ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Π.Μ.Σ. «ΕΦΑΡΜΟΣΜΕΝΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη, σχεδιασμός, διαμόρφωση, ανάλυση δικτύων και υλοποίηση σειράς μαθημάτων σε εικονικό περιβάλλον για τα Δίκτυα Η/Υ.

Γεώργιος Ι. Φωτόπουλος

Εισηγήτρια: Αναστασία Βελώνη, Καθηγήτρια

ΑΘΗΝΑ ΜΑΙΟΣ 2018 ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη, σχεδιασμός, διαμόρφωση, ανάλυση δικτύων και υλοποίηση σειράς μαθημάτων σε εικονικό περιβάλλον για τα Δίκτυα Η/Υ.

Γεώργιος Ι. Φωτόπουλος
Α.Μ. AIS0124

Εισηγήτρια: Αναστασία Βελώνη, Καθηγήτρια

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Γεώργιος Φωτόπουλος, του Ιωάννη, με αριθμό μητρώου ais0124 φοιτητής του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών (πρώην Μηχανικών Η/Υ Συστημάτων Τ.Ε. του Α.Ε.Ι. Πειραιά Τ.Τ.) πριν αναλάβω την εκπόνηση της Διπλωματικής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

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

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

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

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό των δικτύων ηλεκτρονικών υπολογιστών. Την προσπάθειά μου αυτή υποστήριξε η επιβλέπουσα καθηγήτριά μου κα. Αναστασία Βελώνη, την οποία θα ήθελα να ευχαριστήσω.

Θα ήθελα επίσης να ευχαριστήσω, όλους του καθηγητές του μεταπτυχιακού για τις πολύτιμες γνώσεις που μου προσέφεραν και τους νέους δρόμους που μου άνοιξαν στο αντικείμενο της Εφαρμοσμένης Πληροφορικής καθώς και τους συμφοιτητές μου για την άψογη συνεργασία και συννενόηση.

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία ασχολείται με τον σχεδιασμό τη διαμόρφωση και την ανάλυση δικτύων υπολογιστών σε εικονικό περιβάλλον. Για την αποτελεσματικότερη κατανόηση του αντικειμένου δημιουργήθηκαν βιντεομαθήματα σχετικά με τις βασικές αρχές δικτύωσης υπολογιστών και δικτύων υπολογιστών. Τα βιντεομαθήματα παρέχουν τη δυνατότητα στο χρήστη να παρακολουθήσει, ατομικά, αλλά και να υλοποιήσει δίκτυα υπολογιστών σε εικονικό περιβάλλον με σκοπό να ελέγξει τις γνώσεις και τις ικανότητές του σε θέματα που σχετίζονται με τα δίκτυα IP τεχνολογίας. Τα μαθήματα αυτά μπορεί να αποτελέσουν εργαλείο εκμάθησης και ελέγχου των γνώσεων σε φοιτητές, επαγγελματίες αλλά και μαθητές τεχνικών σχολείων στα αντικείμενα που αναφέρονται.

ABSTRACT

The present thesis is about the designing, the development and the analysis of computer networks in a virtual environment in order to support network experiments. For a better understanding of the object there is a list of videos concerning computer networking and internetworks. The video gives the user the ability to perform experiments in order to test his knowledge and skills in topics related to the IP technology. The videos may be used as a learning tool from candidates who participate in similar programs or from professionals who work on the objects referred above.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Δίκτυα και διαδίκτυα Ηλεκτρονικών Υπολογιστών
ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Τεχνολογία IP, Μεταγωγείς, Εικονικά δίκτυα, Δρομολογητές, Πρωτόκολλα Δρομολόγησης, Packetracer.

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Units
CIDR	Classless Inter-Domain Routing
CRC	Cycle Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EGP	Exterior Gateway Protocols
FCS	Frame Check Sequence
FTP	File Transfer Protocol
HDLC	High-Level Data Link Control
HTTP	Hypertext Transfer Protocol
LAN	Local Area Network
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocols
IPX	Internet Packet Exchange
MAC	Media Access Control
MAN	Metropolitan Area Network
NAT	Network Address Translation
NNTP	Network News Transport Protocol
OSI/RM	Open Systems Interconnection Reference Model
OSPF	Open Shortest Path First
PAT	Port Address Translation
PDU	Protocol Data Unit
POP3	Post Office Protocol version 3
PVST	Per Vlan Spanning Tree Protocol
RIP	Routing Information Protocol
RSTP	Rapid Spanning Tree Protocol
SCSI	Small Computer System Interface
SCTP	Stream Control Transmission Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
STP	SPANNING TREE PROTOCOL
TCP	Transmission Control Protocol
TFTP	Trivial Transfer Protocol
UDP	User Datagram Protocol
VoIP	Voice over IP
VLAN	Virtual Local Area Network
VLSM	Variable-Length Subnet Masking
WAN	Wide Area Network

ΚΕΦΑΛΑΙΟ 1

1.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα κάνουμε μία περιγραφή των βασικών εννοιών στα Δίκτυα Υπολογιστών, όπως διαστρωμάτωση, μοντέλα αναφοράς, επίπεδα, υπηρεσίες και θα εστιάσουμε στην περιγραφή πρωτοκόλλων που σχετίζονται με την IP τεχνολογία.

1.2 Δίκτυα Υπολογιστών

Τα προϊόντα της σύγχρονης τεχνολογίας, όλο και περισσότερο ενσωματώνουν λειτουργίες που απαιτούν την αλληλοσύνδεσή τους. Η χρήση υπολογιστικών συστημάτων, ακόμη και σε συγκαλυμμένη μορφή, όπως “έξυπνες” συσκευές (smartphone, smartTV, tablet, …), έχει γενικευθεί και προσφέρει πολλές δυνατότητες διασύνδεσης. Ταυτόχρονα εξαρτάται από τις δυνατότητες διασύνδεσης των συσκευών. Ακόμη, η χρήση του Διαδικτύου έχει εισχωρήσει σε μεγάλο βαθμό στην καθημερινότητα των ατόμων. Η κατανόηση των αρχών λειτουργίας των δικτύων αποτελεί θεμελιώδη γνώση για την ενασχόληση, ιδιαίτερα, με αντικείμενα του χώρου της πληροφορικής.

Ενα **δίκτυο υπολογιστών** ή τηλεπληροφορικής είναι ένα σύστημα επικοινωνιών το οποίο διαθέτει συσκευές τηλεπικοινωνιών, τηλεπικοινωνιακούς κόμβους καθώς και φυσικά μέσα διέλευσης της πληροφορίας (ενσύρματα, οπτικά ή ασύρματα μέσα). Τέτοια δίκτυα είναι το Διαδίκτυο (Internet), τα ιδιωτικά εταιρικά δίκτυα όπως τα τραπεζικά, τα σύγχρονα δίκτυα σταθερής και κινητής τηλεφωνίας, δίκτυα αισθητήρων, τηλεμετρίας, κτλ. Οι κύριες ιδιότητες ενός δικτύου είναι να επιτρέπει σε πολλούς χρήστες να μοιράζονται ή να ανταλλάσσουν πληροφορίες και να εκμεταλεύονται την επεξεργαστική ικανότητα άλλων υπολογιστών, να έχουν πρόσβαση σε βάσεις δεδομένων κτλ. Η μορφή σύνδεσης μεταξύ των κόμβων ενός δικτύου ονομάζεται **τοπολογία δικτύου**.

Σε ένα δίκτυο τηλεπληροφορικής συναντάμε αυστηρούς κανόνες και πρότυπα που διέπουν το τηλεπικοινωνιακό τμήμα και την υλοποίηση του υλικού μέρους καθώς επίσης και κανόνες συνομιλίας μεταξύ των υπολογιστών οι οποίοι ονομάζονται **πρωτόκολλα επικοινωνίας**.

Η δικτύωση, από **το μέσο μετάδοσης (καλώδιο) και την δικτυακή διασύνδεση** μέχρι **το πρόγραμμα-εφαρμογή,** είναι μια αρκετά **πολύπλοκη διαδικασία.**

Για την **υλοποίηση μιας δικτυακής εφαρμογής** η οποία παρέχεται από έναν υπολογιστή σε έναν άλλον, ξεκινώντας από το μηδέν, πρέπει

- να επινοηθεί ένας τρόπος αναπαράστασης των δεδομένων/πληροφοριών με τη μορφή, συνήθως, ηλεκτρικών ή οπτικών σημάτων,
- να κατασκευαστούν ιδιαίτερες **δικτυακές διασυνδέσεις** και **καλώδια**, τα οποία θα **συνδέσουν** τους υπολογιστές μεταξύ τους

- να επινοηθεί και να υλοποιηθεί ο **τρόπος εύρεσης μιας διαδρομής** μέσω της οποίας θα ταξιδέψουν οι πληροφορίες μέχρι τον τελικό προορισμό και να **αποκατασταθεί η επικοινωνία** από άκρο σε άκρο.

Επειδή η στρατηγική αντιμετώπισης κάθε σύνθετου πολύπλοκου προβλήματος είναι αυτό να διαχωριστεί σε περισσότερα μικρότερα επιμέρους θέματα το έργο της δικτύωσης **διασπάστηκε σε επιμέρους λειτουργίε**ς οι οποίες μπορούν να υλοποιηθούν ανεξάρτητα, παρέχοντας και εναλλακτικές επιλογές ανάλογα με τις ανάγκες. Η αντιμετώπιση αυτή ονομάζεται στρωματοποιημένη αρχιτεκτονική (layered architecture).

Με τη στρωματοποιημένη αρχιτεκτονική πετυχαίνουμε

- Διαχωρισμό του προβλήματος της επικοινωνίας σε μικρότερα και πιο εύκολα διαχειρίσιμα προβλήματα
- Εύκολη προσθήκη, αλλαγή ή βελτίωση υπηρεσιών, αφού οι απαιτούμενες αλλαγές περιορίζονται σε ένα συγκεκριμένο επίπεδο.

Ο στόχος είναι η απόκρυψη των λεπτομερειών του υλικού του δικτύου δίνοντας τη δυνατότητα στους υπολογιστές και στις εφαρμογές τους να επικοινωνούν μεταξύ τους ανεξάρτητα από τις φυσικές δικτυακές τους συνδέσεις.

Έτσι διαμορφώθηκε το μοντέλο αναφοράς (*Reference Model*) για τη Διασύνδεση Ανοικτών Συστημάτων (*Open Systems Interconnection* - **OSI**) από τον Διεθνή Οργανισμό Τυποποίησης (*International Organization for Standardization* - **ISO**) που προδιαγράφει **επτά (7) στρώματα επίπεδα** (*seven layers*) τα οποία υλοποιούν συγκεκριμένες λειτουργίες ώστε να **είναι εφικτή η διασύνδεση διαφορετικών υπολογιστικών συστημάτων εφόσον στα αντίστοιχα επίπεδα χρησιμοποιούν συμβατές ή ίδιες τεχνικές και κανόνες *(πρωτόκολλα)***.

1.3 Μοντέλα Αναφοράς

1.3.1 Μοντέλο αναφοράς OSI (OSI/RM)

Το πρότυπο OSI (Open Systems Interconnection) καθορίστηκε ως πρότυπο OSI 7498-1 και αναπτύχθηκε ως ένα μοντέλο για το χαρακτηρισμό και την τυποποίηση των λειτουργιών διαστρωματωμένων συστημάτων επικοινωνιών σε όρους επιπέδων ή στρωμάτων (layers). Βασική αρχή του είναι η αρχή της διαστρωμάτωσης και σύμφωνα με αυτή την αρχή παρόμοιες λειτουργίες ομαδοποιούνται σε λογικά επίπεδα.

Το μοντέλο αναφοράς OSI επηρέασε όχι τόσο τον τρόπο με τον οποίο σχεδιάζουμε όσο τον τρόπο με τον οποίο κατανοούμε τα δίκτυα υπολογιστών. Παρέχει τη βάση αναφοράς για τη διασύνδεση ανοικτών συστημάτων, με σκοπό την υποστήριξη εφαρμογών κατανεμημένης επεξεργασίας. **Ανοικτά συστήματα είναι τα συστήματα τα οποία μπορούν να συνδεθούν καθώς ακολουθούν το μοντέλο αναφοράς OSI και είναι σύμφωνα με αυτό.**

Ο στόχος του OSI και γενικά της προτυποποίησης των πρωτοκόλλων επικοινωνιών είναι τα απομακρυσμένα στοιχεία ενός δικτύου να λειτουργούν αρμονικά μεταξύ τους ανεξάρτητα από το ποιος είναι ο κατασκευαστής τους.

Περί τα τέλη της δεκαετίας του 1980 ο ISO συνιστούσε την εφαρμογή του μοντέλου OSI ως κοινώς αποδεκτού υποδείγματος σχεδιασμού δικτύων. Παρότι δημιουργήθηκαν πρωτόκολλα βασισμένα στο μοντέλο αναφοράς OSI από τον οργανισμό ISO, σε συνεργασία με τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunication Union, ITU), γνωστά ως σειρά πρωτοκόλλων «X» (π.χ. X.25, X.400, X.500 κ.ά.) δεν εφαρμόστηκαν καθώς απέτυχαν εμπορικά.

Εκείνη την εποχή η **στοίβα πρωτοκόλλων TCP/IP, η οποία βασιζόταν σε ελαφρώς διαφορετική διαστρωμάτωση επιπέδων,** ήταν ήδη επί πολύ καιρό σε **χρήση**. Το TCP/IP ήταν θεμελιώδες για το δίκτυο ARPANET και τα άλλα δίκτυα που εξελίχθηκαν στο σημερινό Διαδίκτυο.

Το μοντέλο OSI παραμερίστηκε σταδιακά και σήμερα μόνο ένα υποσύνολό του χρησιμοποιείται ακόμη. Η επικρατούσα αντίληψη είναι ότι οι περισσότερες προδιαγραφές του είναι περίπλοκες και η πλήρης λειτουργικότητά του θα χρειαζόταν μεγάλο χρόνο κατασκευής, αν και συνεχίζουν να υπάρχουν υποστηρικτές του. Έτσι, ιδιαίτερα μετά την εισαγωγή του World Wide Web (WWW) επικρατησε η στοίβα πρωτοκόλλων TCP/IP.

Το μοντέλο αναφοράς OSI έχει επτά επίπεδα. Ένα επίπεδο εξυπηρετεί τόσο το επίπεδο που βρίσκεται πάνω από αυτό, όσο και το επίπεδο που βρίσκεται κάτω από αυτό. Τα τρία χαμηλότερα επίπεδα ασχολούνται με τον έλεγχο της μετάδοσης των μηνυμάτων μέσα στο δίκτυο, ενώ τα τέσσερα ανώτερα επίπεδα παρέχουν την αξιόπιστη μεταβίβαση των δεδομένων μεταξύ των τελικών χρηστών. Έτσι, και τα επτά επίπεδα υλοποιούνται μόνο στους υπολογιστές που λειτουργούν ως τερματικοί σταθμοί.

Εικόνα 1: Επίπεδα και λειτουργίες του μοντέλου OSI

Εικόνα 1.1: Επίπεδα και λειτουργίες του μοντέλου OSI.

<u>Το Φυσικό Επίπεδο (Physical Layer)</u>

Το φυσικό επίπεδο (physical layer) είναι **το χαμηλότερο επίπεδο του μοντέλου OSI**. Ασχολείται με τη μετάδοση ακατέργαστων bits σε ένα κανάλι επικοινωνίας **(φυσικό μέσο επικοινωνίας)** το οποίο μπορεί να είναι απλή δισύρματη γραμμή, ομοαξονικό καλώδιο, οπτική ίνα ή και ασύρματη ζεύξη. Στο φυσικό επίπεδο **γίνεται μετατροπή των δεδομένων από το επίπεδο 2** (ακολουθία bits) **σε ηλεκτρικά σήματα** και η **μετάδοσή τους μέσω ενός επικοινωνιακού διαύλου (μέσο μετάδοσης).** Τα θέματα σχεδίασης έχουν να κάνουν με τη διασφάλιση ότι, όταν η μία πλευρά στέλνει ένα bit 1, αυτό λαμβάνεται από την άλλη πλευρά ως bit 1 και όχι ως bit 0. Επίσης καθορίζει την διάρκεια κάθε bit, την αρχή και το τέλος της μετάδοσης καθώς και το αν η μετάδοση μπορεί να γίνει προς την μια ή και τις δύο κατευθύνσεις ταυτόχρονα. Τα θέματα σχεδίασης εδώ, στην πλειοψηφία τους ασχολούνται με μηχανικές, ηλεκτρικές και διαδικασίες διασυνδέσεις καθώς και με το **φυσικό μέσο μετάδοσης, το οποίο βρίσκεται κάτω από φυσικό επίπεδο.**

Το φυσικό επίπεδο περιλαμβάνει και τους οδηγούς της κάρτας δικτύου, οι οποίοι λένε στο πρωτόκολλο πως να πραγματοποιήσει τη μετάδοση και τη λήψη των δυαδικών ψηφίων.

Δικτυακές συσκευές που λειτουργούν στο επίπεδο αυτό είναι οι κάρτες δικτύου (NICs), τα hubs και οι επαναλήπτες (repeaters). Οι συσκευές αυτές πραγματοποιούν λειτουργίες πάνω σε σήματα. Τα hubs στέλνουν ένα σήμα από μια θύρα σε όλες τις άλλες, οι επαναλήπτες ενισχύουν το σήμα, ώστε να ταξιδέψει σε μεγαλύτερη απόσταση, ενώ οι κάρτες δικτύου αναλαμβάνουν την σωστή μετάφραση των μεταδιδόμενων σημάτων.

Μερικά από τα πρωτόκολλα που συναντούμε στο επίπεδο αυτό είναι (ενδεικτικά):

- Ethernet Physical Layer (IEEE 802.3)
- DSL (Digital Subscriber Line)
- ISDN (Integrated Services Digital Network)
- Bluetooth Physical Layer
- CAN Bus Physical Layer
- Wifi Physical Layer (IEEE 802.3)
- RS232

<u>Το Επίπεδο Σύνδεσης Δεδομένων (Data Link Layer)</u>

Βασικός σκοπός του επιπέδου αυτού είναι να π**αίρνει τα δεδομένα από το φυσικό επίπεδο και να τα προωθεί στο ανώτερο του επίπεδο, το «επίπεδο δικτύου»**, αφού πρώτα εκτελέσει μερικές ουσιώδεις λειτουργίες όπως είναι η ανίχνευση και διόρθωση σφαλμάτων μετάδοσης και ο έλεγχος ροής των πληροφοριών. Βεβαίως το επίπεδο αυτό εκτελεί και το αντίστροφο, δηλαδή δέχεται δεδομένα από το Επίπεδο Δικτύου (Network Layer) και τα αποδίδει στο Φυσικό Επίπεδο (Physical Layer). Τα bit που εκπέμπονται ή λαμβάνονται ομαδοποιούνται σε πλαίσια (frames). Τα πλαίσια οργανώνονται σε πεδία που το καθένα έχει διαφορετική αποστολή.

Το **πεδίο διεύθυνσης (address)** παρέχει τις διευθύνσεις του κόμβου αποστολής και του κόμβου παραλαβής.

Το **πεδίο ελέγχου (Flow Control)** δηλώνει το είδος των πλαισίων δεδομένων (αν δηλ. τα πλαίσια είναι πλαίσια δεδομένων, ή πλαίσια διαχείρισης) του καναλιού σύνδεσης.

Το **πεδίο δεδομένων (Data)** περιέχει τα πραγματικά δεδομένα που μεταδίδονται.

Το **πεδίο ελέγχου λαθών (FCS)**, με βάση αυτό το πεδίο γίνεται ανίχνευση τυχόν λαθών στο πλαίσιο των δεδομένων

Μέρος της επεξεργασίας που γίνεται στα δεδομένα του επιπέδου αυτού είναι και η **προσθήκη των MAC διευθύνσεων του αποστολέα και του παραλήπτη**. Η MAC (Media Access Control) διεύθυνση είναι η διεύθυνση που χαρακτηρίζει μοναδικά μια

κάρτα δικτύου και είναι μοναδική. Το επίπεδο 2 χωρίζεται σε δύο υποεπίπεδα, το **υποεπίπεδο ελέγχου λογικού συνδέσμου (Logical Link Control)** και το **υποεπίπεδο ελέγχου προσπέλασης μέσων (MAC).** Δικτυακές συσκευές που λειτουργούν στο επίπεδο αυτό είναι οι **γέφυρες (bridges).** Οι συσκευές αυτές υποστηρίζουν την προώθηση με βάση την MAC διεύθυνση. Η MAC διεύθυνση χρησιμοποιείται για να αποφασίσει η συσκευή αν χρειάζεται να προωθήσει το πλαίσιο από το ένα δίκτυο στο άλλο. Αν η συσκευή έχει πληροφορία για την διεύθυνση αυτή, τότε αποστέλλει το πλαίσιο στον κόμβο που έχει αυτήν την MAC διεύθυνση, αλλιώς προωθεί το πακέτο σε άλλο δίκτυο, στο οποίο πιθανά να βρίσκεται ο κατάλληλος κόμβος.

Μερικά από τα πρωτόκολλα που συναντούμε στο επίπεδο αυτό είναι:

- SLIP: Serial Line Internet Protocol
- ARP: Address Resolution Protocol
- PPP: Point-to-Point Protocol
- L2TP: Layer 2 Tunneling Protocol
- PPTP: Point-to-Point Tunneling Protocol
- ISDN: Integrated Services Digital Network
- Ethernet (IEEE 802.3)
- IEEE 802.11 WiFi

<u>Το Επίπεδο Δικτύου (Network Layer)</u>

Βασικές λειτουργίες του επιπέδου είναι η οργάνωσή των δεδομένων σε πακέτα επιπέδου δικτύου, η προώθηση και δρομολόγηση των πακέτων από μια πηγή σε ένα προορισμό, και η διευθυνσιοδότηση των κόμβων και των Hosts.

Καθορίζει το βέλτιστο κάθε φορά μονοπάτι για την μετάδοση της πληροφορίας με βάση την πληροφορία που έχουν για την κατάσταση των συνδέσμων, την διεύθυνση του παραλήπτη, την ταχύτητα του δικτύου, τον αριθμό των ενδιάμεσων κόμβων και μια σειρά άλλων πληροφοριών που διατηρούν.

Μερικά από τα πρωτόκολλα που συναντούμε στο επίπεδο αυτό είναι:

- IP: Internet Protocol
- OSPF: Open Shortest Path First
- NAT: Network Address Translation
- ICMP: Internet Control Message Protocol
- BGP: Border Gateway Protocol
- IGMP: Internet Group Management Protocol
- IPSec: Internet Protocol Security
- RIP: Routing Information Protocol
- IPX: Internet Packet Exchange

<u>Το Επίπεδο Μεταφοράς (Transport Layer)</u>

Η βασική λειτουργία του επιπέδου μεταφοράς (transport layer) είναι η **αποδοχή δεδομένων από το ανώτερο επίπεδο ή διάσπαση αυτών σε μικρότερες μονάδες** εάν χρειαστεί, **η μεταφορά τους στο επίπεδο δικτύου** και αναάλογα με την υπηρεσία **η διασφάλιση ότι όλα τα τμήματα φτάνουν σωστά στην άλλη πλευρά**. Επιπλέον όλα αυτά πρέπει να γίνουν αποδοτικά και με τέτοιο τρόπο ώστε να απομονώνουν το επίπεδο συνόδου από τις αναπόφευκτες αλλαγές στην τεχνολογία του υλικού. Υπό κανονικές συνθήκες, το επίπεδο μεταφοράς δημιουργεί μια ξεχωριστή σύνδεση δικτύου για κάθε σύνδεση μεταφοράς που απαιτείται από το επίπεδο συνόδου. Εάν η σύνδεση μεταφοράς απαιτεί υψηλό ρυθμό εξυπηρέτησης (throughput), το επίπεδο μεταφοράς μπορεί να δημιουργήσει πολλαπλές συνδέσεις δικτύου, μοιράζοντας τα δεδομένα ανάμεσα στις συνδέσεις δικτύου για να βελτιώσει το ρυθμό εξυπηρέτησης.

Από την άλλη πλευρά εάν η δημιουργία ή η συντήρηση μιας σύνδεσης δικτύου είναι ακριβή, το επίπεδο μεταφοράς μπορεί να πολυπλέκει πολλές συνδέσεις μεταφοράς στην ίδια σύνδεση δικτύου για να ελαττώσει το κόστος. Σε όλες τις περιπτώσεις το επίπεδο μεταφοράς χρειάζεται πάντα για να κάνει την πολυπλεξία διάφανη στο επίπεδο συνόδου. **Το επίπεδο μεταφοράς καθορίζει επίσης τι είδους υπηρεσίες θα παρέχει το επίπεδο συνόδου**. Ο πιο γνωστός τύπος σύνδεσης μεταφοράς είναι ένα ελεύθερο από σφάλματα από σημείο σε σημείο κανάλι (point to point), το οποίο παραδίδει μηνύματα με την σειρά με την οποία έχουν σταλεί.

Οι κύριες λειτουργίες του είναι:

- Η Αποκατάσταση και τερματισμός της σύνδεσης σε επίπεδο μεταφοράς
- Η Μετάδοση των δεδομένων σύμφωνα με τον απαιτούμενο από το χρήστη βαθμό αξιοπιστίας (δηλ. με επιβεβαίωση παραλαβής πακέτου ή όχι).
- Ο Καθορισμός και επιλογή από το χρήστη της ποιότητας εξυπηρέτησης της σύνδεσης (όταν αυτό υπάρχει).
- Η Δυνατότητα πολύπλεξης μέσω της ίδιας ζεύξης και ο έλεγχος της ροής.

Μερικά από τα πρωτόκολλα που συναντούμε στο επίπεδο αυτό είναι:

- **TCP**: Transmission Control Protocol
- **UDP**: User Datagram Protocol

<u>Το επίπεδο συνόδου (Session Layer)</u>

Το επίπεδο συνόδου (session layer) **επιτρέπει στους χρήστες διαφορετικών μηχανημάτων να εγκαθιστούν συνόδους (sessions) μεταξύ τους**. Μία σύνοδος επιτρέπει μια συνήθη μεταφορά δεδομένων, όπως και το επίπεδο μεταφοράς, αλλά παρέχει και μερικές πρόσθετες υπηρεσίες που είναι χρήσιμες σε πολλές εφαρμογές. Μία σύνοδος μπορεί να χρησιμοποιηθεί για να επιτρέψει τη σύνδεση ενός χρήστη σ' ένα απομακρυσμένο σύστημα καταμερισμού χρόνου (time sharing) ή για να

μεταφέρει ένα αρχείο μεταξύ δύο μηχανών. Στο επίπεδο συνόδου γίνεται έλεγχος διαλόγου, δηλαδή ποια συσκευή έχει σειρά για μετάδοση καθώς και συγχρονισμό (παρακολούθηση μεταδόσεων μακράς διάρκειας, π.χ. βίντεο, ώστε να συνεχιστούν από το σημείο που σταμάτησαν σε περίπτωση απότομης διακοπής).

Οι λειτουργίες του επιπέδου αυτού δε χρησιμοποιούνται πάντα και είναι οι εξής:

- Έναρξη και συντήρηση διαλόγου (ή συνόδου) μεταξύ ενός ή περισσοτέρων σταθμών (ταυτόχρονα).
- Διαχείριση και έλεγχος προσπέλασης της κάθε συνόδου.
- Επανορθωτικές διαδικασίες σε επίπεδο διαλόγου (σε περίπτωση προβλήματος).

<u>Το επίπεδο παρουσίασης (Presentation Layer)</u>

Συγκεκριμένα, ενώ όλα τα κατώτερα επίπεδα ενδιαφέρονται μόνο για την αξιόπιστη μετακίνηση bits από το ένα μέρος στο άλλο, **το επίπεδο παρουσίασης καταπιάνεται με το συντακτικό και τη σημασιολογία των πληροφοριών που μεταδίδονται.** Επίσης, το επίπεδο παρουσίασης ενδιαφέρεται και για άλλα θέματα όπως η **αναπαράσταση πληροφοριών**. Για παράδειγμα, η συμπίεση των δεδομένων χρησιμοποιείται για να ελαττώσει τον αριθμό των bits που πρόκειται να μεταδοθούν και συχνά απαιτείται κρυπτογράφηση για να εξασφαλιστεί η μυστικότητα (**privacy**) και η γνησιότητα (**authentication**) της πληροφορίας. Επειδή οι υπολογιστές χρησιμοποιούν διαφορετικά λειτουργικά συστήματα (Windows, Linux, MacOs) είναι απαραίτητο τα δεδομένα να μετατραπούν σε ένα **κοινό** μορφότυπο (**format**) που να είναι "κατανοητό" και από τους δύο συσκευές που πρόκειται να επικοινωνήσουν. Το επίπεδο παρουσίασης εξασφαλίζει ότι η πληροφορία από το επίπεδο εφαρμογής ενός συστήματος μπορεί να διαβαστεί από το επίπεδο εφαρμογής ενός άλλου συστήματος. **Μετατρέπει τα δεδομένα σε κοινό format και παρέχει υπηρεσίες κρυπτογράφησης, αποκρυπτογράφησης.** Οι λειτουργίες του επιπέδου αυτού δε χρησιμοποιούνται πάντα.

<u>Το επίπεδο εφαρμογής (Application Layer)</u>

Το επίπεδο εφαρμογής (application layer) περιέχει μια ποικιλία πρωτοκόλλων που χρειάζονται συχνά. Η μεταφορά ενός αρχείου μεταξύ δύο διαφορετικών συστημάτων απαιτεί αντιμετώπιση αυτών και άλλων μη συμβατών καταστάσεων. Στο επίπεδο αυτό γίνεται η διαχείριση των κατανεμημένων εφαρμογών όπως το ηλεκτρονικό ταχυδρομείο, η πλόγηση στο WWW, η μεταφορά αρχείων, η απομακρυσμένη σύνδεση, κτλ.

Δεν παρέχει υπηρεσίες σε κανένα άλλο επίπεδο του OSI. Πρωτόκολλα αυτού του επιπέδου είναι το HTTP, FTP, Telnet, SMTP. Οι υπηρεσίες που προσφέρει είναι οι εξής:

- Την εξακρίβωση της ταυτότητας των εφαρμογών που θέλουν να επικοινωνήσουν και την επιβεβαίωση της διαθεσιμότητας τους για συνομιλία.
- Την επιβεβαίωση η τον έλεγχο στο δικαίωμα της συνομιλίας.
- Τον καθορισμό αρμοδιοτήτων.
- Τον καθορισμό των διαδικασιών για τον έλεγχο της ροής των συνόδων και την αξιοπιστία της πληροφορίας.

Μερικά από τα πρωτόκολλα εφαρμογών που συναντούμε στο επίπεδο αυτό είναι:

- HTTP: Hypertext Transfer Protocol
- FTP: File Transfer Protocol
- TFTP: Trivial Transfer Protocol
- TELNET
- SMTP: Simple Mail Transfer Protocol
- SNMP: Simple Network Management Protocol
- IMAP: Internet Message Access Protocol
- POP3: Post Office Protocol version 3
- SET: Secure Electronic Transaction

1.3.2 Το μοντέλο TCP/IP

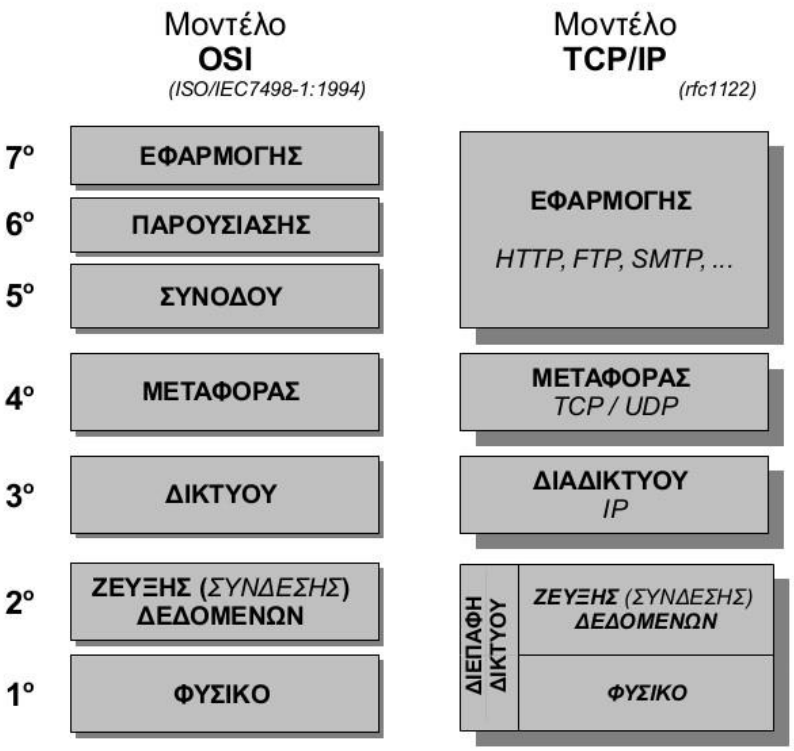
Το **TCP/IP (Transmission Control Protocol/Internet Protocol)** είναι παλιότερο μοντέλο από το OSI, ωστόσο είναι αυτό που έχει επικρατήσει σήμερα. Αναπτύχθηκε από το DoD (Department of Defense) των Η.Π.Α. για να υποστηρίξει τη λειτουργία του δικτύου ARPANET, που αποτελεί τον πρόδρομο του σημερινού Internet. Η αρχιτεκτονική αυτή, που ομοιάζει στο μοντέλο αναφοράς OSI, έχει ως βασικό στόχο **τη διατήρηση του δικτύου ακόμη και όταν ένας η περισσότεροι κόμβοι καταρρεύσουν.** Επίσης, έχει ευελιξία στην αρχιτεκτονική, αφού υποστηρίζει ένα δίκτυο με πολλές εφαρμογές και τη μεταφορά όλων των τύπων πληροφορίας.

Εικόνα 2: : Μοντέλο TCP/IP

Το μοντέλο TCP/IP αποτελείται από τέσσερα (4) επίπεδα:

- Επίπεδο Διασύνδεσης Δικτύου (Επίπεδο 1)
- Επίπεδο Διαδικτύου (Επίπεδο 2
- Επίπεδο Μεταφοράς (Επίπεδο 3)
- Επίπεδο Εφαρμογών (Επίπεδο 4)

Μεταξύ του μοντέλου OSI και TCP/IP υπάρχει αντιστοιχία ως προς τα επίπεδα από τα οποία αποτελούνται. Καθώς το μοντέλο OSI σχεδιάστηκε αργότερα από το TCP/IP οι σχεδιαστές του θέλησαν να εξασφαλίσουν πως το πακέτο πρωτοκόλλων του TCP/IP θα συμπεριλαμβάνονταν στο νέο μοντέλο που σχεδίαζαν καθώς υπήρχαν αρκετά συστήματα τα οποία λειτουργούσαν ήδη με βάση το TCP/IP. Στόχευαν στην ομαλή επικοινωνία με αυτά τα συστήματα. Η αντιστοίχηση των επιπέδων των δύο μοντέλων δίνεται στην εικόνα 3. Το επίπεδο εφαρμογών του TCP/IP αντιστοιχεί στα επίπεδα 5, 6, και 7 του μοντέλου OSI, το επίπεδο μεταφοράς στο επίπεδο 4 του OSI, το επίπεδο διαδικτύου αντιστοιχεί στο επίπεδο 3 του OSI και τέλος το επίπεδο διασύνδεσης δικτύου του TCP/IP αντιστοιχεί στα επίπεδα 1 και 2 του OSI.



Εικόνα 3: Αντιστοίχιση επιπέδων μοντέλου OSI και TCP/IP

<u>Το Επίπεδο Διασύνδεσης Δικτύου</u>

Το επίπεδο διασύνδεσης δικτύου, είναι **το χαμηλότερο επίπεδο** στην ιεραρχία των επιπέδων του μοντέλου TCP/IP. Αντιστοιχεί στο φυσικό επίπεδο και το επίπεδο συνδέσμου μετάδοσης δεδομένων του μοντέλου του OSI. **Επικοινωνεί απευθείας με το δίκτυο και παρέχει την διασύνδεση μεταξύ της αρχιτεκτονικής του δικτύου (π.χ. Ethernet) και του επιπέδου του διαδικτύου**.

<u>Το Επίπεδο Διαδικτύου</u>

Το επίπεδο διαδικτύου είναι το **βασικότερο επίπεδο του μοντέλου**. Είναι το δεύτερο επίπεδο του μοντέλου και χρησιμοποιεί αρκετά πρωτόκολλα για τη **δρομολόγηση και προώθηση των πακέτων**. Τα πακέτα ταξιδεύουν ανεξάρτητα το ένα από το άλλο προς τον προορισμό τους και πιθανά φτάνουν και με διαφορετική σειρά από αυτή με την οποία έφυγαν από τον αποστολέα τους. **Τα ανώτερα επίπεδα αναλαμβάνουν την ανασυγκρότηση των πακέτων, όποτε απαιτείται**, ώστε η πληροφορία να φτάσει σωστά. Οι λειτουργίες του επιπέδου αυτού είναι αντίστοιχες με τις λειτουργίες του επιπέδου δικτύου του μοντέλου OSI. Στο επίπεδο αυτό συναντούμε αρκετά **πρωτόκολλα**, όπως το ARP και ο ICMP, αλλά σίγουρα το βασικότερο και πλέον γνωστό είναι το **IP**. **Το IP είναι ένα πρωτόκολλο μεταγωγής πακέτων που είναι υπεύθυνο για τη διευθυνσιοδότηση και την προώθηση.** Βασικός στόχος του είναι να προωθεί τα πακέτα στον προορισμό τους, όσο το δυνατόν πιο γρήγορα και αποφεύγοντας τις συμφορήσεις του δικτύου.

<u>Το Επίπεδο Μεταφοράς</u>

Το επίπεδο μεταφοράς είναι υ**πεύθυνο για την εγκαθίδρυση και διατήρηση της επικοινωνίας μεταξύ δύο υπολογιστών**. Κύρια λειτουργία του είναι να αναλαμβάνει τον έλεγχο ροής και την τοποθέτηση των πακέτων στη σωστή σειρά, ώστε η πληροφορία να λαμβάνεται τελικά ακέραια και ορθή. Χειρίζεται επίσης και τις αναμεταδόσεις των πακέτων.

Στο επίπεδο αυτό έχουν οριστεί δύο πρωτόκολλα μεταφοράς από άκρο σε άκρο:

- Το πρώτο είναι το **TCP** (Πρωτόκολλα Ελέγχου Μετάδοσης) και
- Το πρωτόκολλο **UDP** (Πρωτόκολλο Αυτοδύναμων Πακέτων Χρήστη).

Το TCP είναι ένα **αξιόπιστο συνδεσμοστρεφές πρωτόκολλο** υπεύθυνο για την αξιόπιστη μετάδοση δεδομένων από έναν κόμβο σε κάποιον άλλο. Για να εγκαθιδρύσει μια αξιόπιστη σύνδεση το TCP χρησιμοποιεί την γνωστή ως «τριμερή χειραψία» **(three-way handshake) με την οποία καθορίζεται ο αριθμός θύρας που θα χρησιμοποιηθεί για την επικοινωνία** καθώς και οι αρχικοί ακολουθιακοί αριθμοί για την μεταφορά των δεδομένων. Το TCP χειρίζεται τα δεδομένα σαν μια ακολουθία (stream) από bytes.

Το User Datagram Protocol (UDP) είναι ένα **αναξιόπιστο ασυνδεσμικό πρωτόκολλο** το οποίο χρησιμοποιείται σε περιπτώσεις όπου **δεν απαιτείται** παράδοση των πακέτων με τη σωστή σειρά ή ο έλεγχος ροής που πραγματοποιείται με την χρήση του TCP. Ο οποιοσδήποτε έλεγχος γίνεται από την εφαρμογή που κάνει χρήση του συγκεκριμένου πρωτοκόλλου. Χρησιμοποιείται επίσης ευρέως σε περιπτώσεις όπου απαιτείται ταχύτατη παράδοση των πακέτων και δεν είναι τόσο κρίσιμη η αξιόπιστη μετάδοσή τους. Τέτοιες περιπτώσεις είναι η μετάδοση βίντεο και ήχου. Και το UDP κάνει χρήση θυρών, ωστόσο αυτές διαφέρουν από τις αντίστοιχες του TCP και επομένως τα δύο πρωτόκολλα μπορούν να χρησιμοποιούν τον ίδιο αριθμό θυρών χωρίς διενέξεις.

<u>Το Επίπεδο Εφαρμογών</u>

Το επίπεδο εφαρμογών είναι το **υψηλότερο επίπεδο του μοντέλου**. Αυτό περιέχει όλα τα πρωτόκολλα ανώτερου επιπέδου. Μερικά αυτά είναι:

- FTP: File Transfer Protocol
- TELNET
- DNS: Domain Name System
- HTTP: Hypertext Transfer Protocol
- SMTP: Simple Mail Transfer Protocol
- NNTP: Network News Transport Protocol

1.4 Το δίκτυο Ethernet

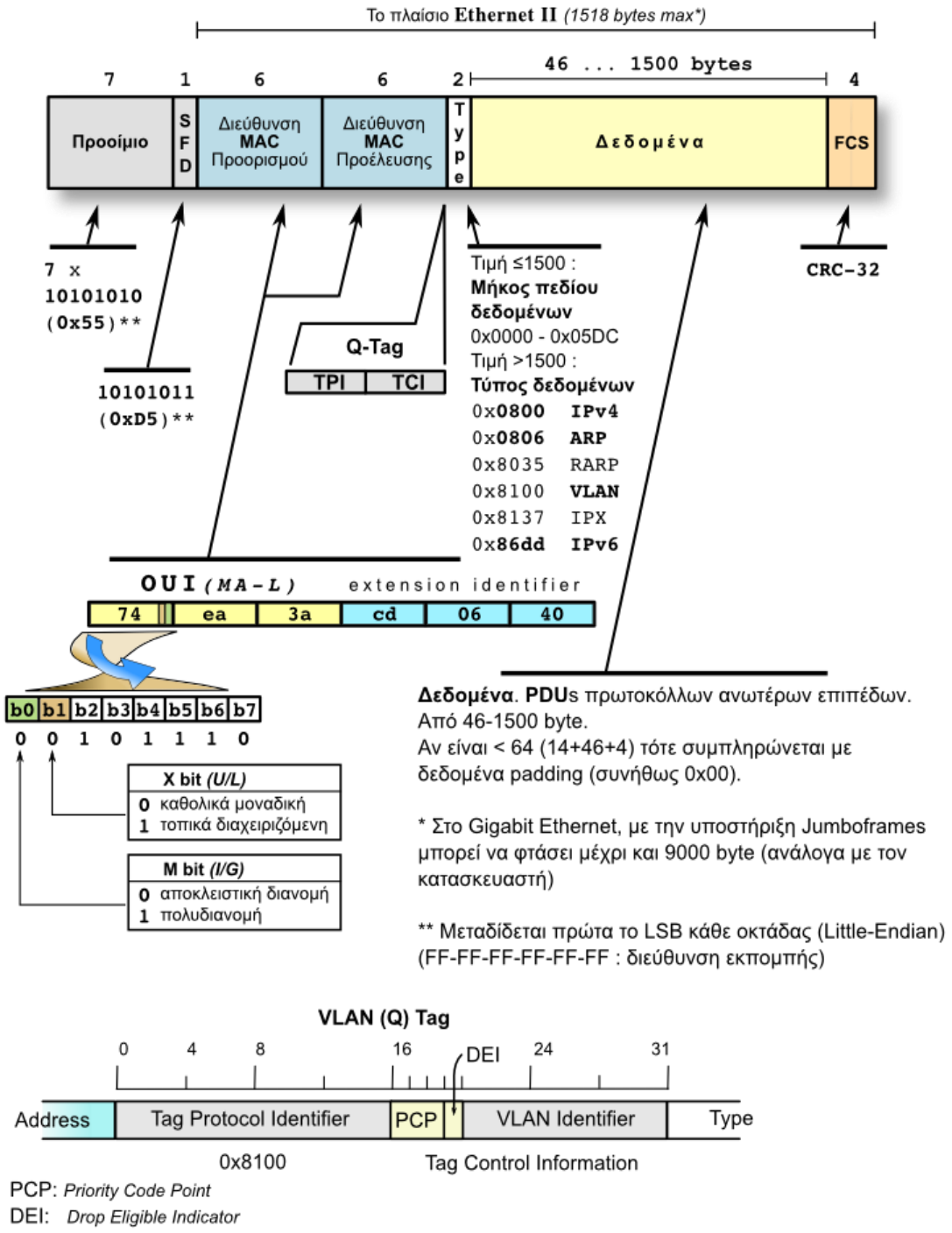
Το **Ethernet** είναι το πιο γνωστό Τοπικό Δίκτυο υπολογιστών ενσύρματης δικτύωσης. Αναπτύχθηκε από την εταιρεία Xerox κατά τη δεκαετία του '70 και έγινε δημοφιλές αφότου η Digital Equipment Corporation και η Intel, από κοινού με τη Xerox (DIX από το αρχικό γράμμα του ονόματος της κάθε εταιρίας), προχώρησαν στην προτυποποίησή του το 1980 με υποστηριζόμενο ρυθμό μετάδοσης δεδομένων 10Mbps. Το 1985 το Ethernet έγινε αποδεκτό επίσημα από τον οργανισμό IEEE ως το πρότυπο 802.3 για ενσύρματα τοπικά δίκτυα (LAN).

Σήμερα οι επιμέρους υπολογιστές του δικτύου συνδέονται ο καθένας σε ανεξάρτητη θύρα ενός μεταγωγέα (switch) ή διανομέα (hub). Έχουν εμφανιστεί νεότερες εκδόσεις του Ethernet οι οποίες χρησιμοποιούν είτε κοινά καλώδια χαλκού με αθωράκιστα (καλώδια UTP) ή θωρακισμένα (καλώδια STP) συνεστραμμένα ζεύγη αγωγών ή οπτικές ίνες:

- **Ethernet** (10MBps)
- **Fast Ethernet** (100 Mbps)
- **Gigabit Ethernet** (1 Gbps)
- **10 Gigabit Ethernet** (10Gbps)
- **40 Gigabit Ethernet** (40Gbps)
- **100 Gigabit Ethernet** (100Gbps)

Οι προδιαγραφές που ορίζει το Ethernet αφορούν το φυσικό επίπεδο και το υποεπίπεδο MAC του μοντέλου αναφοράς OSI. Στη μεγάλη πλειονότητα των περιπτώσεων μαζί με το Ethernet χρησιμοποιείται, στο υποεπίπεδο LLC, το πρωτόκολλο IEEE 802.2. Για τον έλεγχο πρόσβασης στο κοινό μέσο το Ethernet αξιοποιεί τον αλγόριθμο CSMA/CD (Carrier Sense Multiple Access with Collision Detection), στις περιπτώσεις όπου επιτρέπεται μόνο half-duplex σύνδεση.

Πρακτικά, το Ethernet χρησιμοποιεί τη μέθοδο μετάδοσης δεδομένων σε μορφή πακέτων (packet switching) μέγιστου μεγέθους (Maximum Transmission Unit, MTU) 1500 bytes και ελάχιστου 46 bytes. Για το σκοπό αυτό, δεδομένα με μήκος μεγαλύτερο των 1500 bytes τέμνονται σε πακέτα των 46-1500 bytes (το λεγόμενο payload) τα οποία αποστέλλονται διαδοχικά στη γραμμή επικοινωνίας. Αν το payload έχει μήκος μικρότερο των 46 bytes, προστίθενται επιπλέον κενά bytes ώστε αυτό να αποκτήσει το επιθυμητό ελάχιστο μήκος. Επιπλέον του payload, προστίθενται πληροφορίες όπως ο σειριακός αριθμός της κάρτας Ethernet, οι φυσικές διευθύνσεις (MAC addresses) αποστολέα και παραλήπτη, το μήκος του payload, καθώς και δεδομένα για έλεγχο σφαλμάτων κατά τη μετάδοση.



Εικόνα 4: Δομή πλαισίου και διεύθυνσης MAC στο Ethernet

1.5 IP Διευθυνσιοδότηση

1.5.1 Διεύθυνση IP

Μία διεύθυνση IP (IP address - Internet Protocol address), είναι ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές για τη μεταξύ τους αναγνώριση και συνεννόηση σε ένα δίκτυο υπολογιστών που χρησιμοποιεί το Internet Protocol standard. Κάθε συσκευή που ανήκει στο δίκτυο πρέπει να έχει τη δική της μοναδική διεύθυνση. Μία διεύθυνση IP μπορεί να θεωρηθεί το αντίστοιχο μιας διεύθυνσης κατοικίας ή ενός αριθμού τηλεφώνου για έναν υπολογιστή ή άλλη συσκευή δικτύου στο Διαδίκτυο. Όπως κάθε διεύθυνση κατοικίας και αριθμός τηλεφώνου αντιστοιχούν σε ένα και μοναδικό κτίριο ή τηλέφωνο, μια IP address χρησιμοποιείται για τη μοναδική αναγνώριση ενός υπολογιστή ή άλλης συσκευής που συνδέεται στο δίκτυο.

Μια διεύθυνση IP μπορεί να "μοιράζεται" σε πολλές συσκευές - πελάτες είτε επειδή αυτές είναι μέρος ενός shared hosting web server environment, είτε λόγω ενός proxy server (π.χ. ενός Παροχέα Υπηρεσιών Διαδικτύου (ISP) ή μιας υπηρεσίας για εξασφάλιση ανωνυμίας - anonymizer service) που λειτουργούν ως μεσολαβητές. Στην τελευταία περίπτωση (χρήση διακομιστή μεσολάβησης) η πραγματική διεύθυνση IP μπορεί να αποκρύπτεται από το διακομιστή που δέχεται αίτηση.

Domain names

Μια υπηρεσία εύρεσης δικτύου (network lookup service), το Domain Name Service (DNS), δίνει τη δυνατότητα να αντιστοιχηθούν ονόματα υπολογιστών (hostnames) σε μια διεύθυνση IP. Με αυτό τον τρόπο, οι άνθρωποι μπορούν εύκολα να θυμούνται ένα όνομα και όχι μια σειρά αριθμών. Το DNS επιτρέπει σε πολλαπλές διευθύνσεις και ονόματα να δείχνουν σε ένα πόρο του Διαδικτύου.

Δυναμικές και στατικές διευθύνσεις IP

Οι διευθύνσεις IP ορίζονται είτε μόνιμα (για παράδειγμα, σε ένα διακομιστή ο οποίος βρίσκεται πάντα στην ίδια διεύθυνση) είτε προσωρινά από ένα πλήθος διαθέσιμων διευθύνσεων.

Δυναμικές διευθύνσεις IP

Οι δυναμικές διευθύνσεις IP δίνονται για να αναγνωρίζονται προσωρινές συσκευές όπως προσωπικοί υπολογιστές ή προγράμματα πελάτες (clients). Οι ISPs χρησιμοποιούν δυναμική κατανομή (οι διευθύνσεις IP κατανέμονται δυναμικά) για να ορίσουν διευθύνσεις από ένα μικρό πλήθος διαθέσιμων σε ένα μεγαλύτερο αριθμό πελατών. Αυτή η μέθοδος χρησιμοποιείται για

σύνδεση μέσω τηλεφώνου (dial-up), WiFi και άλλες προσωρινές συνδέσεις, επιτρέποντας σε χρήστες φορητών υπολογιστών να συνδέονται αυτόματα σε μια ποικιλία υπηρεσιών χωρίς να χρειάζεται να γνωρίζουν λεπτομέρειες σχετικά με τη δρομολόγηση (routing) του κάθε δικτύου.

