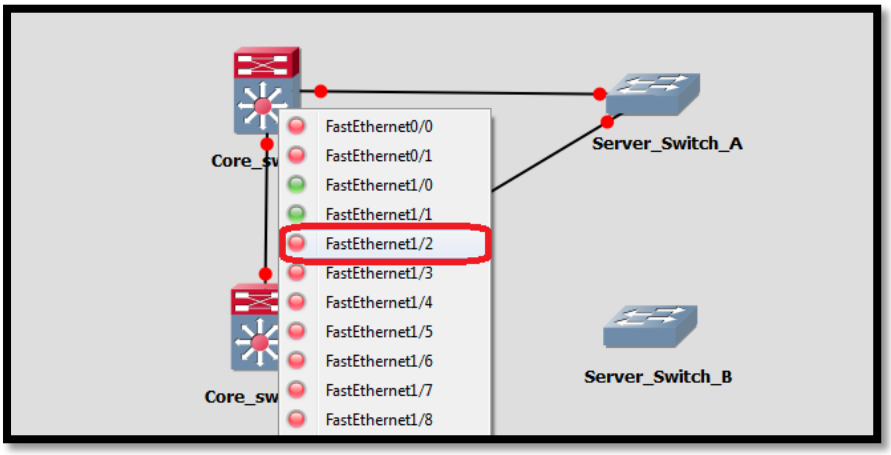
Σε αυτό το σημείο τοποθετούμε το server switch B. Οι ρυθμίσεις γι αυτό ακολουθούνται παρακάτω.

```
                          /*Ρυθμίσεις παραμέτρων*/

Server_Switch_B# config t  /*Είσοδος σε configuration mode*/
Enter configuration commands, one per line.  End with CNTL/Z.

Server_Switch_B(config)# hostname server_switch_B    /*Θέτουμε το hostname
                                                      server switch B*/

server_switch_B(config)# enable secret cisco123  /*Θέτουμε κωδικό για να
                                                μπούμε σε privileged user exec
                                                (enable) mode*/
server_switch_B(config)# line con 0
server_switch_B(config-line)# password cisco123  /*Θέτουμε κωδικό στην κονσόλα
                                                σε cisco123*/
server_switch_B(config-line)# login   /*Υποχρέωσε τον χρήστη να κάνει login*/
server_switch_B(config-line)# exit    /*Έξοδος από configure line mode*/

server_switch_B(config)# line vty 0 1340    /*Ρυθμίζουμε εικονικά τερματικά
                                           από 0 έως 1340 που είναι το μέγιστο */
server_switch_B(config-line)# password cisco123  /* Θέτουμε κωδικό για config-
                                                 line
server_switch_B(config-line)# transport input ssh     /* Εισήγαγε SSH, και
                                                     απενεργοποίησε το telnet*/
server_switch_B(config-line)# login   /*Υποχρέωσε τον χρήστη να κάνει login*/
server_switch_B(config-line)# exit
server_switch_B(config)# service password-encryption  /*Κρυπτογράφηση κωδικών
                                                      συστήματος */
server_switch_B(config)# exit

server_switch_B# write
Building configuration...
[OK]

/*Για να θέσω VLAN ονόματα και id για το κάθε τμήμα. Πρέπει να είμαι σε user
exec mode.   Εδώ χρειάζεται μόνο ένα VLAN να φτιάξουμε για την αρχική
επικοινωνία μεταξύ του server_switch B και του VTP server, δηλαδή το Core
Switch A.*/

server_switch_B# vlan database

 server_switch_B(vlan)# vlan 120 name ManagementVlan /*εδώ προσθέτουμε το vlan
             120 για να επιτύχουμε την αρχική επικοινωνία με το VTP server.*/
VLAN 120 added:
    Name: ManagementVlan

server_switch_B(vlan)# vlan 120 state active
VLAN 120 modified:
    State ACTIVE
```

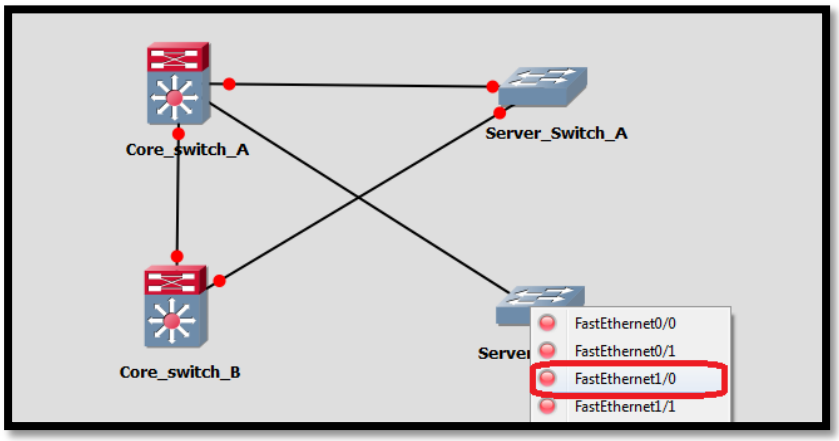
```
server_switch_B(vlan)# show current   /* Ελέγχουμε την κατάσταση των VLANs*/
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 120
    Name: ManagementVlan
    Media Type: Ethernet
    VLAN 802.10 Id: 100120
    State: Operational
    MTU: 1500
    .
    .
    .
    .
server_switch_B(vlan)# exit
APPLY completed.
Exiting....

server_switch_B# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/*Δίνουμε στο server switch με vlan name ManagementVlan και id 120 network ip
172.16.0.101 και μάσκα υποδικτύου 255.255.255.224*/

server_switch_B(config)# interface vlan 120
server_switch_B(config-if)# ip address 172.16.0.101 255.255.255.224
server_switch_B(config-if)# no shutdown
server_switch_B(config-if)# exit
server_switch_B(config)# exit

server_switch_A# vlan database   /*Είσοδος στην βάση που έχει αποθηκευμένα όλα
                                 τα στοιχεία που ρυθμίσαμε για τα vlan μας*/

server_switch_B(vlan)# vtp domain techcom.gr
Changing VTP domain name from NULL to techcom.gr
server_switch_B(vlan)# vtp password cisco123
Setting device VLAN database password to cisco123.

/* Χρησιμοποιούμε το vtp v2-mode. Αυτή η έκδοση είναι η πιο καινούργια του
πρωτοκόλλου του VTP. */

server_switch_B(vlan)# vtp v2-mode
V2 mode enabled.

server_switch_B(vlan)# apply     /* Χρησιμοποιούμε την apply για να
APPLY completed.                 αποθηκευτούν οι αλλαγές στην μνήμη */
```

```
server_switch_B(vlan)# vtp client          /*Ενεργοποιούμε το client mode για να
Setting device to VTP CLIENT mode.         λάβει όλες τις πληροφορίες των VLAN
                                           από τον VTP server. */
server_switch_B(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....

server_switch_B# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/* Με την παρακάτω εντολή ρυθμίζουμε την διεπαφή Fa1/0. */

server_switch_B(config)# interface fa1/0
server_switch_B(config-if)# description CONN WITH CORE A

/* Με την παρακάτω εντολή θέτουμε την διεπαφή Fa1/0 σε trunk mode. Δηλαδή
μεταφέρει πολλαπλά VLANs πάνω από μια σύνδεση. By default περνάνε όλα τα
υφιστάμενα vlan από το trunk. */

server_switch_B(config-if)# switchport mode trunk
*Mar  1 00:14:29.739: %DTP-5-TRUNKPORTON: Port Fa1/0 has become dot1q trunk
*Mar  1 00:14:30.207: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan120,
changed state to down
*Mar  1 00:15:00.315: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
*Mar  1 00:15:00.339: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan120,
changed state to up

server_switch_B(config-if)# no shutdown
server_switch_B(config-if)# exit
server_switch_B(config)# exit                          ^
*Mar  1 00:15:20.987: %SYS-5-CONFIG_I: Configured from console by console

server_switch_B# write
Building configuration...
[OK]
```

```
core_switch_A# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/* Με την παρακάτω εντολή θέτουμε την διεπαφή Fa1/2 σε trunk mode. Δηλαδή
μεταφέρει πολλαπλά VLANs πάνω από μια σύνδεση. By default περνάνε όλα τα
υφιστάμενα vlan από το trunk. */

core_switch_A(config)# interface fa1/2
core_switch_A(config-if)# description CONN WITH SERVER_SW_B
core_switch_A(config-if)# switchport mode trunk
Core_switch_A(config-if)# no shutdown
core_switch_A(config-if)# exit
core_switch_A(config)# exit
*Mar  1 00:07:21.007: %DTP-5-TRUNKPORTON: Port Fa1/2 has become dot1q trunk

core_switch_A# write
Building configuration...
[OK]
```



Εικόνα 5.18: Διασύνδεση μεταξύ του Core switch A και του Server switch B



Εικόνα 5.19: Διασύνδεση μεταξύ του Core switch A και του Server switch B

```
server_switch_B# vlan database    /*Είσοδος στην βάση που έχει αποθηκευμένα όλα
                                    τα στοιχεία που ρυθμίσαμε για τα vlan μας*/
server_switch_B(vlan)# show current   /*Προβολή στοιχείων vlans*/
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 100
    Name: wireless
    Media Type: Ethernet
    VLAN 802.10 Id: 100100
    State: Operational
    MTU: 1500

  VLAN ISL Id: 110
    Name: sales
    Media Type: Ethernet
    VLAN 802.10 Id: 100110
    State: Operational
    MTU: 1500

  VLAN ISL Id: 120
    Name: ManagementVlan
    Media Type: Ethernet
    VLAN 802.10 Id: 100120
    State: Operational
    MTU: 1500
        .
        .
        .
        .
  VLAN ISL Id: 1005
    Name: trbrf-default
    Media Type: TRBRF
    VLAN 802.10 Id: 101005
    State: Operational
    MTU: 4472
    Bridge Type: SRB
    Bridge Number: 15
    STP Type: IBM

server_switch_B(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....
```

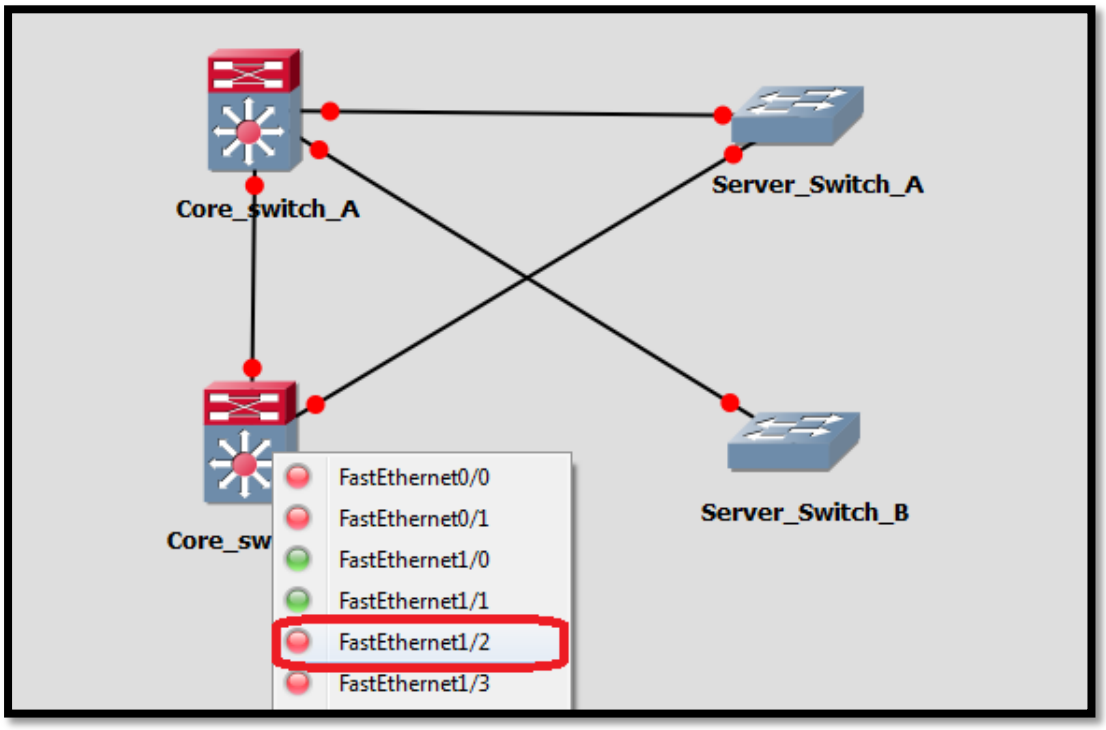
/* Όλες οι θύρες ενός switch πρέπει να ανήκουν σε κάποιο vlan. Το VLAN με id 1 είναι το default vlan όπου όλες οι πόρτες (ports) ανήκουν σε αυτό. */

/* Εδώ μας δείχνει πληροφορίες για τα διάφορα vlan τμήματα που δημιουργήσαμε προηγούμενος. Οι πληροφορίες αυτές είναι το όνομα του VLAN (π.χ. wireless, ManagementVlan, Accounting Office κλπ), επίσης περιέχει το id που θέσαμε για κάθε τμήμα. Το πρωτόκολλο του data link layer που περνάει από το κάθε VLAN τμήμα στην συγκεκριμένη περίπτωση είναι το Ethernet (Media Type). Το πρότυπο 802.10 του οργανισμού IEEE καθορίζει τον τρόπο με τον οποίο θα μαρκάρονται τα πλαίσια (frames) με το κατάλληλο VLAN id κατά την διάρκεια της αποστολής. Δηλαδή έστω ένα πλαίσιο το οποίο μεταδίδεται από ένα VLAN με id 120 όπου είναι το ManagementVlan. Το πλαίσιο αυτό μαρκάρεται με το id 100120. Το MTU – Maximum Transmission Unit είναι το μέγιστο μέγεθος σε bytes που μπορεί να έχει ένα πλαίσιο σε αυτό το VLAN. By default παραμένει στα 1500 bytes */

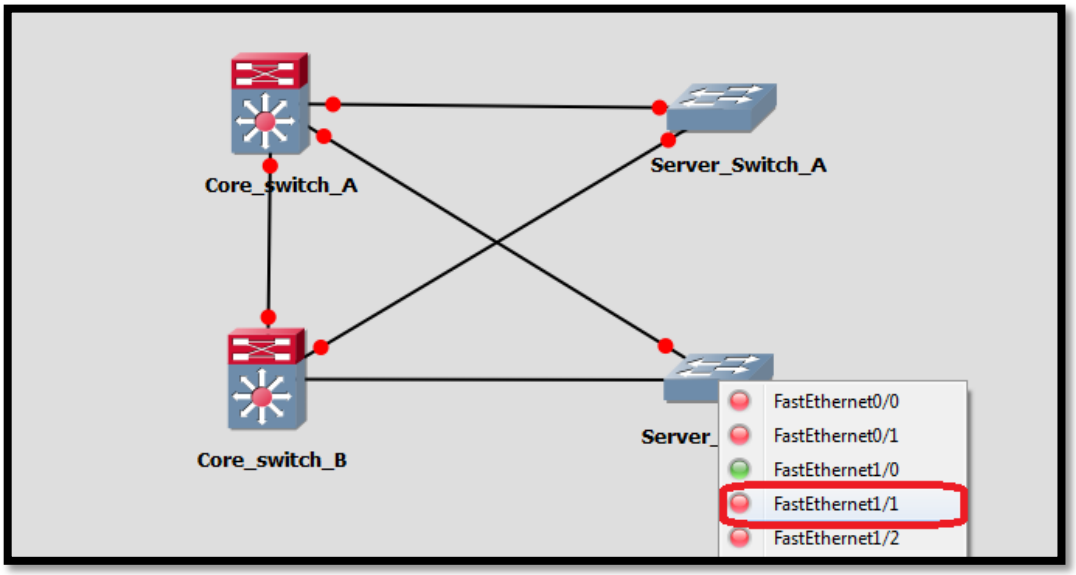
```
server_switch_B# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/*Εδώ ρυθμίζουμε την θύρα fastethernet 1/1 για να συνδεθεί με το Core Switch
B, δηλαδή με την εφεδρική σύνδεση του sever switch B.*/

server_switch_B(config)# interface fa1/1
server_switch_B(config-if)# description CONN WITH CORE B
server_switch_B(config-if)# switchport mode trunk
server_switch_B(config-if)# no shutdown
server_switch_B(config-if)# exit
server_switch_B(config)# exit
*Mar  1 00:22:28.135: %SYS-5-CONFIG_I: Configured from console by console

server_switch_B# write
Building configuration...
[OK]
```

Στην συνέχεια πηγαίνουμε στο core switch B για να ρυθμίσουμε την θύρα επικοινωνίας όπου θα συνδεθεί η εφεδρική σύνδεση του server switch B.

```
Core_switch_B# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/*Ρυθμίζουμε την θύρα fastethernet 1/2 για να συνδεθεί με το server Switch A.

Core_switch_B(config)# interface fa1/2
Core_switch_B(config-if)# description CONN WITH SERVER_SW_B
Core_switch_B(config-if)# switchport mode trunk
Core_switch_B(config-if)# no shutdown
Core_switch_B(config-if)# exit
Core_switch_B(config)# exit
*Mar  1 00:14:40.855: %SYS-5-CONFIG_I: Configured from console by console

Core_switch_B# write
Building configuration...
[OK]
```



Εικόνα 5.20: Διασύνδεση μεταξύ του Core switch B και του Server switch B



Εικόνα 5.21: Διασύνδεση μεταξύ του Core switch B και του Server switch B

Μπαίνοντας στο server switch B μπορούμε να δούμε την λειτουργία του spanning tree protocol το οποίο είναι ενεργοποιημένο εξ αρχής χωρίς να δώσουμε ρυθμίσεις γι αυτό.

```
server_switch_B# show spanning-tree brief
                                        .
                                        .
                                        .
VLAN100
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     c401.08e8.0001
              Cost        19
              Port        41 (FastEthernet1/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     c404.1950.0001
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                  Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0      128.41   128    19 FWD     0 32768 c401.08e8.0001 128.43
FastEthernet1/1      128.42   128    19 BLK    19 32768 c402.07a8.0001 128.43
```

Παρατηρούμε ότι το root bridge επιλέγεται σύμφωνα με την φυσική διεύθυνση MAC. Σε αυτό το σημείο πρέπει να σημειώσουμε ότι δεν θέλουμε να επιλεχθεί σύμφωνα με την MAC διεύθυνση αλλά σύμφωνα με την προτεραιότητα που θα ορίσουμε εμείς.

5.3 Ρυθμίσεις STP για όλο το δίκτυο

Παρακάτω θα επιχειρήσουμε να ρυθμίσουμε το core switch A ώστε να είναι το root bridge για τα VLAN που εξυπηρετεί και θα λειτουργεί σαν εφεδρικό root bridge στα υπόλοιπα VLAN. Αντίστοιχα, το core switch B θα ρυθμιστεί ώστε να είναι το root bridge για τα VLAN που εξυπηρετεί και θα λειτουργεί και αυτό με την σειρά στα υπόλοιπα VLANs που διαθέτει ως εφεδρικό root bridge.

```
core_switch_A# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/*Ρυθμίζουμε τις root bridge προτεραιότητες του core Switch A για κάθε VLAN.

core_switch_A(config)# spanning-tree vlan 100 priority 0
core_switch_A(config)# spanning-tree vlan 110 priority 0
core_switch_A(config)# spanning-tree vlan 120 priority 0
core_switch_A(config)# spanning-tree vlan 130 priority 0
core_switch_A(config)# spanning-tree vlan 140 priority 4096
core_switch_A(config)# spanning-tree vlan 150 priority 4096
core_switch_A(config)# spanning-tree vlan 160 priority 4096
core_switch_A(config)# spanning-tree vlan 170 priority 4096
core_switch_A(config)# exit
core_switch_A# write
Building configuration...
[OK]
```

```
Core_switch_B# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/*Ρυθμίζουμε τις root bridge προτεραιότητες του core Switch B για κάθε VLAN.

Core_switch_B(config)# spanning-tree vlan 100 priority 4096
Core_switch_B(config)# spanning-tree vlan 110 priority 4096
Core_switch_B(config)# spanning-tree vlan 120 priority 4096
Core_switch_B(config)# spanning-tree vlan 130 priority 4096
Core_switch_B(config)# spanning-tree vlan 140 priority 0
Core_switch_B(config)# spanning-tree vlan 150 priority 0
Core_switch_B(config)# spanning-tree vlan 160 priority 0
Core_switch_B(config)# spanning-tree vlan 170 priority 0
Core_switch_B(config)# exit
core_switch_B# write
Building configuration...
[OK]
```

5.4 Εγκαταστάσεις access switch για κάθε όροφο

Όπως είχαμε δει στο 3ο κεφάλαιο που αναφέραμε την δομή του δίκτυο είχαμε προσθέσει σε κάθε όροφο της τηλεπικοινωνιακής εταιρίας access switches. Οι όροφοι της εταιρίας αυτής είναι στο σύνολο τους 4 οπότε θα προσθέσουμε αυτό τον αριθμό από switches. Ξεκινάμε με τις ρυθμίσεις του 3ου ορόφου. Για να το κάνουμε αυτό θα προσθέσουμε ένα access switch στον οποίον θα διασυνδέονται όλοι οι κόμβοι αυτού του ορόφου. Για να τοποθετήσουμε τα access switches ακολουθάμε την ίδια ακριβώς διαδικασία με αυτήν που κάναμε στην παράγραφο 5.1. Δηλαδή θα πάρουμε από το toolbox των routers την συσκευή c3745. Στο menu → change symbol για επιλογή εικονιδίου (icon) διαλέγουμε το switch.

```
    ################## Configuration of 3rd Floor Switch ##################
              ********************************************
3rd_floor# config t
Enter configuration commands, one per line.  End with CNTL/Z.

3rd_floor(config)# hostname 3rd_floor     /* Δίνουμε το hostname 3rd_floor στην
                                             συσκευή και ρυθμίζουμε στοιχεία
3rd_floor(config)# line console 0            πρόσβασης*/
3rd_floor(config-line)# password cisco123
3rd_floor(config-line)# login
3rd_floor(config-line)# line vty 0 15
3rd_floor(config-line)# password cisco123
3rd_floor(config-line)# login
3rd_floor(config-line)# transport input ssh
3rd_floor(config-line)# exit
3rd_floor(config)# service password-encryption
3rd_floor(config)# enable secret cisco123
3rd_floor(config)# exit

*Mar  1 00:03:47.335: %SYS-5-CONFIG_I: Configured from console by console
```

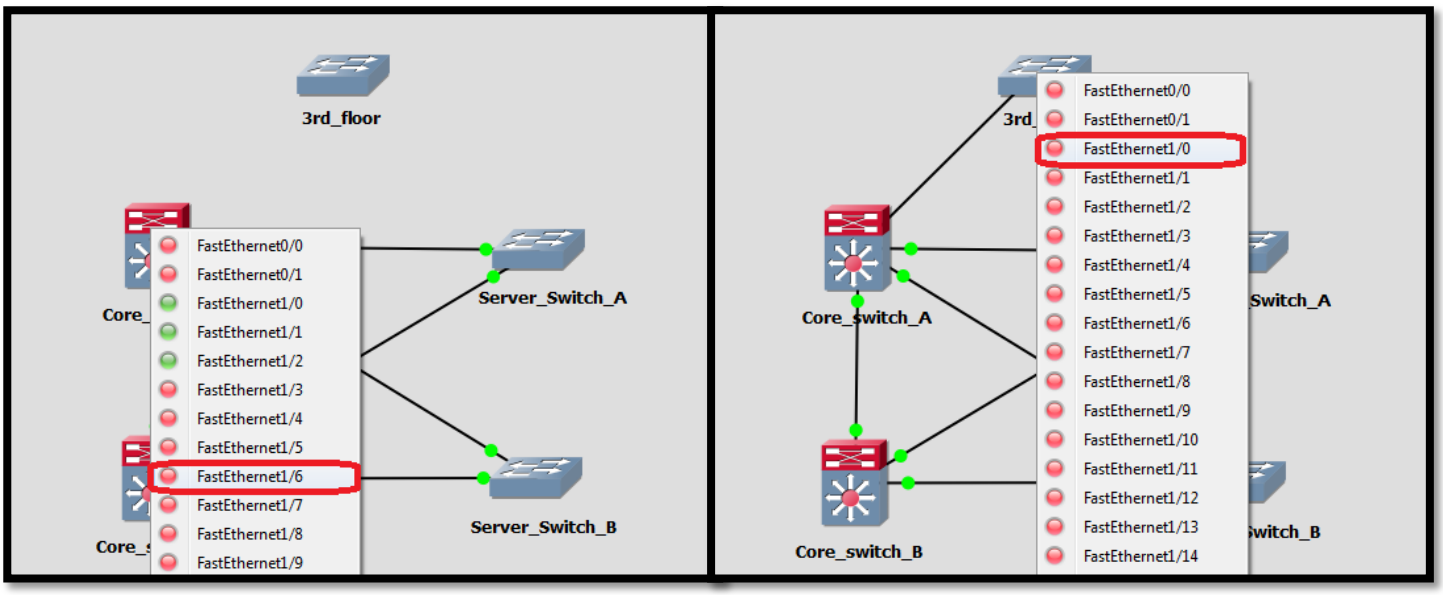
```
3rd_floor# vlan database

3rd_floor(vlan)# vlan 120
VLAN 120 added:
    Name: VLAN0120
3rd_floor(vlan)# exit
APPLY completed.
Exiting....

3rd_floor# config t
Enter configuration commands, one per line.  End with CNTL/Z.

/*Δίνουμε στο switch το vlan name ManagementVlan και id 120 network ip
172.16.0.105 και μάσκα υποδικτύου 255.255.255.224*/

3rd_floor(config)# interface vlan 120
3rd_floor(config-if)# ip address 172.16.0.105 255.255.255.224
3rd_floor(config-if)# no shutdown
3rd_floor(config-if)# exit

3rd_floor(config)# interface fa 1/0                    /* Ρυθμίζουμε τις
3rd_floor(config-if)# description CONN WITH CORE A     συνδέσεις προς το CORE
3rd_floor(config-if)# switchport mode trunk            switch A και B*/
3rd_floor(config-if)# no shutdown
3rd_floor(config-if)# exit

3rd_floor(config)# interface fa 1/1
3rd_floor(config-if)# description CONN WITH CORE B
3rd_floor(config-if)# switchport mode trunk
3rd_floor(config-if)# no shutdown
3rd_floor(config-if)# exit
3rd_floor(config)# exit

*Mar  1 00:08:06.343: %SYS-5-CONFIG_I: Configured from console by console

3rd_floor# vlan database          /*Είσοδος στην βάση που έχει αποθηκευμένα όλα
                                  τα στοιχεία που ρυθμίσαμε για τα vlan μας*/
3rd_floor(vlan)# vtp domain techcom.gr
Changing VTP domain name from NULL to techcom.gr

3rd_floor(vlan)# vtp password cisco123
Setting device VLAN database password to cisco123.
/* Χρησιμοποιούμε το vtp v2-mode. Αυτή η έκδοση είναι η πιο καινούργια του
πρωτοκόλλου του VTP. */
3rd_floor(vlan)# vtp v2-mode
V2 mode enabled.
/* Χρησιμοποιούμε την apply για να αποθηκευτούν οι αλλαγές στην μνήμη */
3rd_floor(vlan)# apply
APPLY completed.

3rd_floor(vlan)# vtp client
Setting device to VTP CLIENT mode.          /*Ενεργοποιούμε το client mode για να
                                            λάβει όλες τις πληροφορίες των VLAN
3rd_floor(vlan)# exit                       από τον VTP server. */
In CLIENT state, no apply attempted.
Exiting....
3rd_floor# write
Building configuration...
[OK]
```

Ρυθμίσεις στο core switch A για σύνδεση με το 3rd floor switch

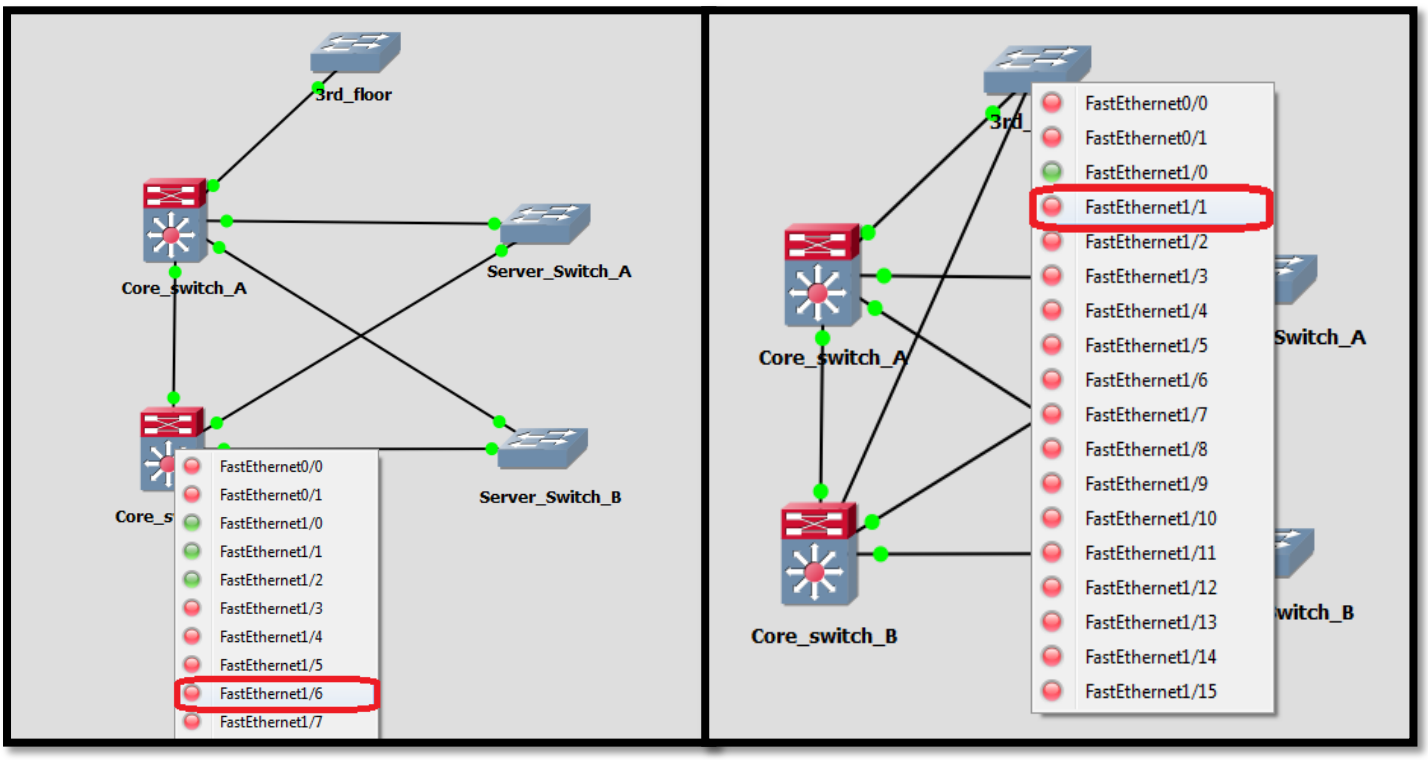
```
core_switch_A# conf t
core_switch_A (config)# interface fastethernet 1/6
core_switch_A (config-if)# description CONN WITH 3rd_FLOOR
core_switch_A (config-if)# switchport mode trunk
core_switch_A (config-if)# no shutdown
core_switch_A (config-if)# exit
core_switch_A (config)# exit
core_switch_A # write
Building configuration...
[OK]
```

Ρυθμίσεις στο core switch B για σύνδεση με το 3rd floor switch

```
core_switch_B# conf t
core_switch_B(config)# interface fastethernet 1/6
core_switch_B(config-if)# description CONN WITH 2nd_FLOOR
core_switch_B(config-if)# switchport mode trunk
core_switch_B(config-if)# no shutdown
core_switch_B(config-if)# exit
core_switch_B(config)# exit
core_switch_B# write
Building configuration...
[OK]
```



Εικόνα 5.22: Διασύνδεση μεταξύ του Core switch A και του switch του 3ου ορόφου



Εικόνα 5.23: Διασύνδεση μεταξύ του Core switch B και του switch του 3ου οροφου

```
################## Configure Access Ports 3rd Floor Switch ##################
                ********************************************

3rd_floor# conf t
3rd_floor(config)# interface range fastethernet 1/2 - 11
3rd_floor(config-if)# switchport mode access
3rd_floor(config-if)# switchport access vlan 140
3rd_floor(config-if)# no shutdown
3rd_floor(config-if)# exit                                  /* Εδώ ρυθμίζουμε τις
                                                            access πόρτες για τα σωστά
3rd_floor(config)# interface fastethernet 1/12              VLANs και απενεργοποιούμε
3rd_floor(config-if)# switchport mode access                αυτές που δεν
3rd_floor(config-if)# switchport access vlan 100            χρισημοποιούναι*/
3rd_floor(config-if)# no shutdown
3rd_floor(config-if)# exit

3rd_floor(config)# interface range fastethernet 1/13 - 15
3rd_floor(config-if)# shutdown
3rd_floor(config-if)# exit

*Mar  1 00:28:21.507: %LINK-5-CHANGED: Interface FastEthernet1/13, changed
state to administratively down
*Mar  1 00:28:21.515: %LINK-5-CHANGED: Interface FastEthernet1/14, changed
state to administratively down
*Mar  1 00:28:21.527: %LINK-5-CHANGED: Interface FastEthernet1/15, changed
state to administratively down

3rd_floor(config)# exit
*Mar  1 00:28:37.847: %SYS-5-CONFIG_I: Configured from console by console

3rd_floor# write
Building configuration...
[OK]
```

```
################## Test run in 3rd Floor Switch ##################
**************************************************

3rd_floor# show run                          /* Με την εντολή show run μπορούμε να
Building configuration...                    δούμε τις τρέχουσες ρυθμίσεις του
                                             switch και να ελέγξουμε αν είναι
Current configuration : 2105 bytes           σωστές. */
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname 3rd_Floor
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Z.Xk$EPiOFkMXqB7PxuzpEwJ2g.
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
!
!
ip tcp synwait-time 5
ip ssh version 1
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
 description CONN WITH CORE A
 switchport mode trunk
!
```

```
interface FastEthernet1/1
 description CONN WITH CORE B
 switchport mode trunk
!
interface FastEthernet1/2
 switchport access vlan 140
!
interface FastEthernet1/3
 switchport access vlan 140
!
interface FastEthernet1/4
 switchport access vlan 140
!
interface FastEthernet1/5
 switchport access vlan 140
!
interface FastEthernet1/6              /* Παρατηρούμε ότι τα interfaces
 switchport access vlan 140            ανίκου σε διάφορα VLANs και ότι κάποια
!                                      interfaces είναι shutdown, δηλαδή
interface FastEthernet1/7              απενεργοποιμένα. */
 switchport access vlan 140
!
interface FastEthernet1/8
 switchport access vlan 140
!
interface FastEthernet1/9
 switchport access vlan 140
!
interface FastEthernet1/10
 switchport access vlan 140
!
interface FastEthernet1/11
 switchport access vlan 140
!
interface FastEthernet1/12
 switchport access vlan 100
!
interface FastEthernet1/13
 shutdown
!
interface FastEthernet1/14
 shutdown
!
interface FastEthernet1/15
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan120
 ip address 172.16.0.105 255.255.255.224
!
ip forward-protocol nd
!
```

```
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
!
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password 7 104D000A061843595F
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password 7 05080F1C22431F5B4A
 login
 transport input ssh
line vty 5 15
 password 7 05080F1C22431F5B4A
 login
 transport input ssh
!
!
end
```

Σε αυτό το σημείο αφού τελειώσαμε με τον 3ο όροφο θα ξεκινήσουμε την διαδικασία εγκατάστασης access switch στον 2ο όροφο. Για να τοποθετήσουμε τα access switches ακολουθάμε την ίδια ακριβώς διαδικασία με αυτήν που κάναμε παραπάνω. Δηλαδή θα πάρουμε από το toolbox των routers την συσκευή c3745. Στο menu → change symbol για επιλογή εικονιδίου (icon) διαλέγουμε το switch.

