ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΔΙΟΙΚΗΤΙΚΗΣ ΜΕΤΑΡΡΥΘΜΙΣΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΥΠΟΕΡΓΟ: «ΔΗΜΙΟΥΡΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΥΛΙΚΟΥ ΠΡΟΓΡΑΜΜΑΤΩΝ ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΤΟΥ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ ΤΗΣ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΒΑΣΕΙ ΣΧΕΔΙΩΝ ΕΚΠΑΙΔΕΥΣΗΣ»

ΤΙΤΛΟΣ ΠΡΟΓΡΑΜΜΑΤΟΣ: «Τεχνολογίες και Διαχείριση Δικτύων»

ΕΚΠΑΙΔΕΥΤΙΚΟ ΥΛΙΚΟ

Κωδικός Πιστοποίησης προγράμματος: 183

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

2007-2013 Ε.Π. ΔΙΟΙΚΗΤΙΚΗ ΜΕΤΑΡΡΥΘΜΙΣΗ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

ΥΠΟΕΡΓΟ: «ΔΗΜΙΟΥΡΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΥΛΙΚΟΥ ΠΡΟΓΡΑΜΜΑΤΩΝ ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΤΟΥ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ ΤΗΣ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΒΑΣΕΙ ΣΧΕΔΙΩΝ ΕΚΠΑΙΔΕΥΣΗΣ»

ΤΙΤΛΟΣ ΠΡΟΓΡΑΜΜΑΤΟΣ:
«Τεχνολογίες και Διαχείριση Δικτύων»

ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ

Μέλη Ομάδας

Συντονιστής:
Δρ. Ζούλιας Εμμανουήλ, Στέλεχος Ε.Κ.Δ.Δ.Α.

Συντάκτες:
Δρ. Κεφαλληνός Διονύσιος, Στέλεχος Γ.Γ.Π.Σ.

Δρ. Παπαμιχαήλ Γεώργιος, Προϊστάμενος Τμήματος Συντονισμού ΙΝ.ΕΠ.

Δαγιακίδης Μιχαήλ, Στέλεχος Ι.Κ.Α.

ΚΕΝΗ ΠΡΩΤΗ ΣΕΛΙΔΑ

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ ΣΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ - ΤΟΠΟΛΟΓΙΕΣ ΚΑΙ ΚΑΛΩΔΙΩΣΗ 8

1.1 Τα Δικτυα Δεδομενων στη ζωη μας 8
1.2 Απο τι αποτελειται ενα Δικτυο 9
1.3 Ειδη Δικτυων / Τοπολογιες 10
1.4 Τεχνικες και μεσα μεταδοσης 12
1.5 Δομημενη Καλωδιωση 15
1.6 Συνδεοντας LANs και WANs 15

2. ΔΙΚΤΥΑΚΕΣ ΣΥΣΚΕΥΕΣ ΚΑΙ ΜΟΝΤΕΛΟ OSI 17

2.1 Το μοντελο αναφορας OSI 17
2.2 Δικτυακες Συσκευες 21

3. ΤΑ ΠΡΩΤΟΚΟΛΛΑ TCP/IP, ARP/RARP 24

3.1 Το μοντελο αναφορας TCP/IP 24
3.2 Διευθυνσεις IP 26
3.3 Αναθεση IP διευθυνσεων, τα πρωτοκολλα ARP / RARP 28
3.4 Διαγνωστικα εργαλεια του TCP/IP, το ICMP 29

4 ΥΠΟΔΙΚΤΥΩΣΗ, SUBNETTING 31

4.1 Τι ειναι η υποδικτυωση 31
4.2 Προεπιλεγμενες και προσαρμοσμενες μασκες 31
4.3 Διευθυνσεις δικτυου και ευρυεκπομπης 32
4.4 Υποδικτυωση με μασκες διαφορετικου μηκους 32

5 ΕΙΣΑΓΩΓΗ ΣΤΟΥΣ ΔΡΟΜΟΛΟΓΗΤΕΣ 34

5.1 Ο δρομολογητης ειναι ενας υπολογιστης 34
5.2 Μεταφεροντας πακετα απο ακρο σε ακρο 35
5.3 Εκκινηση του δρομολογητη 37
5.3 Βασικη ρυθμιση δρομολογητη 39
5.4 Επιβεβαιωση, εντολες #show 42

6 ΔΡΟΜΟΛΟΓΗΣΗ 46

6.1 Τι ειναι η δρομολογηση 46
6.2 Στατικοι δρομοι 47
6.3 Δυναμικη δρομολογηση και Πρωτοκολλα 49

7. ΠΡΩΤΟΚΟΛΛΑ ΔΡΟΜΟΛΟΓΗΣΗΣ RIP, OSPF ΚΑΙ EIGRP 52

7.1 Χαρακτηριστικα του πρωτοκολλου RIP 52
7.2 Ρυθμιση του πρωτοκολλου RIP 54
7.3 Έλεγχος ορθης λειτουργιας του RIP 55
7.4 Χαρακτηριστικα του πρωτοκολλου EIGRP 58
7.5 Λειτουργια του EIGRP 58
7.6 Ρυθμιση και ελεγχος του EIGRP 61
7.7 Χαρακτηριστικα του πρωτοκολλου OSPF 66
7.8 Λειτουργια του OSPF 68

7.9 Ρυθμιση και ελεγχος του OSPF 69
7.10 Εργαστηριακη Άσκηση EIGRP 74
7.11 Εργαστηριακη Άσκηση OSPF 76

8. ΛΙΣΤΕΣ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ 77

8.1 Ανασκοπηση των λιστων ελεγχου προσβασης 77
8.2 Βασικη ρυθμιση 78
8.3 Τυποι λιστων ελεγχου προσβασης 81
8.4 Τοποθετηση και παραδειγματα χρησης των λιστων ελεγχου προσβασης 84

9. ΕΙΣΑΓΩΓΗ ΣΤΟΥΣ ΜΕΤΑΓΩΓΕΙΣ 89

9.1 Απο τα hubs, στις γεφυρες, στους μεταγωγεις 89
9.2 Βασικες λειτουργιες μεταγωγεων 92
9.3 Εκκινηση Μεταγωγεα 97
9.4 Βασικη ρυθμιση μεταγωγεα 98
9.5 Έλεγχος λειτουργιας μεταγωγεα 100

10. ΣΥΓΧΡΟΝΕΣ ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΔΙΚΤΥΟΥ 103

10.1 Ιεραρχικα Δικτυα 103
10.2 Συγκεκλιμενα Δικτυα 114

11. ΙΔΕΑΤΑ ΔΙΚΤΥΑ (*VIRTUAL LANS*) 116

11.1 Εισαγωγη στα VLANs 116
11.2 VLAN και τυποι κινησης 119
11.3 Τοποθετηση σε VLAN 120
11.4 Συνδεσεις VLAN 121
11.5 VLAN Διαχειρισης 125
11.6 Ρυθμισεις VLAN σε μεταγωγεις με Cisco CLI 125
11.7 Εργαστηριακη ασκηση 128

12. ΤΟ ΠΡΩΤΟΚΟΛΛΟ VTP 130

12.1 Εισαγωγη 130
12.2 Λειτουργικα χαρακτηριστικα VTP 130
12.3 Ενεργοποιηση VTP 133
12.4 Ρυθμισεις VTP σε μεταγωγεις με Cisco CLI 134
12.5 Εργαστηριακη ασκηση 135

13. ΔΡΟΜΟΛΟΓΗΣΗ ΜΕΤΑΞΥ VLAN 137

13.1 Εισαγωγη 137
13.2 Ρυθμιση Inter-VLAN Routing σε δρομολογητες με Cisco CLI 140
13.3 Εργαστηριακη ασκηση 140

14. ΑΣΦΑΛΙΣΗ ΘΥΡΩΝ ΜΕΤΑΓΩΓΕΑ 142

14.1 Ρυθμιση του Port Security 142
14.2 Έλεγχος λειτουργιας του port-security 144

15. SPANNING TREE PROTOCOL 145

15.1 Εισαγωγη 145
15.2 Spanning Tree Protocol 146

15.3 ΒΕΛΤΙΩΣΕΙΣ ΚΑΙ ΕΠΕΚΤΑΣΕΙΣ STP 153
15.4 ΡΥΘΜΙΣΕΙΣ PVST+ ΚΑΙ RAPID-PVST ΣΕ CISCO CLI..... 156
15.5 ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 158
15.6 ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 160

16. ΠΟΛΥΕΠΙΠΕΔΗ ΜΕΤΑΓΩΓΗ 162

16.1 ΕΙΣΑΓΩΓΗ 162
16.2 ΜΕΤΑΓΩΓΗ 3ΟΥ ΕΠΙΠΕΔΟΥ ΣΕ CISCO CLI 166
16.3 ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 169
16.4 ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 169

ΠΑΡΑΡΤΗΜΑ ΑΣΚΗΣΕΙΣ ΥΠΟΔΙΚΤΥΩΣΗΣ 171

1. Εισαγωγή στα Δίκτυα Υπολογιστών - Τοπολογίες και Καλωδίωση

1.1 Τα Δίκτυα Δεδομένων στη ζωή μας

Η ανταλλαγή ιδεών και πληροφοριών στην εποχή μας στηρίζεται στα δίκτυα υπολογιστών (θα τα συναντήσουμε και με τον όρο '*δίκτυα δεδομένων*'). Χωρίς να είμαστε μαθηματικά αυστηροί, δίκτυο γενικά είναι μία συλλογή από κόμβους, που συνδέονται με γραμμές, οι οποίες λέγονται κλάδοι. Κάθε κλάδος δεν έχει το ίδιο '*βάρος*' (ταχύτητα ή / και ποιότητα μίας γραμμής), και κάθε κόμβος μπορεί είτε να παράγει τα δεδομένα (τελική συσκευή - *end device*) είτε ενδιάμεσα να τα προωθεί (ενδιάμεση συσκευή - *intermediate device*). Καλή λειτουργία ενός δικτύου σημαίνει αξιόπιστη ανταλλαγή δεδομένων ανάμεσα σε υπολογιστικά συστήματα. Στην πραγματικότητα, η δικτυακή υποδομή εξυπηρετεί τις εφαρμογές, εξυπηρετεί δηλαδή την καθημερινότητα εταιρειών, οργανισμών, φορέων αλλά και την ίδια την προσωπική μας καθημερινότητα.

Στα πρώτα δίκτυα δεδομένων κάθε υπολογιστής συνέδεε πολλά τερματικά τα οποία το μόνο που μπορούσαν να κάνουν είναι να επικοινωνούν μεταξύ τους (**Εικόνα 1.1**)[1]. Η εξέλιξη των μικροϋπολογιστών επέτρεψε την αντικατάσταση των απλών τερματικών με πλήρεις υπολογιστές, τα γνωστά μας PC ή σταθμούς εργασίας (*workstations*). Οι τεχνικές επικοινωνιών που είχαν αναπτυχθεί για τη σύνδεση των απλών τερματικών δεν επαρκούσαν πλέον. Για αυτό το λόγο συμφωνήθηκε ένα πλαίσιο για την προτυποποίηση των επικοινωνιών ανάμεσα σε υπολογιστικά συστήματα διαφορετικών κατασκευαστών, το μοντέλο αναφοράς OSI (*Open System Interconnection*).