Οι χρήστες με δυναμικές διευθύνσεις IP πιθανόν να έχουν προβλήματα στο να τρέχουν δικό τους mail server (διακομιστή ηλεκτρονικού ταχυδρομείου) καθώς τα τελευταία χρόνια υπηρεσίες όπως το mail-abuse.org έχουν συλλέξει λίστες από σειρές (ranges) διευθύνσεων IP (διευθύνσεις δηλαδή που έχουν ίδια κάποια αρχικά ψηφία) και τις έχουν μπλοκάρει.

Η δυναμική κατανομή διευθύνσεων IP απαιτεί έναν κεντρικό διακομιστή (server) για να ακούει τα αιτήματα και να ορίσει έπειτα μια διεύθυνση. Οι διευθύνσεις μπορούν να οριστούν τυχαία ή να βασιστούν σε μια προκαθορισμένη πολιτική (policy). Το πιο συνηθισμένο πρωτόκολλο που χρησιμοποιείται για τον ορισμό διευθύνσεων δυναμικά είναι το Dynamic Host Configuration Protocol (DHCP). Το DHCP περιλαμβάνει ένα lease time που καθορίζει πόσο καιρό μπορεί αυτός που κάνει την αίτηση να χρησιμοποιήσει μια διεύθυνση πριν ζητήσει την ανανέωσή της, επιτρέποντας σε διευθύνσεις να παίρνονται, εαν όποιος τις ζήτησε αποσυνδεθεί.

Είναι σύνηθες να χρησιμοποιείται δυναμική κατανομή για ιδιωτικά δίκτυα. Δεδομένου ότι τα ιδιωτικά δίκτυα σπάνια παρουσιάζουν έλλειψη διευθύνσεων, είναι δυνατό να οριστεί η ίδια διεύθυνση στον ίδιο υπολογιστή με κάθε αίτηση (request) ή να καθοριστεί ένας παρατεταμένος lease time. Αυτές οι δύο μέθοδοι μιμούνται την ανάθεση στατικής διεύθυνσης IP.

Στατικές διευθύνσεις IP

Οι στατικές διευθύνσεις IP χρησιμοποιούνται για να αναγνωρίζονται ημι-μόνιμες συσκευές με σταθερές διευθύνεις IP. Οι εξυπηρετητές (servers) τυπικά χρησιμοποιούν στατικές διευθύνσεις IP. Η στατική διεύθυνση μπορεί να διαμορφωθεί άμεσα (να γίνει configured) επάνω στη συσκευή η ως μέρος της κεντρικής διαμόρφωσης DHCP που συσχετίζει τη MAC address της συσκευής με μια στατική διεύθυνση.

1.5.2 Η Δομή των διευθύνσεων IP (IP addressing version 4)

Κάθε κόμβος, ενός δικτύου Η/Υ (**network node**) που χρησιμοποιεί το πρωτόκολλο TCP/IP ή του Διαδικτύου, έχει μια μοναδική διεύθυνση IP που τον διαφοροποιεί από τους υπόλοιπους. Η διεύθυνση IP αποτελείται από τέσσερις ακέραιους αριθμούς που διαχωρίζονται με τελείες. Κάθε ένας από τους τέσσερις αριθμούς μπορεί να πάρει τιμές από 0-255 στο Δεκαδικό σύστημα, 00000000 – 11111111 στο Δυαδικό ή 00 – FF στο Δεκαεξαδικό σύστημα.

Κόμβος είναι κάθε συσκευή που συνδέεται στο δίκτυο (Η/Υ, Δρομολογητής, Camera, Δικτ. εκτυπωτής, …)

Μορφή IP διεύθυνσης : **q.x.y.z** όπου q,x.y,z ακέραιοι στο διάστημα 0-255

Παράδειγμα IP διεύθυνσης είναι το παρακάτω :

- 10101100.00010010.11011010.01100100 στο Δυαδικό
- 172.18.218.100 στο Δεκαδικό
- AC.12.DA.64 στο Δεκαεξαδικό

Στη πραγματικότητα η IP διεύθυνση αποτελείται από δυο μεταβαλλόμενα μέρη :

Στο πρώτο μέρος προσδιορίζεται το **αναγνωριστικό του δικτύου (network id),** ενώ στο δεύτερο το **αναγνωριστικό του υπολογιστή (host id)** μέσα στο δίκτυο.

Network id	**Host id**

Ανάλογα με το πόσο μεγάλο είναι το τμήμα της IP διεύθυνσης που αφιερώνεται ως διεύθυνση δικτύου οι διευθύνσεις χωρίζονται σε πέντε τάξεις ή τύπους :

Τάξη **A** : 7 bit διεύθυνση δικτύου/24 bit διεύθυνση Η/Υ **& q από 1...126**

Τάξη **B** : 14 bit διεύθυνση δικτύου / 16 bit διεύθυνση Η/Υ **& q από 128...191**

Τάξη **C** : 21 bit διεύθυνση δικτύου / 8 bit διεύθυνση Η/Υ **& q από 192...223**

Τάξη **D** : για χρήση πολλαπλής εκπομπής (multicast) **q από 224...239**

Τάξη **E** : για μελλοντική χρήση **q από 240...254**

Η **Τάξη A** υποστηρίζει 126 (2^7-2)δίκτυα με 16.777.124 Η/Υ ανά δίκτυο. Subnet mask 255.0.0.0

Η **Τάξη B** υποστηρίζει 16.382 (2^{14} -2) δίκτυα με 65.534 Η/Υ ανά δίκτυο. Subnet mask 255.255.0.0

Η **Τάξη C** υποστηρίζει 2.097.150 (2^{21} -2) δίκτυα με 254 Η/Υ ανά δίκτυο. Subnet mask 255.255.255.0

Συνολικά μπορούν να υπάρξουν 3.500.000.000 διευθύνσεις IP για αντίστοιχους κόμβους.

Επειδή παρουσιάζεται μεγάλη σπατάλη στην απόδοση των διευθύνσεων παρουσιάστηκε η ανάγκη για νεότερη έκδοση της διευθυνσιοδότησης IP (ver 6).

Ειδικές Διευθύνσεις IP

Το δίκτυο με διεύθυνση 0 αποτελεί την **μη καθορισμένη Διαδρομή (default route).**

Το δίκτυο με διεύθυνση 127 αποτελεί την **διεύθυνση επιστροφής (Loop back Address).**

Οι διευθύνσεις με αναγνωριστικό υπολογιστή (Host ID) 0 και 255 είναι **δεσμευμένες (reserved)**.

Μια IP διεύθυνση με όλα τα bit του host να είναι 0 αποτελεί τη **διεύθυνση του δικτύου**.

Π.χ. η διεύθυνση 26.0.0.0 αναφέρεται στο δίκτυο 26

η διεύθυνση 128.66.0.0 αναφέρεται στο δίκτυο 128.66

η διεύθυνση 206.32.11.0 αναφέρεται στο δίκτυο 206.32.11

Μια IP διεύθυνση με όλα τα bit του host να είναι 1 είναι η **διεύθυνση εκπομπής (broadcast address)**.

Π.χ το δίκτυο 33 έχει διεύθυνση εκπομπής την 33.255.255.255
το δίκτυο 130.55 έχει διεύθυνση εκπομπής την 130.55.255.255
το δίκτυο 193.100.11 έχει διεύθυνση εκπομπής την 193.100.11.255

Υπάρχουν και διευθύνσεις που είναι δεσμευμένες για **εσωτερικά δίκτυα** (δίκτυα δηλαδή που δεν έχουν άμεση πρόσβαση στο Διαδίκτυο). Τέτοιες είναι οι 10 για Τάξη Α' , από 172.16 ως 172.31 για Τάξη Β' , και από 192.168.0 ως 192.168.255 για Τάξη Γ που δεν μπορούν να χρησιμοποιηθούν στο Διαδίκτυο.

IANA-Δεσμευμένα Ιδιωτικά IPv4 εύρη δικτύων			
	Start	**End**	**No. of addresses**
24-bit Block (/8 prefix, 1 × A)	10.0.0.0	10.255.255.255	16777216
20-bit Block (/12 prefix, 16 × B)	172.16.0.0	172.31.255.255	1048576
16-bit Block (/16 prefix, 256 × C)	192.168.0.0	192.168.255.255	65536

Εικόνα 5: Δεσμευμένες διευθύνσεις

Default Gateway (**προεπιλεγμένη πύλη**) είναι η διεύθυνση IP που χρειάζεται για τη δρομολόγηση ενός πακέτου εκτός των ορίων του τοπικού δικτύου αν αυτό δεν απευθύνεται σε κάποιον από τους σταθμούς του δικτύου. Είναι απαραίτητη σε δίκτυα που συνδέονται στο Διαδίκτυο.

Υπηρεσία DNS είναι η υπηρεσία που αναλαμβάνει την αντιστοίχιση IP διευθύνσεων σε συμβολικά ονόματα με συγκεκριμένη όμως κατάληξη (.com, .edu, .org, info, net, mil, biz αλλά και .gr , .uk, .ca, ru, …).

Η απόδοση διευθύνσεων IP σε ένα δικτυακό Η/Υ γίνεται είτε αυτόματα με **DHCP** (Dynamic Host Configuration Protocol) είτε χειροκίνητα.

Το DHCP είναι μια υπηρεσία που ακολουθεί το μοντέλο Πελάτη Εξυπηρετητή (**Client Server**) και στην οποία ο Εξυπηρετητής αναλαμβάνει να δώσει στους πελάτες IP διευθύνσεις, μάσκα υποδικτύου και διεύθυνση default gateway.

Το **DHCP** επιτρέπει σε ένα υπολογιστή να συνδεθεί σε ένα δίκτυο που στηρίζεται στο IP (IP-based network) χωρίς να έχεις μια προρυθμισμένη διεύθυνση IP. Το DHCP είναι ένα πρωτόκολλο που αποδίδει μια μοναδική διεύθυνση σε κάθε συσκευή , μετά ελευθερώνει και ανανεώνει αυτές τις διευθύνσεις καθώς οι συσκευές εγκαταλείπουν και ξανασυνδέονται στο δίκτυο.

DHCP Server σε ένα τοπικό δίκτυο είναι είτε ο Δρομολογητής (Router) είτε ο Εξυπηρετητής (Server). Σε κάθε περίπτωση μόνο ένας DHCP Server επιτρέπεται σε ένα δίκτυο υπολογιστών.

Μάσκα Υποδικτύου (Netmask ή Subnet Mask) είναι ένας αριθμός 32bit (όσο και η διεύθυνση IP) που χρησιμοποιείται για να διαχωρίσει τα τμήματα δικτύου (network id) και υπολογιστή (host id) σε μια διεύθυνση IP.

Class A default (προκαθορισμένη)	255.0.0.0
Class B default (προκαθορισμένη)	255.255.0.0
Class C default (προκαθορισμένη)	255.255.255.0

Η **Ανεξαρτήτου Κλάσεων Δρομολόγηση Υπερ-περιοχών** (Classless Interdomain Routing - CIDR) καταργεί τις κλάσεις διευθύνσεων με αποτέλεσμα τα τμήματα Δικτύου και Υπολογιστή κάθε διεύθυνσης να καθορίζονται κατά περίπτωση με βάση τις ανάγκες κάθε οργανισμού . Το μέγεθος του τμήματος δικτύου προσδιορίζεται από το πρόθεμα - routing prefix (μια / και ένας αριθμός από bit μάσκας μετά την διεύθυνση) που δηλώνει το μέγεθος της μάσκας δικτύου πχ. Η διεύθυνση 66.100.50.0 με μάσκα 255.255.255.0 εκφράζεται ως : 66.100.50.0/24.

Το σύστημα CIDR χρησιμοποιείται κυρίως από τις Εταιρίες Παροχής Υπηρεσιών Διαδικτύου (ΕΠΥΔ ISP's) για να δίνουν μικρά κομμάτια διευθύνσεων στους πελάτες τους.

Τάξη	Αρχικά bit	Από	Μέχρι	Προκαθορισμένη μάσκα υποδικτύου	Πρόθεμα CIDR
A	0	0.0.0.0	127.255.255.255	255.0.0.0	/8
B	10	128.0.0.0	191.255.255.255	255.255.0.0	/16
C	110	192.0.0.0	223.255.255.255	255.255.255.0	/24

Εικόνα 6: Μάσκες υποδικτύου

Αταξική Δρομολόγηση Δικτυακών Περιοχών

Ο όρος CIDR, ακρωνύμιο των λέξεων "Classless Inter Domain Routing", δηλαδή "Αταξική Δρομολόγηση δικτυακών Περιοχών" προσδιορίζει μια νέα (1993) τεχνική δρομολόγησης πακέτων από/προς δίκτυα διαφορετικών περιοχών που αντικατέστησε την "Ταξική Δρομολόγηση" στο Διαδίκτυο και αφορά την κατανομή IP διευθύνσεων στην Κοινότητα του Διαδικτύου.

Η όρος "τάξη" (class) επίσης αναφέρεται και ως "τύπος". Ο όρος CIDR σχετίζεται επίσης με νέο τύπο διευθύνσεων για τα πακέτα που δεν ανήκουν πλέον σε μία από τις τρεις τάξεις (δηλ. τύπους) class A, class B, class C. Η εξάντληση των διευθύνσεων τύπου B (δίκτυα χωρητικότητας μέχρι 255 χ 255 συστημάτων) και τύπου C (μέχρι 255 συστήματα) οδήγησε στην κατάργηση των "τάξεων" για να βελτιωθεί η χρήση των διευθύνσεων, καθώς ο τρόπος παραχώρησης ήταν μάλλον χαλαρός, δηλαδή ένας οργανισμός με τρέχουσες ανάγκες και μελλοντικές σαφώς μικρότερες των 64.000 συστημάτων εύκολα αποκτούσε διευθύνσεις τύπου B.

Το κάθε δίκτυο πλέον λαμβάνει τόση ποσότητα διευθύνσεων όση πραγματικά χρειάζεται.

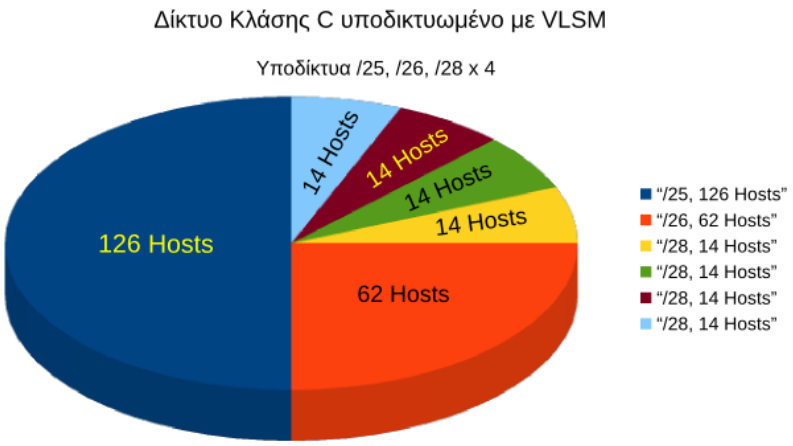
1.6 IP υποδίκτυα

Ο χωρισμός ενός δικτύου σε μικρότερα δίκτυα ονομάζεται υποδικτύωση. Για τον εξωτερικό κόσμο το συνολικό δίκτυο παραμένει ενιαίο. Η συνηθέστερη χρήση των υποδικτύων είναι για τον διαχωρισμό τμημάτων σε οργανισμούς, ανάλογα με τις αρμοδιότητές τους και τις ανάγκες τους σε επίπεδο ιδιωτικότητας και ασφάλειας. Με την χρήση υποδικτύων η διαχείριση του συνολικού δικτύου γίνεται ευκολότερη και αυξάνεται η απόδοσή του.

Ο καθορισμός των υποδικτύων γίνεται από τον διαχειριστή του δικτύου, ο οποίος ανάλογα με τις ανάγκες του οργανισμού, την ήδη υπάρχουσα οργάνωσή του, την τοπολογία του δικτύου και τις μελλοντικές απαιτήσεις ανάπτυξης επιλέγει την κατάλληλη μορφή υποδικτύωσης. Για την επικοινωνία των υποδικτύων είναι απαραίτητη η χρήση δρομολογητή.

Για την δημιουργία υποδικτύων χρησιμοποιούνται bit από το host τμήμα της IP διεύθυνσης. Για παράδειγμα, για την δημιουργία υποδικτύων σε μία τάξης C διεύθυνση αποσπούμε bit από την τελευταία οκτάδα. Παρόμοια, για την δημιουργία υποδικτύων σε μία τάξης B διεύθυνση αποσπούμε bits από τις δύο τελευταίες οκτάδες.

Η μάσκα υποδικτύου (ή δικτύου) είναι ένας 32-bit αριθμός που αποτελείται από συνεχόμενα bits με τιμή 1 και τα υπόλοιπα με τιμή 0. Τα bit με τιμή 1 δηλώνουν τον αριθμό των bit που χρησιμοποιούνται για την δημιουργία υποδικτύων.



Εικόνα 7: Παράδειγμα υποδικτύωσης με χρήση τεχνικής VLSM

Ο συνηθέστερος τρόπος αναπαράστασης της μάσκας είναι με χρήση του χαρακτήρα /. Ο αριθμός που ακολουθεί το / δηλώνει τον αριθμό των συνεχόμενων bits με τιμή 1. Για παράδειγμα, η μάσκα /16 ισοδυναμεί με 255.255.0.0.

Ένα δίκτυο μπορεί να χωρίζεται σε υποδίκτυα που έχουν την ίδια μάσκα ή σε υποδίκτυα με διαφορετική μάσκα (VLSM).

Η πρώτη και τελευταία διεύθυνση σε ένα υποδίκτυο έχουν ειδική σημασία και δεν αποδίδονται σε υπολογιστές. Η πρώτη δηλώνει την διεύθυνση του υποδικτύου και η τελευταία την broadcast διεύθυνση του υποδικτύου.

Μάσκα	CIDR value	Μάσκα	CIDR value
255.0.0.0	/8	255.255.240.0	/20
255.128.0.0	/9	255.255.248.0	/21
255.192.0.0	/10	255.255.252.0	/22
255.224.0.0	/11	255.255.254.0	/23
255.240.0.0	/12	255.255.255.0	/24
255.248.0.0	/13	255.255.255.128	/25
255.252.0.0	/14	255.255.255.192	/26
255.254.0.0	/15	255.255.255.224	/27
255.255.0.0	/16	255.255.255.240	/28
255.255.128.0	/17	255.255.255.248	/29
255.255.192.0	/18	255.255.255.252	/30
255.255.224.0	/19		

Εικόνα 8: Μάσκες υποδικτύων και αντιστοίχιση με CIDR prefix

1.7
Το πρωτόκολλο ICMP

Η αξιοπιστία του Internet στηρίζεται στη δυνατότητα των δρομολογητών να επικοινωνούν μεταξύ τους. Για το λόγο αυτό έχει δημιουργηθεί το πρωτόκολλο *ICMP (Internet Control Message Protocol)*. Συγκεκριμένα το πρωτόκολλο χρησιμοποιείται για τη συγκέντρωση πληροφοριών σχετικά με τις συνδέσεις του δικτύου και τις διαδρομές δρομολόγησης.

1.7.1 Ping

Το ICMP ορίζει τύπους μηνυμάτων για διάφορους σκοπούς. Μεταξύ αυτών είναι και οι τύποι Echo Request και Echo Reply. Το πακέτο Echo Request χρησιμοποιείται για να διαπιστωθεί αν ένας υπολογιστής λειτουργεί. Αν αυτό ισχύει, αυτός θα απαντήσει με ένα πακέτο Echo Reply. Το πρόγραμμα ping χρησιμοποιεί τα μηνύματα αυτά για τον παραπάνω σκοπό. Μπορείτε να ελέγξετε αν ένας τυχαίος υπολογιστής με διεύθυνση *ip_address* λειτουργεί, με την εντολή: **ping *ip_address*** Παρατηρήστε τον αριθμό των πακέτων που στάλθηκαν, το μέγεθός τους, τη συνολική μέση καθυστέρηση και το ποσοστό απώλειας πακέτων.

1.7.2 Traceroute

Ένα ενδιαφέρον πρόγραμμα που χρησιμοποιεί τους μηχανισμούς του πρωτοκόλλου ICMP είναι το traceroute. Χρησιμοποιείται για να βρεθεί η διαδρομή που θα ακολουθήσουν τα πακέτα ενός υπολογιστή προς ένα συγκεκριμένο προορισμό, καθώς και σε περιπτώσεις δυσλειτουργίας, για να ανιχνευτεί ο υπεύθυνος δρομολογητής. Ο ακριβής μηχανισμός που χρησιμοποιείται για το σκοπό αυτό είναι γνωστός με τον όρο Expanding Ring Search. Μπορείτε να χρησιμοποιήσετε την εντολή traceroute ως εξής: **traceroute *ip_address.***

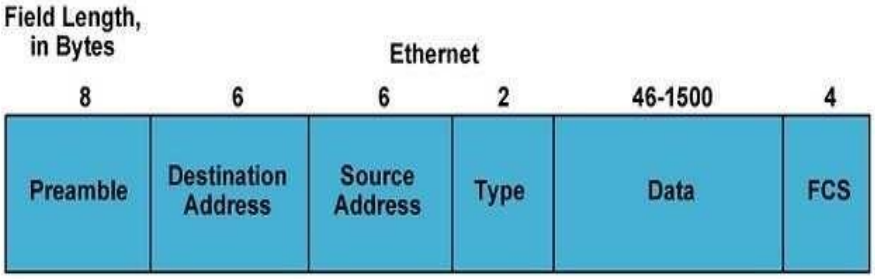
ΚΕΦΑΛΑΙΟ 2

Οι Μεταγωγείς (switches) τα VLAN και το πρωτόκολλο SpanningTree

2.1. Μεταγωγείς επιπέδου 2 (LAYER 2 SWITCHES)

2.1.1 Πλαίσια

Τα LAN εξασφαλίζουν τη μετακίνηση δεδομένων μεταξύ των υπολογιστών και των συσκευών που συμμετέχουν στο LAN, ώστε να μπορούν να επικοινωνούν. Για να γίνει αυτό, το λογισμικό των δικτύων οργανώνει τα δεδομένα σε πλαίσια που λέγονται Ethernet Frames. Τα πλαίσια που ταξιδεύουν μέσα σε ένα δίκτυο περιέχουν ακολουθίες πληροφοριών των οποίων η μορφή είναι τυποποιημένη.
Η μορφή για ένα τέτοιου είδους πλαισίου Ethernet, περιλαμβάνει μια διεύθυνση προορισμού στην αρχή που περιέχει τη διεύθυνση της συσκευής στην οποία αποστέλλεται το πλαίσιο. Ακολουθεί μια διεύθυνση αποστολέα που περιέχει τη διεύθυνση της συσκευής που στέλνει το πλαίσιο. Οι διευθύνσεις ακολουθούνται από διάφορα άλλα πεδία, συμπεριλαμβανομένου το πεδίο δεδομένων που μεταφέρει τα δεδομένα που αποστέλλονται μεταξύ των υπολογιστών, όπως φαίνεται στην εικόνα που ακολουθεί.



Εικόνα 9: : Βασική δομή ενός Ethernet Frame

Τα πλαίσια καθορίζονται από το δεύτερο επίπεδο του μοντέλου αναφοράς OSI, το επίπεδο σύνδεσης δεδομένων. Το μοντέλο αναφοράς OSI αναπτύχθηκε για να οργανώνει τα είδη των πληροφοριών που αποστέλλονται μεταξύ των υπολογιστών. Χρησιμοποιείται για να καθορίσει τον τρόπο με τον οποίο θα αποστέλλονται οι πληροφορίες και να δομήσει την ανάπτυξη των προτύπων για τη μεταφορά των δεδομένων. Από τότε που τα Ethernet switches λειτουργούν βάση των πλαισίων ενός τοπικού δικτύου στο επίπεδο σύνδεσης δεδομένων, θα ακούσετε να αναφέρονται σε αυτά με διάφορες ορολογίες όπως συσκευές διασύνδεσης ή συσκευές δευτέρου επιπέδου ή μεταγωγείς δευτέρου επιπέδου.
Ένα switch δέχεται τυπικά τρία είδη πλαισίων, χωρίς κάποιο συγκεκριμένο προορισμό. Τα πλαίσια αυτά με τη σειράς τους μεταδίδονται προς όλες τις θύρες ενός switch εκτός της θύρας από την οποία έφτασε στο switch. Τέτοιου είδους πλαίσια είναι τα broadcast frames, τα multicast frames και τα unknown unicast frames.

Τα πλαίσια μετάδοσης (broadcast frames) και τα πολλαπλής διανομής πλαίσια (multicast frames) έχουν ένα κοινό χαρακτηριστικό. Κανένα από τα δύο είδη δεν έχει κάποιο συγκεκριμένη διεύθυνση υλικού προορισμού. Η διεύθυνση του αποστολέα είναι επίσης η διεύθυνση υλικού της συσκευής που στέλνει το πλαίσιο. Στη περίπτωση των broadcast frames, η διεύθυνση προορισμού που εμφανίζεται στην κεφαλίδα ενός πακέτου είναι όλα της μορφής 1, που υποδεικνύει πως η μετάδοση πηγαίνει σε όλους τους κόμβους του δικτύου. Στη περίπτωση ενός multicast frame, το πλαίσιο καθορίζει ένα δίκτυο, αλλάζοντας όλα τα bits διεύθυνσης του δέκτη σε 1. Για παράδειγμα, ένα broadcast frame και ένα multicast frame σε δυαδική μορφή φαίνονται στο παρακάτω πίνακα .

Frame Type	Binary Value	Broadcast Address
Broadcast	11111111.11111111.11111111.11111111	255.255.255.255
Multicast	00001010.00000001.11111111.11111111	10.1.255.255

Εικόνα 10: Παράδειγμα Broadcast and Multicast destination addresses

Ένα άγνωστο μοναδικής διανομής πλαίσιο (unknown unicast) είναι παρόμοιο με ένα broadcast frame. Αυτό του είδους πλαισίου αποστέλλεται όταν η διεύθυνση προορισμού είναι άγνωστη από το switch. Σε αυτή τη περίπτωση, το switch προωθεί το πλαίσιο ακολουθώντας την ίδια διαδικασία με το broadcast frame. Το πλαίσιο αποστέλλεται σε όλες τις θύρες εκτός της θύρας που έλαβε το πλαίσιο.

Όταν ένα switch λαμβάνει ένα από αυτά τα πλαίσια με άγνωστες διευθύνσεις προορισμού τότε τα αποστέλλει προς όλες τις θύρες εκτός της θύρας που έλαβε το πλαίσιο. Η διαδικασία αυτή είναι γνωστή με τον όρο πλημμύρα.

Ωστόσο συμβαίνει μόνο σε όλες τις θύρες ενός switch που δεν είναι συνδεδεμένα με εικονικά δίκτυα (Virtual LANs) και σε επιλεγμένες θύρες του switch που είναι συνδεδεμένες με τέτοιου είδους δίκτυα.

Επιπλέον για τα vlans, έχουν αναπτυχθεί τεχνικές που ελέγχουν τις υπερβολικές μεταδόσεις. Τέτοιες τεχνικές είναι το spoofing. Με αυτή τη τεχνική κάποια switches που δεν παίρνουν πλήρης λειτουργικότητα δρομολόγησης, παρεμβαίνουν σε κάποια πρωτόκολλα όπως NetWare's SAP and RIP. Η τεχνική αυτή είναι ιδιαίτερα πολύτιμη για τις γραμμές χαμηλής ταχύτητας, που μπορούν εύκολα να υπερφορτωθούν από διαφημιστικές διανομές, ενημερώσεις διαδρομών του δικτύου ή από την διαθεσιμότητα του διακομιστή.

Κάποια switches επιτρέπουν στο διαχειριστή του δικτύου να επιλέξει ένα μέγιστο επίπεδο διανομής και να απορρίψει τις διανομές που υπερβαίνουν το όριο αυτό. Αν το επίπεδο επιλεχτεί προσεχτικά, το επίπεδο αυτό δεν θα ξεπερνιέται ποτέ παρά μόνο σε περίπτωση που συμβεί broadcast storm.

2.1.2 Διαφορές μεταξύ Bridges και Switches

Όπως έχουμε αναφέρει τα switches είναι συσκευές παρόμοιες με τις γέφυρες παρόλο που έχουν κάποιες σημαντικές λεπτές τεχνολογικές διαφορές μεταξύ τους.

Πρώτον, οι γέφυρες ήταν σχεδιασμένες να λειτουργούν με βάση το λογισμικό ώστε να σχεδιάζουν και να διατηρούν το δικό τους πίνακα φυσικών διευθύνσεων ενώ τα switches σχεδιάστηκαν να λειτουργούν βάση του υλικού αφού χρησιμοποιούν συγκεκριμένη εφαρμογή ολοκληρωμένων κυκλωμάτων για να χτίσουν και να διατηρήσουν τον πίνακα φυσικών διευθύνσεων τους. Διαφορετικά οι γέφυρες και τα switch είναι ταυτόσημα στη λειτουργία τους. Ένα switch επίσης μπορεί να θεωρηθεί ως μια γέφυρα με πολλαπλές θύρες και μπορεί να έχει πολλές περιπτώσεις του Spanning Tree Protocol, ενώ η γέφυρα μπορεί να έχει μόνο μία.

Παρ' όλα αυτά, και τα switches και οι γέφυρες προωθούν πλαίσια του επιπέδου 2, μαθαίνουν τις φυσικές διευθύνσεις εξετάζοντας τη διεύθυνση της πηγής του κάθε πλαισίου που καταφθάνουν σε αυτά και τέλος παίρνουν αποφάσεις προώθησης των πλαισίων με βάση τη διευθυνσιοδότηση του επιπέδου 2.

2.1.3 Λειτουργίες των Layer 2 Switches

Τα switches για να μπορούν να προωθούν τα πλαίσια από τη μία θύρα στην άλλη, αλλά και σε άλλες συσκευές, εκτελούν τρεις διαφορετικές λειτουργίες του επιπέδου 2 που είναι αρκετά σημαντικές: τη λειτουργία Address Learning, Forward/Filter Decisions, και τη λειτουργία Loop Avoidance. Ας δούμε συνοπτικά τις λειτουργίες αυτές μία προς μία.

- **Address Learning** (εκμάθηση διευθύνσεων): Τα switches επιπέδου 2 αποθηκεύουν και διατηρούν τις φυσικές διευθύνσεις (Media Access Control Addresses) των υλικών πηγών του κάθε πλαισίου που λαμβάνονται σε μια διασύνδεση και εισάγουν τις πληροφορίες αυτές σε μια βάση δεδομένων φυσικών διευθύνσεων που λέγεται πίνακας forward/filter.
- **Forward/Filter Decisions** (αποφάσεις προώθηση/φιλτραρίσματος): Όταν ένα πλαίσιο λαμβάνεται σε μία διασύνδεση, το switch κοιτάζει τη διεύθυνση υλικού προορισμού και έπειτα διαλέγει από το πίνακα forward/filter τη κατάλληλη διεπαφή εξόδου για να αποστείλει το πλαίσιο. Με αυτό τον τρόπο, το πλαίσιο προωθείται μόνο από τη σωστή θύρα προορισμού.
- **Loop Avoidance** (αποφυγή βρόχου): Αν δημιουργήσουμε πολλαπλές συνδέσεις μεταξύ των switches σε ένα δίκτυο για λόγους εφεδρείας τότε υπάρχει το ενδεχόμενα να προκληθούν δικτυακοί βρόχοι. Το Spanning Tree Protocol χρησιμοποιείται για να εμποδίσει τη δημιουργία βρόχων στο δίκτυο επιτρέποντας την ύπαρξη εφεδρικών διαδρομών μεταξύ των switches.

2.1.4 Address Learning

Ένα Ethernet switch ελέγχει τη μεταφορά των πλαισίων μεταξύ των θυρών του, που συνδέονται με τα καλώδια Ethernet χρησιμοποιώντας του κανόνες μετάδοσης της κίνησης που περιγράφονται στο πρότυπο 802.1D. Η μετάδοση της κίνησης βασίζεται στην εκμάθηση των φυσικών διευθύνσεων. Τα switches αποφασίζουν τη προώθηση κίνησης βάση των 48-bit φυσικών διευθύνσεων που χρησιμοποιούνται στις προδιαγραφές ενός Ethernet LAN.

Ένα switch που βρίσκεται σε ένα δίκτυο, έρχεται πρώτη φορά σε λειτουργία, ο πίνακας MAC forward/filter είναι κενός.

Όταν μια συσκευή του δικτύου μεταδίδει πλαίσια και μια διεπαφή τα λάβει, το switch τότε τοποθετεί τη διεύθυνση υλικού πηγής που έστειλε το πλαίσιο, στο πίνακα MAC forward/filter, που του επιτρέπει να θυμάται που βρίσκεται η διεπαφή της συσκευής που έστειλε το πλαίσιο. Το switch αναγκάζεται να πλημμυρίσει το δίκτυο, στέλνοντας το πλαίσιο από όλες τις θύρες εκτός από τη θύρα που παρέλαβε το συγκεκριμένο πλαίσιο διότι δεν γνωρίζει τη διεύθυνση προορισμού του πλαισίου.

Αν μια συσκευή απαντήσει σε αυτό το πλαίσιο στέλνοντας ένα άλλο πλαίσιο ως απάντηση, το switch τότε θα πάρει τη φυσική διεύθυνση του αποστολέα και θα τη βάλει στο πίνακα του, συσχετίζοντας τη διεύθυνση αυτή με την διεπαφή που δέχτηκε το πλαίσιο. Έχοντας πλέον το switch και τις δύο σχετικές διευθύνσεις στη βάση δεδομένων του, οι δύο αυτές συσκευές μπορούν να συνδεθούν από σημείο-σε σημείο. Το switch δεν θα χρειαστεί να ξαναπλημμυρίσει το δίκτυο με το πλαίσιο όπως τη πρώτη φορά διότι τα πλαίσια πλέον μπορούν και προωθούνται μόνο μεταξύ αυτών των δύο συσκευών μέσω του switch.

Αν κάποια συσκευή δεν επικοινωνήσει για ένα χρονικό διάστημα με το switch, τότε το switch διαγράφει τις εγγραφές της συγκεκριμένης συσκευής από τη βάση δεδομένων του για να τη διατηρήσει όσο πιο ενημερωμένη μπορεί.

Για το λόγο αυτό, τα επιπέδου 2 switches είναι πολύ ανώτερα των hubs. Σε δίκτυα που είναι συνδεδεμένα μέσω hubs, όλα τα πλαίσια προωθούνται από όλες τις θύρες τους κάθε φόρα, ότι και αν συμβεί.

2.1.5 Forward/Filter Decicions

Αφού τελικά το switch έχει γεμίσει το πίνακα με τις φυσικές διευθύνσεις, έχει όλες τις απαραίτητες πληροφορίες που χρειάζεται για να ξεκινήσει το φιλτράρισμα και τη προώθηση των πλαισίων επιλεκτικά στο δίκτυο. Καθώς το switch μαθαίνει τις φυσικές διευθύνσεις, ταυτόχρονα ελέγχει κάθε πλαίσιο για να πάρει μια απόφαση προώθησης πακέτου βάση της διεύθυνσης προορισμού που έχει το πλαίσιο.

Επίσης, κάθε θύρα του switch μπορεί να κρατάει πλαίσια στην μνήμη της πριν τα μεταδώσει από το καλώδιο Ethernet που είναι συνδεδεμένο σε αυτή. Για παράδειγμα, αν μια θύρα είναι ήδη απασχολημένη προωθώντας κάποιο πλαίσιο, και φτάσει ένα δεύτερο πλαίσιο για μετάδοση, τότε το πλαίσιο κρατείται για ένα μικρό χρονικό διάστημα, ώστε να ολοκληρώσει τη μετάδοση του προηγούμενου πλαισίου.

Για να μεταδώσει το πλαίσιο, το switch τοποθετεί το πλαίσιο στην ουρά μεταγωγής πακέτου.

Όταν ένα πλαίσιο φτάσει σε μια διεπαφή του switch, το switch ελέγχει αν η διεύθυνση προορισμού του υλικού βρίσκεται στο πίνακα forward/filter MAC database. Αν είναι γνωστή και βρίσκεται στον πίνακα η διεύθυνση, τότε το πλαίσιο αποστέλλεται μόνο από την κατάλληλη εγγεγραμμένη διεπαφή εξόδου. Κατά τη διάρκεια της διαδικασίας αυτής, το switch που μεταδίδει το πλαίσιο από τη μια θύρα στην άλλη, δεν πραγματοποιεί καμία αλλαγή σε κανένα πεδίο του πλαισίου. Το switch δεν θα μεταδώσει το πλαίσιο από οποιαδήποτε διεπαφή, εξαιρώντας την διεπαφή προορισμού. Να σημειωθεί πως ένα switch δεν θα προωθήσει κάποιο πλαίσιο που έχει προορισμό έναν σταθμό και βρίσκεται στη βάση δεδομένων προώθησης της θύρας εκτός αν η θύρα είναι συνδεδεμένη με το προορισμό στόχο. Δηλαδή η κίνηση που προορίζεται για μια συσκευή σε μια συγκεκριμένη θύρα, θα σταλεί μόνο σε εκείνη τη θύρα, και καμία άλλη θύρα δεν θα δει τη κίνηση που προορίζεται για την εν λόγω συσκευή. Αυτή η λογική μεταγωγής κρατάει τη κίνηση απομονωμένη μόνο για τα καλώδια Ethernet ή τα τμήματα που απαιτούνται για να λάβουν το πλαίσιο από τον αποστολέα και να μεταδώσουν το πλαίσιο στη συσκευή προορισμού.

Αυτό εμποδίζει τη ροή μη απαραίτητης κίνησης σε άλλα τμήματα του δικτύου, το οποίο είναι τεράστιο πλεονέκτημα για ένα switch. Αυτό έρχεται σε αντίθεση με τα πρώτα συστήματα Ethernet, όπου η κίνηση από οποιονδήποτε σταθμό γινόταν γνωστή σε όλους τους σταθμούς του δικτύου, είτε χρειαζόταν τις πληροφορίες είτε όχι. Το φιλτράρισμα της κίνησης των switches μειώνει το κυκλοφοριακό φόρτο που μεταφέρεται από το σύνολο των καλωδίων Ethernet που είναι συνδεδεμένα στο switch, καθιστώντας έτσι πιο αποτελεσματική χρήση του εύρους ζώνης του δικτύου. Αυτή η διαδικασία ονομάζεται φιλτράρισμα πλαισίου (frame filtering).

Αν όμως η διεύθυνση προορισμού του υλικού δεν είναι γνωστή και δεν είναι εγγεγραμμένη στο πίνακα forward/filter MAC database τότε το πλαίσιο αποστέλλεται από όλες τις ενεργές διεπαφές εκτός της διεπαφής που έφτασε το πλαίσιο. Έπειτα αν κάποια άλλη συσκευή απαντήσει σε αυτό το διαμοιραζόμενο πλαίσιο, τότε το switch θα ενημερώσει τη βάση δεδομένων του με τη διεύθυνση της συσκευής ώστε να έχει τη σωστή διασύνδεση.

2.1.6 Loop Avoidance

Οι εφεδρικές συνδέσεις μεταξύ των switches είναι μια πολύ καλή ιδέα διότι βοηθούν στην αποτροπή πλήρης αποτυχιών του δικτύου σε περίπτωση που μια ενεργή σύνδεση σταματήσει να λειτουργεί.

Παρ’ όλο όμως που οι συνδέσεις αυτές μπορεί να είναι υπερβολικά χρήσιμες, μπορούν να δημιουργήσουν περισσότερα προβλήματα από όσα μπορούν να λύσουν. Κάποια από αυτά τα προβλήματα αναλύονται στη συνέχεια.

Σε ένα δίκτυο μπορεί να προκύψει μεγάλη συσσώρευση από την κίνηση πλαισίων broadcast και multicast που προωθούν τα switches ασταμάτητα. Αυτό συμβαίνει

όταν διαφορετικοί κόμβοι στέλνουν δεδομένα πάνω σε μία σύνδεση, και οι άλλες συσκευές που δέχονται τα δεδομένα αυτά, τα αναμεταδίδουν πίσω στο σύνδεσμο του δικτύου ως απάντηση, προκαλώντας έτσι το συνολικό δίκτυο να υπερφορτωθεί από τη μεγάλη κίνηση δεδομένων και να οδηγήσει στην αποτυχία της επικοινωνίας του δικτύου. Αυτή η διαδικασία ονομάζεται **broadcast storm** ή **network storm** και μπορεί να οφείλεται είτε στη κακιά τεχνολογία που αποτελεί το δίκτυο, είτε σε switches που έχουν χαμηλής ταχύτητας θύρες είτε σε ακατάλληλες διαμορφώσεις του δικτύου.

Επιπλέον, μια συσκευή μπορεί να δεχτεί πολλαπλά αντίγραφα ενός ίδιου πλαισίου διότι μπορεί να έχει φτάσει στη συσκευή από διάφορα τμήματα του δικτύου ταυτόχρονα επιβαρύνοντας έτσι το δίκτυο. Αυτό οδηγεί σε ένα άλλου είδους πρόβλημα.

Ο πίνακας των φυσικών διευθύνσεων ενός switch θα μπορούσε να μπερδευτεί σχετικά με τη τοποθεσία της συσκευής που στέλνει ένα πλαίσιο, αφού το switch δέχεται το ίδιο πλαίσιο από διαφορετικές διεπαφές. Ακόμη χειρότερα το μπερδεμένο switch θα είναι συνεχώς απασχολημένο προσπαθώντας να ενημερώνει το πίνακα διευθύνσεων, με τη διεύθυνση πηγής που θα αποτυχαίνει να προωθεί το πλαίσιο. Αυτό ονομάζεται **thrashing MAC table**.

Τέλος, ένα από τα χειρότερα γεγονότα που μπορούν να συμβούν είναι όταν πολλαπλοί βρόχοι αναπαράγονται μέσω του δικτύου. Βρόχοι μπορούν να δημιουργηθούν μέσα σε άλλους βρόχους, και αν είναι να συμβεί ταυτόχρονα και broadcast storm το δίκτυο δεν θα είναι σε θέση να εκτελέσει τη μεταγωγή πλαισίων.

Αυτά τα προβλήματα λοιπόν, αποτελούν καταστροφή για ένα δίκτυο και είναι καταστάσεις που επιβάλλεται να αποφεύγονται ή να διορθώνονται με κάποιο τρόπο. Ένας τέτοιος τρόπος είναι η χρήση του πρωτοκόλλου **Spanning Tree** για το οποίο θα μιλήσουμε και θα αναλύσουμε περαιτέρω στο επόμενο κεφάλαιο.

2.2 Το πρωτόκολλο CSMA/CD

Τα Ethernet δίκτυα χρησιμοποιούν το πρωτόκολλο Carrier Sense Multiple Access with Collision Detection (CSMA/CD), το οποίο επιτρέπει στις συσκευές να μοιράζονται το εύρος ζώνης ισοδύναμα ενώ παράλληλα αποτρέπουν δύο συσκευές από το να μεταδίδουν ταυτόχρονα στο ίδιο μέσο του δικτύου. Στην ουσία το CSMA/CD δημιουργήθηκε για να αντιμετωπιστεί το πρόβλημα των συγκρούσεων όταν οι κόμβοι μεταδίδουν ταυτόχρονα πακέτα την ίδια στιγμή. Η διαχείριση των συγκρούσεων είναι πολύ κρίσιμη για τη σωστή λειτουργία ενός δικτύου. Όταν ένας κόμβος μεταδίδει πακέτα σε δίκτυο που χρησιμοποιεί το πρωτόκολλο CSMA/CD, όλοι οι υπόλοιποι κόμβοι του δικτύου λαμβάνουν και εξετάζουν τη μετάδοση. Μόνο τα switches και οι δρομολογητές μπορούν να αποτρέψουν αποτελεσματικά μια μετάδοση από το να πολλαπλασιαστεί σε όλο το δίκτυο.

Όταν ένας χρήστης θέλει να μεταδώσει πληροφορίες στο δίκτυο, πρώτα ελέγχει στο μέσο διάδοσης για τη παρουσία ψηφιακού σήματος. Αν δεν υπάρχει κάποιο σήμα και κανένας άλλος χρήστης δεν μεταδίδει πληροφορίες, τότε ο αρχικός χρήστης μπορεί να συνεχίσει τη μετάδοση. Ωστόσο, ο χρήστης που μεταδίδει πληροφορίες

παρακολουθεί συνέχεια το καλώδιο για να είναι σίγουρος πως κανένας άλλος χρήστης δεν έχει αρχίσει να μεταδίδει πληροφορίες παράλληλα.

Αν ο χρήστης εντοπίσει κάποιο άλλο σήμα στο καλώδιο στέλνει ένα διαδοχικό σήμα κίνησης ώστε να προκαλέσει όλους τους χρήστες του δικτύου να σταματήσουν τη παράλληλη μετάδοση πληροφοριών. Οι κόμβοι τότε θα ανταποκριθούν σε αυτό το σήμα κίνησης αναμένοντας για ένα μικρό χρονικό διάστημα πριν ξεκινήσουν την μετάδοση πάλι. Η διαδικασία αυτή είναι γνωστή και ως backoff algorithm. Ο αλγόριθμος αυτός καθορίζει πότε οι σταθμοί που αντιμετωπίζουν συγκρούσεις επιτρέπεται να ξεκινήσουν τη μετάδοση. Ο χρήστης θα πρέπει να εντοπίζει τη σύγκρουση πριν τελειώσει τη μετάδοση ενώ πλαισίου διαφορετικά το πρωτόκολλο δεν μπορεί να λειτουργήσει αξιόπιστα. Αυτό επιτυγχάνεται χρησιμοποιώντας ένα σταθερό χρονικό περιθώριο (slot time), τον απαιτούμενο χρόνο δηλαδή που χρειάζεται για να σταλεί από τον χρήστη σε κάποιον προορισμό και πίσω, και μετριέται σε bits. Ο χρήστης επιπλέον θα πρέπει να συνεχίσει τη μετάδοση ενός πλαισίου για τον ελάχιστο χρόνο του χρονικού περιθωρίου. Σε ένα κατάλληλα διαμορφωμένο δίκτυο, μια σύγκρουση θα πρέπει πάντα να συμβαίνει μέσα σε αυτό το χρονικό περιθώριο καθώς έχει περάσει αρκετή ώρα για να φτάσει το πλαίσιο ως την άλλη άκρη του δικτύου και προς τα πίσω, γνωρίζοντας οι υπόλοιπες συσκευές του δικτύου τη συγκεκριμένη μετάδοση. Το χρονικό αυτό περιθώριο περιορίζει σημαντικά το φυσικό μέγεθος του δικτύου αφού αν ένα τμήμα του δικτύου είναι πολύ μεγάλο, κάποιος χρήστης πιθανόν να μην μπορέσει να ανιχνεύσει τη σύγκρουση μέσα στο χρονικό περιθώριο. Η σύγκρουση που συμβαίνει μετά πέρας του χρονικού περιθωρίου αναφέρεται ως καθυστερημένη σύγκρουση (late collision).

Αν οι συγκρούσεις εξακολουθούν να συμβαίνουν μετά από δεκαπέντε προσπάθειες μεταξύ αυτών των κόμβων τότε θα σταματήσουν εντελώς τη μετάδοση.

Όταν συμβεί κάποια σύγκρουση σε ένα δίκτυο Ethernet αρχικά ένα σήμα κίνησης στέλνεται και ενημερώνει όλες τις συσκευές πως έχει συμβεί σύγκρουση. Στη συνέχεια η σύγκρουση εφαρμόζει τυχαία τον αλγόριθμο backoff και κάθε συσκευή στο δίκτυο σταματάει τη μετάδοση για ένα σύντομο χρονικό διάστημα εώς ότου ο αλγόριθμος backoff τελειώσει. Όλοι οι χρήστες έχουν την ίδια προτεραιότητα να μεταδώσουν αφού τελειώσουν τα χρονικά όρια του αλγόριθμου backoff.

Γι’ αυτό το λόγο τα δίκτυα που χρησιμοποιούν το πρωτόκολλο CSMA/CD έχουν καθυστερήσεις, χαμηλό ρυθμό μετάδοσης και μεγάλη κυκλοφοριακή συμφόρηση.

2.3 Half-Duplex KAI Full-Duplex Επικοινωνία

Η τεχνολογία Ethernet αναπτύχθηκε για να μπορεί να υποστηρίζει περιβάλλοντα που χρησιμοποιούν κοινόχρηστα μέσα. Έτσι επιτρέπεται στους χρήστες να χρησιμοποιούν το ίδιο φυσικό μέσο του δικτύου. Υπάρχουν δύο μέθοδοι επικοινωνίας σε ένα κοινόχρηστο φυσικό μέσο. Η ημι-αμφίδρομη επικοινωνία (Half Duplex Communication) που επιτρέπει στους χρήστες να μεταδίδουν ή να λαμβάνουν πληροφορίες, αλλά όχι ταυτόχρονα και η πλήρης αμφίδρομη επικοινωνία (Full-Duplex Communication) επιτρέπει στους χρήστες να στέλνουν και να λαμβάνουν πληροφορίες ταυτόχρονα.

Η επικοινωνία με τη μέθοδο Half-Duplex ορίζεται στις αρχικές προδιαγραφές του Ethernet στο πρότυπο IEEE 802.3. Το πρωτόκολλο CSMA/CD χρησιμοποιεί τη μέθοδο half-duplex για να μπορεί να αποτρέπει τις συγκρούσεις και να επιτρέπει την επαναμετάδοση αν συμβεί κάποια σύγκρουση. Αν είναι συνδεμένο ένα hub με ένα switch, πρέπει να λειτουργήσει με τη ημι-αμφίδρομη μέθοδο διότι οι τερματικοί σταθμοί θα πρέπει να μπορούν να εντοπίζουν την ύπαρξη των συγκρούσεων. Το πρόβλημα είναι ότι μόνο η ημι-αμφίδρομη μέθοδος μπορεί να λειτουργήσει και αν δυο χρήστες προσπαθήσουν να επικοινωνήσουν ταυτόχρονα θα προκύψει σύγκρουση.