Η διαδικασία ακολουθεί αυτή του 3rd floor switch.

```
################## Configuration of the 2nd Floor Switch ##################
              ***********************************************
2nd_floor# config t
Enter configuration commands, one per line.  End with CNTL/Z.

2nd_floor(config)# hostname 2nd_floor
2nd_floor(config)# line console 0
2nd_floor(config-line)# password cisco123
2nd_floor(config-line)# login
2nd_floor(config-line)# line vty 0 15
2nd_floor(config-line)# password cisco123
2nd_floor(config-line)# login
2nd_floor(config-line)# transport input ssh
2nd_floor(config-line)# exit
2nd_floor(config)# service password-encryption
2nd_floor(config)# enable secret cisco123
2nd_floor(config)# exit

*Mar  1 00:03:47.335: %SYS-5-CONFIG_I: Configured from console by console


2nd_floor# vlan database

2nd_floor(vlan)# vlan 120
VLAN 120 added:
    Name: VLAN0120
2nd_floor(vlan)# exit
APPLY completed.
Exiting....

2nd_floor# config t
Enter configuration commands, one per line.  End with CNTL/Z.

2nd_floor(config)# interface vlan 120
2nd_floor(config-if)# ip address 172.16.0.104 255.255.255.224
2nd_floor(config-if)# no shutdown
2nd_floor(config-if)# exit

2nd_floor(config)# interface fa 1/0
2nd_floor(config-if)# description CONN WITH CORE A
2nd_floor(config-if)# switchport mode trunk
2nd_floor(config-if)# no shutdown
2nd_floor(config-if)# exit
```

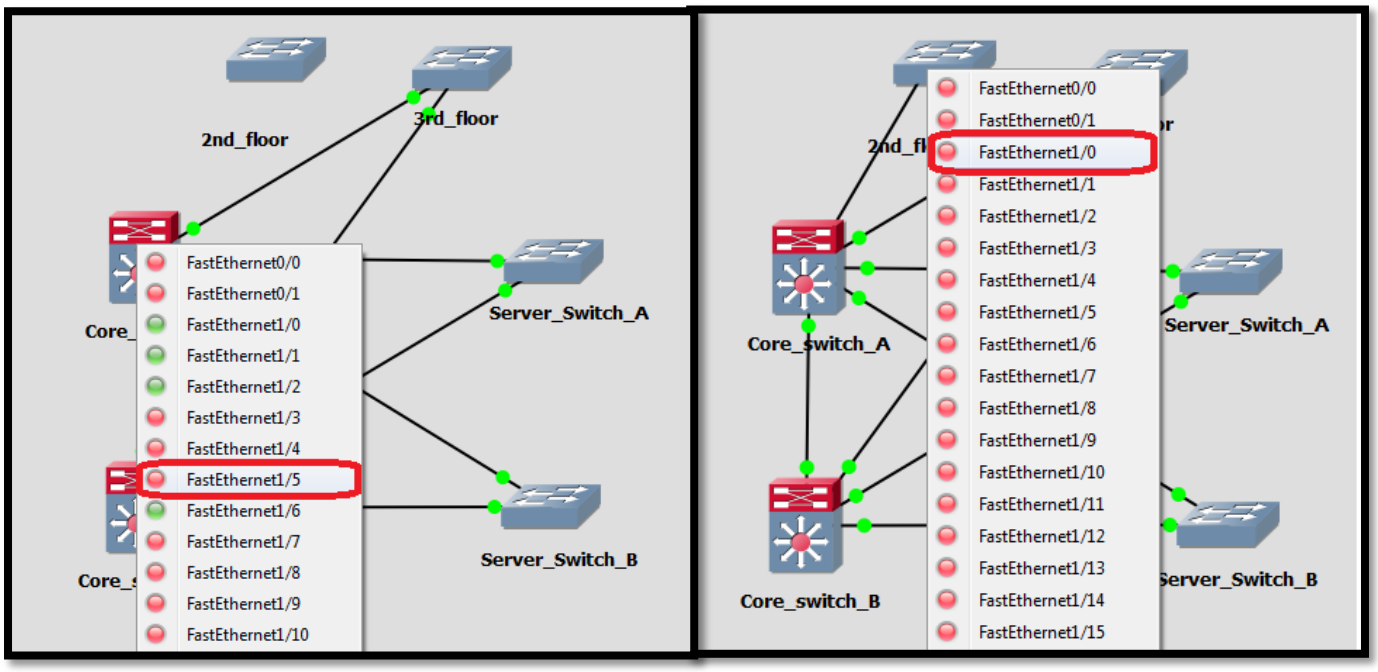
```
2nd_floor(config)# interface fa 1/1
2nd_floor(config-if)# description CONN WITH CORE B
2nd_floor(config-if)# switchport mode trunk
2nd_floor(config-if)# no shutdown
2nd_floor(config-if)# exit
2nd_floor(config)# exit

*Mar  1 00:08:06.343: %SYS-5-CONFIG_I: Configured from console by console

2nd_floor# vlan database
2nd_floor(vlan)# vtp domain techcom.gr
Changing VTP domain name from NULL to techcom.gr

2nd_floor(vlan)# vtp password cisco123
Setting device VLAN database password to cisco123.

2nd_floor(vlan)# vtp v2-mode
V2 mode enabled.

2nd_floor(vlan)# apply
APPLY completed.

2nd_floor(vlan)# vtp client
Setting device to VTP CLIENT mode.

2nd_floor(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....

2nd_floor# write
Building configuration...
[OK]
```

Ρυθμίσεις στο core switch A για την σύνδεση με το 2nd floor switch.

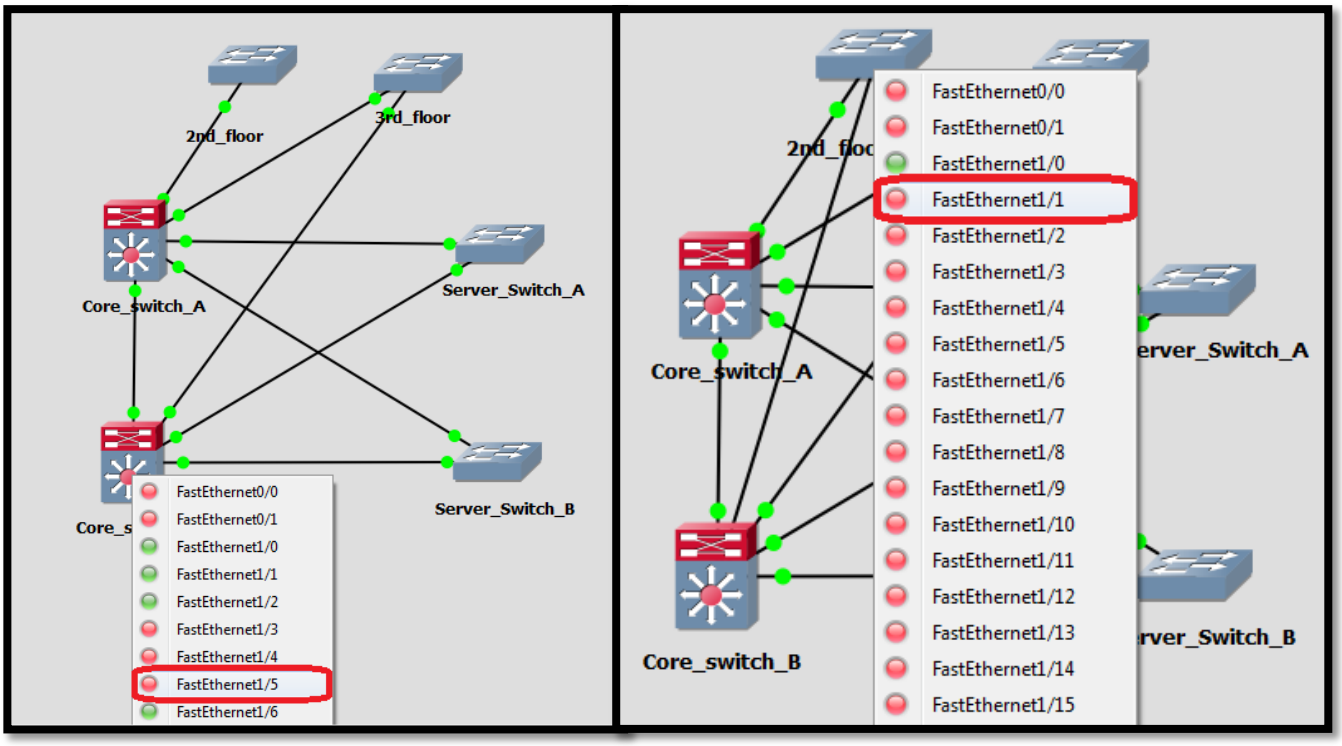
```
core_switch_A# conf t
core_switch_A(config)# interface fastethernet 1/5
core_switch_A(config-if)# description CONN WITH 2nd_FLOOR
core_switch_A(config-if)# switchport mode trunk
core_switch_A(config-if)# no shutdown
core_switch_A(config-if)# exit
core_switch_A(config)# exit
core_switch_A# write
Building configuration...
[OK]
```

Ρυθμίσεις στο core switch B για την σύνδεση με το 2nd floor switch.

```
core_switch_B# conf t
core_switch_B(config)# interface fastethernet 1/5
core_switch_B(config-if)# description CONN WITH 2nd_FLOOR
core_switch_B(config-if)# switchport mode trunk
core_switch_B(config-if)# no shutdown
core_switch_B(config-if)# exit
core_switch_B(config)# exit
core_switch_B# write
Building configuration...
[OK]
```



Εικόνα 5.24: Διασύνδεση μεταξύ του Core switch A και του switch του 2ου ορόφου



Εικόνα 5.25: Διασύνδεση μεταξύ του Core switch B και του switch του 2ου ορόφου

Η διαδικασία ρύθμισης των access ports ακολουθεί αυτή του 3rd floor switch.

```
################## Configure Access Ports 2nd Floor Switch ##################
                ***********************************************

2nd_floor# conf t
2nd_floor(config)# interface range fastethernet 1/2 - 9
2nd_floor(config-if)# switchport mode access
2nd_floor(config-if)# switchport access vlan 150
2nd_floor(config-if)# no shutdown
2nd_floor(config-if)# exit
2nd_floor(config)# interface fastethernet 1/10 - 15
2nd_floor(config-if)# switchport mode access
2nd_floor(config-if)# switchport access vlan 110
2nd_floor(config-if)# no shutdown
2nd_floor(config-if)# exit
2nd_floor(config)# interface range fastethernet 2/0
2nd_floor(config-if)# switchport mode access
2nd_floor(config-if)# switchport access vlan 100
2nd_floor(config-if)# no shutdown
2nd_floor(config-if)# exit
2nd_floor(config)# interface range fastethernet 2/1 - 15
2nd_floor(config-if)# shutdown
2nd_floor(config-if)# exit
2nd_floor(config)# exit
*Mar  1 00:28:37.847: %SYS-5-CONFIG_I: Configured from console by console

2nd_floor# write
Building configuration...
[OK]
```

```
      ################## Test run in 2nd Floor Switch ##################
               ***********************************************

2nd_floor# show run
Building configuration...                    /* Με την εντολή show run μπορούμε να
                                             δούμε τις τρέχουσες ρυθμίσεις του
Current configuration : 2221 bytes           switch και να ελέγχξουμε αν είναι
!                                            σωστές. */
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname 2nd_Floor
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$hN0A$CUbAqBTNK1jyBYIYPbo93/
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
ip tcp synwait-time 5
ip ssh version 1
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
 description CONN WITH CORE A
 switchport mode trunk
```

```
!
interface FastEthernet1/1
 description CONN WITH CORE B
 switchport mode trunk
!
interface FastEthernet1/2
 switchport access vlan 150
!
interface FastEthernet1/3
 switchport access vlan 150
!
interface FastEthernet1/4
 switchport access vlan 150
!
interface FastEthernet1/5
 switchport access vlan 150
!
interface FastEthernet1/6
 switchport access vlan 150
!
interface FastEthernet1/7
 switchport access vlan 150
!
interface FastEthernet1/8
 switchport access vlan 150
!
interface FastEthernet1/9
 switchport access vlan 150
!
interface FastEthernet1/10
 switchport access vlan 110
!
interface FastEthernet1/11
 switchport access vlan 110
!
interface FastEthernet1/12
 switchport access vlan 110
!
interface FastEthernet1/13
 switchport access vlan 110
!
interface FastEthernet1/14
 switchport access vlan 110
!
interface FastEthernet1/15
 switchport access vlan 110
!
interface FastEthernet2/0
 switchport access vlan 100
!
interface FastEthernet2/1
 shutdown
!
interface FastEthernet2/2
 shutdown
!
```

```
/* Παρατηρούμε ότι τα interfaces ανήκου σε διάφορα VLANs και ότι κάποια interfaces είναι shutdown, δηλαδή απενεργοποιημένα. */
```

```
interface FastEthernet2/3
 shutdown
!
interface FastEthernet2/4
 shutdown
!
interface FastEthernet2/5
 shutdown
!
interface FastEthernet2/6
 shutdown
!
interface FastEthernet2/7
 shutdown
!
interface FastEthernet2/8
 shutdown
!
interface FastEthernet2/9
 shutdown
!
interface FastEthernet2/10
 shutdown
!
interface FastEthernet2/11
 shutdown
!
interface FastEthernet2/12
 shutdown
!
interface FastEthernet2/13
 shutdown
!
interface FastEthernet2/14
 shutdown
!
interface FastEthernet2/15
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan120
 ip address 172.16.0.104 255.255.255.224
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
!
```

```
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password 7 030752180500701E1D
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password 7 1511021F07257A767B
 login
 transport input ssh
line vty 5 15
 password 7 1511021F07257A767B
 login
 transport input ssh
!
!
end
```

Σε αυτό το σημείο αφού τελειώσαμε με τον 2ο όροφο θα ξεκινήσουμε την διαδικασία εγκατάστασης access switch στον 1ο όροφο. Για να τοποθετήσουμε τα access switches ακολουθάμε την ίδια ακριβώς διαδικασία με αυτήν που κάναμε παραπάνω. Δηλαδή θα πάρουμε από το toolbox των routers την συσκευή c3745. Στο menu → change symbol για επιλογή εικονιδίου (icon) διαλέγουμε το switch.

Η διαδικασία ακολουθεί αυτή του 3rd floor switch.

```
################## Configuration of the 1st Floor Switch ##################
                ********************************************
1st_floor# config t
Enter configuration commands, one per line.  End with CNTL/Z.

1st_floor(config)# hostname 1st_floor
1st_floor(config)# line console 0
1st_floor(config-line)# password cisco123
1st_floor(config-line)# login
1st_floor(config-line)# line vty 0 15
1st_floor(config-line)# password cisco123
1st_floor(config-line)# login
1st_floor(config-line)# transport input ssh
1st_floor(config-line)# exit
1st_floor(config)# service password-encryption
1st_floor(config)# enable secret cisco123
1st_floor(config)# exit

*Mar  1 00:03:47.335: %SYS-5-CONFIG_I: Configured from console by console


1st_floor# vlan database

1st_floor(vlan)# vlan 120
VLAN 120 added:
    Name: VLAN0120
1st_floor(vlan)# exit
APPLY completed.
Exiting....

1st_floor# config t
Enter configuration commands, one per line.  End with CNTL/Z.

1st_floor(config)# interface vlan 120
1st_floor(config-if)# ip address 172.16.0.104 255.255.255.224
1st_floor(config-if)# no shutdown
1st_floor(config-if)# exit

1st_floor(config)# interface fa 1/0
1st_floor(config-if)# description CONN WITH CORE A
1st_floor(config-if)# switchport mode trunk
1st_floor(config-if)# no shutdown
1st_floor(config-if)# exit
```

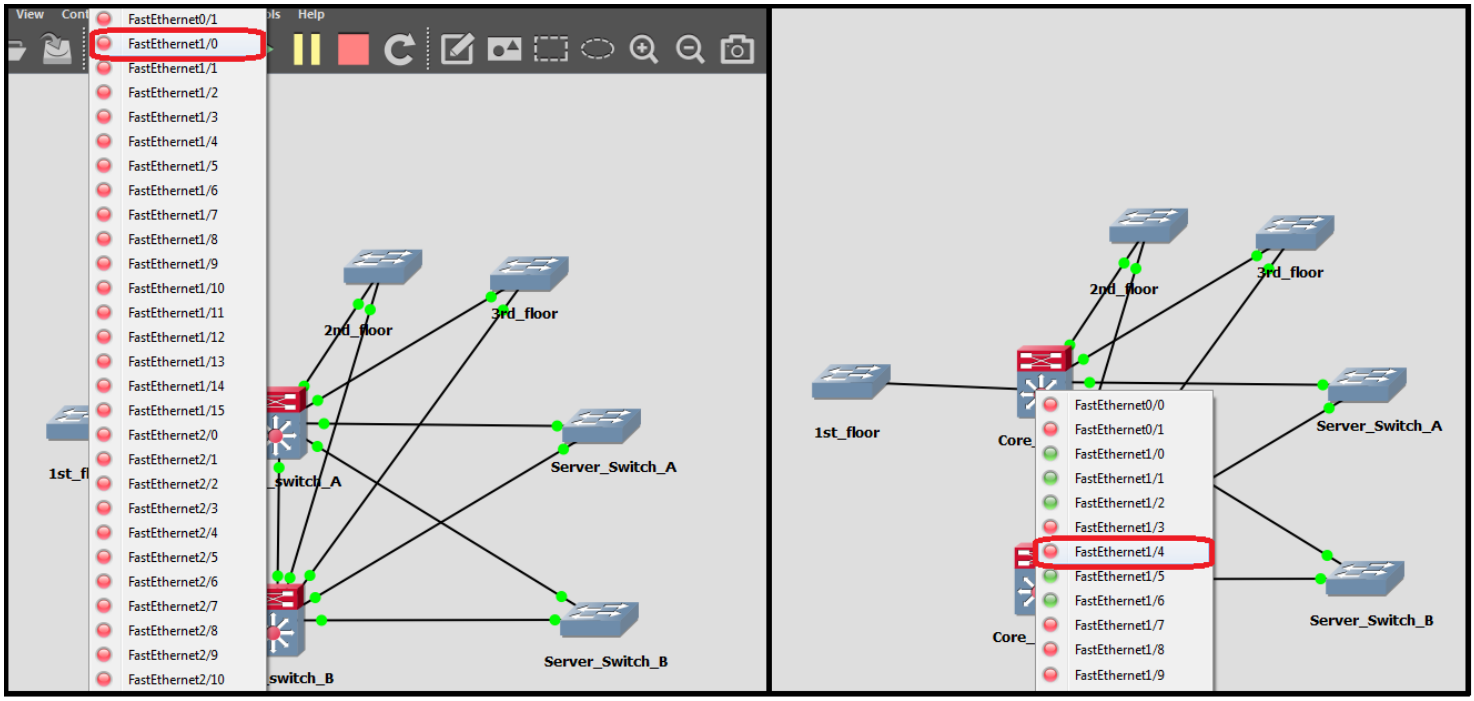
```
1st_floor(config)# interface fa 1/1
1st_floor(config-if)# description CONN WITH CORE B
1st_floor(config-if)# switchport mode trunk
1st_floor(config-if)# no shutdown
1st_floor(config-if)# exit
1st_floor(config)# exit

*Mar  1 00:08:06.343: %SYS-5-CONFIG_I: Configured from console by console

1st_floor# vlan database
1st_floor(vlan)# vtp domain techcom.gr
Changing VTP domain name from NULL to techcom.gr

1st_floor(vlan)# vtp password cisco123
Setting device VLAN database password to cisco123.

1st_floor(vlan)# vtp v2-mode
V2 mode enabled.

1st_floor(vlan)# apply
APPLY completed.

1st_floor(vlan)# vtp client
Setting device to VTP CLIENT mode.

1st_floor(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....

1st_floor# write
Building configuration...
[OK]
```

Ρυθμίσεις στο core switch A για την σύνδεση του 1st floor switch.

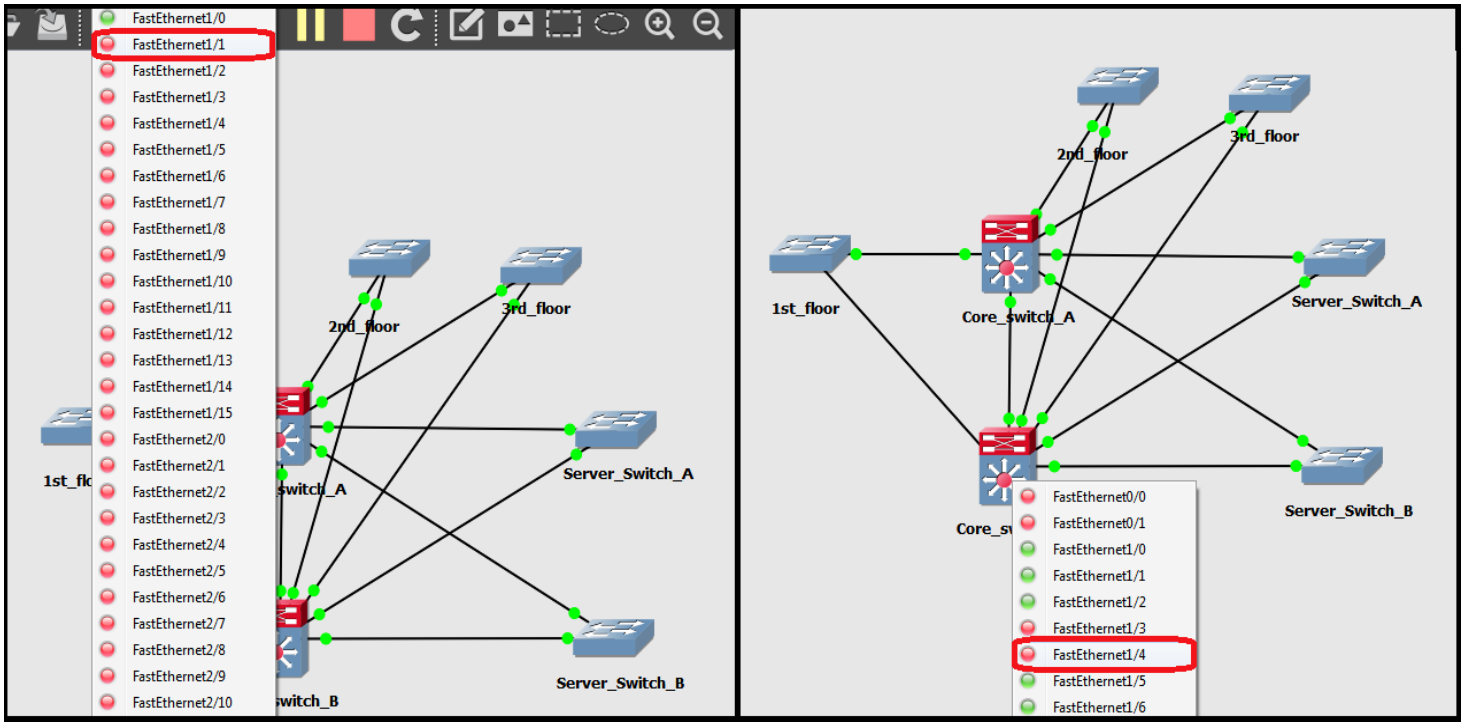
```
core_switch_A# conf t
core_switch_A(config)# interface fastethernet 1/4
core_switch_A(config-if)# description CONN WITH 1std_FLOOR
core_switch_A(config-if)# switchport mode trunk
core_switch_A(config-if)# no shutdown
core_switch_A(config-if)# exit
core_switch_A(config)# exit
core_switch_A# write
Building configuration...
[OK]
```

Ρυθμίσεις στο core switch B για την σύνδεση του 1st floor switch.

```
core_switch_B# conf t
core_switch_B(config)# interface fastethernet 1/4
core_switch_B(config-if)# description CONN WITH 1st_FLOOR
core_switch_B(config-if)# switchport mode trunk
core_switch_B(config-if)# no shutdown
core_switch_B(config-if)# exit
core_switch_B(config)# exit
core_switch_B# write
Building configuration...
[OK]
```



Εικόνα 5.26: Διασύνδεση μεταξύ του Core switch A και του switch του 1ου οροφου



Εικόνα 5.27: Διασύνδεση μεταξύ του Core switch B και του switch του 1ου οροφου

Η διαδικασία ρύθμισης των access ports ακολουθεί αυτή του 3rd floor switch.

```
################## Configure Access Ports 1st Floor Switch ##################
**********************************************

1st_floor# conf t
1st_floor(config)# interface range fastethernet 1/2 - 10
1st_floor(config-if)# switchport mode access
1st_floor(config-if)# switchport access vlan 130
1st_floor(config-if)# no shutdown
1st_floor(config-if)# exit
1st_floor(config)# interface range fastethernet 1/11 - 15
1st_floor(config-if)# switchport mode access
1st_floor(config-if)# switchport access vlan 110
1st_floor(config-if)# no shutdown
1st_floor(config-if)# exit
1st_floor(config)# interface range fastethernet 2/0
1st_floor(config-if)# switchport mode access
1st_floor(config-if)# switchport access vlan 110
1st_floor(config-if)# no shutdown
1st_floor(config-if)# exit

1st_floor(config)# interface fastethernet 2/1
1st_floor(config-if)# switchport mode access
1st_floor(config-if)# switchport access vlan 100
1st_floor(config-if)# no shutdown
1st_floor(config-if)# exit
```

```
1st_floor(config)# interface range fastethernet 2/2 - 15
1st_floor(config-if)# shutdown
1st_floor(config-if)# exit
1st_floor(config)# exit
*Mar  1 00:28:37.847: %SYS-5-CONFIG_I: Configured from console by console

1st_floor# write
Building configuration...
[OK]

       ################## Test run in 1st Floor Switch ##################
              ************************************************

 1st_floor# show run
 Building configuration...                  /* Με την εντολή show run μπορούμε να
                                            δούμε τις τρέχουσες ρυθμίσεις του
 Current configuration : 2221 bytes         switch και να ελέγχξουμε αν είναι
 !                                          σωστές. */
 version 12.4
 service timestamps debug datetime msec
 service timestamps log datetime msec
 service password-encryption
 !
 hostname 1st_Floor
 !
 boot-start-marker
 boot-end-marker
 !
 enable secret 5 $1$qlq6$Tvj6CcSUrFx/KSbu74oTp0
 !
 no aaa new-model
 memory-size iomem 5
 no ip icmp rate-limit unreachable
 ip cef
 !
 !
 !
 no ip domain lookup
 ip auth-proxy max-nodata-conns 3
 ip admission max-nodata-conns 3
 !
 !
 !
 !
 !
 ip tcp synwait-time 5
 ip ssh version 1
 !
 !
 interface FastEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
 !
```

```
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
 description CONN WITH CORE A
 switchport mode trunk
!
interface FastEthernet1/1
 description CONN WITH CORE B
 switchport mode trunk
!
interface FastEthernet1/2
 switchport access vlan 130
!
interface FastEthernet1/3
 switchport access vlan 130
!
interface FastEthernet1/4
 switchport access vlan 130
!
interface FastEthernet1/5
 switchport access vlan 130
!
interface FastEthernet1/6
 switchport access vlan 130
!
interface FastEthernet1/7
 switchport access vlan 130
!
interface FastEthernet1/8
 switchport access vlan 130
!
interface FastEthernet1/9
 switchport access vlan 130
!
interface FastEthernet1/10
 switchport access vlan 130
!
interface FastEthernet1/11
 switchport access vlan 110
!
interface FastEthernet1/12
 switchport access vlan 110
!
interface FastEthernet1/13
 switchport access vlan 110
!
interface FastEthernet1/14
 switchport access vlan 110
!
```

```
/* Παρατηρούμε ότι τα interfaces ανίκουν
σε διάφορα VLANs και ότι κάποια
interfaces είναι shutdown, δηλαδή
απενεργοποιημένα. */
```

```
interface FastEthernet1/15
 switchport access vlan 110
!
interface FastEthernet2/0
 switchport access vlan 110
!
interface FastEthernet2/1
 switchport access vlan 100
!
interface FastEthernet2/2
 shutdown
!
interface FastEthernet2/3
 shutdown
!
interface FastEthernet2/4
 shutdown
!
interface FastEthernet2/5
 shutdown
!
interface FastEthernet2/6
 shutdown
!
interface FastEthernet2/7
 shutdown
!
interface FastEthernet2/8
 shutdown
!
interface FastEthernet2/9
 shutdown
!
interface FastEthernet2/10
 shutdown
!
interface FastEthernet2/11
 shutdown
!
interface FastEthernet2/12
 shutdown
!
interface FastEthernet2/13
 shutdown
!
interface FastEthernet2/14
 shutdown
```

```
!
interface FastEthernet2/15
 shutdown
!
interface Vlan1
 no ip address
!
interface Vlan120
 ip address 172.16.0.103 255.255.255.224
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
!
!
control-plane
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password 7 00071A1507545A545C
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password 7 070C285F4D06485744
 login
 transport input ssh
line vty 5 15
 password 7 070C285F4D06485744
 login
 transport input ssh
!
!
end
```

Σε αυτό το σημείο αφού τελειώσαμε με τον 1ο όροφο θα ξεκινήσουμε την διαδικασία εγκατάστασης access switch στο ισόγειο. Για να τοποθετήσουμε τα access switches ακολουθάμε την ίδια ακριβώς διαδικασία με αυτήν που κάναμε παραπάνω. Δηλαδή θα πάρουμε από το toolbox των routers την συσκευή c3745. Στο menu → change symbol για επιλογή εικονιδίου (icon) διαλέγουμε το switch.

Η διαδικασία ακολουθεί αυτή του 3rd floor switch.

```
################## Configuration of the ground Floor Switch ##################
                ********************************************
Ground_Floor# config t
Enter configuration commands, one per line.  End with CNTL/Z.

Ground_Floor(config)# hostname Ground_Floor
Ground_Floor(config)# line console 0
Ground_Floor(config-line)# password cisco123
Ground_Floor(config-line)# login
Ground_Floor(config-line)# line vty 0 15
Ground_Floor(config-line)# password cisco123
Ground_Floor(config-line)# login
Ground_Floor(config-line)# transport input ssh
Ground_Floor(config-line)# exit
Ground_Floor(config)# service password-encryption
Ground_Floor(config)# enable secret cisco123
Ground_Floor(config)# exit

*Mar  1 00:03:47.335: %SYS-5-CONFIG_I: Configured from console by console


Ground_Floor# vlan database

Ground_Floor(vlan)# vlan 120
VLAN 120 added:
    Name: VLAN0120
Ground_Floor(vlan)# exit
APPLY completed.
Exiting....

Ground_Floor# config t
Enter configuration commands, one per line.  End with CNTL/Z.

Ground_Floor(config)# interface vlan 120
Ground_Floor(config-if)# ip address 172.16.0.102 255.255.255.224
Ground_Floor(config-if)# no shutdown
Ground_Floor(config-if)# exit

Ground_Floor(config)# interface fa 1/0
Ground_Floor(config-if)# description CONN WITH CORE A
Ground_Floor(config-if)# switchport mode trunk
Ground_Floor(config-if)# no shutdown
Ground_Floor(config-if)# exit
```

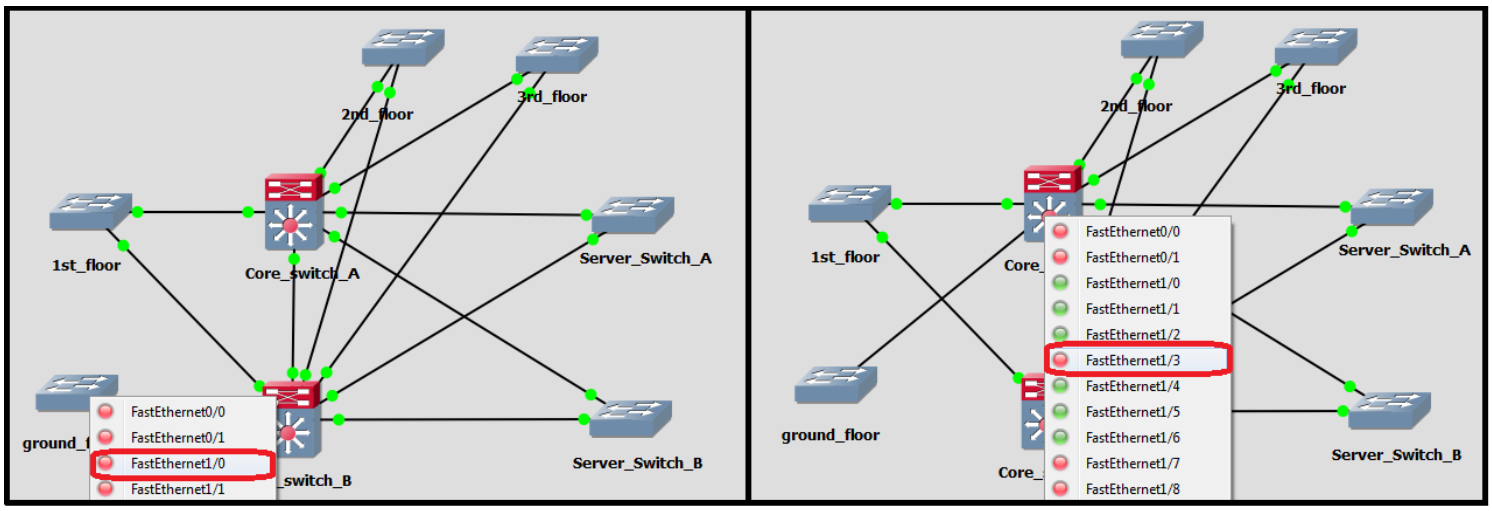
```
Ground_Floor(config)# interface fa 1/1
Ground_Floor(config-if)# description CONN WITH CORE B
Ground_Floor(config-if)# switchport mode trunk
Ground_Floor(config-if)# no shutdown
Ground_Floor(config-if)# exit
Ground_Floor(config)# exit

*Mar  1 00:08:06.343: %SYS-5-CONFIG_I: Configured from console by console

Ground_Floor# vlan database
Ground_Floor(vlan)# vtp domain techcom.gr
Changing VTP domain name from NULL to techcom.gr

Ground_Floor(vlan)# vtp password cisco123
Setting device VLAN database password to cisco123.

Ground_Floor(vlan)# vtp v2-mode
V2 mode enabled.

Ground_Floor(vlan)# apply
APPLY completed.

Ground_Floor(vlan)# vtp client
Setting device to VTP CLIENT mode.

Ground_Floor(vlan)# exit
In CLIENT state, no apply attempted.
Exiting....

Ground_Floor# write
Building configuration...
[OK]
```

Ρυθμίσεις στο core switch A για σύνδεση του Ground Floor Switch.

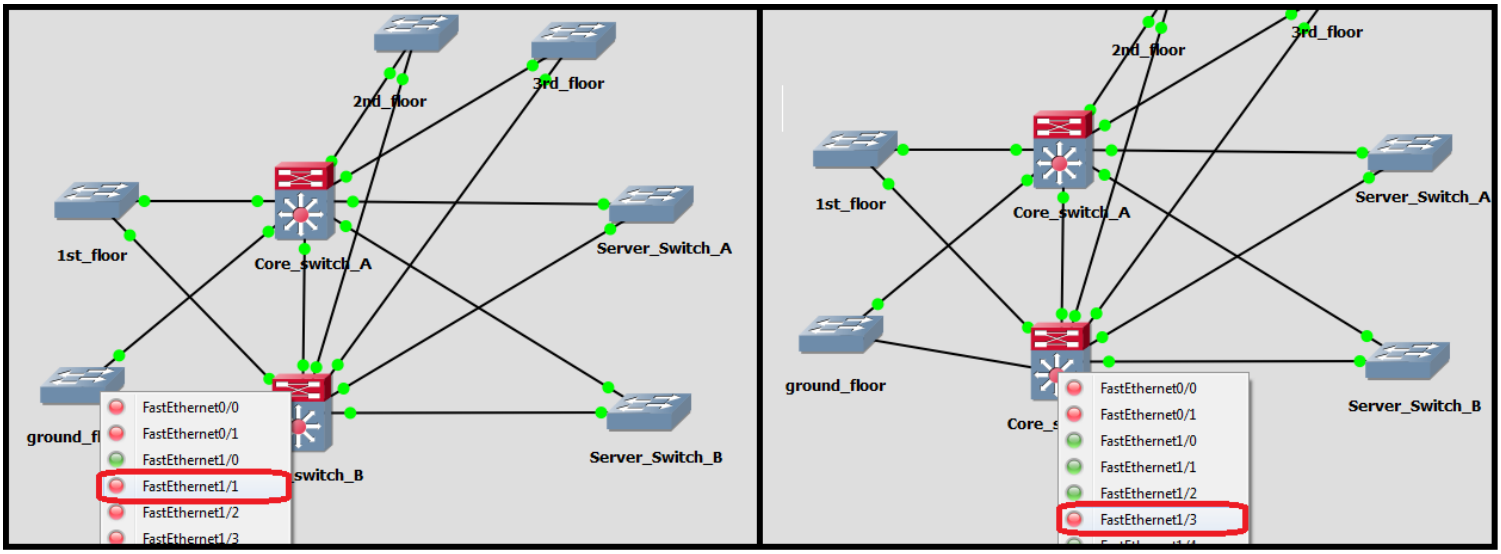
```
core_switch_A# conf t
core_switch_A(config)# interface fastethernet 1/3
core_switch_A(config-if)# description CONN WITH GROUND_FLOOR
core_switch_A(config-if)# switchport mode trunk
core_switch_A(config-if)# no shutdown
core_switch_A(config-if)# exit
core_switch_A(config)# exit
core_switch_A# write
Building configuration...
[OK]
```

Ρυθμίσεις στο core switch B για σύνδεση του Ground Floor Switch.

```
core_switch_B# conf t
core_switch_B(config)# interface fastethernet 1/3
core_switch_B(config-if)# description CONN WITH GROUND_FLOOR
core_switch_B(config-if)# switchport mode trunk
core_switch_B(config-if)# no shutdown
core_switch_B(config-if)# exit
core_switch_B(config)# exit
core_switch_B# write
Building configuration...
[OK]
```



Εικόνα 5.28: Διασύνδεση μεταξύ του Core switch A και του switch του ισογείου



Εικόνα 5.29: Διασύνδεση μεταξύ του Core switch B και του switch του ισογείου

Η διαδικασία ρύθμισης των access ports ακολουθεί αυτή του 3rd floor switch.

```
Ground_Floor# config t
Ground_Floor(config)# interface fastethernet 1/2
Ground_Floor(config-if)# switchport mode access
Ground_Floor(config-if)# switchport access vlan 140
Ground_Floor(config-if)# no shutdown
Ground_Floor(config-if)# exit

Ground_Floor(config)# interface range fastethernet 1/3 - 6
Ground_Floor(config-if)# switchport mode access
Ground_Floor(config-if)# switchport access vlan 170
Ground_Floor(config-if)# no shutdown
Ground_Floor(config-if)# exit

Ground_Floor(config)# interface fastethernet 1/7
Ground_Floor(config-if)# switchport mode access
Ground_Floor(config-if)# switchport access vlan 100
Ground_Floor(config-if)# no shutdown
Ground_Floor(config)# exit

Ground_Floor(config)# interface range fastethernet 1/8 - 15
Ground_Floor(config-if)# shutdown
Ground_Floor(config-if)# exit
```

5.5 Εγκατάσταση και ρύθμιση ASA firewall στο κεντρικό δίκτυο

Σε αυτό το σημείο θα προχωρήσουμε στην εγκατάσταση και στην ρύθμιση του ASA Firewall. Σημειώνεται ότι οι ρυθμίσεις και οι εντολές στην συσκευή αυτή διαφέρουν λίγο από αυτές στα IOS λειτουργικά συστήματα που χρισημοποιήσαμε μέχρι τώρα. Οι εντολές που θα εφαρμοστούν είναι οι παρακάτω.

```
techcom-firewall> enable
Password:
techcom-firewall# conf t
techcom-firewall(config)# hostname techcom-firewall
techcom-firewall(config)# enable password cisco123
/* Οι παρακάτω δύο εντολές υποχρεώνουν τον χρήστη να εισάγει username και password
κατά την εισαγωγή του στο σύστημα μέσω της console port. *\
techcom-firewall(config)# aa authentication serial console LOCAL
techcom-firewall(config)# username firewall_1 password cisco123

/*Παρακάτω ρυθμίζονται οι 3 θύρες του firewall, δύο που συνδαίονται στους core
switches και μία που συνδέετε στο internet.  Στο firewall είναι απαραίτητο να της
ονομάσουμε με την εντολή nameif όπως κάναμε παρακάτω.  *\

techcom-firewall(config)# interface gigabitethernet 0
techcom-firewall(config-if)# ip address 172.16.0.202 255.255.255.248
techcom-firewall(config-if)# nameif inside-core-a
techcom-firewall(config-if)# no shutdown
techcom-firewall(config-if)# exit

techcom-firewall(config)# interface gigabitethernet 1
techcom-firewall(config-if)# ip address 172.16.0.210 255.255.255.248
techcom-firewall(config-if)# nameif inside-core-b
techcom-firewall(config-if)# no shutdown
techcom-firewall(config-if)# exit

techcom-firewall(config)# interface gigabitethernet 2
techcom-firewall(config-if)# nameif outside
techcom-firewall(config-if)# ip address 200.200.200.1 255.255.255.0
techcom-firewall(config-if)# no shutdown
techcom-firewall(config-if)# exit

/* Με τις παρακάτω εντολές δημιουργούμε ένα κλειδί χρισημοποιόντας το RSA Public
Key Cryptosystem.  Αυτό το κλειδί χρισημοποιήται με την σειρά του για την σύνδεση
στο command line του firewall μέσω ssh. *\

techcom-firewall(config)# crypto key generate rsa modulus 1024
techcom-firewall(config)# ssh 172.16.192.0 255.255.255.248 inside-core-a
techcom-firewall(config)# ssh 172.16.192.0 255.255.255.248 inside-core-b
techcom-firewall(config)# ssh timeout 30
techcom-firewall(config)# aaa authentication ssh console LOCAL
```

```
/* Παρακάτω ρυθμίζεται η δρομοπλόγηση του firewall.  Πρώτα βάζουμε ένα default
route έτσι ώστε όλοι οι προορισμοί εκτός του δικτύου να δρομολογούνται από την
outside θύρα προς την IP του ADSL VPN router. *\

techcom-firewall(config)# route outside 0.0.0.0 0.0.0.0 172.16.0.217

/* Σε αυτό το σημείο, ρυθμίζουμε το routing προτόκολλο OSPF. Με τις εντολές αυτές
ορίζουμε ποια από τα directly connected networks θα συμμετέχουν στο OSPF.
Συγκεκρημένα, επιλέγουμε τα υποδίκτυα που συνδέουν τους δύο Core Switches. *\

techcom-firewall(config)# router ospf 1
techcom-firewall(config-ospf)# network 172.16.0.200 255.255.255.248 area 0
techcom-firewall(config ospf)# network 172.16.0.208 255.255.255.248 area 0
techcom-firewall(config ospf)# exit


/* Οι παρακάτω εντολές access list απαγορεύουν οποιαδύποτε επικοινωνία από
«έξω προς τα μέσα» εκτός από αυτή που έρχεται από το branch υποδίκτυο
(172.16.1.0/24)  Έτσι προστατεύεται το εσωτερκό υποδίκτυο των κεντρικών
γραφείων και επιτρέπονται μόνο συνδέσεις από το branch υποδίκτυο. *\

techcom-firewall(config)# access-list outside_access_in extended permit ip
172.16.1.0 0.0.0.255 any
techcom-firewall(config)# access-group outside_access_in in interface outside
techcom-firewall(config)# exit
techcom-firewall# write
Building configuration...
[OK]
```

Ρυθμίσεις στο core switch A, την σύνδεσή του με το ASA Firewall και τις ρυθμίσεις του routing προτοκόλλου OSPF.