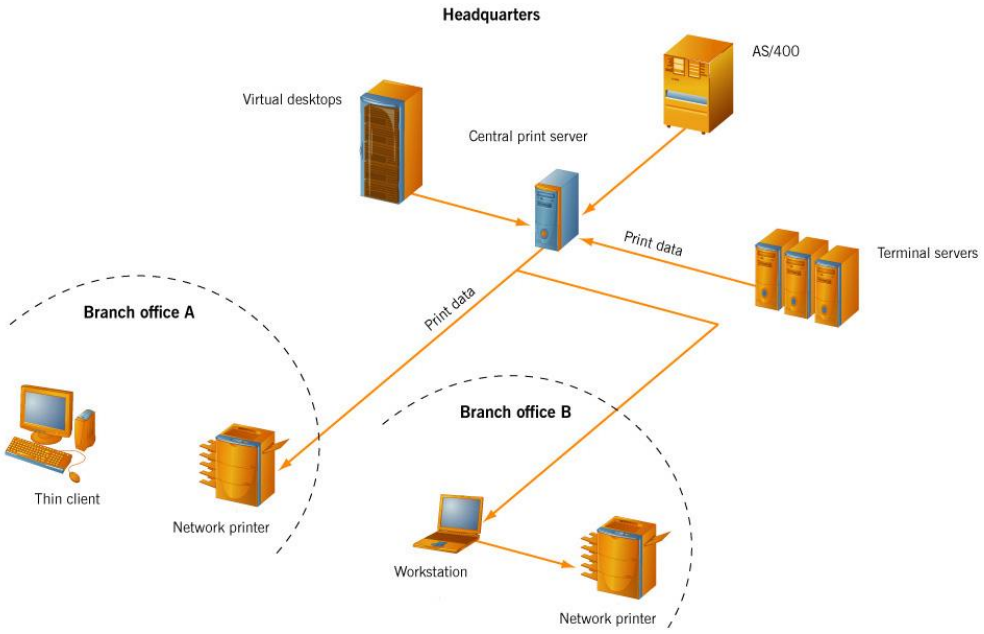
Εικόνα 1.1 Τερματικό VT100

[1] http://commons.wikimedia.org/wiki/File:DEC_VT100_terminal.jpg

Τα σημερινά δίκτυα υπολογιστών έχουν εξελιχθεί και μπορούν να μεταφέρουν κείμενο, φωνή, εικόνα, βίντεο ανάμεσα σε μία πληθώρα συσκευών τελικού χρήστη. Το *Internet* (Διαδίκτυο) επιτρέπει την άμεση και παραστατική ανταλλαγή ιδεών σπάζοντας γεωγραφικούς και άλλους περιορισμούς. Η εργασία, η ενημέρωση και η ψυχαγωγία έχουν αλλάξει ριζικά. Η πρόσβαση στο *Internet* σε μερικά χρόνια θα θεωρείται βασικό ανθρώπινο δικαίωμα, όπως το νερό ή το ηλεκτρικό ρεύμα. Είναι ωστόσο μακρύς ο αγώνας για την καταπολέμηση του ψηφιακού αναλφαβητισμού και την εξοικείωση όλων των ομάδων του πληθυσμού με τις νέες τεχνολογίες και την ορθή χρήση τους.

1.2 Από τι αποτελείται ένα Δίκτυο

Από τη σκοπιά του τεχνικού πληροφοριακών συστημάτων (*IT Professional*) δίκτυο είναι μία συλλογή από διασυνδεμένες συσκευές (*hosts)*. Λέγοντας *host* πρακτικά εννοούμε κάθε ηλεκτρονική συσκευή που διαθέτει μία κάρτα δικτύου (NIC, *Network Interface Card*), ενσύρματη ή ασύρματη. Έτσι *host* είναι ο υπολογιστής του γραφείου μας, ο δικτυακός εκτυπωτής στο διάδρομο της εργασίας μας, ένας κοινός δίσκος όπου όλοι οι υπάλληλοι έχουν πρόσβαση, μία δικτυακή κάμερα παρακολούθησης, αλλά και το '*έξυπνο*' τηλέφωνό μας ή η '*έξυπνη*' τηλεόραση στο σαλόνι μας (**Εικόνα 1.2**)[1].



Εικόνα 1.2 Κοινή χρήση πόρων εκτύπωσης

Για να λειτουργήσει ένα δίκτυο χρειάζονται λοιπόν τέσσερις συνιστώσες:

- Συσκευές (*devices*)
- Μέσα μετάδοσης (*media*)

[1] http://commons.wikimedia.org/wiki/File:Network_printing.jpg

- Κανόνες και πρωτόκολλα (*rules, protocols*)
- Μηνύματα (*messages*)

Οι δικτυακές συσκευές με τις οποίες έχει άμεση επαφή ο τελικός χρήστης είναι οι τελικές συσκευές (*end devices*). Από αυτές ξεκινά και σε αυτές καταλήγει η πληροφορία. Τέτοιες είναι οι προσωπικοί υπολογιστές, οι εξυπηρετητές, τα κινητά, οι ταμπλέτες, οι δικτυακοί εκτυπωτές κλπ.

Οι συσκευές που διαχειρίζονται την κίνηση της πληροφορίας ανάμεσα στην πηγή και τον προορισμό λέγονται ενδιάμεσες συσκευές (*intermediate devices*). Οι δύο πιο τυπικές ενδιάμεσες συσκευές είναι οι δρομολογητές (*routers*) και οι μεταγωγείς (*switches*).

Τα μέσα μετάδοσης αναλαμβάνουν τη φυσική μεταφορά της πληροφορίας, συνήθως με τη μορφή ηλεκτρικών σημάτων, είτε μέσα σε καλώδιο (ενσύρματη - *wired*, επικοινωνία) είτε στον ελεύθερο χώρο (ασύρματη - *wireless*, επικοινωνία).

Λέγοντας πρωτόκολλα εννοούμε το σύνολο των συμφωνημένων κανόνων που κυβερνούν την επικοινωνία ανάμεσα σε δύο υπολογιστικά συστήματα. Χωρίς τέτοιους κανόνες η επικοινωνία είναι αδύνατη. Τα πρωτόκολλα ρυθμίζουν τις λεπτομέρειες σε όλα τα επίπεδα της επικοινωνίας, π.χ. από τα γεωμετρικά και ηλεκτρικά χαρακτηριστικά ενός ακροδέκτη μέχρι τον τρόπο ψηφιακής αναπαράσταση αλφαριθμητικών χαρακτήρων, ήχων ή εικόνων.

1.3 Είδη Δικτύων / Τοπολογίες

Σε ένα τοπικό δίκτυο (LAN, *Local Area Network*) όλες οι συσκευές βρίσκονται σε έναν περιορισμένο γεωγραφικά χώρο. Μία αίθουσα διδασκαλίας, ένα κτίριο γραφείων, αλλά και το σπίτι μας είναι τυπικά παραδείγματα τοπικών δικτύων. Η διασύνδεση των συσκευών επιτυγχάνεται είτε ασύρματα είτε με χάλκινα καλώδια σε έκταση μερικών δεκάδων μέτρων το πολύ, χωρίς να είναι απαραίτητη η συνδρομή σε κάποια τηλεπικοινωνιακή υπηρεσία. Η τεχνολογία τοπικών δικτύων που έχει επικρατήσει είναι το Ethernet στις διάφορες εκδοχές του.

Τα δίκτυα ευρείας περιοχής (WAN, *Wide Area Networks*) συνδέουν πόλεις, χώρες, ολόκληρο τον κόσμο. Μπορούμε επίσης να πούμε ότι ένα WAN δεν είναι τίποτα άλλο παρά πολλά τοπικά δίκτυα (LANs) διασυνδεμένα, π.χ. τα σημεία παρουσίας μίας τράπεζας ή μία αλυσίδα σούπερ μάρκετ. Εκτείνονται σε δεκάδες, εκατοντάδες ή και χιλιάδες χιλιόμετρα και απαιτείται η συνδρομή σε έναν τηλεπικοινωνιακό πάροχο (*telco* ή *service provider*). Τεχνολογίες δικτύων ευρείας περιοχής (WAN) είναι το ISDN, το Frame Relay, οι δορυφορικές ή μικροκυματικές, αλλά και το ADSL του σπιτιού μας.

Τα μητροπολιτικά δίκτυα (MAN, *Metropolitan Area Network*) μπορούν να θεωρη-θούν μία ενδιάμεση κατάσταση ανάμεσα σε LAN και WAN. Οι αποστάσεις είναι

μεγαλύτερες από αυτές των τοπικών δικτύων, ωστόσο συνήθως δε χρησιμοποιούνται εξωτερικές τηλεπικοινωνιακές υπηρεσίες. Οι μεγάλες στρατιωτικές, βιομηχανικές ή πανεπιστημιακές εγκαταστάσεις (*campus topologies*) συνιστούν τυπικά μητροπολιτικά δίκτυα. Οι μητροπολιτικές τεχνολογίες συνήθως είναι επέκταση τοπικών τεχνολογιών, π.χ. Metro Ethernet, Wi-Max κλπ.

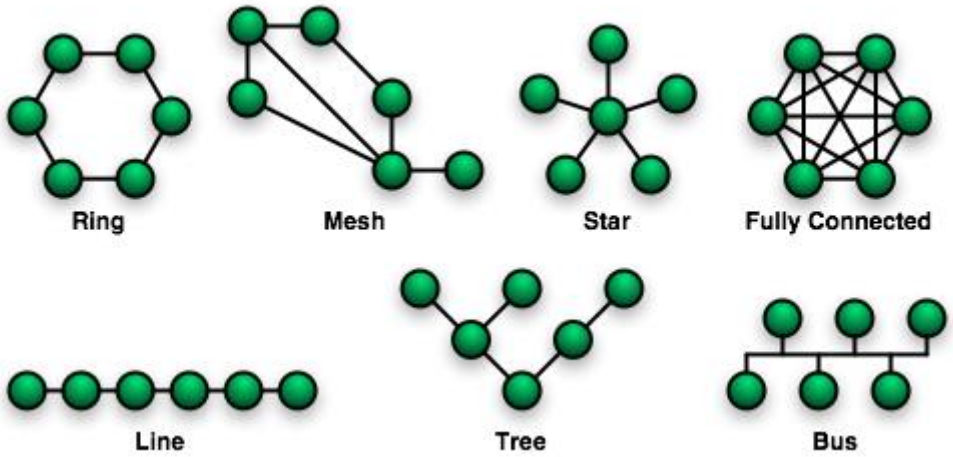
Συχνά αναφερόμαστε και στα δίκτυα προσωπικής εμβέλειας (PAN, *Personal Area Networks*) που συνδέουν ένα μικρό αριθμό συσκευών σε μικρές αποστάσεις, της τάξης των λίγων μέτρων, για την ανταλλαγή δεδομένων με μικρές συνήθως ταχύτητες. Το Bluetooth ή το NFC μπορούν να θεωρηθούν PAN τεχνολογίες (**Εικόνα 1.3**)[1].