Αντιθέτως η μέθοδος της πλήρης αμφίδρομης επικοινωνίας χρησιμοποιεί δύο ζευγάρια καλωδίων την ίδια στιγμή και χρησιμοποιεί συνδέσεις από σημείο σε σημείο μεταξύ της συσκευής που μεταδίδει και της συσκευής που λαμβάνει τα δεδομένα. Η μέθοδος πλήρης αμφίδρομης επικοινωνίας καθορίζεται στο πρότυπο 802.3x και δεν χρησιμοποιεί το πρωτόκολλο CSMA/CD ούτε slot times. Ως εκ τούτου έχουμε ταχύτερη μετάδοση, καλύτερη αποτελεσματικότητα και υποστήριξη μεγαλύτερων αποστάσεων σε σχέση με την ημι-αμφίδρομη μεταφορά. Επίσης, υποστηρίζει ταυτόχρονη επικοινωνία παρέχοντας ξεχωριστές διαδρομές για τις μεταδιδόμενες και τις λαμβανόμενες πληροφορίες, με αποτέλεσμα την εξάλειψη των συγκρούσεων. Πλήρη αμφίδρομη επικοινωνία μπορούμε να έχουμε σε έξι διαφορετικές περιπτώσεις:

1. Σε απευθείας συνδέσεις μεταξύ χρήστη και switch.
2. Σε απευθείας συνδέσεις μεταξύ δύο switches.
3. Σε απευθείας συνδέσεις μεταξύ δύο χρηστών.
4. Σε απευθείας συνδέσεις μεταξύ switch και router.
5. Σε απευθείας συνδέσεις μεταξύ δύο router.
6. Σε απευθείας συνδέσεις μεταξύ router και χρήστη.

2.4 Μέθοδοι Προώθησης Πλαισίου

Τα switches υποστηρίζουν **τρεις διαφορετικές μεθόδους** για να προωθούν τα πλαίσια. Κάθε μία μέθοδος από αυτές αντιγράφει ολόκληρο ή μέρος του πλαισίου στη μνήμη του, παρέχοντας έτσι διαφορετικά επίπεδα καθυστέρησης και αξιοπιστίας. Μικρότερη καθυστέρηση σημαίνει ταχύτερη προώθηση του πλαισίου.

1. Η **μέθοδος Store and Forward** αντιγράφει ολόκληρο το πλαίσιο στη μνήμη του και εκτελεί τον έλεγχο Cycle Redundancy Check (CRC) για να εξασφαλίσει απόλυτα την ακεραιότητα του πλαισίου. Ωστόσο, αυτό επίπεδο ελέγχου, για τυχόν σφάλματα στο πλαίσιο, προκαλεί τη μεγαλύτερη καθυστέρηση από τις υπόλοιπες μεθόδους.
2. Η **μέθοδος Cut Through** (Real Time) αντιγράφει ένα μέρος της κεφαλίδας του πλαισίου για να καθορίσει τη διεύθυνση προορισμού. Αυτό το κομμάτι είναι τα πρώτα 6 bytes μετά την εισαγωγή. Η μέθοδος αυτή επιτρέπει τα πλαίσια να μεταφέρονται με τη ταχύτητα του καλωδίου και έχει το μικρότερο επίπεδο

καθυστέρησης και από τις τρεις μεθόδους. Επιπλέον δεν συμβαίνει έλεγχος για σφάλματα στο πλαίσιο με αυτή τη μέθοδο.

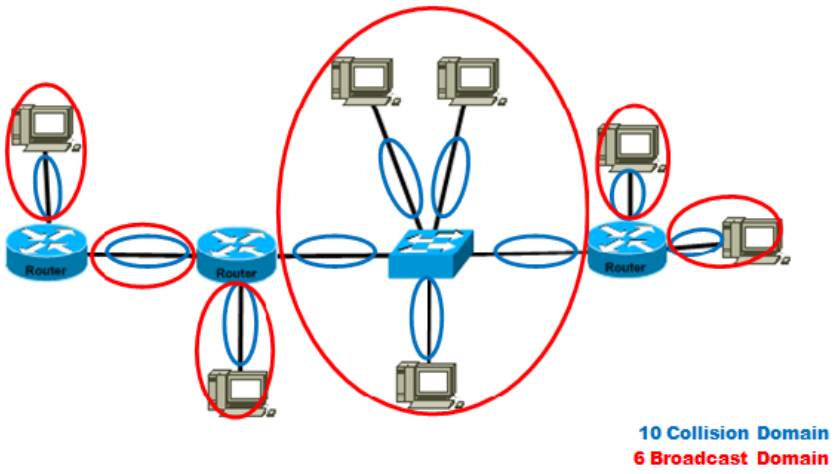
3. Η **μέθοδος Fragment Free** (Modified Cut Through) αντιγράφει μόνο τα 64 πρώτα bytes του πλαισίου για έλεγχο σφαλμάτων. Οι περισσότερες συγκρούσεις και αλλοιώσεις συμβαίνουν σε αυτό το τμήμα του πλαισίου. Η μέθοδος αυτή είναι συνδυασμός των μεθόδων CRC και Cut Through για την καλύτερη αξιοπιστία και ταχύτητα.

2.5 Broadcast και Collision Domains

Τομέας εκπομπής (broadcast domain) είναι το τμήμα στο οποίο προωθείται μία εκπομπή. Ένας τέτοιος τομέας περιέχει όλες τις συσκευές οι οποίες μπορούν να επικοινωνήσουν μεταξύ τους με βάση το data link layer χρησιμοποιώντας τη εκπομπή. Όλες οι θύρες ενός hub ή ενός switch ανήκουν στον ίδιο τομέα μετάδοσης εξ' ορισμού. Οι θύρες ενός δρομολογητή ανήκουν σε διαφορετικό τομέα μετάδοσης και οι δρομολογητές δεν προωθούν τις εκπομπές από το ένα τμήμα εκπομπής στο άλλο. Στην εικόνα που ακολουθεί μπορούμε να δούμε πως ακριβώς σχηματίζονται οι τομείς εκπομπής.

Τομέας σύγκρουσης (collision domain) είναι το τμήμα στο οποίο μπορούν να συμβούν συγκρούσεις πακέτων/πλαισίων. Οι συγκρούσεις συμβαίνουν όταν δύο συσκευές στέλνουν πακέτα την ίδια στιγμή στο κοινόχρηστό τμήμα του δικτύου. Τα πακέτα συγκρούονται μεταξύ τους και οι συσκευές πρέπει εκ νέου να τα ξαναστείλουν, πράγμα που μειώνει την απόδοση της λειτουργίας του δικτύου. Συγκρούσεις έχουμε συχνά σε περιβάλλοντα που υπάρχουν συνδέσεις μέσω hubs, διότι κάθε θύρα του hub βρίσκεται στο ίδιο τομέα σύγκρουσης. Αντιθέτως, κάθε θύρα ενός switch ή ενός router αποτελεί ξεχωριστό τομέα σύγκρουσης.

Στην εικόνα που ακολουθεί μπορούμε να δούμε πως ακριβώς σχηματίζονται οι τομείς σύγκρουσης.



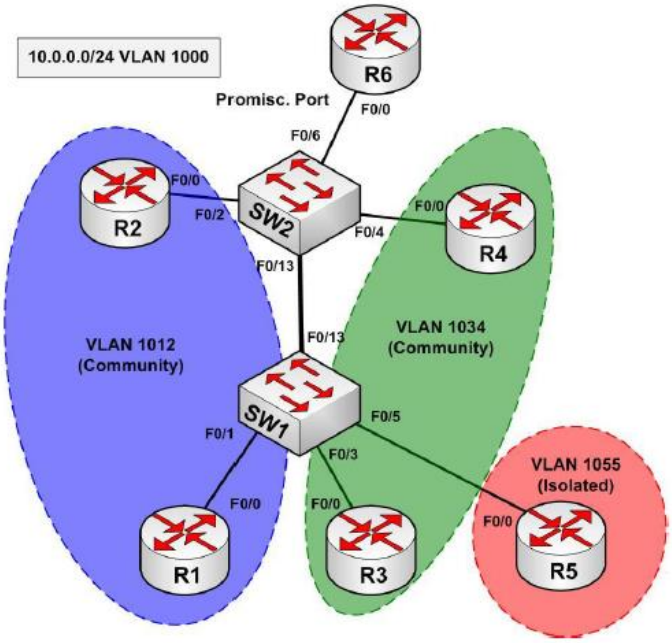
Εικόνα 11: Collision Domains και Broadcast Domains

2.6 Εικονικά Δίκτυα- (Virtual Local Area Network-VLANs)

Ένα τοπικό δίκτυο που αποτελείται μόνο από switches επιπέδου 2 αναφέρεται και ως flat network topology. Ένα τέτοιο δίκτυο αποτελεί ένα ενιαίο τομέα μετάδοσης, έτσι ώστε κάθε συνδεδεμένη συσκευή να παρακολουθεί την οποιαδήποτε αποστολή πακέτου που μεταδίδεται.

Εξ' αιτίας της φύσης του επιπέδου 2, τα flat networks δεν μπορούν να έχουν επιπλέον διαδρομές για να εξισορροπήσουν το φορτίο ή να έχουν ανοχή σε σφάλματα. Για να συμβεί κάτι τέτοιο θα πρέπει να εισάγουμε στο δίκτυο λειτουργίες δρομολόγησης του επιπέδου 3. Η τεχνολογία των switches μας δίνει τη δυνατότητα να ξεπεράσουμε αυτό το πρόβλημα των περιορισμών των flat networks. Τα δίκτυα μεταγωγής μπορούν να υποδιαιρεθούν σε vlans.

Ένα εικονικό τοπικό δίκτυο (Virtual Local Area Network-VLAN) είναι μια ομάδα που αποτελείται από σταθμούς εργασίας, διακομιστές και δικτυακές συσκευές και φαίνονται αν ανήκουν στο ίδιο τοπικό δίκτυο ανεξαρτήτως της γεωγραφική τους κατανομής. Ένα τέτοιο δίκτυο επιτρέπει σε ένα δίκτυο από υπολογιστές και χρήστες να επικοινωνούν σε ένα τεχνητό περιβάλλον σαν να συνυπάρχουν σε ένα τοπικό δίκτυο και μοιράζονται ένα ενιαίο τομέα σύγκρουσης και ένα ενιαίο τομέα μετάδοσης. Τα vlans εφαρμόζονται για να επιτύχουμε την επεκτασιμότητα του τοπικού μας δικτύου, την ασφάλεια του και την εύκολη διαχείριση του δικτύου που μπορούν χωρίς πρόβλημα να προσαρμοστούν στις αλλαγές και στις απαιτήσεις του δικτύου γρήγορα, καθώς και στην μετεγκατάσταση των σταθμών εργασίας και των διακομιστών.



Εικόνα 12:Διαφορετικά VLNAN σε ένα LAN

Τα switches επιπέδου 2 που έχουν διαμορφωθεί με τη χαρτογράφηση των vlans και παρέχουν τη λογική σύνδεση μεταξύ των χρηστών ενός vlan, επιτρέπουν τη λειτουργία και την εφαρμογή των vlans.

2.6.1 VLAN Membership

Όταν ένα VLAN παρέχεται σε switch που συνδέεται απευθείας με κάποιον χρήστη, ο χρήστης θα πρέπει να έχει κάποια μέσα για να μπορέσει να συμμετέχει στο VLAN. Τα switches της σειράς Catalyst της εταιρίας Cisco χρησιμοποιούν δύο μεθόδους συμμετοχής: static vlans και dynamic vlans.

Το static VLAN προσφέρει τη συμμετοχή του χρήστη βάση της θύρας, όταν οι θύρες του switch έχουν ανατεθεί σε συγκεκριμένα vlans. Οι χρήστες γίνονται μέλη ενός vlan, βάση της θύρας του switch στην οποία είναι συνδεδεμένοι. Δεν απαιτείται κάποιο πρωτόκολλο συμμετοχής για τις συσκευές. Αυτόματα θεωρούν πως έχουν συνδεθεί σε κάποιο vlan όταν συνδέονται σε μια θύρα. Κανονικά οι συσκευές δεν γνωρίζουν καν την ύπαρξη των vlans. Η θύρα του switch και το vlan του φαίνεται και χρησιμοποιείται απλά όπως κάθε άλλο κομμάτι του δικτύου, μαζί με άλλους χρήστες που χρησιμοποιούν το ίδιο καλώδιο. Οι θύρες των switches ανατίθενται σε vlans χειροκίνητα από τον διαχειριστή του δικτύου. Οι θύρες ενός switch μπορούν να ανατεθούν και να ομαδοποιηθούν σε πολλά vlans. Ακόμα και αν συνδέονται αρκετές συσκευές στο ίδιο switch, η κίνηση δεν θα περάσει από τις συσκευές αυτές αν είναι συνδεδεμένες σε θύρες που ανήκουν σε διαφορετικά vlans. Για να συμβεί αυτό, είτε μια συσκευή επιπέδου 3 θα μπορούσε να χρησιμοποιηθεί για τη δρομολόγηση πακέτων ή μια εξωτερική συσκευή επιπέδου 2 θα μπορούσε να χρησιμοποιηθεί μεταξύ δύο vlans για τη σύνδεση τους. Η στατική θύρα συμμετοχής χρήστη σε vlan γίνεται βάση του υλικού, με εφαρμογή ειδικών ολοκληρωμένων κυκλωμάτων (Application Specific Integrated Circuits-ASICs) στο switch. Η χρήση αυτού του είδους συμμετοχής προσφέρει καλή απόδοση του vlan διότι η χαρτογράφηση όλων των θυρών γίνεται σε επίπεδο υλικού χωρίς να απαιτούνται περίπλοκες αναζητήσεις σε κάποιο πίνακα.

Τα dynamic vlans χρησιμοποιούνται για παροχή των χρηστών με βάση τη φυσική διεύθυνση της συσκευής του. Όταν μια συσκευή συνδέεται με μια θύρα του switch, το switch πρέπει να κάνει αναζήτηση σε μια βάση δεδομένων για να εξακριβώσει τη συμμετοχή του χρήστη στο vlan. Στα δυναμικά VLANs, αντίθετα με τα static vlans, δεν απαιτούν από το διαχειριστή να διαμορφώσει τις θύρες των switches, αλλά να διαμορφώσει ένα κεντρικό εξυπηρετητή που λέγεται Vlan Member Policy Server (VMPS). Το VMPS χρησιμοποιείται για να χειριστεί τις παραμέτρους των θυρών των switches που συμμετέχουν σε vlan. Το VMPS περιέχει μια βάση δεδομένων από όλες τις φυσικές διευθύνσεις των υπολογιστών καθώς και σε ποιο vlan ανήκουν αυτές οι φυσικές διευθύνσεις. Τις πληροφορίες αυτές πρέπει να τις εκχωρεί ο διαχειριστής κάθε φορά που συνδέεται μια καινούργια συσκευή. Για το λόγο αυτό μπορούμε να υποθέσουμε πως έχουμε χαρτογράφηση του vlan μέσω των φυσικών διευθύνσεων των υπολογιστών (Vlan-to-Mac Address). Τα dynamic vlans αναπτύχθηκαν με στόχο να παρέχουν ευελιξία και περιπλοκότητα κάτι που τα static vlans δεν παρείχαν. Λόγω

της περιπλοκότητας τους, των απαιτήσεων και την συνεχή επίβλεψη από το διαχειριστή του δικτύου, τα συναντάμε πολύ σπάνια και προτείνονται από τους διαχειριστές και τους τεχνικού δικτύων η χρήση των static vlans.

2.6.2 VLAN Trunks

Όπως έχουμε ήδη αναφέρει οι συνδεδεμένες συσκευές των τελικών χρηστών ενός δικτύου δεν έχουν επίγνωση της ύπαρξης των vlans και της δομής τους, και φαίνονται πως είναι συνδεδεμένες σε ένα κανονικό τμήμα του δικτύου. Επίσης για να έχουμε επικοινωνία μεταξύ διαφορετικών vlans απαιτείται η χρήση ενός δρομολογητή ή μιας εξωτερικής γέφυρας.

Μία σύνδεση trunk ή μια θύρα του switch που είναι διαμορφωμένη ως trunk port, μπορεί να μεταφέρει πακέτα όχι από ένα, αλλά από όλα τα vlans που υπάρχουν στο δίκτυο χρησιμοποιώντας μία μόνο σύνδεση. Τέτοιες συνδέσεις είναι πιο ωφέλιμες μεταξύ switches ή σε συνδέσεις μεταξύ switches και routers.

Καθώς ο αριθμός των vlans αυξάνεται σε ένα δίκτυο, αυξάνεται και ο αριθμός των συνδέσεων μεταξύ τους. Είναι εφικτό να συνδεθούν δύο switches μεταξύ τους με ξεχωριστές συνδέσεις για το κάθε vlan. Αλλά είναι πιο αποτελεσματική η χρήση των συνδέσεων trunking αφού μπορεί να αντικαταστήσει πολλές ατομικές συνδέσεις των vlans.

2.6.3 VLAN Frame Tagging

Με τη χρήση των συνδέσεων trunk έχουμε μεταφορά δεδομένων από διάφορα VLANs τα οποία ένα switch θα πρέπει να λάβει και αναμεταδώσει γνωρίζοντας το προορισμό τους. Για να επιτευχθεί αυτό η διαδικασία frame identification ή tagging, εκχωρεί ένα μοναδικό αναγνωριστικό σε κάθε πλαίσιο που μεταφέρεται μέσω της σύνδεσης trunk. Αυτό το αναγνωριστικό μπορεί να είναι είτε κάποιος αριθμός ή κάποιο χρώμα, αν έχει σχεδιαστεί σε διάγραμμα του δικτύου με κάποιο συγκεκριμένο χρώμα.

Το vlan frame identification αναπτύχθηκε για τα δίκτυα μεταγωγής. Καθώς πλαίσια μεταφέρονται μέσω της trunk σύνδεσης, το αναγνωριστικό τοποθετείται στη κεφαλίδα του πλαισίου. Καθώς τα switches δέχονται και αναμεταδίδουν τα πλαίσια αυτά, το αναγνωριστικό τους εξετάζεται για να καθοριστεί σε ποιο vlan ανήκουν.

Αν τα πλαίσια πρέπει να μεταφέρονται μεταξύ συνδέσεων trunk το αναγνωριστικό vlan παραμένει στην επικεφαλίδα του πλαισίου. Διαφορετικά αν έχουν ως προορισμό κάποιον τελικό χρήστη τα switches αφαιρούν το αναγνωριστικό αυτό πριν μεταδοθεί το πλαίσιο στο χρήστη. Ως εκ τούτου, τα ίχνη των συνεταιρίζεσθαι vlans παραμένουν κρυφά στον τελικό χρήστη.

Η ταυτοποίηση του vlan αναγνωριστικού μπορεί να διεξαχθεί με διαφορετικές μεθόδους, που κάθε μια από αυτές χρησιμοποιεί διαφορετικό μηχανισμό αναγνωριστικού πλαισίου και μερικά είναι κατάλληλα για συγκεκριμένες δικτυακές συσκευές.

2.6.4 Inter-Switch Link Protocol

Το Inter-Switch Link Protocol (ISL) πρωτόκολλο έχει δημιουργηθεί από την εταιρία Cisco με σκοπό τη διατήρηση του vlan αναγνωριστικού του πλαισίου της πηγής μέσω των συνδέσεων trunk. Το ISL εφαρμόζει την ταυτοποίηση πλαισίου στο επίπεδο 2 εμπεριέχοντας κάθε πλαίσιο μεταξύ της επικεφαλίδας και της ουράς. Οποιοδήποτε Cisco switch ή router που είναι διαμορφωμένο για το ISL μπορεί να διαχειριστεί και να καταλάβει τις πληροφορίες του ISL vlan.

Όταν ένα πλαίσιο προορίζεται από μία trunk σύνδεση για κάποιο router ή switch, το ISL προσθέτει μια επικεφαλίδα μεγέθους 26-byte και μια ουρά μεγέθους 4byte στο πλαίσιο. Η πηγή vlan αναγνωρίζεται από το αναγνωριστικό vlan (VLAN ID) που έχει μέγεθος 10-bit και βρίσκεται στην επικεφαλίδα. Η ουρά περιέχει έναν έλεγχο CRC για να εγγυηθεί την ακεραιότητα του νέου περιλαμβανομένου πλαισίου. Επειδή το ISL προσθέτει στην αρχή και στο τέλος του πλαισίου πληροφορίες, μερικές φορές αναφέρεται και ως double tagging.

2.6.5 VLAN Trunking Protocol

Η διαμόρφωση ενός μικρού vlan δικτύου και των συνδέσεων vlan trunk είναι εύκολο να διαχειριστεί. Αντιθέτως όμως, η διαχείριση των vlan και των vlan trunking ports σε τεράστια δίκτυα με interconnected switches είναι αρκετά δύσκολο.

Η Cisco ανέπτυξε το πρωτόκολλο Vlan Trunking Protocol (VTP), το οποίο είναι αρκετά χρήσιμο στη δημιουργία, διαχείριση και τη συντήρηση ενός μεγάλου τοπικού δικτύου που περιέχει πολλά interconnected switches. Με το VTP επίσης μπορούμε να διαχειριστούμε την πρόσθεση, την αφαίρεση και την μετονομασία ενός vlan από ένα κεντρικό σημείο χωρίς καμία χειροκίνητη παρέμβαση. Έτσι, το VTP μειώνει τη διαχείριση του δικτύου σε ένα δίκτυο μεταγωγής.

2.7 Layer 3 Switching

Μέχρι στιγμής έχουμε αναφερθεί στα switches που λειτουργούν στο δεύτερο επίπεδο του μοντέλου αναφοράς OSI, το επίπεδο σύνδεσης δεδομένων. Ωστόσο, υπάρχουν switches που λειτουργούν με βάση το τρίτο επίπεδο, το επίπεδο δικτύου.

Στο επίπεδο αυτό, ως γνωστόν, λειτουργούν οι συσκευές δρομολογητές. Υπάρχουν όμως και τα επιπέδου 3 switches που έχουν όλες τις δυνατότητες των switches επιπέδου 2 και επιπλέον μπορούν να εκτελέσουν λειτουργίες ενός δρομολογητή και να μεταφέρουν δεδομένα μεταξύ των LANs και WANs με την ταχύτητα του καλωδίου. Κάποιες από τις τεχνολογίες που εφαρμόζουν αυτού του τύπου τα switches συμπεριλαμβάνουν πρωτόκολλα δρομολόγησης πύλης δικτύου όπως το RIP (Routing Information Protocol) και το OSPF (Open Shortest Path First). Τα επιπέδου 3 switches δρομολογούν τα δεδομένα μεταξύ των διαφορετικών τμημάτων του δικτύου περιορίζοντας τον αριθμό των πρωτοκόλλων δρομολόγησης, και χρησιμοποιούν περισσότερο την τεχνολογία των ASIC κυκλωμάτων παρά των RISC κυκλωμάτων ή το λογισμικό.

2.7.1 Λειτουργία των Layer 3 Switches

Τα επιπέδου 3 switches είναι κατασκευασμένα για τη μεταγωγή πλαισίων και πακέτων και αυτό τα κάνει να διαφέρουν από τα επιπέδου 2 switches. Τα επιπέδου 2 switches παρ' όλο που μπορούν να χωρίσουν σε τμήματα τους τομείς μετάδοσης, αλλά δεν μπορούν να δρομολογήσουν τα δεδομένα σε διαφορετικά δίκτυα. Όταν χρειάζεται να δρομολογηθεί ένα πακέτο δεδομένων τότε αξιοποιούνται τα πρωτοκόλλα δρομολόγησης του επιπέδου 3.

Μία από τις μεθόδους δρομολόγησης που χρησιμοποιούν τα επιπέδου 3 switches όταν λαμβάνουν κάποιο πακέτο δεδομένων είναι πως στέλνουν το πρώτο πακέτο που λαμβάνουν σε κάποιο δρομολογητή ή σε route server ώστε να αποφασιστεί αν τα επόμενα πακέτα δεδομένων στη σειρά θα είναι καλύτερο να δρομολογηθούν ή να γίνει μεταγωγή αυτών. Αν αποφασιστεί να δρομολογηθούν τότε η μετάδοση των πακέτων γίνεται μέσω του δρομολογητή. Αν αποφασιστεί πως η μεταγωγή είναι ταχύτερη μέθοδος τότε τα πακέτα θα προωθηθούν μέσω του switch επιπέδου 3.

Αυτό επιτυγχάνεται διαμέσου των ακολούθων βημάτων:

1. Τα πακέτα δεδομένων στέλνονται προς το switch, μέσω διάφορων μέσων, χρησιμοποιώντας τα πρωτοκόλλα του επιπέδου 1.
2. Το switch ελέγχει τη φυσική διεύθυνση επιπέδου 2 της συσκευής προορισμού για να δει αν η συσκευή είναι μέλος του τοπικού δικτύου.
3. Αν η συσκευή ανήκει στο τοπικό δίκτυο, τότε το switch προωθεί τα δεδομένα χρησιμοποιώντας τα πρωτοκόλλα του επιπέδου 2 και τις τεχνικές μεταγωγής πακέτων.
4. Αν η συσκευή προορισμού δεν ανήκει στο τοπικό δίκτυο, πρέπει να προωθηθεί βάση των πρωτοκόλλων του επιπέδου 3, όπως το IP ή το IPX.
5. Στη συνέχεια το switch επιπέδου 3 στέλνει το πρώτο πακέτο δεδομένων από την ακολουθία των πακέτων σε ένα δρομολογητή το οποίο θα εκτελέσει τις λειτουργίες δρομολόγησης RIP ή OSPF.
6. Η διεύθυνση IP επιπέδου 3 και η φυσική διεύθυνση επιπέδου 2 της συσκευής προορισμού αποφασίζονται και γίνεται γνωστή η καλύτερη διαδρομή.
7. Αφού τα πρωτόκολλα του επιπέδου 3 έχουν εφαρμοστεί, το πακέτο IP εμπεριέχεται στο πλαίσιο.
8. Ο τελικός σταθμός αποφασίζει αν είναι ταχύτερος τρόπος να συνεχιστεί η μετάδοση των πακέτων μέσω της δρομολόγησης χρησιμοποιώντας τα πρωτόκολλα επιπέδου 3 ή να γίνει η μεταγωγή των δεδομένων μέσω των πρωτοκόλλων του επιπέδου 2.
9. Αν αποφασιστεί πως η δρομολόγηση είναι ταχύτερη, τότε τα εναπομείναντα πλαίσια δρομολογούνται.
10. Αν αποφασιστεί πως η μεταγωγή είναι ταχύτερη, τότε τα πλαίσια αποστέλλονται πίσω στο switch, το οποίο πλέον γνωρίζει από το

δρομολογητή πώς να στείλει τα δεδομένα στο προορισμό του ξεχωριστού δικτύου και ποια διαδρομή είναι καλύτερη.

11. Τα εναπομείναντα πλαίσια μπορούν να σταλούν μέσω της μεταγωγής με τη ταχύτητα του καλωδίου χρησιμοποιώντας τα πρωτόκολλα επιπέδου 2.

Τα επιπέδου 3 switches έχουν δύο μεθόδους μεταγωγής δεδομένων. Η πρώτη μέθοδος είναι η Packet-by-Packet Layer 3 (PPL3). Τα switches ψάχνουν κάθε πακέτο για να προσδιορίσουν τη λογική διεύθυνση προορισμού επιπέδου 3 (όπως είναι η διεύθυνση IP προορισμού). Τα PPL3 switches λειτουργούν ουσιαστικά ως υψηλής ταχύτητας δρομολογητές που έχουν κατασκευασμένη τη λειτουργία δρομολόγησης στο υλικό τους και όχι στο λογισμικό τους. Όπως και οι δρομολογητές, εκτός από τη προώθηση πακέτων προς το προορισμό, έτσι και τα PPL3 switches εκτελούν και άλλες λειτουργίες που ένα δρομολογητής εκτελεί όπως να χρησιμοποιεί τον έλεγχο των πακέτων για βεβαιώσει την ακεραιότητα του πακέτου, να ενημερώνει τις πληροφορίες του χρόνου ζωής του πακέτου (Time to Live – TTL) μετά από κάθε άλμα, και να επεξεργάζεται την επιπλέον πληροφορία στην επικεφαλίδα του πακέτου. Τα PPL3 switches επικοινωνούν μεταξύ τους χρησιμοποιώντας τα πρωτοκόλλα RIP και OSFP με σκοπό να μάθουν την ολική τοπολογία του δικτύου.

Η άλλη μέθοδος που χρησιμοποιείται για την δρομολόγηση πακέτων είναι η Cut-Through ή Flow Control. Τα switches που χρησιμοποιούν αυτή τη μέθοδο ελέγχουν μόνο το πρώτο πακέτο, από μια σειρά πακέτων που δέχονται, ώστε να καθορίσουν τη λογική διεύθυνση προορισμού επιπέδου 3, και στη συνέχεια προωθούν τα υπόλοιπα πακέτα χρησιμοποιώντας τη φυσική διεύθυνση του επιπέδου 2. Έτσι μπορούμε να πετύχουμε υψηλότερα ποσοστά διεκπεραίωσης δεδομένων.

Τέλος, τα switches επιπέδου 3 αποτελούν συνήθως τη ραχοκοκαλιά των τοπικών δικτύων. Οι δρομολογητές συνδέουν κυρίως τα τοπικά δίκτυα με μεγαλύτερα δίκτυα ευρείας περιοχής ή για τη σύνδεση μεταξύ των vlans.

2.8. Spanning Tree Protocol

2.8.1 Εισαγωγή

Το Spanning Tree Protocol (STP) είναι ένα πρωτόκολλο διαχείρισης σύνδεσης, που ανήκει στο δεύτερο επίπεδο του μοντέλου αναφοράς OSI, το επίπεδο σύνδεσης δεδομένων και λειτουργεί στις συσκευές διασύνδεσης, τους μεταγωγείς (switches). Το πρωτόκολλο βασίζεται σε αλγόριθμο, τον οποίο ανέπτυξε η Radia Perlman ενώ εργαζόταν για την εταιρία Digital Equipment Corporation (DEC) το 1990. Τότε η τεχνολογία των switches δεν υπήρχε αλλά χρησιμοποιούσαν τη τεχνολογία των γεφυρών (Bridges) που ουσιαστικά εξυπηρετούν τον ίδιο σκοπό με τα switches, αφού τα switches αποτελούν ένα σύνολο από bridges. Για το λόγο αυτό οι ορολογίες που

μπορεί να χρησιμοποιούνται και να αναφερθούν στη συνέχεια μπορεί να περιέχουν κάποιες από τις ορολογίες των γεφυρών.

Η βασική λειτουργία του πρωτοκόλλου είναι να εξασφαλίζει την εξάλειψη των βρόχων σε ένα τοπικό δίκτυο μεταγωγής όταν τα switches συνδέονται μεταξύ τους μέσω πολλαπλών διαδρομών, και δημιουργούν παραπάνω από μια διαδρομές για έναν προορισμό, με στόχο να επιτρέπει μόνο μία ενεργή διαδρομή, την καλύτερη, μεταξύ δύο σταθμών. Τις επιπλέον διαδρομές τις μπλοκάρει προσωρινά και τις κρατάει ως εφεδρικές σε περίπτωση που η ενεργή διαδρομή σταματήσει να λειτουργεί ή υπάρξει κάποιο πρόβλημα σε αυτήν. Τότε την αντικαταστεί με κάποια από τις εφεδρικές.

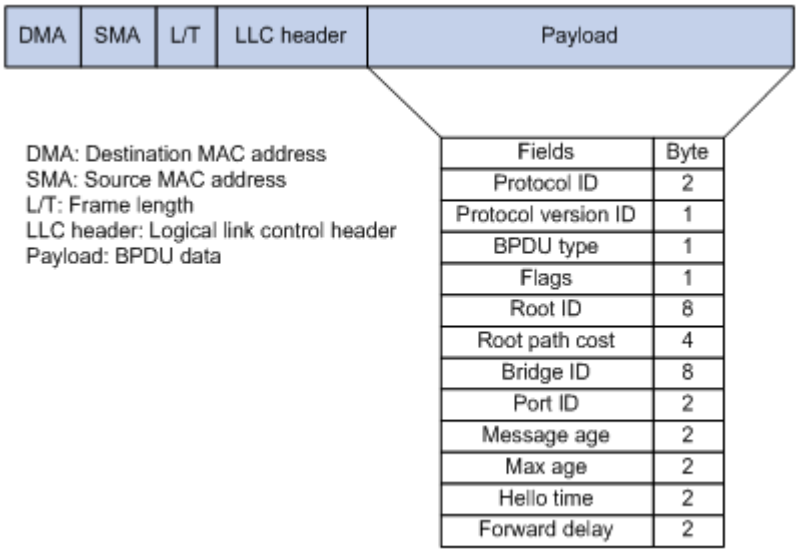
2.8.2 Λειτουργία του πρωτοκόλλου STP

2.8.2.1 BPDU

Η σωστή λειτουργία του STP βασίζεται στην επικοινωνία μεταξύ των switches, με στόχο να γίνουν γνωστοί οι φυσικοί βρόχοι του δικτύου και να αφαιρεθούν θέτοντας συγκεκριμένες περιττές θύρες σε κατάσταση μπλοκαρίσματός ή αναμονής. Η επικοινωνία αυτή γίνεται μέσω της ανταλλαγής κάποιων μηνυμάτων που περιέχουν δεδομένα. Τα μηνύματα ανταλλάσσονται με τη μορφή πλαισίων των Bridge Protocol Data Units (BPDUs). Τα μηνύματα αυτά περνούν μεταξύ των switches με σκοπό να βοηθήσουν το STP να υπολογίσει και να μάθει τη τοπολογία του δικτύου. Τα switches στέλνουν ένα πλαίσιο BPDU χρησιμοποιώντας τη μοναδική φυσική διεύθυνση (MAC address) της ίδιας της θύρας ως τη διεύθυνση της πηγής. Το switch που στέλνει το πλαίσιο από τη θύρα δεν γνωρίζει για τα υπόλοιπα switches γύρω από αυτό. Τα μηνύματα BPDU προωθούνται από όλα τα switches, μεταξύ αυτών, προς όλες τις θύρες των switches με αποτέλεσμα οι πληροφορίες να εξαπλώνονται σε όλα τα switches του δικτύου. Επομένως, ένα μήνυμα BPDU έχει μια διεύθυνση προορισμού, τη γνωστή διεύθυνση πολλαπλής διανομής του STP **01-80c2-00-00-00** ώστε να φτάσει σε όλα τα switches που βρίσκονται σε κατάσταση ακρόασης. Τα μηνύματα αυτά αποστέλλονται τυπικά ανά 1 ως 4 δευτερόλεπτα. Από προεπιλογή, τα μηνύματα BPDU αποστέλλονται κάθε 2 δευτερόλεπτα σε κάθε θύρα για να εξασφαλίσουν ένα σταθερό δίκτυο χωρίς τυχαίους βρόχους δεδομένων. Αυτά τα μηνύματα ελέγχου περιέχουν πληροφορίες σχετικά με το switch που έστειλε το μήνυμα και θα χρησιμοποιηθούν από τον παραλήπτη switch για να πάρει αποφάσεις του πρωτόκολλου αν αυτό είναι απαραίτητο.

Υπάρχουν τρεις τύποι μηνυμάτων BPDUs : το configuration BPDU (CBPDU) που χρησιμοποιείται για τον υπολογισμό σχεδίασης της τοπολογίας δέντρου του STP, και το Topology Change Notification (TCN) BPDU που χρησιμοποιείται για να αναφέρει αλλαγές που έχουν συμβεί στη τοπολογία του δικτύου και το Topology Notification Acknowledgement (TCA).

Παρακάτω βλέπουμε τα πεδία ενός configuration BPDU μηνύματος καθώς και το μέγεθος του κάθε πεδίου.



Fields	Byte
Protocol ID	2
Protocol version ID	1
BPDU type	1
Flags	1
Root ID	8
Root path cost	4
Bridge ID	8
Port ID	2
Message age	2
Max age	2
Hello time	2
Forward delay	2

Εικόνα 13: Πεδία του μηνύματος Configuration BPDU

- **Protocol Identifier** (2 bytes): Περιέχει τη τιμή 0000 για το πρότυπο IEEE 802.1d.
- **Version Identifier** (1 byte): Περιέχει τη τιμή 0.
- **Message Type** (1 byte): Περιέχει το τύπου του μηνύματος του BPDU, Configuration ή TCN BPDU.
- **Flags** (1 byte): Περιέχει 8 bit. Από τα 8 αυτά bit μόνο τα δύο χρησιμοποιούνται. Το 1ο bit που περιέχει τη πληροφορία για το αν υπάρχει αλλαγή στη τοπολογία (Topology Change bit: TC) και το 8ο bit που περιέχει τη πληροφορία βεβαίωσης (Topology Change Acknowledgement: TCA) για το αν έχει υπάρξει αλλαγή στο τοπολογία.

  1:Topology Change Flag

  2:unused 0

  3:unused 0

  4:unused 0

  5:unused 0

  6:unused 0

  7:unused 0

  8:Topology Change Ack

- **Root ID** (8 bytes): Περιέχει το μοναδικό αναγνωριστικό του switch, που ο αποστολέας πιστεύει πως είναι το switch ρίζα (root switch) καταγράφοντας τον αριθμό προτεραιότητας (2 bytes) ακολουθούμενο από τη φυσική διεύθυνση (MAC Address) (6 bytes).

- **Root Path Cost** (4 bytes): Περιέχει τη πληροφορία του κόστους της διαδρομής από τη θύρα μετάδοσης προς το root switch.
- **Bridge ID ή Switch ID** (8 bytes): Περιέχει το μοναδικό αναγνωριστικό του switch που μεταδίδει το μήνυμα.
- **Port ID** (2 bytes): Περιέχει το αναγνωριστικό της θύρας του switch μέσω του οποίου μεταδόθηκε το μήνυμα.
- **Message Age** (2 bytes): Περιέχει το συνολικό χρόνο που έκανε το μήνυμα BPDU να μεταδοθεί από το root switch προς το επόμενο switch. Το root switch στέλνει το BPDU μήνυμα με μια τιμή 0 και κάθε επόμενο switch που δέχεται το μήνυμα προσθέτει 1 σε αυτή τη τιμή.
- **Maximum Age ή Max Age** (2 bytes): Περιέχει τη τιμή του χρονικού ορίου που θέτει το root switch και χρησιμοποιείται για να περιοριστεί το χρονικό διάστημα για το οποίο θεωρείται έγκυρο το τελευταίο μήνυμα και μετά διαγράφεται. Η προεπιλεγμένη τιμή είναι 20 δευτερόλεπτα.
- **Hello Time** (2 bytes): Περιέχει τη χρονική στιγμή για το πόσο συχνά στέλνονται τα μηνύματα από το root switch. Η προεπιλεγμένη τιμή είναι 2 δευτερόλεπτα.
- **Forward Delay** (2 bytes): Περιέχει το χρονικό όριο για το οποίο τα switches θα πρέπει να περιμένουν πριν μεταβούν σε μια νέα κατάσταση αφού έχει προηγηθεί κάποια αλλαγή στη τοπολογία του δικτύου. Η προεπιλεγμένη τιμή είναι 15 δευτερόλεπτα.

2.8.2.2 Εκλογή του Switch Root

Σε ένα δίκτυο για να συμφωνούν όλα τα switches σε μια τοπολογία χωρίς βρόχους, πρέπει να υπάρχει ένα κοινό σημείο αναφοράς που θα το χρησιμοποιούν για καθοδήγηση. Το σημείο αναφοράς αυτό ονομάζεται **Root Switch** ή Root Bridge.

Το root switch επιλέγεται μέσω μιας διαδικασίας εκλογής μεταξύ όλων των συνδεδεμένων switches στο δίκτυο. Κάθε switch έχει μια μοναδική ταυτότητα, το αναγνωριστικό του switch, το Switch ID, που χρησιμοποιούν για να ξεχωρίζει το καθένα τον εαυτό του από τα υπόλοιπα. Το αναγνωριστικό αποτελείται από τιμή των 8 byte και περιέχει δύο πεδία. Την προτεραιότητα γέφυρας ή την προτεραιότητα μεταγωγέα (Bridge Priority ή Switch Priority) (2 bytes). Είναι η προτεραιότητα ή το βάρος ενός switch σε σχέση με τα άλλα switches. Το πεδίο προτεραιότητας έχει ένα εύρος τιμής από το 0 – 65,535. Η προεπιλεγμένη τιμή για όλες τις συσκευές που εκτελούν το πρότυπο IEEE STP version είναι 32,768. Η τιμή αυτή μπορεί να αλλαχτεί από τον χρήστη. Και τη φυσική διεύθυνση (MAC Address) (6 bytes). Η διεύθυνση αυτή, είναι μία μοναδική ταυτότητα που αποδίδεται στα switches για την επικοινωνία. Αυτή η διεύθυνση μπορεί να προκύψει είτε από τον ίδιο τον κατασκευαστή της συσκευής είτε από ένα πλήθος 1024 διευθύνσεων που έχουν ανατεθεί σε κάθε κατασκευαστή, εξαρτώντας το μοντέλο του switch. Σε κάθε περίπτωση, η διεύθυνση αυτή είναι μόνιμη, μοναδική και δεν μπορεί να αλλαχτεί από τον χρήστη.

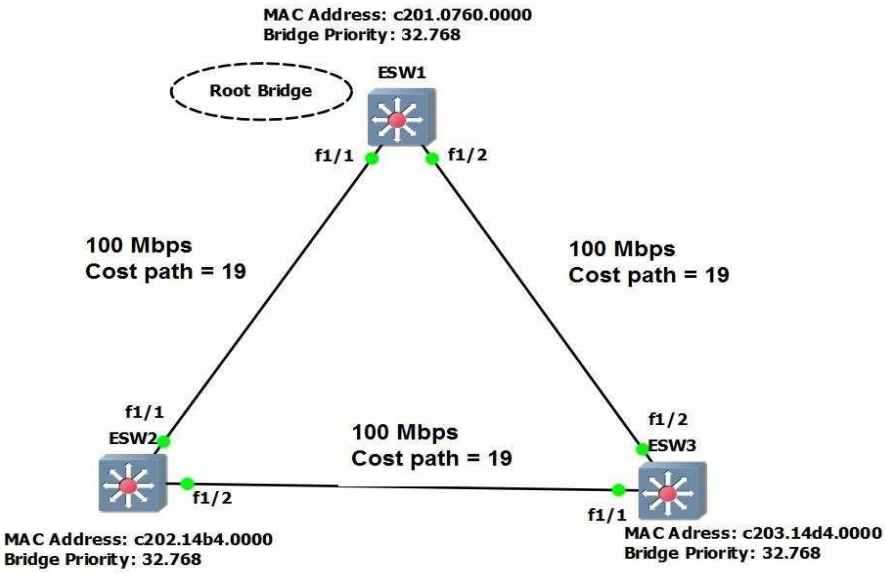
Όταν ένα switch έρθει σε λειτουργία για πρώτη φορά δεν έχει πλήρη εικόνα για το ποιες άλλες συσκευές υπάρχουν γύρω του και έτσι θεωρεί τον εαυτό του ως root switch. Αυτό όπως είναι λογικό αλλάζει καθώς και άλλα switches μπαίνουν σε λειτουργία και μπαίνουν στην διαδικασία της εκλογής στέλνοντας τα δικά τους μηνύματα BPDU. Παρόλα αυτά, μόνο τα μηνύματα που έχουν πληροφορίες για το πραγματικό root switch εξακολουθούν να προωθούνται μέσω των switches. Τα υπόλοιπα μηνύματα θεωρούνται τελικά κατώτερα σε σχέση με αυτά που έχουν τις πληροφορίες του πραγματικού root switch με αποτέλεσμα να μην προωθούνται πλέον και ως εκ τούτου να χάνονται από το δίκτυο.

Η λειτουργία της εκλογής του Root Bridge ή του Root Switch έχει ως εξής: Κάθε switch ξεκινάει τη λειτουργία του στέλνοντας μηνύματα BPDUs που περιέχουν το αναγνωριστικό γέφυρας ρίζας (Root Bridge ID) ίδιο με το δικό του αναγνωριστικό γέφυρας (Bridge ID) και το αναγνωριστικό αποστολέα γέφυρας (Sender Bridge ID) που είναι ίδιο με το αναγνωριστικό γέφυρας (Bridge ID) του. Το αναγνωριστικό αποστολέα γέφυρας ενημερώνει τα υπόλοιπα switches για το ποιος είναι ο αποστολέας του BPDU μηνύματος.

Τα λαμβανόμενα μηνύματα BPDU αναλύονται για να ανακοινωθεί το καλύτερο root switch. Καλύτερο switch root είναι το switch που έχει τη χαμηλότερη τιμή του root bridge ID. Όπως αναφέραμε το root bridge ID περιέχει δύο πεδία. Αν δύο switches έχουν ίδια προτεραιότητα γέφυρας τότε καλύτερο είναι το switch με τη μικρότερη φυσική διεύθυνση. Επομένως, όταν ένα switch λάβει ένα μήνυμα BPDU στο οποίο αναφέρεται καλύτερο root bridge ID, τότε το switch αντικαθιστά το δικό του root bridge ID με αυτό του μηνύματος BPDU που έλαβε. Επίσης απαιτείται να ορίσει το νέο root bridge ID στο μήνυμα BPDU που θα προωθήσει διατηρώντας το δικό του αναγνωριστικό αποστολέα γέφυρας.

Όταν όλα τα switches στείλουν μεταξύ τους μηνύματα BPDU η εκλογή θα συγκλίνει και όλα τα switches θα συμφωνούν στην ιδέα πως κάποιο από αυτά είναι η γέφυρα ρίζα. Είναι προφανές πως αν ένα switch μπει σε λειτουργία με χαμηλότερη τιμή προτεραιότητας ή ίσης τιμής προτεραιότητας και χαμηλότερης τιμής της φυσικής διεύθυνσης θα στέλνει μηνύματα BPDU υποστηρίζοντας πως αυτό είναι η νέα γέφυρα ρίζα. Λόγω του ότι όντως καινούργια switches έχουν μικρότερη τιμή αναγνωριστικού γέφυρας, όλα τα switches θα το θεωρούν και θα το καταγράψουν ως τη νέα γέφυρα ρίζα. Η εκλογή γέφυρας ρίζας είναι μια συνεχόμενη διαδικασία η οποία προκαλείται σε αλλαγές της τιμής του αναγνωριστικού γέφυρας ρίζας στα μηνύματα BPDU κάθε δύο δευτερόλεπτα.

Ένα παράδειγμα εκλογής του root switch μπορούμε να δούμε στην εικόνα που ακολουθεί:



Εικόνα 14: Παράδειγμα εκλογής του root switch.

Σε αυτό το δίκτυο έχουμε τρία switches τα οποία έχουν την ίδια τιμή προτεραιότητας γέφυρας 32,768. Διασυνδέονται μεταξύ τους με συνδέσεις FastEthernet και έχουν τη προεπιλεγμένη τιμή κόστους διαδρομής 19. Τα τρία switches προσπαθούν να εκλέξουν τον εαυτό τους ως γέφυρα ρίζα αλλά έχουν ίδια τιμή προτεραιότητα γέφυρας. Συνεπώς η εκλογή γίνεται με κριτήριο τη χαμηλότερη φυσική διεύθυνση μεταξύ αυτών, και προφανώς τη μικρότερη φυσική διεύθυνση κατέχει το switch ESW1.

2.8.2.3 Επιλογή των Root Ports

Αφού ολοκληρωθεί η εκλογή του switch root ως σημείο αναφοράς για όλο το δίκτυο, πρέπει κάθε ένα από τα υπόλοιπα switch να κατανοήσει ποια είναι η σχέση του με το σημείο αναφοράς δηλαδή το root switch. Για να επιτευχθεί κάτι τέτοιο επιλέγεται μία από τις θύρες κάθε switch ως **θύρα ρίζας (Root Port**). Η root port έχει κατεύθυνση πάντα προς το τρέχον switch root, και η θύρα που θα επιλεχτεί είναι αυτή που θα έχει το μικρότερο cost path προς το root switch. Το STP χρησιμοποιεί τον όρο «κόστος» για να καθορίσει αρκετά πράγματα. Η επιλογή μιας root port συνεπάγεται την αξιολόγηση του κόστους διαδρομής της ρίζας (Root Path Cost). Το root path cost του κάθε switch προσδιορίζεται με τον εξής τρόπο:

Πρώτον το root switch στέλνει ένα μήνυμα BPDU με ένα root path cost ίσο με το 0 διότι οι θύρες που στέλνουν το μήνυμα είναι οι θύρες του root switch. Στη συνέχεια όταν το επόμενο κοντινό switch παραλάβει αυτό το μήνυμα προσθέτει το path cost της ίδιας της θύρας που έφτασε το μήνυμα. Έπειτα προωθεί το μήνυμα BPDU με το νέο αθροιστικό κόστος ως το root path cost. Τέλος το root path cost αυξάνεται από την είσοδο του cost path της θύρας καθώς λαμβάνονται τα μηνύματα BPDU σε κάθε επόμενο switch. Μετά την προσαύξηση του root path cost, τα switches καταγράφουν τις τιμές αυτές στη μνήμη. Όταν ένα BPDU μήνυμα λαμβάνεται από μια άλλη θύρα και το νέο root path cost είναι μικρότερο από την προηγούμενη τιμή που είχε αποθηκεύσει η θύρα, αυτή η χαμηλότερη τιμή γίνεται το νέο path cost του switch.

Επιπρόσθετα το χαμηλότερο κόστος της τιμής ενημερώνει το switch πως η διαδρομή προς το root switch είναι καλύτερη χρησιμοποιώντας αυτή θύρα σε σχέση με τις άλλες θύρες. Ως εκ τούτου η νέα root port είναι η θύρα που έχει τη μικρότερη τιμή του root path cost.

Ένα switch μπορεί να έχει ενεργή μόνο μία θύρα ρίζας. Το root path cost προς το root switch υπολογίζεται από το άθροισμα των path cost που έχουν εκχωρηθεί εξ ορισμού σε κάθε θύρα για το ελάχιστο path cost. Οι εκχωρήσεις γίνονται συνήθως ως συνάρτηση του εύρους ζώνης των συνδέσεων. Όσο πιο μεγάλο είναι το εύρος ζώνης τόσο πιο μικρό είναι το path cost.

Bandwidth	Path Cost
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
200 Mbps	12
622 Mbps	6
1 Gbps	4
2 Gbps	3
10 Gbps	2

Εικόνα 15: Αντιστοιχία εύρους ζώνης με κόστος διαδρομής.

2.8.2.4 Επιλογή των Designated Ports

Μετά την επιλογή των root ports, το STP κάνει έναν επιπλέον υπολογισμό και αναγνωρίζει μία καθορισμένη θύρα (Designated Port) σε κάθε switch του δικτύου με παρόμοιο τρόπο όπως και τις θύρες ρίζας.

Τα switches επιλέγουν τη designated port σε σχέση με το συνολικό path cost προς τη root port. Αν υπάρχει ισοπαλία μεταξύ δύο switches ή παραπάνω, τότε γίνεται έλεγχος για το Bridge ID και επιλέγουν με βάση το κριτήριο αυτό τη designated port. Το ίδιο ισχύει και για την επιλογή της root port.

Η θύρα αυτή χρησιμοποιείται για την προώθηση κίνησης από και προς τα switches στο δίκτυο. Επιπλέον, είναι η θύρα που συνδέει το switch στο φυσικό σημείο σύνδεσης του ορισμένου switch. Κάθε switch έχει μόνο μία designated port. Οι υπόλοιπες θύρες που δεν έχουν οριστεί ως root port ή designated port θεωρούνται ως εναλλακτικές (Alternative Ports ή Non Designated Ports), μπαίνουν σε κατάσταση μπλοκαρίσματος (blocking) και δεν προωθείται κίνηση μέσω αυτών των θυρών.