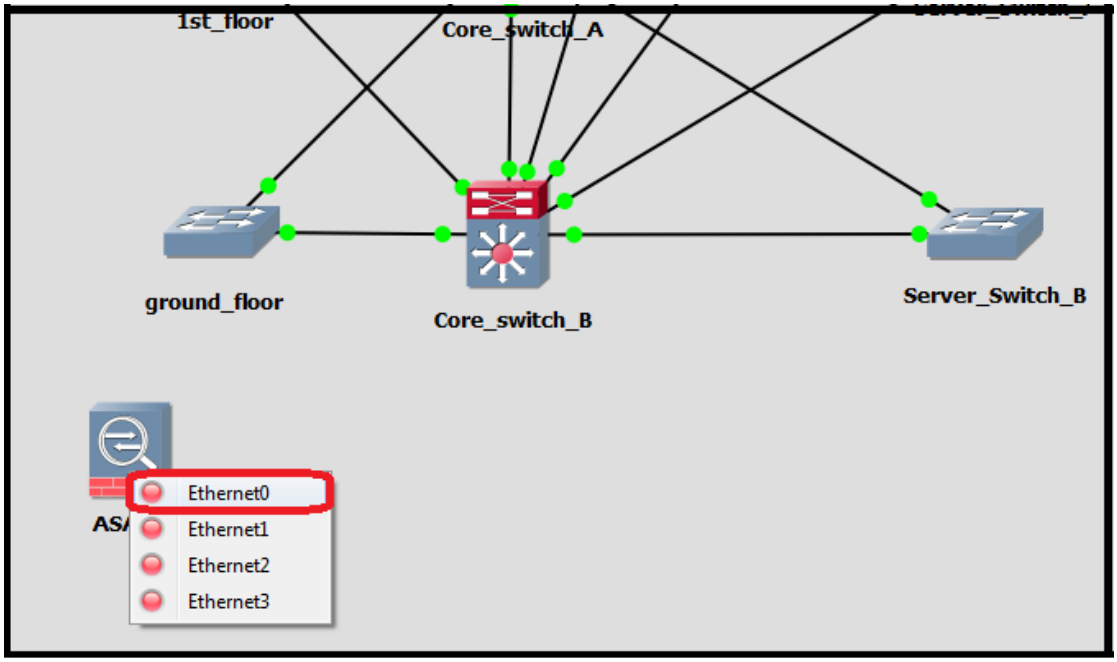
```
core_switch_A# conf t
Enter configuration commands, one per line.  End with CNTL/Z.

core_switch_A(config)# interface fastEthernet 0/0
core_switch_A(config-if)# description CONN WITH ASA_1
core_switch_A(config-if)# ip address 172.16.0.201 255.255.255.248
core_switch_A(config-if)# no shutdown

*Mar  1 00:59:39.531: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state
to up
*Mar  1 00:59:40.531: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up

core_switch_A(config-if)# exit
```

```
/* Παρακάτω ρυθμίζεται η δρομοπλόγηση του Core Switch A.  Πρώτα βάζουμε ένα
default route έτσι ώστε όλοι οι προορισμοί εκτός του δικτύου να δρομολογούνται
προς το ASA Firewall που έχει IP διεύθυνση 172.16.0.202. *\

core_switch_A(config)# ip route 0.0.0.0 0.0.0.0 172.16.0.202

/* Σε αυτό το σημείο, ρυθμίζουμε το routing προτόκολλο OSPF. Με τις εντολές αυτές
ορίζουμε ποια από τα directly connected networks θα συμμετέχουν στο OSPF.  Εδώ
ορίζουμε όλα τα directly connected networks να συμμετέχουν ή να γίνονται
advertised στο OSPF.  *\

core_switch_A(config)# router ospf 1
core_switch_A(config-router)# network 172.16.0.0 255.255.255.192 area 0
core_switch_A(config-router)# network 172.16.0.64 255.255.255.224 area 0
core_switch_A(config-router)# network 172.16.0.96 255.255.255.224 area 0
core_switch_A(config-router)# network 172.16.0.128 255.255.255.240 area 0
core_switch_A(config-router)# network 172.16.0.144 255.255.255.240 area 0
core_switch_A(config-router)# network 172.16.0.160 255.255.255.240 area 0
core_switch_A(config-router)# network172.16.0.176 255.255.255.240 area 0
core_switch_A(config-router)# network172.16.0.192 255.255.255.248 area 0
core_switch_A(config-router)# network172.16.0.200 255.255.255.248 area 0

/* Από αυτά τα interfaces δεν θέλουμε να στέλνονται OSPF advertisements αφού δεν
υπάρχουν OSPF Routers συνδεδεμένα σε αυτά τα VLAN.  Έτσι τα ορίζουμε ως passive.*\
core_switch_A(config-router)# passive-interface vlan 100
core_switch_A(config-router)# passive-interface vlan 110
core_switch_A(config-router)# passive-interface vlan 120
core_switch_A(config-router)# passive-interface vlan 130
core_switch_A(config-router)# passive-interface vlan 140
core_switch_A(config-router)# passive-interface vlan 150
core_switch_A(config-router)# passive-interface vlan 160
core_switch_A(config-router)# passive-interface vlan 170
Core_switch_A(config-router)# exit
Core_switch_A(config)# exit

core_switch_A# write
Building configuration...
[OK]
```

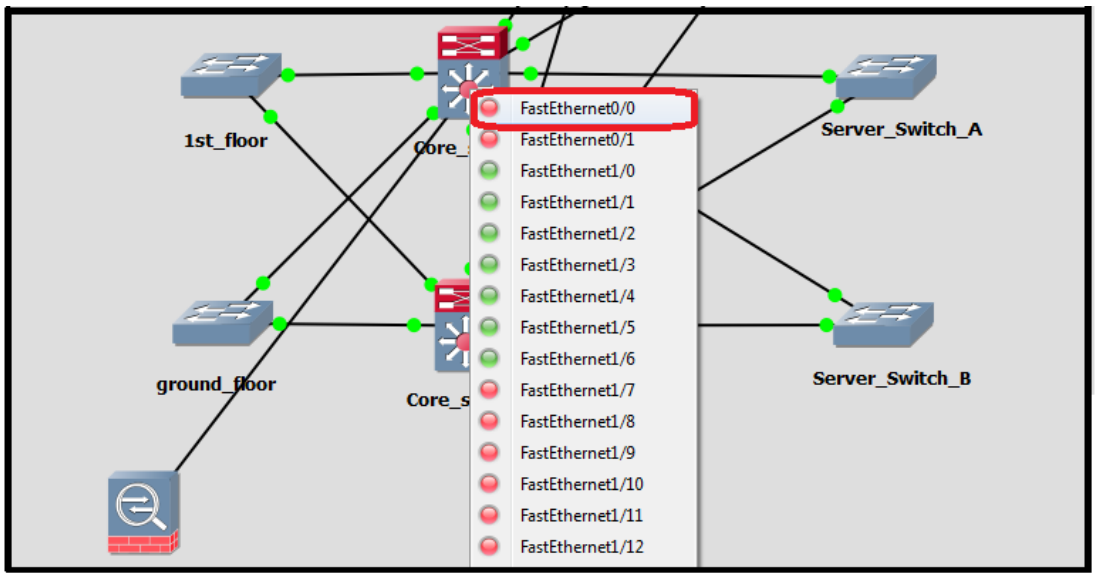
Με παρόμοιο τρόπο ρυθμίζουμε το core switch B, την σύνδεσή του με το ASA Firewall και τις ρυθμίσεις του routing προτοκόλλου OSPF.

```
Core_switch_B# conf t
Enter configuration commands, one per line.  End with CNTL/Z.

Core_switch_B(config)# interface fastEthernet 0/0
Core_switch_B(config-if)# description CONN WITH ASA_1
Core_switch_B(config-if)# ip address 172.16.0.209 255.255.255.248
Core_switch_B(config-if)# no shut
Core_switch_B(config-if)# exit
```

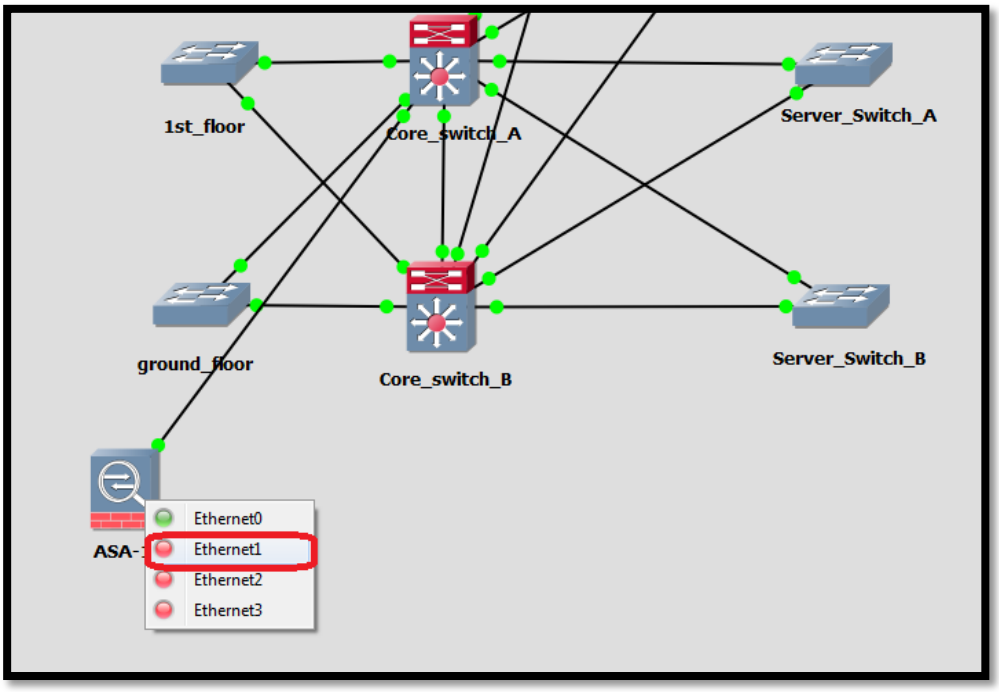
```
/* Παρακάτω ρυθμίζεται η δρομοπλόγηση του Core Switch A.  Πρώτα βάζουμε ένα
default route έτσι ώστε όλοι οι προορισμοί εκτός του δικτύου να δρομολογούνται
προς το ASA Firewall που έχει IP διεύθυνση 172.16.0.210. *\

Core_switch_B(config)# ip route 0.0.0.0 0.0.0.0 172.16.0.210

*Mar  1 01:01:03.631: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state
to up
*Mar  1 01:01:04.631: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up

/* Σε αυτό το σημείο, ρυθμίζουμε το routing προτόκολλο OSPF. Με τις εντολές αυτές
ορίζουμε ποια από τα directly connected networks θα συμμετέχουν στο OSPF.  Εδώ
ορίζουμε όλα τα directly connected networks να συμμετέχουν ή να γίνονται
advertised στο OSPF.  *\

core_switch_B(config)# router ospf 1
core_switch_B(config-router)# network 172.16.0.0 255.255.255.192 area 0
core_switch_B(config-router)# network 172.16.0.64 255.255.255.224 area 0
core_switch_B(config-router)# network 172.16.0.96 255.255.255.224 area 0
core_switch_B(config-router)# network 172.16.0.128 255.255.255.240 area 0
core_switch_B(config-router)# network 172.16.0.144 255.255.255.240 area 0
core_switch_B(config-router)# network 172.16.0.160 255.255.255.240 area 0
core_switch_B(config-router)# network 172.16.0.176 255.255.255.240 area 0
core_switch_B(config-router)# network 172.16.0.192 255.255.255.248 area 0
core_switch_B(config-router)# network 172.16.0.208 255.255.255.248 area 0

/* Από αυτά τα interfaces δεν θέλουμε να στέλνονται OSPF advertisements αφού δεν
υπάρχουν OSPF Routers συνδεδεμένα σε αυτά τα VLAN.  Έτσι τα ορίζουμε ως passive.*\

core_switch_B(config-router)# passive-interface vlan 100
core_switch_B(config-router)# passive-interface vlan 110
core_switch_B(config-router)# passive-interface vlan 120
core_switch_B(config-router)# passive-interface vlan 130
core_switch_B(config-router)# passive-interface vlan 140
core_switch_B(config-router)# passive-interface vlan 150
core_switch_B(config-router)# passive-interface vlan 160
core_switch_B(config-router)# passive-interface vlan 170
Core_switch_B(config-router)# exit
Core_switch_B(config)# exit

core_switch_B# write
Building configuration...
[OK]
```



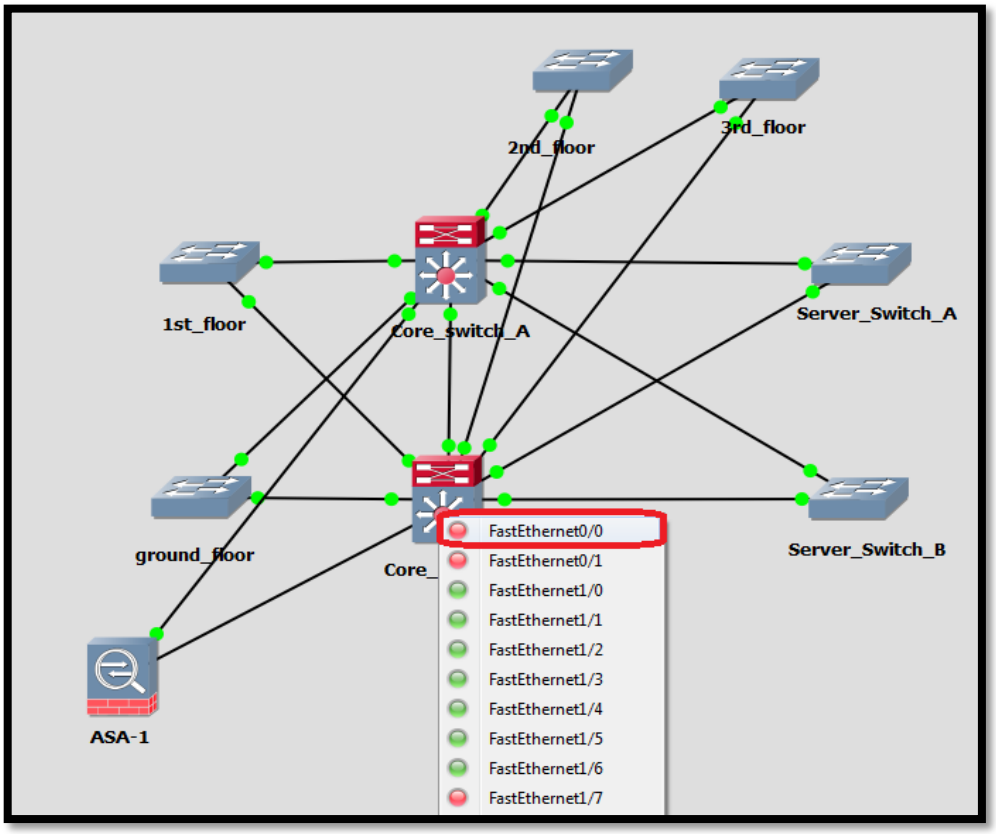
Εικόνα 5.30: Διασύνδεση μεταξύ του Core switch A με το ASA firewall του δικτύου



Εικόνα 5.31: Διασύνδεση μεταξύ του Core switch A με το ASA firewall του δικτύου



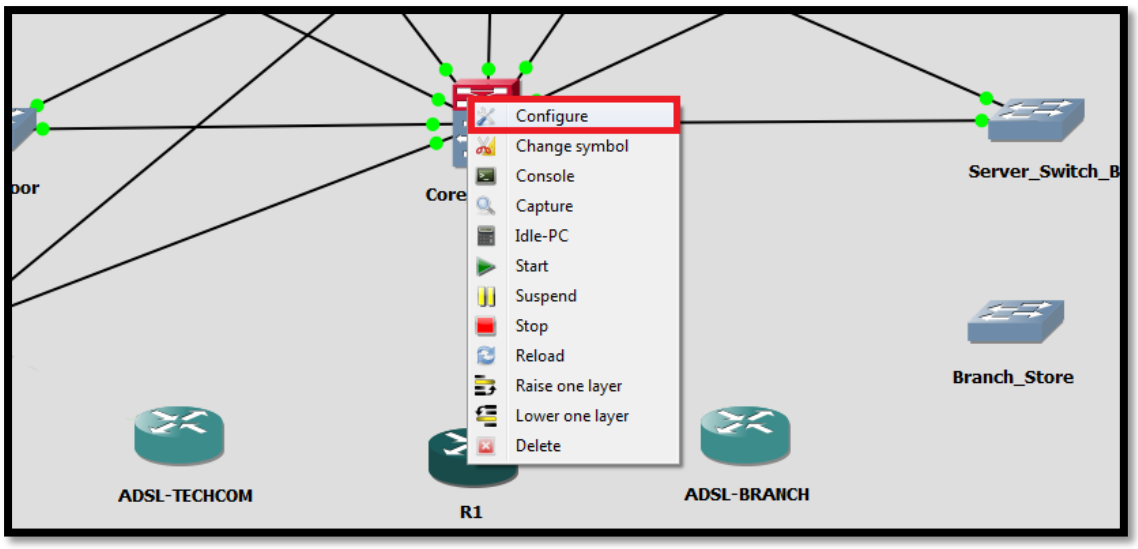
Εικόνα 5.32: Διασύνδεση μεταξύ του Core switch B με το ASA firewall του δικτύου



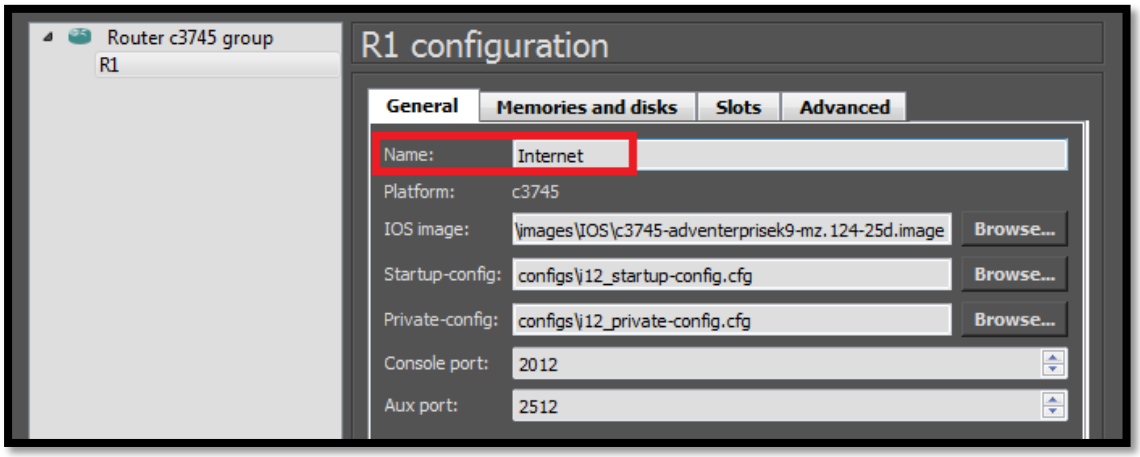
Εικόνα 5.33: Διασύνδεση μεταξύ του Core switch B με το ASA firewall του δικτύου

5.6 Εγκατάσταση VPN Routers

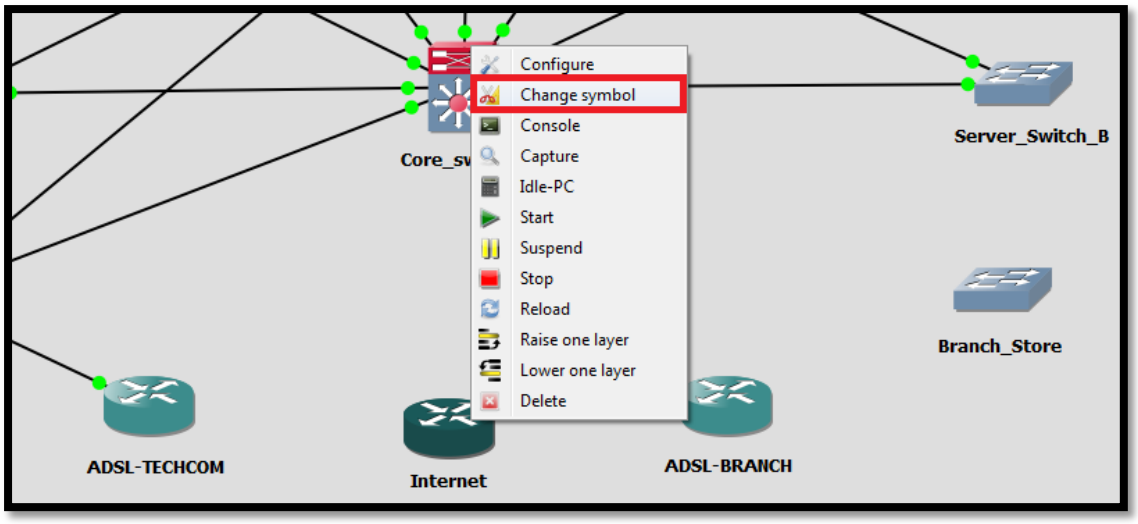
Σε αυτό το σημείο θα προχωρήσουμε στην εγκατάσταση των VPN δρομολογητών, θα τοποθετηθεί ένα στα κεντρικά γραφεία της εταιρίας και ένα στο υποκατάστημα της. Στο υποκατάστημα αυτό θα υπάρχει και ένα switch που θα διασυνδέει τους hosts του υποδικτύου. Για να προσομοιώσουμε στην VPN σύνδεση, δημιουργούμε ένα cloud το οποίο θα αντιπροσωπεύει το διαδίκτυο (Internet). Για το δικό μας δίκτυο αυτό το cloud δεν θα είναι τίποτα παραπάνω από ένας απλός cisco router 3745. Ο λόγος αυτός οφείλεται διότι επικεντρωνόμαστε κυρίως στο δίκτυο της εταιρίας, στην VPN λειτουργία και όχι τόσο στην λειτουργία του διαδικτύου το οποίο είναι κάτι ευρύτερο και δεν μας απασχολεί.
Κάνουμε δεξί κλίκ πάνω στον router R1 και αλλάζουμε το όνομα του σε Internet και αλάζουμε το εικονίδιο του σε cloud.



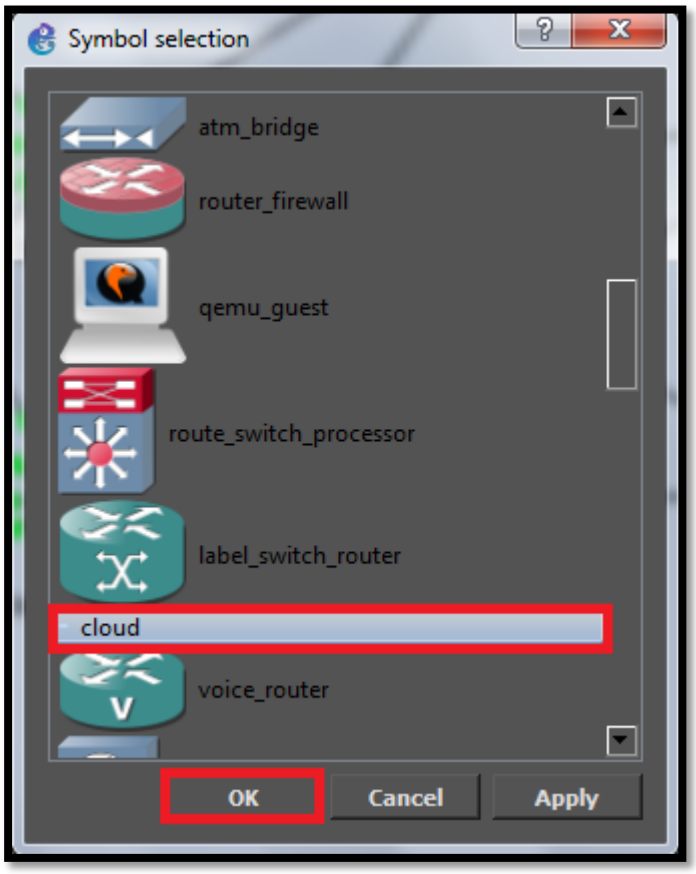
Εικόνα 5.34: Διαδικασία μεταονομασίας του router R1 σε Internet



Εικόνα 5.35: Διαδικασία μεταονομασίας του router R1 σε Internet



Εικόνα 5.36: Διαδικασία αλλαγής συμβόλου



Εικόνα 5.37: Επιλογή συμβόλου

Στην συνέχεια θα εφαρμόσουμε τις παρακάτω ρυθμίσεις στο R1 που ονομάσαμε ως Internet. Κάθε θύρα ρυθμίζεται σε διαφορετικό υποδίκτυο όπως θα γινόταν και στο πραγματικό Internet. Γίνεται αυτόματα δρομολόγηση μεταξύ των δύο υποδικτύων.

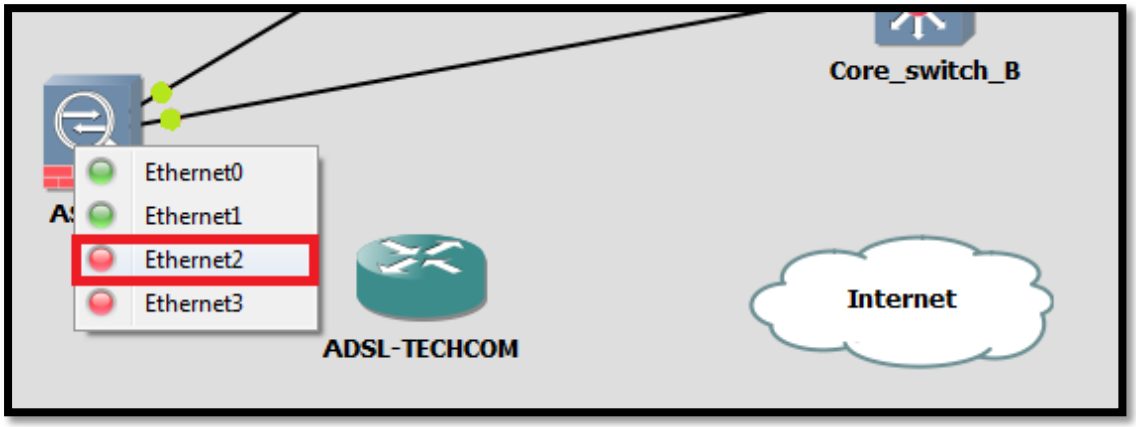
```
R1> enable
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.

R1(config)# hostname internet
internet(config)# interface fastethernet 0/0
internet(config-if)# ip address 200.200.200.2 255.255.255.0
internet(config-if)# no shut
internet(config-if)# exit

internet(config)# interface fastethernet 0/1
internet(config-if)# ip address 200.200.201.2 255.255.255.0
internet(config-if)# no shut
internet(config-if)# exit
internet(config)# exit
internet# write
Building configuration...
[OK]
```

Στην συνέχεια θα τοποθετήσουμε τον VPN δρομολογητή στα κεντρικά γραφεία. Θα το ονομάσουμε ως ADSL TECHCOM. Οι ρυθμίσεις βρίσκονται παρακάτω:

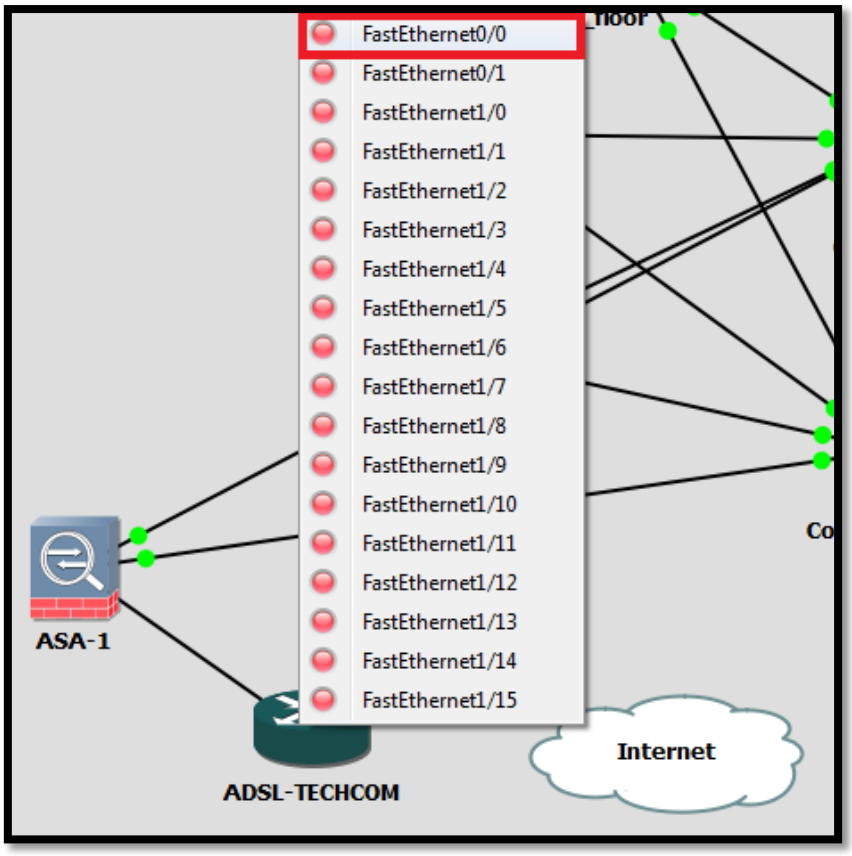
```
R1> enable
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.

/* παρακάτω ρυθμίζουμε hostname και τις ρυθμίσεις πρόσβασης στην συσκευή όπως
κάναμε σε όλα τα ενεργά στοιχεία μέχρι τώρα. */

R1(config)# hostname adsl-techcom
adsl-techcom(config)# line console 0
adsl-techcom(config-line)# password cisco123
adsl-techcom(config-line)# login
adsl-techcom(config-line)# line vty 0 15
adsl-techcom(config-line)# password cisco123
adsl-techcom(config-line)# login
adsl-techcom(config-line)# transport input ssh
adsl-techcom(config-line)# exit
adsl-techcom(config)# service password-encryption
adsl-techcom(config)# enable secret cisco123
adsl-techcom(config)# exit

/* Παρακάτω ρυθμίζεται η θύρα η οποία συνδέετε στο firewall.  Χρισιμοποιήται η
κατάλληλη IP δυεύθυνση του συγκεκρημένου υποδικτύου. */
adsl-techcom(config)# interface fastethernet 0/0
adsl-techcom(config-if)# ip address 172.16.0.217 255.255.255.248
adsl-techcom(config-if)# no shut
adsl-techcom(config-if)# exit
```

```
/* Παρακάτω ρυθμίζεται η θύρα η οποία συνδέετε στο Internet.  Αυτή έχει
routable IP διεύθυνση όπως θα είχε στο πραγματικό Internet.  Μέσω αυτής της
θύρας θα λειτουργείσει το VPN. */

adsl-techcom(config)# interface fastethernet 0/1
adsl-techcom(config-if)# ip address 200.200.200.1 255.255.255.0
adsl-techcom(config-if)# no shut
adsl-techcom(config-if)# exit

/* Παρακάτω ρυθμίζεται το routing με στατικό τρόπο.  Δρομολογούνται κατάλληλα
τα υποδίκτυα σύμφωνα με τις εντολές αυτές. */

adsl-techcom(config)# ip route 0.0.0.0 0.0.0.0 200.200.200.2
adsl-techcom(config)# ip route 172.16.0.0 255.255.255.128 172.16.1.218
adsl-techcom(config)# ip route 172.16.0.128 255.255.255.192 172.16.1.218
adsl-techcom(config)# ip route 172.16.0.192 255.255.255.240 172.16.1.218
adsl-techcom(config)# ip route 172.16.0.208 255.255.255.248 172.16.1.218

/* Παρακάτω ρυθμίζεται το IP Security Key Exchange (IKE) το οποίο λειτουργεί
στα πλαίσια των εντολών isakmp.  Στην 1η φάση, ρυθμίζουμε το setup μεταξύ των
δύο routers.  Εδώ «συμφωνούν» τα δύο VPN routers για τον τρόπο ανταλλαγής
πληροφοριών με ασφάλεια.  Οι ρυθμίσεις αυτές θα πρέπει να είναι ίδιες και στις
δύο άκρες του VPN. */

adsl-techcom(config)# crypto isakmp enable /*Ενεργοποιούμε το isakmp*/
adsl-techcom(config)# crypto isakmp policy 10 /* Ορίζουμε μία πολιτική*/

/*ορίζουμε τον τρόπο πιστοποίησης ως pre shared key*/
adsl-techcom(config-isakmp)# authentication pre-share

/* επιλέγουμε το md5 ως αλγόριθο hash */
adsl-techcom(config-isakmp)# hash md5

/* επιλέγουμε το Data Encryption Standard (DES) ως αλγόρυθμο κρυπτογράφησης */
adsl-techcom(config-isakmp)# encryption des

/*εδώ ορίζεται το Diffie-Hellman group identifier, το οποίο επιτρέπει στις δύο
άκρες να δημιουργήσουν ένα κοινό κωδικό χωρίς την μετάδωσή του */
adsl-techcom(config-isakmp)# group 2

/* ορίζουμε τον χρόνο σε δευτερόλεπτα που θα ισχύει η σύνδεση πριν
ξαναεξεταστούν τα στοιχεία ασφάλειας */
adsl-techcom(config-isakmp)# lifetime 3600
adsl-techcom(config-isakmp)# exit

/* Παρακάτω ορίζουμε τον απομακρυσμένο router στον οποίο θα συνδεθεί και με
πιο τρόπο θα γίνει η επαλυθευση της ασφάλειας (key security) */
adsl-techcom(config)# crypto isakmp key security address 200.200.201.1
255.255.255.0

/* Παρακάτω ορίζουμε το σύνολο των αλγόρυθμων και προτοκόλλων που θα
αξιοποιηθούν για την δημιουργία ενός IPSec tunnel. */
adsl-techcom(config)# crypto ipsec transform-set hoset esp-des esp-md5-hmac
```

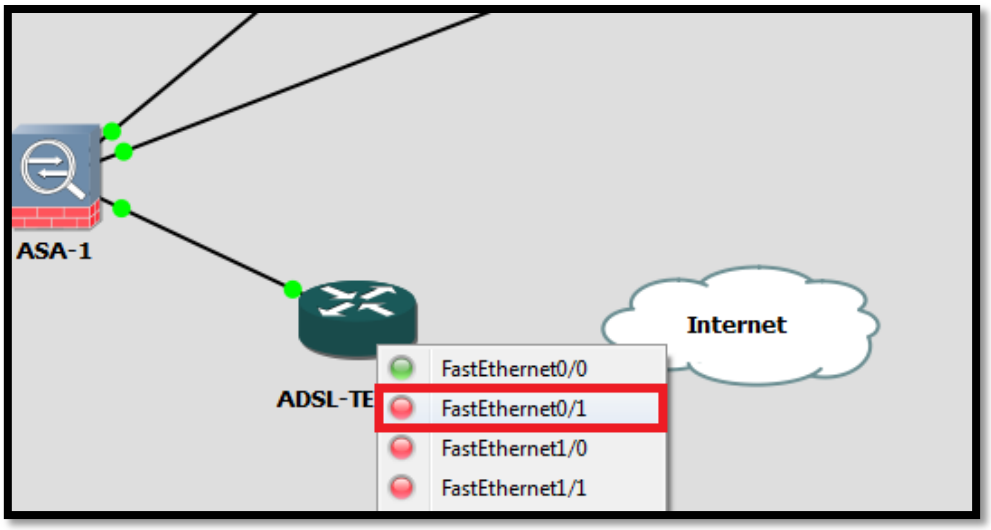
```
/* Μέσω της παρακάτω access list, ορίζουμε ποια τοπικά υποδίκτυα επιτρέπεται
να επικοινωνούν με ποια απομαρκσυμένα δίκυα. */
adsl-techcom(config)# access-list 101 permit ip 172.16.0.0 0.0.0.255
172.16.1.0 0.0.0.255

/* Εδώ ρυθμίζεται το σύνολο των ρυθμίσεων που θα πρέπει να εφαρμοστούν στο VPN
tunnel. Ορίζουμε τον απομαρισμένο router, εφαρμόζουμε το transform set που
ορίσαμε παραπάνω και εφαρμόζουμε και την access list που ορίσαμε παραπάνω.
Όλα αυτά τα βάλαμε στο crypto map με όνομα homap.*/
adsl-techcom(config)# crypto map homap 10 ipsec-isakmp
adsl-techcom(config-crypto-map)# set peer 200.200.201.1
adsl-techcom(config-crypto-map)# set transform-set hoset
adsl-techcom(config-crypto-map)# match address 101
adsl-techcom(config-crypto-map)# exit

/* Το crypto map με όνομα homap ερφαρμόζεται στο interface που συνδέετε στο
Internet.*/
adsl-techcom(config)# interface fastethernet 0/1
adsl-techcom(config-if)# crypto map homap
adsl-techcom(config-if)# exit
adsl-techcom(config)# exit
adsl-techcom# write
Building configuration...
[OK]
```



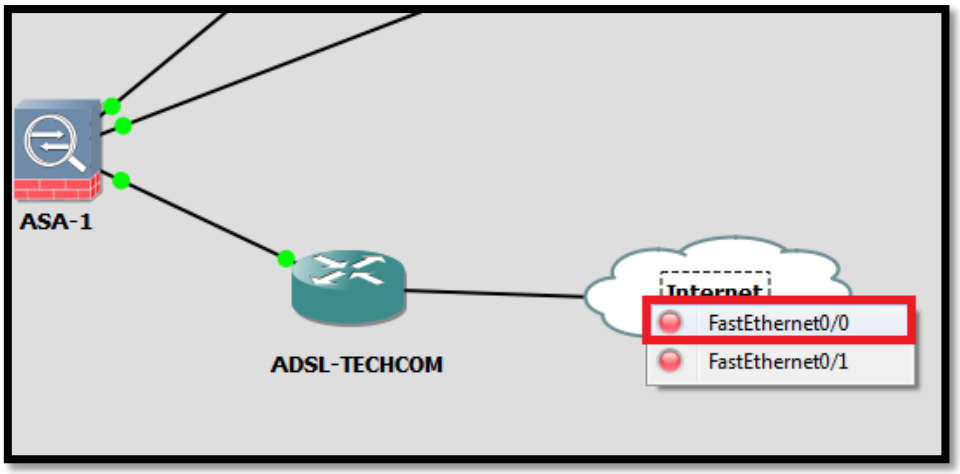
Εικόνα 5.38: Διασύνδεση μεταξύ του ASA Firewall και του ADSL-TECHCOM



Εικόνα 5.39: Διασύνδεση μεταξύ του ASA Firewall και του ADSL-TECHCOM



Εικόνα 5.40: Διασύνδεση μεταξύ του ADSL-TECHCOM και του Internet



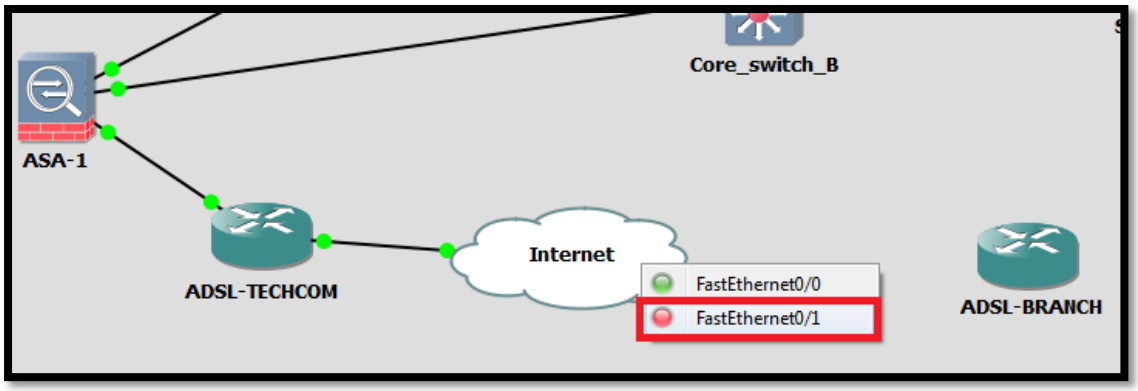
Εικόνα 5.41: Διασύνδεση μεταξύ του ADSL-TECHCOM και του Internet

Σε αυτό το σημείο θα ξεκινήσουμε με τις ρυθμίσεις του ADSL Router του υποκαταστήματος. Παρακάτω είναι οι ρυθμίσεις του VPN δρομολογητή που βρίσκεται στο υποκατάστημα.