Εικόνα 1.3 Πληρωμή με τεχνολογία NFC

Η τοπολογία ενός δικτύου καθορίζει τον τρόπο με τον οποίο διατάσσονται οι κόμβοι και οι κλάδοι του. Στην τοπολογία αστέρα (*star*) όλες οι περιφερειακές συσκευές συνδέονται ακτινικά με ένα κεντρικό σημείο. Για το λόγο αυτό τέτοιες τοπολογίες θα τις συναντήσουμε και με την ονομασία "*hub and spoke*". Σε μία αρτηρία (*bus*) οι κόμβοι συνδέονται σε σειρά, ο ένας μετά τον άλλο. Το δίκτυο βρόχου (*mesh*) είναι αυτό όπου ο κάθε σταθμός είναι συνδεμένος με τους άλλους με δύο τουλάχιστο δρόμους και με τέτοιο τρόπο που να κλείνουν βρόχους. Η **Εικόνα 1.4**[2] δείχνει με τυπικό τρόπο διάφορες τοπολογίες.

[1] http://commons.wikimedia.org/wiki/File:Nfc_machine.jpg

[2] http://commons.wikimedia.org/wiki/File:NetworkTopologies.png



Εικόνα 1.4 Τοπολογίες

Είναι απαραίτητη εδώ η διάκριση ανάμεσα σε φυσική και λογική τοπολογία. Η φυσική τοπολογία (*physical topology*) ορίζει την πραγματική θέση και σύνδεση συσκευών και μέσων μετάδοσης. Η φυσική τοπολογία απεικονίζει τις διαδρομές των καλωδίων (*cable runs*). Αντίθετα η λογική τοπολογία (*logical topology*) απεικονίζει τη διαδρομή της πληροφορίας. Σε ένα δίκτυο τα δύο είδη τοπολογιών δεν ταυτίζονται υποχρεωτικά. Για παράδειγμα, το *hub* υλοποιεί μία φυσική τοπολογία αστέρα (*hub and spoke*) ενώ η λογική τοπολογία είναι αρτηρίας (*bus*).

1.4 Τεχνικές και μέσα μετάδοσης

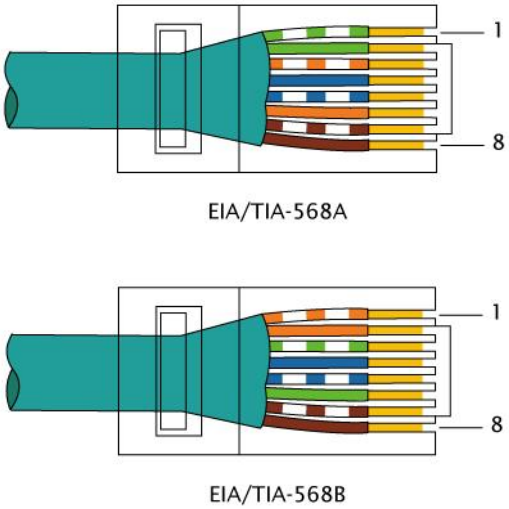
Σε αυτή την ενότητα γίνεται μία σύντομη αναφορά σε θέματα μετάδοσης, με έμφαση στο κοινό καλώδιο χαλκού (*Unshielded Twisted Pair* - UTP) που σήμερα χρησιμοποιείται σχεδόν σε όλες τις εγκαταστάσεις τοπικών δικτύων.

Υπενθυμίζεται ότι τα σήματα διακρίνονται σε αναλογικά και ψηφιακά. Τα κανάλια / μέσα μετάδοσης είναι τέτοια που φυσικά δεν επιτρέπουν την αυτούσια μετάδοση των σημάτων πληροφορίας όπως γεννιούνται από την πηγή τους, χωρίς δηλαδή κάποια επεξεργασία. Αυτή η επεξεργασία του σήματος πληροφορίας που το καθιστά κατάλληλο για μετάδοση μέσα στο κανάλι λέγεται διαμόρφωση (*modulation*). Η αναλυτική παρουσίαση των μεθόδων διαμόρφωσης άπτεται της επιστήμης του ηλεκτρολόγου μηχανικού και δεν είναι στις άμεσες προτεραιότητες του συγκεκριμένου υλικού.

Τα πιο γνωστά φυσικά μέσα μετάδοσης είναι τα συρμάτινα χάλκινα καλώδια, τα ομοαξονικά, οι οπτικές ίνες και οι ασύρματες ζεύξεις.

Το αθωράκιστο συνεστραμμένο καλώδιο (UTP, *Unshielded Twisted Pair*) με ακροδέκτες RJ-45 έχει κυριαρχήσει στις εγκαταστάσεις τοπικών δικτύων (LANs). Πρόκειται για τέσσερα ζευγάρια συρμάτων συνεστραμμένων ανά ζεύγος και όλα μαζί, κλει-σμένα μέσα σε ένα εύκαμπτο πλαστικό κέλυφος. Η συστροφή προκαλεί

την ακύρωση μη επιθυμητών σημάτων και παρεμβολών ανάμεσα στους αγωγούς αυτούς, που, ας μην ξεχνάμε, διαρρέονται από ρεύματα υψηλών συχνοτήτων. Για τον ίδιο λόγο θα πρέπει τα καλώδια να είναι σωστά τερματισμένα στους RJ-45 ακροδέκτες με 'καθαρό' τρόπο. Ανάλογα με τη διάταξη των χρωματικά κωδικοποιημένων συρμάτων του UTP καλωδίου στον ακροδέκτη, ένας τερματισμός μπορεί να ακολουθεί το πρότυπο T568A ή T568B (τυποποίηση κατά EIA/TIA). Η **Εικόνα 1.5**[1] δείχνει τις δύο επιλογές. Ανάλογα με την τοποθέτηση των συρμάτων μέσα στον ακροδέκτη, ένα UTP καλώδιο διακρίνεται σε ευθύ (*straight-through*), ανάστροφο (*crossover*) ή κονσόλας (*rollover)*. Ο **Πίνακας 1.1** δείχνει τις τυπικές χρήσεις του κάθε τύπου.



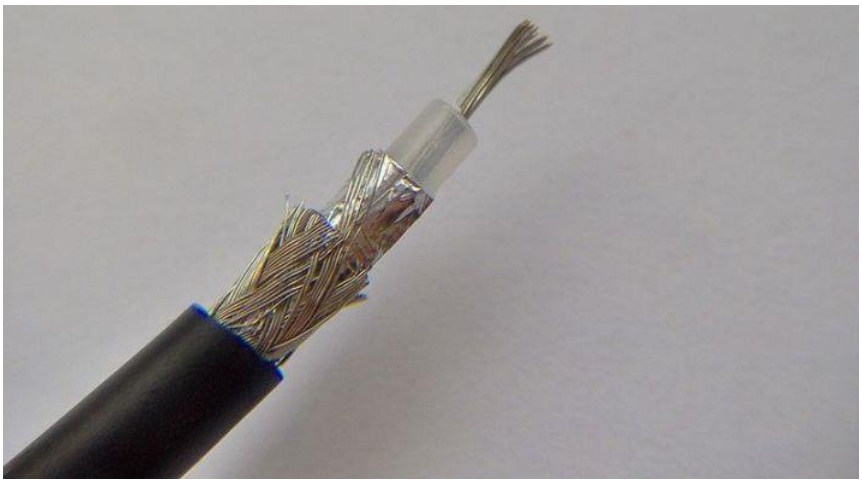
Εικόνα 1.5 RJ-45 ακροδέκτες κατά EIA/TIA T568A και T568B

ΠΙΝΑΚΑΣ 1.1 Χρήση τύπων καλωδίων στο Τοπικό Δίκτυο	
Ευθύ (*straight-through*)	Υπολογιστής με μεταγωγέα Δρομολογητής με μεταγωγέα
Ανάστροφο (*crossover*)	Δρομολογητής με δρομολογητή Μεταγωγέας με μεταγωγέα Υπολογιστής με υπολογιστή
Rollover	Σύνδεση με τη θύρα Console μιας συσκευής

Τα ομοαξονικά καλώδια χρησιμοποιήθηκαν αρχικά για τις πρώτες αναλογικές συνδέσεις με απαιτήσεις υψηλού εύρους ζώνης: εικόνα, κομβικές συνδέσεις του τηλεφωνικού συστήματος, συνδέσεις κορμού με αναμεταδότες. Επίσης χρησιμοποιήθηκαν στα πρώτα τοπικά δίκτυα, γνωστά με τα πρότυπα 10BASE2 και 10BASE5.

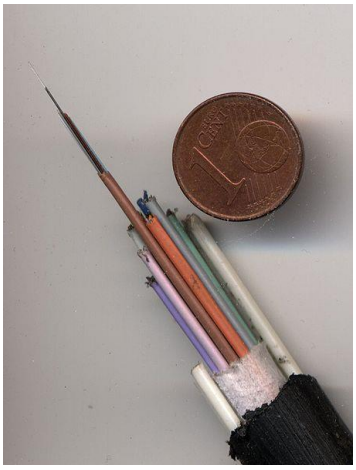
[1] http://commons.wikimedia.org/wiki/File:RJ-45_TIA-568A_Right.png
http://commons.wikimedia.org/wiki/File:RJ-45_TIA-568B_Right.png

Σε ένα ομοαξονικό καλώδιο (*coaxial cable* ή *coax*) ο κεντρικός αγωγός περιβάλλεται από έναν εξωτερικό αγωγό (**Εικόνα 1.6**)[1]. Η όλη διάταξη περιβάλλεται από μονωτικό και προστατευτικό κάλυμμα, ενώ ανάμεσα στους δύο αγωγούς τοποθετείται διηλεκτρικό υλικό. Σαν μέσο μετάδοσης στα δίκτυα δεδομένων, χρησιμοποιήθηκε σε τοπικά δίκτυα πριν την εμφάνιση και κυριαρχία των καλωδίων συνεστραμμένων ζευγών. Ήταν δύσχρηστο λόγω της μεγάλης διαμέτρου του, της μηχανικής δυσκαμψίας και των δυσκολιών στις συνδέσεις (σύνδεσμοι και τερματισμοί).



Εικόνα 1.6 Ομοαξονικό καλώδιο

Η χρήση των οπτικών ινών (*fiber optic cable*) για τη μετάδοση δεδομένων σε υψηλές ταχύτητες στηρίζεται στην ιδιότητα μίας ίνας γυαλιού ή πλαστικού να '*εγκλωβίζει*' τις ακτίνες φωτός και να τις οδηγεί στο τέρμα του καλωδίου. Ένα καλώδιο οπτικής ίνας αποτελείται από τρεις ομόκεντρες διηλεκτρικές στρώσεις, την κεντρική ίνα (*core*), την επίστρωση (*cladding*) και το κάλυμμα (*jacket*), όπως φαίνεται στην **Εικόνα 1.7**[2].