2.8.2.5 Port States

Στα τοπικά δίκτυα μεταγωγών επειδή η τοπολογία των switches μπορεί να αλλάξει σε διαφορετικές χρονικές στιγμές και σε διαφορετικά σημεία του δικτύου με αποτέλεσμα τα switches να προσαρμόζονται σε αυτές τις αλλαγές. Η προσαρμογή γίνεται με τη μετάβαση σε διαφορετικές καταστάσεις των θυρών των switches. Οι θύρες μπορούν να μεταβούν σε πέντε διαφορετικές καταστάσεις:

- **Blocking:** Όλες οι θύρες των switches όταν ενεργοποιούνται για πρώτη φορά είναι εξ ορισμού σε κατάσταση μπλοκαρίσματος. Οι θύρες σε αυτή τη κατάσταση δεν μπορούν να προωθήσουν κίνηση ούτε να προσθέσουν τις φυσικές διευθύνσεις από άλλες συσκευές στο πίνακα των φυσικών διευθύνσεων. Μπορούν να ακούν μόνο τα BPDUs μηνύματα από τα γειτονικά switches για να μαθαίνουν αλλαγές που γίνονται στο δίκτυο. Σκοπός αυτής της κατάστασης είναι να αποτρέψει τη δημιουργία βρόχων.
- **Listening:** Μία θύρα μεταβαίνει σε αυτή τη κατάσταση όταν το switch πιστεύει ότι η θύρα αυτή μπορεί να επιλεχτεί ως root port ή designated port. Με άλλα λόγια προετοιμάζεται η θύρα στη προώθηση δεδομένων. Σε αυτή τη κατάσταση δεν μπορεί ούτε να λάβει ούτε να στείλει δεδομένα. Επιτρέπεται όμως να δέχεται και να στέλνει BPDUs μηνύματα για να πάρει μέρος στη διαδικασία της δημιουργίας της τοπολογίας του STP. Τότε η θύρα μπορεί να χαρακτηριστεί ως root port ή designated port αφού το switch ενημερώνει τα υπόλοιπα switches στέλνοντας BPDUs μηνύματα. Αν η θύρα δεν χαρακτηριστεί ως root port ή designated port τότε επιστρέφει στη κατάσταση blocking.
- **Learning:** Αν η θύρα χαρακτηριστεί ως root port ή designated port, μετά από μια χρονική περίοδο που λέγεται forward delay, στη κατάσταση listening, επιτρέπεται να μεταβεί στη κατάσταση learning. Η θύρα εξακολουθεί να στέλνει και να δέχεται BPDUs μηνύματα όπως και πριν. Σε αυτή τη κατάσταση επιπλέον μπορεί να μαθαίνει και να προσθέτει στο πίνακα του τις φυσικές διευθύνσεις άλλων συσκευών. Forward delay είναι ο χρόνος που χρειάζεται για τη μετάβαση από τη κατάσταση learning στη κατάσταση listening, η οποία εξ ορισμού είναι δεκαπέντε δευτερόλεπτα.
- **Forwarding:** Μετά από άλλη μια χρονική περίοδο forward delay στη κατάσταση learning επιτρέπεται στη θύρα να μεταβεί στη κατάσταση forwarding. Σε αυτή τη κατάσταση η θύρα μπορεί να στέλνει και να δέχεται πακέτα δεδομένων, να συλλέγει τις φυσικές διευθύνσεις και να τις προσθέτει στο πίνακα του, να στέλνει και να δέχεται BPDUs μηνύματα. Η θύρα πλέον σε πλήρη λειτουργικότητα.
- **Disabled:** Οι θύρες μεταβαίνουν σε αυτή τη κατάσταση όταν απενεργοποιούνται από τον διαχειριστή του δικτύου ή από το ίδιο το σύστημα εξαιτίας κάποιου ελαττώματος. Η κατάσταση αυτή είναι

ιδιαίτερη και δεν αποτελεί μέρος της φυσιολογικής εξέλιξης του STP για μια θύρα.

2.8.2.6 Topology Change Notification

Σε ένα τοπικό δίκτυο μεταγωγής, αν συμβούν αλλαγές στη τοπολογία τότε πρέπει να ληφθούν υπόψη οι αλλαγές στη διαδικασία εκμάθησης των φυσικών διευθύνσεων. Με την οποιαδήποτε αλλαγή ή τροποποίηση του δικτύου μπορεί να επιφέρει αλλαγές στις διαδρομές που ακολουθούν οι μεταδόσεις των δεδομένων διαμέσου των θυρών των switches. Για το λόγο αυτό είναι αναγκαίος ένας μηχανισμός με σκοπό την ενημέρωση της νέας επικοινωνίας μεταξύ των θυρών και των φυσικών διευθύνσεων που απαιτείται. Αυτός ο μηχανισμός ονομάζεται Topology Change. Στόχος του είναι να ενημερώνει όλα τα switches για τις αλλαγές που έχουν συμβεί στη τοπολογία του δικτύου και τα αναγκάζει να διαγράψουν όλες τις φυσικές διευθύνσεις των συσκευών που είχαν αποθηκεύσει.

Η ενημέρωση για την οποιαδήποτε αλλαγή στη τοπολογία ενός ενεργού δικτύου γίνεται με την μετάδοση των TCN BPDUs μηνυμάτων από τα switches μέσω των root ports προς το root switch. Σε αυτό το περιεχόμενο του μηνύματος δεν περιέχονται πεδία πληροφοριών γιατί είναι προειδοποιητικό μήνυμα για το root switch. Ωστόσο, διαφέρει από το configuration BPDU μήνυμα και δεν εμπεριέχεται σε κάποιο από τα πεδία του διότι τα Configuration BPDUs μηνύματα προέρχονται από τα non-designated switches και δεν παραμένουν στη μνήμη των switches αλλά διαγράφονται. Γι’ αυτό το λόγο χρησιμοποιούνται για τη διαδικασία αυτή τα TCN BPDUs μηνύματα.

Υπάρχουν δύο περιπτώσεις στις οποίες συμβαίνει ανίχνευση αλλαγή της τοπολογίας ενός δικτύου. Όταν ένα switch αλλάξει τη κατάσταση μιας θύρας σε κατάσταση forwarding και είναι ταυτόχρονα και designated ή όταν το switch αλλάξει τη κατάσταση μιας θύρα σε κατάσταση blocking. Δηλαδή όταν μια θύρα γίνεται ενεργή ή παύει να λειτουργεί. Τότε το switch στέλνει μέσω του root port ένα TCN BPDU μήνυμα έτσι ώστε να το λάβει το root switch και να ενημερωθεί για την αλλαγή που προέκυψε.

Έτσι λοιπόν, κάθε switch όταν ανιχνεύει μία αλλαγή ή δέχεται ένα τέτοιο μήνυμα, αρχίζει και στέλνει το ίδιο μήνυμα κάθε δύο δευτερόλεπτα που είναι ο χρόνος hello time μέχρι να παραλάβει επιβεβαίωση από κάποιο γειτονικό switch που βρίσκεται από πάνω του. Όταν τα γειτονικά switches λάβουν το TCN BPDU μήνυμα τότε θα το διαδώσουν προς το root switch. Αφού λάβει το μήνυμα το root switch, τότε θα στείλει πίσω ένα μήνυμα επιβεβαίωσης μέσω των designated ports. Άλλωστε, τα TCN BPDUs μηνύματα αποστέλλονται προς το root switch. Επιπλέον, προσθέτει το topology change flag στο configuration BPDU μήνυμα που διαδίδει έτσι ώστε όλα τα υπόλοιπα switches να ενημερωθούν για την αλλαγή που έγινε και πως τις φυσικές διευθύνσεις που έχουν μάθει οι θύρες τους πλέον μπορεί να είναι λανθασμένες. Με αυτό τον τρόπο, το topology change flag, αναγκάζει τα switches να μειώσουν το μέγιστο χρόνο εκμάθησης του πίνακα διευθύνσεων από τη προεπιλεγμένη τιμή (300 δευτερόλεπτα)

στη τιμή του χρόνου του forward delay. Με αυτό τον τρόπο τα switches αναγκάζονται να διαγράψουν συντομότερα από το κανονικό χρονικό όριο τις φυσικές διευθύνσεις που έχουν μάθει, διευκολύνοντας την αλλοίωση του πίνακα διευθύνσεων που θα μπορούσε να συμβεί με την αλλαγή της τοπολογίας του δικτύου. Ωστόσο, οι φυσικές διευθύνσεις των συσκευών που επικοινωνούν ενεργά κατά τη διάρκεια αυτής της ενέργειας, θα παραμείνουν στο πίνακα των switches. Η ενέργεια αυτή διαρκεί 15+20=35 δευτερόλεπτα (forward delay + max age).

2.8.2.7 Χρόνος Σύγκλισης (Convergence Time)

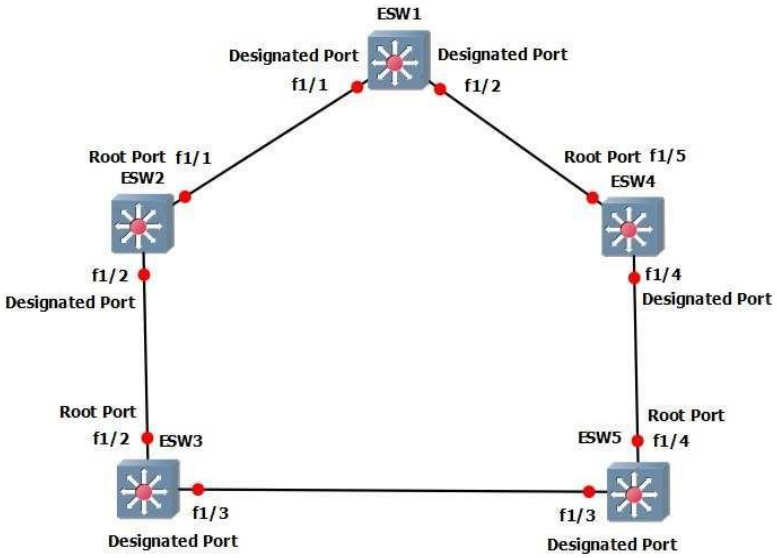
Το κομμάτι αυτό συγκεκριμένα υπολογίζει ποια ακριβώς είναι η χρονική στιγμή την οποία όλα τα switches έχουν φτάσει στη τελική τους διαμόρφωση στη τοπολογία του STP, και συνεπώς την ολοκλήρωση της λειτουργίας του πρωτοκόλλου.

Υπάρχουν αρκετές και διαφορετικές περιπτώσεις στις οποίες το STP εκτελεί μια επαναδιαμόρφωση των switches, που μπορεί να είναι είτε μερική είτε ολική. Η πιο απλή περίπτωση είναι όταν ξεκινούμε τη λειτουργία ενός δικτύου και τα switches θα ενεργοποιηθούν για πρώτη φορά και θα πρέπει να συμφωνήσουν σε μια νέα τοπολογία και βάση δεδομένων. Με απλά λόγια είναι το χρονικό διάστημα που απαιτείται για τις θύρες των switches όταν έρχονται για πρώτη φορά σε λειτουργία να μεταβούν από τη κατάσταση blocking σε κατάσταση forwarding και να ξεκινήσει η προώθηση των δεδομένων. Ο συνολικός χρόνος σύγκλισης των θυρών από τη μετάβαση της κατάσταση τους από listening σε learning και forwarding είναι συνολικά 30 δευτερόλεπτα (15+15 ή 2* forward delay). Αυτό συμβαίνει διότι οι θύρες δεν βρίσκονταν σε κατάσταση blocking με αποτέλεσμα να εξοικονομούν 20 δευτερόλεπτα που είναι ο χρόνος max age. Αν οι θύρες βρίσκονται στη κατάσταση blocking τότε ο χρόνο μετάβασης σε κατάσταση forwarding είναι 50 δευτερόλεπτα (15+15 ή 2* forwarding delay + 20 (max age)) που είναι και ο προεπιλεγμένος χρόνος των switches. Ο χρόνος αυτός γίνεται να αλλαχτεί από τον διαχειριστή του δικτύου αλλά δεν συνιστάται. Αυτή η χρονική σύγκλιση ονομάζεται Initial Convergence.

Μια άλλη περίπτωση είναι όταν έχουμε επαναδιαμόρφωση της τοπολογίας του δέντρου του STP όταν μια ενεργή σύνδεση παθαίνει κάποια βλάβη και καταρρέει. Αυτού του είδους η επαναδιαμόρφωση της τοπολογίας μπορεί να είναι μερική γιατί αν έχει καταρρεύσει μια σύνδεση θα πρέπει να αντικατασταθεί από κάποια άλλη. Τέτοιου είδος σύγκλισης ονομάζεται Convergence After a Failure.

Ακόμη και μια διακοπή σύνδεσης στο δίκτυο έχει διαφορετικές επιπτώσεις και επιδράσεις στο χρόνο επανασύγκλισης του STP ανάλογα σε ποιο σημείο της τοπολογίας έχει συμβεί η βλάβη. Ωστόσο, δεν είναι θέμα της φυσικής τοποθεσίας, αλλά θέμα αντίληψης των switches. Το STP αναφέρεται σε δύο ειδών βλάβες. Την άμεση βλάβη (Direct Failure) και την έμμεση βλάβη (Indirect Failure).

Για να καταλάβουμε τι ακριβώς είναι το direct failure και τι το indirect failure, και από ποια προοπτική βλέπει τη κάθε βλάβη ένα switch ας δούμε το παρακάτω δίκτυο και θα εξηγήσουμε πως αντιλαμβάνεται το STP τις βλάβες.



Εικόνα 16: Δίκτυο παραδείγματος

Αν για παράδειγμα το root port του switch ESW2 έχει κάποια βλάβη το ίδιο το switch θα θεωρήσει τη βλάβη αυτή ως direct failure. Το switch θα εντοπίσει άμεσα πως η φυσική του θύρα δεν λειτουργεί και το STP θα ενεργήσει αναλόγως για να επιλύσει το πρόβλημα. Την ίδια βλάβη αντίστοιχα το switch ESW3 θα την αντιμετωπίσει ως indirect failure. Αυτό θα συμβεί, γιατί η θύρα που έχει το πρόβλημα ανήκει στο switch ESW2 και όχι στο switch ESW3. Το switch ESW3 θα χάσει το δρόμο του προς root switch που είναι το switch ESW1 και θα πρέπει να ενημερωθεί μέσω των BPDUs μηνυμάτων από τα γειτονικά switch για την αλλαγή που έχει συμβεί στη τοπολογία αφού δεν μπορεί πλέον να προωθήσει πληροφορίες μέσω του ESW2.

Επομένως καταλαβαίνουμε πως όταν μία θύρα ενός switch έχει κάποια βλάβη και δεν λειτουργεί, το ίδιο το switch την θεωρεί ως direct failure ενώ αντίθετα τα γειτονικά switch την αντιμετωπίζουν ως indirect failure.Και στις δύο περιπτώσεις, κατά τη διάρκεια της σύγκλισης δεν έχουμε προώθηση της κίνησης δεδομένων μέσω των switches.

2.8.3 Rapid Spanning Tree Protocol

Μέχρι τώρα έχουμε αναφερθεί στο αρχικό STP. Το STP για εκείνη την εποχή που χρησιμοποιήθηκε δούλεψε σωστά. Με το πέρασμα των χρόνων και την εξέλιξη της τεχνολογίας, συνεπώς και την εξέλιξη των δικτύων και των τηλεπικοινωνιών, η ανάγκη για αναβάθμιση των διάφορων πρωτοκόλλων ήταν απαραίτητη μιας και οι απαιτήσεις της τεχνολογίας των τοπικών δικτύων αυξάνονταν παράλληλα. Έτσι και το STP δέχτηκε κάποιες βελτιώσεις. Μία από τις βελτιώσεις που δέχτηκε στη πάροδο του χρόνου ήταν η εισαγωγή του Rapid Spanning Tree Protocol (RSTP) που εισήχθη ως το πρότυπο IEEE 802.1w. Αρχικά η IEEE δημοσίευσε τη τροποποίηση του πρότυπου 802.1w το 2001. Έπειτα, το 2004 η επιτροπή του IEEE ενημερώνει το πρότυπο 802.1d και στη συνέχεια παίρνει τις λεπτομέρειες του τροποποιημένου προτύπου 802.1w και τις προσθέτουν στο πρότυπο 802.1d-2004.

2.8.3.1 Σύγκριση RSTP με STP και επιπλέον χαρακτηριστικά

Εάν συγκρίνουμε τα δύο πρωτόκολλα STP και RSTP θα δούμε ότι έχουν πάρα πολλές ομοιότητες και ουσιαστικά το RSTP λειτουργεί όπως και το αυθεντικό STP.

- Εκλέγει το root switch χρησιμοποιώντας τις ίδιες παραμέτρους και τις ίδιες προϋποθέσεις.
- Επιλέγει το root port σε κάθε switch με τους ίδιους κανόνες.
- Επιλέγει τις designated ports σε κάθε τομέα του τοπικού δικτύου με τους ίδιους κανόνες.
- Τοποθετεί τις θύρες των switches στις διάφορες καταστάσεις, από forwarding ή blocking.

Παρ' όλο που τα δυο πρωτόκολλα φαίνεται να δουλεύουν ακριβώς με τον ίδιο τρόπο, έχουν μια σημαντική διαφορά, που είναι και ο κύριος λόγος που δημιουργήθηκε το RSTP. Η διαφορά αυτή είναι ο χρόνος σύγκλισης. Το STP για να συγκλίνει χρειάζεται 30-50 δευτερόλεπτα ανάλογα με το είδος της βλάβης στο δίκτυο, με τις προεπιλεγμένες ρυθμίσεις όταν πρέπει να ακολουθούνται όλοι οι χρόνοι αναμονής. Χρόνος αρκετά μεγάλος και σημαντικός που είναι απαράδεκτος για την εποχή μας. Το RSTP έρχεται να βελτιώσει αυτή τη σύγκλιση, όταν υπάρξουν αλλαγές στη τοπολογία του δικτύου, μέσα σε λίγα δευτερόλεπτα (ή σε αργές συνθήκες, σε περίπου 10 δευτερόλεπτα).

Το RSTP αλλάζει και προσθέτει στο STP τρόπους με τους οποίους αποφεύγει να περιμένει τους χρόνους του STP, με αποτέλεσμα τις γρήγορες μεταβολές των καταστάσεων των θυρών των switches από forward σε blocking και το αντίστροφο. Πιο συγκεκριμένα, το RSTP ορίζει περισσότερες περιπτώσεις στις οποίες ένα switch μπορεί να αποφύγει την αναμονή των χρονομέτρων ως την λήξη τους, όπως είναι οι ακόλουθες.

- Προσθέτει έναν νέο μηχανισμό στο να αντικαταστεί το root port, χωρίς να περιμένει να φτάσει σε κατάσταση forwarding (σε ορισμένες περιπτώσεις).
- Προσθέτει έναν νέο μηχανισμό στο να αντικαταστεί το designated port, χωρίς να περιμένει να φτάσει σε κατάσταση forwarding (σε ορισμένες περιπτώσεις).
- Μειώνει τους χρόνους αναμονής σε περίπτωση που το RSTP πρέπει να περιμένει.

Με το RSTP, κάθε switch ξεχωριστά, αναπαράγει RSTP Configuration BPDUs μηνύματα κάθε δύο δευτερόλεπτα (hello time). Αντιθέτως, στο STP κάθε switch αναμεταδίδει ένα hello μήνυμα το οποίο αναπαράγεται από το root switch. Το τοπικά παραγόμενο BPDU μήνυμα εξυπηρετεί το ρόλο του "διασώστη" που επαληθεύει τη συνδεσιμότητα μεταξύ των γειτονικών switches. Για παράδειγμα, όταν ένα switch σταματήσει να δέχεται hellos από ένα άλλο γειτονικό συνδεδεμένο switch, τότε μπορεί να υποθέσει με σιγουριά πως έχει χαθεί η συνδεσιμότητα σε αυτή τη θύρα χωρίς να περιμένει να λήξουν τα χρονόμετρα του πρωτοκόλλου. Απώλεια συνδεσιμότητας θεωρείται όταν τρία συνεχόμενα hellos μηνύματα έχουν

χαθεί. Ένα switch μπορεί να επιταχύνει περαιτέρω τη διαδικασία ανακατεύθυνσης παρακολουθώντας τις διασυνδέσεις του ώστε να ανιχνεύσει θύρες και συνδέσεις που δεν λειτουργούν χωρίς να χρειάζεται να περιμένει για τα χαμένα RSTP Hellos.

2.8.3.2 RSTP Port Roles

Ο καλύτερος τρόπος για να καταλάβουμε πως λειτουργούν οι μηχανισμοί που αναφέραμε προηγουμένως, είναι να εξηγήσουμε πως η εναλλακτική θύρα (alternate port) και η εφεδρική θύρα (backup port) δουλεύουν. Είναι δύο νέοι ρόλοι που το RSTP προσθέτει επιπλέον στο αρχικό STP.

2.8.3.3 Λειτουργία Εναλλακτικής Θύρας

Όπως με το STP, τα switches καθόριζαν μία από τις θύρες τους ως root port έτσι και το RSTP ακολουθεί την ίδια συνθήκη με τους ίδιους ακριβώς κανόνες για να επιλέξει το root port. Έπειτα όμως το RSTP προχωράει κάνοντας ένα ακόμη βήμα, επιλέγοντας μία ή παραπάνω θύρες ως εναλλακτικές πιθανές root ports. Για να οριστεί μία θύρα ως εναλλακτική θα πρέπει και το root port και το alternate port να δέχονται hellos μηνύματα που θα αναγνωρίζουν το ίδιο root switch. Μία alternate port ουσιαστικά δουλεύει ως τη δεύτερη καλύτερη επιλογή για το root port. Η alternate port μπορεί να αναλαμβάνει τον ρόλο του root port, συχνά πολύ γρήγορα, χωρίς να απαιτείται αναμονή σε άλλες ενδιάμεσες καταστάσεις του RSTP.

Για παράδειγμα, όταν ένα root port καταρρεύσει, ή όταν σταματήσει δέχεται hellos, τότε το switch αλλάζει το ρόλο του root port σε disable port και την κατάσταση του από forwarding σε discarding. Στη συνέχεια, χωρίς να περιμένει άλλα χρονόμετρα, το switch αλλάζει το ρόλο του alternate port σε root port και τη κατάστασή του σε forwarding. Επίσης σημαντικό είναι να σημειωθεί πως το νέο root port δεν χρειάζεται επίσης να ξοδέψει χρόνο σε άλλες καταστάσεις όπως τη learning, αλλά αντιθέτως μπαίνει απευθείας σε κατάσταση forwarding.

2.8.4 Per Vlan STP and Per Vlan STP+

Με την εξέλιξη της τεχνολογίας και την εισαγωγή των Virtual LANs (VLANs) στα δίκτυα μεταγωγής, τα οποία χρησιμοποιούνται πλέον, για περαιτέρω υποδιαίρεση των μεταδιδόμενων ή ανεπαρκών τομέων, με σκοπό την απομόνωση της μεταδιδόμενης κίνησης βάση την ομάδα χρηστών ή τύπο εφαρμογής και να υποστηρίξει την εξισορρόπηση του φορτίου σε όλες τις περιττές συνδέσεις.

Το πρότυπο 802.1D (STP) σε συνδυασμό με το πρότυπο 802.1Q (vlans) θέτουν αυστηρούς περιορισμούς στη ποικιλομορφία των vlans που μπορεί να διαμορφωθεί. Πιο συγκεκριμένα, το STP υποθέτει πως θα πρέπει να υπάρχει μία μοναδική λογική τοπολογία στο δίκτυο μεταγωγής. Αυτό σημαίνει πως η χρήση του STP σε ένα δίκτυο όπου vlans επεκτείνονται σε πολλά switches χρησιμοποιώντας το πρωτόκολλο πολλαπλών γραμμών (trunking protocol)

όπως το 802.1Q προϋποθέτει πως όλα τα vlans μοιράζονται την ίδια τοπολογία. Με τον τρόπο αυτό μειώνεται ο βαθμός απομόνωσης της κίνησης δεδομένων που μπορούν να παρέχουν, και σπαταλούν εύρος ζώνης κατά τη διάρκεια της μετάδοσης και υπερχείλισης των πακέτων δεδομένων. Επιπλέον, η μοναδική τοπολογία εξαναγκάζει κάθε εφεδρική διαδρομή να είναι σε κατάσταση blocking για όλη τη διάρκεια της κίνησης δεδομένων, σπατάλη της χωρητικότητας του εύρους ζώνης που μπορεί να αποφευχθεί, αν πολλαπλές λογικές τοπολογίες μπορούν να συνυπάρχουν σε κάποιο δίκτυο μεταγωγής.

Η έλλειψη για την επίγνωση των vlans οδήγησε στην ανάπτυξη ενός άλλου συνόλου κατοχυρωμένων βελτιώσεων, από τον οργανισμό IEEE και την εταιρία CISCO, για την επίγνωση των vlans στο STP, όπως το Per-Vlan Spanning Tree (PVST) και το PVST+ .

2.8.5 PVST

Με το PVST μας επιτρέπεται να έχουμε στο δίκτυο μας αρκετές περιπτώσεις του STP που να εκτελούνται. Με την εκτέλεση διαφορετικής περίπτωσης του STP σε μια βάση ανά vlan, μπορούμε να τρέξουμε μερικά vlans σε θύρες που είναι σε κατάσταση blocking από κάποια άλλη περίπτωση του STP που τρέχει σε κάποιο άλλο vlan. Σε μια τέτοια περίπτωση, μπορούμε να ορίσουμε τη προτεραιότητα της κάθε θύρας σε κάθε βάση του vlan, επιτρέποντας μας να χρησιμοποιήσουμε τις εφεδρικές διαδρομές του δικτύου να τρέχουν ίδιο ποσό της κίνησης δεδομένων σε κάθε σύνδεση. Τα vlans ξεχωριστά καθορίζουν από ποιες συνδέσεις θα προωθήσουν κίνηση και ποιες θα μπλοκάρουν.

Όπως με τον καθορισμό προτεραιότητας των θυρών, η θύρα με τη μικρότερη τιμή προτεραιότητας για κάθε vlan είναι αυτή που θα προωθεί τα πλαίσια. Αν δύο ή παραπάνω θύρες έχουν την ίδια τιμή προτεραιότητας για ένα συγκεκριμένο vlan, τότε η θύρα με τη χαμηλότερη τιμή θύρας θα προωθήσει τα πλαίσια για το vlan.

Το PVST είναι μια ανεπτυγμένη λύση της εταιρίας CISCO για τα προβλήματα κλιμάκωσης και σταθερότητας που σχετίζονται με το STP σε μεγάλης κλίμακας δίκτυα που εκτείνονται στη τοπολογία μορφής δέντρου. Το PVST δημιουργεί μια ξεχωριστή περίπτωση του STP σε κάθε vlan στο τμήμα του switch. Αυτή η εγκατάσταση δίνει σε κάθε vlan μία μοναδική τοπολογία του STP που περιέχει το δικό του κόστος θύρας, κόστος διαδρομής, προτεραιότητα και root switch.

Χρησιμοποιώντας ξεχωριστές περιπτώσεις του PVST σε κάθε vlan, μειώνουμε το χρόνο σύγκλισης για τον υπολογισμό εκ νέου του STP και αυξάνουμε την αξιοπιστία του δικτύου. Με την εκτέλεση του PVST, το γενικό μέγεθος της τοπολογίας του STP μειώνεται σε σημαντικό βαθμό. Επιπλέον, βελτιώνει την κλιμάκωση και μειώνει το χρόνο σύγκλισης με αποτέλεσμα να παρέχει ταχύτερα την επαναφορά του δικτύου σε περίπτωση κατάρρευσης του δικτύου. Επιτρέπει επίσης, τον έλεγχο των διαδρομών που προωθούν κίνηση σε κάθε βάση υποδικτύου.

Το PVST ωστόσο, δημιουργεί μειονεκτήματα στη τοπολογία του STP. Χρησιμοποιεί περισσότερη επεξεργαστική ισχύ και καταναλώνει περισσότερο εύρος ζώνης για να μπορεί να υποστηρίξει τη διατήρηση της τοπολογίας του STP και τα μηνύματα BPDUs για κάθε vlan διότι επιτρέπεται για κάθε vlan να έχουμε ένα root switch. Αυτό δίνει τη δυνατότητα στο STP να αξιοποιήσει με τον καλύτερο τρόπο την κίνηση δεδομένων για κάθε vlan επιτρέποντας να ρυθμίσουμε το root switch στο κέντρο του κάθε vlan.

Με το PVST σημαίνει πως 1.000 vlans θα εκτελούν 1.000 διαφορετικές περιπτώσεις του STP. Λόγω της φύσης του, το PVST χρειάζεται τη χρήση συνδέσεων Cisco Inter-Switch Link (ISL) και κανάλια ενθυλάκωσης μεταξύ των switches. Σε δίκτυα που συνυπάρχουν το STP και το PVSTP, μπορεί να συμβούν προβλήματα διαλειτουργικότητας. Κάθε ένα από αυτά απαιτεί και διαφορετική μέθοδο ενθυλάκωσης έτσι ώστε τα μηνύματα BPDUs να μην ανταλάσονται ποτέ μετάξύ των τύπων του STP. Οι συνδέσεις ISL χρησιμοποιούν μια τοπολογία STP για κάθε vlan, χρησιμοποιώντας το PVST πάνω στα κανάλια του ISL. Επίσης το PVST λειτουργεί εξ' ορισμού στα switches της εταιρίας CISCO, το οποίο σημαίνει την επιλογή της καλύτερης δυνατής διαδρομής, συνεχίζοντας ο χρόνος σύγκλισης να είναι αργός.

2.8.6 PVST+

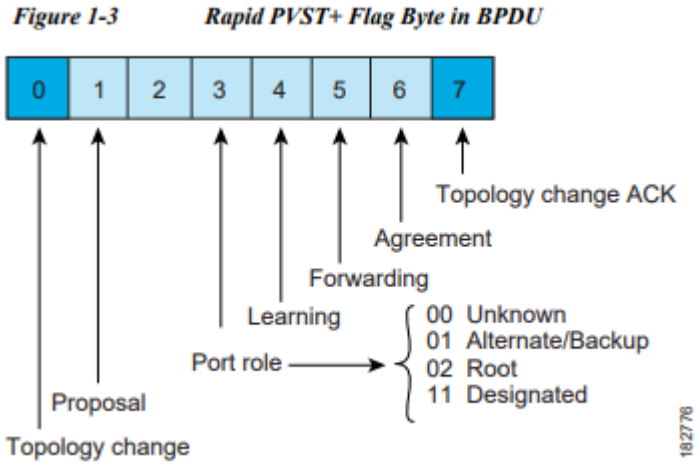
Όσο αφορά τη τεχνολογία του PVST+ , η εταιρία CISCO, δεν έχει τεκμηριώσει πολύ ορθά τη λειτουργία της. Το πρότυπο 802.1Q μπορεί να χρησιμοποιήσει το PVST+ για να χαρτογραφήσει πολλαπλές τοπολογίες του STP στη τοπολογία του αυθεντικού προτύπου 802.1Q που υποστηρίζουν τα switches. Ο τύπος σύγκλισης ταιριάζει αρκετά με το τύπο σύγκλισης του STP, που έχει μόνο μία περίπτωση του STP ανεξαρτήτως του αριθμό των vlan που υπάρχουν στο δίκτυο. Η διαφορά είναι πως με το PVST+, η σύγκλιση συμβαίνει σε κάθε βάση των vlan, με κάθε vlan να τρέχει τη δικιά του περίπτωση του STP, το οποίο μας δείχνει πως τώρα έχουμε μια αποτελεσματική εκλογή του root switch για κάθε vlan.

Για να επιτραπεί στο PVST+ η λειτουργία, υπάρχει ένα πεδίο μέσα στα μηνύματα BPDUs που δέχεται το εκτεταμένο ID συστήματος (Extended System ID) ώστε το PVST+ να μπορεί να έχει ένα διαμορφωμένο root switch για κάθε περίπτωση του STP.

Το PVST+ υποστηρίζει αποτελεσματικά τρεις ομάδες του STP που μπορούν να λειτουργούν σε ένα κοινό δίκτυο. Switches που υποστηρίζουν το PVST, PVST+ και το CST/MST πάνω στο πρότυπο IEEE 802.1Q μπορούν να επικοινωνούν και να δουλεύουν άρτια.

Για να συμβεί αυτό, το PVST+ λειτουργεί ως μεταφραστής μεταξύ των switches που υποστηρίζουν το STP και των switches που υποστηρίζουν PVST. Το PVST+ μπορεί να επικοινωνήσει απευθείας με το με PVST μέσω των ISL καναλιών.

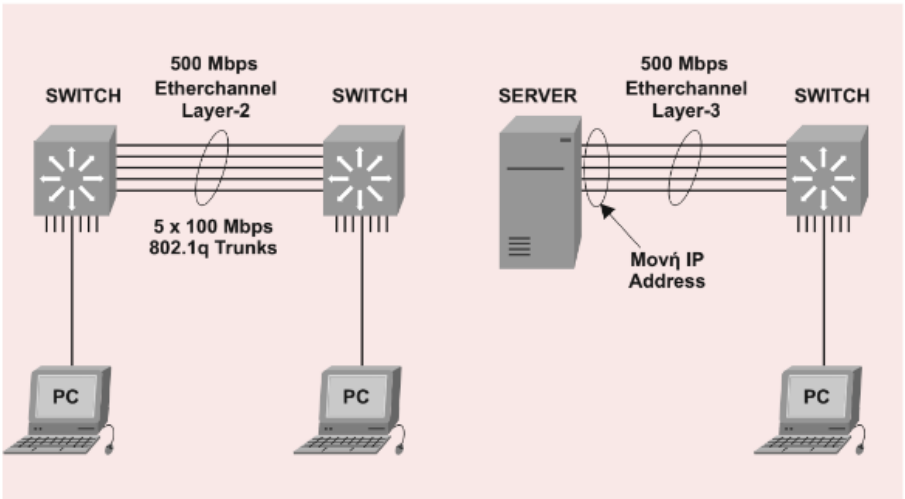
Για να επικοινωνήσει με το STP όμως, το PVST+ ανταλλάζει μηνύματα BPDUs με το STP στο vlan 1. BPDUs από άλλα vlans εξαπλώνονται διαμέσου των STP τμημάτων του δικτύου από σήραγγες. Το PVST+ στέλνει αυτά τα BPDUs χρησιμοποιώντας μια μοναδική διεύθυνση πολλαπλής διανομής έτσι ώστε τα CST switches να προωθήσουν τα μηνύματα αυτά προς τα κατώτερα γειτονικά switches. Τελικά, τα tunneled BPDUs μηνύματα θα καταλήξουν σε άλλα PVST+ switches που θα τα καταλάβουν.



Εικόνα 17 : Χρήση των σημαίων του πακέτου BPDU στο PVST+

2.9 EtherChannel (IEEE 802.3ad)

Συχνά υπάρχει η ανάγκη για περισσότερες από μια συνδέσεις ανάμεσα στα switch ώστε να έχουμε αυξημένη χωρητικότητα, εφεδρεία και κατανομή φόρτου. Για τη περίπτωση αυτή δημιουργήθηκε το EtherChannel που είναι μια λογική ομαδοποίηση πολλών κομβικών συνδέσεων (από 2 ως 8) μεταξύ των switch, ώστε να εμφανίζονται σαν μια ενιαία γραμμή σύνδεσης, με χωρητικότητα τη συνολική των συμμετεχόντων γραμμών.



Εικόνα 18: Σχήμα EtherChannel

Το EtherChannel χρησιμοποιείται κυρίως στις κομβικές ζεύξεις μεταξύ switch αλλά και ενίοτε για σύνδεση με ακραίες συσκευές όπως servers. Οι γραμμές που απαρτίζουν το EtherChannel πρέπει να είναι της ίδιας ταχύτητας και όταν αυτό υλοποιηθεί εμφανίζει μια ενιαία MAC address στη τερματική συσκευή.

Αν δεν εφαρμοζόταν το EtherChannel δεν θα μπορούσαν να λειτουργήσουν παράλληλες συνδέσεις μεταξύ των switch διότι θα τις απενεργοποιούσε το πρωτόκολλο Spanning Tree (SPT) για την αποφυγή των βρόγχων γεφύρωσης. Το STP αντιλαμβάνεται το EtherChannel ως μια γραμμή και έτσι δεν παρεμποδίζει τη λειτουργία του.

Μια παραλλαγή του είναι το layer-3 EtherChannel όπου αποδίδεται μια ενιαία IP διεύθυνση στο καταληκτικό interface.

2.10 Network Address Transaltion (NAT)

Το NAT αποτελεί ένα πρωτόκολλο 3ου επιπέδου το οποίο χρησιμοποιείται για την αντιστοίχιση των ιδιωτικών IP διευθύνσεων που υπάρχουν σε ένα LAN με τις δημόσιες IP διευθύνσεις του Internet που είναι καταχωρημένες από την IANA (Internet Assigned Numbers Authority).

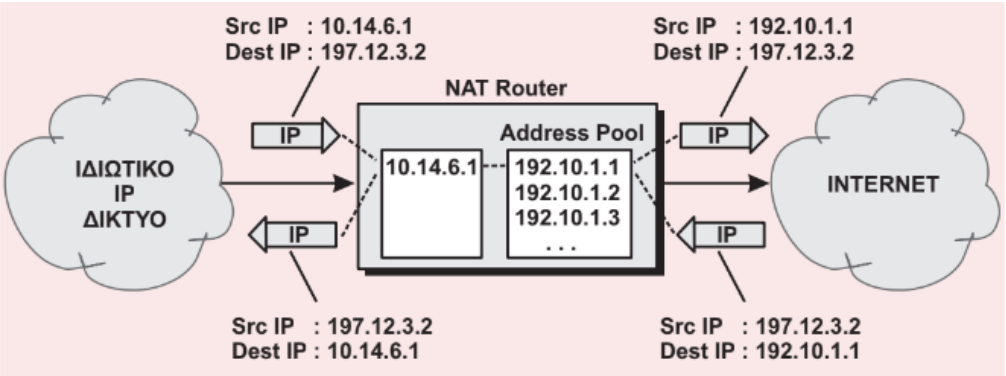
Η IANA έχει ορίσει συγκεκριμένο πακέτο διευθύνσεων IP που δεν μπορούν να υπάρχουν στο Internet και οι οποίες χρησιμοποιούνται ως ιδιωτικές διευθύνσεις σε τοπικά δίκτυα.

Πρακτικά λοιπόν το NAT υλοποιείται εκεί που συνδέεται το δημόσιο Internet με κάθε ιδιωτικό δίκτυο. Έτσι καταφέρνουμε να έχουμε την ίδια ιδιωτική IP διεύθυνση σε διαφορετικούς υπολογιστές που ανήκουν σε διαφορετικά τοπικά δίκτυα οπουδήποτε, αλλά όταν αποκτούν πρόσβαση στο Net μέσω του NAT αποκτούν διαφορετικές δημόσιες καταχωρημένες διευθύνσεις.

Θα μπορούσαμε λοιπόν να ανάγουμε το NAT ως ένα ιδιωτικό εταιρικό τηλεφωνικό κέντρο που ενώ προς το δημόσιο δίκτυο έχει ένα αριθμό κλήσης, εσωτερικά εξυπηρετεί 10 τηλέφωνα .Ανάλογα του Τηλεφωνικού Κέντρου και του εσωτερικού τηλεφώνου θα θεωρήσουμε αντίστοιχα τον δρομολογητή και το PC.

Οι τύποι NAT είναι οι εξής : Στατικός , δυναμικός και ο Port Translation.

1. **Στατικός** (Static) : Σε αυτόν τον τύπο η αντιστοίχιση μεταξύ των ιδιωτικών IP διευθύνσεων κάθε τοπικού δικτύου καθώς και των δημόσιων IP του Internet είναι σταθερή. Χρησιμοποιείται σε servers του τύπου web / mail servers των οποίων οι διευθύνσεις είναι σταθερές.
2. **Δυναμικός** (Dynamic/pool) : Με τον τύπο αυτό μια μικρή ομάδα εξωτερικών IP διευθύνσεων εξυπηρετεί τις εσωτερικές IP χωρίς να αντιστοιχίζονται μία προς μία. Όταν ένας υπολογιστής θέλει να επικοινωνήσει με το Internet αντιστοιχίζεται με την πρώτη ελεύθερη IP της ομάδας των εξωτερικών διευθύνσεων.



Εικόνα 19: Δυναμικό NAT

3. **Port Address Translation** Σε αυτό το τύπο μια καταχωρημένη IP διεύθυνση μπορεί ταυτόχρονα να χρησιμοποιηθεί από πολλούς χρήστες του τοπικού δικτύου μέσω των θυρών στο TCP.Η περίπτωση αυτή εμφανίζεται συχνότερα

από τις άλλες καθώς υποστηρίζει τη μοναδική σύνδεση ενός LAN με το Internet, μέσω π.χ. ενός ADSL/VDSL δρομολογητή.

Η τελευταία περίπτωση ονομάζεται και **NAT overloading** (υπερφόρτωση διευθύνσεων) και αποτελεί βασικό παράγοντα μαζικοποίησης του Ίντερνετ, αφού μπορούμε να έχουμε πρόσβαση από πολλά PC ενός LAN αρκεί να υπάρχει έστω και μία δημόσια διεύθυνση Διαδικτύου. Ο τύπος αυτός εκμεταλλεύεται τη δυνατότητα τη δυνατότητα πολύπλεξής του TCP/IP protocol stack που στην ουσία επιτρέπει να επιτυγχάνονται περισσότερες της μιας ταυτόχρονες συνδέσεις με το Ίντερνετ χρησιμοποιώντας τις θύρες TCP(ή UDP). Για να καταλάβουμε καλύτερα το μηχανισμό αυτό αξίζει να θυμηθούμε ότι στους header των IP και TCP πακέτων έχουμε

- Διεύθυνση Αποστολέα με την εσωτερική IP του (π.χ. 192.168.1.2)
- TCP Θύρα Αποστολέα (ή UDP), προσωρινή, που βάζει ο αποστολέας, σε αυτό το πακέτο, για να χαρακτηρίσει το συγκεκριμένο session.
- IP δημόσια Διεύθυνση Παραλήπτη.
- Θύρα Προορισμού , ο αριθμός θύρας TCP που σχετίζεται με την εφαρμογή (π.χ. web).

Ο συνδυασμός των τεσσάρων αυτών αριθμών προσδιορίζει μια συγκεκριμένη TCP/IP σύνδεση. Ας δούμε ένα παράδειγμα λειτουργίας του τύπου Port Address Translation.

	SOURCE		DESTINATION	
	IP address	TCP port	IP address	TCP port
ΑΙΤΗΣΗ				
Από PC προς Router :	192.168.1.5	1331	192.168.1.1	80
Από Router προς Web Srv:	210.10.2.1	1331	221.11.3.1	80
ΑΠΑΝΤΗΣΗ				
Από Web Srv προς Router:	221.11.3.1	80	210.10.2.1	1331
Από Router προς PC:	192.168.1.1	80	192.168.1.5	1331

Εικόνα 20: Αντιστοίχιση πορτών Ε/ Ε στο Port Address Translation

Έστω ότι έχουμε ένα ιδιωτικό δίκτυο όπου η επικοινωνία των σταθμών του γίνεται με private IP διευθύνσεις (π.χ. 10.x.x.x) . Το δίκτυο αυτό συνδέεται στο Ίντερνετ μέσω ενός δρομολογητή ο οποίος διαθέτει λειτουργία NAT και έχει μια δημόσια εξωτερική IP διεύθυνση.

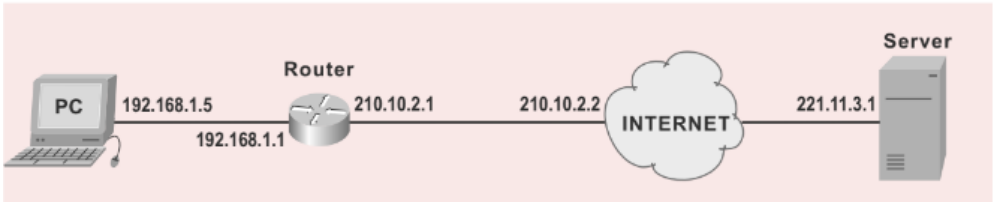
Ας υποθέσουμε ότι ένα PC του δικτύου επιχειρεί να συνδεθεί με ένα web server κάπου στο διαδίκτυο. Ο δρομολογητής λαμβάνει το IP πακέτο που έρχεται από το PC με προορισμό το Ίντερνετ και πριν το διώξει αντιγράφει την ιδιωτική IP διεύθυνση του PC αλλά και τον αριθμό της θύρας και τα τοποθετεί σε ένα πίνακα. Ο δρομολογητής αλλάζει την ιδιωτική IP διεύθυνση του αποστολέα(καθώς δεν είναι γνωστή στο Ίντερνετ) με τη δική του δημόσια IP

διεύθυνση. Επίσης αντικαθιστά την TCP θύρα αποστολέα με ένα TCP προσωρινό αριθμό που δίνει ο ίδιος για να χαρακτηρίσει την συγκεκριμένη επικοινωνία (session) και μετά αποστέλλει το πακέτο προς το Ίντερνετ.

Ο ειδικός αυτός πίνακας του δρομολογητή διαθέτει τώρα την αντιστοιχία της ιδιωτικής IP διεύθυνσης του PC και του αριθμού της θύρας TCP που έδωσε ο δρομολογητής.

Στην απάντηση ο web server αποστέλλει το πακέτο στην εξωτερική IP διεύθυνση του δρομολογητή με TCP πόρτα προορισμού , τον αριθμό που είχε ορίσει ο δρομολογητής για το session αυτό.

Ο δρομολογητής ελέγχει την TCP θύρα προορισμού στο εισερχόμενο πακέτο και δρομολογεί αντίστοιχα στο κατάλληλο PC με την εσωτερική του διεύθυνση. Αν ένα δεύτερο PC θέλει μια άλλη σύνδεση με το Ίντερνετ, ο δρομολογητής χορηγεί στα πακέτα του δεύτερου PC μια νέα TCP θύρα , ενώ διατηρεί την ίδια IP διεύθυνση αποστολέα και το στέλνει στο διαδίκτυο, ξεχωρίζοντας τα δύο μηνύματα με τον διαφορετικό αριθμό TCP θύρας.



Εικόνα 21: Παράδειγμα μετατροπής Port Translation

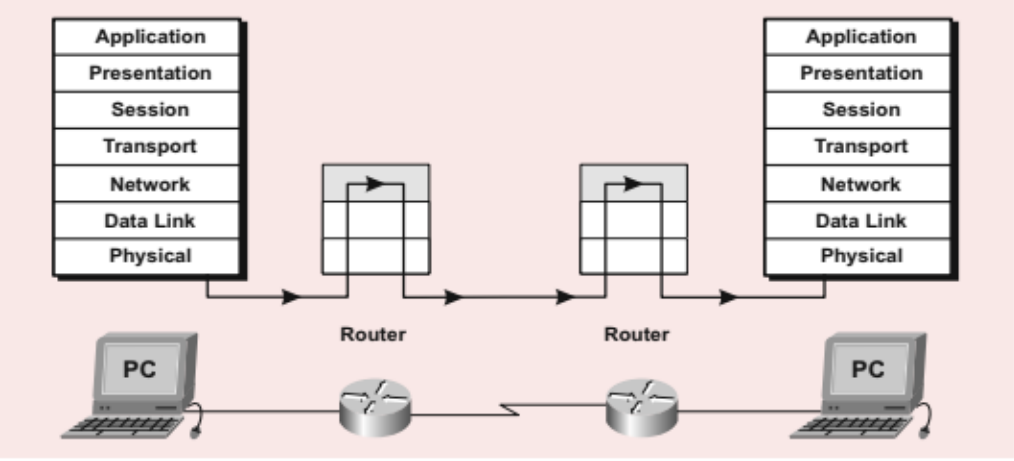
Στον παραπάνω πίνακα παρουσιάζεται ένα παράδειγμα μετατροπής τύπου Port Translation. Ένα PC που ανήκει σε ένα τοπικό δίκτυο με ιδιωτική IP διεύθυνση 192.168.1.5 προσπαθεί να βγει στο Διαδίκτυο μέσω του Δρομολογητή που έχει εσωτερική IP 192.168.1.1 και εξωτερική 210.10.2.1 με σκοπό να προσπελάσει σελίδες σε ένα Εξυπηρετητή Web με εξωτερική IP 221.11.3.1.

ΚΕΦΑΛΑΙΟ 3 Οι Δρομολογητές και τα πρωτόκολλα δρομολόγησης

3.1 Δρομολογητές (Router)

Δρομολογητές (Router) ονομάζονται οι κόμβοι που διακινούν τα IP πακέτα στα δίκτυα υπολογιστών και στα διαδίκτυα . Γνωρίζουμε ότι το IP είναι πρωτόκολλο τρίτου επιπέδου που εξασφαλίζει την επικοινωνία στο Διαδίκτυο και διασυνδέει τους συνδρομητές των δικτύων μεταφέροντας IP πακέτα και προωθώντας τα από κόμβο σε κόμβο, σε connectionless μορφή, δηλαδή χωρίς να είναι επακριβώς προκαθορισμένη η διαδρομή τους μέσω του δικτύου από τον αποστολές ως τον τελικό αποδέκτη. Οι δρομολογητές είναι οι κόμβοι του δικτύου που παραλαμβάνουν και προωθούν τα IP πακέτα προς τον τελικό αποδέκτη, επιλέγοντας τη βέλτιστη ανάμεσα στις δυνατές εναλλακτικές διαδρομές.

Με την ευρύτερη έννοια δρομολογητές είναι οι συσκευές που δρομολογούν πακέτα δεδομένων βασιζόμενοι στη πληροφορία του τρίτου επιπέδου του μοντέλου OSI ή του επιπέδου δικτύου όπως αυτό είναι διαφορετικά γνωστό. Γι' αυτό πρέπει να έχουν τη δυνατότητα να διαβάζουν τις διευθύνσεις τρίτου επιπέδου, άρα να κατανοούν το αντίστοιχο πρωτόκολλο. Στη πράξη οι δρομολογητές εξαρτώνται από το εκάστοτε πρωτόκολλο, αλλά υπάρχουν και δρομολογητές πολλαπλών πρωτοκόλλων που έχουν ευρύτερες δυνατότητες ταυτόχρονης δρομολόγησης πακέτων διαφορετικών πρωτοκόλλων π.χ. IP, IPX (Novell) και AppleTalk.



Εικόνα 22: Η λειτουργία του Δρομολογητή

Θα επικεντρωθούμε στους IP δρομολογητές μιας και το IP ως βάση του Διαδικτύου έχει επικρατήσει των άλλων πρωτοκόλλων του τρίτου επιπέδου κάτι που ισχύει εξίσου και στα ιδιωτικά δίκτυα.