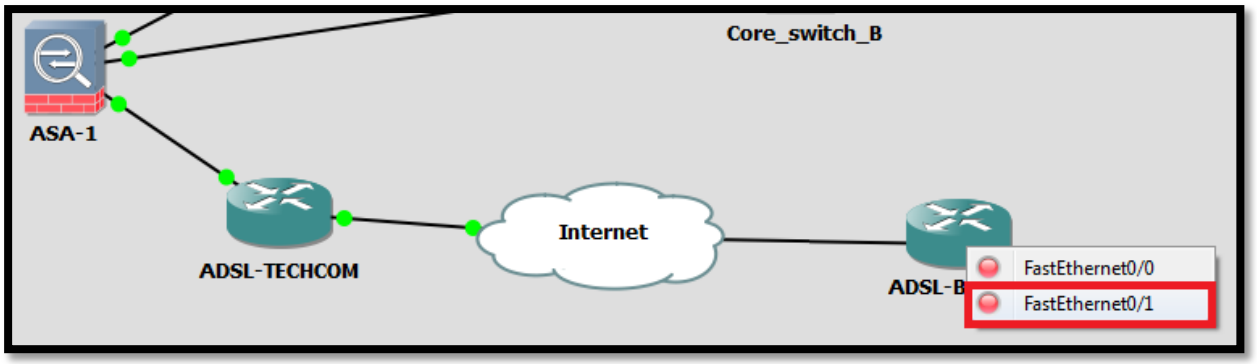
```
 R1> enable
 R1# conf t
 Enter configuration commands, one per line.  End with CNTL/Z.

/* παρακάτω ρυθμίζουμε hostname και τις ρυθμίσεις πρόσβασης στην συσκευή όπως
κάναμε σε όλα τα ενεργά στοιχεία μέχρι τώρα. */
 R1(config)# hostname adsl-branch
 adsl-branch(config)# line console 0
 adsl-branch(config-line)# password cisco123
 adsl-branch(config-line)# login
 adsl-branch(config-line)# line vty 0 15
 adsl-branch(config-line)# password cisco123
 adsl-branch(config-line)# login
 adsl-branch(config-line)# transport input ssh
 adsl-branch(config-line)# exit
 adsl-branch(config)# service password-encryption
 adsl-branch(config)# enable secret cisco123
 adsl-branch(config)# exit

 /* Παρακάτω ρυθμίζεται η θύρα η οποία συνδέετε στο branch switch.
 Χρισιμοποιήται η κατάλληλη IP δυεύθυνση του συγκεκρημένου υποδικτύου. */
 adsl-branch(config)# interface fastethernet 0/0
 adsl-branch(config-if)# ip address 172.16.1.1 255.255.255.240
 adsl-branch(config-if)# no shut
 adsl-branch(config-if)# exit
```

```
/* Παρακάτω ρυθμίζεται η θύρα η οποία συνδέετε στο Internet.  Αυτή έχει
routable IP διεύθυνση όπως θα είχε στο πραγματικό Internet.  Μέσω αυτής της
θύρας θα λειτουργείσει το VPN. */
adsl-branch(config)# interface fastethernet 0/1
adsl-branch(config-if)# ip address 200.200.201.1 255.255.255.0
adsl-branch(config-if)# no shut
adsl-branch(config-if)# exit

/* Παρακάτω ρυθμίζεται το routing με στατικό τρόπο.  Δρομολογούνται κατάλληλα
τα υποδίκτυα σύμφωνα με τις εντολές αυτές. */
adsl-branch(config)# ip route 0.0.0.0 0.0.0.0 200.200.200.2
adsl-branch(config)# ip route 172.16.0.0 255.255.255.128 172.16.1.218
adsl-branch(config)# ip route 172.16.0.128 255.255.255.192 172.16.1.218
adsl-branch(config)# ip route 172.16.0.192 255.255.255.240 172.16.1.218
adsl-branch(config)# ip route 172.16.0.208 255.255.255.248 172.16.1.218

/* Παρακάτω ρυθμίζεται το IP Security Key Exchange (IKE) το οποίο λειτουργεί
στα πλαίσια των εντολών isakmp.  Στην 1η φάση, ρυθμίζουμε το setup μεταξύ των
δύο routers.  Εδώ «συμφωνούν» τα δύο VPN routers για τον τρόπο ανταλλαγής
πληροφοριών με ασφάλεια.  Οι ρυθμίσεις αυτές θα πρέπει να είναι ίδιες και στις
δύο άκρες του VPN. */

adsl-branch(config)# crypto isakmp enable /*Ενεργοποιούμε το isakmp*/
adsl-branch(config)# crypto isakmp policy 10 /* Ορίζουμε μία πολιτική*/

/*ορίζουμε τον τρόπο πιστοποίησης ως pre shared key*/
adsl-branch(config-isakmp)# authentication pre-share

/* επιλέγουμε το md5 ως αλγόριθο hash */
adsl-branch(config-isakmp)#  hash md5

/* επιλέγουμε το Data Encryption Standard (DES) ως αλγόρυθμο κρυπτογράφησης */
adsl-branch(config-isakmp)#  encryption des

/*εδώ ορίζεται το Diffie-Hellman group identifier, το οποίο επιτρέπει στις δύο
άκρες να δημιουργήσουν ένα κοινό κωδικό χωρίς την μετάδωσή του */
adsl-branch(config-isakmp)# group 2

/* ορίζουμε τον χρόνο σε δευτερόλεπτα που θα ισχύει η σύνδεση πριν
ξαναεξεταστούν τα στοιχεία ασφάλειας */
adsl-branch(config-isakmp)# lifetime 3600
adsl-branch(config-isakmp)# exit

/* Παρακάτω ορίζουμε τον απομακρυσμένο router στον οποίο θα συνδεθεί και με
πιο τρόπο θα γίνει η επαλυθευση της ασφάλειας (key security) */
adsl-branch(config)# crypto isakmp key security address 200.200.200.1
255.255.255.0

/* Παρακάτω ορίζουμε το σύνολο των αλγόρυθμων και προτοκόλλων που θα
αξιοποιηθούν για την δημιουργία ενός IPSec tunnel. */
adsl-branch(config)# crypto ipsec transform-set hoset esp-des esp-md5-hmac
```

```
/* Μέσω της παρακάτω access list, ορίζουμε ποια τοπικά υποδίκτυα επιτρέπεται
να επικοινωνούν με ποια απομαρκσυμένα δίκυα. */
adsl-branch(config)# access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.0.0
0.0.0.255

/* Εδώ ρυθμίζεται το σύνολο των ρυθμίσεων που θα πρέπει να εφαρμοστούν στο VPN
tunnel. Ορίζουμε τον απομαρισμένο router, εφαρμόζουμε το transform set που
ορίσαμε παραπάνω και εφαρμόζουμε και την access list που ορίσαμε παραπάνω.
Όλα αυτά τα βάλαμε στο crypto map με όνομα homap.*/
adsl-branch(config)# crypto map homap 10 ipsec-isakmp
adsl-branch(config-crypto-map)# set peer 200.200.200.1
adsl-branch(config-crypto-map)# set transform-set hoset
adsl-branch(config-crypto-map)# match address 101
adsl-branch(config-crypto-map)# exit

/* Το crypto map με όνομα homap ερφαρμόζεται στο interface που συνδέετε στο
Internet.*/
adsl-branch(config)# interface fastethernet 0/1
adsl-branch(config-if)# crypto map homap
adsl-branch(config-if)# exit
adsl-branch(config)# exit
adsl-branch#  write
Building configuration...
[OK]
```



Εικόνα 5.42: Διασύνδεση μεταξύ του ADSL-BRANCH και του Internet

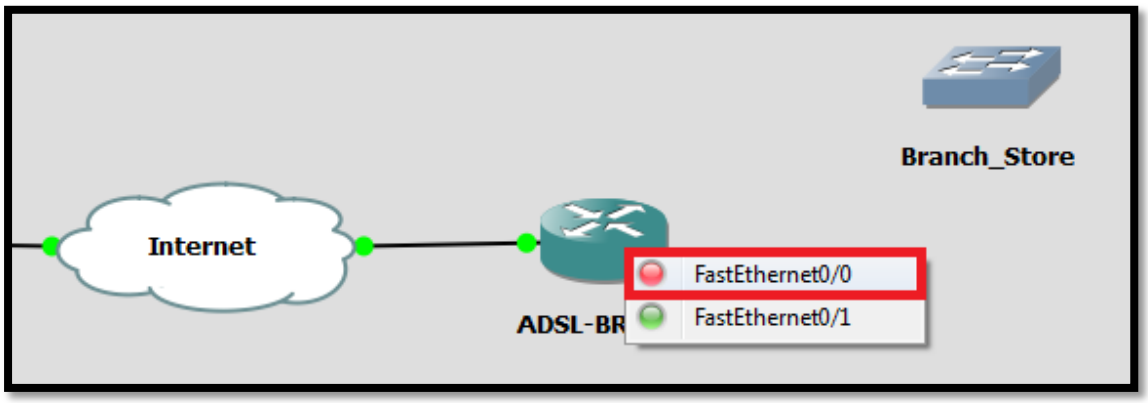


Εικόνα 5.43: Διασύνδεση μεταξύ του ADSL-BRANCH και του Internet

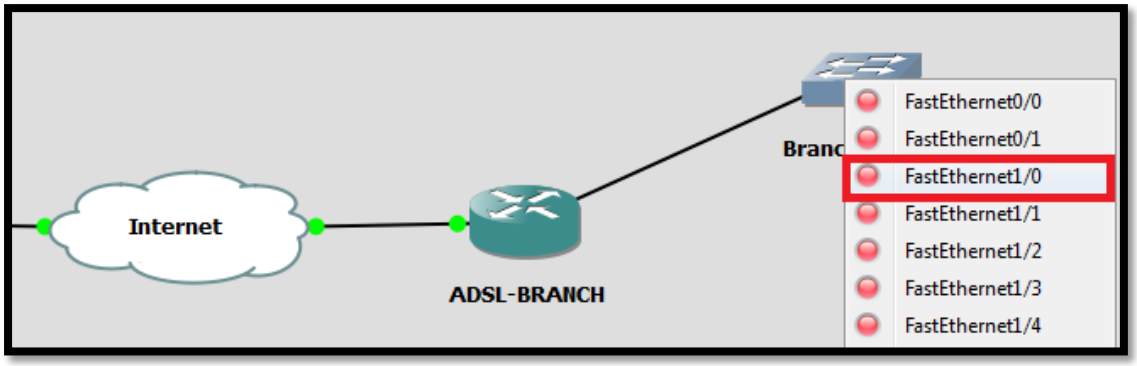
Σε αυτό το σημείο θα τοποθετήσουμε ένα switch για το υποκατάστημα. Οι ρυθμίσεις που εφαρμόστηκαν είναι οι εξής. Σημειώνεται ότι οι ρυθμίζεις είναι παρόμοιες με αυτές των switch των κεντρικών γραφείων.

```
################### Configuration of the branch store ###################
            ************************************************

Branch_Store# conf t
Enter configuration commands, one per line.  End with CNTL/Z.

Branch_Store(config)# hostname Branch_Store
Branch_Store(config)# enable secret cisco123
Branch_Store(config)# line con 0
Branch_Store(config)# password cisco123
Branch_Store(config)# login
Branch_Store(config)# exit
Branch_Store(config)# line vty 0 15
Branch_Store(config-line)# password cisco123
Branch_Store(config-line)# login
Branch_Store(config-line)# transport input ssh
Branch_Store(config-line)# exit
Branch_Store(config)# service password-encryption
Branch_Store(config)# exit
```

```
Branch_Store# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch_Store(config)# interface fastethernet 1/0
Branch_Store(config-if)# description CONN WITH ADSL_VPN_Branch
Branch_Store(config-if)# switchport mode access
Branch_Store(config-if)# no shutdown
Branch_Store(config-if)# exit

Branch_Store(config)# interface range fastethernet 1/2 - 6
Branch_Store(config-if)# switchport mode access
Branch_Store(config-if)# no shutdown
Branch_Store(config-if)# exit

Branch_Store(config)# interface range fastethernet 1/7 - 15
Branch_Store(config-if)# switchport mode access
Branch_Store(config-if)# no shutdown
Branch_Store(config-if)# exit

Branch_Store(config)# interface vlan 1
Branch_Store(config-if)# ip address 172.16.1.2 255.255.255.240
Branch_Store(config-if)# no shutdown
Branch_Store(config-if)# exit

Branch_Store(config)# interface fastEthernet 1/0
Branch_Store(config-if)# description CONN WITH ASA_2
Branch_Store(config-if)# switchport mode access
Branch_Store(config-if)# no shutdown
Branch_Store(config-if)# exit

Branch_Store(dhcp-config)# ip dhcp pool branch
Branch_Store(dhcp-config)# network 172.16.1.0 255.255.255.240
Branch_Store(dhcp-config)# default-router 172.16.1.1
Branch_Store(dhcp-config)# exit
Branch_Store(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.6
Branch_Store(config)# exit

Branch_Store# write
Building configuration...
[OK]
```



Εικόνα 5.44: Διασύνδεση μεταξύ του ADSL-BRANCH με το switch Branch_Store

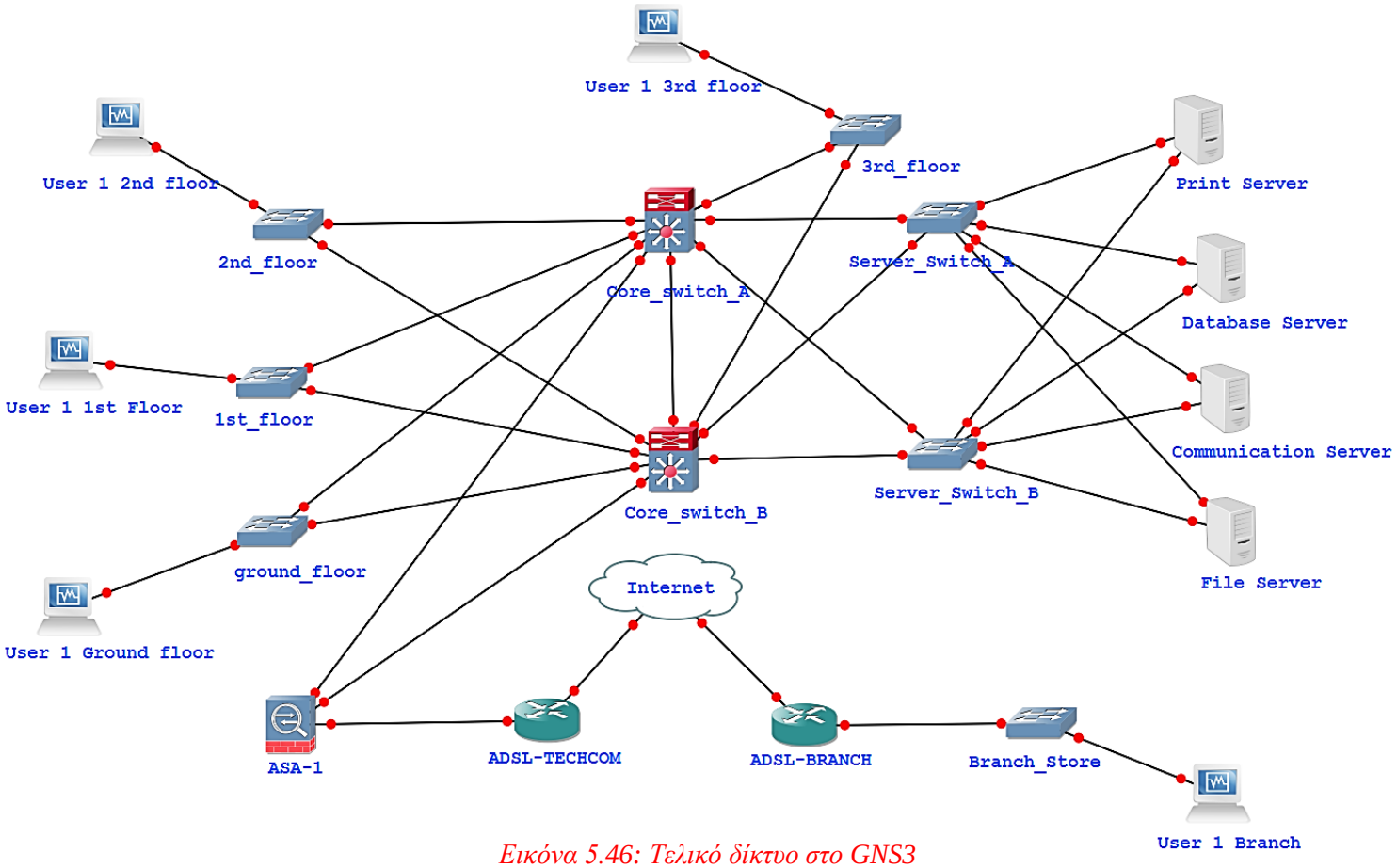


Εικόνα 5.45: Διασύνδεση μεταξύ του ADSL-BRANCH με το switch Branch_Store

Με τις παρακάτω δύο εντολές, βλέπουμε την κατάσταση του VPN. Με την εντολή show crypto ipsec sa βλέπουμε το IP Security Association μεταξύ των δύο routers. Με την εντολή show crypto isakmp sa μας δείχνει την κατάσταση της σύνδεσης. Με τα παρακάτω δύο αποτελέσαματα, βλέπουμε ότι η σύνδεση λειτουργεί ομαλά.

```
User Access Verification

Password:

ADSL-TECHCOM# show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: homap, local addr 200.200.200.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
   current_peer 200.200.201.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 200.200.200.1, remote crypto endpt.: 200.200.201.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:


ADSL-TECHCOM# show crypto isakmp sa
dst             src             state          conn-id slot status

ADSL-TECHCOM# show crypto isakmp sa
dst             src             state          conn-id slot status
200.200.200.1   200.200.201.1   QM_IDLE              1    0 ACTIVE
```

5.7 Έλεγχος επικοινωνίας μεταξύ των κόμβων του κάθε υποδικτύου



Εικόνα 5.46: Τελικό δίκτυο στο GNS3

Μετά από τις παραπάνω ρυθμίσεις θα προσθέσουμε τα pc σε κάθε LAN υποδίκτυο και τους servers στο υποδίκτυο του server LAN. Εμείς παρακάτω θα τεστάρουμε την επικοινωνία ως εξής:

Χρήστες που θα χρησιμοποιηθούν			
User 1 Ground Floor	Έλεγχος έγκυρης IP	Έλεγχος Ping από user σε user	Έλεγχος traceroute
User 1 1st Floor	Έλεγχος έγκυρης IP	Έλεγχος Ping από user σε user	Έλεγχος traceroute
User 2 2nd Floor	Έλεγχος έγκυρης IP	Έλεγχος Ping από user σε user	Έλεγχος traceroute
User 3 3rd Floor	Έλεγχος έγκυρης IP	Έλεγχος Ping από user σε user	Έλεγχος traceroute
User 1 Branch	Έλεγχος έγκυρης IP	Έλεγχος Ping από user σε user	Έλεγχος traceroute

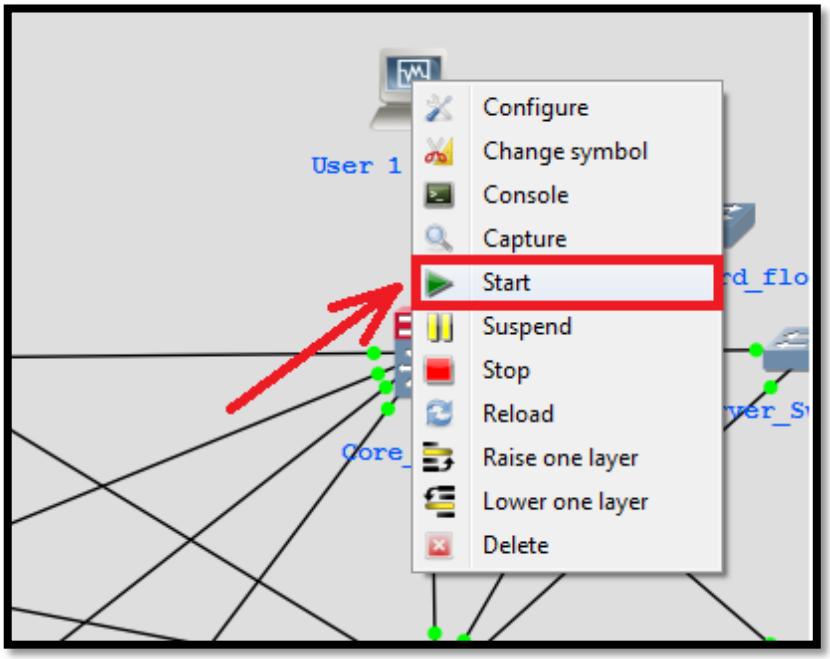
Πίνακας 5.3: Ενδεικτικός πίνακας κόμβων που θα εφαρμοστούν οι έλεγχοι λειτουργίας του δικτύου

Οι εν λόγω χρήστες που θα χρησιμοποιήσουμε για τους ελέγχους που αναγράφει ο πίνακας 5.3 είναι εικονικά μηχανήματα που δημιουργήσαμε στο virtual box. Σε αυτά έχει εγκατασταθεί λογισμικό Windows XP καθότι υποστηρίζει αυτή την συγκεκριμένη έκδοση λογισμικού για τα εικονικά μηχανήματα και καμία άλλη. Οι έλεγχοι που περιγράφουμε στον πίνακα 5.3 θα εφαρμοστούν από χρήστη σε χρήστη. Λόγω του ότι κάθε pc στο GNS3 χρησιμοποιεί κι από ένα εικονικό μηχάνημα για την προσωμοίωση έχουμε φτιάξει 5 εικονικά μηχανήματα που αντιπροσωπεύουν τους χρήσες και είναι σε κάθε υποδίκτυο και 4 επίσης εικονικά μηχανήματα που αντιπροσωπεύουν τους servers στο server LAN.
Συνεπώς, θα ελέγξουμε αν τα εικονικά μηχανήματα των χρηστών που περιλαμβάνονται στον πίνακα 5.3 έχουν πάρει έγκυρη IP και default IP gateway, θα εφαρμόσουμε ελέγχους ping επικοινωνίας προκειμένου να διαπιστόσουμε ότι δεν υπάρχει κάποιο πρόβλημα στην επικοινωνία μεταξύ των χρηστών του δικτύου.

5.7.1 Έλεγχοι έγκυρης IP διεύθυνσης σε κάθε χρήστη

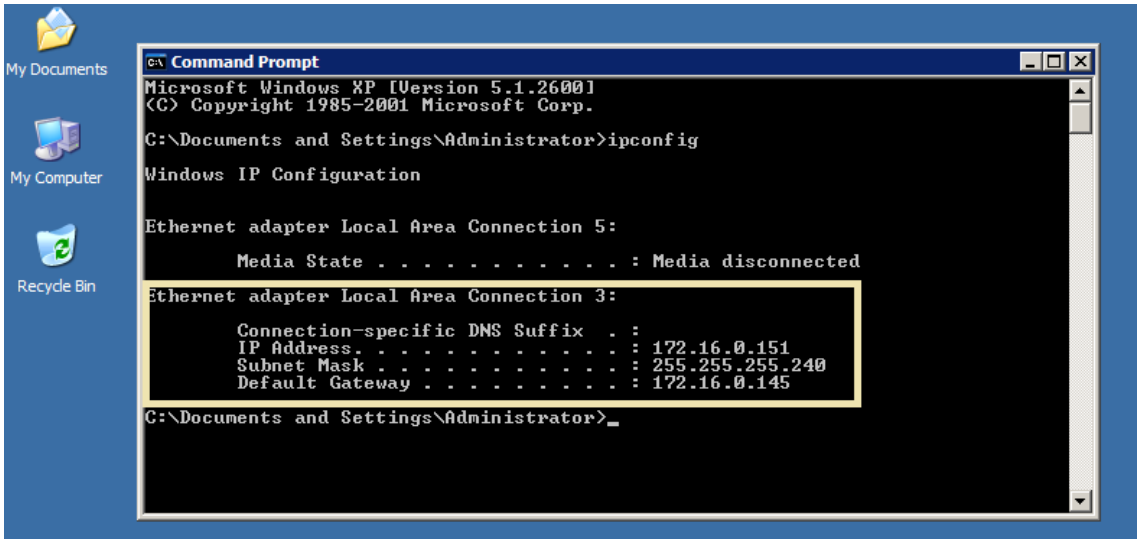
1. **Για τον user 1 στον 3^{ο} όροφο:**

   Κάνουμε δεξί κλίκ πάνω στον User 1 3rd floor και επιλέγουμε το start. Μόλις το κάνουμε αυτό θα τρέξει το αντίστοιχο τερματικό που βρίσκεται στο virtual box. Σημειώνεται ότι αλλάξαμε τις ρυθμίσεις στο εικονίκό μηχάνημα στο network και επιλέξαμε το Host only adapter προκειμένου να μπορεί να συγχρονιστεί με το GNS3.



Εικόνα 5.47: Εκκίνηση του User 1 3rd floor

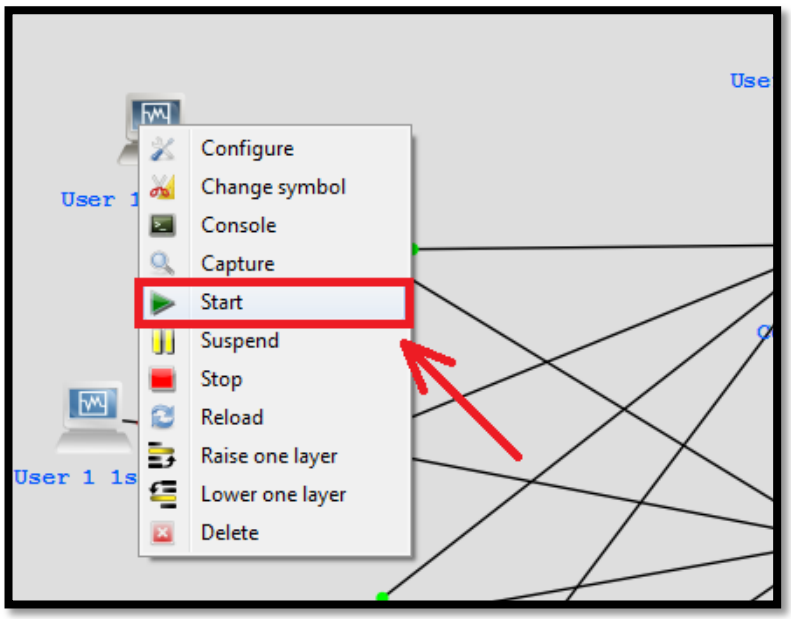
Σε αυτό το σημείο είμαστε στο εικονικό μηχάνημα του user 1 3rd floor. Αν πάμε στο CMD του εικονικού μηχανήματος και εκτελέσουμε την εντολή ipconfig παρατηρούμε ότι ο user 1 του 3ου ορόφου έχει πάρει κανονικά IP διεύθυνση από τα core switches που αναλαμβάνουν τον ρόλο του DHCP server.



Εικόνα 5.48: Εκτέλεση της εντολής ipconfig στον User 3 3rd Floor

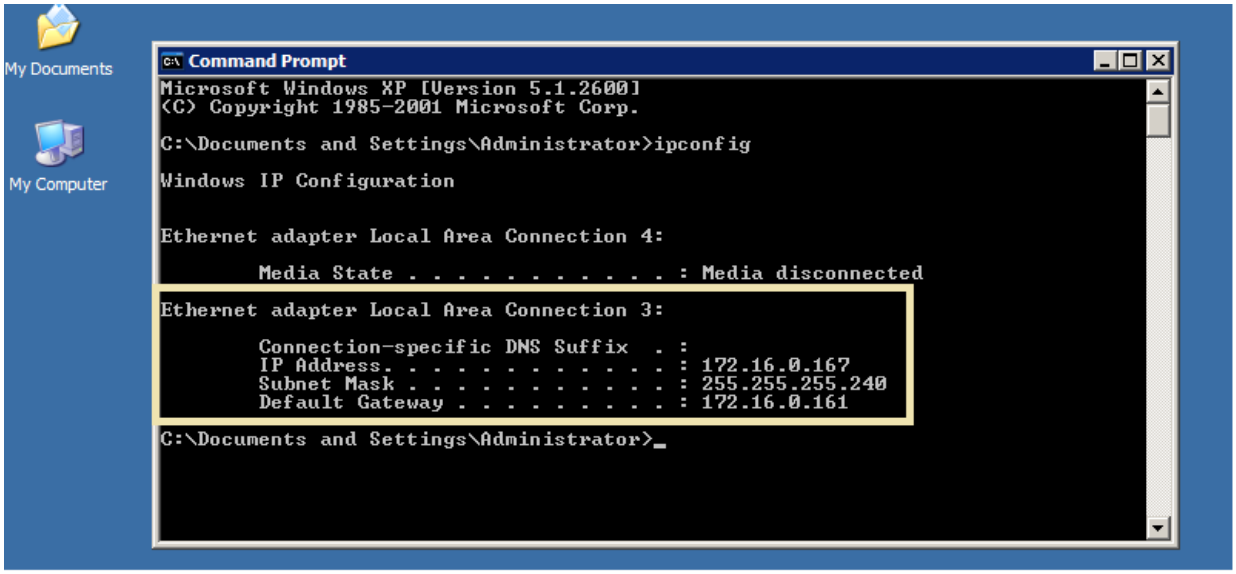
2. **Για τον user 1 στον 2ο όροφο:**

Κάνουμε δεξί κλίκ πάνω στον User 1 2nd floor και επιλέγουμε το start. Μόλις το κάνουμε αυτό θα τρέξει το αντίστοιχο τερματικό που βρίσκεται στο virtual box. Σημειώνεται ότι αλλάξαμε τις ρυθμίσεις στο εικονικό μηχάνημα στο network και επιλέξαμε το Host only adapter προκειμένου να μπορεί να συγχρονιστεί με το GNS3.



Εικόνα 5.49: Εκκίνηση του User 1 2nd floor

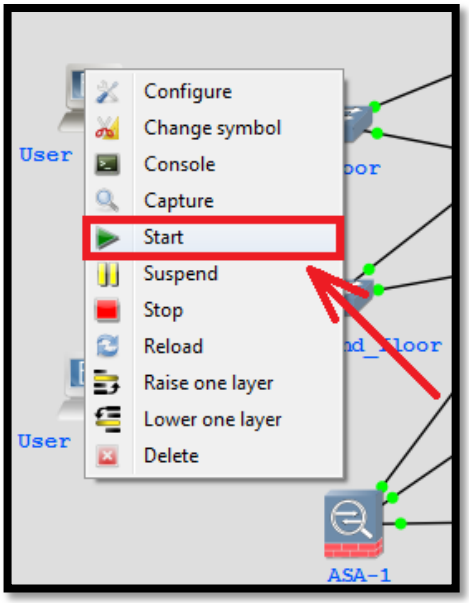
Σε αυτό το σημείο είμαστε στο εικονικό μηχάνημα του user 1 2nd floor. Αν πάμε στο CMD του εικονικού μηχανήματος και εκτελέσουμε την εντολή ipconfig παρατηρούμε ότι ο user 1 του 2ου ορόφου έχει πάρει κανονικά IP διεύθυνση από τα core switches που αναλαμβάνουν τον ρόλο του DHCP server.



Εικόνα 5.50: Εκτέλεση της εντολής ipconfig στον User 2 2nd Floor

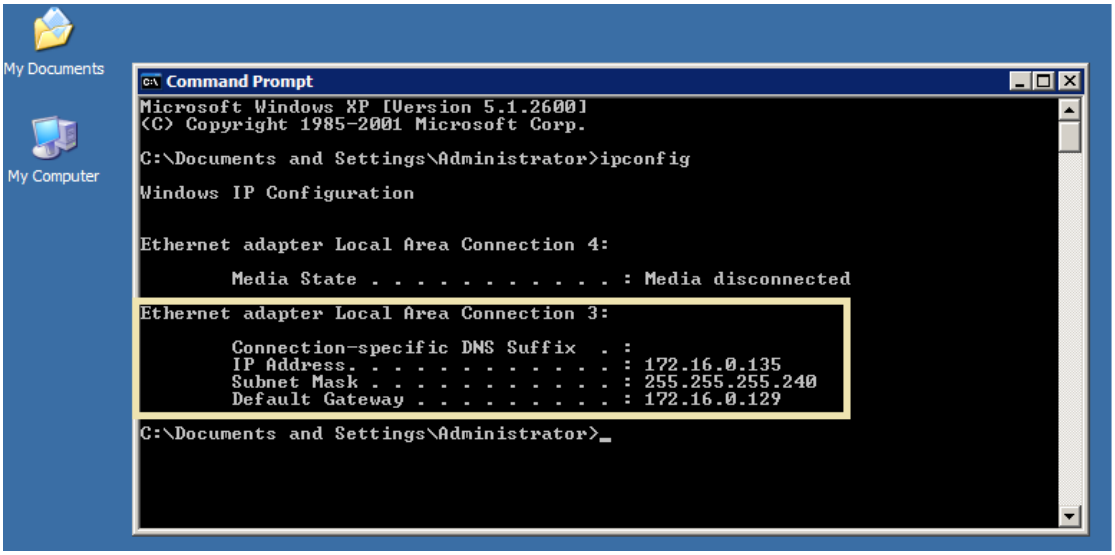
3. **Για τον user 1 στον 1ο όροφο:**

Κάνουμε δεξί κλίκ πάνω στον User 1 2nd floor και επιλέγουμε το start. Μόλις το κάνουμε αυτό θα τρέξει το αντίστοιχο τερματικό που βρίσκεται στο virtual box. Σημειώνεται ότι αλλάξαμε τις ρυθμίσεις στο εικονίκό μηχάνημα στο network και επιλέξαμε το Host only adapter προκειμένου να μπορεί να συγχρονιστεί με το GNS3.