Εικόνα 1.7 Καλώδιο οπτικής ίνας

Εγκαταστάσεις οπτικών ινών θα συναντήσει κανείς σε επίγειες και υποθαλάσσιες τηλεπικοινωνιακές συνδέσεις ή σε βιομηχανικό περιβάλλον, όπου υπάρχει υψηλό

[1] http://commons.wikimedia.org/wiki/File:Coaxial_cable_cut.jpg
[2] http://commons.wikimedia.org/wiki/File:Optical-fiber-pbc.jpg

επίπεδο ηλεκτρομαγνητικών θορύβων. Πιο συχνά θα συναντήσουμε οπτικά καλώδια σε μητροπολιτικά δίκτυα αλλά και στο τοπικό μας δίκτυο, για συνδέσεις κορμού (backbone) ή για τη σύνδεση εξυπηρετητών.

1.5 Δομημένη Καλωδίωση

Ένα σημερινό κτίριο (επαγγελματικός / βιομηχανικός χώρος, αλλά και κατοικία) περιλαμβάνει στο σχεδιασμό του συστήματα ασθενών ρευμάτων που εξυπηρετούν συνδέσεις μεταξύ υπολογιστών, αναλογικών και ψηφιακών τηλεφωνικών συσκευών, συστημάτων παρακολούθησης, και άλλων τερματικών. Η δομημένη καλωδίωση δίνει μία ενοποιημένη αντιμετώπιση προτείνοντας ένα μοναδικό, γενικού σκοπού, ευέλικτο και επεκτάσιμο καλωδιακό σύστημα. Στην πράξη περιλαμβάνει τη μελέτη, τους τρόπους υλοποίησης, τα υλικά και την εγγύηση των επιδόσεων. Δύο από τα πολλά πλεονεκτήματα είναι η επεκτασιμότητα / ευελιξία στις ανακατατάξεις θέσεων στους χώρους εργασίας και οι προδιαγραφές ποιότητας και επιδόσεων της τελικής εγκατάστασης.

Μία πλήρης εγκατάσταση περιλαμβάνει τυπικά τα εξής υποσυστήματα:

- Κεντρικό κατανεμητή
- Ενδιάμεσους κατανεμητές
- Κατακόρυφη καλωδίωση
- Οριζόντια καλωδίωση
- Υποσύστημα θέσης εργασίας

1.6 Συνδέοντας LANs και WANs

Κάθε δικτυακή συσκευή έχει μία σειρά από διεπαφές (*interfaces*) για την επικοινωνία της με άλλες δικτυακές συσκευές ή για ρυθμίσεις και διαχείριση (*configuration and management*). Από τις διεπαφές αυτές, κάποιες απαιτούν συνδεσιμότητα (*connectivity*) και κάποιες όχι.

Η σύνδεση κονσόλας (*console*) είναι μία σειριακή σύνδεση χαμηλής ταχύτητας που χρησιμοποιείται για την αρχική ρύθμιση (*initial configuration*) της συσκευής ή σε ειδικές περιπτώσεις (συντήρηση, ανάκτηση κωδικού - *password recovery* κ.λ.π.). Το *console interface* συνδέεται με την κοινή σειριακή θύρα (COM / RS-232) ενός υπολογιστή που εκτελεί μία εφαρμογή προσομοίωσης τερματικού (*terminal emulation*). Με τον τρόπο αυτό αποκτούμε πρόσβαση εισόδου-εξόδου (I/O *access*) στο λειτουργικό σύστημα της συσκευής μας και πραγματοποιούμε τις αρχικές ρυθμίσεις σε δρομολογητές και μεταγωγείς.

Στα δίκτυα που μας ενδιαφέρουν τα *interfaces* επικοινωνίας είναι IP *interfaces*, διακινούν δηλαδή κομμάτια πληροφορίας (PDUs, *Protocol Data Units*) σύμφωνα με την οικογένεια των πρωτοκόλλων TCP/IP. Ένα τέτοιο *interface* θα είναι είτε τοπικό (LAN) είτε ευρείας περιοχής (WAN). Η τοπική διασύνδεση θα είναι ασφαλώς μία

Ethernet διασύνδεση, και η καλωδίωση θα υλοποιείται με τα γνωστά μας UTP καλώδια.

Σχετικά με τις WAN συνδέσεις, έχουμε να επισημάνουμε αρχικά ότι αυτές πραγματοποιούνται πάντοτε με τη μεσολάβηση ενός τηλεπικοινωνιακού παρόχου που προσφέρει ένα σημείο πρόσβασης στο δίκτυό του μέσω ενός DCE (*Data Circuit Equipment*) που μπορεί να είναι ένα *modem* ή μια συσκευή τερματισμού και διαμόρφωσης. Η πληροφορία ξεκινά και καταλήγει σε ένα DTE (*Data Termination Equipment*) που τυπικά είναι ο δρομολογητής του συνδρομητή. Το DTE και το DCE βρίσκονται και τα δύο στο χώρο του συνδρομητή (CPE, *Customer Premises Equipment*) και συνδέονται με ένα σειριακό πρωτόκολλο, όπως είναι τα X.21, V35 ή EIA/TIA 449.

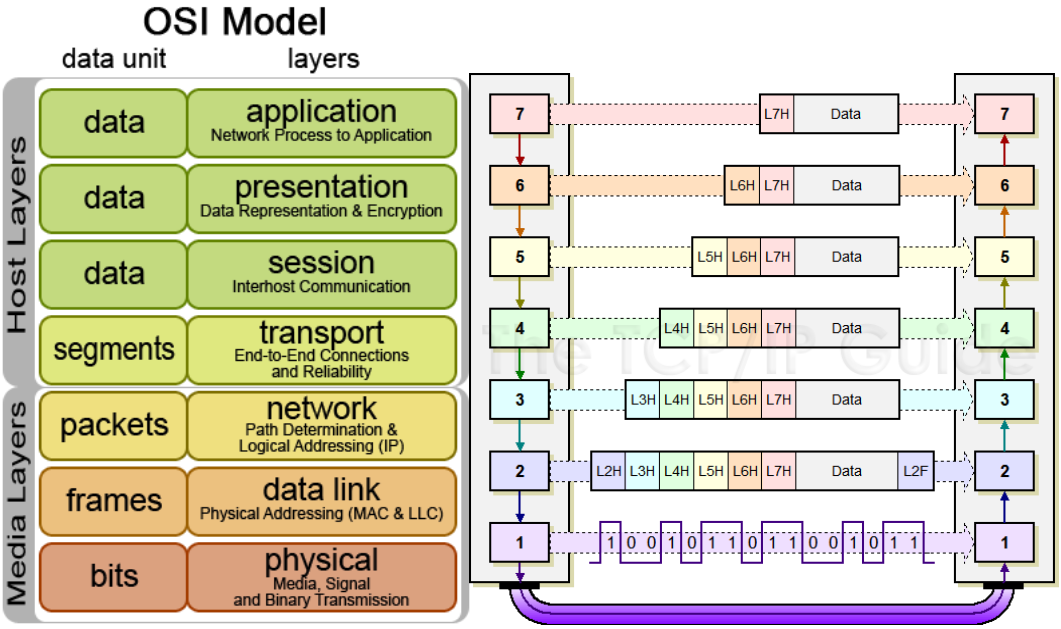
2. Δικτυακές Συσκευές και Μοντέλο OSI

2.1 Το μοντέλο αναφοράς OSI

Η επικοινωνία, είτε είναι φυσική (*face-to-face*) είτε μέσω δικτυακών υποδομών, επιτυγχάνεται με το σχεδιασμό και την εφαρμογή κανόνων που λέγονται πρωτόκολλα επικοινωνίας (*communication protocols*). Στα δίκτυα δεδομένων που μας ενδιαφέρουν, τα πρωτόκολλα υλοποιούνται σε επίπεδο υλικού και λογισμικού στους *hosts* (τερματικές συσκευές) και σε κάθε άλλη δικτυακή συσκευή που συμμετέχει με τον τρόπο της στην επικοινωνία. Η συλλογή των πρωτοκόλλων που επιτρέπουν μία συγκεκριμένη επικοινωνία συχνά αναφέρεται και ως σουίτα ή στοίβα (*protocol suite / stack*).

Για την αλληλεπίδραση των πρωτοκόλλων, που οδηγεί σε επιτυχή επικοινωνία, χρησιμοποιείται ένα μοντέλο με επίπεδα (*layered model*). Οι δύο βασικές αρχές που διέπουν αυτή την 'επιπεδοποίηση' (*layering*) είναι:

- Κάθε επίπεδο εξυπηρετείται από το προηγούμενο (χαμηλότερο) και παρέχει υπηρεσίες στο επόμενό του (υψηλότερο). Έτσι, το Επίπεδο 2 (*Data Link Layer*) εξυπηρετεί το Επίπεδο 3 (*Network Layer*) λαμβάνοντας τα πακέτα (*packets*), ενθυλακώνοντάς τα σε πλαίσια (*frames*) και προετοιμάζοντας την πληροφορία για να 'κατέβει' στο φυσικό μέσο.
- Κάθε επίπεδο λειτουργεί ανεξάρτητα από το προηγούμενο (χαμηλότερο) και το επόμενό του (υψηλότερο). Με αυτό τον τρόπο, η μετάβαση από το IPv4 (πρωτόκολλο του Επιπέδου 3) στο IPv6 (ένα άλλο πρωτόκολλο του 3^{ου} Επιπέδου) δεν απαιτεί αλλαγές στα πρωτόκολλα του 2^{ου} (π.χ. Ethernet) ούτε του 4^{ου} (π.χ. TCP / UDP) Επιπέδων.



Εικόνα 2.1 Το Μοντέλο Αναφοράς OSI και η ενθυλάκωση (*encapsulation*)

Η μετάδοση της πληροφορίας καθίσταται δυνατή με τη συνεισφορά του κάθε επιπέδου σε μία διαδικασία που λέγεται ενθυλάκωση (*encapsulation*). Πρόκειται για τον τεμαχισμό της πηγαίας πληροφορίας και την προσθήκη επιπλέον *bytes* ελέγχου (*overhead*) ώστε αυτή να μπορέσει να κυκλοφορήσει στο σύρμα ή στον αέρα μέχρι τον προορισμό. Όπως φαίνεται και στην **Εικόνα 2.1**[1], η ενθυλάκωση γίνεται από τα υψηλότερα στα χαμηλότερα επίπεδα του μοντέλου. Αντίστοιχα κατά τη λήψη γίνεται η αποθυλάκωση (*decapsulation*) μέχρι την ανάκτηση του αρχικού μηνύματος ακέραιου. Κάθε επίπεδο χρησιμοποιεί τις δικές του μονάδες δεδομένων (PDUs, *Protocol Data Units*). Μεταξύ των πρωτοκόλλων του Επιπέδου 4 ανταλλάσσονται τεμάχια (*segments*), στο Επίπεδο 3 ανταλλάσσονται πακέτα (*packets*), στο Επίπεδο 2 πλαίσια (*frames*) και στο χαμηλότερο επίπεδο (φυσικό επίπεδο) κυκλοφορούν *bits*, στη γνω-στή μας μορφή παλμοσειρών.