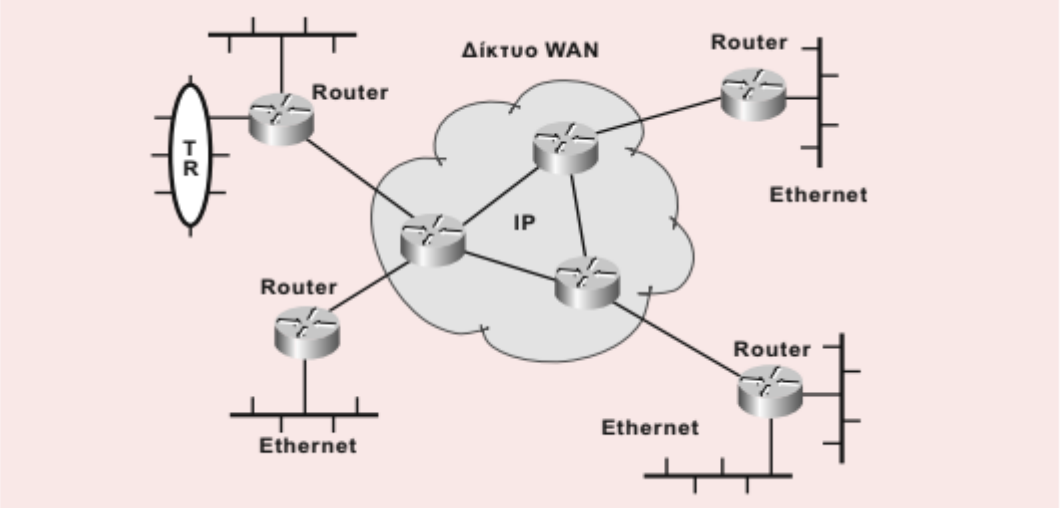
Οι σημαντικότερες λειτουργίες που προσφέρουν οι δρομολογητές είναι:

- Δρομολόγηση σε δικτύωση πλέγματος ή βρόγχου.
- Μείωση όγκου σε ευρεία εκπομπή (broadcast).
- Έλεγχο προσπέλασης
- Διασύνδεση τοπικών δικτύων διαφορετικής τεχνολογίας

Δικτύωση πλέγματος (mesh): Αυτή είναι και η πλέον ενδιαφέρουσα ιδιότητα του δρομολογητή. Προωθεί τα IP πακέτα από δρομολογητή σε δρομολογητή μέσα σε δίκτυα πλέγματος ή βρόγχου (δηλαδή δίκτυα με πολλαπλές συνδέσεις μεταξύ των κόμβων τους) επιλέγοντας τη συντομότερη κάθε φορά διαδρομή ως τον τελικό παραλήπτη. Η επιλογή του δρόμου γίνεται με βάση τη διεύθυνση δικτύου του αποδέκτη, που υπάρχει σε κάθε IP πακέτο και των πινάκων δρομολόγησης που φροντίζουν να διατηρούν οι δρομολογητές στη μνήμη τους. Οι πίνακες αυτοί ενημερώνονται είτε στατικά από τους διαχειριστές των δικτύων είτε δυναμικά από τα πρωτόκολλα δρομολόγησης π.χ. RIP, OSPF κτλ. τα οποία μεταφέρουν συνεχώς πληροφορίες από γειτονικούς δρομολογητές για τα δίκτυα που αυτοί εξυπηρετούν και τη τοπολογία του δικτύου.

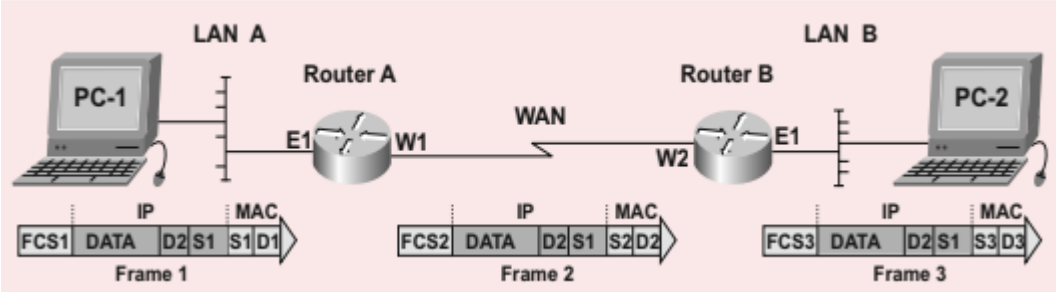
Μείωση όγκου σε ευρεία εκπομπή (broadcast): Η διασύνδεση των τοπικών δικτύων με μεταγωγείς (switches) έχει περιορισμούς στην επεκτασιμότητα που προσφέρει διότι τα Broadcast πακέτα του κάθε σταθμού π.χ. ARP, DHCP κτλ. διαδίδονται σε όλο το τοπικό δίκτυο παρενοχλώντας το σύνολο των σταθμών του Τοπικού Δικτύου (LAN). Διαχωρίζοντας τα τοπικά δίκτυα σε μικρότερα μέσω δρομολογητών περιορίζονται τα broadcast domains και συνεπώς η ενόχληση των σταθμών και η φόρτιση (υπερβολική χρήση) του δικτύου.

Διασύνδεση διαφορετικών τοπικών δικτύων. Παρότι με την επέκταση του Ethernet σπάνια συναντάμε τοπικά δίκτυα άλλης μορφής αυτή είναι μια σημαντική ικανότητα των δρομολογητών που μπορούν να έχουν διάφορα interfaces φυσικής πρόσβασης ώστε να μπορούν να διασυνδέσουν ετερογενή δίκτυα στο χαμηλό επίπεδο ενώ η επικοινωνία των πακέτων γίνεται μέσω του τρίτου επιπέδου. Επίσης έχουν την ικανότητα διασύνδεσης με ποικιλία WAN interface π.χ. ATM, ISDN, PPP, FR, SDH, κτλ.



Εικόνα 23: Βασικές Λειτουργίες των Δρομολογητών

Ας παρακολουθήσουμε ένα IP πακέτο κατά τη πορεία του από τον υπολογιστή PC-1 προς τον υπολογιστή PC-2 που βρίσκονται σε δυο διαφορετικά τοπικά δίκτυα και συνδέονται μέσω δρομολογητή και μιας WAN διασύνδεσης όπως φαίνεται στο παρακάτω σχήμα.



Εικόνα 24: Σύνδεση 2 δικτύων με 2 δρομολογητές

Το PC-1 για να στείλει δεδομένα προς το PC-2 πρέπει να τα τοποθετήσει σε ένα πακέτο IP, να συμπληρώσει τις IP διευθύνσεις αποστολέα και παραλήπτη στη προμετωπίδα του IP πακέτου και στη συνέχεια να το φορτώσει πάνω σε ένα πλαίσιο (Ethernet Frame) για αποστολή. Η τελευταία αυτή ενέργεια είναι η ενθυλάκωση (encapsulation) του πακέτου σε frame 2^{ου} επιπέδου. Οι διευθύνσεις αποστολέα και παραλήπτη του IP πακέτου δεν αλλάζουν σε όλη τη διαδρομή ανεξαρτήτως του πλήθους των δρομολογητών που θα διασχίσει και διατηρούνται αναλλοίωτες μέχρι τον τελικό παραλήπτη.

Ας θεωρήσουμε ότι το PC-1 γνωρίζει αυτές τις IP διευθύνσεις είτε από το διαχειριστή του δικτύου, είτε από την εφαρμογή, είτε μέσα από αυτόματες διαδικασίες DNS, DHCP, RARP που περιγράφονται σε άλλα σημεία.

Το PC-1 για να κατασκευάσει το Ethernet frame που ενθυλακώνει το IP πακέτο, θα πρέπει να τοποθετήσει τις φυσικές (MAC) διευθύνσεις, αποστολές και παραλήπτη, στην προμετωπίδα του frame. Αποστολέας είναι το ίδιο το PC και προφανώς γνωρίζει τη MAC address της θύρας του. Παραλήπτης του πλαισίου είναι η Ethernet θύρα E1 του δρομολογητή A. Το PC-1 είναι πιθανόν να βρει τη MAC διεύθυνση της θύρας E1 του δρομολογητή A, στο πίνακα ARP που διατηρεί στη μνήμη του, αν αυτή έχει καταγραφεί από προηγούμενη επικοινωνία. Αν όμως η διεύθυνση αυτή δεν υπάρχει στη μνήμη, τότε πρέπει να ζητήσει στέλνοντας ένα broadcast μήνυμα ARP request προς το default gateway, Που είναι η IP διεύθυνση της θύρας E1 του δρομολογητή A, ώστε να αναγκάσει το δρομολογητή να απαντήσει επιστρέφοντας τη MAC διεύθυνση της θύρας αυτής.

Έχοντας πλέον το PC-1 όλες τις απαραίτητες διευθύνσεις ολοκληρώνει τη κατασκευή του Ethernet πλαισίου με τελικό βήμα τον υπολογισμό του FCS στο τέλος του frame.

Το ethernet frame είναι δευτέρου επιπέδου και επομένως δεν μπορεί να διασχίσει μεγαλύτερα δίκτυα πέραν του τοπικού δικτύου LAN. Η ζωή του θα ξεκινήσει με τη κατασκευή και την αποστολή του από το PC-1 και θα τερματίσει φθάνοντας στη θύρα E1 του δρομολογητή A.

Ο δρομολογητής A που το παραλαμβάνει θα αφαιρέσει το header και το FCS του Ethernet frame , αφού πρώτα ελέγξει το FCS ώστε να διαπιστώσει ότι το πακέτο δεν έχει σφάλματα από τη μετάδοση στο LAN, και θα κρατήσει το μεταφερόμενο IP πακέτο για να το δρομολογήσει προς τον επόμενο κόμβο ενθυλακώνοντας το όμως σε ένα νέο frame.

Για τη δρομολόγηση ο δρομολογητής A θα βασιστεί στον εσωτερικό πίνακα δρομολόγησης που διατηρεί στη μνήμη του ο οποίος έχει ενημερωθεί είτε στατικά από το διαχειριστή του δικτύου, είτε δυναμικά μέσω πρωτοκόλλων δρομολόγησης π.χ. RIP, OSPF, EIGRP. Στο ενδεχόμενο που ο πίνακας δεν έχει εγγραφή δρομολόγησης για το τελικό IP δίκτυο, τότε το πακέτο θα αποσταλεί προς τη θύρα του δρομολογητή που έχει προκαθοριστεί ως θύρα γενικής δρομολόγησης (default route) δηλαδή, ως θύρα στην οποία αποστέλλονται όλα τα πακέτα για τα οποία δεν υπάρχει άλλη συγκεκριμένη οδηγία στον πίνακα δρομολόγησης. Το default route στους δρομολογητές είναι αντίστοιχο με το default gateway που ορίζεται στα PC για εξωτερική επικοινωνία όπως περιγράφεται πιο κάτω.

Ο δρομολογητής A θα κατασκευάσει ένα νέο Ethernet frame που θα μεταφέρει το IP Πακέτο πάνω στη WAN γραμμή, μέχρι δηλαδή την W2 θύρα του δρομολογητή B. Οι διευθύνσεις αποστολέα και παραλήπτη στο νέο Ethernet frame είναι τα MAC address των θυρών W1 και W2 των δυο δρομολογητών αντίστοιχα, ενώ οι διευθύνσεις του πακέτου IP παραμένουν αναλλοίωτες. Ο δρομολογητής A υπολογίζει ένα νέο FCS που το επισυνάπτει στο τέλος του frame και στέλνει το frame στο δρομολογητή B μέσω της WAN σύνδεσης.

Η ιστορία επαναλαμβάνεται και στο τελικό δρομολογητή B αφού πρώτα ελέγξει μέσω του FCS ότι το frame έφθασε σωστά, απορρίπτει την παλιά προμετωπίδα και το FCS και με τη σειρά του φτιάχνει ένα νέο frame για να ενθυλακώσει το IP πακέτο, ώστε να το μεταφέρει μέσω του LAN B στο τελικό αποδέκτη που είναι το PC-2.

Ο δρομολογητής B διαθέτει και αυτός εσωτερικό πίνακα ARP που έχει αποθηκευμένες τις αντιστοιχίες των IP διευθύνσεων με τις MAC διευθύνσεις των σταθμών του LAN B.

3.1.1 Default Gateway

Γενικά ή έννοια gateway αναφέρεται σε μια συσκευή ή σε μια θύρα μέσω της οποίας εξασφαλίζεται η πρόσβαση σε ένα διαφορετικό δίκτυο. Το default gateway, για τα δίκτυα IP, είναι μια εκ των προτέρων προσδιορισμένη θύρα

προς την οποία μια συσκευή, ένα δίκτυο ή μια εφαρμογή, αποστέλλει τα IP πακέτα όταν δεν προκύπτει από άλλη διαδικασία ποια είναι η κατάλληλη θύρα για τη δρομολόγησή τους. Για παράδειγμα ως default gateway ορίζεται σε κάθε υπολογιστή, ενός εσωτερικού τοπιού δικτύου, η διεύθυνση του δρομολογητή του δικτύου αυτού, ο οποίος εξασφαλίζει τη πρόσβαση των υπολογιστών του δικτύου στο Διαδίκτυο.

Έτσι όταν ένας υπολογιστής θέλει να στείλει IP Πακέτα προς κάποια εξωτερική άγνωστη IP διεύθυνση τότε ανατρέχει στην IP διεύθυνση του default gateway και με τη συνήθη διαδικασία ARP βρίσκει την φυσική διεύθυνση Mac address του προκαθορισμένου default gateway ώστε να φτιάξει τα ethernet frames πάνω στα οποία θα φορτωθούν τα IP πακέτα για να φθάσουν στο default gateway και τελικά μέσω αυτού να δρομολογηθούν προς τον εξωτερικό τελικό αποδέκτη.

Ας σημειωθεί ότι η IP διεύθυνση των προς αποστολή πακέτων είναι πάντα αυτή του τελικού αποδέκτη και όχι του default gateway. Να τονίσουμε ότι η διεύθυνση IP ενός πακέτου δεν αλλάζει αλλά παραμένει πάντα σταθερή καθ' όλη τη πορεία μέσα από διαφορετικά δίκτυα μέχρι να φθάσει στον τελικό αποδέκτη.

3.1.2 Πίνακας δρομολόγησης

Είναι ο ηλεκτρονικός πίνακας που διατηρούν οι δρομολογητές στη μνήμη τους όπου αποθηκεύονται οι διαδρομές (και συχνά πρόσθετα στοιχεία όπως metrics) για συγκεκριμένες διευθύνσεις δικτύων προορισμού. Στη πλειονότητά τους δείχνουν για κάθε τελική διεύθυνση προορισμού, την επόμενη IP διεύθυνση δηλαδή τη διεύθυνση της θύρας του αμέσως επόμενου κόμβου προς την οποία θα πρέπει να σταλούν τα πακέτα ώστε να πορευθούν προς το επιθυμητό τελικό προορισμό.

Στους σύγχρονους δρομολογητές συναντάμε συχνά και τις ορολογίες, πίνακας δρομολόγησης (RIB-Routing Information Base) και πίνακας προώθησης (FIB-Forwarding Information Base). Ο πίνακας προώθησης (FIB) είναι μια απλουστευμένη εκδοχή του πίνακα δρομολόγησης (RIB), που συχνά δημιουργείται επιπροσθέτως και φορτώνεται στη προσωρινή μνήμη (RAM) του δρομολογητή με σκοπό να επιταχύνει τη διαδικασία προώθησης των πακέτων. Για παράδειγμα οι εγγραφές των διευθύνσεων προορισμού της FIB είναι ταξινομημένες έτσι ώστε να ελαχιστοποιείται ο χρόνος αναζήτησης και να επιταχύνεται η επιλογή της θύρας εξόδου προς την οποία ο δρομολογητής πρέπει να προωθήσει το IP πακέτο, για κάθε διεύθυνση προορισμού.

Διακρίνουμε τις εγγραφές στους πίνακες δρομολόγησης σε στατικές και δυναμικές. Οι στατικές εγγραφές εισάγονται από το διαχειριστή του δρομολογητή και δεν αλλάζουν με αλλαγές του δικτύου, αν δεν τις αλλάξει ο ίδιος. Χρησιμοποιούνται σε μικρού μεγέθους δίκτυα με λίγους δρομολογητές.

Χρειάζεται ιδιαίτερη προσοχή με τις στατικές εγγραφές καθώς μπορεί να δημιουργηθούν, εκ λάθους, βρόγχοι δρομολόγησης που απενεργοποιούν όλο το δίκτυο εγκλωβίζοντας τα πακέτα σε κυκλικές διαδρομές.

Οι δυναμικές εγγραφές δημιουργούνται και συντηρούνται αυτόματα από τον ίδιο το δρομολογητή παρακολουθώντας τις αλλαγές του δικτύου. Η συνεχής ενημέρωση των πινάκων γίνεται με τη βοήθεια πληροφοριών, για τη τοπολογία του δικτύου, που συλλέγονται και ανταλλάσσονται μεταξύ των δρομολογητών μέσω των πρωτοκόλλων δρομολόγησης. Επιπλέον οι δρομολογητές έχουν άμεση εσωτερική πληροφόρηση και από τις θύρες τους, για τις διευθύνσεις και τη διαθεσιμότητα των δικτύων που είναι απευθείας συνδεδεμένα σε αυτές.

Στον πίνακα δρομολόγησης καταγράφονται μόνο οι βέλτιστες, από όλες τις προσφερόμενες εναλλακτικές διαδρομές.

Στον παρακάτω πίνακα βλέπουμε ένα τυπικό πίνακα δρομολόγησης.

NETWORK DESTINATION	ADDRESS MASK	NEXT HOP	INTERFACE	METRIC
192.168.1.0	255.255.255.0	--	Eth 0	0
192.168.2.0	255.255.255.0	--	Ser 1	0
194.219.239.108	255.255.255.252	192.168.1.1	Eth 0	1
192.168.3.0	255.255.255.0	192.168.2.2	Ser 1	1
192.168.4.0	255.255.255.0	192.168.1.1	Eth 0	1
0.0.0.0	0.0.0.0	192.168.1.1	Eth 0	1

Εικόνα 25: Παράδειγμα Πίνακα Δρομολόγησης

Το πεδίο Destination μας δείχνει τη διεύθυνση του δικτύου προορισμού, δηλαδή εκεί που πρέπει να φτάσουν τα πακέτα IP. Συνδυάζεται με το επόμενο πεδίο της μάσκας ώστε να διακρίνεται αν πρόκειται για υποδίκτυο (subnet). Η τιμή 0000 της διεύθυνσης ή της μάσκας δηλώνει το default route δηλαδή καλύπτει, σαν μπαλαντέρ, όλες τις υπόλοιπες διευθύνσεις που δεν περιλαμβάνει ο πίνακας, ώστε να γνωρίζει ο δρομολογητής προς τα πού θα δρομολογεί τα αγνώστου παραλήπτη πακέτα.

Το πεδίο **Next hop** δείχνει την IP διεύθυνση της θύρας εισόδου στον επόμενο κόμβο.

Το πεδίο **Interface** δείχνει τη θύρα εξόδου των πακέτων από το δρομολογητή στην πορεία τους προς τον τελικό προορισμό.

Το πεδίο **metric** είναι ένας δείκτης ποιότητας, απόστασης ή κόστους διαδρομής.

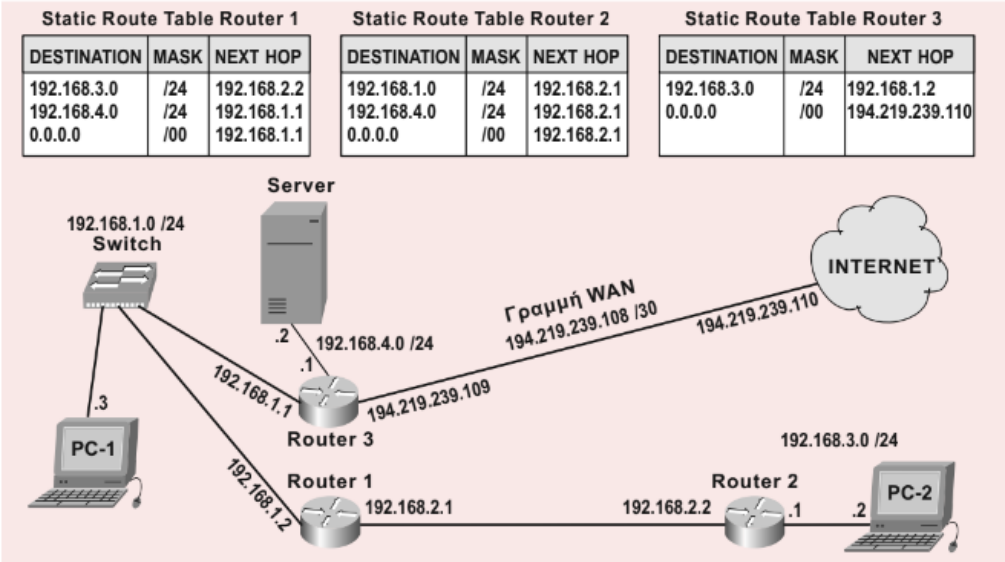
Τα δυο αυτά τελευταία πεδία διαφέρουν στην εμφάνισή τους από κατασκευαστή σε κατασκευαστή.

Στο παράδειγμα του παρακάτω σχήματος, που απεικονίζει ένα μικρό δίκτυο με μια στατική διεύθυνση για πρόσβαση στο Διαδίκτυο, βλέπουμε τις εγγραφές που πρέπει να εισάγουμε στους πίνακες δρομολόγησης των τριών δρομολογητών, ώστε να έχουν επαρκή πληροφορία για να δρομολογούν τη κίνηση προς τα δίκτυα του παραδείγματος.

Επειδή ο κάθε δρομολογητής αναγνωρίζει τα δίκτυα που είναι απ΄ευθείας συνδεδεμένα στις θύρες του, δεν χρειάζεται να κάνουμε εγγραφές για αυτά, τα άμεσα συνδεδεμένα δίκτυα.

Όπως φαίνεται στο σχήμα, ο δρομολογητής R1 για να επικοινωνήσει με το δίκτυο 192.168.3.0/24 (κάτω δεξιά) που δεν είναι απευθείας συνδεδεμένο πάνω του, θα πρέπει να χρησιμοποιήσει σαν επόμενο κόμβο αποστολής των πακέτων το δρομολογητή R2 Και πιο συγκεκριμένα να στείλει τα πακέτα στη θύρα του με διεύθυνση 192.168.2.2 που προσδιορίζεται ως «next hop», επειδή αυτή είναι η κατάλληλη θύρα για να φθάσουμε στον επόμενο κόμβο (R2). Αυτό μας οδηγεί να συμπληρώσουμε τη πρώτη εγγραφή του πίνακα 1.

Επίσης για να επικοινωνήσει ο R1 με τον Server, που είναι στο δίκτυο 192.168.4, θα πρέπει να χρησιμοποιήσει σαν επόμενο κόμβο αποστολής των πακέτων τον R3 και πιο συγκεκριμένα τη θύρα του με διεύθυνση 192.168.1.1, πράγμα που μας δημιουργεί τη δεύτερη εγγραφή.



Εικόνα 26: Παράδειγμα πινάκων στατικής δρομολόγησης

Παρατηρούμε επίσης ότι για να βγει ο R1 στο Διαδίκτυο, θα πρέπει να χρησιμοποιήσει σαν επόμενο κόμβο αποστολής των πακέτων τον R3 και μάλιστα πάλι την ίδια θύρα με διεύθυνση 192.168.1.1.

Αυτό μας οδηγεί στη Τρίτη εγγραφή του πίνακα. Η διεύθυνση 0.0.0.0 εννοεί «οποιαδήποτε διεύθυνση», ενώ η μάσκα /00 εννοεί «οποιαδήποτε μάσκα»,

διότι στο Διαδίκτυο υπάρχουν εκατομμύρια διαφορετικές διευθύνσεις όλων των κλάσεων και δεν θα μπορούσαμε φυσικά να τις γράψουμε όλες σε ένα πίνακα.

Η συγκεντρωτική αυτή εγγραφή ονομάζεται default route και καθοδηγεί το δρομολογητή, για το που πρέπει να στέλνει τα πακέτα εκείνα, για τα οποία δεν υπάρχουν άλλες οδηγίες στον πίνακα δρομολόγησης.

Με τον ίδιο τρόπο συμπληρώνονται οι πίνακες στατικής δρομολόγησης των υπολοίπων δρομολογητών.

3.2 Τα πρωτόκολλα δρομολόγησης (routing protocols)

Όπως γνωρίζουμε οι δρομολογητές καλούνται να επιλέξουν το βέλτιστο δρόμο μέσα σε ένα δίκτυο. Για να το επιτύχουν αυτό πρέπει να γνωρίζουν την τοπολογία του δικτύου και τη κατάσταση των γραμμών. Οι δρομολογητές (router) που λειτουργούν ως τροχονόμοι των πακέτων στο δίκτυο, χτίζουν εσωτερικούς πίνακες δρομολόγησης βασιζόμενοι στα στοιχεία της τοπολογίας του δικτύου που έχουν συλλέξει και βάσει των πινάκων αυτών επιλέγουν τη βέλτιστη διαδρομή.

Για τη συλλογή των πληροφοριών της τοπολογίας, οι δρομολογητής εκπέμπουν ειδικά πακέτα προς τους υπόλοιπους δρομολογητής του δικτύου ερευνώντας τις δυνατές διαδρομές διασύνδεσης, ενημερώνοντάς τους για την παρουσία τους και τα δίκτυα που εξυπηρετούν. Οι λειτουργίες αυτές γίνονται με τα πρωτόκολλα δρομολόγησης.

Υπάρχουν δυο τύποι πρωτοκόλλων δρομολόγησης, τα εσωτερικά και τα εξωτερικά. **Εσωτερικά πρωτόκολλα** ονομάζουμε αυτά που λειτουργούν εντός ενός αυτόνομου συστήματος και τα συναντάμε ως **Interior Gateway Protocols**.

Αυτόνομο σύστημα ονομάζουμε ένα ευρύτερο, ενιαίο και ομοιόμορφο από πλευράς δρομολόγησης και διευθυνσιοδότησης IP περιβάλλον, με κοινή διαχείριση. Τυπικό παράδειγμα αυτόνομου συστήματος είναι το δίκτυο ενός ISP (Internet Service Provider).

Εξωτερικά ονομάζουμε τα πρωτόκολλα που λειτουργούν μεταξύ διαφορετικών αυτόνομων συστημάτων και τα συναντάμε ως **Exterior Gateway Protocols,** που ως σκοπό έχουν να ανταλλάσσονται πληροφορίες δρομολόγησης μεγάλης κλίμακας όχι μόνο μεταξύ δρομολογητής, αλλά μεταξύ διαφορετικών αυτόνομων συστημάτων.

Βασικοί εκπρόσωποι των εσωτερικών πρωτοκόλλων είναι τα RIP, OSPF, IGRP, EIGRP,IS-IS και εξωτερικών τα BGP και EGP.

Για το εσωτερικά πρωτόκολλα χρησιμοποιούνται δυο βασικοί αλγόριθμοι επιλογής βέλτιστου δρόμου, που είναι οι **Distance Vector** και **Link State**.

3.2.1 Distance Vector

Ο αλγόριθμος Distance Vector (ή Bellman-Ford) υπολογίζει τον βέλτιστο δρόμο, στηριζόμενος στον ελάχιστο αριθμό των hops μεταξύ δυο δρομολογητής, ανεξάρτητα από τα φορτία κίνησης που υπάρχουν. Οι δρομολογητής αυτού του τύπου ανανεώνουν την εικόνα του δικτύου, επικοινωνώντας περιοδικά με τους γειτονικούς δρομολογητής και ανταλλάσσοντας τους πίνακες δρομολόγησης. Την τεχνική χρησιμοποιούν τα πρωτόκολλα RIP (Routing Information Protocol) και το IGRP (Interior Gateway Routing Protocol) της Cisco. Πλεονέκτημά τους η απλότητα εφαρμογής τους και μειονέκτημα οι φτωχές επιδόσεις και τα μειωμένα χαρακτηριστικά.

Καταρχήν με τη τεχνική Distance Vector πρέπει να αποδοθεί μια γραμμή, ένα κόστος (που έχει σχέση με τη ταχύτητα, delay, ποιότητα κτλ) σε όλες τις point to point ζεύξεις μεταξύ των δρομολογητών του δικτύου. Αυτό βοηθά καθώς για την επικοινωνία δυο μακρινών δρομολογητών, θα επιλεγεί από τον αλγόριθμο η διαδρομή, που αθροιστικά οι ζεύξεις εμφανίζουν το χαμηλότερο κόστος. Αν όλες οι γραμμές είναι ισοδύναμες και έχουν το ίδιο κόστος, τότε ο αλγόριθμος πρακτικά επιλέγει τη διαδρομή με τα λιγότερα άλματα (hops).

Η λειτουργία του αλγορίθμου είναι απλή. Ο κάθε router στην αρχή ξέρει μόνο τα συνδεδεμένα απευθείας στις θύρες του δίκτυα, και τους άμεσα συνδεδεμένους γειτονικούς router με το κόστος των ζεύξεων αυτών. Αυτό αποτελεί τον αρχικό route table του κάθε router. Στη συνέχεια κάθε router σε περιοδικά διαστήματα (πχ 30 sec) στέλνει στους γείτονές του τον πίνακα αυτό. Οι γείτονες συγκρίνουν τη λαμβανόμενη πληροφορία με αυτή που έχουν στο δικό τους πίνακα, συμπληρώνουν ότι αυτοί δεν έχουν και αντικαθιστούν ότι αποτελεί βελτίωση σε ότι ήδη έχουν π.χ. πρόσβαση σε ένα δίκτυο με χαμηλότερο «κόστος». Το νέο βελτιωμένο πίνακα που προκύπτει τον ξαναστέλνουν πάλι στους γείτονες στον επόμενο χρονικό κύκλο. Έτσι με τη πάροδο του χρόνου, όλοι οι κόμβοι του δικτύου επιλέγουν τις βέλτιστες διαδρομές.

3.2.2 Link State

Ο link state είναι στην ουσία η καλύτερη μέθοδος δρομολόγησης με πολλά χρήσιμα χαρακτηριστικά, που επιπλέον λαμβάνει υπόψη της εκτός από τον αριθμό των hops και πρόσθετες παραμέτρους, όπως η ταχύτητα της γραμμής, η ποιότητά της, η καθυστέρηση λόγω κίνησης και η τυχόν προτεραιότητα μετάδοσης.

Λειτουργία : Για την εφαρμογή των αλγορίθμων Link State κάθε router κατασκευάζει ένα πίνακα συνδεσιμότητας, δηλαδή ένα χάρτη με τη μορφή ενός γράφου, που δείχνει ποιοι δρομολογητές είναι συνδεδεμένοι με ποιους, ώστε να έχει τη πλήρη εικόνα του δικτύου. Για να επιτευχθεί κάτι τέτοιο, κάθε δρομολογητής αρχικά στέλνει σε όλους τους άλλους τις πληροφορίες σχετικά με τις συνδέσεις του, δηλαδή με ποιους άλλους δρομολογητές και με ποια

δίκτυα συνδέεται. Με τη λήψη όλων αυτών των στοιχείων κάθε δρομολογητής ανεξάρτητα δημιουργεί το δικό του χάρτη όλου του δικτύου. Στη συνέχεια ο κάθε κόμβος με τη χρήση του συνολικού χάρτη και εφαρμόζοντας ένα κοινό αλγόριθμο ελάχιστης διαδρομής όπως τον αλγόριθμο του Dijkstra υπολογίζει την ελαχίστου κόστους διαδρομή από τον εαυτό του προς κάθε άλλο κόμβο του δικτύου.

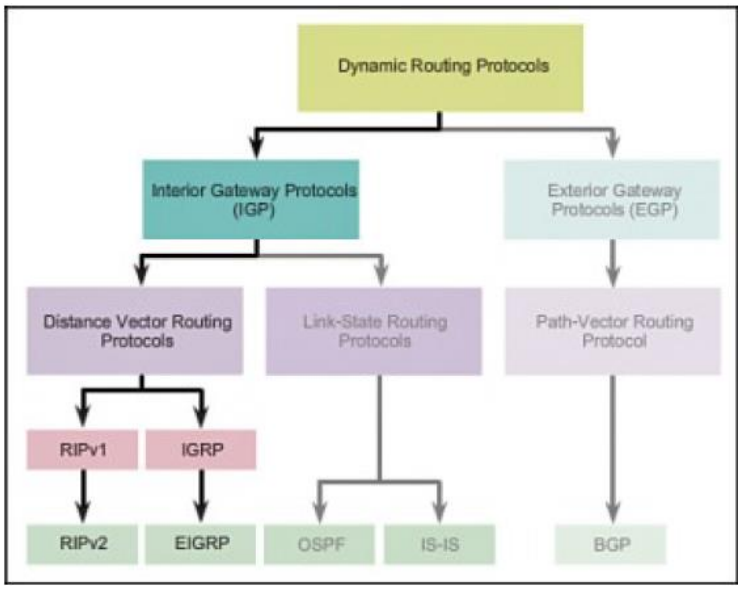
Το αποτέλεσμα για το δρομολογητή μοιάζει με δένδρο, που ξεκινάει από τον ίδιο το δρομολογητή ενώ οι κλάδοι του απλώνονται σε όλους τους άλλους δρομολογητές του δικτύου, με τρόπο ώστε οι διαδρομές να είναι οι βέλτιστες και από πλευράς «κόστους».

Το δένδρο αυτό επιτρέπει στο δρομολογητή να φτιάξει το πίνακα δρομολόγησης αφού του δείχνει ξεκάθαρα το next hop του κάθε κλάδου προς οποιοδήποτε τελικό προορισμό.

Η συλλογή των βέλτιστων αυτών κατευθύνσεων προς τα εξυπηρετούμενα δίκτυα αποτελεί το πίνακα δρομολόγησης. Στη συνέχεια δεν ανταλλάσσονται μεταξύ των δρομολογητών πίνακες δρομολόγησης , παρά μόνο πληροφορίες σχετικά με αλλαγές στις συνδέσεις πχ διακοπές ή αποκαταστάσεις γραμμών.

Τα πρωτόκολλα OSPF και IS-IS βασίζονται στη τεχνική αυτή. Πλεονέκτημα των Link State πρωτοκόλλων στη πράξη είναι τα πλούσια χαρακτηριστικά και οι αυξημένες δυνατότητες και επιδόσεις τους, όπως η ταχεία σύγκλιση σε περιπτώσεις διακοπής γραμμών, ενώ μειονέκτημα είναι η αυξημένη πολυπλοκότητα και η εμπειρία που απαιτείται για το προγραμματισμό τους.

Επιπλέον υπάρχουν και τα υβριδικά(μικτά) πρωτόκολλα που προσπαθούν να συνδυάσουν τα πλεονεκτήματα των δυο κατηγοριών δηλαδή της απλότητας των Distance Vector και των δυνατών χαρακτηριστικών Link State. Στη κατηγορία αυτή ανήκει το EIGRP (Enchanced IGRP) που είναι ιδιωτικό (proprietary) της εταιρίας Cisco.



Εικόνα 27: Πρωτόκολλα Δυναμικής Δρομολόγησης

3.2.3 RIP (Routing Information Protocol)

Το RIP είναι ένα εσωτερικό πρωτόκολλο που στηρίζεται στη τεχνική distance vector επιτρέποντας σε ένα Δρομολογητή να ενημερώσει τους υπόλοιπους δρομολογητές του δικτύου για το ποια δίκτυα μπορεί να προσπελάσει και σε ποια απόσταση βρίσκονται από αυτόν.

Οι πίνακες δρομολόγησης των δρομολογητών ως προς το πρωτόκολλο RIP, περιέχουν εγγραφές που η κάθε μια περιλαμβάνει ένα ζεύγος τιμών που είναι μια διεύθυνση IP και ένας απαριθμητής (metric) ο οποίος καθορίζει την απόσταση σε hops προς το συγκεκριμένο προορισμό.

Για να υπολογιστεί η απόσταση μεταξύ αποστολέα και παραλήπτη, ώστε να επιλεγεί η βέλτιστη διαδρομή, χρησιμοποιείται σαν μέτρο ο αριθμός των συνδέσεων (hops) μεταξύ των δρομολογητών από τις οποίες περνά η πληροφορία μέχρι να καταλήξει στον αποδέκτη. Ο μέγιστος αριθμός hops εδώ είναι το 15 που αποτελεί και ένα σημαντικό περιορισμό του πρωτοκόλλου. Όταν ο απαριθμητής των Hops πάρει τη τιμή 16 τότε ο προορισμός θεωρείται απροσπέλαστος.

Με το πρωτόκολλο αυτό οι δρομολογητές κάθε 30'' ανταλλάσσουν τις πληροφορίες των πινάκων δρομολόγησης ακόμα και όταν δεν υπάρχουν αλλαγές αποστέλλοντας ένα ειδικό πακέτο.

Όταν ένας δρομολογητής λάβει ένα πακέτο RIP με κάποια αλλαγή, τότε τροποποιεί την εγγραφή του πίνακα δρομολόγησής του, μόνο εφόσον η τιμή του απαριθμητή των Hops του πακέτου RIP είναι μικρότερη από αυτήν που ήδη υπάρχει στον πίνακα.

Υπάρχουν δυο χρονιστές που σχετίζονται με το RIP. Ο πρώτος ονομάζεται timeout timer και έχει τιμή 180 δευτερολέπτων, προσδιορίζει δε πόσο χρόνο διατηρεί ένας δρομολογητής μια εγγραφή στο πίνακα δρομολόγησής του πριν τη θεωρήσει απροσπέλαστη, αν δεν λάβει εν τω μεταξύ μια ανανέωση της εγγραφής αυτής μέσω του πακέτου RIP. Ο χρονιστής αυτός ξεκινά κάθε φορά που δημιουργείται μια εγγραφή ή που φθάνει μια ανανέωσή της. Ο δεύτερος χρονιστής ονομάζεται garbage collection timer και ενεργοποιείται μετά το πέρας των 180 δευτερολέπτων του timeout. Με την εκπνοή του χρονιστή αυτού που έχει τιμή 120 δευτερολέπτων, η συγκεκριμένη εγγραφή του πίνακα διαγράφεται.

Όταν ένας δρομολογητής λαμβάνει ένα πακέτο RIP το στέλνει στη συνέχεια προς όλες τις άλλες κατευθύνσεις αυξάνοντας τον απαριθμητή των Hop καταά 1 συμπεριλαμβάνοντας και τον εαυτό του.

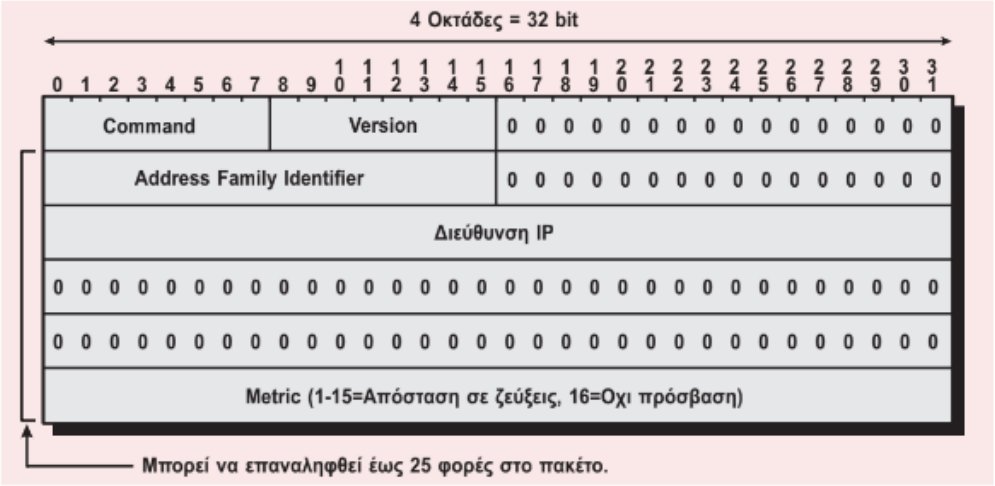
Τα πακέτα του RIP μεταδίδονται πάνω από UDP πρωτόκολλο στη πόρτα 520 (208H) με ip διεύθυνση 255.255.255.255 και MAC FF-FF-FF-FF-FF-FF, δηλαδή είναι broadcast κίνηση που επηρεάζει κάθε συνδεδεμένο σταθμό στο δίκτυο.

Στο RIP οι σταθμοί διακρίνονται σε δυο κατηγορίες, σε ενεργούς και παθητικούς. Σαν ενεργοί χαρακτηρίζονται αυτοί που εκπέμπουν το πακέτο με

τα στοιχεία δρομολόγησης, ενώ παθητικοί είναι αυτοί που λαμβάνουν τέτοια πακέτα. Ενεργοί είναι συνήθως οι δρομολογητές και παθητικοί οι υπολογιστές.

Το RIP έχει σχεδιαστεί για διασύνδεση LAN και θεωρείται ότι έχει κακή εκμετάλλευση γραμμής λόγω των συνεχών εκπομπών ενημερωτικών πακέτων. Παρόλα αυτά είναι πολύ διαδεδομένο, λόγω της απλότητάς του και της αποδοχής από τους χρήστες του TCP/IP.

Το πακέτο του RIP αποτελείται από τα παρακάτω πεδία:



Εικόνα 28: Το πακέτο του RIP

Command που με τιμή 1 προσδιορίζει πακέτο απαίτησης για αποστολή πληροφοριών του πίνακα δρομολόγησης, ενώ με τη τιμή 2 πακέτο απάντησης που περιέχει τα ζητούμενα στοιχεία.

Version, των 8 bit, που προσδιορίζει τον αριθμό έκδοσης του RIP.

Address Family Identifier των 16 bit που έχει τιμή 2 για πρωτόκολλο IP.

IP Address όπου καταγράφεται η διεύθυνση προορισμού του IP.

Metric, που παίρνει τιμές από 1 ως και 15 και καταγράφει τον αριθμό των Hops. Αν το πεδίο έχει τη τιμή 16, σημαίνει ότι δεν υπάρχει δρόμος σύνδεσης με την επιθυμητή διεύθυνση. Σημειώνεται επίσης ότι μπορούν να υπάρχουν το πολύ ως 25 ζεύγη εγγραφών (IP διεύθυνση - Metric) σε κάθε πακέτο RIP.

RIP Version 2

Οι διάφορες αδυναμίες του RIP οδήγησαν στην ανάπτυξη μιας βελτιωμένης έκδοσης της RIPv2 που τυποποιήθηκε τελικά το 1998 με το RFC2453. Έγινε προσπάθεια να διατηρηθεί συμβατότητα με τη προηγούμενη έκδοση και οι σημαντικότερες διαφορές είναι:

1. Υποστηρίζει μάσκες διευθυνσιοδότησης IP με μεταβλητό μήκος (VLSM Variable Length Subnet Mask). Στην έκδοση 1 δεν μεταφέρονται μάσκες έτσι αν χρειαζόταν να γίνει υποδικτύωση στο δίκτυο θα έπρεπε να συμφωνηθεί σταθερή μάσκα για όλα τα σημεία του δικτύου. Η δεύτερη έκδοση RIPv2 συναντάται και ως classless RIP σε σχέση με τον όρο classful για τη RIPv1.
2. Η αποστολή των πινάκων δρομολόγησης στους γειτονικούς δρομολογητές με broadcast που δημιουργούσε μεγάλες επιβαρύνσεις στα δίκτυα και στους σταθμούς που δεν συμμετέχουν στη δρομολόγηση, αντικαταστάθηκε με

αποστολή multicast στην IP διεύθυνση 224.0.0.9 στην οποία γίνονται συνδρομητές μόνο οι κόμβοι του δικτύου ώστε να λαμβάνουν τις ενημερώσεις.

3. Χρησιμοποιείται η διαδικασία επιβεβαίωσης ταυτότητας (MD5 - authentication) για τους δρομολογητές που συμμετέχουν στο RIP domain, ώστε να μη δέχεται το δίκτυο μη πιστοποιημένα updates και έτσι να διασφαλίζεται από τυχόν κακόβουλες επιθέσεις.

Ο περιορισμός του μέγιστου πλήθους των hops σε 15 παρέμεινε και στη δεύτερη έκδοση για λόγους συμβατότητας με την παλιά.

3.2.4 OSPF (Open Shortest Path First)

Το OSPF είναι ένα εσωτερικό πρωτόκολλο αρκετά πολυπλοκότερο του RIP, που χρησιμοποιεί τη τεχνική Link State. Πλεονέκτημα αυτής της τεχνικής έναντι της distance vector, είναι η δυνατότητα χρήσης ιεραρχικής τοπολογίας, η γρήγορη ανταπόκριση σε αλλαγές του δικτύου, η χρήση της σε μεγάλα δίκτυα, η εξισορρόπηση του φορτίου μεταξύ εναλλακτικών βέλτιστων διαδρομών κλπ. Το OSPF περιγράφεται αναλυτικά στο RFC 1583.

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

Ενώ το RIP βασίζεται σε σχετικές πληροφορίες δρομολόγησης, το OSPF βοηθά τους δρομολογητές να σχηματίσουν μόνοι τους μια πλήρη εικόνα του δικτύου και να υπολογίζουν σαφώς τη βέλτιστη διαδρομή βασιζόμενο σε ένα αλγόριθμο που ονομάζεται Dijkstra.

Αυτό έχει σαν αποτέλεσμα την ταχύτατη αναδρομολόγηση μεταξύ εναλλακτικών διαδρομών σε περιπτώσεις προβλημάτων του δικτύου.

Το OSPF πλεονεκτεί επίσης για το ότι αποστέλλει ενημερωτικά πακέτα μόνο για τις τυχόν αλλαγές της κατάστασης των συνδέσεων εφόσον υπάρχουν, σε αντίθεση με το RIP που στέλνει ενημερωτικά πακέτα κάθε 30 δευτερόλεπτα έστω και αν το δίκτυο λειτουργεί κανονικά και χωρίς αλλαγές.

Το πακέτο OSPF

Τα πακέτα OSPF μεταφέρονται μέσω του IP πρωτοκόλλου και είναι πέντε διαφορετικών τύπων:

Hello. Τα πακέτα hello μεταφέρουν πληροφορίες σχετικά με γειτονικούς δρομολογητές.

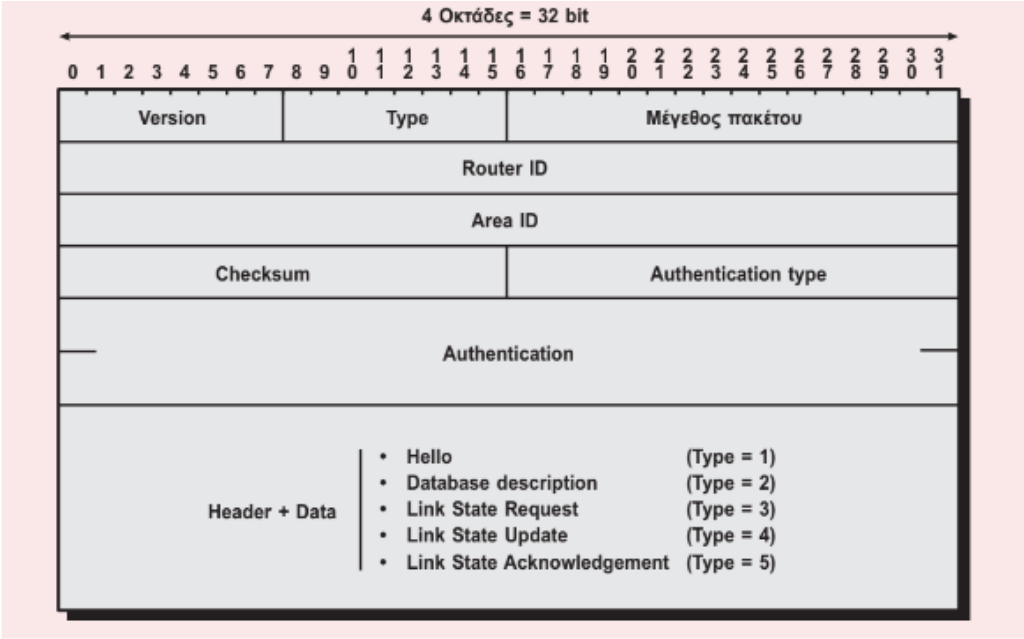
Περιγραφή βάσης δεδομένων, Το πακέτο της περιγραφής της βάσης δεδομένων μεταφέρει πληροφορίες που απαιτούνται για να ενημερώσουν τις βάσεις τοπολογικών δεδομένων σε γειτονικές συσκευές.

Link State Request.

Link State Update. Τα link state request ζητούν πληροφορίες τοπολογίας από γειτονικούς δρομολογητές.

Link State Ack. Τα Link state ack επιβεβαιώνουν την παραλαβή πληροφοριών τοπολογίας.

Το **πακέτο OSPF** που φαίνεται στο παρακάτω σχήμα αποτελείται από τα παρακάτω πεδία:



Εικόνα 29: Το πακέτο του OSPF

Version, για τον αριθμό έκδοσης του πρωτοκόλλου

Type, όπου περιγράφεται ο τύπος του πρωτοκόλλου

Length, των 2 Byte, όπου περιέχεται το μήκος του πακέτου συμπεριλαμβανομένου και του header.

Router ID, που περιγράφει τον αποστολέα του πακέτου

Area ID, για τη διεύθυνση της περιοχής που βρίσκεται ο αποστολέας. Περιοχή (OSPF area) ονομάζεται ομάδα δικτύων, Η/Υ και δρομολογητή.

Checksum, των 2 byte για την αναγνώριση σφαλμάτων του header.

Authentication type και πεδίο **Authentication** που χρησιμοποιούνται για την επικύρωση του πακέτου.

Λειτουργία OSPF

Τα βασικά βήματα που ακολουθεί ένας OSPF δρομολογητής είναι:

- Εντοπισμός των γειτονικών δρομολογητών
- Επιλογή του designated δρομολογητή.

- Δημιουργία σχέσεων επικοινωνίας με τους γειτονικούς δρομολογητές.
- Συγχρονισμός των βάσεων δεδομένων.
- Επεξεργασία του πίνακα δρομολόγησης
- Δημοσίευση των καταστάσεων των γραμμών προς το υπόλοιπο δίκτυο.

Οι δρομολογητές εκτελούν τις παραπάνω ενέργειες κάθε φορά που ξεκινούν τη λειτουργία τους ή όταν συμβαίνει κάποια αλλαγή στο δίκτυο.

1. Ο εντοπισμός των γειτονικών δρομολογητών γίνεται συστηματικά με τη χρήση των πακέτων Hello τα οποία επιβεβαιώνουν και τη δυνατότητα επικοινωνίας μεταξύ των γειτονικών δρομολογητών. Τα πακέτα hello μεταφέρουν εκτός των άλλων και πληροφορίες όπως τη μάσκα των IP διευθύνσεων των Interfaces, τις IP διευθύνσεις του designated και του backup designated δρομολογητή όπως θα δούμε στη συνέχεια, καθώς και τις διευθύνσεις των γειτονικών δρομολογητών που έχουν εντοπιστεί από πακέτα hello στα άλλα interfaces του δρομολογητή.
2. Ο προσδιορισμός του designated και του backup designated δρομολογητή γίνεται μετά από ανάλυση των στοιχείων που έχουν συλλεχθεί από τα πακέτα hello. Η διαδικασία επιλογής είναι κάπως πολύπλοκη και βασίζεται στην υποψηφιότητα και την προτεραιότητα των δρομολογητών. Κάθε δίκτυο OSFP έχει ένα designated δρομολογητή και έναν backup designated δρομολογητή.