Εικόνα 5.51: Εκκίνηση του User 1 1st Floor

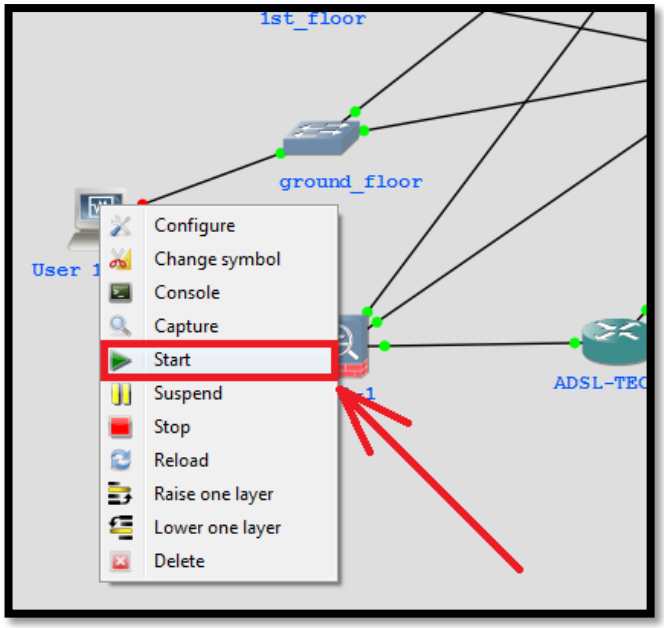
Σε αυτό το σημείο είμαστε στο εικονικό μηχάνημα του user 1 1st floor. Αν πάμε στο CMD του εικονικού μηχανήματος και εκτελέσουμε την εντολή ipconfig παρατηρούμε ότι ο user 1 του 1ου ορόφου έχει πάρει κανονικά IP διεύθυνση από τα core switches που αναλαμβάνουν τον ρόλο του DHCP server.



Εικόνα 5.52: Εκτέλεση της εντολής ipconfig στον User 1 1st Floor

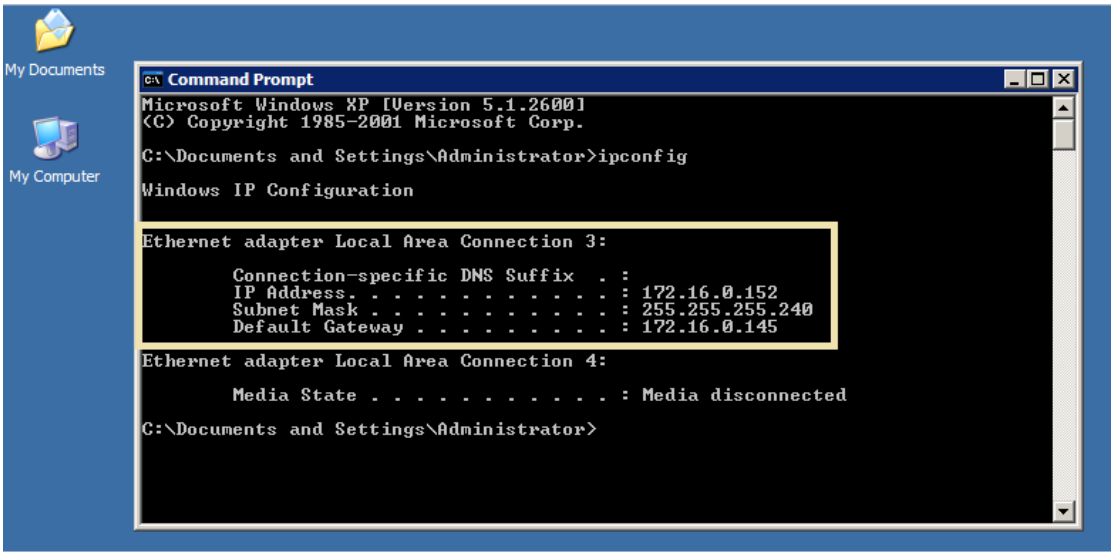
4. **Για τον user 1 στον ισόγειο:**

Κάνουμε δεξί κλίκ πάνω στον User 1 ground floor και επιλέγουμε το start. Μόλις το κάνουμε αυτό θα τρέξει το αντίστοιχο τερματικό που βρίσκεται στο virtual box. Σημειώνεται ότι αλλάξαμε τις ρυθμίσεις στο εικονίκό μηχάνημα στο network και επιλέξαμε το Host only adapter προκειμένου να μπορεί να συγχρονιστεί με το GNS3.



Εικόνα 5.53: Εκτέλεση του User 1 ground Floor

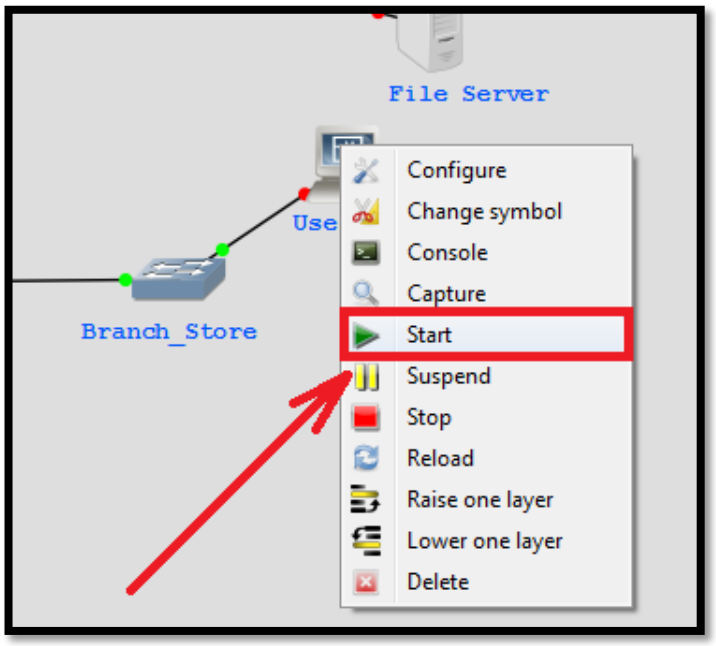
Σε αυτό το σημείο είμαστε στο εικονικό μηχάνημα του user 1 ground floor. Αν πάμε στο CMD του εικονικού μηχανήματος και εκτελέσουμε την εντολή ipconfig παρατηρούμε ότι ο user 1 του ισογείου έχει πάρει κανονικά IP διεύθυνση από τα core switches που αναλαμβάνουν τον ρόλο του DHCP server.



Εικόνα 5.54: Εκτέλεση της εντολής ipconfig στον User 1 ground Floor

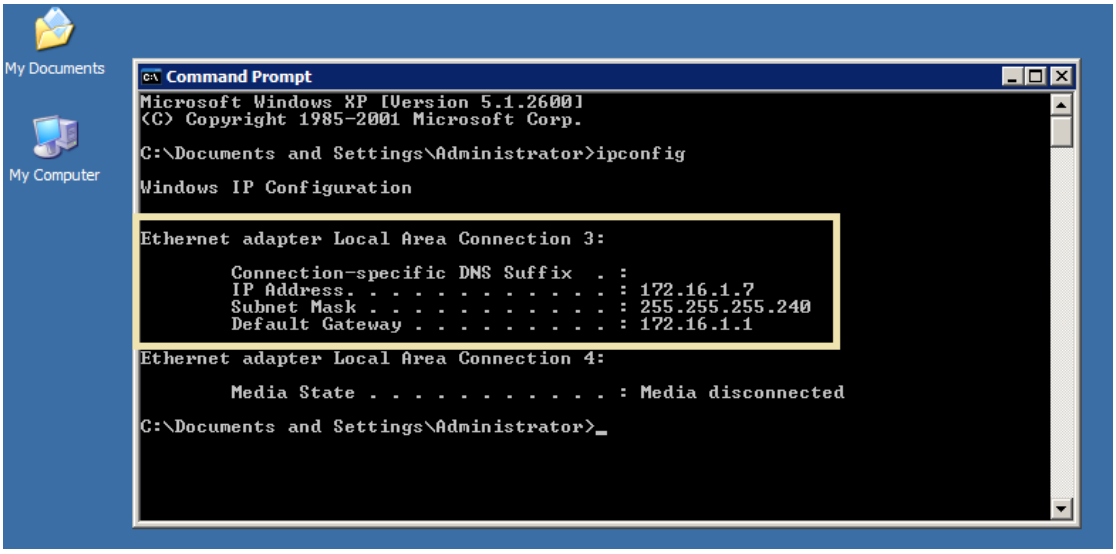
5. **Για τον user 1 στο υποκατάστημα:**

Κάνουμε δεξί κλίκ πάνω στον User 1 branch και επιλέγουμε το start. Μόλις το κάνουμε αυτό θα τρέξει το αντίστοιχο τερματικό που βρίσκεται στο virtual box. Σημειώνεται ότι αλλάξαμε τις ρυθμίσεις στο εικονίκό μηχάνημα στο network και επιλέξαμε το Host only adapter προκειμένου να μπορεί να συγχρονιστεί με το GNS3.



Εικόνα 5.55: Εκτέλεση του User 1 branch

Σε αυτό το σημείο είμαστε στο εικονικό μηχάνημα του user 1 branch. Αν πάμε στο CMD του εικονικού μηχανήματος και εκτελέσουμε την εντολή ipconfig παρατηρούμε ότι ο user 1 του υποκαταστήματος έχει πάρει κανονικά IP διεύθυνση από τα core switches που αναλαμβάνουν τον ρόλο του DHCP server.

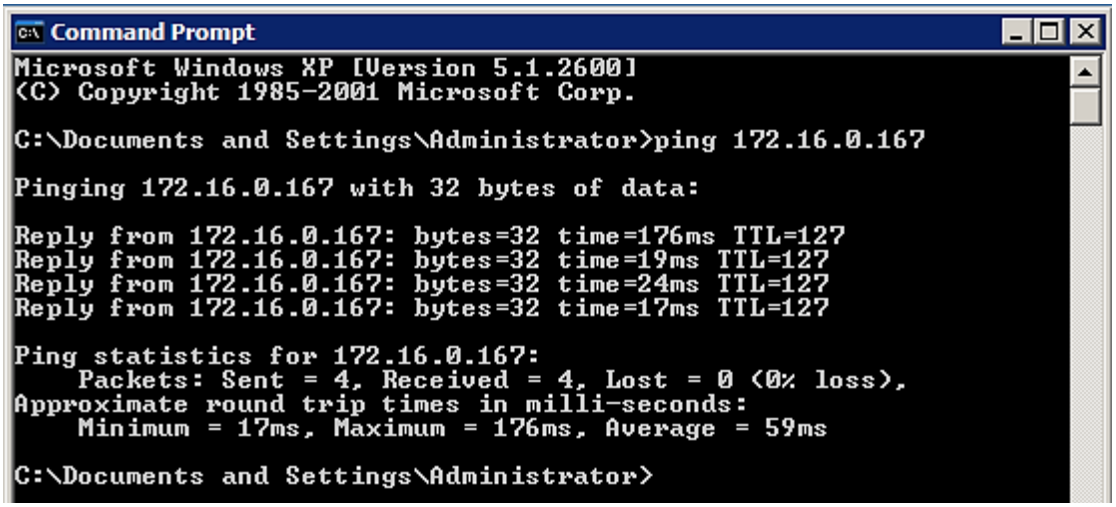


Εικόνα 5.56: Εκτέλεση της εντολής ipconfig στον User 1 branch

5.7.2 Έλεγχοι επικοινωνίας ping από χρήστη σε χρήστη

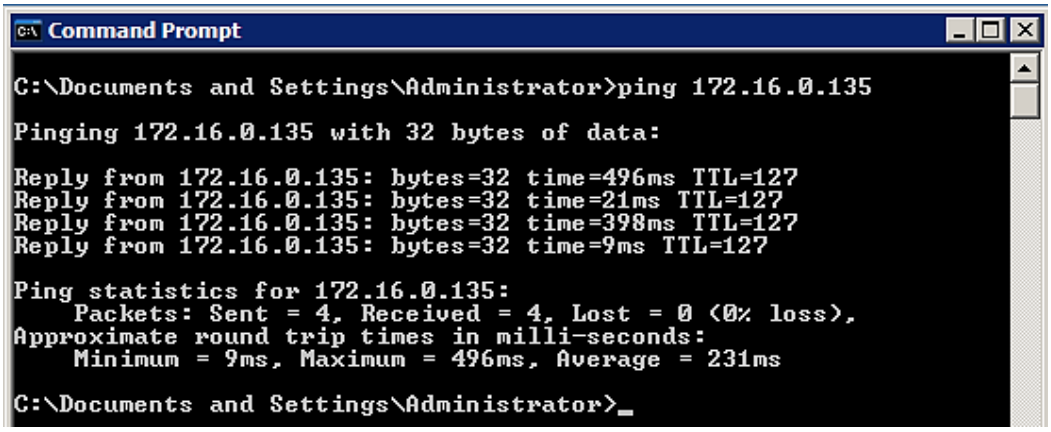
1. **Για τον user 1 του 3ου ορόφου:**

Ping προς user 1 του 2ου ορόφου



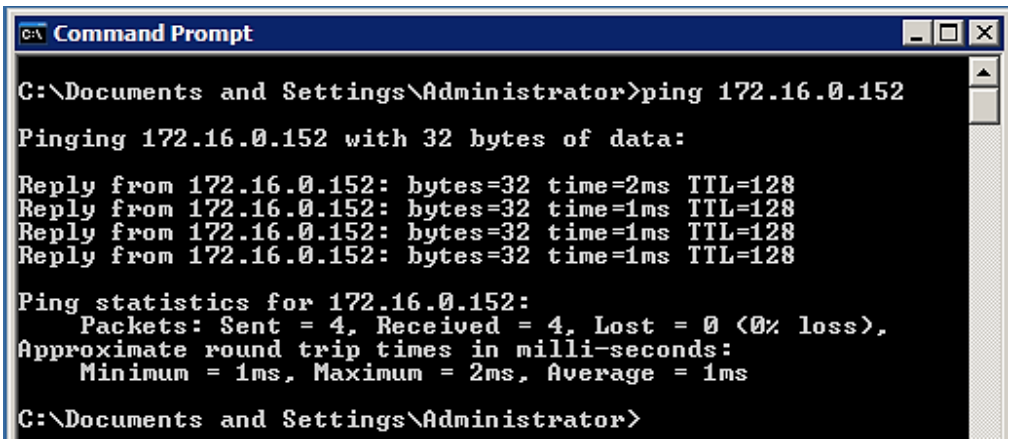
Εικόνα 5.57: Επιτυχές ping προς user 1 του 2ου ορόφου

Ping προς user 1 του 1ου ορόφου



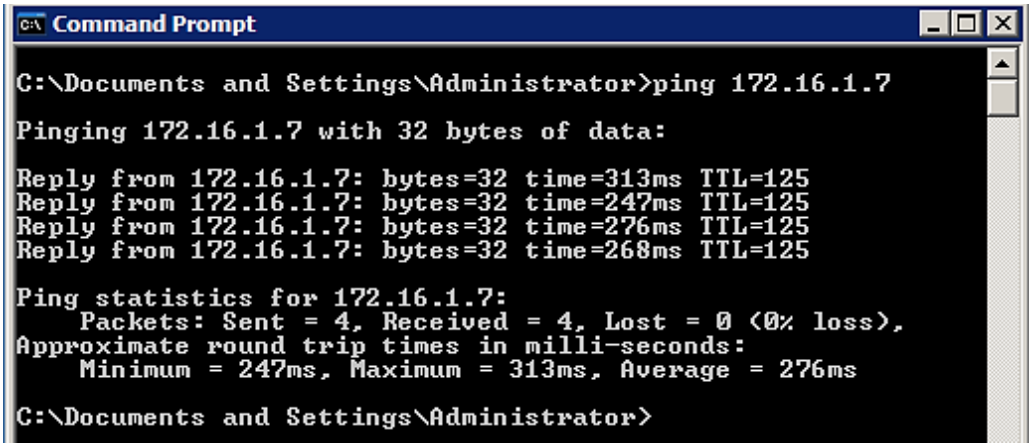
Εικόνα 5.58: Επιτυχές ping προς user 1 του 1ου ορόφου

Ping προς user 1 του ισογείου



Εικόνα 5.59: Επιτυχές ping προς user 1 του ισογείου

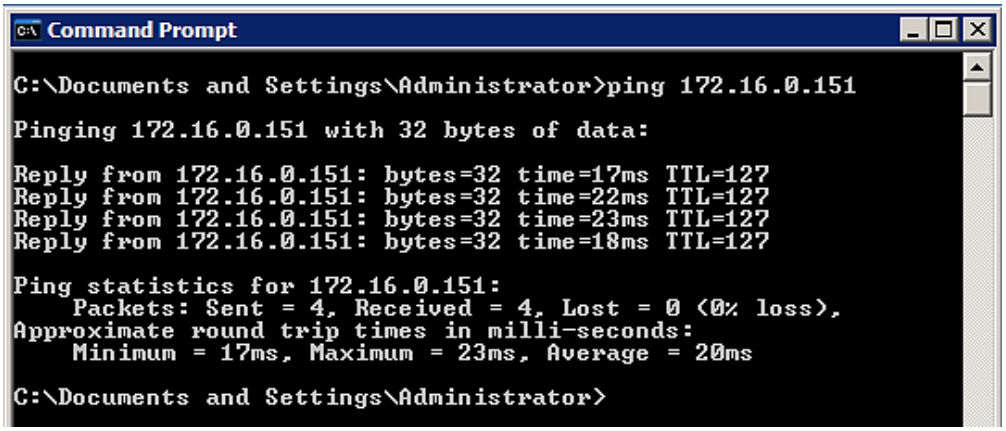
Ping προς user 1 του υποκαταστήματος



Εικόνα 5.60: Επιτυχές ping προς user 1 του υποκαταστήματος

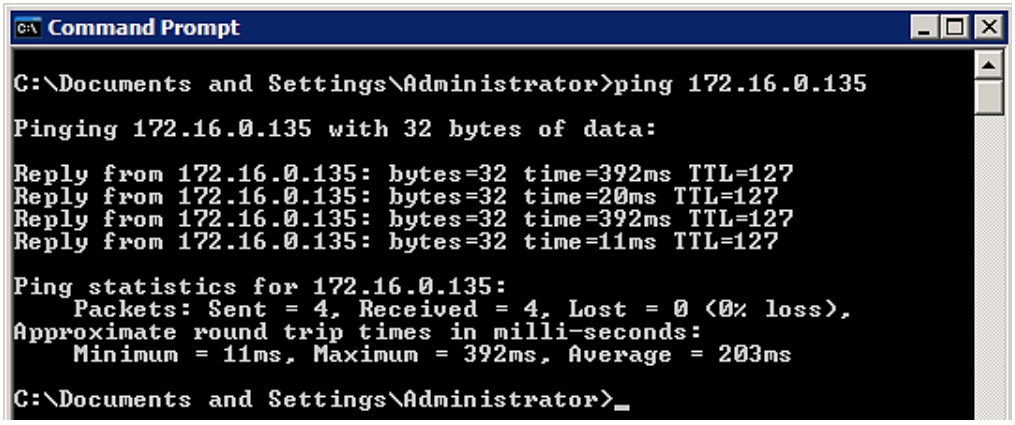
2. **Για τον user 1 του 2ου ορόφου:**

Ping προς user 1 του 3ου ορόφου



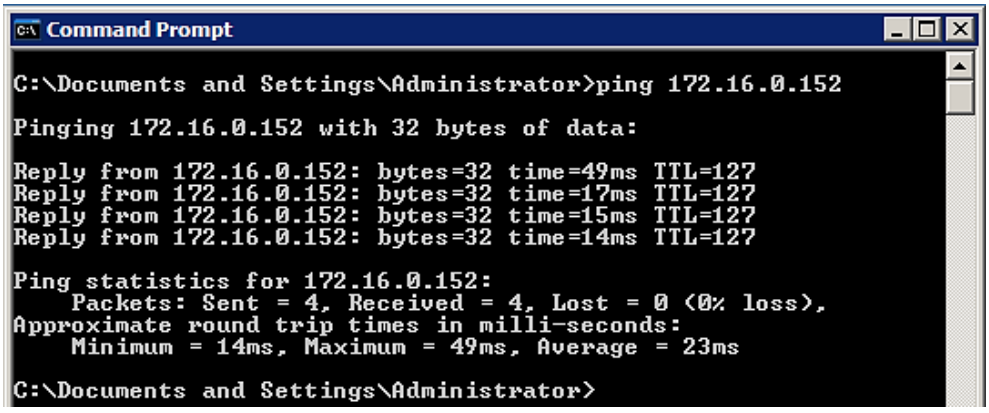
Εικόνα 5.61: Επιτυχές ping προς user 1 του 3ου ορόφου

Ping προς user 1 του 1ου ορόφου



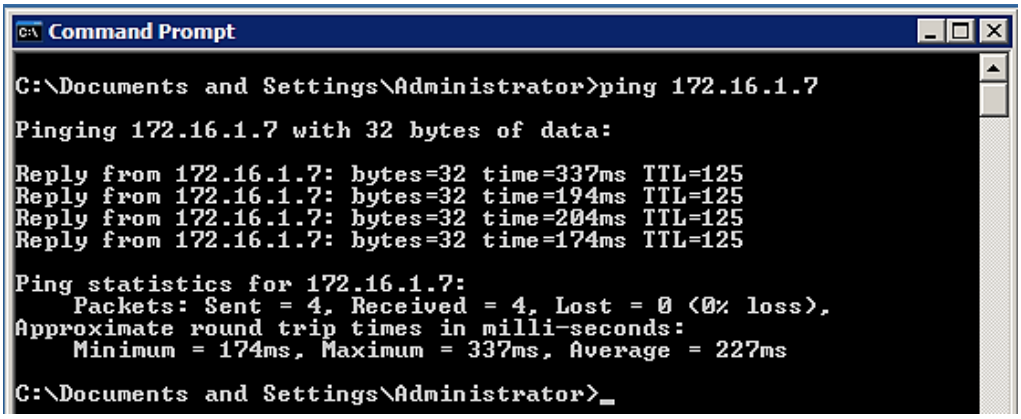
Εικόνα 5.62: Επιτυχές ping προς user 1 του 1ου ορόφου

Ping προς user 1 του ισογείου



Εικόνα 5.63: Επιτυχές ping προς user 1 του ισογείου

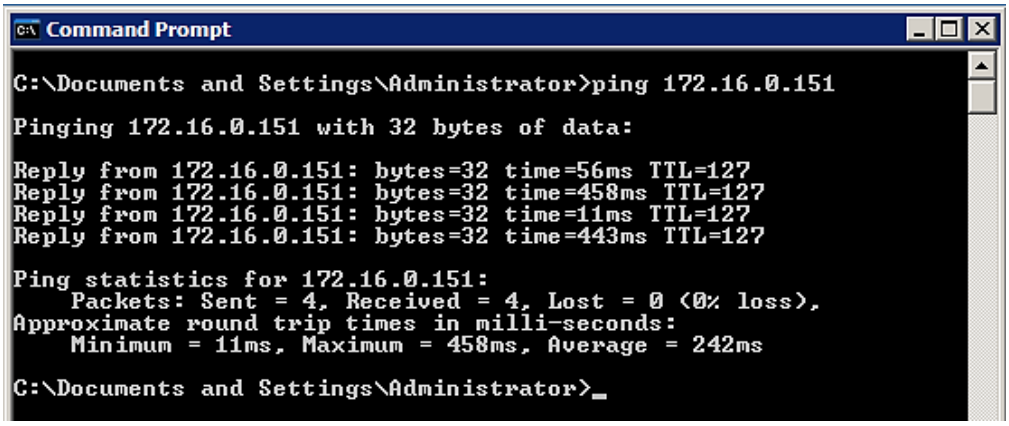
Ping προς user 1 του υποκαταστήματος



Εικόνα 5.64: Επιτυχές ping προς user 1 του υποκαταστήματος

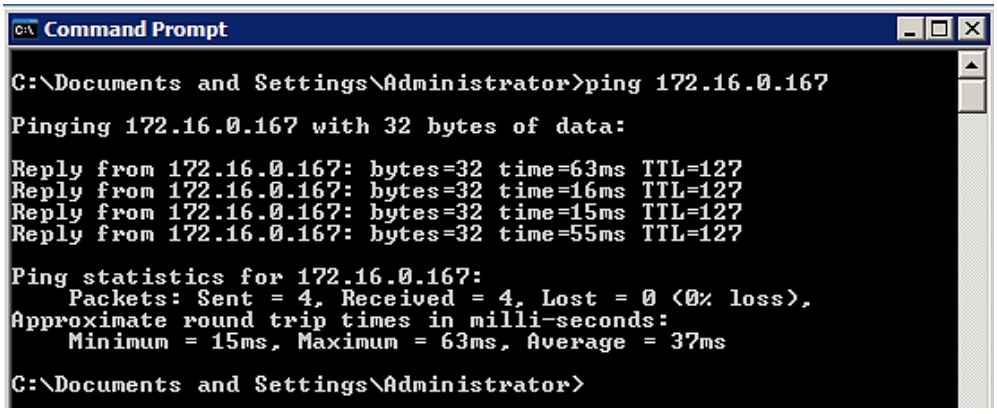
3. **Για τον user 1 του 1ου ορόφου:**

Ping προς user 1 του 3ου ορόφου



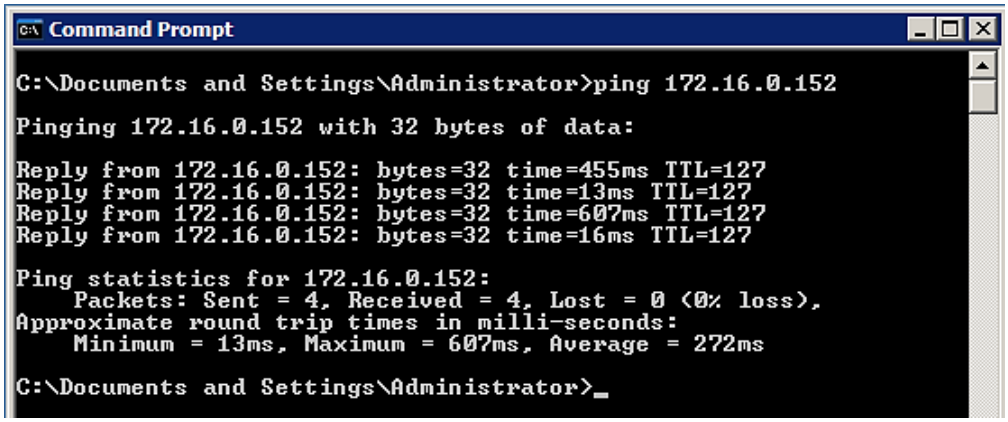
Εικόνα 5.65: Επιτυχές ping προς user 1 του 3ου ορόφου

Ping προς user 1 του 2ου ορόφου



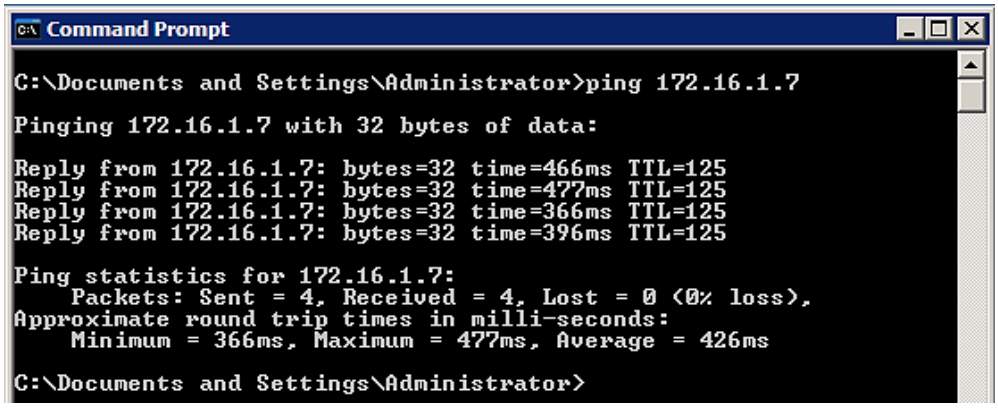
Εικόνα 5.66: Επιτυχές ping προς user 1 του 2ου ορόφου

Ping προς user 1 του ισογείου



Εικόνα 5.67: Επιτυχές ping προς user 1 του ισογείου

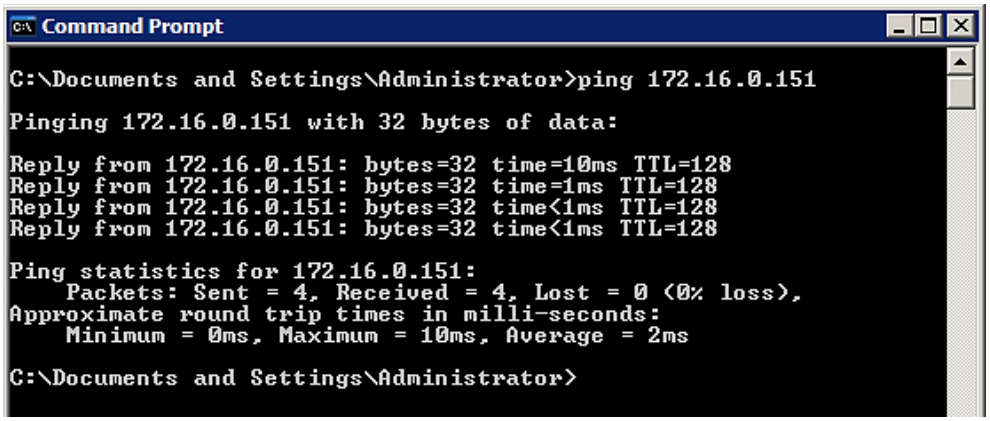
Ping προς user 1 του υποκαταστήματος



Εικόνα 5.68: Επιτυχές ping προς user 1 του υποκαταστήματος

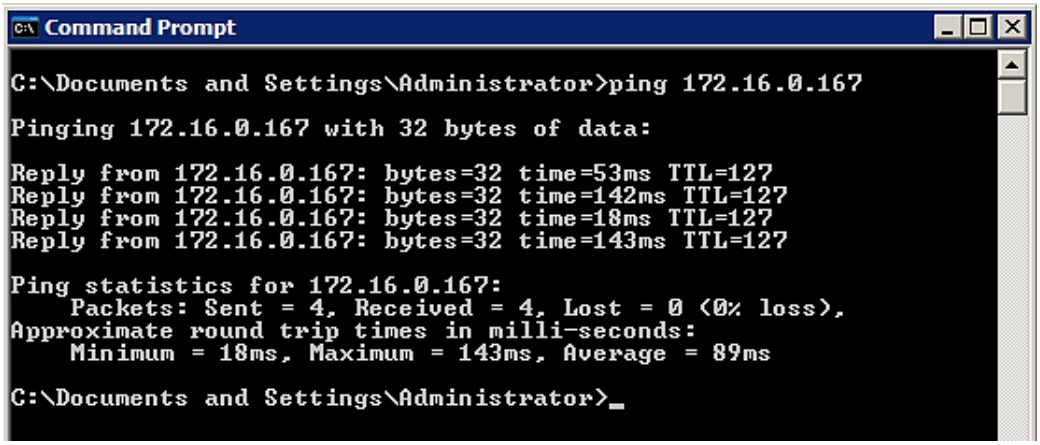
4. **Για τον user 1 του ισογείου:**

Ping προς user 1 του 3^{ου} ορόφου



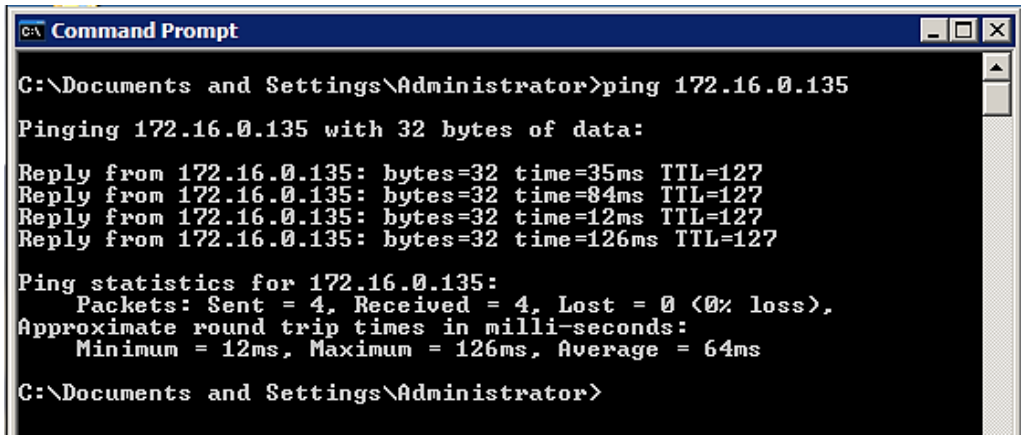
Εικόνα 5.69: Επιτυχές ping προς user 1 του 3ου ορόφου

Ping προς user 1 του 2ου ορόφου



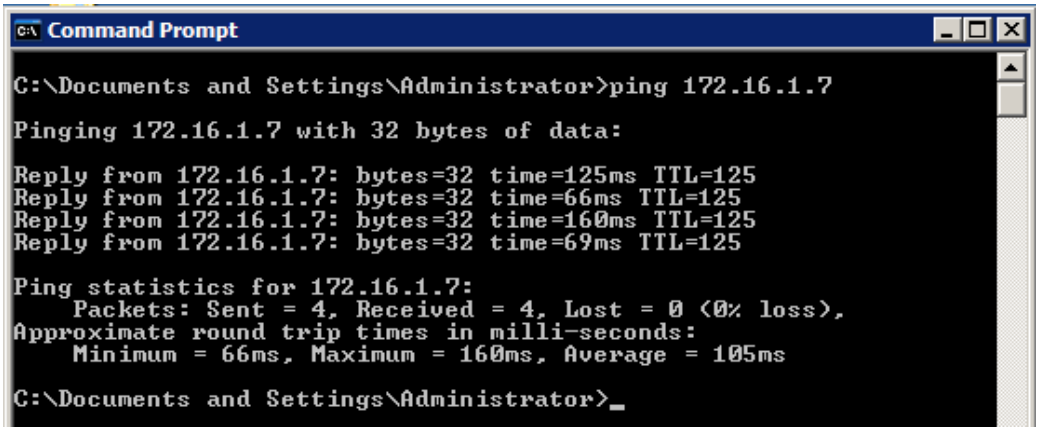
Εικόνα 5.70: Επιτυχές ping προς user 1 του 2ου ορόφου

Ping προς user 1 του 1ου ορόφου



Εικόνα 5.71: Επιτυχές ping προς user 1 του 2ου ορόφου

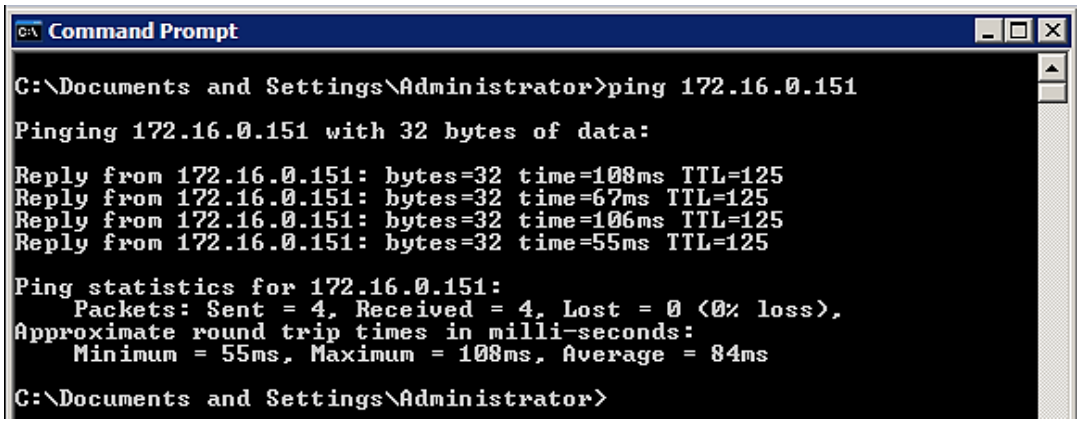
Ping προς user 1 του υποκαταστήματος



Εικόνα 5.72: Επιτυχές ping προς user 1 του 2ου ορόφου

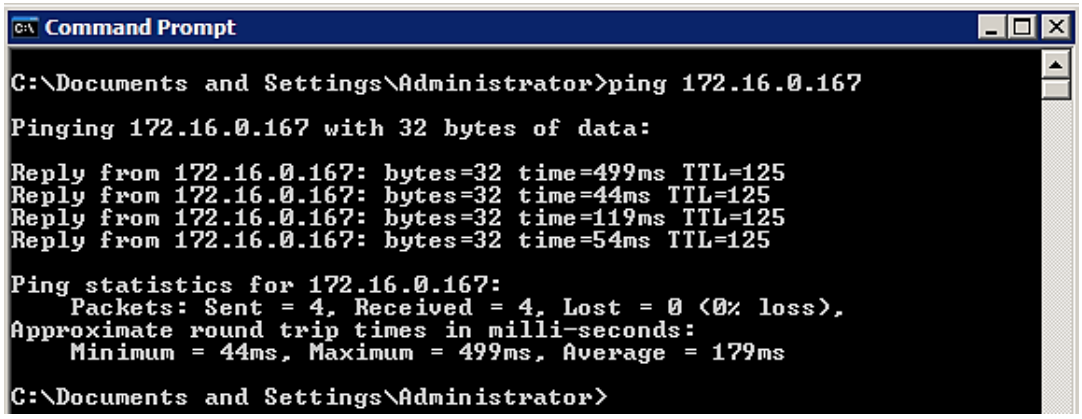
5. **Για τον user 1 στο υποκατάστημα:**

Ping προς user 1 του 3ου ορόφου



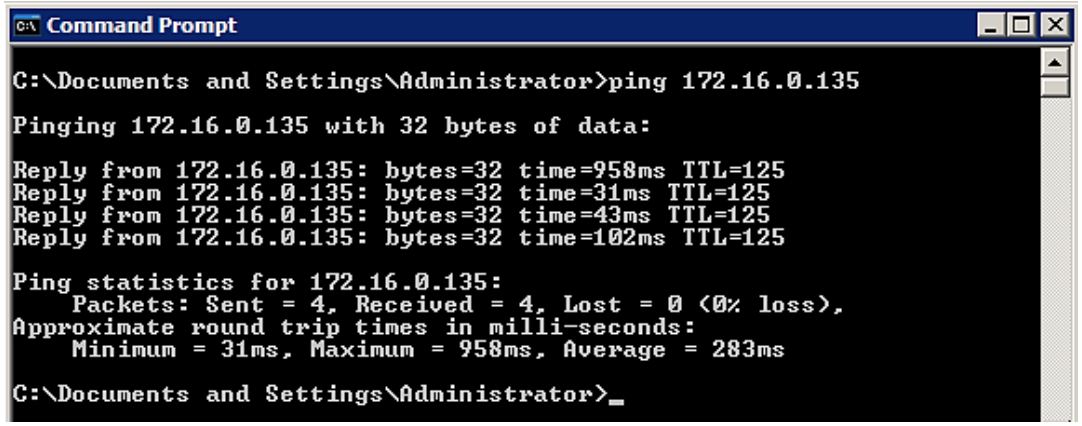
Εικόνα 5.73: Επιτυχές ping προς user 1 του 3ου ορόφου