Συνοπτικά, οι λειτουργίες καθενός από τα επτά επίπεδα του μοντέλου OSI είναι:

Επίπεδο Εφαρμογών (*Application*)
Το κοντινότερο στον άνθρωπο επίπεδο, παρέχει τον τρόπο για να μπορεί η μία εφαρμογή να συνομιλεί με την άλλη. Οι λειτουργίες του προσδιορίζονται σε μεγάλο βαθμό από το χρήστη της εφαρμογής, για αυτό και οι τυποποιήσεις του είναι οι λιγότερο καθορισμένες. Μερικές από τις υπηρεσίες που παρέχει το επίπεδο εφαρμογών είναι:

- Εξακρίβωση της ταυτότητας των εφαρμογών που επιθυμούν να επικοινωνήσουν.
- Έλεγχος και επιβεβαίωση της διαθεσιμότητας για συνομιλία.
- Έλεγχος ροής των συναλλαγών και ακεραιότητα της πληροφορίας.

Επίπεδο Παρουσίασης (*Presentation*)
Αναλαμβάνει την αναπαράσταση της πληροφορίας που μεταφέρεται από εφαρμογή σε εφαρμογή. Επιχειρεί δηλαδή την κατάλληλη τροποποίηση των δεδομένων ώστε να είναι κατανοητά από την εφαρμογή και τελικά να μην απαιτείται από τις απομακρυσμένες συσκευές χρήση κοινού κώδικα. Μερικές από τις υπηρεσίες προς αυτή την κατεύθυνση είναι:

- Μετατροπή σύνταξης δεδομένων (π.χ. από ASCII σε EBCDIC).
- Συμπίεση / αποσυμπίεση.
- Κρυπτογράφηση για ασφάλεια στη μεταφορά.

Επίπεδο Συνόδου (*Session*)
Παρέχει τα αναγκαία μέσα για την οργάνωση και το συγχρονισμό του διαλόγου ανάμεσα στις εφαρμογές, που γίνεται στα πιο πάνω επίπεδα. Η διαδικασία της αποκατάστασης μίας συνόδου (*binding*) περιλαμβάνει λειτουργίες όπως η πιστοποίηση ταυτότητας του χρήστη, η χρέωση και η ποιότητα της συνόδου. Υπηρεσίες σε αυτό το σημείο είναι:

- Έναρξη και συντήρηση του διαλόγου.

[1] http://commons.wikimedia.org/wiki/File:Osi-model.png

- Διαχείριση και έλεγχος προσπέλασης.
- Αποκατάσταση νέας σύνδεσης μετά από διακοπή.

Επίπεδο Μεταφοράς (*Transport*)

Μπορεί να θεωρηθεί ως μια διεπαφή λογισμικού (ένα *software interface)* ανάμεσα στα τρία χαμηλότερα επίπεδα, που συνήθως υλοποιούνται στις δικτυακές συσκευές και στα τρία υψηλότερα επίπεδα που σχετίζονται με τις εφαρμογές. Φροντίζει για τη διαφανή μεταφορά δεδομένων προς τα ανώτερα επίπεδα σύμφωνα με προκαθορισμένο από την εφαρμογή βαθμό αξιοπιστίας. Μερικές από τις λειτουργίες του είναι:

- Αποκατάσταση και τερματισμός της σύνδεσης σε επίπεδο μεταφοράς, π.χ. η διαδικασία αποκατάστασης κλήσης με χρήση TCP.
- Λογική διευθυνσιοδότηση υπηρεσιών / διαδικασιών, π.χ. οι TCP / UDP θύρες.
- Έλεγχος ροής (*flow control*), π.χ. με τη μέθοδο παραθύρων (*windowing*) του TCP.
- Καθορισμός και επιλογή από την εφαρμογή της ποιότητας εξυπηρέτησης της σύνδεσης (*reliable* / *unreliable*, *connection-oriented* / *connectionless*).

Τα πρωτόκολλα του 4^{ου} Επιπέδου που έχουν σήμερα κυριαρχήσει στις επικοινωνίες δεδομένων είναι το TCP για αξιόπιστη μετάδοση και το UDP για αναξιόπιστη.

Επίπεδο Δικτύου (*Network*)

Είναι το πρώτο επίπεδο από κάτω προς τα πάνω που παρέχει τα μέσα για την αποκατάσταση, υποστήριξη και τερματισμό συνδέσεων από άκρο σε άκρο (*host-to-host communication*). Επίσης, είναι ανεξάρτητο από το φυσικό μέσο (*medium-independent*). Το σημαντικότερο πρωτόκολλο του 3^{ου} Επιπέδου είναι το IP. Δύο είναι οι βασικές υπηρεσίες που παρέχει:

- Λογική διευθυνσιοδότηση, *logical addressing*, π.χ. οι γνωστές μας IP διευθύνσεις.
- Επιλογή διαδρομής (*route selection*) για τη μεταφορά δεδομένων με τη μορφή πακέτων.

Επίπεδο Σύνδεσης Δεδομένων (*Data Link*)

Βασικός σκοπός του 2^{ου} Επιπέδου είναι η πρόσβαση στο μέσο μετάδοσης. Οι σημαντικότερες υπηρεσίες που παρέχει είναι:

- Ενθυλάκωση των πακέτων για τον σχηματισμό πλαισίων, ανάλογα με τον τρόπο μετάδοσης.
- Φυσική διευθυνσιοδότηση (*physical addressing)*, π.χ. οι MAC διευθύνσεις του Ethernet.
- Έλεγχος της πρόσβασης / ζεύξης, είτε με ανταγωνιστικές (*contention-based*) είτε με αιτιοκρατικές (*deterministic*) μεθόδους, π.χ. η μέθοδος CSMA/CD του *legacy* Ethernet.
- Ανίχνευση σφαλμάτων, συνήθως με χρήση τεχνικών ισοτιμίας.

Πρωτόκολλα του Επιπέδου 2 για τοπικά δίκτυα είναι το Ethernet, Token Bus, Token Ring κ.λ.π. Στα δίκτυα WAN θα συναντήσουμε τα LAPB, Frame Relay, Point-to-Point Protocol, HDLC, κ.λ.π.

Φυσικό Επίπεδο (*Physical*)
Στο επίπεδο αυτό τα *bits* κωδικοποιούνται και μεταφέρονται πάνω στο φυσικό μέσο. Αντικείμενό του είναι τα ηλεκτρικά, μηχανικά και λειτουργικά χαρακτηριστικά μίας σύνδεσης, όπως ο τύπος της σύνδεσης, τα χαρακτηριστικά των παλμών, ο συγχρονισμός κ.λ.π.

2.2 Δικτυακές Συσκευές

Οι δικτυακές συσκευές είναι ενδιάμεσες συσκευές που αναλαμβάνουν την προώθηση της πληροφορίας χωρίς να την αλλοιώνουν. Είναι συνήθως ολοκληρωμένα υπολογιστικά συστήματα με το δικό τους λειτουργικό σύστημα (*firmware*, υλικολογισμικό) που καθορίζει σε μεγάλο βαθμό τη λειτουργία τους. Οι σημαντικότερες δικτυακές συσκευές είναι:

Repeater (αναμεταδότης)
Πρόκειται για έναν ενισχυτή με μία είσοδο και μία έξοδο. Το σήμα εισόδου ενισχύεται χωρίς καμία επεξεργασία με σκοπό την αύξηση της εμβέλειας του δικτύου. Με αυτό το σκεπτικό, ένα *repeater* λειτουργεί στο Φυσικό Επίπεδο του μοντέλου αναφοράς OSI.

Hub
Το *hub* μπορεί να χαρακτηριστεί ως ένα *multi-port repeater*, γιατί προωθεί σήμα που εισέρχεται σε μία θύρα του έξω από όλες τις θύρες, εκτός από τη θύρα εισόδου. Λειτουργεί στο Φυσικό Επίπεδο και υλοποιεί μία λογική τοπολογία αρτηρίας (*bus*). Τα *hubs* χρησιμοποιήθηκαν στα πρώτα τοπικά δίκτυα με δομημένη UTP καλωδίωση, καταργώντας έτσι το ομοαξονικό καλώδιο (**Εικόνα 2.2**[1]). Στα δίκτυα με hubs η μετάδοση είναι *half-duplex* και όλες οι συσκευές (*hosts)* ανήκουν στο ίδιο *collision domain*. Τα τοπικά δίκτυα με *hub* λειτουργούν σε ταχύτητα 10 Mbps.

Εικόνα 2.2 10BASE-T *hub*

Bridge
Καθώς το πλήθος των χρηστών και οι απαιτήσεις σε εύρος ζώνης των εφαρμογών (*bandwidth-intensive applications*) αυξάνουν, αυξάνει η πιθανότητα συγκρούσεων σε ένα δίκτυο με *hubs*, αφού όλες οι συσκευές (*hosts)* βρίσκονται σε ένα μεγάλο

[1] http://commons.wikimedia.org/wiki/File:HubSynOptics_rackable.jpg

collision domain. Μεγάλο πλήθος συγκρούσεων σημαίνει πτώση της επίδοσης του δικτύου, αδυναμία σύνδεσης των συσκευών και πιθανή κατάρρευση.

Είναι λοιπόν απαραίτητη η κατάτμηση ενός 'μεγάλου' δικτύου με *hubs* σε μικρότερα *collision domains,* ώστε να μειωθεί, στο μέτρο του δυνατού, η πιθανότητα συγκρούσεων. Αυτό επιτυγχάνεται με τη χρήση μίας γέφυρας (*bridge*). Η γέφυρα έχει δύο πόρτες και χωρίζει το τοπικό δίκτυο σε δύο μικρότερα *collision domains*. Όταν δύο συσκευές στην ίδια πλευρά της γέφυρας θέλουν να επικοινωνήσουν μεταξύ τους, η κίνηση δεν περνά στην απέναντι πλευρά, Η γέφυρα λοιπόν παίρνει μία απόφαση, ανάλογα με τον προορισμό ενός πλαισίου, για το εάν θα το προωθήσει ή όχι. Αφού μπορεί να διαβάζει τις MAC *addresses* των εισερχόμενων *frames (πλαισίων),* μία γέφυρα λειτουργεί στο Επίπεδο 2 του μοντέλου OSI. Για αυτό το λόγο λέμε ότι η γέφυρα πραγματοποιεί L2 *segmentation* στο τοπικό μας δίκτυο.