   Ο designated δρομολογητής έχει αρμοδιότητα να δημιουργεί την εκπομπή πακέτων για τη κατάσταση των γραμμών ώστε να ενημερώνει όλους τους δρομολογητές σε όλα τα δίκτυα μιας περιοχής OSFP.
   Ο designated δρομολογητής και ο backup designated δρομολογητής δημιουργούν για το σκοπό αυτό σχέσεις γειτονίας με τους υπόλοιπους δρομολογητές. Ο backup designated δρομολογητής είναι έτοιμος να αναλάβει τις λειτουργίες του designated δρομολογητή σε περίπτωση αστοχίας του τελευταίου.
3. Εκτός από τις σχέσεις γειτονίας που προαναφέραμε μεταξύ όλων των δρομολογητών με τους designated και backup designated δρομολογητές, δημιουργούνται σχέσεις γειτονίας μεταξύ δρομολογητών και όταν αυτοί συνδέονται με point to point συνδέσεις. Οι σχέσεις γειτονίας αποκαθίστανται με χρήση πακέτων περιγραφής βάσης δεδομένων τα οποία περιέχουν μια περίληψη της κατάστασης της κάθε σύνδεσης.
4. Ο συγχρονισμός των βάσεων δεδομένων επιτυγχάνεται με τη χρήση πακέτων link state request και link state update. Στη πράξη το link state update είναι η απάντηση στο πακέτο link state request και περιέχει τις πληροφορίες της βάσης δεδομένων που απαιτήθηκαν. Όταν όλα τα πακέτα request έχουν απαντηθεί οι βάσεις δεδομένων όλων των δρομολογητών είναι ταυτόσημες και λέμε ότι οι δρομολογητές είναι συγχρονισμένοι.
5. Η δημιουργία του πίνακα δρομολόγησης σε ένα δρομολογητή γίνεται με την επεξεργασία της βάσης δεδομένων, που περιγράφει τη κατάσταση των συνδέσεων, με τη χρήση SPF αλγορίθμου. Ο πίνακας δρομολόγησης δημιουργείται κάθε φορά από την αρχή χωρίς να γίνονται προσθήκκες ή

αφαιρέσεις από τον υπάρχοντα. Σε περίπτωση που ο αλγόριθμος για δυο διαφορετικούς δρόμους εμφανίσει το ίδιο κόστος, το OSPF μπορεί να κατανέμει το φορτίο ομοιόμορφα μεταξύ τους.

6. Κάθε δρομολογητής στο OSPF εκπέμπει περιοδικά την κατάσταση των συνδέσεών του. Ετσι η απουσία τέτοιας εκπομπής για κάποιο χρονικό διάστημα ανιχνεύεται από τους γείτονες και τότε ο συγκεκριμένος δρομολογητής θεωρείται εκτός επικοινωνίας.

3.2.5 Σύγκριση RIP vs OSPF

Οι RIP δρομολογητές μαζεύουν μεγάλο ποσό άχρηστης πληροφορίας και δημιουργούνται λανθασμένες δρομολογήσεις λόγω της μεγάλης καθυστέρησης σύγκλισης. 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 και για μεγάλα δίκτυα ή δίκτυα που αλλάζουν αρκετά γρήγορα και συχνά 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.

Οι OSPF δρομολογητές έχουν καλύτερη - γρηγορότερη σύγκλιση, διότι οι αλλαγές προωθούνται άμεσα και όχι περιοδικά. Οι ενημερώσεις στέλνονται μόνο σε περίπτωση αλλαγής και γίνονται με ip multicast μετάδοση.

Οι αποφάσεις δρομολόγησης λαμβάνονται με βάση το κόστος των συνδέσεων και έτσι προτιμάται η αληθινά βέλτιστη διαδρομή.

Το αντίτιμο που πληρώνουμε για τις περισσότερες δυνατότητες του πρωτοκόλλου είναι η πολυπλοκότητα στην ρύθμιση και στην άρση βλαβών.

Επίσης απαιτείται περισσότερη επεξεργαστική ισχύς και μνήμη στους δρομολογητές.

Features	RIP		OSPF
	Version 1	Version 2	
Algorithm	Bellman-Ford		Dijkstra
Path Selection	Hop based		Shortest Path
Routing	Classful	Classless	Classless
Transmission	Broadcast	Multicast	Multicast
Administrative Distance	120		*110*
Hop Count Limitation	15		No Limitation
Authentication	No	MD5	MD5
Protocol	UDP		IP
Convergence Time	RIP>OSPF		

Εικόνα 30: Σύγκριση πρωτοκόλλων RIP και OSPF

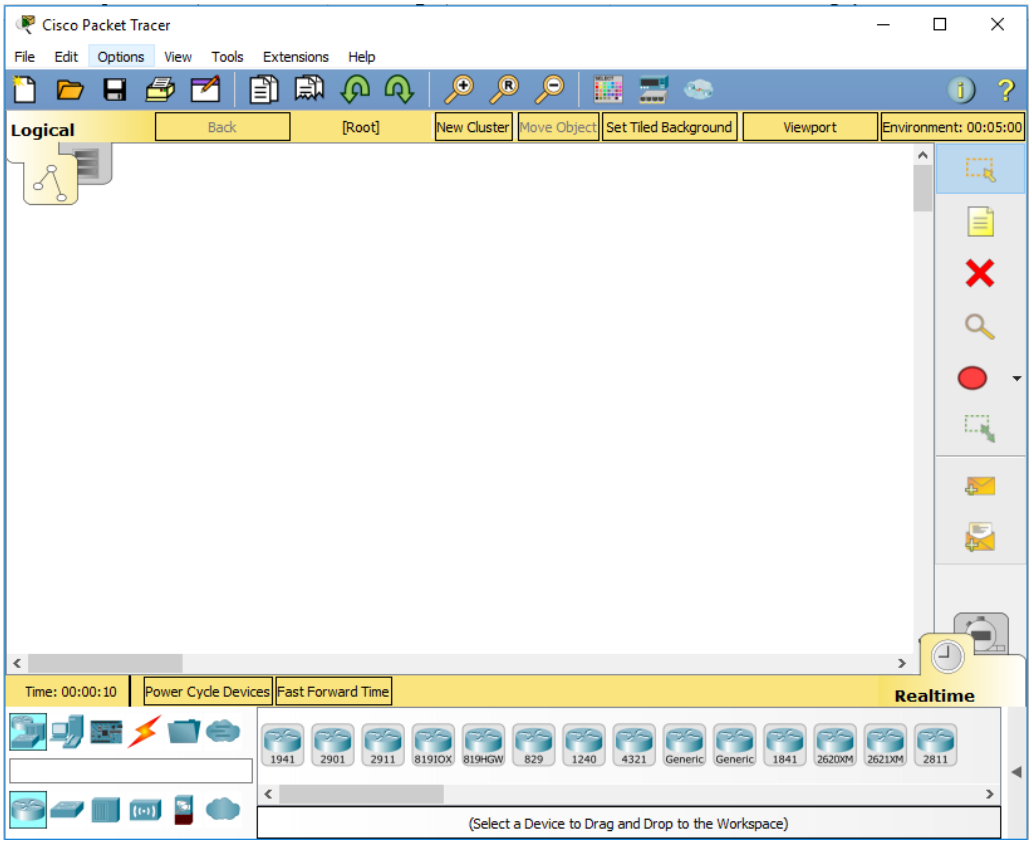
ΚΕΦΑΛΑΙΟ 4

ΥΛΟΠΟΙΗΣΗ ΜΑΘΗΜΑΤΩΝ ΣΤΗΝ ΕΦΑΡΜΟΓΗ PACKET TRACER

Σε αυτό το κεφάλαιο θα παρουσιαστεί ο σχεδιασμός και η ανάπτυξη του περιβάλλοντος για την υποστήριξη δικτυακών πειραμάτων καθώς επίσης και όλα τα εργαλεία και μέσα που χρησιμοποιήθηκαν κατά την πορεία ανάπτυξης της. Επίσης θα γίνει πλήρης παρουσίαση του περιβάλλοντος και των λειτουργιών που υποστηρίζει.

4.1 Ανάλυση του εργαλείου Cisco Packet Tracer

Το Cisco Packet Tracer είναι ένα πρόγραμμα προσομοίωσης δικτύων που έχει δημιουργηθεί από την εταιρία Cisco. Το εργαλείο αυτό επιτρέπει στους χρήστες να σχεδιάζουν οποιαδήποτε τοπικά δίκτυα ή δίκτυα WAN και Cloud από το μηδέν. Η δημιουργία δικτυακών τοπολογιών, η επιλογή από μία πληθώρα συσκευών όπως υπολογιστές, laptops, tablets, δρομολογητές, μεταγωγείς, εξυπηρετητές και συνδέσεις με διαφορετικά είδη καλωδίων, δημιουργούν την αίσθηση ενός πραγματικού περιβάλλοντος δικτύωσης. Το γραφικό περιβάλλον του το καθιστά εύκολο στη χρήση ενώ η προσομοίωση γίνεται σε πραγματικές συσκευές με πραγματικές συνθήκες.



Εικόνα 31 : Το περιβάλλον του Packet Tracer

Το Cisco Packet Tracer είναι διαθέσιμο για λειτουργικά Windows και Linux, αλλά και για κινητά τηλέφωνα. Για να κατεβάσει κανείς τον προσομοιωτή της Cisco χρειάζεται να κάνεις εγγραφή στο Cisco Networking Academy. Το CPT διαθέτει μια σειρά από προσομοιωμένα πρωτόκολλα στρώματος εφαρμογής, όπως HTTP και DNS, καθώς και βασικά πρωτόκολλα δρομολόγησης με RIP, OSPF και EIGRP.

Το γραφικό περιβάλλον του CPT είναι πολύ πρακτικό και πολύ εύκολο στη χρήση. Παρέχει ρεαλισμό στην προσομοίωση, καθώς προσομοιώνει πραγματικές συσκευές σε πραγματικές συνθήκες. Εκτός από το γραφικό περιβάλλον, υπάρχει επίσης και την Command List (CLI), η οποία επιτρέπει τον προγραμματισμό των δικτυακών συσκευών.

Το Cisco Packet Tracer 6.3 έχει κυκλοφορήσει στις 22 Δεκεμβρίου το 2015 από τη Cisco. Πρόκειται για μια έκδοση συντήρησης με netacad login ενεργοποιημένη κατά την εκκίνηση της εφαρμογής. Αντικατέστησε το Cisco Packet Tracer 6.2 Φοιτητών και Cisco Packet Tracer 6.2 Instructor. Το Cisco Packet Tracer 6.2 περιλαμβάνει ASA 5505 τείχους προστασίας με τη διαμόρφωση της γραμμής εντολών. Περιλαμβάνει επίσης ένα NetFlow συλλέκτη ως Desktop εφαρμογή στη συσκευή διακομιστή, πρωτόκολλα δρομολόγησης για το IPv6 (OSPFv3, EIGRPv6, RIPng), DHCP snooping εντολές, το IPv6 CEF, IPSEC.

Το Packet Tracer 6.2 εισήγαγε την υποστήριξη τηλεφωνίας 3G / 4G, καθώς και ένα νέο Cisco 819 ISR δρομολογητής με ενσωματωμένο ασύρματο σημείο πρόσβασης. Σε αυτήν την έκδοση προστέθηκαν επίσης και οι βελτιώσεις OSPF και EIGRP. Το Packet Tracer 7.0 έχει κυκλοφορήσει στις 17 Ιουνίου 2016. Αυτή είναι μια νέα σημαντική έκδοση που περιλαμβάνει 3 νέους δρομολογητές Cisco (819IOX, 829, 1240 routers), ένα νέο IE2000 διακόπτη industral και τεράστια βελτιωμένα πρωτόκολλα. Ακόμη έχουν προστεθεί οι δυνατότητες Python και javascript scripting.

Παλαιότερα μόνο οι σπουδαστές των προγραμμάτων CCNA Academy μπορούσαν να έχουν δωρεάν λήψη του εργαλείου για εκπαιδευτική χρήση. Από τον Αύγουστο του 2017 προσφέρεται δωρεάν στο ευρύ κοινό.

4.2 Εκπαιδευτική Αξία

Η Cisco δημιούργησε το Packet Tracer για να χρησιμοποιηθεί σαν συμπληρωματικό βοήθημα για τους σπουδαστές της είτε είναι στην αίθουσα διδασκαλίας είτε μελετούν μόνοι τους. Οι εκπαιδευτές μπορούν να παρουσιάσουν περίπλοκες τεχνικές έννοιες. Μπορούν να συνθέσουν, να πειραματιστούν, να εκτελέσουν προμελετημένα σενάρια και να εντοπίσουν σφάλματα σε ένα περίπλοκο εικονικό δίκτυο σε λιγότερο χρόνο σε σχέση με ένα πραγματικό. Η προσομοίωση διευκολύνει την παρουσίαση εσωτερικών λειτουργιών του δικτύου και την ανάλυση της δρομολόγησης των δεδομένων ακριβώς την στιγμή που συμβαίνει, πράγμα δύσκολο σε πραγματικές συνθήκες

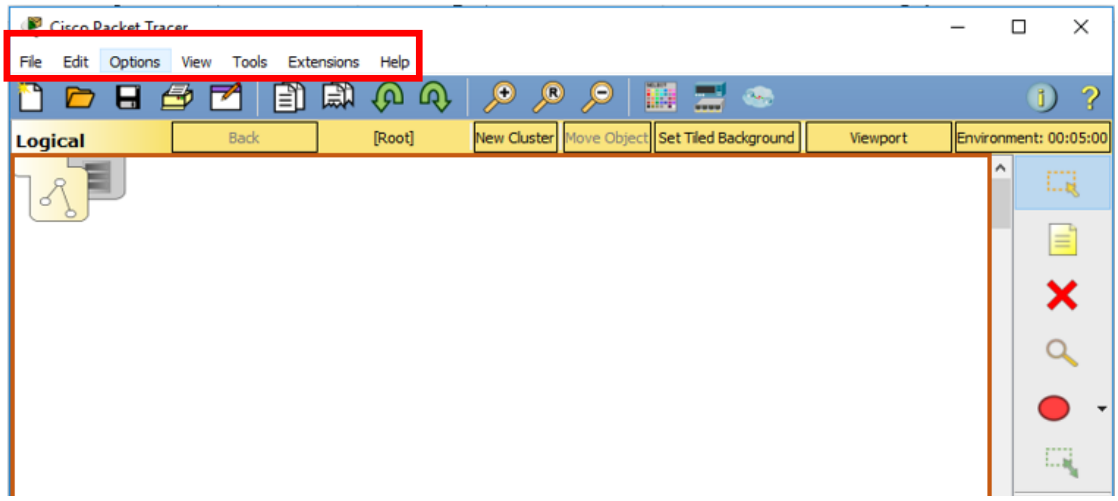
(real time). Οι σπουδαστές όταν μελετούν μόνοι τους έχουν στη διάθεση τους την λειτουργικότητα πλήθους πανάκριβων μηχανημάτων και την ευχέρεια κάθε πειραματισμού χωρίς τον κίνδυνο να προκαλέσουν ζημιά. Μάλιστα το Packet Tracer τους εκπαιδεύει στο να είναι προσεκτικοί. Δεν τους επιτρέπει να αλλάζουν εξαρτήματα σε αναμμένη συσκευή έστω και αν είναι εικονική! Πρέπει πρώτα να την σβήσουν "εικονικά"!.

Αφού "εγκατασταθούν" και ρυθμιστούν οι συσκευές μπορούν να αρχίσουν οι δοκιμές από τμήματα του δικτύου και να επεκταθούν στο σύνολό του. Οι δοκιμές γίνονται σε πραγματικό χρόνο με τα μέρη του δικτύου να ανταλλάσσουν πακέτα δεδομένων στα πλαίσια των λειτουργιών που τους έχουμε αναθέσει. Όταν παρουσιαστεί κάποιο πρόβλημα στο δίκτυο τότε ο Packet Tracer μας δίνει την δυνατότητα να παρακολουθήσουμε την διακίνηση των πακέτων βήμα - βήμα στην περιοχή που παρουσιάστηκε το σφάλμα. Μπορούμε να εξετάσουμε τη δρομολόγηση και τη δομή των πακέτων σχεδόν σε κάθε δυνατή λεπτομέρεια. Εξάλλου βασίζεται στο μοντέλο αναφοράς OSIκαι τα αντίστοιχα πρωτόκολλα.

4.3 Επισκόπηση περιβάλλοντος εργασίας του Cisco Packet Tracer

Πάμε να δούμε το περιβάλλον εργασίας ορισμένα εργαλεία και συσκευές του packet tracer πιο αναλυτικά προκειμένου να το χρησιμοποιήσουμε για τις ανάγκες των πειραμάτων.

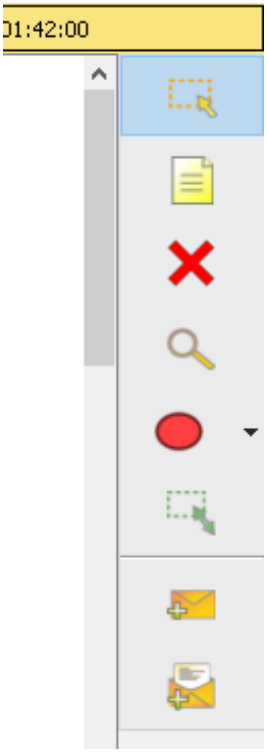
Η **μπάρα του menu** περιέχει: το αρχείο(File), την επεξεργασία(Edit), τις επιλογές(Options), την εμφάνιση(View), τα εργαλεία(Tools), τις επεκτάσεις(Extentions), και την βοήθεια(Help).



Εικόνα 32: Η μπάρα του μενού

Η κύρια **μπάρα εργαλείων** περιέχει εικονίδια με συντομεύσεις από : το αρχείο, την επεξεργασία, την εμφάνιση και τα εργαλεία.

Εικόνα 33: Η μπάρα των εργαλείων



Στα δεξιά της εφαρμογής βλέπουμε την μπάρα εργαλειών που περιέχει όλα τα στοιχεία που χρησιμοποιούνται πιο συχνά στον χώρο εργασίας του packet tracer

Εδώ βλέπουμε το **εργαλείο επιλογής** το οποίο το χρησιμοποιούμε για να επιλέγουμε ,να τονίζουμε και να μετακινούμε τα αντικείμενα ,τίς συσκευές καθώς επίσης και τις ενσύρματες συνδέσεις.

Το **εργαλείο μετακίνησης** της διάταξης χρησιμοποιείται για να μετακινούμε ολόκληρο το χώρο εργασίας μέσα σε κάποιο «λογικό» πλαίσιο-έκταση.

Το **εργαλείο τοποθέτησης σημειώσεων** το χρησιμοποιούμε προκειμένου να προσθέτουμε σχόλια στον χώρο εργασίας.

Το **εργαλείο διαγραφής** χρησιμοποιείται για την διαγραφή συσκευών, σημειώσεων, αντικειμένων που δημιουργήθηκαν από την παλέτα σχεδίων και τέλος των ενσύρματων συνδέσεων.

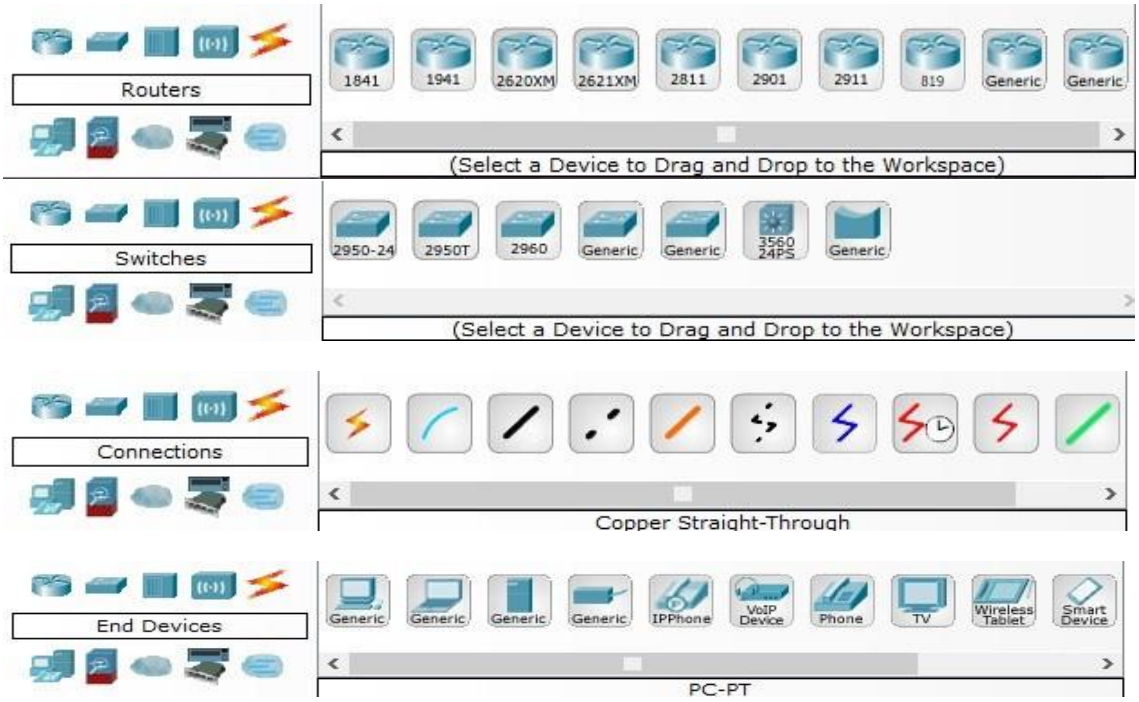
Η **παλέτα σχεδίων** χρησιμοποιείται για την εισαγωγή σχεδίων και έχει ως προεπιλογή το πολύγωνο.

Εργαλείο προσθήκης πληροφοριών ελέγχου(PDU). Με αυτό δημιουργούμε πακέτα ICMP τα οποία περιέχουν πληροφορίες χρησιμοποιούμενες από τις δικτυακές συσκευές επιπέδου δικτύου (router).

Εργαλείο δημιουργίας σύνθετων πακέτων PDU.

Πλαίσιο επιλογής τύπου συσκευής ή σύνδεσης.

Όπως βλέπουμε και στα παρακάτω στιγμιότυπα της οθόνης (Screenshot) το περιβάλλον έχει αυτή τη μορφή και περιέχει πολλές δυνατότητες όπως:



Εικόνα 34: Επιλογών Υλικών δικύωσης

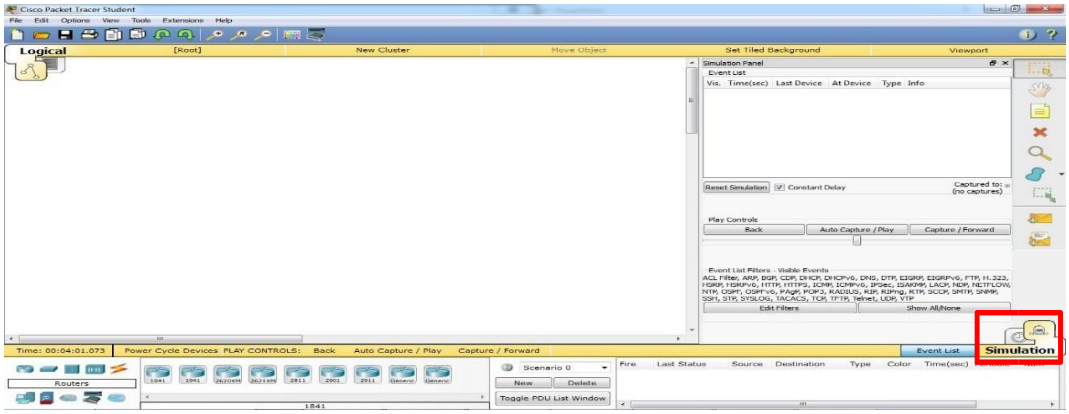
Διαθέτει όλο τον συνολικό εξοπλισμό (routers, switches, servers, υπολογιστές, διάφορα είδη καλωδίων για τις μεταξύ τους συνδέσεις) . Όπως βλέπουμε και στις εικόνες περιέχει και διαφορετικά είδη όπως π.χ. στα switches έχει και του επιπέδου 2 και του επιπέδου 3 που υποστηρίζει και δρομολόγηση μαζί.

Ο εξοπλισμός που θα χρειαστούμε κυρίως είναι στην ακόλουθη εικόνα.

Εικόνα 35: Εξοπλισμός εφαρμογών

Η καρτέλα προσομοίωσης

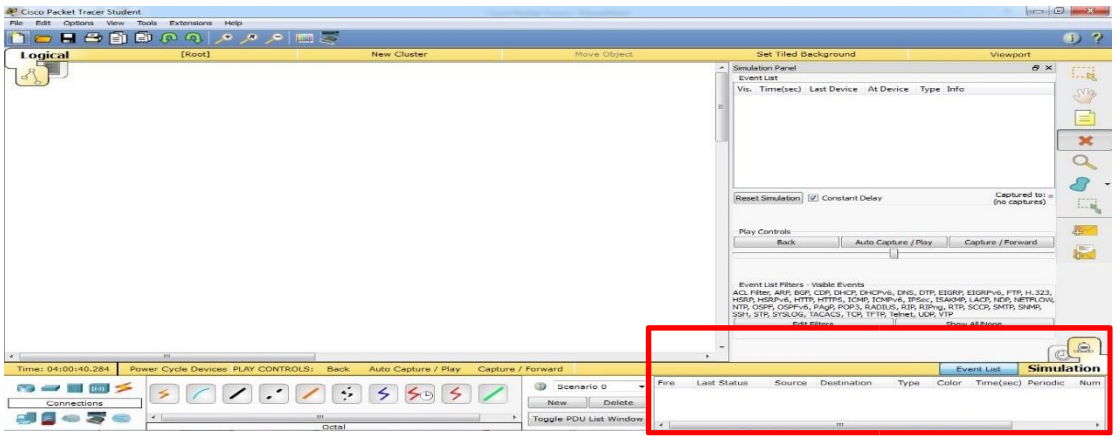
Κάτω από την καρτέλα πραγματικού χρόνου βρίσκεται αυτό της προσομοίωσης. Στην κατάσταση προσομοίωσης έχουμε την δυνατότητα να παρατηρούμε την κίνηση του δικτύου σε σύγκριση με τον χρόνο τον οποίο τον ρυθμίζει απευθείας ο χρήστης.



Εικόνα 36: Καρτέλα προσομοίωσης

Πακέτα PDU κατά την διάρκεια την προσομοίωσης

Εδώ επίσης μπορούμε να ελέγχουμε τα πακέτα που τοποθετούνται στο δίκτυο κατά την διάρκεια την προσομοίωσης



Εικόνα 37: Εμφάνιση προσομοίωσης

Στην προσομοίωση χρησιμοποιήσαμε ένα Cisco Router 2811 και ένα Switch 2960. Προκειμένου να λειτουργήσει σωστά ένα δίκτυο, πρέπει εκτός από τον κατάλληλο εξοπλισμό – ο οποίος θα προγραμματιστεί σωστά, να κάνουμε και τις απαραίτητες συνδέσεις μεταξύ τους. Το Cisco Packet Tracer διαθέτει στο χρήστη όλους τους δυνατούς τρόπους σύνδεσης. Χρησιμοποιήθηκε κατά κύριο λόγο ευθύ (copper straight-through) καλώδιο, δηλαδή καλώδιο χαλκού απευθείας εξόδου αλλά και το διασταυρωμένο καλώδιο (crossover cable). Για λόγους ευκολίας υπάρχει η επιλογή της αυτόματης σύνδεσης μεταξύ των συσκευών αλλά ως καλή πρακτική η Cisco προτείνει να μην χρησιμοποιείται από τους εκπαιδευόμενους.

Επίσης συχνά χρησιμοποιήθηκε η τεχνική των σχολίων σε πλαίσια που όχι μόνο βοηθά στη σχεδίαση αλλά δίνει και άμεση άποψη της υλοποίησης σε έναν έμπειρο χρήστη.

Τέλος θα πρέπει να αναφέρουμε τη χρησιμότητα της επιλογής επιπλέον πληροφοριών σε κάθε σχέδιο, από το μενού Option → Preferences → Interface.

ΚΕΦΑΛΑΙΟ 5

Η Εφαρμογή Camtasia studio

Σε αυτό το κεφάλαιο αναφέρονται οι δυνατότητες και η χρήση της εφαρμογής δημιουργίας εκπαιδευτικών video που επιλέχθηκε να είναι το Camtasia Studio.

5.1 Δυνατότητες του Camtasia studio

Το Camtasia studio είναι μια εφαρμογή η οποία βοηθάει στην διδασκαλία υπολογιστικών κυρίως μαθημάτων εργαστηρίου, όπως spss, excel, word, photoshop, flash κλπ., χωρίς την χρήση βιντεοπροβολέα, όπου αρκετά συχνά καλούμαστε να αντιμετωπίσουμε πρακτικά προβλήματα φωτεινότητας, ευκρίνειας κλπ. σε αίθουσες διδασκαλίας που δεν είναι κατάλληλα διαμορφωμένες. Το Camtasia studio είναι μια εφαρμογή που επιτρέπει στον καθηγητή να δημιουργήσει video-μαθήματα (Εικόνα 38). Οι φοιτητές την ώρα του εργαστηρίου παρακολουθούν ανεξάρτητα το video-μάθημα χρησιμοποιώντας ακουστικά (ο καθένας χρησιμοποιώντας τον προσωπικό του υπολογιστή) και ταυτόχρονα μπορούν να υλοποιούν τα βήματα που βλέπουν και ακούν από το video. Η χρήση του video-μαθήματος μπορεί να γίνει και τμηματικά, ένα μέρος του εργαστηρίου να είναι κανονική διάλεξη και το υπόλοιπο (η άσκηση) να γίνεται μέσω του video-μαθήματος.

Στα πλεονεκτήματα της χρήσης του είναι τα ακόλουθα:

1. Επιτάχυνση της διαδικασίας μάθησης από τους φοιτητές. Πλέον ο καθένας μαθαίνει με το δικό του ρυθμό και μπορεί να ρωτήσει το διδάσκοντα χωρίς να διακόπτει το μάθημα. Επίσης, αν κάποιοι φοιτητές έχουν ιδιαίτερο πρόβλημα στην κατανόηση, μπορούν να κάνουν επανάληψη σε ένα συγκεκριμένο τμήμα του video-μαθήματος, ενώ σε αντίθετη περίπτωση μπορεί να καθυστερούν συνολικά το μάθημα.

2. Υπάρχει καλύτερος έλεγχος του μαθήματος από το διδάσκοντα, πλέον ο ρόλος του είναι να λύσει συγκεκριμένες απορίες των φοιτητών και να ελέγχει την πρόοδο του εργαστηρίου.

3. Οι φοιτητές (εφόσον το επιθυμεί και ο διδάσκων) θα έχουν τη δυνατότητα και από το σπίτι να επαναλάβουν το εργαστήριο μέσω του video, γεγονός που είναι ιδιαίτερα χρήσιμο αν χάσουν κάποιο μάθημα.

Η εφαρμογή υπάρχει σε δύο προγράμματα το Camtasia Recorder και τα Camtasia Studio. Το Camtasia Recorder το χρησιμοποιείτε για να καταγράψετε σε video το μάθημα και αποθηκεύει αρχεία σε μορφή .camproj αρχεία ενώ με το Camtasia Studio μπορείτε να επεξεργαστείτε αρχείου τύπου .camproj και

να τα μετατρέψετε σε οποιοδήποτε format video από το μενού “File” και “produce video as”.

5.2 Δημιουργία Βιντεο με το camtasia

Εικόνα 38: Δημιουργία Βίντεο

Εισαγωγή στις βασικές λειτουργίες του Camtasia Recorder και βασικές ρυθμίσεις για την καταγραφή video

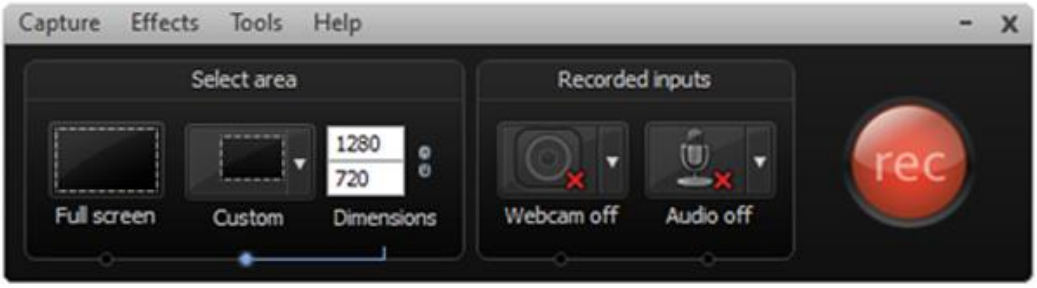
Το Camtasia διαθέτει ποικίλες λειτουργίες. Δύο από αυτές είναι η καταγραφή-δημιουργία video και η επεξεργασία. Η καταγραφή γίνεται με το εργαλείο Camtasia Recorder. Όταν ολοκληρώσουμε την βιντεοσκόπηση τότε μπορούμε μέσω του Camtasia Studio να επεξεργαστούμε το video που δημιουργήσαμε αφαιρώντας τα σημεία που θέλουμε (π.χ. αν κάναμε κάποιο λάθος κατά τη βιντεοσκόπηση μπορούμε να αφαιρέσουμε αυτό το τμήμα του βίντεο), προσαρμόζοντας τον ήχο, προσθέτοντας κάποια εφέ κοκ.

Εικόνα 39 : Εναρξη εγγραφής Βίντεο

5.2.1 Έναρξη του Camtasia Recorder

Ανοίγουμε το Camtasia Studio και επιλέγουμε το "Record the Screen" αν επιθυμούμε να κάνουμε καταγραφή.

Στη συνέχεια εμφανίζεται το παρακάτω παράθυρο (Screen Recorder) από το οποίο μπορούμε να κάνουμε όλες τις ρυθμίσεις που αφορούν την βιντεοσκόπηση.



Εικόνα 40: Ρύθμιση επιλογών εγγραφής Βίντεο

5.2.2. Ρύθμιση μικροφώνου και ήχου

Από την περιοχή "Recorded inputs" ρυθμίζουμε τον ήχο πατώντας στο βελάκι που είναι δίπλα στο εικονίδιο του μικροφώνου. Επιλέγουμε από την εμφανιζόμενη λίστα το μικρόφωνο από το οποίο επιθυμούμε να ακουγόμαστε (επιλέγουμε το εξωτερικό μικρόφωνο και όχι αυτό που ενδεχομένως έχει ενσωματωμένο ο υπολογιστής μας ή οποιοδήποτε άλλο μπορεί να υπάρχει όπως πχ αυτό μίας κάμερας).

Στη συνέχεια ρυθμίζουμε την ένταση του μικροφώνου από την μπάρα που εμφανίζεται ώστε να ακουγόμαστε δυνατά και καθαρά.

Για να έχουμε ένα καλό αποτέλεσμα δεν πρέπει η ένταση του μικροφώνου να είναι απαραίτητα στο μέγιστο σημείο της αλλά ανάλογα με το μικρόφωνο που χρησιμοποιούμε και την απόσταση που έχουμε από αυτό θα βρούμε το σημείο εκείνο που ο ήχος μας είναι ικανοποιητικός.

Εικόνα 41: Ρύθμιση μικροφώνου και ήχου

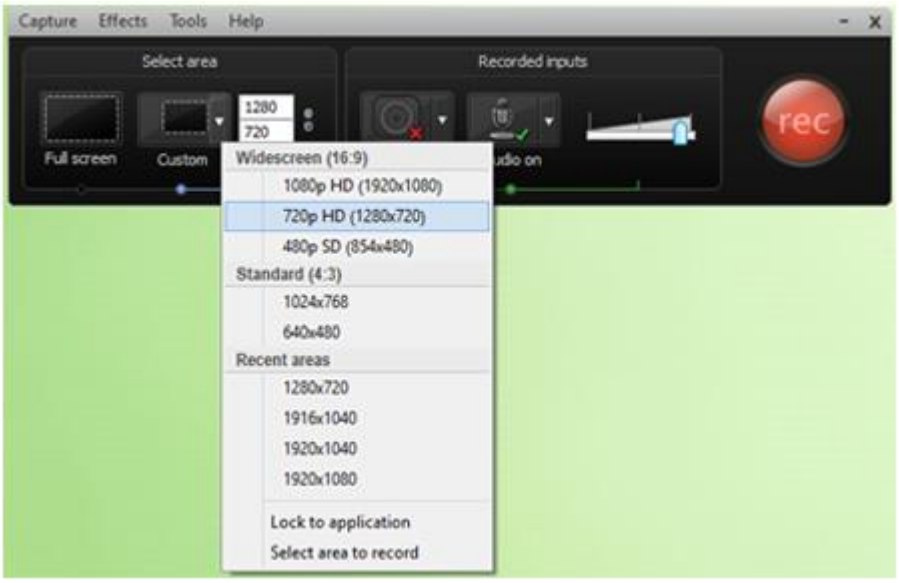
5.2.3. Διαστάσεις του video και περιοχή εγγραφής

Μπορούμε να βιντεοσκοπήσουμε είτε ολόκληρη την οθόνη μας είτε μέρος αυτής.

- Αν επιθυμούμε να βιντεοσκοπήσουμε ολόκληρη την οθόνη μας τότε πατάμε το κουμπί Full Screen
- Αν επιθυμούμε να βιντεοσκοπήσουμε μέρος αυτής από το βελάκι που εμφανίζεται δίπλα στο κουμπί Custom επιλέγουμε μία από τις προτεινόμενες διαστάσεις. Προτείνεται η επιλογή 720p HD (1280x720)
- Πατάμε το Select area to record για να επιλέξουμε μόνοι μας ακριβώς πιο κομμάτι της οθόνης θα βιντεοσκοπήσουμε

Αν επιλέξουμε το Select area to record θα εμφανιστούν στην οθόνη δύο κόκκινες γραμμές και ο δείκτης του ποντικιού μας θα μετατραπεί σε σταυρό. Σύρουμε κρατώντας πατημένο το πλήκτρο του ποντικιού για να καλύψουμε όλη την περιοχή που θέλουμε να βιντεοσκοπηθεί.

Το φωτεινό ορθογώνιο που εμφανίζεται μας δείχνει το τμήμα της οθόνης που θα εμφανίζεται στο video. Ότι είναι εκτός αυτού δεν θα φαίνεται. Μπορούμε να μετακινήσουμε το ορθογώνιο αυτό για να βιντεοσκοπήσουμε ακριβώς την περιοχή που θέλουμε, πηγαίνοντας σε μία από τις ακμές του και σύροντας το όταν το δείκτης του ποντικιού αλλάξει σε σταυρό.

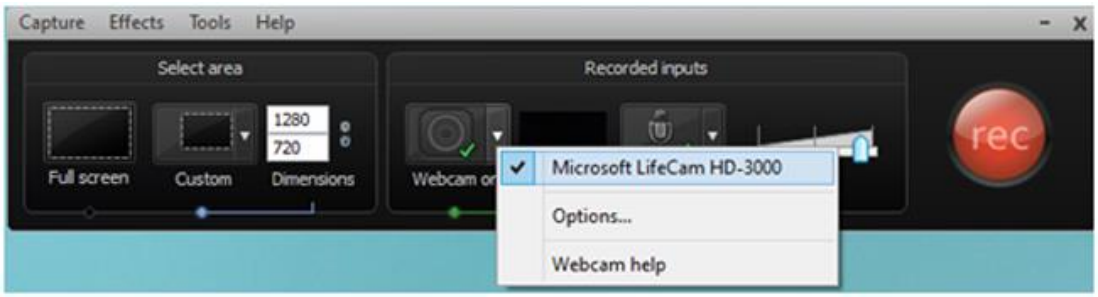


Εικόνα 42: Επιλογή διαστάσεων του Βίντεο

5.2.4. Video με καταγραφή οθόνης αλλά και κάμερας

Για να δημιουργήσουμε video στο οποίο θα καταγράφεται η οθόνη αλλά ο ομιλητής μέσω της κάμερας του υπολογιστή του ενεργοποιούμε την κάμερα πατώντας πάνω στο εικονίδιο Webcam. Αν θέλουμε να αλλάξουμε την κάμερα από την οποία γίνεται η λήψη πατάμε στο βελάκι και επιλέγουμε από την λίστα την επιθυμητή (πχ αν έχουμε προσθέσει εξωτερική κάμερα στο laptop μας και

θέλουμε η λήψη να γίνεται από αυτήν και όχι από την ενσωματωμένη που υπάρχει στο laptop).



Εικόνα 43: Χρήση μιας Webcam

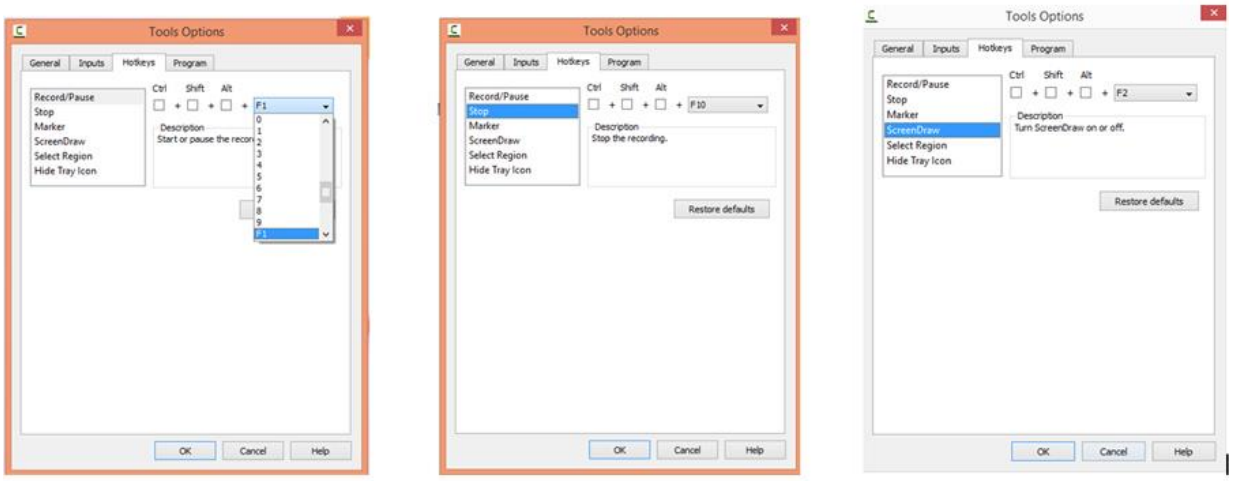
5.2.5. Συντομεύσεις πληκτρολογίου

Είναι σημαντικό όταν γίνεται η βιντεοσκόπηση να μπορούμε να κάνουμε παύση ή διακοπή της εγγραφής ανά πάσα στιγμή και με τον τρόπο που είναι πιο εξυπηρετικός κάθε φορά. Υπάρχουν δύο τρόποι. Ο ένας είναι να εντοπίσουμε το αντίστοιχο κουμπί στο Camtasia Recorder και ο δεύτερος είναι πατώντας ένα κουμπί στο πληκτρολόγιο. Επιλέγουμε από το κουμπί "Tools -->Options " . Στην καρτέλα Hotkeys στην αριστερή πλευρά εμφανίζονται σε ένα πλαίσιο οι λειτουργίες που είναι διαθέσιμες κατά την βιντεοσκόπηση και δεξιά πατώντας πάνω στο βελάκι μπορούμε να επιλέξουμε με ποιό κουμπί από το πληκτρολόγιο επιθυμούμε να εκτελείται κάθε λειτουργία.

Αν λοιπόν θέλουμε να πατάμε το F1 για να ξεκινά η εγγραφή και να κάνουμε παύση τότε επιλέγουμε από το αριστερό πλαίσιο το Record/Pause και δεξιά το F1.

Στη συνέχεια επιλέγουμε το Stop και δεξιά το αντίστοιχο πλήκτρο που επιθυμούμε. Ομοίως για τις υπόλοιπες επιλογές αν θεωρούμε ότι κάποια από αυτές μας είναι χρήσιμη. Τέλος πατάμε OK και μπορούμε πατώντας είτε το F1 (ή όποιο κουμπί έχουμε επιλέξει) είτε το REC να ξεκινήσουμε την καταγραφή. Με το ίδιο πλήκτρο βέβαια κάνουμε και παύση.

Για να χρησιμοποιήσουμε το εργαλείο Screen Draw που μας δίνει τη δυνατότητα να γράφουμε με τη γραφίδα και να προσθέτουμε σχήματα πάνω στην οθόνη μας ή σε οποιαδήποτε εφαρμογή προβάλουμε κατά την εγγραφή του video επιλέγουμε επίσης μια συντόμευση πληκτρολογίου πχ το πλήκτρο F2. Έτσι πατώντας το πλήκτρο αυτό ενώ γίνεται η εγγραφή, εμφανίζονται στο παράθυρο Screen Recorder όλες οι διαθέσιμες επιλογές.



Εικόνα 44: Χρήση πλήκτρων συντόμευσης

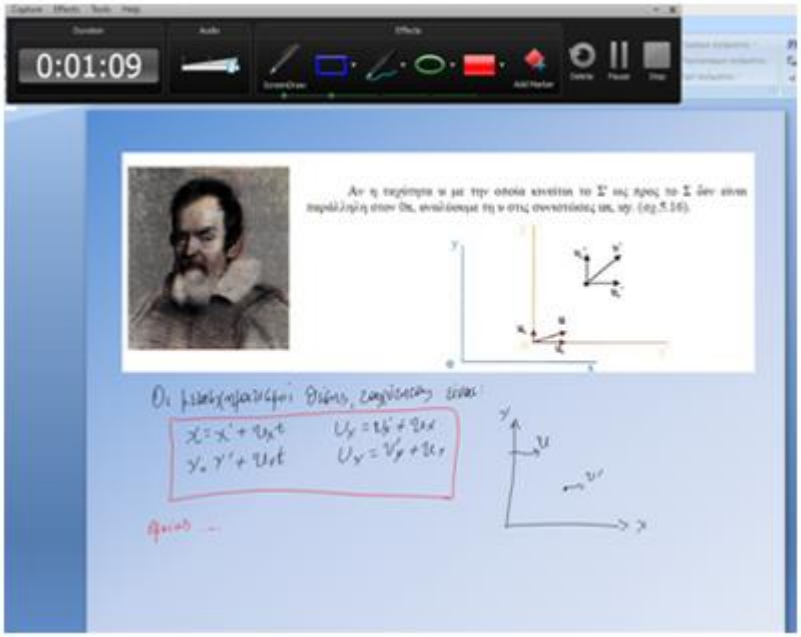
5.2.6. Εγγραφή, παύση και διακοπή

Αφού διαμορφώσουμε την οθόνη μας έτσι ώστε να έχουμε κλειστά όλα τα αρχεία που δεν θέλουμε να φαίνονται ή αντίστοιχα ανοιχτά όλα όσα θέλουμε να δείξουμε στο video τότε μπορούμε να ξεκινήσουμε την εγγραφή πατώντας από το πληκτρολόγιο το κουμπί που ορίσαμε στο προηγούμενο βήμα ή πατώντας το κουμπί REC από το Recorder. Γίνεται αντίστροφη μέτρηση και μετά από 3 δευτερόλεπτα η εγγραφή αρχίζει. Μπορούμε ανά πάσα στιγμή να πατήσουμε Παύση (κουμπί Pause) ή διακοπή (κουμπί Stop) αν ολοκληρώσαμε το video μας.

Εικόνα 45: Εγγραφή και παύση εγγραφής

Στην περίπτωση που κάνουμε κάποιο λάθος μπορούμε να επαναλάβουμε το σημείο που δεν μας άρεσε και έπειτα κάνοντας μία μικρή επεξεργασία να αφαιρέσουμε από το τελικό video μόνο το τμήμα εκείνο που δεν ήταν καλό. Επομένως δεν είναι απαραίτητο κάθε φορά να σταματάμε την εγγραφή και να ξεκινάμε από την αρχή αφού μπορούμε εύκολα να αφαιρέσουμε ότι δεν μας άρεσε στο τέλος.

5.2.7. Χρήση του Screen Draw-γράφουμε με τη γραφίδα μας στην οθόνη ή σε οποιαδήποτε εφαρμογή



Εικόνα 46: Χρήση του Screen Draw για σχεδίαση

Πατώντας από το πληκτρολόγιο το κουμπί F2 που ορίσαμε παραπάνω ως συντόμευση για το Screen Draw αυτόματα εμφανίζονται στο παράθυρο Screen Recorder κάποια επιπλέον εργαλεία. Μεταξύ άλλων μπορούμε να χρησιμοποιήσουμε τη γραφίδα (Pen), αλλά και σχήματα όπως αυτά που εμφανίζονται στην παρακάτω εικόνα, ενώ παράλληλα έχουμε τη δυνατότητα να αλλάζουμε χρώμα και πάχος γραμμής σε αυτά.

Εικόνα 47: Επιλογή εργαλείων στο Screen Draw

5.2.8. Αποθήκευση του video

Όταν ολοκληρώσουμε το video αυτόματα εμφανίζεται το παράθυρο Preview στο οποίο αναπαράγεται το video που δημιουργήσαμε.

- Μπορούμε να αποθηκεύσουμε το αρχείο μας και να το επεξεργαστούμε αμέσως μετά, πατώντας του κουμπί Save and Edit.
- Αν θέλουμε να έχουμε τη δυνατότητα να επεξεργαστούμε το αρχείο αλλά δεν θέλουμε αυτό να γίνει τώρα πατάμε το βελάκι κάτω από το Save and Edit και επιλέγουμε Save as. Στη συνέχεια ονομάζουμε το αρχείο μας και

ορίζουμε που θα αποθηκευτεί. Όταν χρειαστεί μπορούμε να το ανοίξουμε και να το επεξεργαστούμε μέσω του Camtasia Studio.