Ping προς user 1 του 2ου ορόφου



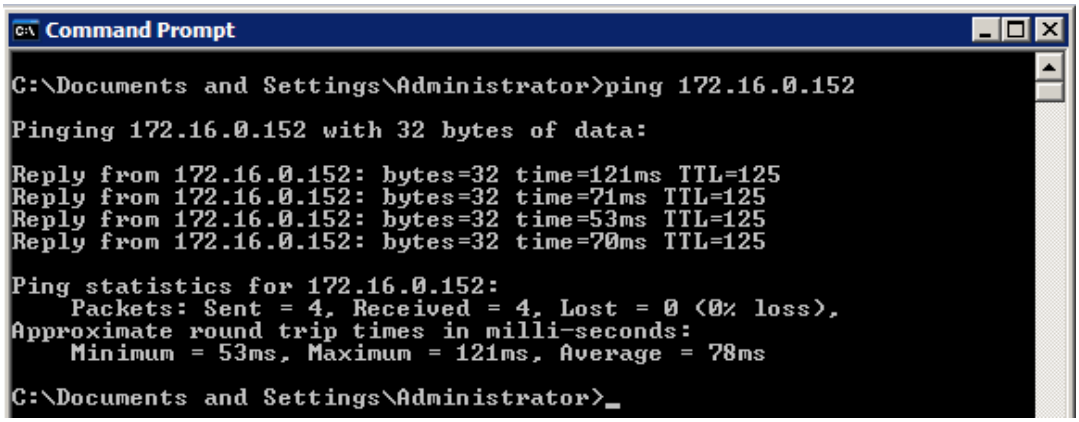
Εικόνα 5.74: Επιτυχές ping προς user 1 του 2ου ορόφου

Ping προς user 1 του 1ου ορόφου



Εικόνα 5.75: Επιτυχές ping προς user 1 του 1ου ορόφου

Ping προς user 1 του ισογείου



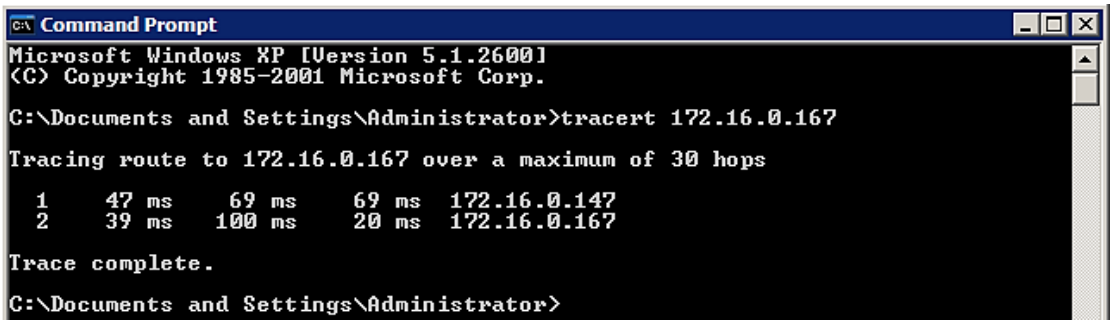
Εικόνα 5.76: Επιτυχές ping προς user 1 του ισογείου

6. Συμπέρασμα

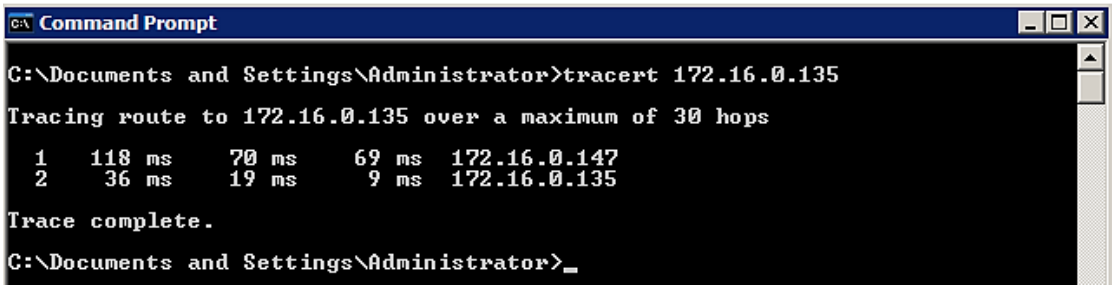
Όπως παρατηρήσαμε ο έλεγχος ping στέφθηκε με απόλυτη επιτυχία και δεν συνέβη καμία απώλεια πακέτων καθόλη την διάρκεια τον ping επικοινωνιών ανάμεσα στους χρήστες. Αυτό αποδεικνύει ότι το δίκτυο μας δουλεύει και ότι είναι απόλυτα λειτουργικό.

5.7.3 Έλεγχοι traceroute από χρήστη σε χρήστη

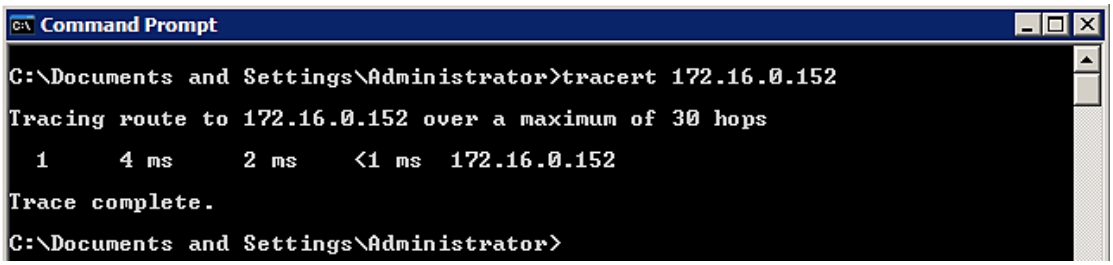
1. **Για τον user 1 του 3ου ορόφου:**



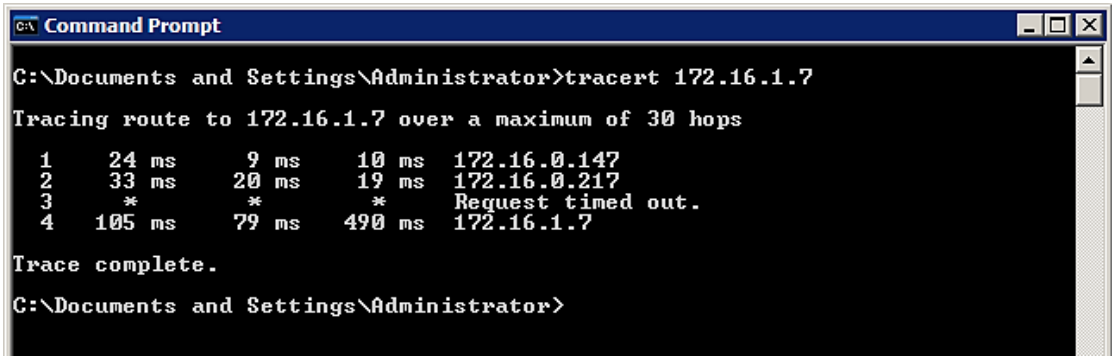
Εικόνα 5.77: Εκτέλεση tracert προς τον χρήστη του 2ου ορόφου



Εικόνα 5.78: Εκτέλεση tracert προς τον χρήστη του 1ου ορόφου

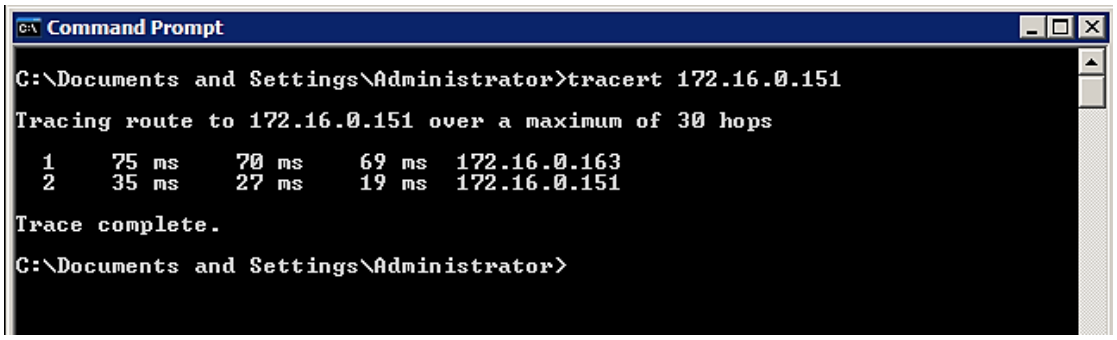


Εικόνα 5.79: Εκτέλεση tracert προς τον χρήστη του ισογείου

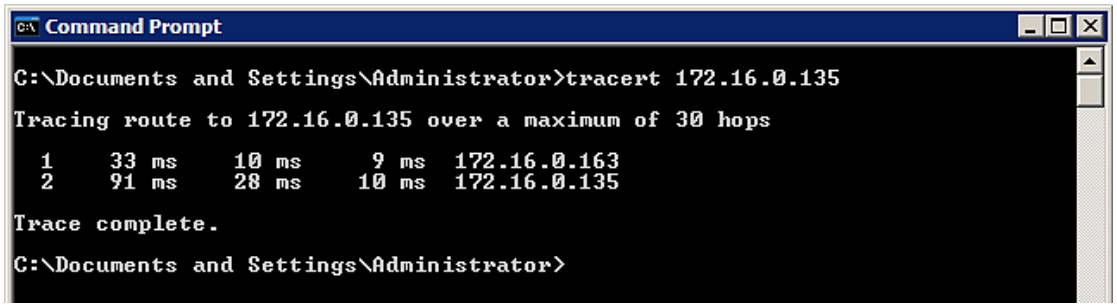


Εικόνα 5.80: Εκτέλεση tracert προς τον χρήστη του υποκαταστήματος

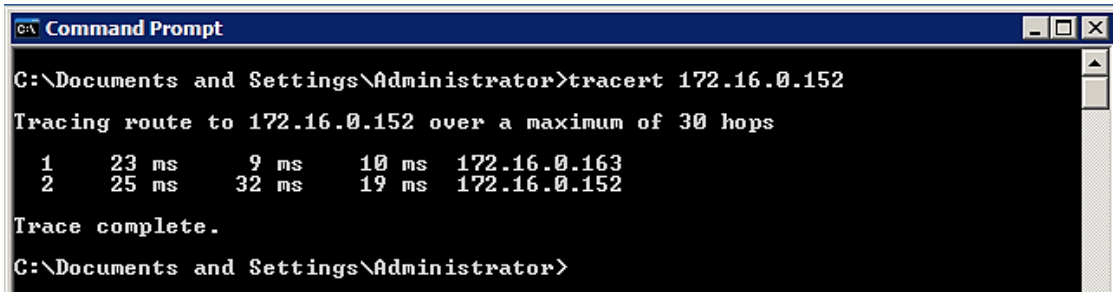
2. **Για τον user 1 του 2ου ορόφου:**



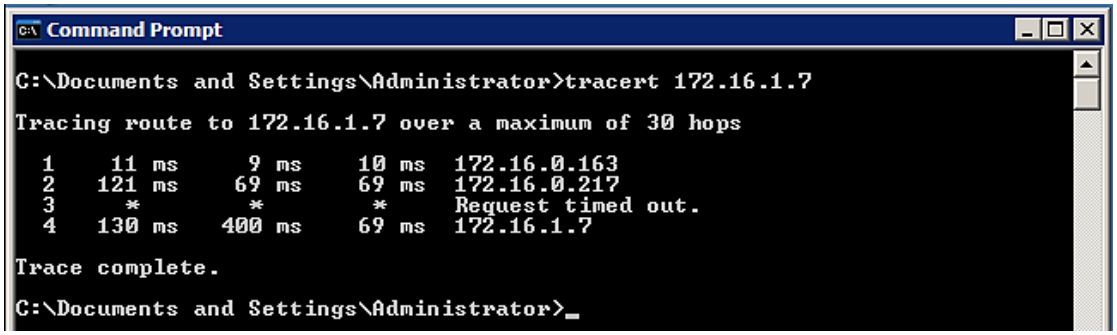
Εικόνα 5.81: Εκτέλεση tracert προς τον χρήστη του 3ου ορόφου



Εικόνα 5.82: Εκτέλεση tracert προς τον χρήστη του 1ου ορόφου

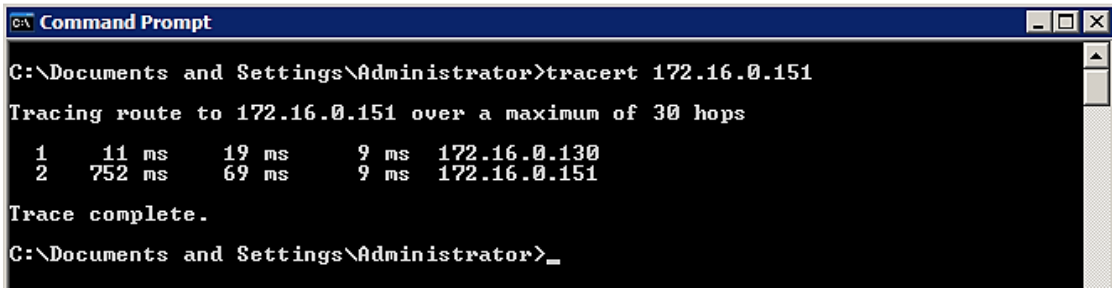


Εικόνα 5.83: Εκτέλεση tracert προς τον χρήστη του ισογείου

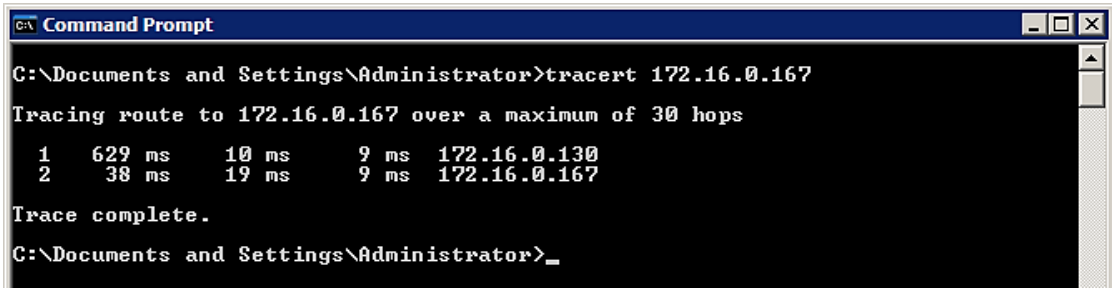


Εικόνα 5.84: Εκτέλεση tracert προς τον χρήστη του υποκαταστήματος

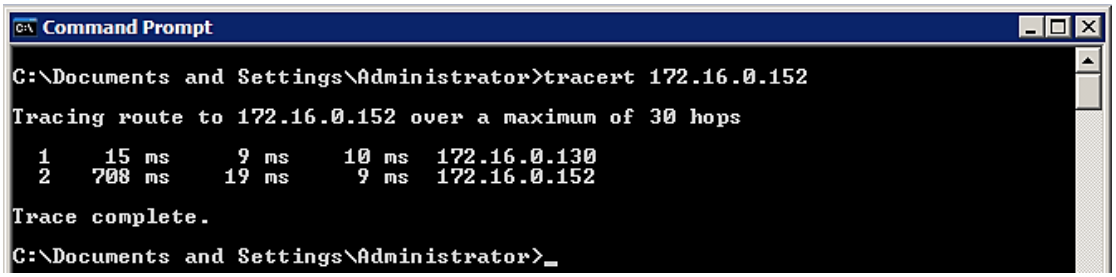
3. **Για τον user 1 του 1ου ορόφου:**



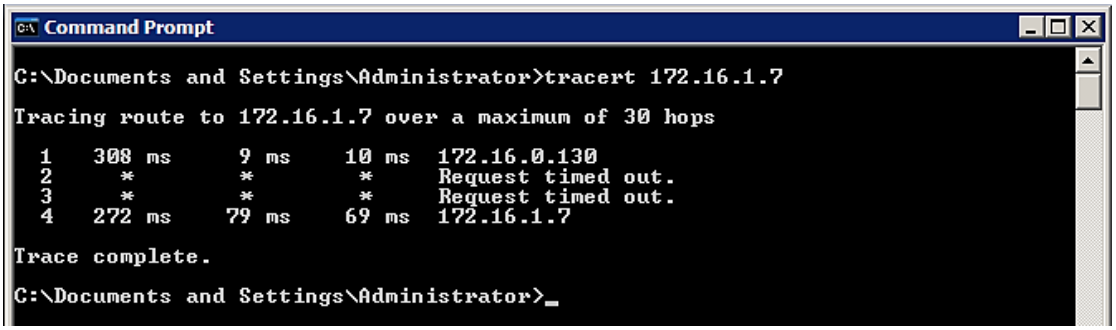
Εικόνα 5.85: Εκτέλεση tracert προς τον χρήστη του 3ου ορόφου



Εικόνα 5.86: Εκτέλεση tracert προς τον χρήστη του 2ου ορόφου

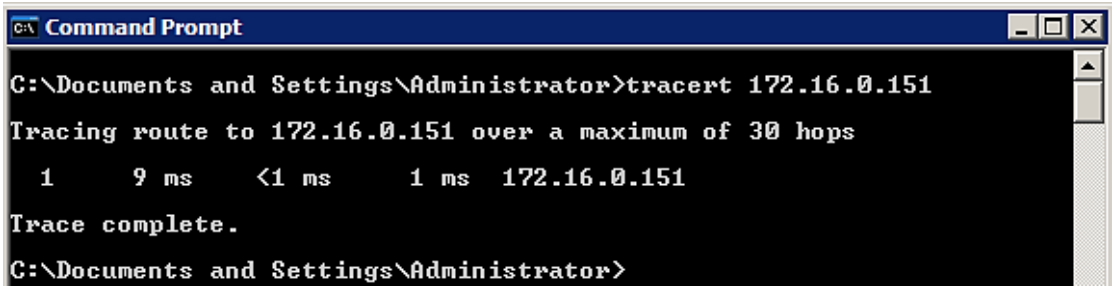


Εικόνα 5.87: Εκτέλεση tracert προς τον χρήστη του ισογείου

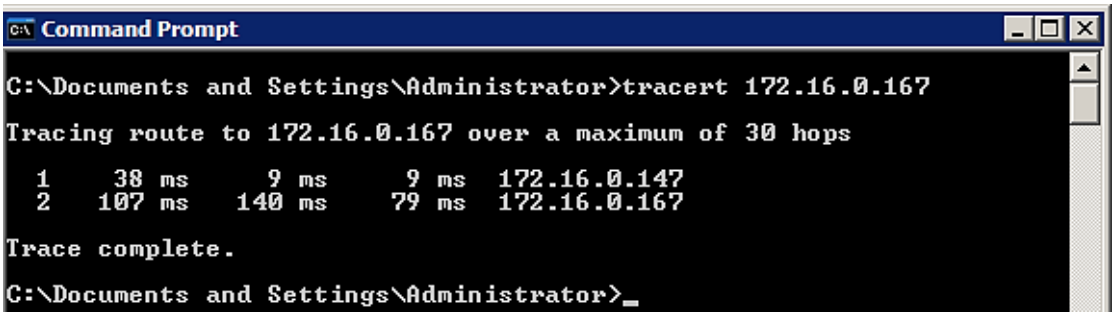


Εικόνα 5.88: Εκτέλεση tracert προς τον χρήστη του υποκαταστήματος

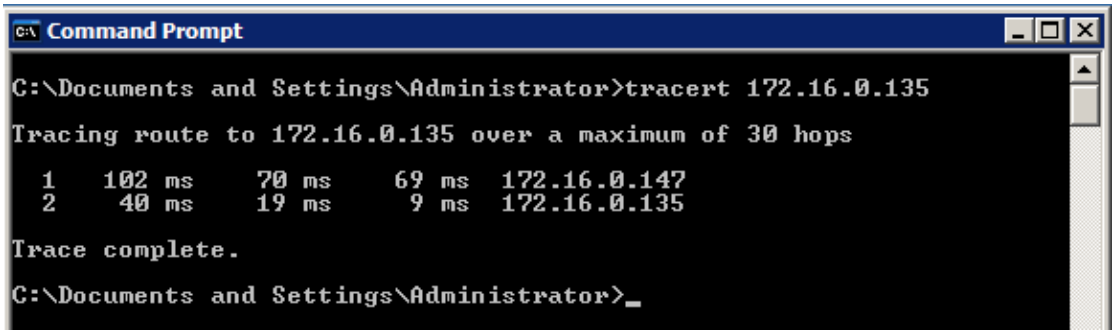
4. **Για τον user 1 του ισογείου:**



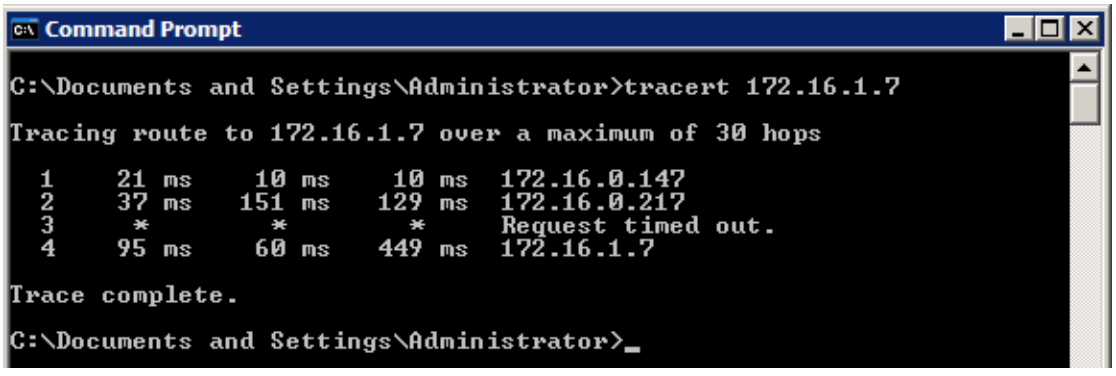
Εικόνα 5.89: Εκτέλεση tracert προς τον χρήστη του 3ου ορόφου



Εικόνα 5.90: Εκτέλεση tracert προς τον χρήστη του 2ου ορόφου

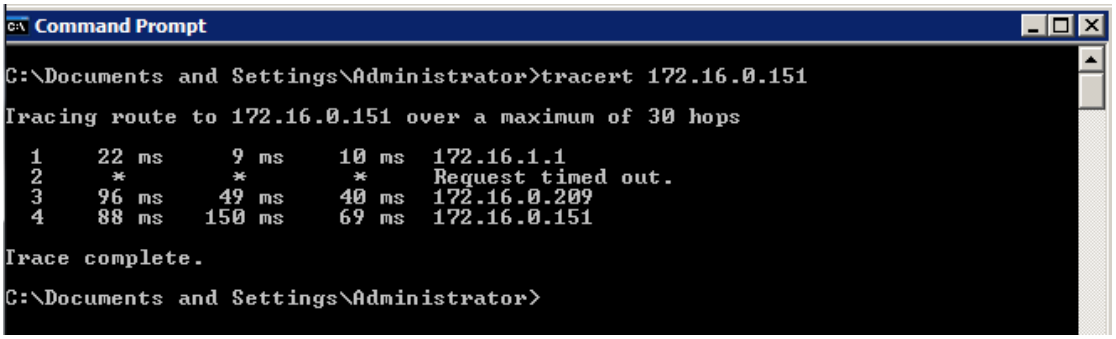


Εικόνα 5.91: Εκτέλεση tracert προς τον χρήστη του 1ου ορόφου

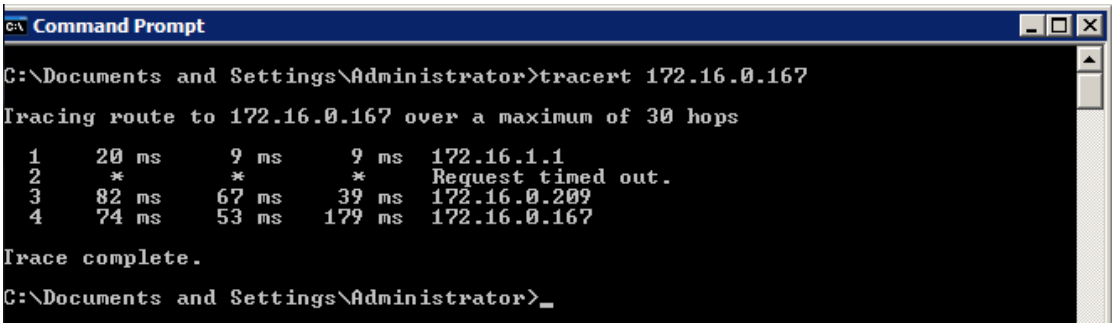


Εικόνα 5.92: Εκτέλεση tracert προς τον χρήστη του υποκαταστήματος

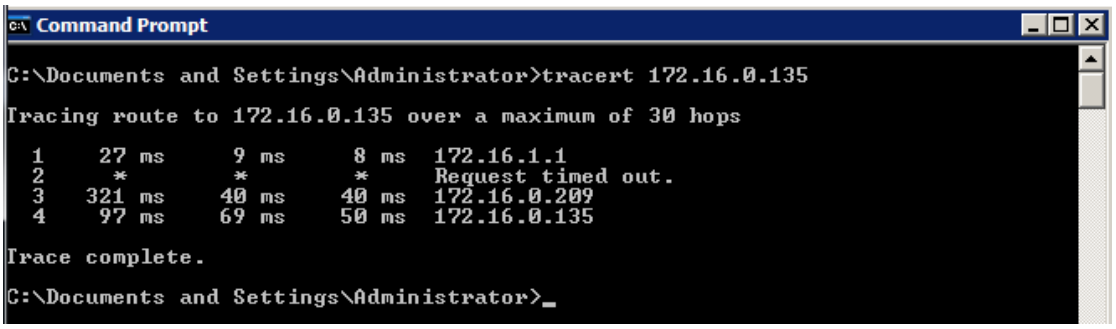
5. **Για τον user 1 του υποκαταστήματος:**



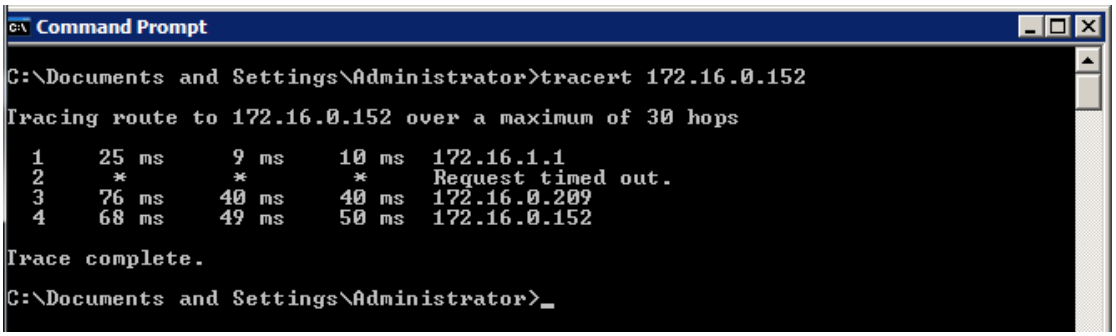
Εικόνα 5.93: Εκτέλεση tracert προς τον χρήστη του 3ου ορόφου



Εικόνα 5.94: Εκτέλεση tracert προς τον χρήστη του 2ου ορόφου



Εικόνα 5.95: Εκτέλεση tracert προς τον χρήστη του 1ου ορόφου



Εικόνα 5.96: Εκτέλεση tracert προς τον χρήστη του ισογείου

6. Συμπέρασμα για τα αποτελέσματα των traceroutes

Σε κάθε εκτέλεση της εντολής tracert, παρατηρούμε την διαδρομή που παίρνει ένα πακέτο για να φτάσει στον προορισμό του. Παρατηρούμε τα εξής:

1. Στην διαδικασία tracert έχουμε μία εγγραφή «Request timed out.». Αυτή είναι η έλλειψη απάντησης που έχουμε από το firewall αφού είναι ρυθμισμένο έτσι ώστε να μην απατάει σε ICMP πακέτα αυτού του τύπου. Ωστόσο, το tracert συνεχίζει και φτάνει στον προορισμό με επιτυχία.

2. Σε επικοινωνίες από το branch προς τα κεντρικά γραφεία, ποτέ δεν βλέπουμε την IP του ADSL router των κεντρικών γραφείων στην λίστα του tracert. Αντίστοιχα, σε επικοινωνίας από τα κεντρικά προς το branch, δεν βλέπουμε την IP του ADSL router του branch. Αυτό είναι λόγο του ότι υπάρχει το VPN tunnel στο οποίο μπαίνει το πακέτο στο πρώτο VPN router που συναντάει. Το πακέτο βρίσκεται εντός του tunnel μέχρι που βγει από το αντίστοιχο interface του απέναντι router. Στην ουσία του πακέτο δεν «αντιλαμβάνεται» το δεύτερο router του VPN tunnel κι έτσι δεν καταγράφεται στο tracert.

3. Οι διαδρομές είναι οι αναμενόμενες και συμπεραίνουμε ότι η δρομολόγηση σε όλη τη διαδρομή των παραπάνω επικοινωνιών πραγματοποιούνται σωστά.

5.7.4 Ρυθμίσεις των εξυπηρετητών (servers) του δικτύου

Όπως αναφέραμε προηγουμένως οι servers δεν είναι κι αυτοί τίποτε άλλο από εικονικά μηχανήματα που έχουμε δημιουργήσει και έχουν κι αυτά windows XP. Όπως είδαμε παραπάνω οι τερματικές συσκευές αποκτάνε δικτυακά στοιχεία μέσω DHCP ωστόσο, οι servers θα πρέπει να ρυθμιστούν με στατικές IP όπως προβλέπουν οι καλές πρακτικές του δικτύου. Κάθε server έχει δύο κάρτες δικτύου για εφεδρεία και κάθε κάρτα συνδέεται σε ένα από τα δύο server switches. Για να λειτουργήσει αυτή η διάταξη, θα χρειαστούν δύο IP διευθύνσεις για κάθε server, δηλαδή, μία για κάθε κάρτα δικτύου.

Στον παρακάτω πίνακα απεικονίζονται οι διευθύνσεις που θα χρησιμοποιηθούν:

A/A	Server	IP 1ης Κάρτας	IP 2ης Κάρτας	Subnet Mask	Default gateway
1	Communication Server	172.16.0.180	172.16.0.181	255.255.255.240	172.16.0.177
2	Print Server	172.16.0.182	172.16.0.183	255.255.255.240	172.16.0.177
3	Database Server	172.16.0.184	172.16.0.185	255.255.255.240	172.16.0.177
4	File Server	172.16.0.186	172.16.0.187	255.255.255.240	172.16.0.177

Πίνακας 5.4: Ενδεικτικός πίνακας διευθύνσεων IP που θα αναθέσουμε στους servers του δικτύου

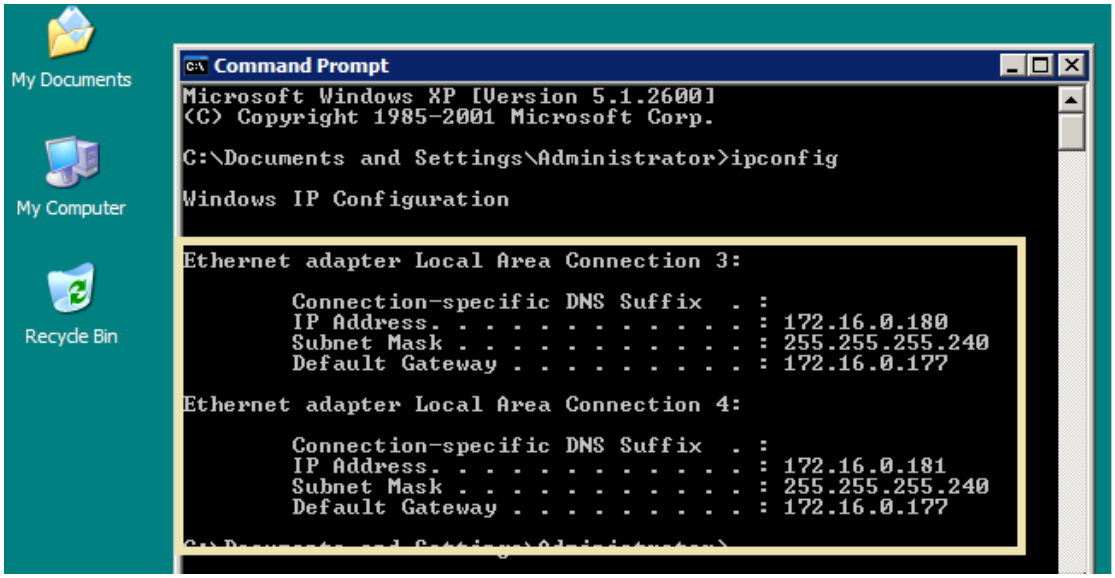
Αφού εισάγουμε τις IP διευθύνσεις στους servers του δικτύου θα προχωρήσουμε στους ίδιους ελέγχους με αυτούς που εφαρμόσαμε και στους χρήστες. Δηλαδή θα ελέγξουμε τις IP διευθύνσεις τους και θα εφαρμόσουμε ελέγχους επικοινωνίας ping από τους χρήστες προς τους servers. Στον πίνακα 5.5 εμφανίζονται αναλυτικά οι έλεγχοι που θα εφαρμόσουμε για να ελέγξουμε την σωστή λειτουργία των servers.