Switch (μεταγωγέας)
Ένα *switch* αναφέρεται συχνά και ως *multi-port bridge*, **Εικόνα 2.3**[1]. Ανάλογα με τη MAC διεύθυνση προορισμού ενός πλαισίου, το *switch* το προωθεί ακριβώς και αποκλειστικά στη συσκευή με τη συγκεκριμένη MAC. Δημιουργείται δηλαδή ένα είδος προσωρινού αποκλειστικού κυκλώματος ανάμεσα στις δύο πόρτες των συσκευών που επικοινωνούν. Μία τέτοια επικοινωνία πραγματοποιείται χωρίς συγκρούσεις (*collision-free*) και αμφίδρομη (*full-duplex*). Εφόσον το *switch* είναι δυνατό να διαβάζει MAC διευθύνσεις, είναι μία συσκευή που λειτουργεί στο 2^{ο} Επίπεδο του OSI.

Εικόνα 2.3 100BASE-T *switch*

Σε ένα *switch* το μέγεθος του *collision domain* έχει εκφυλιστεί σε μία και μόνο πόρτα. Υπάρχουν δηλαδή τόσα *Layer 2 segments* στο τοπικό μας δίκτυο όσες και οι πόρτες του. Για αυτό λέμε ότι το *switch* πραγματοποιεί *micro-segmentation*.

Router
Ο δρομολογητής (*router*) είναι μία δικτυακή συσκευή του 3^{ου} OSI Επιπέδου, που δέχεται, επεξεργάζεται και προωθεί πακέτα (θυμίζουμε ότι το πακέτο είναι το *Protocol Data Unit,* PDU, του 3^{ου} Επιπέδου του OSI). Οι βασικές λειτουργίες του είναι δύο:

- Επιλογή διαδρομής (*best path selection*): το router διαβάζει τα 32 bits της IP διεύθυνσης προορισμού κάθε εισερχόμενου πακέτου και λαμβάνει μία

[1] http://commons.wikimedia.org/wiki/File:Linksys48portswitch.jpg

απόφαση για τη διεπαφή (*interface*) εξόδου στο οποίο θα προωθήσει το πακέτο.

- Προώθηση πακέτων (*packet forwarding*): αφού καθορίσει το *interface* εξόδου το *router* προωθεί την πληροφορία, με την έννοια ότι κατασκευάζει ένα πλαίσιο (*frame*) που ταιριάζει με την τεχνολογία διασύνδεσης που χρησιμοποιεί το *interface* εξόδου. Το *router* λοιπόν όχι μόνο προωθεί τα πακέτα αλλά και συνδέει διαφορετικές μεταξύ τους τεχνολογίες, π.χ. το εισερχόμενο πακέτο είναι ενθυλακωμένο (*encapsulated*) σε ένα πλαίσιο Ethernet ενώ το εξερχόμενο σε ένα πλαίσιο PPP.

Στην **Εικόνα 2.4** δίνονται τα κυριότερα σύμβολα που θα χρησιμοποιηθούν στις εικόνες και τα διαγράμματα του παρόντος εγχειριδίου.

Εικόνα 2.4 – Βασικές δικτυακές συσκευές και συνδέσεις

3. Τα Πρωτόκολλα TCP/IP, ARP/RARP

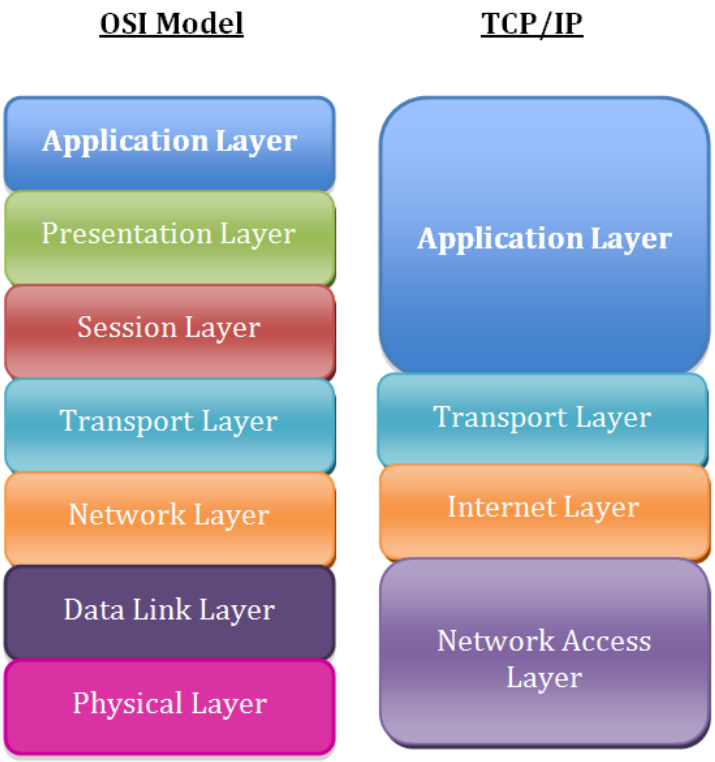
3.1 Το μοντέλο αναφοράς TCP/IP

Το μοντέλο αναφοράς TCP/IP (*TCP/IP Reference Model*) δημιουργήθηκε για να καλύψει την ανάγκη ενός δικτύου που να μπορεί να '*επιβιώνει*' κάτω από οποιεσδήποτε συνθήκες. Οι αρχικές έρευνες και υλοποιήσεις έγιναν προς τα τέλη της δεκαετίας του 1970 από τους επιστήμονες του Αμερικανικού Υπουργείου Άμυνας. (DoD, *Department of Defense*). Ίσως κανείς εκείνη την εποχή δεν ήταν σε θέση να προβλέψει, ούτε καν να οραματιστεί, ότι το σημερινό *Internet* στηρίχθηκε σε αυτές τις ιδέες.

Τα τέσσερα επίπεδα του μοντέλου TCP/IP είναι:

- Επίπεδο Πρόσβασης στο Δίκτυο, *Network Access Layer*
- Επίπεδο Διαδικτύου, *Internet Layer*
- Επίπεδο Μεταφοράς, *Transport Layer*
- Επίπεδο Εφαρμογών, *Application Layer*

Θα προχωρήσουμε σε μία παρουσίαση των λειτουργιών του κάθε επιπέδου, καθώς και σε μία παράλληλη μελέτη των δύο μοντέλων αναφοράς, του OSI και του TCP/IP (**Εικόνα 3.1**[1]).



Εικόνα 3.1 OSI και TCP/IP

[1] http://commons.wikimedia.org/wiki/File:Application_Layer.png

Επίπεδο Εφαρμογών (*Application*): το μοντέλο TCP/IP συγκεντρώνει όλες τις λειτουργίες των εφαρμογών σε ένα επίπεδο. Έτσι το TCP/IP *Application Layer* αναλαμβάνει την αναπαράσταση, την κωδικοποίηση και τον έλεγχο του διαλόγου σε επίπεδο εφαρμογής. Πρωτόκολλα του επιπέδου αυτού είναι τα FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*), Telnet, DNS (*Domain Name System*).

Επίπεδο Μεταφοράς (*Transport*): Είναι το 3° Επίπεδο του μοντέλου TCP/IP και αναλαμβάνει τον τεμαχισμό και την επανασυναρμολόγηση των δεδομένων που πηγάζουν από τις εφαρμογές. Εδώ τα πρωτόκολλα λειτουργούν κατά περίπτωση με περισσότερη ή λιγότερη αξιοπιστία υλοποιώντας από άκρο σε άκρο (*end-to-end*) λειτουργίες. Η επικοινωνία από άκρο σε άκρο, ο έλεγχος ροής και η αξιόπιστη μετάδοση μέσω αρίθμησης και επιβεβαίωσης λήψης είναι μερικά από τα καθήκοντα του Επιπέδου Μεταφοράς του μοντέλου TCP/IP, με τα TCP (*Transmission Control Protocol*) και UDP (*User Datagram Protocol*) να είναι τα βασικά πρωτόκολλα.

Στο Επίπεδο Διαδικτύου (*Internet*) του TCP/IP πραγματοποιείται η επιλογή της καλύτερης διαδρομής (*best path determination*) και η προώθηση των πακέτων (*packet forwarding*). Οι σημαντικότερες λειτουργίες του IP (*Internet Protocol*) είναι η λογική διευθυνσιοδότηση (*logical addressing*), η δημιουργία πακέτων και η δρομολόγησή τους προς τον προορισμό.

Το Πρώτο Επίπεδο του μοντέλου TCP/IP συγκεντρώνει τις λειτουργίες των δύο χαμηλότερων επιπέδων του μοντέλου OSI, δηλαδή προετοιμάζει και μεταδίδει το πακέτο πάνω στο φυσικό μέσο. Αυτό περιλαμβάνει όλες τις σχετικές LAN (Ethernet, Token Ring κλπ) και WAN (PPP, Frame Relay, HDLC) τεχνολογίες καθώς και τις μεθόδους ηλεκτρικής και μηχανικής διασύνδεσης.

Αντιπαραβάλλοντας τα δύο μοντέλα, TCP/IP και OSI, αρχικά επισημαίνουμε ότι το TCP/IP είναι ένα μοντέλο πρωτοκόλλων (*protocol model*) ενώ το OSI είναι ένα μοντέλο αναφοράς (*reference model*). Ένα μοντέλο πρωτοκόλλων περιγράφει τις λειτουργίες κάθε επιπέδου μέσα σε μία συγκεκριμένη σουίτα πρωτοκόλλων, στην περίπτωσή μας τη σουίτα TCP/IP. Ένα μοντέλο αναφοράς παρέχει ένα κοινό πλαίσιο για τη σχεδίαση και λειτουργία των υποδομών χωρίς όμως να είναι μία προδιαγραφή υλοποίησης. Σχετικά με τα κοινά σημεία των δύο μοντέλων:

- Και τα δύο ακολουθούν τη διαστρωματωμένη (*layered*) φιλοσοφία.
- Και τα δύο έχουν επίπεδο Εφαρμογών, αν και οι υπηρεσίες είναι διαφορετικές στο καθένα.
- Και τα δύο έχουν συγκρίσιμα επίπεδα μεταφοράς και δικτύου.
- Και τα δύο στηρίζονται σε τεχνολογίες μεταγωγής πακέτου (*packet switching*) και όχι μεταγωγής κυκλώματος (*circuit switching*).

Όσο για τις διαφορές τους:

- Το μοντέλο TCP/IP συνδυάζει τα τρία ανώτερα επίπεδα του OSI στο δικό του *Application Layer*.

- Το μοντέλο TCP/IP συνδυάζει τα δύο χαμηλότερα επίπεδα του OSI στο δικό του *Network Access Layer*.
- Το μοντέλο OSI, ως αναλυτικότερο, χρησιμοποιείται περισσότερο στην εκπαίδευση / κατάρτιση για την καλύτερη κατανόηση των μηχανισμών της επικοινωνίας.