- Εξάγουμε άμεσα το αρχείο σε video πατώντας το κουμπί Produce αν δεν επιθυμούμε να κάνουμε καμία αλλαγή ή επεξεργασία.
- Τέλος, διαγράφουμε την καταγραφή που μόλις κάναμε αν δεν μας ικανοποιεί πατώντας το Delete

Εικόνα 48: Αποθήκευση του Βίντεο

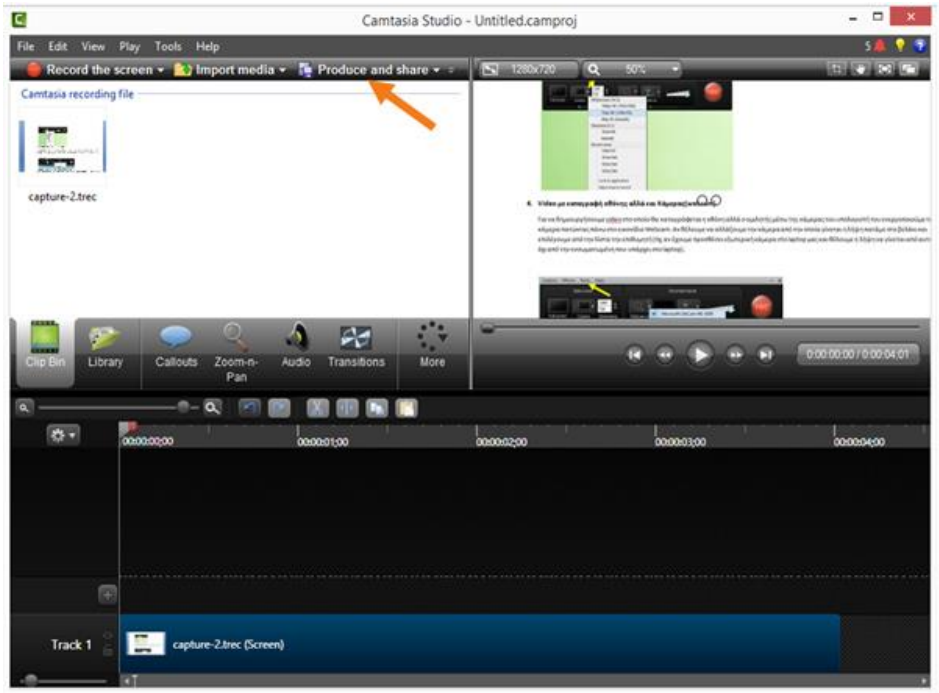
5.2.9 Παραγωγή Produce

Από το παράθυρο Production Wizard που εμφανίζεται μετά την αποθήκευση μπορούμε να ορίσουμε τι μορφή και ποιά χαρακτηριστικά αναπαραγωγής θα περιέχει. Καθώς στην προκειμένη περίπτωση αυτό που μας ενδιαφέρει είναι τα video μας να μπορεί να αναπαραχθεί σε όσο το δυνατόν περισσότερους υπολογιστές και κινητές συσκευές δεν επιλέγουμε κάποια εξεζητημένη μορφή video αλλά αυτήν που εξυπηρετεί περισσότερο δηλαδή MP4 σε 720p (MP4 only (up to 720p)). Πατάμε Επόμενο και ορίζουμε το όνομα και το φάκελο στον οποίο θα αποθηκεύσουμε το video. Στη συνέχεια ακολουθεί η μετατροπή του video που διαρκεί μερικά λεπτά. Όταν ολοκληρωθεί αυτόματα αναπαράγεται το video.

Εικόνα 49: Παραγωγή βίντεο και μετατροπή τύπου αρχείου

5.2.10 Αποθήκευση και Εξοδος Save and Edit

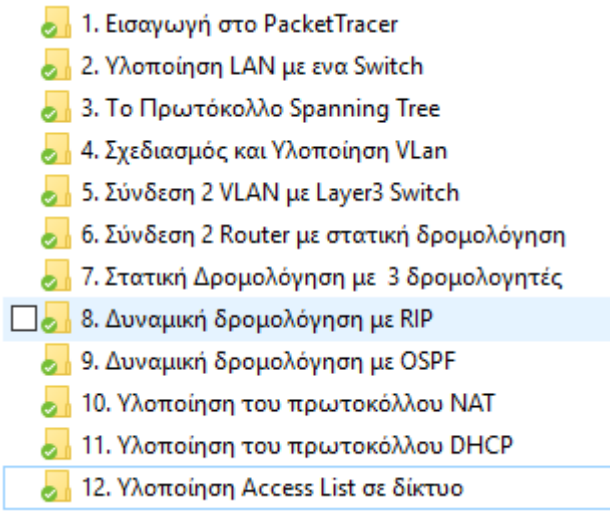
Επιλέγοντας Save and Edit αφού γίνει η αποθήκευση μεταφερόμαστε στο παράθυρο του Camtasia Studio όπου μπορούμε να κάνουμε επεξεργασία. Όταν ολοκληρώσουμε την επεξεργασία επιλέγουμε Produce and Share προκειμένου να εξάγουμε το video στην τελική του μορφή ακολουθώντας τα βήματα που περιγράφονται παραπάνω.



Εικόνα 50: Τελικό στάδιο παραγωγής

ΚΕΦΑΛΑΙΟ 6 Η Υλοποίηση των πειραμάτων

Σε αυτό το κεφάλαιο αναφέρονται τα δώδεκα πειράματα που εκετελέστηκαν, η μεθοδολογία που ακολουθήθηκε και τα αρχεία pkt που αποθηκεύθηκαν με την υλοποίηση των δικτυακών εφαρμογών.

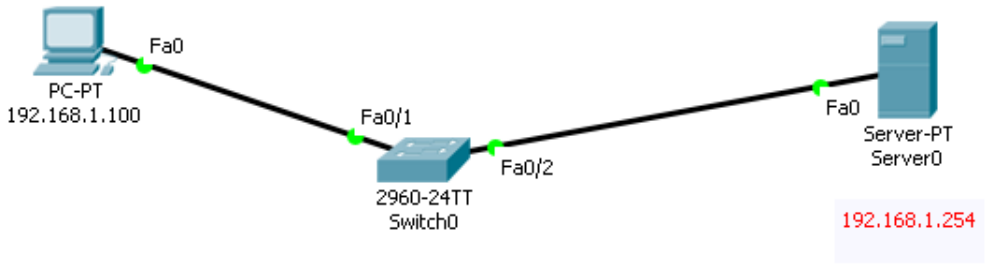


Εικόνα 51: Λίστα παραδειγμάτων και Βίντεο

6.1 Εισαγωγή στο Packet Tracer

Κατεβάζουμε την τελευταία έκδοση της εφαρμογής Packet Tracer από το δικτυακό τόπο Cisco NetAcad (https://www.netacad.com)

Εγκαθιστούμε το προϊόν και το εκτελούμε



Εικόνα 52 : Δημιουργία ενός μικρού τοπικού δικτύου

Εξέλιξη Παραδείγματος

Αυτό είναι ένα βασικό μάθημα εισαγωγικό στη λειτουργία της εφαρμογής PacketTracer.

Θα παρουσιάσουμε τη δημιουργία ενός μικρού τοπικού δικτύου (LAN).

Για να το κάνουμε αυτό επιλέγουμε από το πλαίσιο επιλογής τύπου συσκευής End Devices παίρνουμε έναν υπολογιστή PC και με τη διαδικασία Drag n Drop το σύρουμε και το τοποθετούμε στο περιβάλλον εργασίας (workspace).

Κατόπιν πηγαίνουμε στους μεταγωγείς (switches) διαλέγουμε ένα 2960 και το τοποθετούμε δίπλα στον υπολογιστή

Τώρα έχουμε έναν υπολογιστή και ένα μεταγωγέα.

Επιστρέφουμε στην κατηγορία επιλογής τύπου συσκευής End Devices για να επιλέξουμε ένα Εξυπηρετητή (Server) και να τον τοποθετήσουμε δεξιά από το μεταγωγέα.

Τώρα πρέπει να συνδέσουμε τις συσκευές μεταξύ τους και να κάνουμε μερικές δοκιμές για να δούμε ότι ο υπολογιστής επικοινωνεί με τον Εξυπηρετητή.

Από τον υπολογιστή μέχρι το μεταγωγέα χρειαζόμαστε ένα ευθύ καλώδιο (straight through cable) έτσι πηγαίνω στην επιλογή καλώδια και αναζητώ ένα τέτοιο.

Αφού το επιλέξω το καλώδιο πηγαίνω πάνω στον υπολογιστή και με κλικ επιλέγω τη θύρα FastEthernet0.

Στη συνέχεια πηγαίνω στο μεταγωγέα και πάλι με κλικ επιλέγω τη πρώτη διαθέσιμη θύρα που είναι η FastEthernet0/1. Αφήνω το ποντίκι και η σύνδεση επιτυγχάνεται.

Τώρα πρέπει να συνδέσω το μεταγωγέα με το Δρομολογητή. Πάλι επιλέγω ευθύ καλώδιο και με κλικ στο Δρομολογητή επιλέγω τη θύρα FastEthernet0 και πηγαίνω στην επόμενη διαθέσιμη θύρα του που είναι η FastEthernet0/2. Η σύνδεση επιτυγχάνεται.

Για να μπορέσει να επικοινωνήσει ο υπολογιστής με τον Εξυπηρετητή θα πρέπει να επιλεγούν και να τοποθετηθούν διευθύνσεις IP στις συσκευές.

Για να φαίνονται οι διευθύνσεις θα τις τοποθετήσω σε σχόλια και έτσι γράφω 192.168.1.254 για τον Εξυπηρετητή και 192.168.1.100 για τον υπολογιστή.

Πηγαίνω στις ρυθμίσεις του Εξυπηρετητή –> Config - > Interface → FastEthernet0 και δίνω την IP 192.168.1.254 και όταν επιλέγω τη Subnet Mask συμπληρώνεται αυτόματα η προκαθορισμένη 255.255.255.0. Προσέχω την επιλογή Port Status να είναι ενεργοποιημένη και κλείνω τις ρυθμίσεις.

Πηγαίνω στις ρυθμίσεις του υπολογιστή → Config → Interface → FastEthernet0 και δίνω την IP 192.168.1.100 και όταν επιλέγω τη Subnet Mask συμπληρώνεται αυτόματα η προκαθορισμένη 255.255.255.0. Προσέχω την επιλογή Port Status να είναι ενεργοποιημένη και κλείνω τις ρυθμίσεις.

Μετακινώντας το ποντίκι πάνω σε κάθε συσκευή βλέπω και τις ρυθμίσεις IP που έχει.

Τώρα και οι δυο υπολογιστές έχουν ρυθμιστεί και βλέπω πως τα ενδεικτικά LED στις συνδέσεις έχουν γίνει παντού πράσινα. Πρέπει όμως να δοκιμάσω την επικοινωνία με τη χρήση της εντολής ping.

Πηγαίνω στις ρυθμίσεις του υπολογιστή → Desktop → Command Prompt → C:\> και δίνω την εντολή ping 192.168.1.254 με την οποία παίρνω απάντηση (reply) 4 φορές.

Αυτό σημαίνει ότι η διευθυνσιοδότηση που επιλέξαμε λειτούργησε και έχουμε ένα τοπικό δίκτυο σε λειτουργία καθώς επίσης ότι μπορούμε να το επεκτείνουμε με άλλους 22+2 υπολογιστές αφού έχουμε διαθέσιμες θύρες στο μεταγωγέα μας.

Τώρα μπορούμε να δοκιμάσουμε κάτι διαφορετικό.

Πηγαίνουμε στον Εξυπηρετητή –> Config - > Services → FTP και προσθέτουμε ένα χρήστη με το όνομα student και κωδικό πρόσβασης student με δικαιώματα Ανάγνωσης και Εγγραφής.

Πηγαίνουμε στον Εξυπηρετητή –> Config - > Services → HTTP και διορθώνουμε την εμφάνιση της αρχικής σελίδας index.html.

Κλείνουμε τις ρυθμίσεις και πηγαίνουμε στον υπολογιστή.

Πηγαίνω στις ρυθμίσεις του υπολογιστή → Desktop → Web Browser και στο πεδίο διεύθυνση πληκτρολογώ τη διεύθυνση 192.168.1.254 του Εξυπηρετητή.

Βλέπω το index.html που τροποποίησα πριν και πλοηγούμαι στις επιλογές του.

Πηγαίνω στις ρυθμίσεις του υπολογιστή → Desktop → Command Prompt → C:\> και δίνω την εντολή ftp 192.168.1.254 για να συνδεθώ στον FTP Server.

Δίνω όνομα και κωδικό student και συνδέομαι.

Με την εντολή quit αποσυνδέομαι από τον FTP Server.

Πηγαίνω στο κάτω δεξιά μέρος της οθόνης και αλλάζω το mode από RealTime σε Simulation.

Εδώ μπορώ να δοκιμάσω τα πακέτα που περνούν ανάλογα με την εφαρμογή/πρωτόκολλο που τρέχει με παρόμοιο τρόπο όπως της εφαρμογής WireShark .

Μπορώ να προσθέσω λοιπόν ένα PDU, με την επιλογή του εικονιδίου με τον κίτρινο φάκελο που έχει ένα σταυρό κάτω αριστερά, στον υπολογιστή

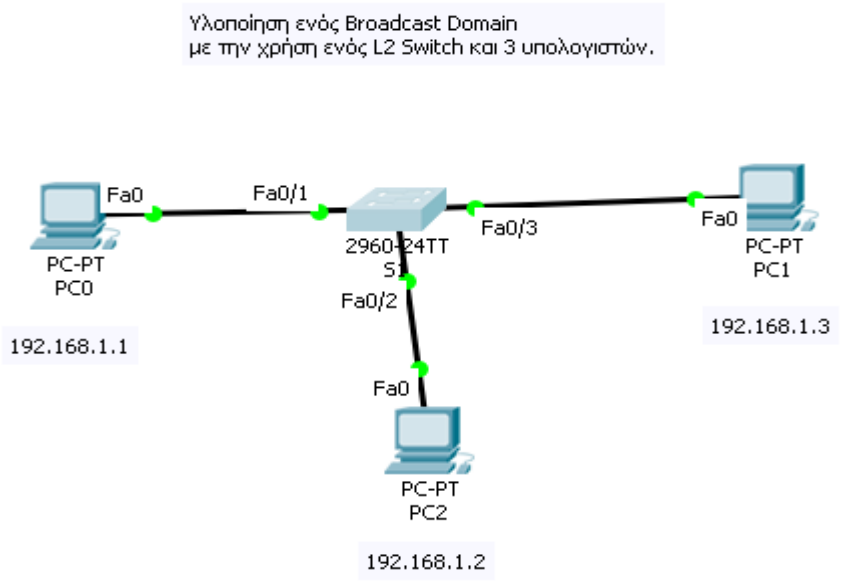
Στην επιλογή Edit Filters επιλέγω μόνο το πρωτόκολλο ICMP και στη συνέχεια επιλέγω το Auto Capture/Play

Παρακολουθώ τη μετακίνηση των πακέτων ICMP μεταξύ των συσκευών.

Τέλος αποθηκεύω το αρχείο με το όνομα **Intro.pkt.**

6.2 Υλοποίηση LAN με ενα Switch

One-broadcast-domain.pkt



Εικόνα 53 : Υλοποίηση LAN με τρεις υπολογιστές

Στο παράδειγμα αυτό χρησιμοποιούμε ένα Μεταγωγέα 2960 και τρεις Προσωπικούς Υπολογιστές PC (PC0, PC1, PC2) για να κάνουμε τον έλεγχο καλής λειτουργίας.

Ξεκινάμε τοποθετώντας με τη γνωστή διαδικασία τον εξοπλισμό στην περιοχή του πειράματος.

Στη συνέχεια κάνουμε τις συνδέσεις με ευθεία καλώδια (straight through).

Επιλέγουμε το δίκτυο 192.168.1.0/24 για να δώσουμε διευθύνσεις στις συσκευές.

Στις ρυθμίσεις των τριών υπολογιστών βάζουμε τις παρακάτω διευθύνσεις:

192.168.1.1/24 στο PC0

192.168.1.3/24 στο PC1

192.168.1.2/24 στο PC2

Με την εντολή **# show version** βλέπουμε πληροφορίες για τη συσκευή του μεταγωγέα όπως το μοντέλο του, τις θύρες που έχει και την έκδοση του λογισμικού IOS που χρησιμοποιεί.

```
Switch#show ver
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

System returned to ROM by power-on

Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.


24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0001.96B8.E0E1
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01


Switch    Ports  Model              SW Version            SW Image
------    -----  -----              ----------            ----------
*    1    26     WS-C2960-24TT      12.2                  C2960-LANBASE-M

Configuration register is 0xF


Switch#
```

Εικόνα 54 : Η εντολή show version

Για την παρουσίαση των θυρών του switch και του SVI έχουμε τα παρακάτω:

Η εντολή **# show ip interface brief** μας δείχνει την κατάσταση των θυρών του switch.

```
Switch#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down

Switch#
```

Εικόνα 55 : Η εντολή show ip interface brief

Η κατάσταση σε layer 1 φαίνεται με το status και σε layer 2 με το protocol.

Οι θύρες FE01, … FE03 που χρησιμοποιούνται βλέπουμε ότι έχουν το layer 1 UP και το Layer 2 UP.

```
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.254   YES manual up                    up
Switch#
```

Εικόνα 56 : Η κατάσταση των θυρών FastEthernet

Στη τελευταία γραμμή που δείχνει το interface VLAN1 είναι και αυτό UP, UP και έχει και IP Address στο layer 3.

Το interface Vlan1 έχει αρχική ρύθμιση (by default) administratively down και δεν έχει IP Address.

Την IP τη βάζουμε με τον παρακάτω τρόπο:

 # conf t

 # interface vlan 1

 # ip address 192.168.1.254 255.255.255.0

 # no shutdown (επειδή όλα τα Layer 3 interfaces η cisco τα έχει shutdown για λόγους ασφαλείας)

 # cntl +z

 # write

Στη συνέχεια με την εντολή **# show vlan** βλέπω ότι όλες οι πόρτες ανήκουν στον vlan1.

```
------- --------- ----------------- ------------------------------------------
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
 --More--
```

Εικόνα 57 : Η εντολή show vlan

 # copy running-config startup-config (αποθήκευση του προγραμματισμού στο switch)

Σε ότι αφορά το δεύτερο τμήμα της άσκησης με το MAC Address Table

Με την εντολή **# show mac-address-table**

βλέπουμε τις MAC διευθύνσεις των host που επικοινωνούν με το switch. Αρχικά ο πίνακας είναι κενός και δεν βλέπουμε καμμιά επειδή δεν έχει γίνει καμία επικοινωνία και δεν έχει κάποιο άλλο switch ώστε να χρησιμοποιήσει το πρωτόκολλο spanning tree για να μάθει τις διευθύνσεις.

```
------- --------- ----------------- ----------------------------------------
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

Switch#
```

Εικόνα 58 : Η εντολή show mac-address table

Πρέπει να βάλουμε IP διευθύνσεις στα PC και να κάνουμε Ping από το ένα PC στα άλλα δύο διαδοχικά.

Αν επιστρέψουμε στο switch και εκτελέσουμε πάλι την τελευταία εντολή

 # show mac-address-table βλέπουμε τις τρεις MAC διευθύνσεις των υπολογιστών που επικοινώνησαν. Άρα βλέπουμε πως το switch έμαθε τις τρεις MAC διευθύνσεις δυναμικά.

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00d0.ba25.30a5    DYNAMIC     Fa0/2
   1    00d0.bceb.1ca8    DYNAMIC     Fa0/1
   1    00e0.8f2e.a89d    DYNAMIC     Fa0/3
Switch#
```

Εικόνα 59 : Η εντολή show mac addresses-table μετά το ping

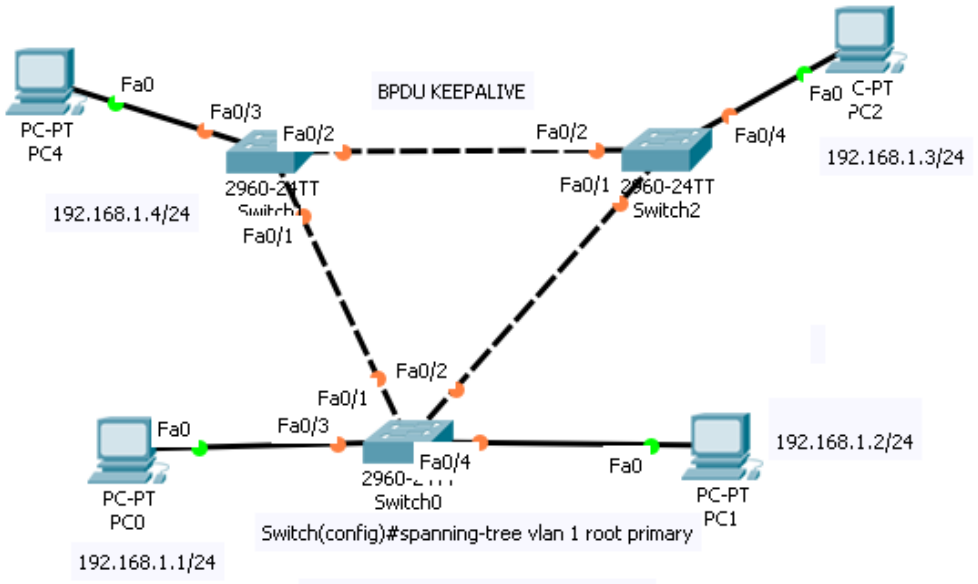
Αυτό είναι ένα broadcast domain με ένα και μοναδικό Vlan to Vlan 1.

Το Vlan 1 είναι εργοστασιακά φτιαγμένο και δεν διαγράφεται ούτε αλλάζει όνομα.

Τέλος αποθηκεύουμε το πείραμα με την επιλογή Save_As και το όνομα One-broadcast-domain.pkt

6.3 Το πρωτόκολλο Spanning-Tree

Spanning-tree.pkt



Εικόνα 60 : Η τοπολογία για το Spanning-Tree

Χρησιμοποιούμε 3 switch L2 2960 (24 port 10/100 +2 port 10/100/1000)

Στο παράδειγμα αυτό χρησιμοποιούμε και τέσσερις Προσωπικούς Υπολογιστές PC (PC0, PC1, PC2, PC4) για να κάνουμε τον έλεγχο καλής λειτουργίας.

Ξεκινάμε τοποθετώντας με τη γνωστή διαδικασία τον εξοπλισμό στην περιοχή του πειράματος.

Στη συνέχεια κάνουμε τις συνδέσεις με ευθεία καλώδια (straight through) μεταξύ υπολογιστών και μεταγωγέα και με διασταυρωμένα καλώδια (crossover) μεταξύ των μεταγωγέων.

Επιλέγουμε το δίκτυο 192.168.1.0/24 για να δώσουμε διευθύνσεις στις συσκευές.

Στις ρυθμίσεις των τριών υπολογιστών βάζουμε τις παρακάτω διευθύνσεις:

- 192.168.1.1/24 στο PC0
- 192.168.1.2/24 στο PC1
- 192.168.1.3/24 στο PC2
- 192.168.1.4/24 στο PC4

Θα χρησιμοποιήσουμε το πρωτόκολλο Cisco PVST+ (Per Vlan Spanning Tree Plus) που τρέχει 1 Instance για κάθε Vlan. Με το πρωτόκολλο αυτό μπορεί ένα switch να είναι root (ο κυρίαρχος του spanning tree) για το Vlan 1 ενώ για το Vlan 2 μπορεί άλλο switch ως root (κυρίαρχος).

Με την παρακάτω εντολή βλέπω πληροφορίες για το πρωτόκολλο ST :

Switch# show spanning-tree

Κοιτάζω τη MAC Address του Switch (Bridge ID) και τη MAC Address του Root. Αν είναι ίδιες σημαίνει ότι το switch αυτό είναι το root.

Παρακάτω βλέπω το Switch 0 :

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0000.0C89.3CB2
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     0000.0C89.3CB2
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

Switch#
```

Εικόνα 61 : Η εντολή show spanning-tree στο Switch 0

Παρακάτω βλέπω το Switch 1 :

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0000.0C89.3CB2
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000D.BDD7.DCD8
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/1            Root FWD 19        128.1    P2p

Switch#
```

Εικόνα 62 : Η εντολή show spanning-tree στο Switch 1

Παρακάτω βλέπω το Switch 2 :

```
Switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0000.0C89.3CB2
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.631B.7B0C
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/1            Root FWD 19        128.1    P2p

Switch#
```

Εικόνα 63 : Η εντολή show spanning-tree στο Switch 2

Αν δεν είναι ίδιες στο πάνω κομμάτι (Root ID) βλέπω τις πληροφορίες για το root και στο κάτω τη πληροφορία για το switch (Bridge ID) που είμαστε συνδεδεμένοι.

Το root ID priority έχει τη τιμή 32768+1 για ένα vlan.

Όταν ξεκινάει να εκτελείται το πρωτόκολλο spanning-tree ψάχνει στη τοπολογία να βρει το switch με τη μικρότερη MAC Address και αυτό το switch ορίζεται ως root.

Η εντολή που ορίζει το root switch είναι η παρακάτω:

 # spanning-tree vlan 1 root primary στο switch που θέλουμε να γίνει root.

Υπάρχει και άλλος τρόπος για να μειώσεις το priority βάζοντας συγκεκριμένο αριθμό αλλά η παραπάνω εντολή το μειώνει δυο φορές Χ 4096. Δηλαδή το νέο priority γίνεται 32768-9182=**24577**.

Το γεγονός ότι ένα switch είναι Root σημαίνει ότι η διαδρομή που περνάει μέσα από αυτό είναι η συντομότερη. Η συντομότερη διαδρομή είναι αυτή που έχει το χαμηλότερο path cost.

Το patch cost για το Ethernet είναι 100

Το patch cost για το Fast Ethernet είναι 19

Το patch cost για το Gigabit Ethernet είναι 4

Το patch cost για το 10G Ethernet είναι 2

Με την εντολή **# show spanning-tree** μπορούμε να δούμε το P**ort Role, Port Status** και το **Path Cost** για κάθε πόρτα του switch. Οι επιτρεπτές καταστάσεις είναι οι παρακάτω:

- **Altn** **BLK** Role **Alternate** κατάσταση **block**
- **Root** **FWD** Role **Root** κατάσταση **forward**
- **Desg** **FWD** Role **Designated** κατάσταση **forward**

Στο παράδειγμά μας το **Path Cost** είναι **19** επειδή όλες οι συνδέσεις έχουν επιλεγεί να είναι Fast Ethernet 100Mbps.

Παρακάτω βλέπω δυο εντολές στο Switch 0 :

Switch# show interfaces status

```
Switch#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          auto    auto  10/100BaseTX
Fa0/2                        connected    1          auto    auto  10/100BaseTX
Fa0/3                        connected    1          auto    auto  10/100BaseTX
Fa0/4                        connected    1          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        notconnect   1          auto    auto  10/100BaseTX
Fa0/7                        notconnect   1          auto    auto  10/100BaseTX
Fa0/8                        notconnect   1          auto    auto  10/100BaseTX
Fa0/9                        notconnect   1          auto    auto  10/100BaseTX
Fa0/10                       notconnect   1          auto    auto  10/100BaseTX
Fa0/11                       notconnect   1          auto    auto  10/100BaseTX
Fa0/12                       notconnect   1          auto    auto  10/100BaseTX
Fa0/13                       notconnect   1          auto    auto  10/100BaseTX
Fa0/14                       notconnect   1          auto    auto  10/100BaseTX
Fa0/15                       notconnect   1          auto    auto  10/100BaseTX
Fa0/16                       notconnect   1          auto    auto  10/100BaseTX
Fa0/17                       notconnect   1          auto    auto  10/100BaseTX
Fa0/18                       notconnect   1          auto    auto  10/100BaseTX
Fa0/19                       notconnect   1          auto    auto  10/100BaseTX
Fa0/20                       notconnect   1          auto    auto  10/100BaseTX
Fa0/21                       notconnect   1          auto    auto  10/100BaseTX
Fa0/22                       notconnect   1          auto    auto  10/100BaseTX
Fa0/23                       notconnect   1          auto    auto  10/100BaseTX
```

Εικόνα 64 : Η εντολή show interfaces status

Switch# show spanning-tree summary

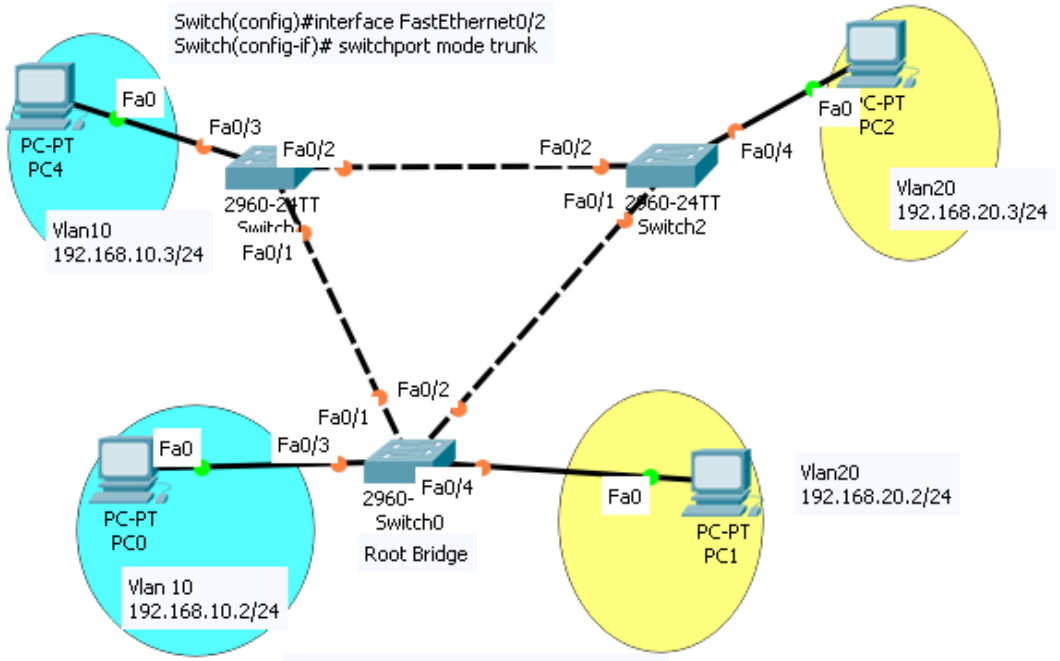
```
Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: default
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    0         0        0          4          4

---------------------- -------- --------- -------- ---------- ----------
1 vlans                     0         0        0          4          4

Switch#
```

Εικόνα 65 : Η εντολή show spanning-tree summary

6.4 Σχεδιασμός και υλοποίηση VLAN

Vlan-spanning-tree.pkt

Τα εικονικά Τοπικά Δίκτυα (Virtual LAN) είναι το αποτέλεσμα μιας ομαδοποίησης Υπολογιστών και λοιπών συσκευών ενός μεγάλου LAN, σε μικρότερες εικονικές ομάδες των οποίων τα μέλη μπορούν να επικοινωνούν μόνο μεταξύ τους σαν να βρίσκονται σε ένα ανεξάρτητο LAN.Η ομαδοποίηση αυτή ορίζεται σε switch χωρίς οι σταθμοί του δικτύου να εμπλέκονται στη διαδικασία. Ένα Switch μπορεί να υποστηρίξει ένα ή περισσότερα VLAN και έτσι κάθε πόρτα του Switch πρέπει με κάποιο τρόπο να καθορίζεται σε ποιο VLAN ανήκει.



Εικόνα 66 : Η τοπολογία για το VLAN

Χρησιμοποιούμε 3 switch L2 2960 (24 port 10/100 +2 10/100/1000)

Στο παράδειγμα αυτό χρησιμοποιούμε και τέσσερις Προσωπικούς Υπολογιστές PC (PC0, PC1, PC2, PC4) για να κάνουμε τον έλεγχο καλής λειτουργίας.

Ξεκινάμε τοποθετώντας με τη γνωστή διαδικασία τον εξοπλισμό στην περιοχή του πειράματος.

Στη συνέχεια κάνουμε τις συνδέσεις με ευθεία καλώδια (Straight Through) μεταξύ υπολογιστών και μεταγωγέα και με διασταυρωμένα καλώδια (Crossover) μεταξύ των μεταγωγέων (Switches).

Επιλέγουμε το δίκτυο 192.168.10.0/24 και το δίκτυο 192.168.20.0/24 για να δώσουμε διευθύνσεις στις συσκευές.

Στις ρυθμίσεις των τριών υπολογιστών βάζουμε τις παρακάτω διευθύνσεις:

- 192.168.10.2/24 στο PC0

- 192.168.20.2/24 στο PC1
- 192.168.20.3/24 στο PC2
- 192.168.10.3/24 στο PC4

Πρέπει να δημιουργήσουμε δυο VLAN σε κάθε ένα από τα τρία switch.

Το ένα θα είναι το vlan 10 (μπλέ χρώμα) και το δεύτερο το vlan 20 (κίτρινο χρώμα).

Το vlan 1 ήδη υπάρχει από τον κατασκευαστή και δεν μπορεί να αφαιρεθεί. Η μόνη ρύθμιση που επιτρέπεται σε αυτό είναι να απενεργοποιηθεί (να γίνει shutdown δηλαδή).

Ο προγραμματισμός γίνεται στο global configuration mode του κάθε switch.

Στη συνέχεια πηγαίνουμε σε καθένα από τα τρία switch και τα προγραμματίζουμε όπως παρακάτω:

 # enable

 # conf t

 # vlan 10

 # vlan 20

 # int FastEthernet0/3

 # switchport mode access (ορίζεται η πόρτα FE0/3 ως access)

 # switchport access vlan 10 (η πόρτα FE0/3 ανήκει πλέον στο vlan 10)

 # int FastEthernet0/4

 # switchport mode access (ορίζεται η πόρτα FE0/4 ως access)

 # switchport access vlan 20 (η πόρτα FE0/4 ανήκει πλέον στο vlan 20)

 # Cntl/Z

 # write

Στη συνέχεια πρέπει να κάνουμε trunk τις συνδέσεις μεταξύ των switch ώστε να περνάνε οι πληροφορίες από όλα τα vlan σύμφωνα με το πρωτόκολλο 802.1q.

Στο **Switch0** δίνουμε τις παρακάτω εντολές:

Switch(config)#interface FastEthernet0/1

Switch(config-if)# switchport mode trunk

Switch(config)#interface FastEthernet0/2

Switch(config-if)# switchport mode trunk

 # Cntl/Z

 # write

Στο **Switch0** κάνουμε τις δύο συνδέσεις trunk και τη μία που έμεινε από τον δεύτερο (**Switch1**) ή από το τρίτο (**Switch2**) επειδή η σύνδεση δηλώνεται σε μια από τις δυο πλευρές της. Δηλαδή αν μια σύνδεση γίνει trunk από τη μια πλευρά δεν χρειάζεται να ξαναγίνει από την απέναντι πλευρά.

Στο **Switch1** δίνουμε τις παρακάτω εντολές:

Switch(config)#interface FastEthernet0/2

Switch(config-if)# switchport mode trunk

 # Cntl/Z

 # write

Αν πάω στο Switch0 με την εντολή **# show interface trunk**

```
Switch#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20
Fa0/2       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20
Fa0/2       1,10,20

Switch#
```

Εικόνα 67 : Η εντολή show interface trunk

βλέπω ότι οι θύρες FastEthernet0/1 και FastEthernet0/2 είναι ρυθμισμένες ως trunk και επιτρέπουν να περάσουν τα vlan 1, 10, 20.

Το ίδιο μπορώ να δω και στα άλλα δυο switch με την ίδια εντολή και να προσθέσω όποια άλλη σύνδεση χρειάζεται να οριστεί ως trunk.

Αν πάω στο Switch1 με την εντολή **# show interface trunk**

```
Switch#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1
Fa0/2       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20
Fa0/2       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20
Fa0/2       none

Switch#
```

Εικόνα 68 : Η εντολή show interface trunk

Αν πάω στο Switch2 με την εντολή **# show interface trunk**

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1
Fa0/2       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20
Fa0/2       1,10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20
Fa0/2       1,10,20

Switch#
```

Εικόνα 69 : Η εντολή show interface trunk

Αν πάμε στη γραμμή εντολών του κάθε υπολογιστή θα δούμε ότι το ping απαντά μόνο σε υπολογιστές του ίδιου Vlan ανεξάρτητα από το switch που είναι συνδεδεμένοι οι δυο υπολογιστές.

Μπορούμε για παράδειγμα να προσθέσουμε ένα υπολογιστή PC5 στο Switch0 (port FastEthernet 0/5) και να του δώσουμε IP Address 192.168.10.10 . Αν δοκιμάσουμε το ping από το PC0 θα αποτύχει επειδή οι δυο υπολογιστές δεν βρίσκονται στο ίδιο vlan. Πρέπει να προσθέσουμε το PC5 στο Vlan10 για να μπορούν να επικοινωνήσουν με τις παρακάτω εντολές στο Switch0:

 # enable

 # conf t

 # int FastEthernet0/5

 # switchport mode access (ορίζεται η πόρτα FE0/5 ως access)

 # switchport access vlan 10 (η πόρτα FE0/5 ανήκει πλέον στο vlan 10)

 # Cntl/Z

 # write

Αν δοκιμάσουμε πάλι το ping από το PC0 θα επιτύχει επειδή οι δυο υπολογιστές βρίσκονται στο vlan 10.

VLAN Assignment

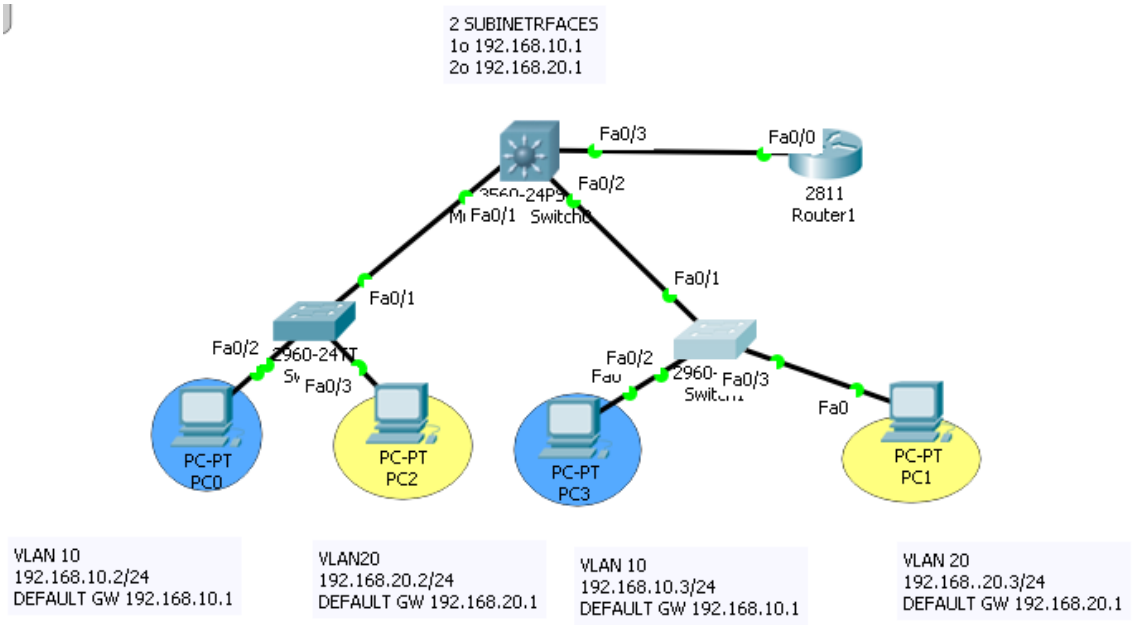
Assigning Ports to VLANs

Cisco Switch IOS Commands	
Enter global configuration mode.	S1 # **configure terminal**
Enter interface configuration mode for the SVI.	S1(config) # **interface** *interface_id*
Configure the management interface IP address.	S1(config) # **ip address 172.17.99.11**
Set the port to access mode.	S1(config-if) # **switchport mode access**
Assign the port to a VLAN.	S1(config-if) # **switchport access vlan** *vlan_id*
Return to the privileged EXEC mode.	S1(config-if) # **end**

Εικόνα 70 : Οι εντολές ανάθεσης θυρών σε VLAN

6.5 Σύνδεση 2 VLAN με Layer3 Switch

Intervlan_layer3.pkt



Εικόνα 71 : Η τοπολογία για το InterVLAN Routing

Για να επικοινωνήσουν υπολογιστές από διαφορετικά VLAN και διαφορετικά δίκτυα πρέπει να χρησιμοποιήσουμε μια layer 3 συσκευή για να κάνει το routing.

Το VLAN λειτουργεί layer 2 ώστε να αποκλείει την επικοινωνία μεταξύ διαφορετικών VLAN.

Χρησιμοποιούμε το layer 3 Switch Cisco 3560 για να επιτύχουμε το intervlan routing.

Χρησιμοποιούμε επίσης 2 switch L2 2960 (24 port 10/100 +2 10/100/1000) καθώς και τέσσερις Προσωπικούς Υπολογιστές PC (PC0, PC1, PC2, PC3) όπως και ένα Δρομολογητή 2811 (Router1) για να επιτύχουμε και επικοινωνία με το L3 switch αξιοποιώντας την δυνατότητα που έχουμε με τα L3 switches να μετατρέπουμε μια L2 θύρα σε L3 και να παίρνει IP διεύθυνση.

Ξεκινάμε τοποθετώντας με τη γνωστή διαδικασία τον εξοπλισμό στην περιοχή του πειράματος.

Στη συνέχεια κάνουμε τις συνδέσεις με ευθεία καλώδια (Straight Through).

Επιλέγουμε το δίκτυο 192.168.10.0/24 και το δίκτυο 192.168.20.0/24 για να δώσουμε διευθύνσεις στις συσκευές.

Στις ρυθμίσεις των τριών υπολογιστών βάζουμε τις παρακάτω διευθύνσεις:

- 192.168.10.2/24 στο PC0 με Default Gateway 192.168.10.1
- 192.168.20.3/24 στο PC1 με Default Gateway 192.168.20.1
- 192.168.20.2/24 στο PC2 με Default Gateway 192.168.20.1

- 192.168.10.3/24 στο PC3 με Default Gateway 192.168.10.1

Πρέπει να δημιουργήσουμε δυο VLAN σε κάθε ένα από τα τρία switch.

Το ένα θα είναι το vlan 10 (μπλέ χρώμα) και το δεύτερο το vlan 20 (κίτρινο χρώμα).

Το vlan 1 ήδη υπάρχει από τον κατασκευαστή και δεν μπορεί να αφαιρεθεί. Η μόνη ρύθμιση που επιτρέπεται σε αυτό είναι να απενεργοποιηθεί (να γίνει shutdown δηλαδή).

Ο προγραμματισμός γίνεται στο global configuration mode του κάθε switch.

Στο Switch0 δίνουμε τις παρακάτω εντολές:

 # enable

 # configure terminal

 # vlan 10

 # vlan 20

 # exit

 # int FastEthernet0/2

 # switchport mode access (ορίζεται η πόρτα FE0/2 ως access)

 # switchport access vlan 10 (η πόρτα FE0/2 ανήκει πλέον στο vlan 10)

 # exit

 # int FastEthernet0/3

 # switchport mode access (ορίζεται η πόρτα FE0/3 ως access)

 # switchport access vlan 20 (η πόρτα FE0/3 ανήκει πλέον στο vlan 20)

 # exit

 # int FastEthernet0/1

 # switchport mode dynamic desirable

 # no shutdown

 # Cntl/Z

 # write

Στο **Switch1** δίνουμε τις παρακάτω εντολές:

 # enable

 # conf t

 # vlan 10

 # vlan 20

 # exit

 # int FastEthernet0/2

 # switchport mode access (ορίζεται η πόρτα FE0/2 ως access)

 # switchport access vlan 10 (η πόρτα FE0/2 ανήκει πλέον στο vlan 10)

 # exit

 # int FastEthernet0/3

 # switchport mode access (ορίζεται η πόρτα FE0/3 ως access)

 # switchport access vlan 20 (η πόρτα FE0/3 ανήκει πλέον στο vlan 20)

 # exit

 # int FastEthernet0/1

 # no shutdown

 # Cntl/Z

 # write

Στο Δρομολογητή (Router1) δίνουμε τις παρακάτω εντολές:

 # enable

 # conf t

 # int FastEthernet0/0

 # ip address 10.10.10.2 255.255.255.0

 # no shutdown

 # ip route 0.0.0.0 0.0.0.0 10.10.10.1

 # Cntl/Z

 # write

Τέλος στο L3 Switch 3560 δίνουμε τις παρακάτω εντολές:

 # enable

 # conf t

 # vlan 10

 # vlan 20

 # ip routing **(ενεργοποιούμε τη δυνατότητα δρομολόγησης)**

 # int FastEthernet0/1

 # switchport trunk encapsulation dot1q

 # switchport mode trunk

 # no shutdown

 # int FastEthernet0/2

 # switchport trunk encapsulation dot1q

 # switchport mode trunk

 # no shutdown

 # int FastEthernet0/3 (ρυθμίζω το interface για το default router)

 # no switchport (για να κάνουμε το Interface L3 capable)

 # ip address 10.10.10.1 255.255.255.0

 # no shutdown

 # interface Vlan10 (ρυθμίζω το vlan interface με την ip address)

 # ip address 192.168.10.1 255.255.255.0

 # interface Vlan20 (ρυθμίζω το vlan interface με την ip address)

 # ip address 192.168.20.1 255.255.255.0

 # ip classless

 # ip route 0.0.0.0 0.0.0.0 10.10.10.2 (ρυθμίζω το default route)

 # exit

 # write

Με την εντολή

 # show ip interface brief βλέπω την κατάσταση των Interfaces

```
Switch#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        10.10.10.1      YES manual up                    up
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  down                  down
FastEthernet0/6        unassigned      YES unset  down                  down
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 192.168.10.1    YES manual up                    up
Vlan20                 192.168.20.1    YES manual up                    up
Switch#
```

Εικόνα 72 : Η καταάσταση των θυρών του L3 Switch

Με την εντολή

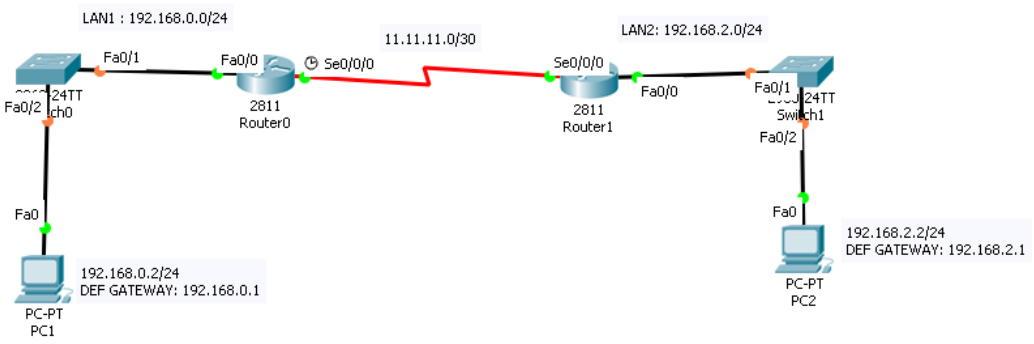
 # show ip route βλέπω το πίνακα δρομολόγησης

```
Switch#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/3
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
S*   0.0.0.0/0 [1/0] via 10.10.10.2
```

Εικόνα 73 : Ο Πίνακας δρομολόγησης του L3 Switch

6.6 Σύνδεση 2 δρομολογητών με στατική δρομολόγηση

Static_route_example1.pkt



Εικόνα 74 : Η τοπολογία για τη εφαρμογή της στατικής δρομολόγησης

Στο παράδειγμα αυτό χρησιμοποιούμε δυο Δρομολογητές 2811 δυο Μεταγωγείς 2960 και δυο Προσωπικούς Υπολογιστές PC για να κάνουμε τον έλεγχο καλής λειτουργίας.

Ξεκινάμε τοποθετώντας με τη γνωστή διαδικασία τον εξοπλισμό στην περιοχή του πειράματος.

Συνδέουμε τους υπολογιστές με τους μεταγωγείς και τους μεταγωγείς με τους δρομολογητές με καλώδια σύνδεσης straight through.

Τους δύο δρομολογητές μεταξύ τους τους συνδέουμε με σειριακή σύνδεση μέσω των interfaces Serial 0/0/0.

Στη συνέχεια επιλέγουμε τα δίκτυα 192.168.0.0/24 και 192.168.2.0/24.

Στις ρυθμίσεις των δυο υπολογιστών βάζουμε την IP διεύθυνση 192.168.0.2/24 με default gateway 192.168.0.1 στο PC1 αριστερό και τη διεύθυνση 192.168.2.2/24 με και default gateway 192.168.2.1 στο PC2.

Πάμε στο πρώτο Δρομολογητή Router 0 και επιλέγουμε το Command Line Interface CLI για να δώσουμε τις παρακάτω εντολές:

Enter

>enable ή εναλλακτικά en

 # configure terminal ή εναλλακτικά conf t για να πάμε σε global config mode

 # interface FastEthernet 0/0

 # ip address 192.168.0.1 255.255.255.0

 # no shutdown

Εδώ ανάβει το πράσινο led στο interface FE0/0

 # exit

 # interface serial0/0/0

 # ip address 11.11.11.1 255.255.255.252 επειδή έχουμε πρόθεμα /30

 # clock rate 128000

 # no shutdown

 # end

 # copy running-config startup-config

Παρατηρούμε ότι δεν ανάβει το πράσινο Led επειδή δεν έχουμε ρυθμίσει τον απέναντι δρομολογητή (Router1)

Πάμε στο δεύτερο Δρομολογητή Router 1

Enter

>enable

 # configure terminal

 # interface FastEthernet 0/0

 # ip address 192.168.2.1 255.255.255.0

 # no shutdown

Εδώ ανάβει το πράσινο led στο interface FE0/0

 # exit

 # interface serial0/0/0

 # ip address 11.11.11.2 255.255.255.252

 # no shutdown (αυτή η πλευρά δεν χρειάζεται clock)

 # end

 # copy running-config startup-config

Εδώ ανάβουν τα πράσινα led σε όλα τα interfaces

Πάμε στο πρώτο PC και από στο Desktop → Command Prompt εκτελούμε τις εντολές για να δούμε τη συνδεσιμότητα:

C:\>ipconfig /all

C:\>ping 192.168.2.2

Η εντολή δεν απαντά επειδή δεν βλέπει το δεύτερο δίκτυο και μπορούμε μόνο να κάνουμε ping στον τοπικό Δρομολογητή Router0.

Για να επιτύχουμε την επικοινωνία πρέπει να προγραμματίσουμε τους 2 Δρομολογητές.