Έλεγχοι των servers				
Servers	**Έλεγχος έγκυρης IP**		**Έλεγχος ping από user σε user**	**Έλεγχος ping από user σε user**
Communication Server	**Κάρτα δικτύου 1**	**Κάρτα δικτύου 2**	**Κάρτα δικτύου 1**	**Κάρτα δικτύου 2**
	✓	✓	✓	✓
Print Server	✓	✓	✓	✓
Database Server	✓	✓	✓	✓
File Server	✓	✓	✓	✓

Πίνακας 5.5: Ενδεικτικός έλεγχοι που θα εφαρμόσουμε για τους servers του δικτύου μας

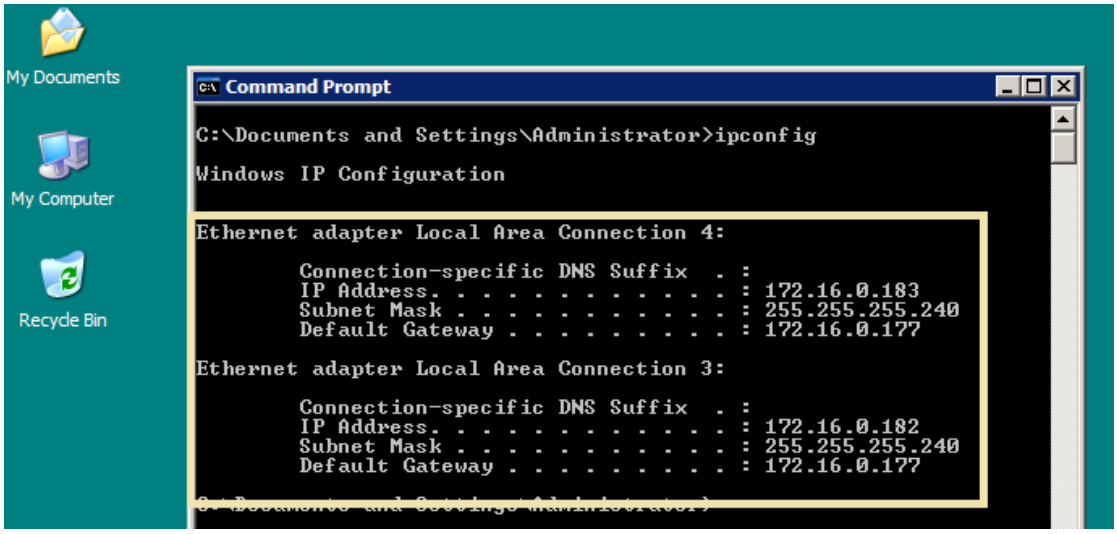
Έλεγχος έγκυρης IP διεύθυνσης

Communication Server



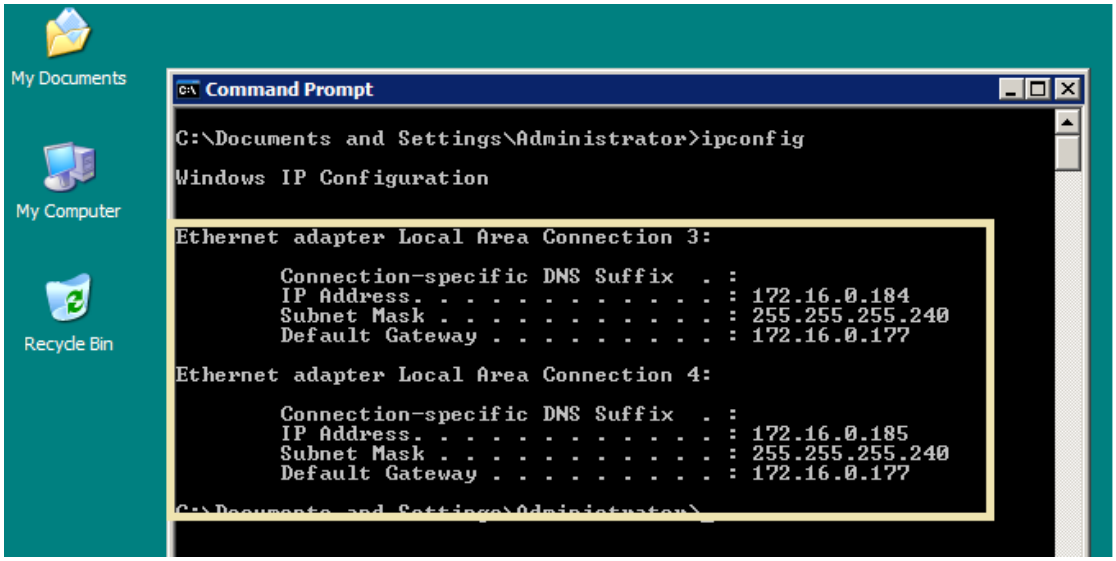
Εικόνα 5.97: Εκτέλεση ipconfig στο CMD του Communication Server

Print Server



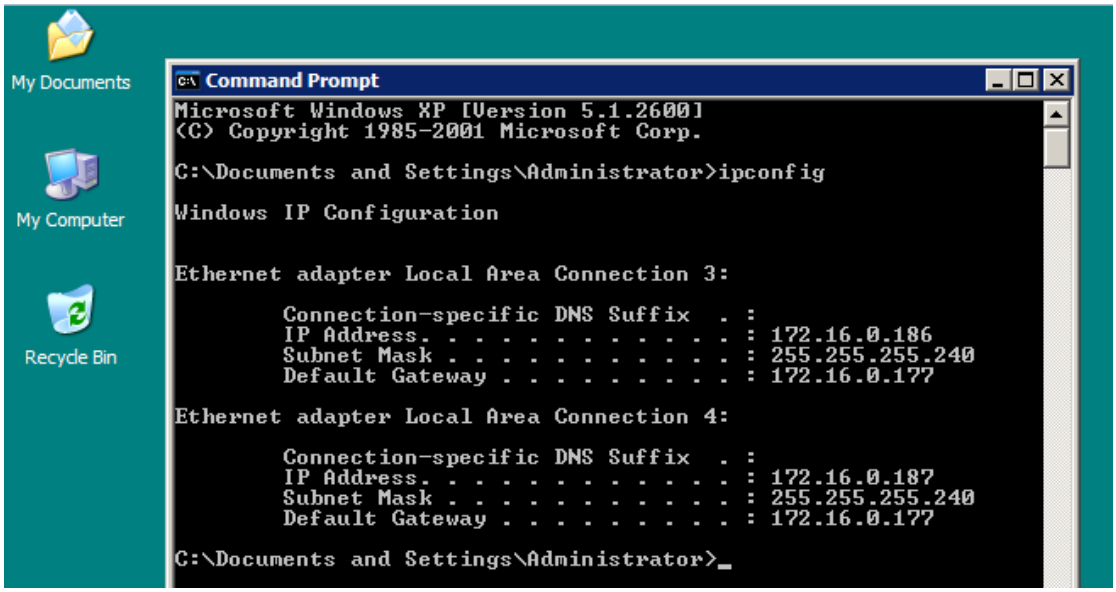
Εικόνα 5.98: Εκτέλεση ipconfig στο CMD του Print Server

Database Server



Εικόνα 5.99: Εκτέλεση ipconfig στο CMD του Database Server

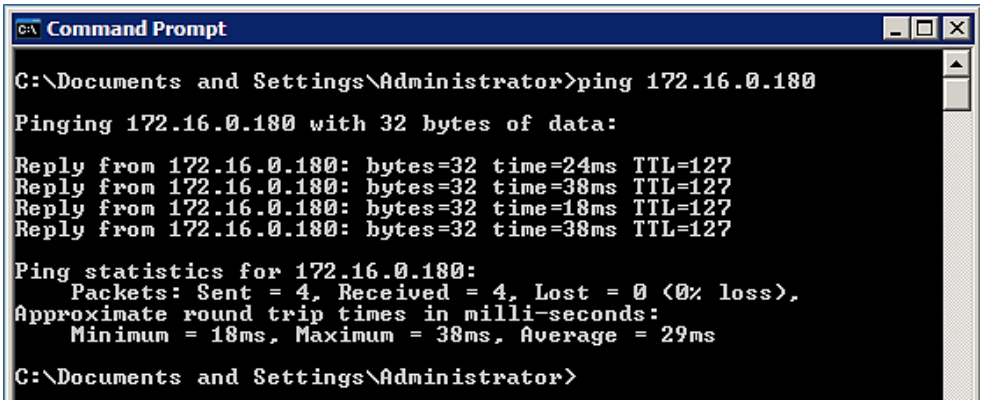
File Server



Εικόνα 5.100: Εκτέλεση ipconfig στο CMD του File Server

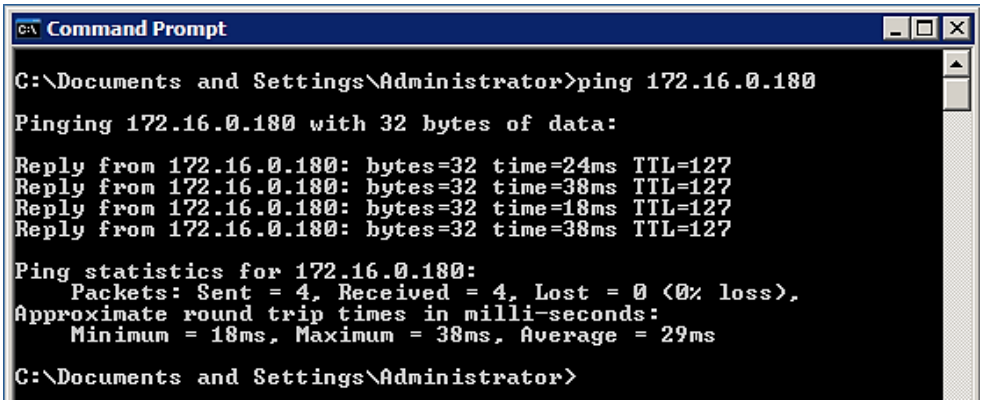
Έλεγχος επικοινωνίας ping από server προς χρήστες

User 1 3rd floor → Communication Server (κάρτα δικτύου 1)



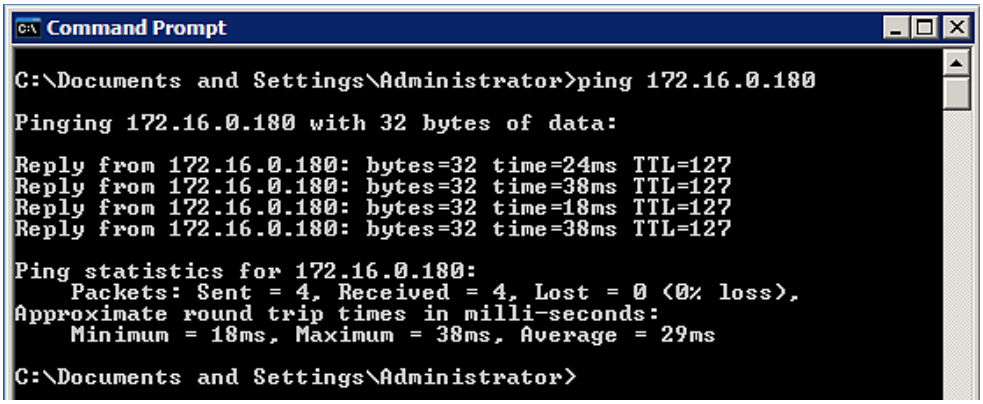
Εικόνα 5.101: Εκτέλεση ping από τον χρήστη του 3ου ορόφου προς τον Communication Server (NIC 1)

User 1 2nd floor → Communication Server (κάρτα δικτύου 1)



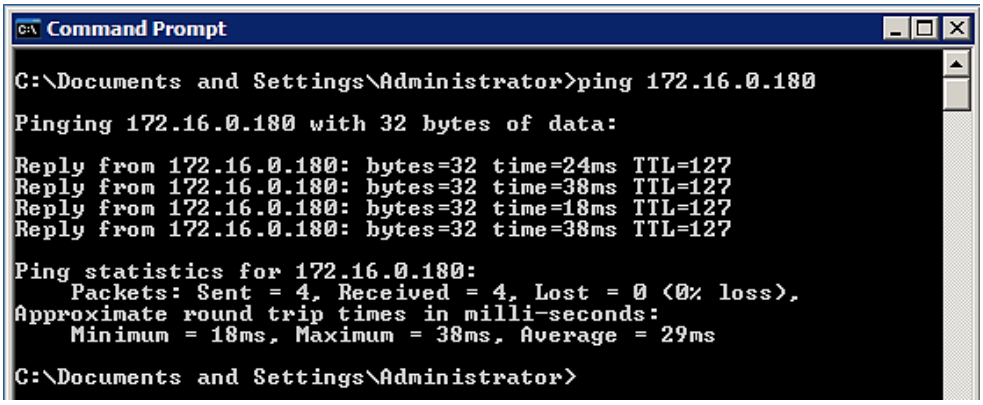
Εικόνα 5.102: Εκτέλεση ping από τον χρήστη του 2ου ορόφου προς τον Communication Server (NIC 1)

User 1 1st floor → Communication Server (κάρτα δικτύου 1)



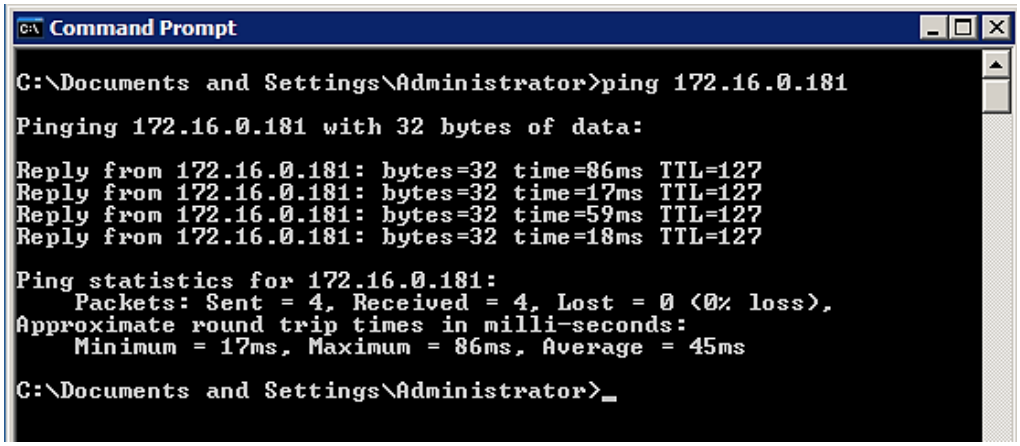
Εικόνα 5.103: Εκτέλεση ping από τον χρήστη του 1ου ορόφου προς τον Communication Server (NIC 1)

User 1 ground floor → Communication Server (κάρτα δικτύου 1)



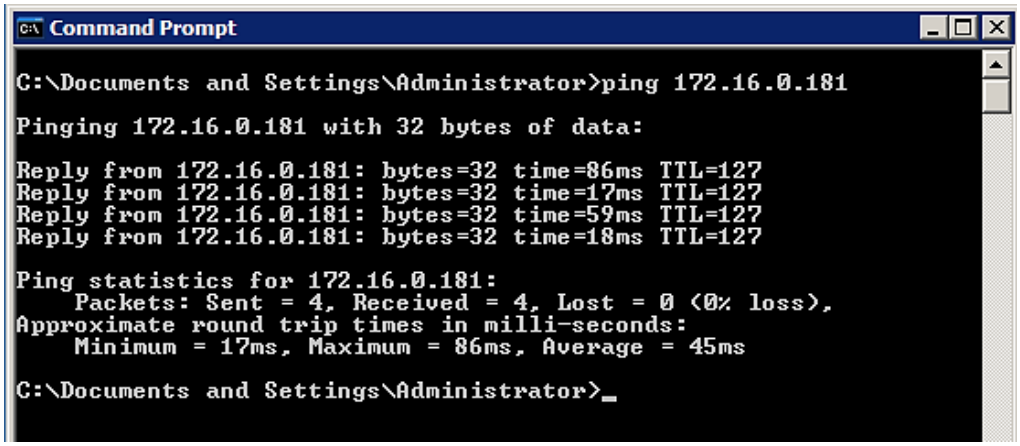
Εικόνα 5.104: Εκτέλεση ping από τον χρήστη του ισογείου προς τον Communication Server (NIC 1)

User 1 branch → Communication Server (κάρτα δικτύου 1)



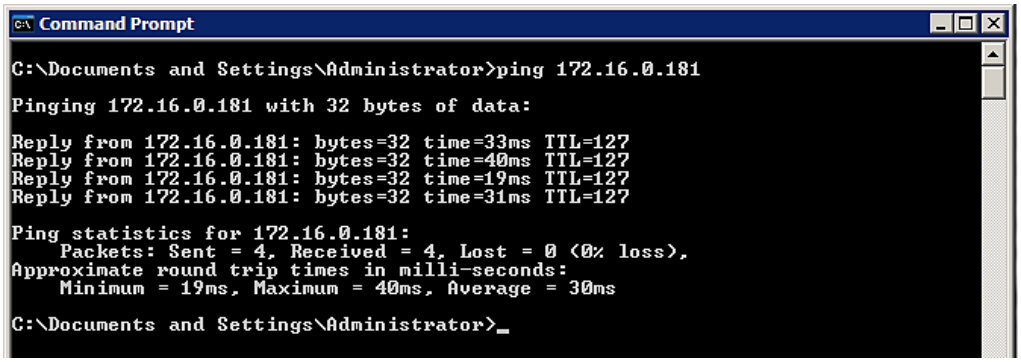
Εικόνα 5.105: Εκτέλεση ping από τον χρήστη του υποκαταστήματος προς τον Communication Server (NIC 1)

User 1 3rd floor → Communication Server (κάρτα δικτύου 2)



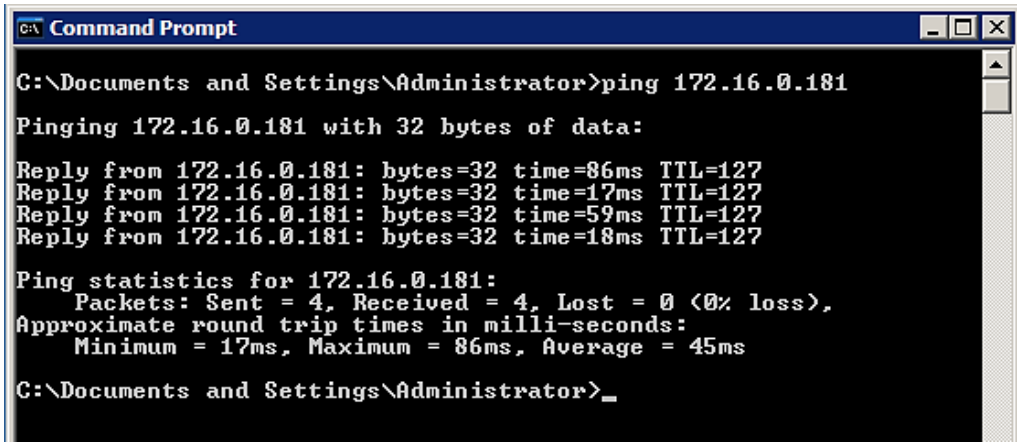
Εικόνα 5.106: Εκτέλεση ping από τον χρήστη του 3ου ορόφου προς τον Communication Server (NIC 2)

User 1 2nd floor → Communication Server (κάρτα δικτύου 2)



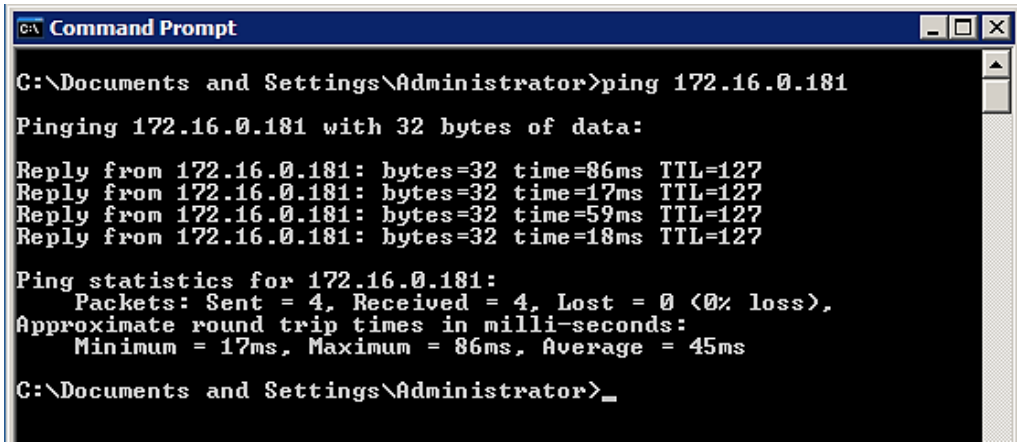
Εικόνα 5.107: Εκτέλεση ping από τον χρήστη του 2ου ορόφου προς τον Communication Server (NIC 2)

User 1 1st floor → Communication Server (κάρτα δικτύου 2)



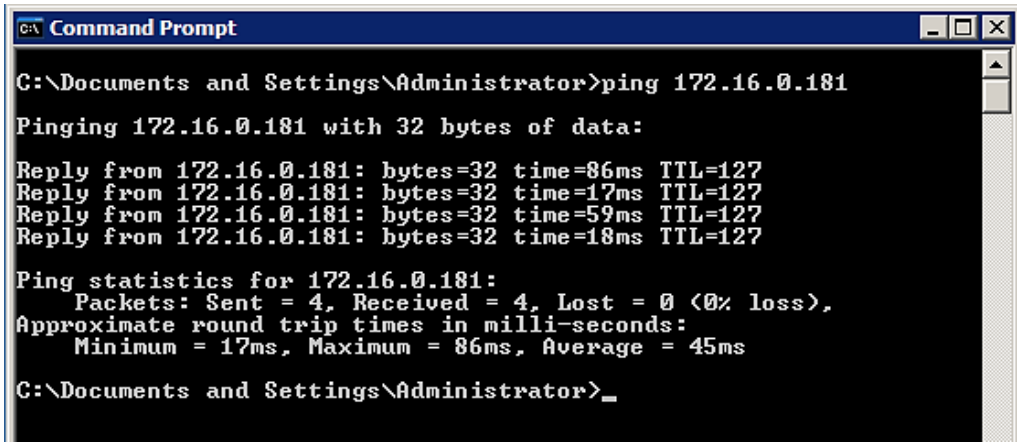
Εικόνα 5.108: Εκτέλεση ping από τον χρήστη του 1ου ορόφου προς τον Communication Server (NIC 2)

User 1 ground floor → Communication Server (κάρτα δικτύου 2)



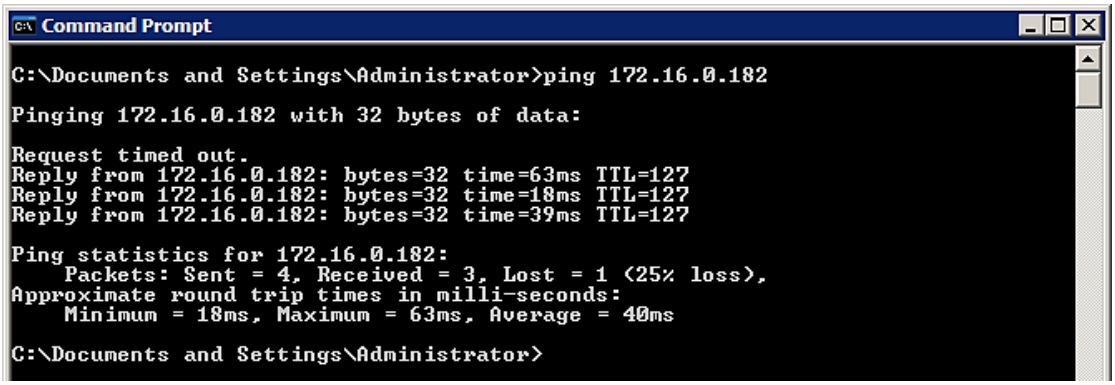
Εικόνα 5.109: Εκτέλεση ping από τον χρήστη του ισογείου προς τον Communication Server (NIC 2)

User 1 branch → Communication Server (κάρτα δικτύου 2)



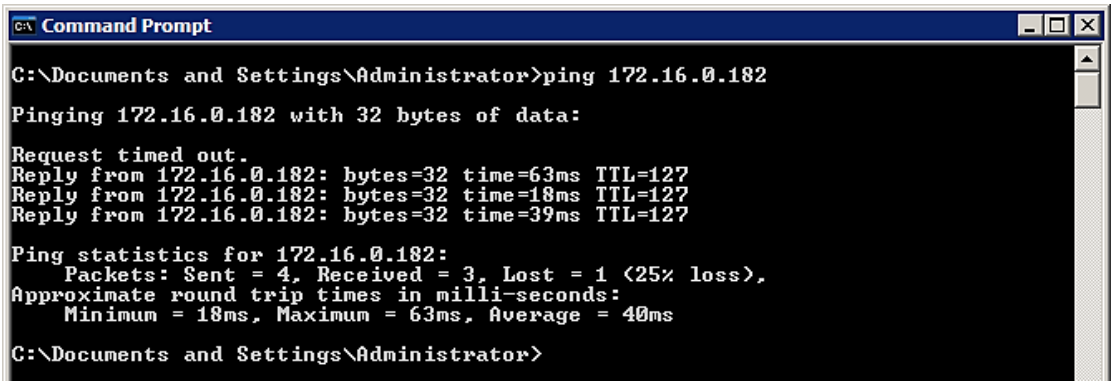
Εικόνα 5.110: Εκτέλεση ping από τον χρήστη του υποκαταστήματος προς τον Communication Server (NIC 2)

User 1 3rd floor → Print Server (κάρτα δικτύου 1)



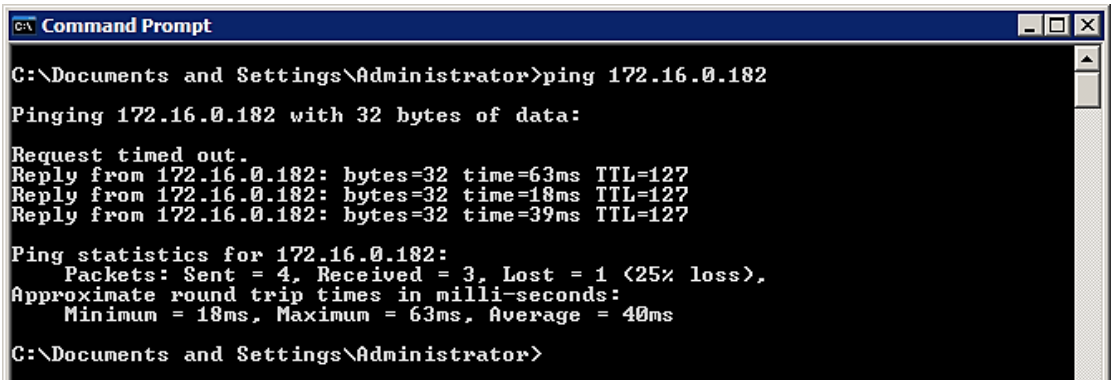
Εικόνα 5.111: Εκτέλεση ping από τον χρήστη του 3ου ορόφου προς τον Print Server (NIC 1)

User 1 2nd floor → Print Server (κάρτα δικτύου 1)



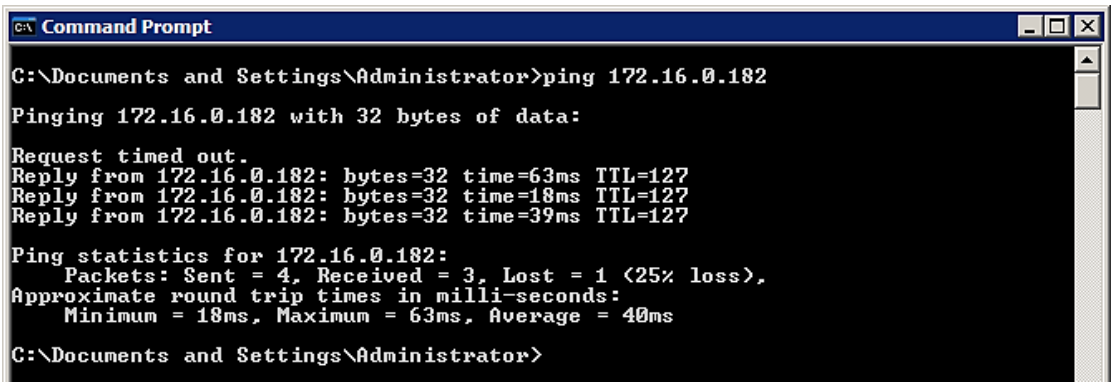
Εικόνα 5.112: Εκτέλεση ping από τον χρήστη του 2ου ορόφου προς τον Print Server (NIC 1)

User 1 1st floor → Print Server (κάρτα δικτύου 1)



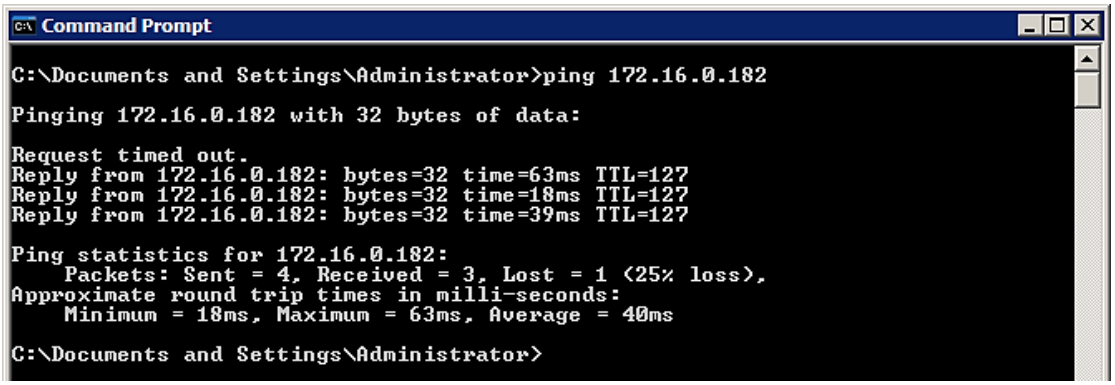
Εικόνα 5.113: Εκτέλεση ping από τον χρήστη του 1ου ορόφου προς τον Print Server (NIC 1)

User 1 ground floor → Print Server (κάρτα δικτύου 1)



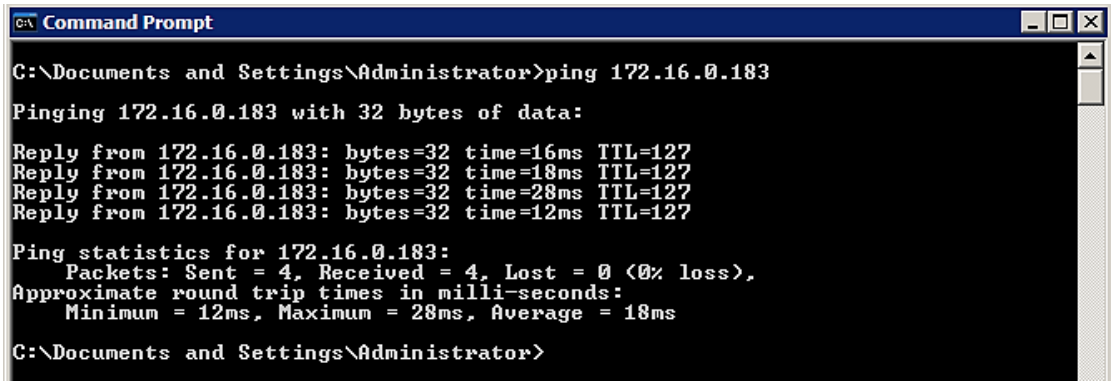
Εικόνα 5.114: Εκτέλεση ping από τον χρήστη του ισογείου προς τον Print Server (NIC 1)

User 1 branch → Print Server (κάρτα δικτύου 1)



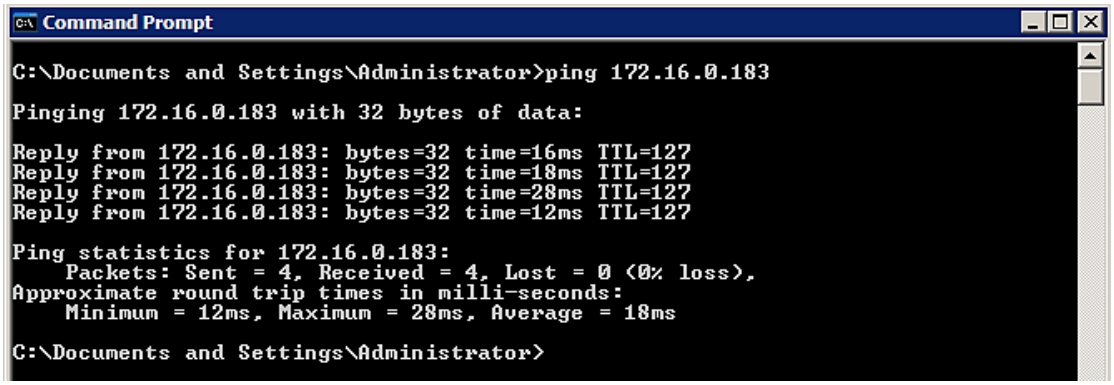
Εικόνα 5.115: Εκτέλεση ping από τον χρήστη του υποκαταστήματος προς τον Print Server (NIC 1)

User 1 3rd floor → Print Server (κάρτα δικτύου 2)



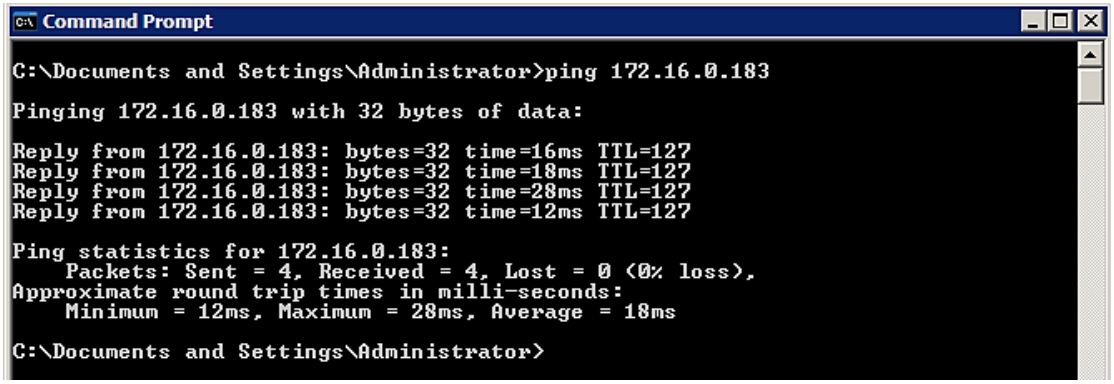
Εικόνα 5.116: Εκτέλεση ping από τον χρήστη του 3ου ορόφου προς τον Print Server (NIC 2)

User 1 2nd floor → Print Server (κάρτα δικτύου 2)



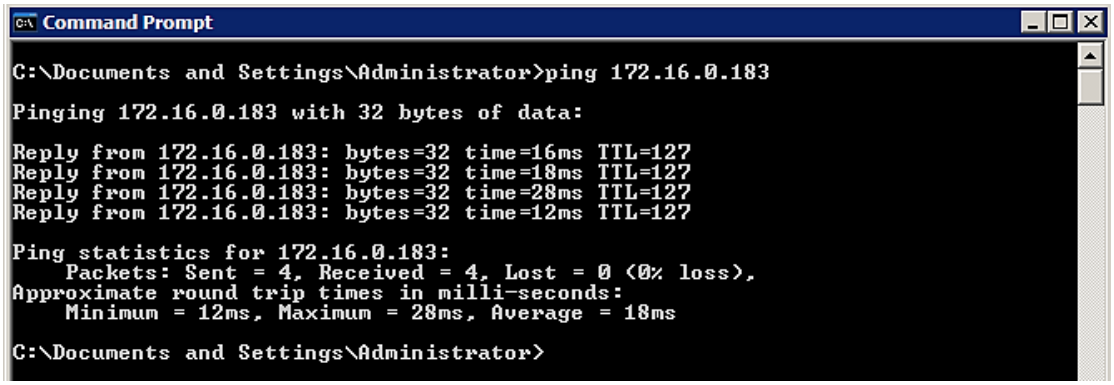
Εικόνα 5.117: Εκτέλεση ping από τον χρήστη του 2ου ορόφου προς τον Print Server (NIC 2)

User 1 1st floor → Print Server (κάρτα δικτύου 2)



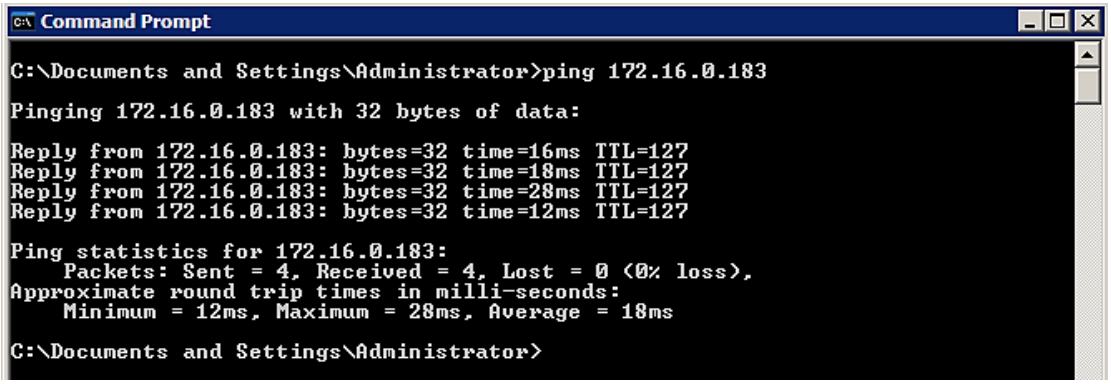
Εικόνα 5.118: Εκτέλεση ping από τον χρήστη του 1ου ορόφου προς τον Print Server (NIC 2)

User 1 ground floor → Print Server (κάρτα δικτύου 2)



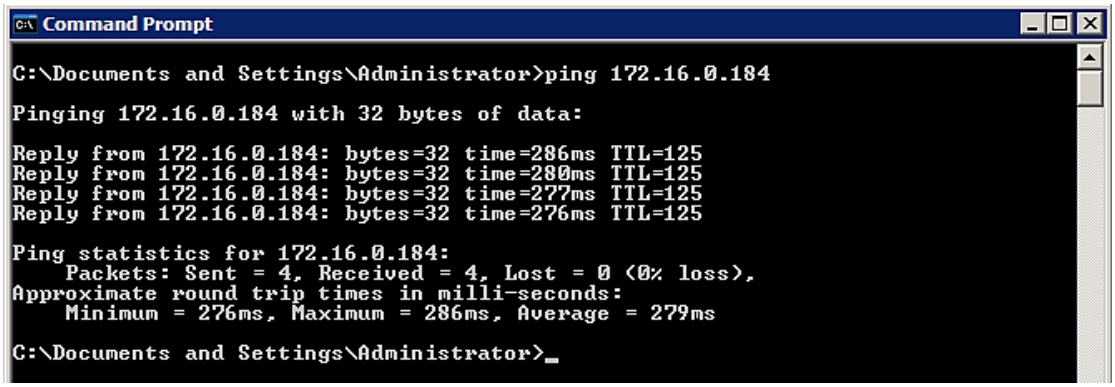
Εικόνα 5.119: Εκτέλεση ping από τον χρήστη του ισογείου προς τον Print Server (NIC 2)

User 1 branch → Print Server (κάρτα δικτύου 2)



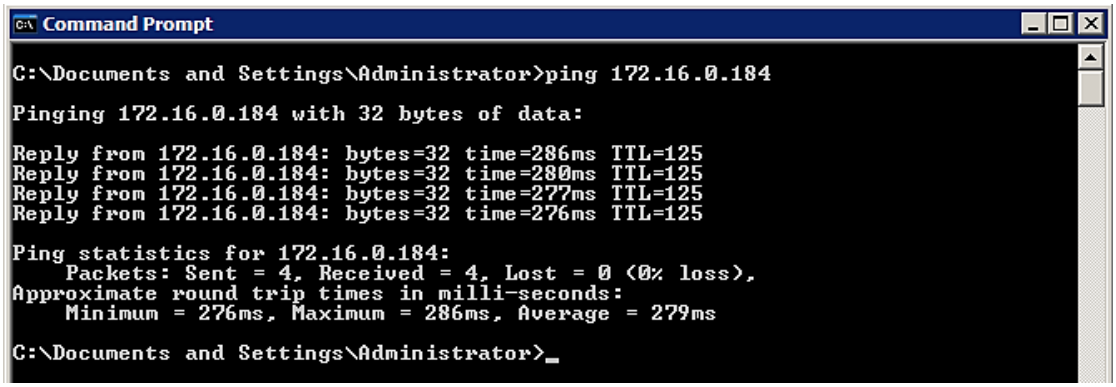
Εικόνα 5.120: Εκτέλεση ping από τον χρήστη του υποκαταστήματος προς τον Print Server (NIC 2)

User 1 3rd floor → Database Server (κάρτα δικτύου 1)