3.2 Διευθύνσεις IP

Δύο βασικές λειτουργίες του πρωτοκόλλου IP είδαμε ότι είναι η από άκρο σε άκρο (*end-to-end* ή *host-to-host*) επικοινωνία και η λογική διευθυνσιοδότηση (*logical addressing*). Η IP διεύθυνση είναι ένας αριθμός με ιεραρχική δομή, με την έννοια ότι υποστηρίζει τη δημιουργία ομάδων από συσκευές (*hosts*). Κάθε τέτοια ομάδα λέγεται δίκτυο (*network*) ή υποδίκτυο (*subnet*) και κατά περίπτωση θα τη συναντήσουμε και ως *broadcast domain*.Τα πιο σημαντικά *bits* του αριθμού είναι κοινά για μηχανήματα που ανήκουν στο ίδιο δίκτυο, ενώ τα λιγότερο σημαντικά καθορίζουν το συγκεκριμένο *host*. Μέσα σε ένα τοπικό δίκτυο ένα *host*, ή καλύτερα μία κάρτα δικτύου (*network adapter* ή *network interface card, NIC*), προσδιορίζεται μοναδικά και από μία φυσική διεύθυνση, τη MAC (*Medium Access Control*) *address*.

Ανατομία μίας IP διεύθυνσης

Η IP διεύθυνση είναι ένας αριθμός που αποτελείται από 32 *bits*. Για την αναπαράστασή του στο χαρτί χρησιμοποιούμε μία μορφή που λέγεται *dotted decimal*: ο δυαδικός αριθμός των 32 *bits* χωρίζεται με τελείες (*dots*) σε τέσσερα πεδία των οκτώ *bits* το καθένα, και το κάθε πεδίο παριστάνεται σε δεκαδική μορφή. Για παράδειγμα, σε δυαδική μορφή η IP διεύθυνση είναι:

11000000101010000000000100001000

Χωρίζοντας τον αριθμό σε τέσσερα πεδία προκύπτει:

11000000.10101000.00000001.00001000

Και τελικά, με τη μετατροπή στο δεκαδικό σύστημα προκύπτει:

192.168.1.8

Είδαμε ότι τα πιο σημαντικά bits του αριθμού ορίζουν το δίκτυο, και θα τα συναντήσουμε ως τμήμα δικτύου (*network part* ή *network portion*) της διεύθυνσης. Τα λιγότερο σημαντικά *bits* αποτελούν το τμήμα υπολογιστή (*host part* ή *host portion*) της IP διεύθυνσης. Όπως μας διδάσκει η συνδυαστική, όσο περισσότερα *bits* έχει το *host part*, τόσο περισσότερα μηχανήματα μπορούν να διευθυνσιοδοτηθούν από το συγκεκριμένο δίκτυο.

Κλάσεις IP διευθύνσεων

Για τη διαχείριση της δυνατότητας διευθυνσιοδότησης μεγαλύτερων ή μικρότερων δικτύων οι IP διευθύνσεις έχουν χωριστεί σε κλάσεις, που ορίζονται ανάλογα με την τιμή της πρώτης οκτάδας:

Κλάση IP διεύθυνσης	1η οκτάδα, δυαδικό	1η οκτάδα, δεκαδικό

Κλάση A	**0**0000000 – **0**1111111	1 – 126
Κλάση B	**10**000000 – **10**111111	128 – 191
Κλάση C	**110**00000 – **110**11111	192 – 223
Κλάση D	**1110**0000 – **1110**1111	224 – 239
Κλάση E	**1111**0000 – **1111**1111	240 – 255

Οι αριθμοί της κλάσης A χρησιμοποιούν την πρώτη οκτάδα για το τμήμα του δικτύου και τις υπόλοιπες τρεις (24 *bits*) για το τμήμα του *host*. Χρησιμοποιούνται σε πολύ μεγάλα δίκτυα, με εκατομμύρια διαθέσιμες *host* διευθύνσεις. Το δίκτυο 127.0.0.0 από άποψη αριθμητικής ανήκει στην κλάση A, όμως δεν μπορεί να χρησιμοποιηθεί σε ένα πραγματικό IP *interface*. Πρόκειται για *loopback* διευθύνσεις, που χρησιμοποιούνται για να κατευθύνει ένας *host* πακέτα στον εαυτό του, κάτι πολύ χρήσιμο για δοκιμές (*testing)*.

Η κλάση B έχει σχεδιαστεί για μεσαία / μεγάλα δίκτυα, με το κομμάτι του δικτύου να καταλαμβάνει τα δύο πρώτα *bytes* και το τμήμα του *host* τα άλλα δύο. Αντίστοιχα στην κλάση C τρεις οκτάδες χρησιμοποιούνται για να προσδιορίσουν το δίκτυο και μία για να προσδιορίσει το *host*. Έως 254 προς χρήση IP διευθύνσεις μπορούν να διατεθούν από ένα δίκτυο κλάσης C.

Οι κλάσεις D και E έχουν ειδικές χρήσεις. Οι αριθμοί με κλάση D χρησιμοποιούνται ως *multicast* διευθύνσεις. Όταν ένα IP πακέτο έχει μία *multicast* διεύθυνση προορισμού, αυτό απευθύνεται σε περισσότερους από έναν *hosts*. Η κλάση E χρησιμοποιείται για ερευνητικούς σκοπούς. Δε θα δούμε να χρησιμοποιούνται σε ένα πραγματικό δίκτυο διευθύνσεις από την κλάση αυτή.

Δημόσιες και ιδιωτικές διευθύνσεις

Κάθε μηχάνημα στο δημόσιο *Internet* έχει μία μοναδική διεύθυνση IP. Οι προς χρήση διευθύνσεις είναι πεπερασμένες και, με τη ραγδαία εξάπλωση του Διαδικτύου τέθηκε γρήγορα το θέμα της εξάντλησής τους. Ένα εντελώς νέο σύστημα λογικής διευθυνσιοδότησης των δημόσιων *hosts*, δηλαδή ένα νέο πρωτόκολλο του 3^{ου} Επιπέδου, θα ήταν η οριστική λύση στο πρόβλημα. Μέχρι όμως το νέο αυτό πρωτόκολλο (πρόκειται ασφαλώς για το IPv6) να εδραιωθεί, το *Private Addressing (ιδιωτική διευθυνσιοδότηση)* σε συνδυασμό με τη μετάφραση (NAT, *Network Address Translation*) χρησιμοποιούνται σαν μία προσωρινή λύση (*workaround*). Οι ιδιωτικές διευθύνσεις μπορούν να επαναχρησιμοποιούνται σε δύο οικίες, σχολεία ή εταιρικά δίκτυα, σε οποιοδήποτε μέρος του κόσμου. Οι διευθύνσεις αυτές δε μπορούν να δρομολογηθούν στο Διαδίκτυο. Προκειμένου να αποκτήσουν τα 'εντός' μηχανήματα πρόσβαση στις υπηρεσίες του *Internet* χρησιμοποιούνται τεχνικές μετάφρασης (NAT) της IP διεύθυνσης προέλευσης.

Το *RFC 1918* ορίζει τρία blocks ιδιωτικών IP διευθύνσεων ως εξής:

Κλάση	**Διάστημα Ιδιωτικών Διευθύνσεων του RFC 1918**
A	10.0.0.0 έως 10.255.255.255

B	172.16.0.0 έως 172.31.255.255
C	192.168.0.0 έως 192.168.255.255

Με τον τρόπο αυτό, οι υπολογιστές μίας σχολικής αίθουσας στην Αθήνα και το Τορόντο μπορεί να χρησιμοποιούν διευθύνσεις από το δίκτυο 192.168.10.0 για τη μεταξύ τους 'εσωτερική' επικοινωνία και να απολαμβάνουν των υπηρεσιών του 'εξωτερικού' *Internet* με μεταφρασμένες, παγκόσμια μοναδικές, διευθύνσεις.

Λογικές και φυσικές διευθύνσεις

Θεωρούμε εδώ αναγκαία την αντιπαραβολή ανάμεσα στις διευθύνσεις IP και MAC ενός *host*. Η βασική διαφορά είναι ότι η IP είναι μία λογική διεύθυνση του 3^{ου} Επιπέδου του OSI, ενώ η MAC είναι η φυσική διεύθυνση του 2^{ου} Επιπέδου. Επιστρέφοντας στη λογική και φυσική διευθυνσιοδότηση, μπορούμε να παραθέσουμε τον παρακάτω πίνακα:

Διεύθυνση IP	**Διεύθυνση MAC**
Λειτουργεί στο 3^{ο} Επίπεδο του OSI	Λειτουργεί στο 2^{ο} Επίπεδο του OSI
Λογική διεύθυνση	Φυσική διεύθυνση
Ιεραρχική δομή (*hierarchical addressing*)	Μη-ιεραρχική δομή (*flat addressing*)
Έχει μήκος 32 *bits*	Έχει μήκος 48 *bits*
Παράσταση σε *dotted decimal* μορφή	Παράσταση σε δεκαεξαδική μορφή
Αποδίδεται από τη διαχείριση του δικτύου, είτα αυτόματα είτε με το χέρι	Αποδίδεται στην κατασκευή και δεν αλλάζει (*burned address*)

3.3 Ανάθεση IP διευθύνσεων, τα πρωτόκολλα ARP / RARP

Κάθε μηχάνημα μέσα σε ένα IP δίκτυο πρέπει να έχει τη δική του ξεχωριστή λογική διεύθυνση. Αυτή μπορεί να αποδοθεί είτε στατικά είτε δυναμικά.

Λέγοντας στατική απόδοση (*static assignment*) της διεύθυνσης IP, εννοούμε ότι αυτή ρυθμίζεται με το χέρι από το διαχειριστή του δικτύου και παραμένει η ίδια μέχρι ο διαχειριστής να την αλλάξει. Οι εξυπηρετητές, οι δρομολογητές ή οι κοινοί εκτυπωτές είναι hosts του δικτύου μας στους οποίου αποδίδουμε μία διεύθυνση IP με το χέρι.

Η δυναμική (*dynamic*) ανάθεση στηρίζεται σε ένα πρωτόκολλο που τρέχει τόσο στον *host* που αναζητά διεύθυνση IP όσο και σε κάποιον εξυπηρετητή. Πρόκειται δηλαδή για μία αρχιτεκτονική τύπου πελάτη / εξυπηρετητή (*client / server*). Πριν μελετήσουμε τέτοιες μεθόδους, ενδείκνυται να συζητήσουμε για το *Address Resolution Protocol*, ARP.

Ας θεωρήσουμε ένα host που θέλει να στείλει δεδομένα μέσα στο τοπικό δίκτυο σε ένα συγκεκριμένο προορισμό (*unicast* κίνηση). Κατά τη διαδικασία της ενθυλάκωσης

(*encapsulation*) ο αποστολέας οφείλει να 'κατεβάσει' το IP πακέτο στο επίπεδο Σύνδεσης Δεδομένων και να το τοποθετήσει σε ένα Ethernet πλαίσιο. Για τη συμπλήρωση όλων των πεδίων του πλαισίου, είναι απαραίτητη η γνώση της φυσικής (MAC) διεύθυνσης του υπολογιστή προορισμού. Το πρωτόκολλο ARP παρέχει λοιπόν τη φυσική (OSI *Layer* 2) διεύθυνση όταν είναι γνωστή η λογική (OSI *Layer* 3) διεύθυνση ενός μηχανήματος. Αυτό γίνεται με την αποστολή ειδικών μηνυμάτων ευρυεκπομπής (*broadcast*) από τον αποστολέα, με σκοπό τη δημιουργία και συντήρηση του πίνακα ARP. Ο πίνακας αυτός αντιστοιχίζει τη διεύθυνση IP με τη διεύθυνση MAC για κάθε υπολογιστή μέσα στο τοπικό μας δίκτυο.