Πάμε στον πρώτο Router0 και δίνουμε τις εντολές:

 # exit

 # ip route 192.168.2.0 255.255.255.0 11.11.11.2

 # show ip route

Πάμε στον δεύτερο Router1 και δίνουμε τις εντολές:

 # exit

 # ip route 192.168.2.0 255.255.255.0 11.11.11.1

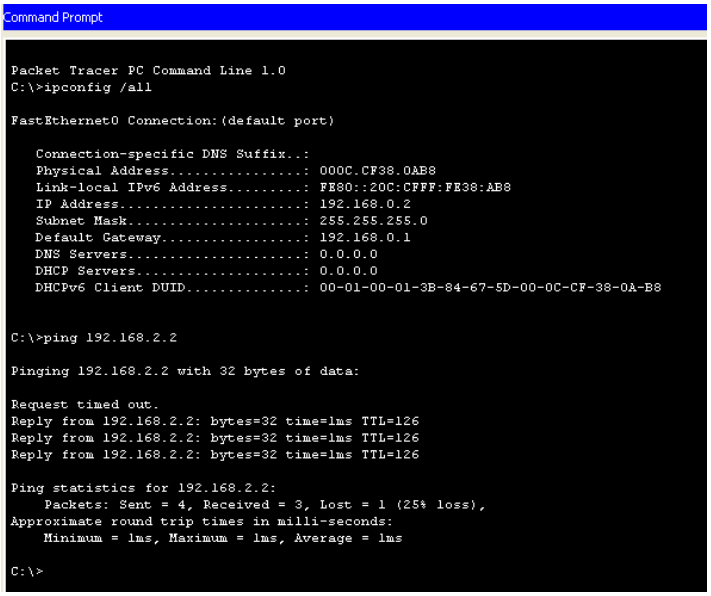
 # show ip route

Πάμε στο πρώτο PC και από στο Desktop → Command Prompt

C:\>ipconfig /all

C:\>ping 192.168.2.2

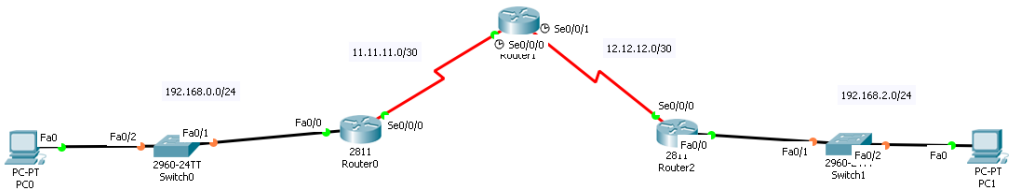
Η εντολή ping απαντά επειδή έχει επιτευχθεί η στατική δρομολόγηση και οι τελικοί υπολογιστές μπορούν πλέον να επικοινωνούν μέσω των Δρομολογητών



Εικόνα 75 : Αποτελέσματα του ipconfig και ping

6.7 Στατική Δρομολόγηση με 3 δρομολογητές

static_route_3R.pkt



Εικόνα 76 : Η τοπολογία για τη στατική δρομολόγηση με 3 δρομολογητές

Στο παράδειγμα αυτό χρησιμοποιούμε τρεις Δρομολογητές 2811 δυο Μεταγωγείς 2960, δυο Προσωπικούς Υπολογιστές PC για να κάνουμε τον έλεγχο καλής λειτουργίας.

Ξεκινάμε τοποθετώντας με τη γνωστή διαδικασία τον εξοπλισμό στην περιοχή του πειράματος.

Στη συνέχεια επιλέγουμε το δίκτυο 192.168.0.0/24, το 192.168.2.0/24, το 11.11.11.0/30 και το 12.12.12.0/30

Στις ρυθμίσεις των δυο υπολογιστών βάζουμε τη διεύθυνση 192.168.0.3/24 στο PC1 και τη διεύθυνση 192.168.2.3/24 στον PC2.

Πάμε στο πρώτο Δρομολογητή Router 0

Enter

>enable

 # configure terminal

 # interface FastEthernet 0/0

 # ip address 192.168.0.1 255.255.255.0

 # no shutdown

 # exit

Εδώ ανάβει το πράσινο led στο interface FE0/0

 # interface serial0/0/0

 # ip address 11.11.11.1 255.255.255.252

 # no shutdown

 # end

 # copy running-config startup-config

Πάμε στο δεύτερο Δρομολογητή Router 2

Enter

>enable

 # configure terminal

 # interface FastEthernet 0/0

 # ip address 192.168.2.1 255.255.255.0

 # no shutdown

 # exit

Εδώ ανάβει το πράσινο led στο interface FE0/0

 # interface serial0/0/0

 # ip address 12.12.12.1 255.255.255.252

 # no shutdown

 # end

 # copy running-config startup-config

Εδώ ανάβει το πράσινο led στο interface FE0/0

Πάμε στον τρίτο Router1 και δίνουμε τις εντολές:

Enter

>enable

 # configure terminal

 # interface serial0/0/0

 # ip address 11.11.11.2 255.255.255.252

 # clock rate 2000000

 # interface serial0/0/1

 # ip address 12.12.12.2 255.255.255.252

 # clock rate 2000000

 # end

 # copy running-config startup-config

Πάμε στο πρώτο PC και από στο Desktop → Command Prompt

C:\>ipconfig /all

C:\>ping 192.168.2.3

Η εντολή δεν απαντά επειδή δεν βλέπει το δεύτερο δίκτυο και μπορούμε μόνο να κάνουμε ping στον τοπικό Δρομολογητή Router0.

Για να επιτύχουμε την επικοινωνία πρέπει να προγραμματίσουμε τους 3 Δρομολογητές όσο αφορά τον τρόπο δρομολόγησης (στατική δρομολόγηση).

Πάμε στον Router0 και δίνουμε τις εντολές:

Enter

>enable

 # configure terminal

 # ip route 0.0.0.0 0.0.0.0 11.11.11.2

 # write

Πάμε στον δεύτερο Router1 και δίνουμε τις εντολές:

Enter

>enable

 # configure terminal

 # ip route 192.168.0.0 255.255.255.0 11.11.11.1

 # ip route 192.168.2.0 255.255.255.0 12.12.12.1

 # write

Πάμε στον Router2 και δίνουμε τις εντολές:

Enter

>enable

 # configure terminal

 # ip route 0.0.0.0 0.0.0.0 12.12.12.2

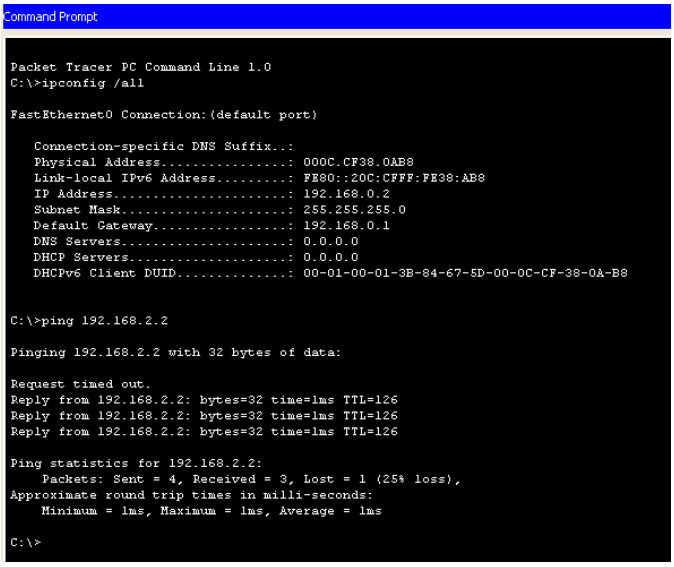
 # write

Πάμε πάλι στο πρώτο PC και από στο Desktop → Command Prompt

C:\>ipconfig /all

C:\>ping 192.168.2.3

Η εντολή ping απαντά επειδή έχει επιτευχθεί η δρομολόγηση και οι τελικοί υπολογιστές μπορούν πλέον να επικοινωνούν μέσω των Δρομολογητών



Εικόνα 77 : Αποτελέσματα του ipconfig και ping από το PC0

Πάμε στο Router1 και δίνουμε τις εντολές:

show ip route (για να δούμε τον πίνακα δρομολόγησης)

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     11.0.0.0/30 is subnetted, 1 subnets
C       11.11.11.0 is directly connected, Serial0/0/0
     12.0.0.0/30 is subnetted, 1 subnets
C       12.12.12.0 is directly connected, Serial0/0/1
S    192.168.0.0/24 [1/0] via 11.11.11.1
S    192.168.2.0/24 [1/0] via 12.12.12.1
```

Εικόνα 78 : Η εντολή show ip route στο Δρομολογητή 1

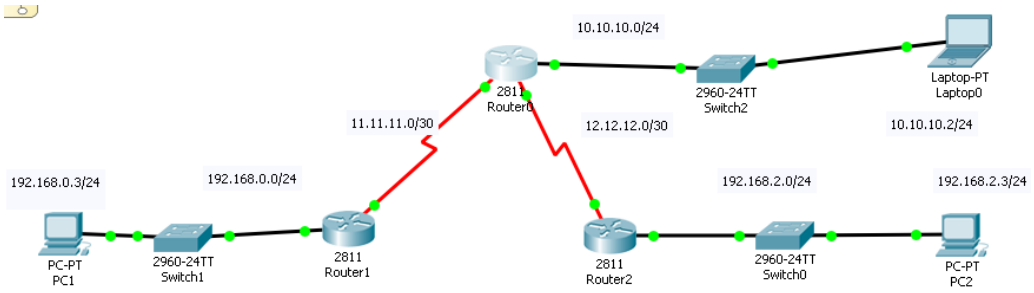
show ip interface brief (για να δούμε την κατάσταση των Interfaces)

```
Router#sh 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
Serial0/0/0            11.11.11.2      YES manual up                    up
Serial0/0/1            12.12.12.2      YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Εικόνα 79 : Η εντολή show ip interface brief στο Δρομολογητή 1

6.8 Δυναμική δρομολόγηση με RIP

rip_route_3R.pkt



Εικόνα 80 : Η τοπολογία για τη δρομολόγηση με RIP

Στο παράδειγμα αυτό χρησιμοποιούμε τρεις Δρομολογητές 2811, τρεις Μεταγωγείς 2960, δυο Προσωπικούς Υπολογιστές PC και ένα φορητό υπολογιστή Laptop για να κάνουμε τον έλεγχο καλής λειτουργίας.

Ξεκινάμε τοποθετώντας με τη γνωστή διαδικασία τον εξοπλισμό στην περιοχή του πειράματος.

Στη συνέχεια επιλέγουμε το δίκτυο 192.168.0.0/24 το 192.168.2.0/24 το 10.10.10.0/24, το 11.11.11.0/30 και το 12.12.12.0/30

Στις ρυθμίσεις των δυο υπολογιστών βάζουμε τη διεύθυνση 192.168.0.3/24 στο PC1 και τη διεύθυνση 192.168.2.3/24 στον PC2.

Πάμε στο πρώτο Δρομολογητή Router 1

Enter

>enable

 # configure terminal

 # interface FastEthernet 0/0

 # ip address 192.168.0.1 255.255.255.0

 # no shutdown

 # exit

Εδώ ανάβει το πράσινο led στο interface FE0/0

 # interface serial0/0/0

 # ip address 11.11.11.1 255.255.255.252

 # clock rate 2000000

 # no shutdown

 # end

 # copy running-config startup-config

Πάμε στο δεύτερο Δρομολογητή Router 2

Enter

>enable

 # configure terminal

 # interface FastEthernet 0/0

 # ip address 192.168.2.1 255.255.255.0

 # no shutdown

 # exit

Εδώ ανάβει το πράσινο led στο interface FE0/0

 # interface serial0/0/0

 # ip address 12.12.12.1 255.255.255.252

 # no shutdown

 # end

 # copy running-config startup-config

Εδώ ανάβει το πράσινο led στο interface FE0/0

Πάμε στο τρίτο Δρομολογητή Router 0

Enter

>enable

 # configure terminal

 # interface FastEthernet 0/0

 # ip address 10.10.10.1 255.255.255.0

 # no shutdown

 # exit

Εδώ ανάβει το πράσινο led στο interface FE0/0

 # interface serial0/0/0

 # ip address 11.11.11.2 255.255.255.252

 # no shutdown

 # exit

 # interface serial0/0/1

 # ip address 12.12.12.2 255.255.255.252

 # end

 # copy running-config startup-config

Εδώ ανάβουν τα πράσινα led σε όλα τα interfaces

Πάμε στο πρώτο PC και από στο Desktop → Command Prompt

C:\>ipconfig /all

C:\>ping 192.168.2.3

Η εντολή δεν απαντά επειδή δεν βλέπει το δεύτερο δίκτυο και μπορούμε μόνο να κάνουμε ping στον τοπικό Δρομολογητή Router1.

Για να επιτύχουμε την επικοινωνία πρέπει να προγραμματίσουμε τους 3 Δρομολογητές για να χρησιμοποιούν δυναμική δρομολόγηση με το πρωτόκολλο RIP και συγκεκριμένα με τη δεύτερη έκδοση RIPv2.

Πάμε στον πρώτο Router1 και δίνουμε την εντολή:

 # router rip

 # version 2

 # network 192.168.0.0

 # network 11.11.11.0

 # no auto-summary (για να διαφημίσει τη μάσκα υποδικτύου)

Πάμε στον δεύτερο Router2 και δίνουμε την εντολή:

 # router rip

 # version 2

 # network 192.168.2.0

 # network 12.12.12.0

 # no auto-summary (για να διαφημίσει τη μάσκα υποδικτύου)

Πάμε στον Router0 και δίνουμε την εντολή:

 # router rip

 # version 2

 # network 10.10.10.0

 # network 11.11.11.0

 # network 12.12.12.0

 # no auto-summary (για να διαφημίσει τη μάσκα υποδικτύου)

Πάμε στο πρώτο PC και από το Desktop → Command Prompt

C:\>ipconfig /all

C:\>ping 192.168.2.3 & στη συνέχεια C:\>ping 192.168.0.3

Η εντολή ping απαντά* επειδή έχει επιτευχθεί η δυναμική δρομολόγηση με το RIP και οι τελικοί υπολογιστές μπορούν πλέον να επικοινωνούν μέσω των Δρομολογητών.

Πάμε στο φορητό υπολογιστή και από στο Desktop → Command Prompt

C:\>ipconfig /all

C:\>ping 192.168.2.3 & στη συνέχεια C:\>ping 192.168.0.3

Η εντολή ping απαντά* επειδή έχει επιτευχθεί η δυναμική δρομολόγηση με το RIP και το φορητό είναι άμεσα συνδεδεμένο με το δρομολογητή Router0 μέσα από το switch2.

*Σημείωση Το πρώτο ping reply χάνεται επειδή πρέπει να υλοποιηθεί το πρωτόκολλο ARP για να μάθει τη MAC address του απέναντι υπολογιστή.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.3: bytes=32 time=1ms TTL=126
Reply from 192.168.0.3: bytes=32 time=1ms TTL=126
Reply from 192.168.0.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Με την εντολή **# show ip route** σε κάθε δρομολογητή βλέπουμε πληροφορίες για τη δρομολόγηση μεταξύ των δικτύων δηλαδή τα δίκτυα με τα οποία έχει συνδεθεί ο δρομολογητή μας και τον τρόπο σύνδεσης. (o=ospf, r=rip, c=directly connected)

Για το router1

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 11.11.11.2 to network 0.0.0.0

     11.0.0.0/30 is subnetted, 1 subnets
C       11.11.11.0 is directly connected, Serial0/0/0
     12.0.0.0/30 is subnetted, 1 subnets
R       12.12.12.0 [120/1] via 11.11.11.2, 00:00:17, Serial0/0/0
C    192.168.0.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/2] via 11.11.11.2, 00:00:17, Serial0/0/0
R*   0.0.0.0/0 [120/1] via 11.11.11.2, 00:00:17, Serial0/0/0

Router#
```

Για το router2

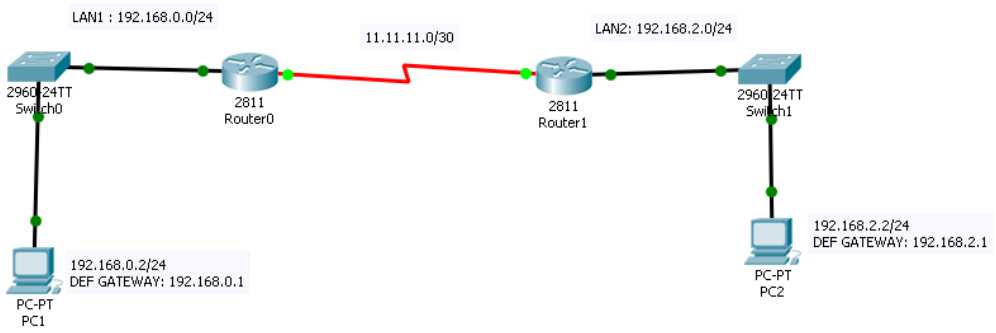
```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 12.12.12.2 to network 0.0.0.0

     11.0.0.0/30 is subnetted, 1 subnets
R       11.11.11.0 [120/1] via 12.12.12.2, 00:00:27, Serial0/0/0
     12.0.0.0/30 is subnetted, 1 subnets
C       12.12.12.0 is directly connected, Serial0/0/0
R    192.168.0.0/24 [120/2] via 12.12.12.2, 00:00:27, Serial0/0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
R*   0.0.0.0/0 [120/1] via 12.12.12.2, 00:00:27, Serial0/0/0

Router#
```

Για το router0

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/0
     11.0.0.0/30 is subnetted, 1 subnets
C       11.11.11.0 is directly connected, Serial0/0/0
     12.0.0.0/30 is subnetted, 1 subnets
C       12.12.12.0 is directly connected, Serial0/0/1
R    192.168.0.0/24 [120/1] via 11.11.11.1, 00:00:24, Serial0/0/0
R    192.168.2.0/24 [120/1] via 12.12.12.1, 00:00:11, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 10.10.10.2

Router#
```

6.9 Δυναμική δρομολόγηση με OSPF

ospf_example.pkt



Εικόνα 81 : Η τοπολογία για τη δρομολόγηση με OSPF

Στο παράδειγμα αυτό χρησιμοποιούμε δυο Δρομολογητές 2811 δυο Μεταγωγείς 2960 και δυο Προσωπικούς Υπολογιστές PC για να κάνουμε τον έλεγχο καλής λειτουργίας.

Ξεκινάμε τοποθετώντας με τη γνωστή διαδικασία τον εξοπλισμό στην περιοχή του πειράματος.

Στη συνέχεια επιλέγουμε το δίκτυο 192.168.0.0/24 το 192.168.2.0/24 και το δίκτυο 11.11.11.0/30.

Στις ρυθμίσεις των δυο υπολογιστών βάζουμε τη διεύθυνση 192.168.0.2/24 με DG 192.168.0.1 στο PC1 και τη διεύθυνση 192.168.2.2/24 με DG 192.168.2.1 στον PC2.

Πάμε στο πρώτο Δρομολογητή Router 0

Enter

>enable

 # configure terminal

 # interface FastEthernet 0/0

 # ip address 192.168.0.1 255.255.255.0

 # no shutdown

 # exit

Εδώ ανάβει το πράσινο led στο interface FE0/0

 # interface serial0/0/0

 # ip address 11.11.11.1 255.255.255.252

 # clock rate 2000000

 # no shutdown

 # end

 # copy running-config startup-config

Πάμε στο δεύτερο Δρομολογητή Router 1

Enter

>enable

 # configure terminal

 # interface FastEthernet 0/0

 # Ip address 192.168.2.1 255.255.255.0

 # no shutdown

 # exit

Εδώ ανάβει το πράσινο led στο interface FE0/0

 # interface serial0/0/0

 # ip address 11.11.11.2 255.255.255.252

 # no shutdown

 # end

 # copy running-config startup-config

Εδώ ανάβει το πράσινο led στο interface FE0/0

Πάμε στο πρώτο PC και από στο Desktop → Command Prompt

C:\>ipconfig /all

C:\>ping 192.168.2.2

Η εντολή δεν απαντά επειδή δεν βλέπει το δεύτερο δίκτυο και μπορούμε μόνο να κάνουμε ping στον τοπικό Δρομολογητή Router1.

Για να επιτύχουμε την επικοινωνία πρέπει να προγραμματίσουμε τους δυο Δρομολογητές για να χρησιμοποιούν δυναμική δρομολόγηση με το πρωτόκολλο OSPF.

Πάμε στον πρώτο **Router0** και δίνουμε την εντολή:

 # router ospf 1 (το 1 είναι το process ID)

 # router-id 1.1.1.1 (το router-id ανταλλάσσεται στο hello packet του OSPF)

 # network 192.168.0.0 0.0.0.255 area 0 (το 0.0.0.255=wildcard είναι το ανάποδο του netmask)

 # network 11.11.11.0 0.0.0.3 area 0

 # do write

Πάμε στον δεύτερο **Router1** και δίνουμε την εντολή:

 # router ospf 1

 # router-id 2.2.2.2

 # network 192.168.2.0 0.0.0.255 area 0

 # network 12.12.12.0 0.0.0.3 area 0

 # do write

Περιμένουμε λίγο για να τρέξει το πρωτόκολλο και να δούμε ότι οι δρομολογητές συνδέονται.

Με την παρακάτω εντολή :

 # show ip ospf neighbor

βλέπουμε το router ID του απέναντι router όπως παρακάτω:

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address
Interface
2.2.2.2           0   FULL/  -        00:00:30    11.11.11.2
Serial0/0/0
Router#
```

Με την παρακάτω εντολή :

 # no router rip

βγάζουμε το πρωτόκολλο rip αν έχει μείνει από προηγούμενη εγκατάσταση όπως εδώ.

Με την παρακάτω εντολή :

 # show ip route

βλέπουμε τα δίκτυα με τα οποία έχει συνδεθεί ο δρομολογητή μας και τον τρόπο σύνδεσης. (o=ospf, r=rip, c=directly connected)

Στο Router0 βλέπουμε τα παρακάτω:

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     11.0.0.0/30 is subnetted, 1 subnets
C       11.11.11.0 is directly connected, Serial0/0/0
C    192.168.0.0/24 is directly connected, FastEthernet0/0
O    192.168.2.0/24 [110/65] via 11.11.11.2, 00:13:50, Serial0/0/0

Router#
```

Στο Router1 βλέπουμε τα παρακάτω:

```
Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     11.0.0.0/30 is subnetted, 1 subnets
C       11.11.11.0 is directly connected, Serial0/0/0
O    192.168.0.0/24 [110/65] via 11.11.11.1, 00:11:03, Serial0/0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0

Router#
```

Πάμε στο πρώτο PC και από στο Desktop → Command Prompt

C:\>ipconfig /all

C:\>ping 192.168.2.2

Η εντολή ping απαντά* επειδή έχει επιτευχθεί η δυναμική δρομολόγηση με το OSPF και οι τελικοί υπολογιστές μπορούν πλέον να επικοινωνούν μέσω των Δρομολογητών.

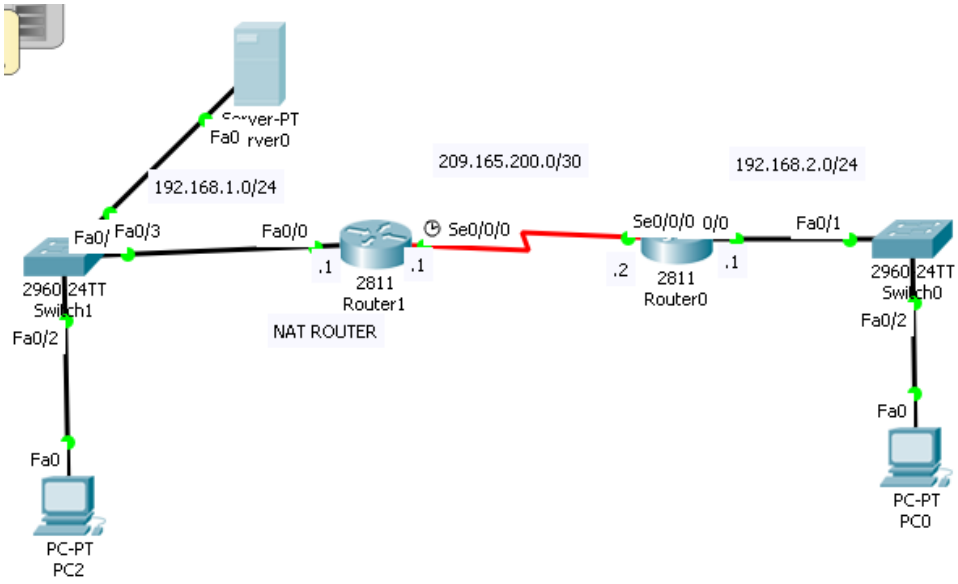
*Σημείωση Το πρώτο ping reply χάνεται επειδή πρέπει να υλοποιηθεί το πρωτόκολλο ARP για να μάθει τη MAC address του απέναντι υπολογιστή.

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

6.10 Υλοποίηση του πρωτοκόλλου NAT

nat.pkt



Εικόνα 82 : Η τοπολογία για το πρωτόκολλο NAT

Στο παράδειγμα αυτό χρησιμοποιούμε δυο Δρομολογητές 2811 δυο Μεταγωγείς 2960, ένα Υπολογιστή ρυθμισμένο ως Web Server και δυο Προσωπικούς Υπολογιστές PC για να κάνουμε τον έλεγχο καλής λειτουργίας.

Ξεκινάμε τοποθετώντας με τη γνωστή διαδικασία τον εξοπλισμό στην περιοχή του πειράματος.

Στη συνέχεια επιλέγουμε το δίκτυο 192.168.1.0/24 το 192.168.2.0/24 και το δίκτυο 209.165.200.0/30.

Στις ρυθμίσεις των δυο υπολογιστών βάζουμε τη διεύθυνση 192.168.2.2/24 με DG 192.168.2.1 στο PC0 και τη διεύθυνση 192.168.1.2/24 με DG 192.168.1.1 στο PC2.

Στον υπολογιστή Server-PT βάζουμε τη διεύθυνση 192.168.1.3/24 με DG 192.168.1.1

Πάμε στο πρώτο Δρομολογητή **Router1**

Enter

>enable

 # configure terminal

 # interface FastEthernet 0/0

 # ip address 192.168.1.1 255.255.255.0

 # no shutdown

 # exit

Εδώ ανάβει το πράσινο led στο interface FE0/0

 # interface serial0/0/0

 # ip address 209.165.200.1 255.255.255.252

 # clock rate 2000000

 # no shutdown

 # exit

 # ip route 192.168.2.0 255.255.255.0 209.165.200.2

 # copy running-config startup-config

Πάμε στο δεύτερο Δρομολογητή **Router0**

Enter

>enable

 # configure terminal

 # interface FastEthernet 0/0

 # ip address 192.168.2.1 255.255.255.0

 # no shutdown

 # exit

Εδώ ανάβει το πράσινο led στο interface FE0/0

 # interface serial0/0/0

 # ip address 209.165.200.2 255.255.255.252

 # no shutdown

 # exit

 # ip route 192.168.1.0 255.255.255.0 209.165.200.1

 # copy running-config startup-config

Πάμε πάλι στο πρώτο Δρομολογητή **Router1** για να ρυθμίσουμε το NAT

 # interface FastEthernet 0/0

 # ip nat inside

 # interface serial 0/0/0

 # ip nat outside

 # exit (για να φύγω από το IF config και να γυρίσω στο global config)

 # access-list 1 permit 192.168.1.0 0.0.0.255

 # ip nat inside source list 1 interface 192.168.1.0 0.0.0.255 overload (ώστε να μεταφράζονται όλες οι διευθύνσεις του δικτύου 192.168.1.0 με την IP διεύθυνση του serial 0/0/0 (209.165.200.1) και στην ουσία γίνεται Port Address Translation)

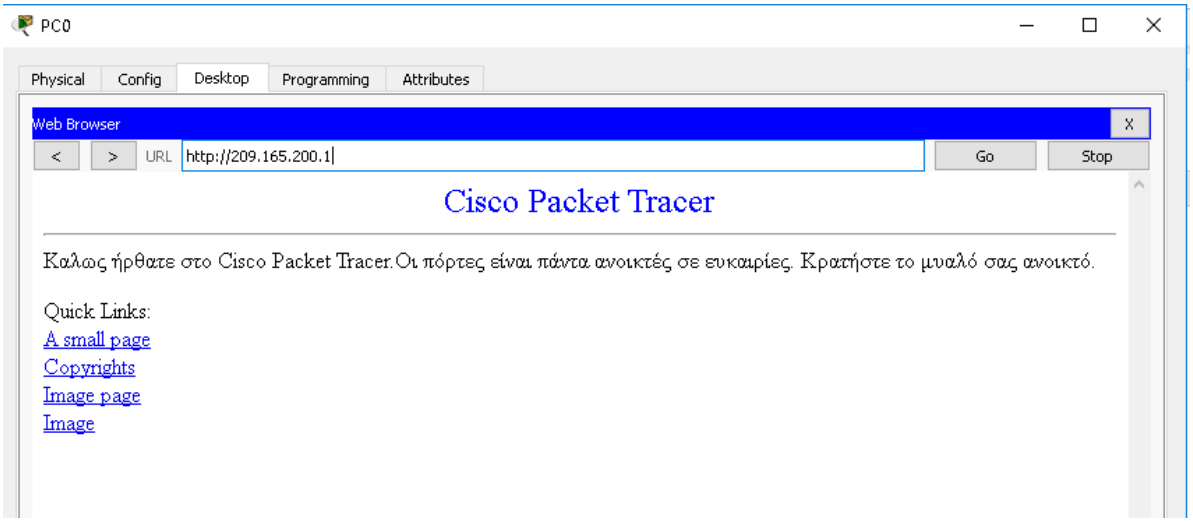
Με την εντολή

 # ip nat inside source static tcp 192.168.1.3 80 209.165.200.1 80 για να δούμε από εξωτερικό δίκτυο το webserver (port 80) που έχει IP 192.168.1.3 (εσωτερική).

Δοκιμή από εξωτερικό PC (πχ PC0) για το Web Server. Από την επιλογή PC0→ Desktop → Command Prompt εκτελώ την παρακάτω εντολή:

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 209.165.200.1: bytes=32 time=1ms TTL=126
Reply from 209.165.200.1: bytes=32 time=1ms TTL=126
Reply from 209.165.200.1: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Και στη συνέχεια από τον Web Browser του PC0 συνδέομαι στη διεύθυνση του Web Server που τώρα έχει μεταφραστεί στην **209.165.200.1:80**



Εικόνα 83 : Σύνδεση στην θύρα του Web Server από το PC0

Με την παρακάτω εντολή στο Router1

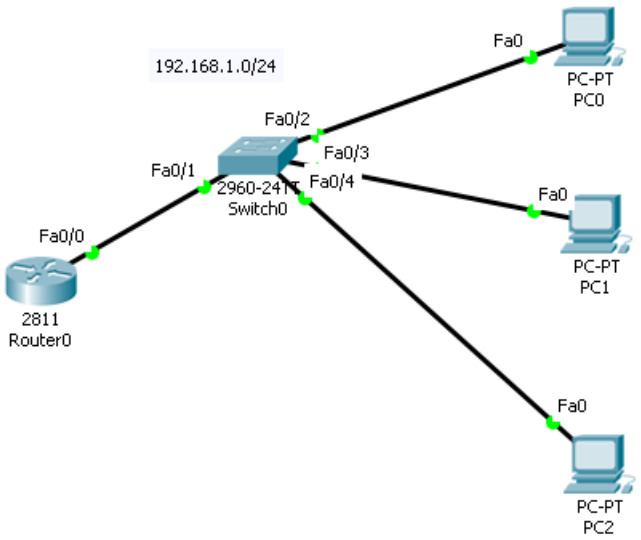
 # show ip nat translation (βλέπω τη μετάφραση μετά από αντίστοιχη κίνηση στο δίκτυο)

```
Router#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 209.165.200.1:80   192.168.1.3:80     ---                ---

Router#
```

Εικόνα 84 : Εμφάνιση της αντιστοίχισης του πρωτοκόλλου NAT

6.11 Υλοποίηση του πρωτοκόλλου DHCP

dhcpv4.pkt



Εικόνα 85 : Η τοπολογία για το πρωτόκολλο DHCP

Στο παράδειγμα αυτό χρησιμοποιούμε ένα Δρομολογητή 2811 ένα Μεταγωγέα 2960 και τρεις Προσωπικούς Υπολογιστές PC για να κάνουμε τον έλεγχο καλής λειτουργίας.

Ξεκινάμε τοποθετώντας με τη γνωστή διαδικασία τον εξοπλισμό στην περιοχή του πειράματος.

Στη συνέχεια επιλέγουμε το δίκτυο 192.168.1.0/24.

Στις ρυθμίσεις των δυο υπολογιστών βάζουμε τη διεύθυνση 192.168.0.2/24 στο PC1 τη διεύθυνση 192.168.2.2/24 στον PC2 και τη διεύθυνση 192.168.3.2 στο PC3.

Πάμε στο Δρομολογητή **Router0** για να ξεκινήσουμε το προγραμματισμό του

Enter

>enable

 # configure terminal

 # interface FastEthernet 0/0

 # ip address 192.168.0.1 255.255.255.0

 # no shutdown

 # exit

Εδώ ανάβει το πράσινο led στο interface FE0/0 και συνεχίζουμε τις εντολές για την ενεργοποίηση και ρύθμιση του DHCP:

 # ip dhcp excluded-addresses 192.168.1.1 192.168.1.10 (εξαιρούμε αυτές τις διευθύνσεις από την αυτόματη απόδοση με DHCP)

 # ip dhcp pool lan

 # network 192.168.1.0 255.255.255.0

 # default-router 192.168.1.1 (ορίζουμε ποιο θα είναι το DG στα PC που θα πάρουν διευθύνσεις με το DHCP)

 # dns-server 212.205.212.205 (ορίζουμε ποιο θα είναι το DNS Server στα PC που θα πάρουν διευθύνσεις με το DHCP)

 # write

 # copy running-config startup-config

Πάμε στο πρώτο PC και από στο Desktop → Command Prompt

C:\>ipconfig /all

C:\>ping 192.168.2.2

C:\>ping 192.168.3.2

Η εντολή δεν απαντά επειδή οι 3 υπολογιστές δεν βρίσκονται στο ίδιο δίκτυο και μπορούμε μόνο να κάνουμε ping στον εαυτό μας (localhost 127.0.0.1).

Για να επιτύχουμε την επικοινωνία πρέπει να προγραμματίσουμε τους τρεις υπολογιστές για να μπορούν να παίρνουν αυτόματα διευθύνσεις, μάσκα, έξοδο διαφυγής και primary DNS server αυτόματα με το πρωτόκολλο DHCP.

Πρέπει να πάμε σε κάθε PC και στην κάρτα δικτύου του να του ενεργοποιήσουμε το DHCP. Στη συνέχεια ξαναδίνουμε τις παρακάτω εντολές:

C:\>ipconfig /all

C:\>ping 192.168.2.2

C:\>ping 192.168.3.2

Αν όλα είναι καλά η επικοινωνία μας έχει επιτευχθεί.

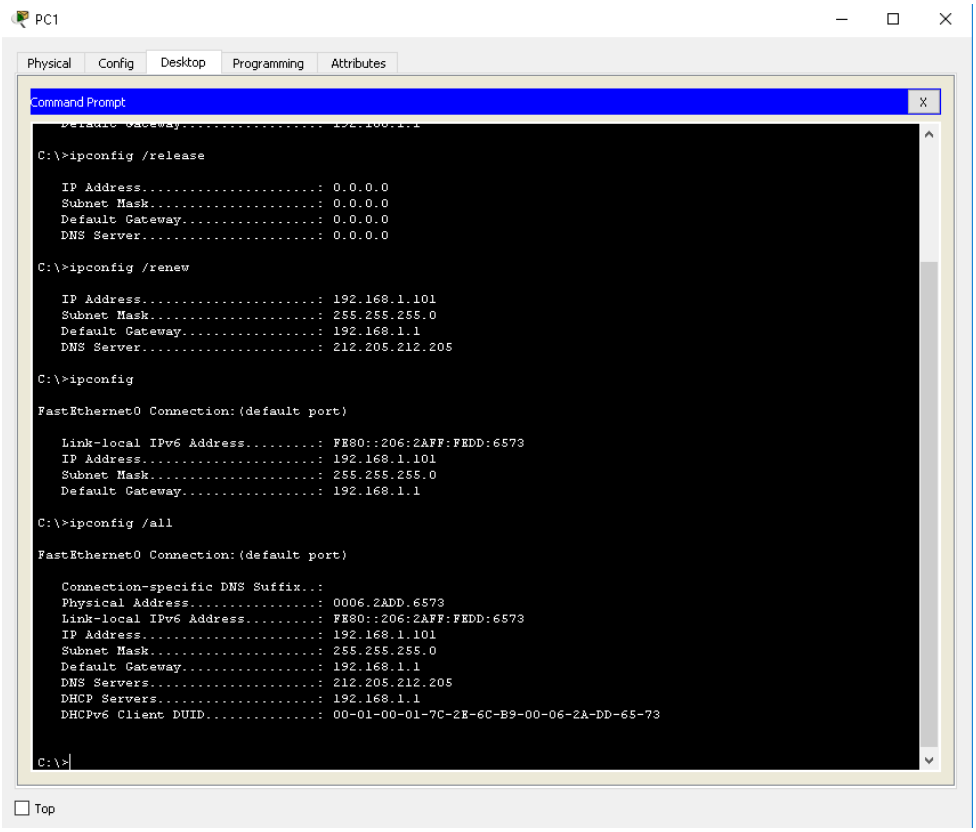
Μπορούμε να αλλάξουμε το DHCP pool και με τις εντολές ipconfig /release και ipconfig/renew να αναγκάσουμε τον DHCP server να μας δώσει νέες διευθύνσεις από τη νέα δεξαμενή διευθύνσεων (dhcp ip pool).

Για παράδειγμα με την εντολή

 # ip dhcp excluded-addresses 192.168.1.1 192.168.1.100

Στο Router θα δώσουμε εντολή στον DHCP να δίνει διευθύνσεις από .101 και πάνω.

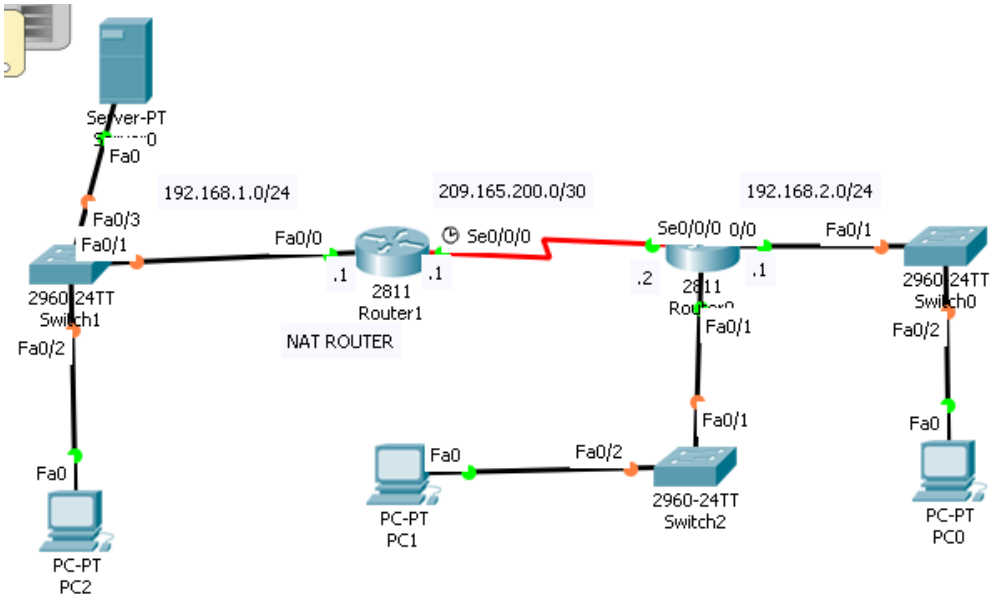
Είτε με release & renew είτε με αλλαγή από DHCP σε Static και ανάποδα οι τρεις υπολογιστές παίρνουν νέες διευθύνσεις από το νέο pool που είναι .101 ως .254



Εικόνα 86 : Απελευθέρωση και ανανέωση IP διευθύνσεων

6.12 Υλοποίηση Access List σε δίκτυο

Acl.pkt



Εικόνα 87 : Η τοπολογία για την υλοποίηση Access List σε δίκτυο

Στο παράδειγμα του NAT (video10) προσθέτω ένα νέο δίκτυο το 192.168.3.0/24 με ένα μεταγωγέα 2960-24 και ένα PC (PC1).

Πηγαίνω στον πρώτο δρομολογητή (router 1) και προσθέτω την access list που απαγορεύει το δίκτυο 192.168.3.0/24

 # conf t

 # accesslist 2 deny 192.168.3.0 0.0.0.255

 # accesslist 2 permit any

 # interface serial 0/0/0

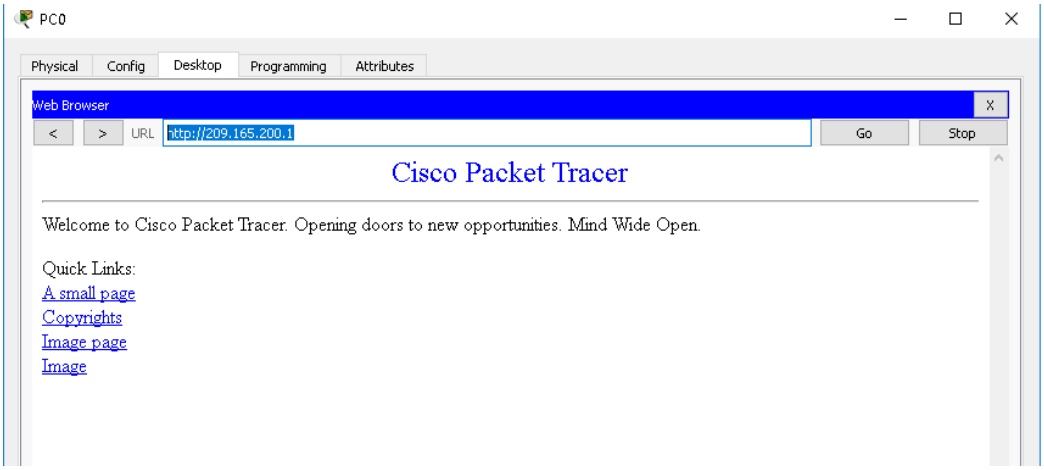
 # ip access-group 2 in

 # write

Δοκιμάζω από web browser των δυο PC να μπω στο web server.

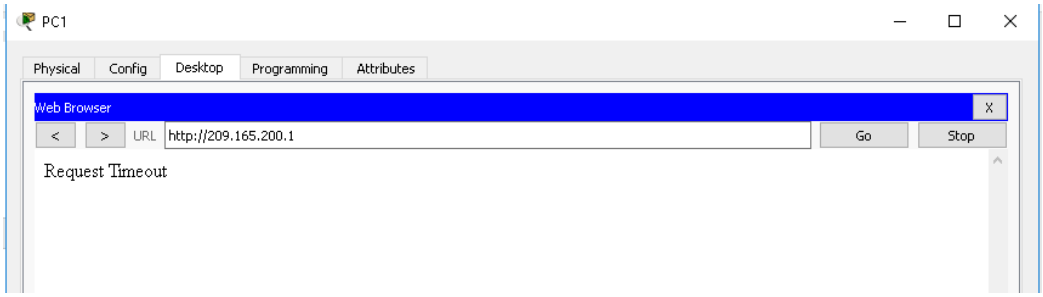
Το ένα PC συνδέεται ενώ το δεύτερο δεν του επιτρέπεται η σύνδεση λόγω του περιορισμού που εισαγάγαμε με την access list.

Από το PC0 συνδέεται



Εικόνα 88 : Η σύνδεση στο Web Server από το PC0

Από το PC1 δεν συνδέεται



Εικόνα 89 : Η αποτυχία σύνδεσης στο Web Server από το PC1

ΚΕΦΑΛΑΙΟ 7 Επίλογος Συμπεράσματα

Σε αυτό το κεφάλαιο αναφέρονται τα συμπεράσματα από την πορεία ανάπτυξης και θα γίνουν μερικές προτάσεις για την επέκταση της εργασίας.

Η τεχνολογία στον χώρο των επικοινωνιών προχωράει αλματωδώς και κάθε νέα εφαρμογή, κάθε νέα εφεύρεση, κάθε νέο project αποτελούν ισχυρά μέσα για την εκπλήρωση του σκοπού αυτού. Η μελέτη και εφαρμογή των δρομολογητών δικτύων (Network Routers) και των αντιστοίχων πρωτοκόλλων δρομολόγησης αντιπροσωπεύουν ένα ακόμη δείγμα της ακάθεκτης και συνεχώς επιταχυνόμενης προόδου στον τομέα αυτό.

Κατά το σχεδιασμό ενός συστήματος, θα πρέπει η προτεινόμενη λύση να προσομοιώνεται, έτσι ώστε να αντιμετωπίζονται τυχόν προβλήματα που προκύπτουν. Με βάση την εφαρμογή στα πλαίσια της εργασία σαν καλή πρακτική είναι προτιμότερο να διαχωρίζεται η προτεινόμενη λύση σε στάδια εφαρμογής, καθώς έτσι είναι πιο εύκολη η απομόνωση και ο εντοπισμός ενός προβλήματος που μπορεί να εμφανιστεί σε μια εφαρμογή.

Επομένως, είναι αναμφισβήτητα πολύ σημαντικό να μας παρέχεται η δυνατότητα να μπορούμε να ελέγξουμε ένα δίκτυο πριν την υλοποίησή του, σε ένα εικονικό περιβάλλον.

Όπως ήδη περιγράφηκε εκτενώς, στη διπλωματική εργασία χρησιμοποιήσαμε ως λογισμικό προσομοίωσης το Cisco Packet Tracer, προκειμένου να παραμετροποιήσουμε εικονικά τις συσκευές του δικτύου μας και να μελετήσουμε συνολικά τη λειτουργία του δικτύου.

Το λογισμικό αυτό μπορεί να λειτουργεί σε διαφορετικές πλατφόρμες –στην εργασία αυτή χρησιμοποιήθηκε η αγγλική cross platform το δε γραφικό περιβάλλον του, δίνει τη δυνατότητα να προσθέσουμε και να αφαιρέσουμε συσκευές δικτύου κατά βούληση. Στη διπλωματική μας, παραμετροποιήθηκαν και χρησιμοποιήθηκαν διαφορετικές συσκευές δικτύου, οι οποίες εντάχθηκαν στις τοπολογίες δικτύων που επιλέχθηκαν και υλοποιήθηκαν.

Μετά την εγκατάσταση και τη ρύθμιση των συσκευών, έγιναν οι δοκιμές τόσο σε πραγματικό χρόνο (real time), όσο και σε περιβάλλον προσομοίωσης (simulation), με τα μέρη του δικτύου να ανταλλάσσουν πακέτα δεδομένων, στα πλαίσια των λειτουργιών που ανατέθηκαν. Οι έλεγχοι του δικτύου τόσο σε πραγματικό χρόνο, όσο και στο περιβάλλον προσομοίωσης είναι πανομοιότυποι και είναι στην ευχέρεια του χρήστη επιλέξει τον τρόπο με τον οποίο θα εξετάσει το δίκτυο που έχει υλοποιήσει. Στις προσομοιώσεις μας παρουσιάσαμε και τους δύο παραπάνω τρόπους για λόγους παρουσίασης των δυνατοτήτων του εργαλείου προσομοίωσης που χρησιμοποιήσαμε, καθώς και

για λόγους ποικιλομορφίας στην παρουσίαση των αποτελεσμάτων. Το Cisco Packet Tracer μας έδωσε τη δυνατότητα να παρακολουθήσουμε και να εξετάσουμε τη δρομολόγηση και τη δομή των πακέτων σε κάθε λεπτομέρεια, και να αντιμετωπίσουμε τυχόν προβλήματα που προέκυπταν.

Συμπερασματικά, το Cisco Packet Tracer είναι ένα ισχυρό πρόγραμμα προσομοίωσης δικτύου, ένα σημαντικό συμπληρωματικό βοήθημα, που επιτρέπει στους χρήστες:

- να δημιουργήσουν ένα δίκτυο με σχεδόν απεριόριστο αριθμό συσκευών,
- να πειραματιστούν με τη συμπεριφορά του δικτύου,
- να εκτελέσουν προμελετημένα σενάρια σε πραγματικό χρόνο (real time), αλλά και με ελεγχόμενο τρόπο (simulation mode),
- να πραγματοποιήσουν παρατηρήσεις στα γεγονότα που συμβαίνουν στο δίκτυο, με δυνατότητα χρήσης φίλτρων για παρατηρήσεις εξειδικευμένων συμβάντων,
- να εντοπίσουν τυχόν σφάλματα στο δίκτυο που έχουν δημιουργήσει στο περιβάλλον του Cisco Packet Tracer, να τα ελέγξουν εξονυχιστικά και να τα αντιμετωπίσουν πριν την υλοποίηση του πραγματικού δικτύου, στο οποίο ο εντοπισμός σφαλμάτων θα αποτελούσε μια χρονοβόρα διαδικασία.

Γενικότερα, το λογισμικό αυτό δίνει τη δυνατότητα εξοικειωσης με τα δίκτυα υπολογιστών. Πιο συγκεκριμένα με τη δημιουργία διαφορετικών τοπολογιών δικτύων, χρησιμοποιώντας τον εξοπλισμό της Cisco, μπορεί να μελατηθεί λεπτομερώς η δικτυακή λειτουργία. Για το λόγο αυτό χρησιμοποιώντας το λογισμικό αυτό δημιουργήσαμε αρχικά ένα μικρό δίκτυο (1η προσομοίωση) για να εστιάσουμε και να κατανοήσουμε τη λειτουργία ενός Μεταγωγέα ή ενός Δρομολογητή και στη συνέχεια να χτίσουμε σταδιακά μεγαλύτερα δίκτυα με επιμέρους χαρακτηριστικά, να τα παραμετροποιήσουμε ώστε να λειτουργούν σωστά. Ελέγχθηκε εξονυχιστικά η ορθή λειτουργία του δικτύου, σε κάθε πείραμα που δημιουργήσαμε. Αποδείχτηκε ότι το λογισμικό αυτό είναι εύκολο στη χρήση και εξυπηρετεί το σκοπό του φτάνει ο χρήστης να είναι εξοικειωμένος με τις διαδικτυακές τεχνολογίες επικοινωνίας.

Κλείνοντας, θα θέλαμε να τονίσουμε ότι οι Δρομολόγητές αποτελούν το παρόν και το μέλλον των δικτύων, αφού η εφαρμογή τους ερευνάται και εξελίσσεται σε παγκόσμια κλίμακα στο χώρο των δικτύων. Από τη μεριά τους οι πάροχοι πρόσβασης υπηρεσιών Διαδικτύου φροντίζουν επισταμένα για την υποστήριξη, την επέκταση και τη συνεχή διαθεσιμότητα της Δρομολογητών ώστε να είναι το Διαδίκτυο πάντα διαθέσιμο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Άρης Αλεξόπουλος - Γιώργος Λαγογιάννης Τηλεπικοινωνίες και Δίκτυα Υπολογιστών 10η Εκδοση, Εκδόσεις Γιαλός 2016.

[2] A. S. Tanenbaum, Δίκτυα Υπολογιστών, Τέταρτη Αμερικάνικη Έκδοση, Εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ, 2007.

[3] Todd Lammle, CCNA Routing and Switching Complete Study Guide, Second Edition, Sybex A Wiley Brand, 2016.

[4] Wendell Odom, CCNA Routing and Switching 200-125 Official Cert Guide Library, Cisco Press, 2016

[5] Routing and Switching Essentials Companion Guide, Cisco Press, 2014

[6] KUROSE ROSS, Computer Networking A Top-Down Approach, ‘Εκτη Αμερικάνικη Έκδοση, Εκδόσεις PEARSON, 2013.

[7] Charles E. Spurgeon & Joann Zimmerman: Ethernet The Definitive Guide, Second Edition, O’Reilly Media Inc, 2014.

[8] Douglas E. Comer: Διαδίκτυα με TCP/IP αρχές, πρωτόκολλα και αρχιτεκτονικές, (4η έκδοση). Αθήνα: Κλειδάριθμος, 2001.

[9] «Wikipedia: TCP/IP,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/TCP/IP. [Πρόσβαση 27 1 2018].

[10] https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/RPVSpanningTree.pdf

[11] «Wikipedia: Διεύθυνση_IP,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/Διεύθυνση_IP. [Πρόσβαση 30 01 2018].