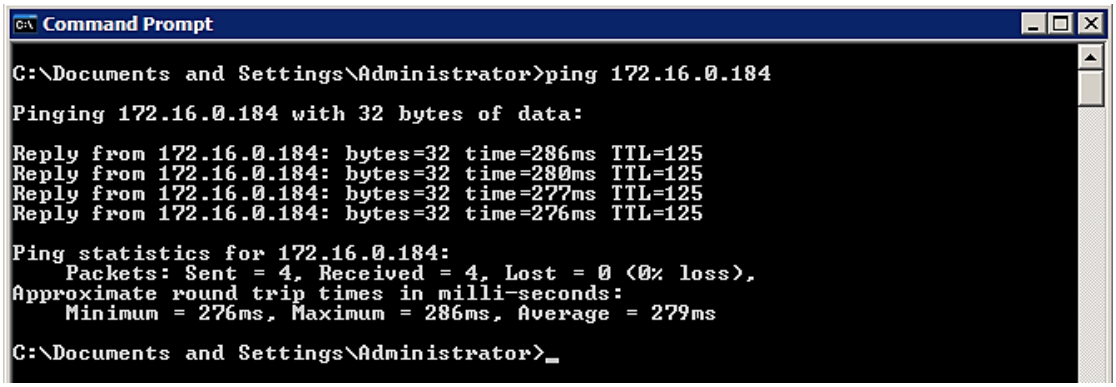
Εικόνα 5.121: Εκτέλεση ping από τον χρήστη του 3ου ορόφου προς τον database Server (NIC 1)

User 1 2 nd floor → Database Server (κάρτα δικτύου 1)



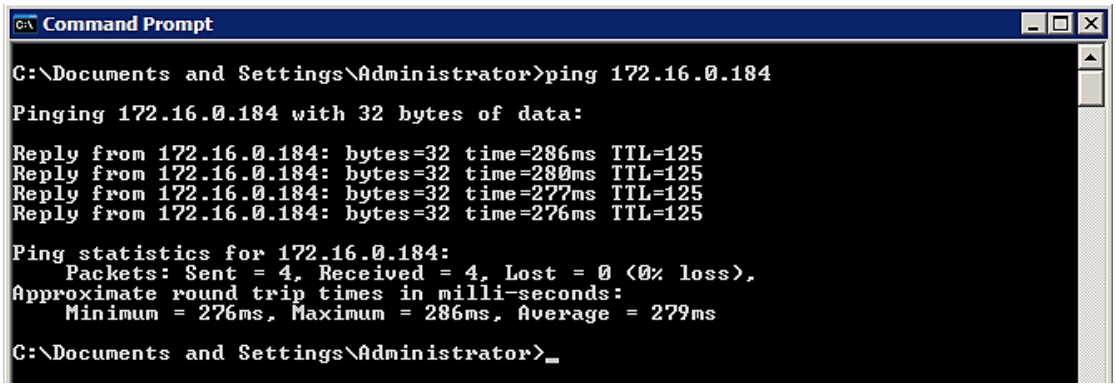
Εικόνα 5.122: Εκτέλεση ping από τον χρήστη του 2ου ορόφου προς τον database Server (NIC 1)

User 1 1st floor → Database Server (κάρτα δικτύου 1)



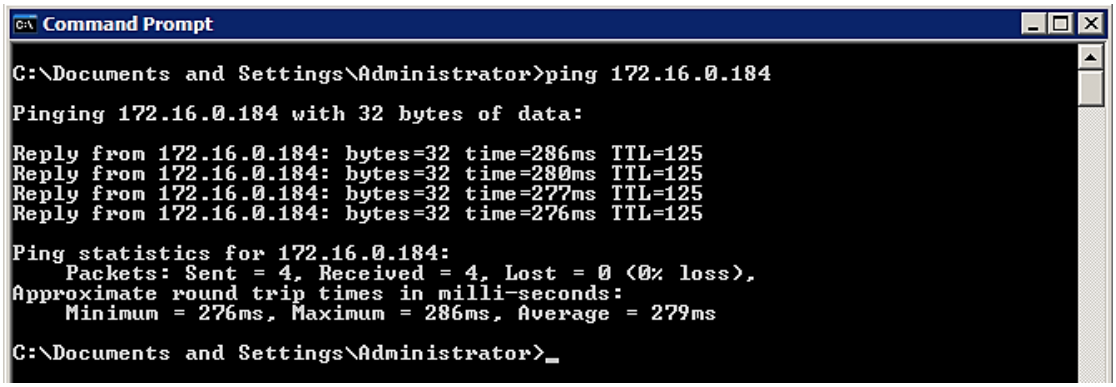
Εικόνα 5.123: Εκτέλεση ping από τον χρήστη του 1ου ορόφου προς τον database Server (NIC 1)

User 1 ground floor → Database Server (κάρτα δικτύου 1)



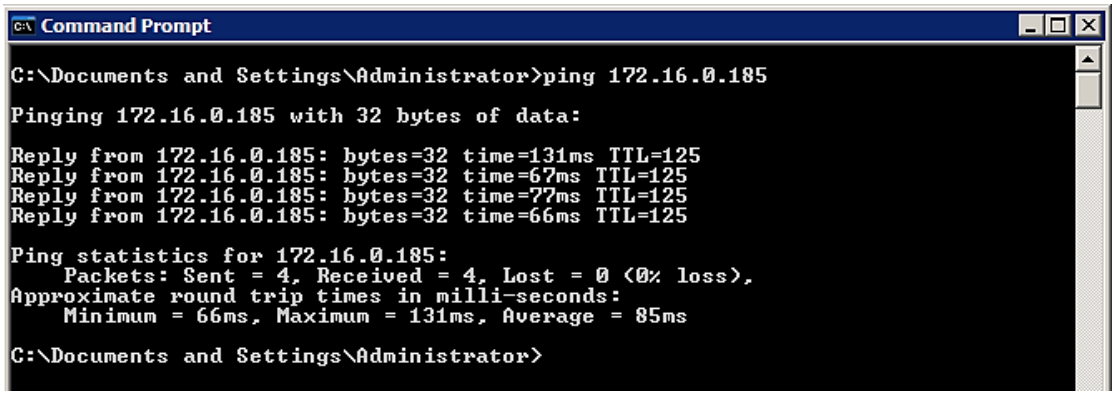
Εικόνα 5.124: Εκτέλεση ping από τον χρήστη του ισογείου προς τον database Server (NIC 1)

User 1 branch → Database Server (κάρτα δικτύου 1)



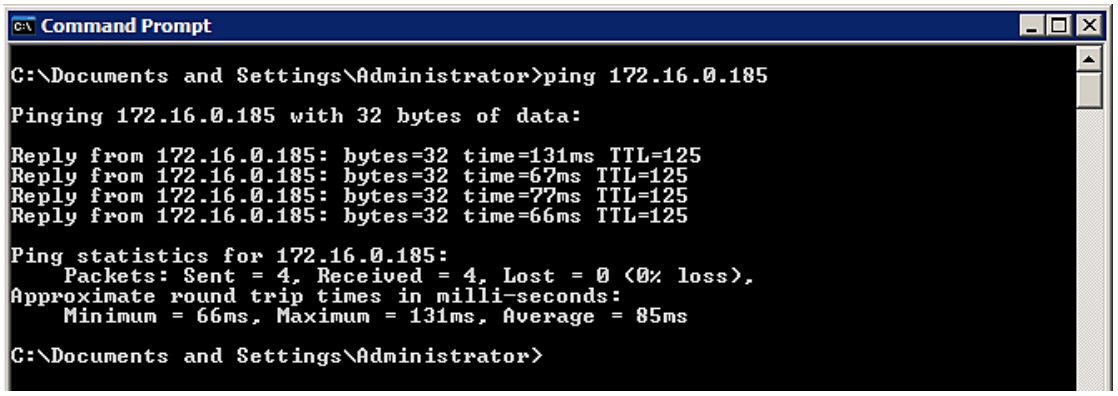
Εικόνα 5.125: Εκτέλεση ping από τον χρήστη του υποκαταστήματος προς τον database Server (NIC 1)

User 1 3rd floor → Database Server (κάρτα δικτύου 2)



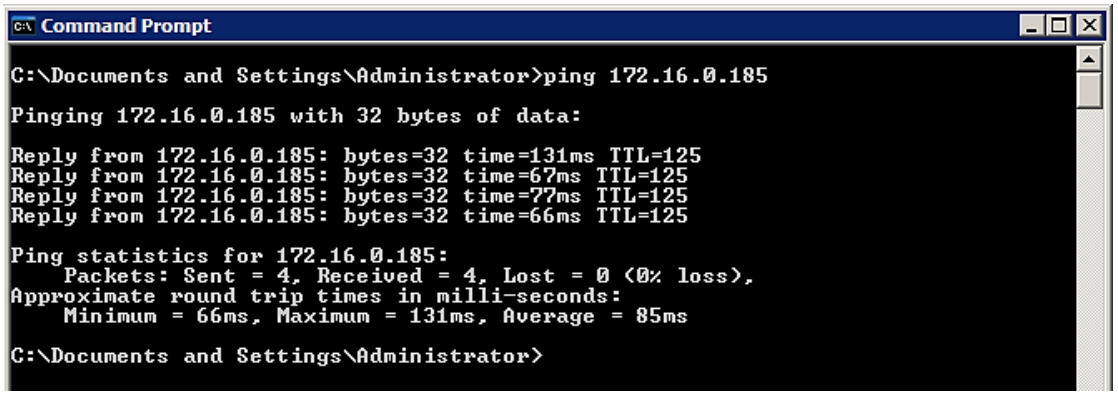
Εικόνα 5.126: Εκτέλεση ping από τον χρήστη του 3ου ορόφου προς τον database Server (NIC 2)

User 1 2 nd floor → Database Server (κάρτα δικτύου 2)



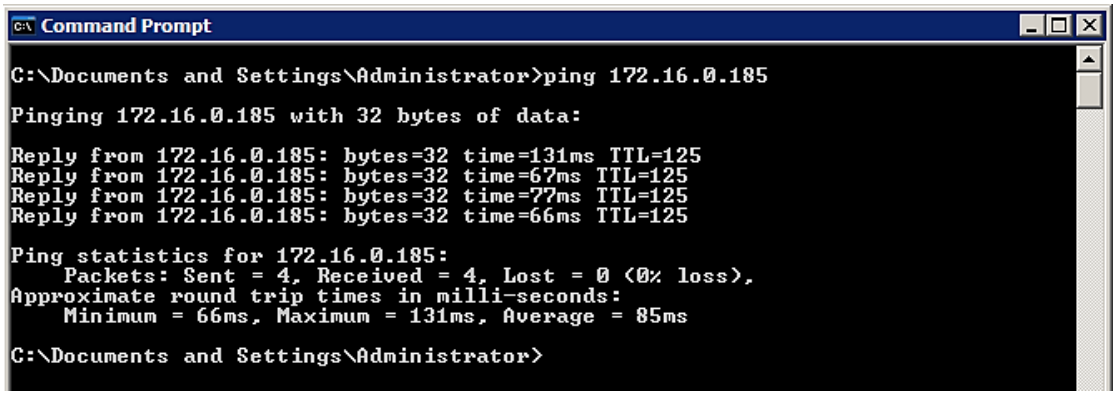
Εικόνα 5.127: Εκτέλεση ping από τον χρήστη του 2ου ορόφου προς τον database Server (NIC 2)

User 1 1st floor → Database Server (κάρτα δικτύου 2)



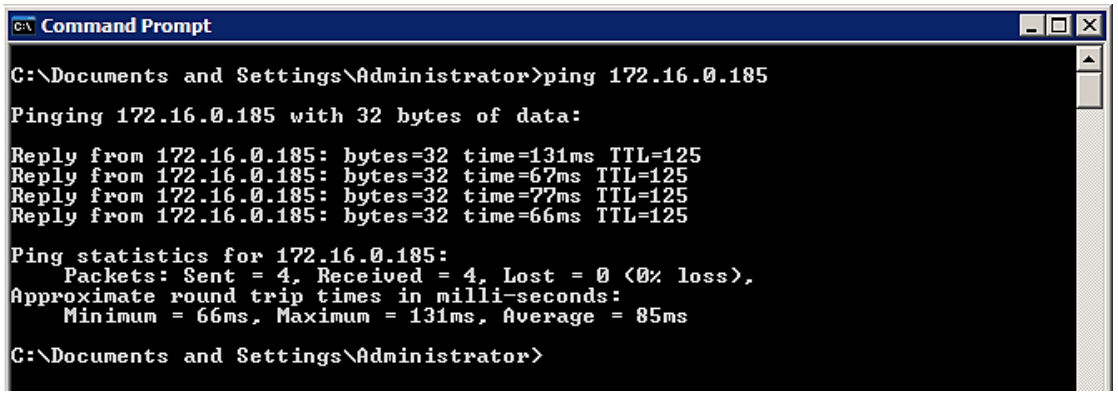
Εικόνα 5.128: Εκτέλεση ping από τον χρήστη του 1ου ορόφου προς τον database Server (NIC 2)

User 1 ground floor → Database Server (κάρτα δικτύου 2)



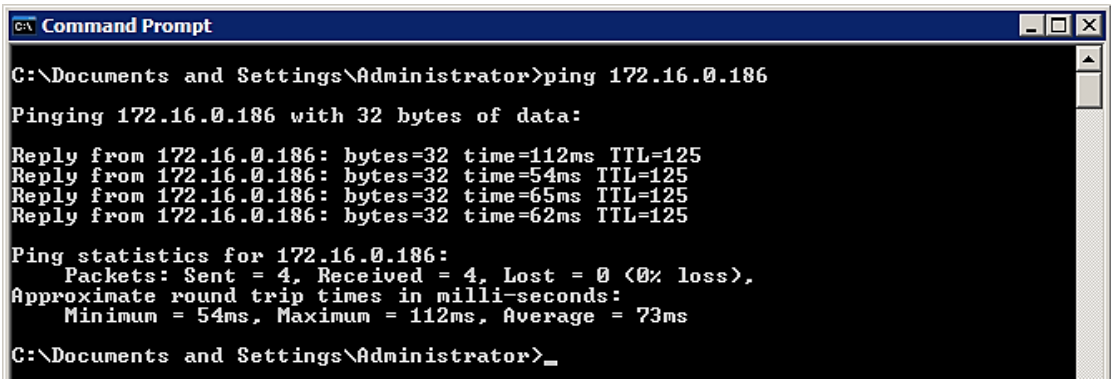
Εικόνα 5.129: Εκτέλεση ping από τον χρήστη του ισογείου προς τον database Server (NIC 2)

User 1 branch → Database Server (κάρτα δικτύου 2)



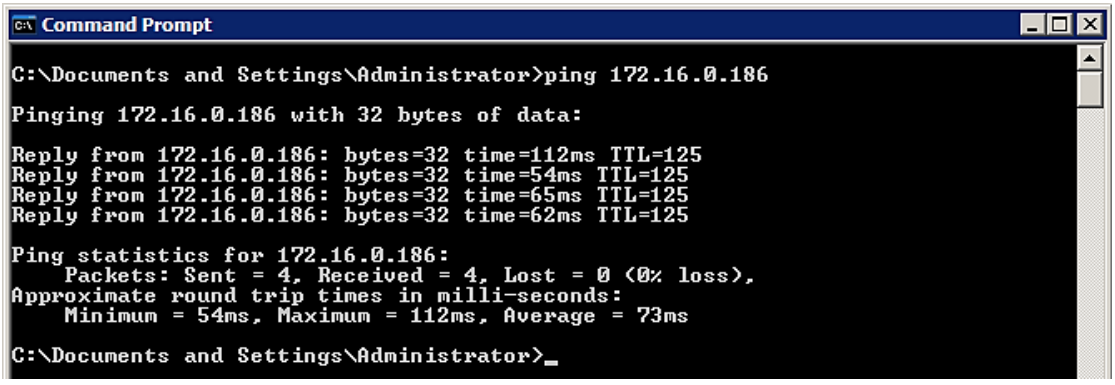
Εικόνα 5.130: Εκτέλεση ping από τον χρήστη του υποκαταστήματος προς τον database Server (NIC 2)

User 1 3rd floor → File Server (κάρτα δικτύου 1)



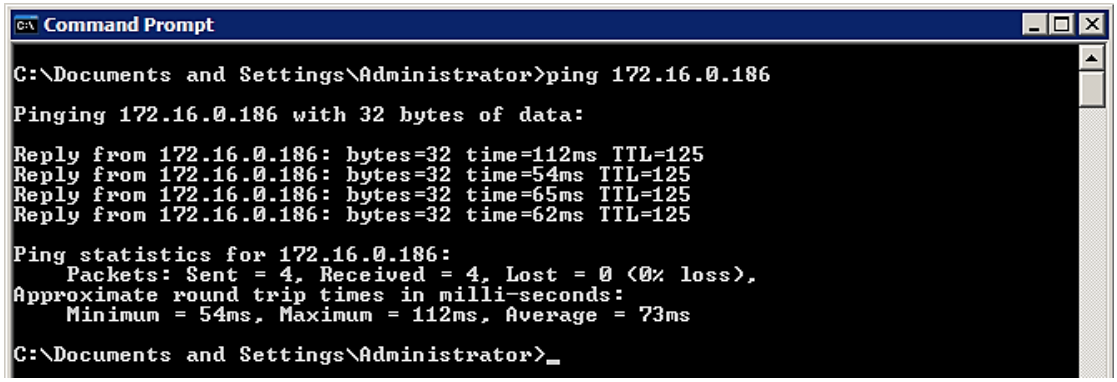
Εικόνα 5.131: Εκτέλεση ping από τον χρήστη του 3ου ορόφου προς τον file Server (NIC 1)

User 1 2 nd floor → File Server (κάρτα δικτύου 1)



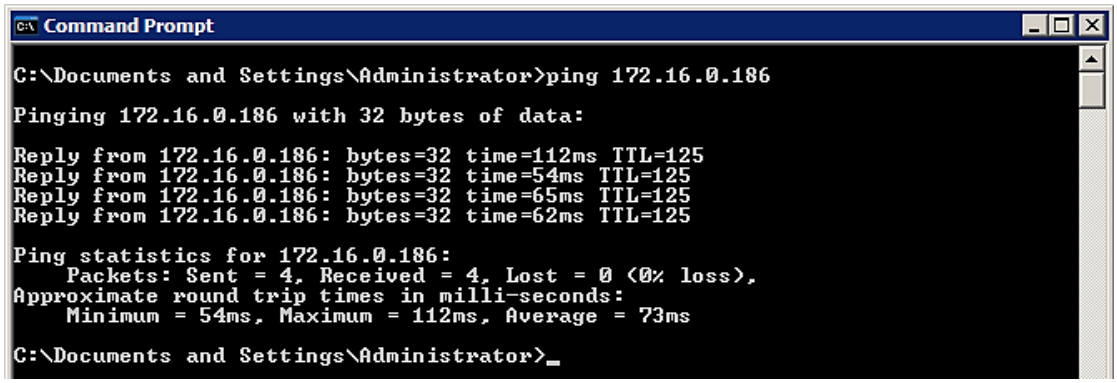
Εικόνα 5.132: Εκτέλεση ping από τον χρήστη του 2ου ορόφου προς τον file Server (NIC 1)

User 1 1st floor → File Server (κάρτα δικτύου 1)



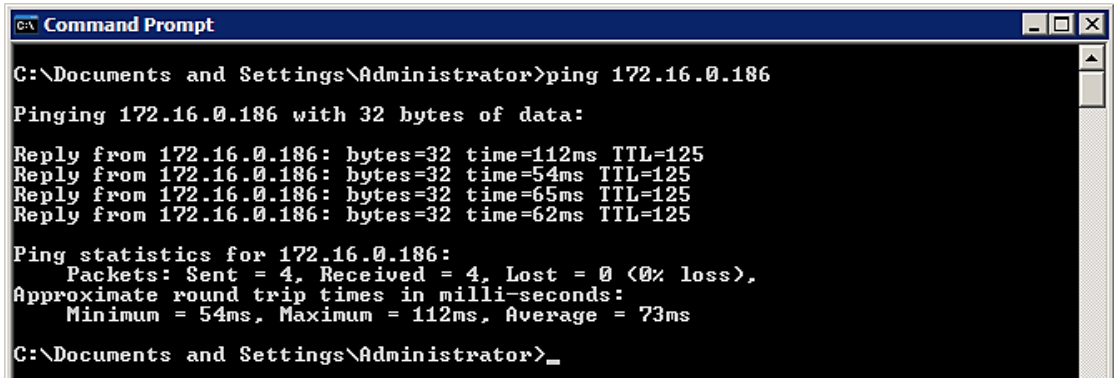
Εικόνα 5.133: Εκτέλεση ping από τον χρήστη του 1ου ορόφου προς τον file Server (NIC 1)

User 1 ground floor → File Server (κάρτα δικτύου 1)



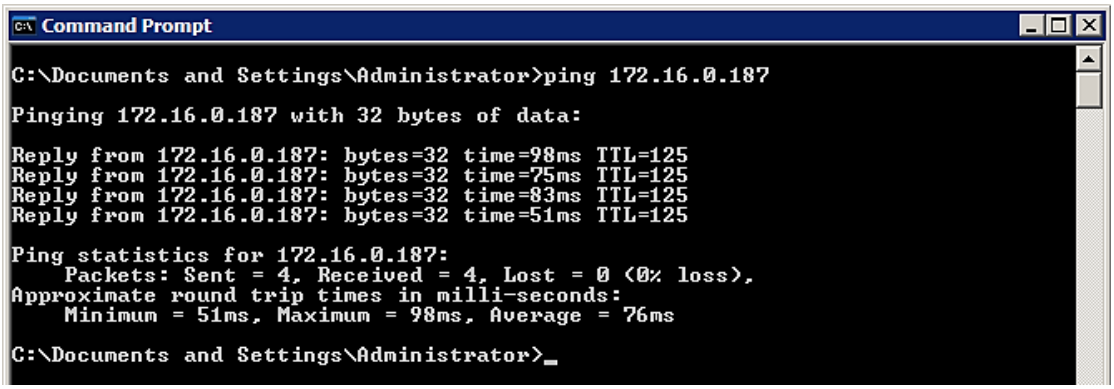
Εικόνα 5.134: Εκτέλεση ping από τον χρήστη του ισογείου προς τον file Server (NIC 1)

User 1 branch → File Server (κάρτα δικτύου 1)



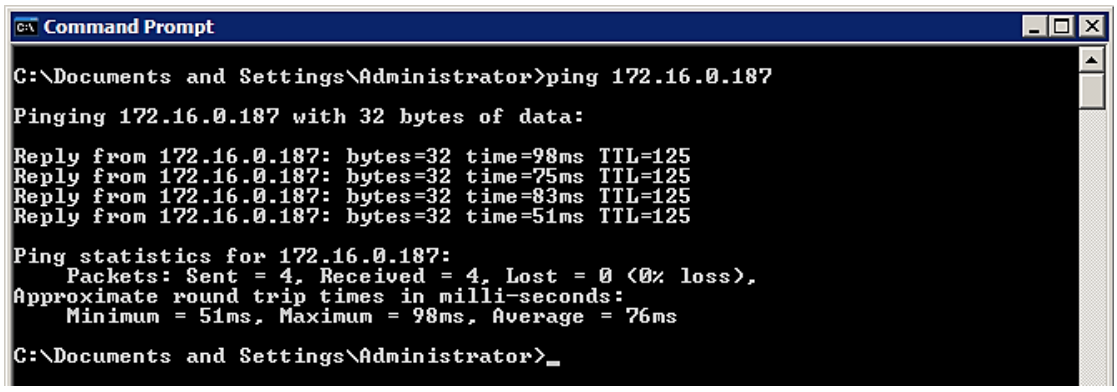
Εικόνα 5.135: Εκτέλεση ping από τον χρήστη του υποκαταστήματος προς τον file Server (NIC 1)

User 1 3rd floor → File Server (κάρτα δικτύου 2)



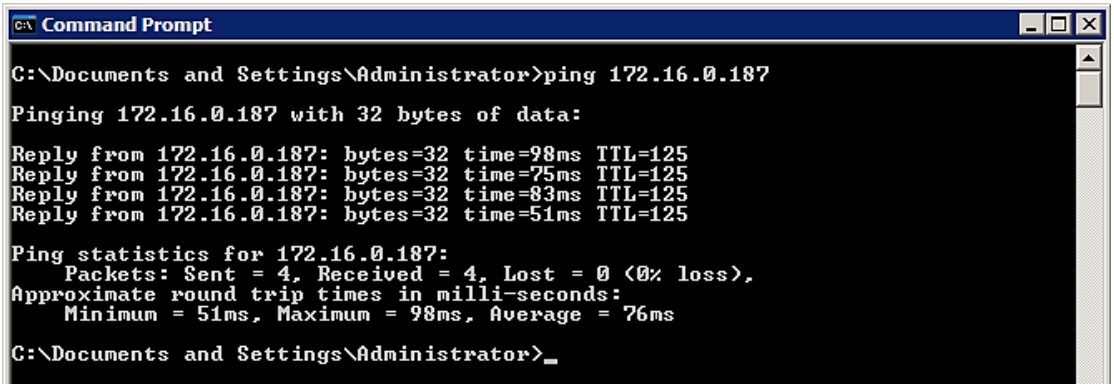
Εικόνα 5.136: Εκτέλεση ping από τον χρήστη του 3ου ορόφου προς τον file Server (NIC 2)

User 1 2 nd floor → File Server (κάρτα δικτύου 2)



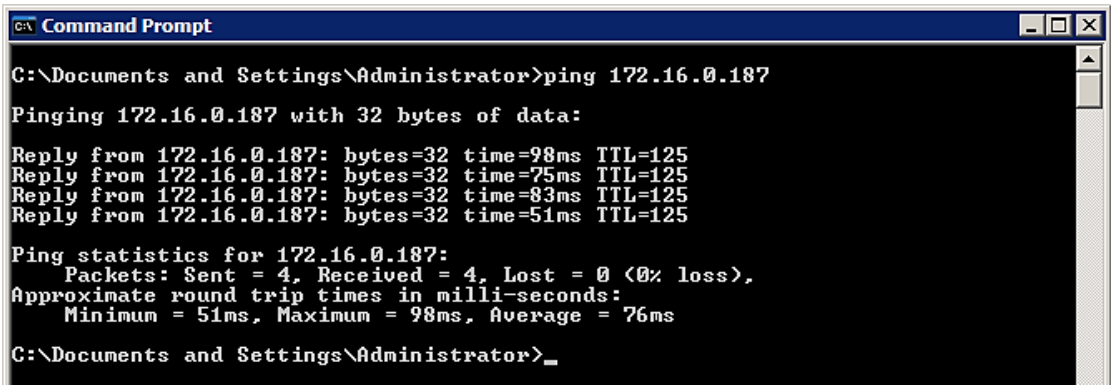
Εικόνα 5.137: Εκτέλεση ping από τον χρήστη του 2ου ορόφου προς τον file Server (NIC 2)

User 1 1st floor → File Server (κάρτα δικτύου 2)



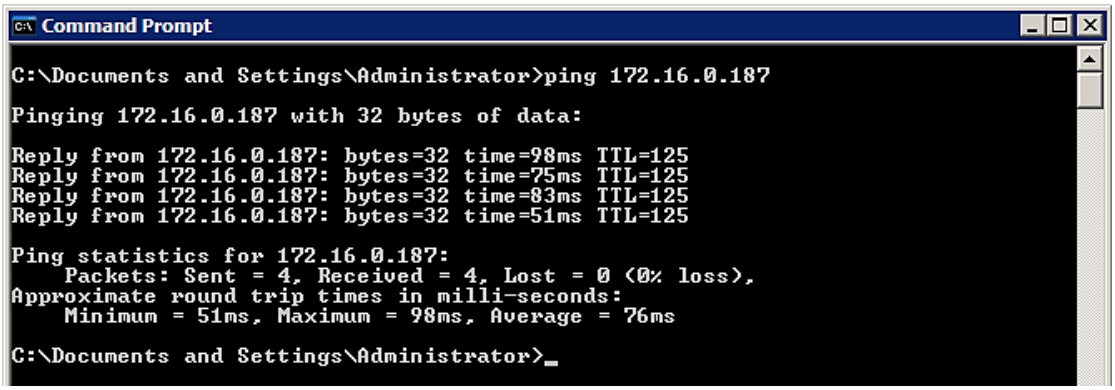
Εικόνα 5.138: Εκτέλεση ping από τον χρήστη του 1ου ορόφου προς τον file Server (NIC 2)

User 1 ground floor → File Server (κάρτα δικτύου 2)



Εικόνα 5.139: Εκτέλεση ping από τον χρήστη του ισογείου προς τον file Server (NIC 2)

User 1 branch → File Server (κάρτα δικτύου 2)



Εικόνα 5.140: Εκτέλεση ping από τον χρήστη του υποκαταστήματος προς τον file Server (NIC 2)

Με το κλείσιμο της πτυχιακής αυτής ο αναγνώστης θα είναι σε θέση να κατανοήσει τις ενέργειες που επιτελεί και λαμβάνει ένας τεχνικός δικτύων τόσο στην υλοποίηση δικτυακών τοπολογιών όσο και στην ασφάλεια αυτών. Αναφέραμε με ποίον τρόπο σχεδιάζεται ένα εταιρικό δίκτυο, το κόστος υλοποίησης αυτού, την ρύθμιση των συσκευών τόσο σε πρακτικό αλλά και σε θεωρητικό επίπεδο. Επίσης περιγράψαμε πολικές και κανόνες ασφάλειας που υποχρεούται μια εταιρία να ακολουθήσει προκειμένου το δίκτυο της να είναι ασφαλές από τις εξής απειλές:

- Ανάθεση κωδικών ασφαλείας σε συσκευές όπως μεταγωγείς και δρομολογητές που λανσάρει στην αγορά η εταιρία Cisco, προκειμένου να αποφύγουμε τις επιθέσεις από τρίτα πρόσωπα που έχουν ως στόχο την καταστροφή ενός δικτύου

- Ρύθμιση αυτών των συσκευών σε πρακτικό επίπεδο και καταγραφή ενός εργονομικού σχεδιασμού για το δίκτυο (π.χ. πρόληψη για μελλοντική επέκταση του δικτύου κλπ.)

- Για επιπλέον ασφάλεια αναφέραμε και εφαρμόσαμε ASA firewalls (επίσης συσκευή ασφαλείας που λανσάρει στην αγορά η εταιρία Cisco) και περιγράψαμε πως αυτά μπορούν να ρυθμιστούν

- Αναφέραμε επίσης μέτρα ασφάλειας για την πρόληψη τυχών φυσικών καταστροφών όπως εφαρμογή πυρασφάλειας σε περίπτωση πυρκαγιάς, εφεδρικές διαδρομές σε περίπτωση που καταστραφεί κάποια από αυτές να μην τεθεί εκτός λειτουργίας το δίκτυο κ.ο.κ.

- Μέτρα που θα πρέπει να ληφθούν από την εκάστοτε εταιρία ή οργανισμό που διαθέτει ένα δίκτυο τόσο στην συντήρηση αυτού όσο και στην χρήση που θα πρέπει να κάνουν σε αυτό οι εργαζόμενοι του.

Πέραν αυτού περιγράψαμε σε θεωρητικό επίπεδο την λειτουργία των βασικών πρωτοκόλλων επικοινωνίας καθώς και τον πρωτοκόλλων που εφαρμόσαμε στο δίκτυο μας. Επίσης περιγράψαμε την βασική δομή με την οποία λειτουργούν τα δίκτυα υπολογιστών και τις υπηρεσίες που μπορούν να προσφέρουν στην ανθρώπινη κοινωνία. Η δυνατότητα προσομοίωσης IOS λογισμικού Cisco που παρέχει το GNS3 είναι πολύ σημαντική καθότι ένας τεχνικός δικτύων με αυτόν τον τρόπο μπορεί να πειραματιστεί και να εξοικειωθεί με αυτό το IOS χωρίς τον κίνδυνο καταστροφής μιας συσκευής. Επίσης το γεγονός ότι το GNS3 είναι ευρύτερα διαθέσιμό στο κοινό λόγω του ότι είναι open source πρόγραμμα το καθιστά πολύ αξιόπιστο και σταθερό. Βέβαια υπάρχει ακόμη ανάγκη για βελτιώσεις οι οποίες πρέπει να γίνουν καθότι χρησιμοποιεί πολλούς φυσικούς πόρους από το σύστημα ενός υπολογιστή και η σταθερότητα του εξαρτάται από την επεξεργαστική ισχύ που διαθέτει.

ΠΗΓΕΣ – ΦΥΣΙΚΑ ΠΡΟΣΩΠΑ

Λάζαρος Αγαπίδης – Ειδικός Τηλεπικοινωνιών / Πιστοποιημένος εκπαιδευτής ακαδημίας Cisco

ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ

1. http://www.cnc.uom.gr/services/pdf/section1%282%29.pdf
2. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-TCP-IP-Introduction.html
3. http://el.wikipedia.org/wiki/Broadcast
4. http://www.diktyas.gr/index.php/2012-01-22-20-45-27/2012-01-22-22-33-47/lan
5. http://www.diktyas.gr/index.php/2013-03-13-19-12-51/2012-01-22-21-57-40/-bit-
6. http://www.diktyas.gr/index.php/2013-03-13-19-12-51/2012-01-22-21-57-40/-utp
7. http://www.diktyas.gr/index.php/2013-03-13-19-12-51/2012-01-22-21-57-40/2012-01-22-21-55-31
8. http://dide.flo.sch.gr/Plinet/Meetings/Meeting23/VirtualBox-WhatItIs.pdf
9. https://eclass.teicrete.gr/modules/document/file.php/TP129/%CE%95%CE%A1%CE%93%CE%91%CE%A3%CE%A4%CE%97%CE%A1%CE%99%CE%91_%CE%9C%CE%91%CE%9D%CE%99%CE%A6%CE%91%CE%92%CE%91/01.%CE%A3%CE%B7%CE%BC%CE%B5%CE%B9%CF%8E%CF%83%CE%B5%CE%B9%CF%82/OS-Lab-1-VirtualBox-Ubuntu-Installation-130601.pdf
10. http://dide.flo.sch.gr/Plinet/Tutorials-STEMP/Linux-Ubuntu.pdf
11. http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-NetworkTerminology.html
12. http://en.wikipedia.org/wiki/Network_Convergence
13. http://en.wikipedia.org/wiki/Optical_fiber
14. ftp://120.105.184.208/soft/Router%20%AB%FC%A5O%A5%DC%BDd/Cisco%20Router%20Configuration%20Commands.pdf
15. http://www.techrepublic.com/blog/data-center/10-commands-you-should-master-when-working-with-the-cisco-ios-104071/
16. http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r/frf001.pdf
17. http://www.perle.com/downloads/software/833is/ciscocmdmanual.pdf
18. https://perso.ens-lyon.fr/christophe.crespelle/enseignements/ASR/cisco-config.pdf
19. http://computernetworkingnotes.com/switching-vlan-stp-vtp-dtp-ether-channels/basic-switch-configurations.html
20. http://www.perle.com/downloads/software/833is/ciscocmdmanual.pdf
21. http://gonda.nic.in/swangonda/pdf/ccnaguide.pdf
22. http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series switches/data_sheet_c78-720918.html
23. http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd80322c0c.html
24. http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/product_data_sheet0900aecd80371991.html
25. http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.html
26. www.cisco.com/c/en/us/products/collateral/wireless/aironet-700-series/data_sheet_c78-726725.html
27. http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-c-series-switches/data_sheet_c78-639705.html
28. http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vlans.html
29. http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html

30. http://el.wikipedia.org/wiki/SSH
31. https://www.siteground.com/tutorials/email/pop3-imap-smtp-ports.htm
32. http://diktia.weebly.com/uploads/6/4/5/1/6451366/_protokolla_epikoinonias.pdf
33. http://pages.cs.aueb.gr/~xgeorge/MTMC/slides/16-Protocols.pdf
34. http://el.wikipedia.org/wiki/UDP
35. http://el.wingwit.com/Networking/internet-networking/69755.html
36. http://diktya-epal-g.ggia.info/wp-content/uploads/2009/12/Kefalaio_7_Diadiktywsh_internet_7_4_Prwtokollo_UDP.pdf
37. http://web.teipir.gr/new/ecs/pelab_1/tcp/inter4.htm
38. http://www.dmst.aueb.gr/dds/norma/internet/udp.htm
39. http://vivliothmmy.ee.auth.gr/187/1/diplomatiki.pdf
40. caclab.csd.auth.gr/askisi2.doc
41. http://el.wikipedia.org/wiki/EIGRP
42. http://en.wikipedia.org/wiki/Cisco_Discovery_Protocol
43. http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html

Ε-BOOK ΠΑΡΟΥΣΙΑΣΕΙΣ

Cisco Networking Academy, CCNA Routing and Switching 4.0, Scaling Networks

ΠΗΓΕΣ–ΒΙΒΛΙΑ

1) Τεχνολογία Δικτύων Επικοινωνιών – Σχολικό εγχειρίδιο ΕΠΑΛ
2) Δικτύωση Υπολογιστών 4η Έκδοση – James F. Kurose, Keith W. Ross – Εκδόσεις Μ.Γκιούρδας
3) Δίκτυα Υπολογιστών 5η Αμερικάνικη έκδοση Tanebaum Andrew S. Wetherall David J.
4) Δορυφορικές Επικοινωνίες 3η έκδοση – Παναγιώτης Γ. Κωττής, Χρήστος Ν. Κάψάλης
5) Τηλεπικοινωνίες και δίκτυα υπολογιστων 8η έκδοση Άρης Αλεξόπουλος, Γιώργος Λαγογίαννης
6) Ψηφιακές Επικοινωνίες – Andy Bateman
7) Ασύρματα Δίκτυα – Πέτρος Νικοπολίδης, Mohammad Salameh Obaidat, Γιώργος Παπαδημητρίου, Ανδρέας Πομπόρτσης
8) Ασύρματες Επικοινωνίες 2η έκδοση – Theodore S. Rapparot
3) GNS3 Network Simulation Guide – Chris Welsh
4) The Book of GNS3 – Jason C. Neumann
5) Cisco IOS Configuration Fundamentals Command Reference
6) Ο ΟΔΗΓΟΣ ΤΗΣ CISCO ΓΙΑ ΤΗ ΔΙΚΤΥΩΣΗ 2η έκδοση – Jim Doherty, Neil Anderson, Paul Della Maggiora Εκδόσεις Κλειδάριθμος