Το πρωτόκολλο RARP (*Reverse Address Resolution Protocol*) αποδίδει μία διεύθυνση IP σε έναν υπολογιστή όταν είναι γνωστή η MAC του. Ο υπολογιστής που δε γνωρίζει την IP διεύθυνσή του στέλνει ένα αίτημα (RARP *Request*) στο δίκτυο μέχρι ένας εξυπηρετητής (RARP *Server*) να απαντήσει και να του στείλει την IP. Μειονέκτημα του RARP είναι ότι δε μπορεί να ρυθμίσει άλλες παραμέτρους (π.χ. την προεπιλεγμένη πύλη) παρά μόνο την IP διεύθυνση. Αντίθετα, το πρωτόκολλο DHCP (*Dynamic Host Configuration Protocol*) παρέχει μία μεγάλη συλλογή ρυθμίσεων (DHCP *options*) και χρησιμοποιείται σήμερα για την αυτόματη απόδοση των IP ρυθμίσεων (IP *settings*) των υπολογιστών στο τοπικό δίκτυο.

3.4 Διαγνωστικά εργαλεία του TCP/IP, το ICMP

Το πρωτόκολλο IP μεταφέρει πακέτα από την πηγή στον προορισμό με έναν μη-αξιόπιστο τρόπο, με την έννοια ότι δε διαθέτει τρόπο για την επιβεβαίωση της ορθής λήψης στον προορισμό (*best effort delivery*). Ένα πακέτο μπορεί να μη φθάσει στον προορισμό εξαιτίας αστοχίας του υλικού, κακών ρυθμίσεων ή λανθασμένης πληροφορίας δρομολόγησης. Για την αναγνώριση τέτοιων προβλημάτων, το IP διαθέτει ενσωματωμένα μία σειρά από διαγνωστικά εργαλεία, τα εργαλεία που παρέχονται από το πρωτόκολλο ICMP (*Internet Control Message Protocol*). Η χρήση των εντολών του ICMP είναι πολύ σημαντική κατά την προσπάθεια επίλυσης προβλημάτων (*troubleshooting*).

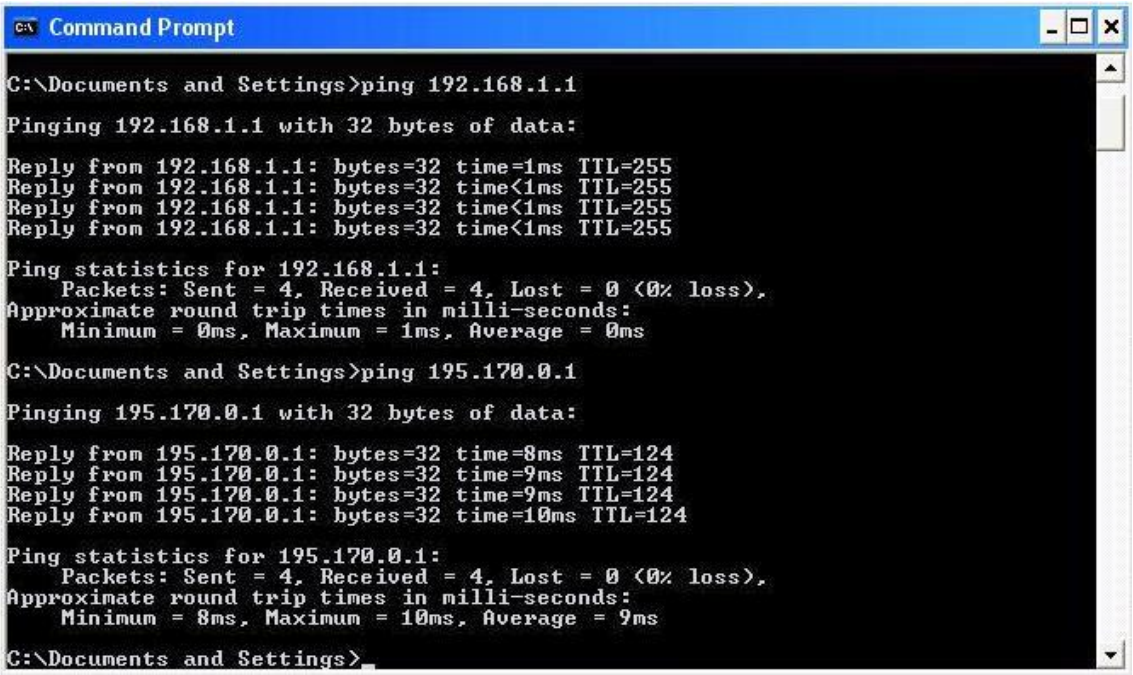
Το ICMP μήνυμα είναι ένα κοινό IP πακέτο, που ενθυλακώνεται σε ένα πλαίσιο από κάποιο LAN ή WAN πρωτόκολλο του Επιπέδου Πρόσβασης στο Δίκτυο. Ο τύπος του μηνύματος ορίζεται στο ομώνυμο πεδίο, ενώ ο κωδικός εξειδικεύει περαιτέρω για κάθε τύπο. Ο παρακάτω πίνακας δείχνει τους τύπους των ICMP μηνυμάτων

ICMP	Τύπος Μηνύματος
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect / change request
8	Echo request
9	Router advertisement
10	Router selection

11	Time exceeded
12	Parameter problem
13	Timestamp request
14	Timestamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask reply

Θα πρέπει να τονίσουμε ότι το ICMP παρέχει ένα μηχανισμό αναφοράς σφαλμάτων στο τρίτο Επίπεδο του μοντέλου OSI, και ενημερώνει μόνο τον αποστολέα του πακέτου για την αποτυχία στη μετάδοση. Δεν είναι δυνατή η ενημέρωση των ενδιάμεσων κόμβων για αλλαγές στην τοπολογία του δικτύου μέσω του πρωτοκόλλου ICMP.

Τα ICMP μηνύματα που όλοι ίσως έχουμε χρησιμοποιήσει είναι τα echo request και reply, το γνωστό μας ping. Η εντολή ping μας δίνει πληροφορία για τη διαθεσιμότητα ενός συγκεκριμένου host στο 3° Επίπεδο. Η **Εικόνα 3.2** μας δείχνει τη χρήση αυτής της εντολής από τη γραμμή εντολών ενός Windows host.



Εικόνα 3.2 ICMP echo request / reply

4 Υποδικτύωση, Subnetting

4.1 Τι είναι η υποδικτύωση

Η γρήγορη ανάπτυξη του *Internet* και οι ανάγκες διασύνδεσης των εταιρειών και οργανισμών απαίτησαν ένα μηχανισμό λογικού διαχωρισμού μίας IP κλάσης σε περισσότερα δίκτυα. Τα λογικά αυτά σύνολα IP αριθμών ονομάζονται υποδίκτυα, subnets.

Ένα υποδίκτυο δημιουργείται όταν δανειζόμαστε (*borrow*) *bits* από το τμήμα του υπολογιστή (*host part*) για το τμήμα του δικτύου (*network part*), ξεκινώντας ασφαλώς από έναν *classfull* IP αριθμό. Θεωρείστε για παράδειγμα το δίκτυο κλάσης C 195.170.10.0. Η τελευταία οκτάδα αντιπροσωπεύει το *host part*. Εάν δανειστούμε τα τρία σημαντικότερα (αριστερά) *bits* του *host part*, τότε προκύπτει ο παρακάτω πίνακας:

195.170.10.00000000 ➔ 195.170.10.**000**|00000		
195.170.10.**000**|00000	195.170.10.0 /27	1° υποδίκτυο
195.170.10.**001**|00000	195.170.10.32 /27	2° υποδίκτυο
195.170.10.**010**|00000	195.170.10.64 /27	3° υποδίκτυο
195.170.10.**011**|00000	195.170.10.96 /27	4° υποδίκτυο
195.170.10.**100**|00000	195.170.10.128 /27	5° υποδίκτυο
195.170.10.**101**|00000	195.170.10.160 /27	6° υποδίκτυο
195.170.10.**110**|00000	195.170.10.192 /27	7° υποδίκτυο
195.170.10.**111**|00000	195.170.10.224 /27	8° υποδίκτυο

Έχοντας δανειστεί 3 *host bits*, δημιουργούμε 2^3=8 νέα υποδίκτυα. Από αυτά, το πρώτο λέγεται και *subnet zero*, γιατί όλα τα δανεισμένα *bits* είναι ίσα με μηδέν. Αντίστοιχα, το τελευταίο (εδώ το 8°) υποδίκτυο, λέγεται και *subnet ones*, μιας και τα δανεισμένα *bits* είναι όλα ένα. Στους παλαιότερους δρομολογητές δεν ήταν δυνατό να χρησιμοποιηθούν αυτά τα δύο υποδίκτυα, για αυτό και συχνά μπορεί να συναντήσουμε ότι τα προς χρήση υποδίκτυα είναι 2^n-2, όπου n ο αριθμός των δανεισμένων από το *host part bits*.

4.2 Προεπιλεγμένες και προσαρμοσμένες μάσκες

Ένας IP *host* χρησιμοποιεί την IP διεύθυνση σε συνδυασμό με τη μάσκα υποδικτύου (*subnet mask*) για να βρει σε ποιο IP δίκτυο ανήκει, κάνοντας την πράξη του λογικού ΚΑΙ (AND) ανάμεσα στους δύο αριθμούς. Ο παρακάτω πίνακας δείχνει τις προεπιλεγμένες μάσκες (*default subnet masks*) για τις τρεις βασικές κλάσεις IP αριθμών.

Κλάση	Μήκος του Network Part	Μάσκα υποδικτύωσης
A	8 bits	255.0.0.0
B	16 bits	255.255.0.0
C	24 bits	255.255.255.0

Με το δανεισμό *bits* από το *Network part* αυξάνεται το μήκος της μάσκας υποδικτύωσης σε σχέση με την προεπιλεγμένη. Θεωρείστε το δίκτυο κλάσης C 195.170.10.0. Ανάλογα με το πλήθος των δανεισμένων bits, επιβάλλονται οι *subnet masks* του πίνακα:

Δανεισμένα Bits	Μήκος Μάσκας	Μάσκα
0	24 bits	255.255.255.0
1	25 bits	255.255.255.128
2	26 bits	255.255.255.192
3	27 bits	255.255.255.224
4	28 bits	255.255.255.240
5	29 bits	255.255.255.248
6	30 bits	255.255.255.252

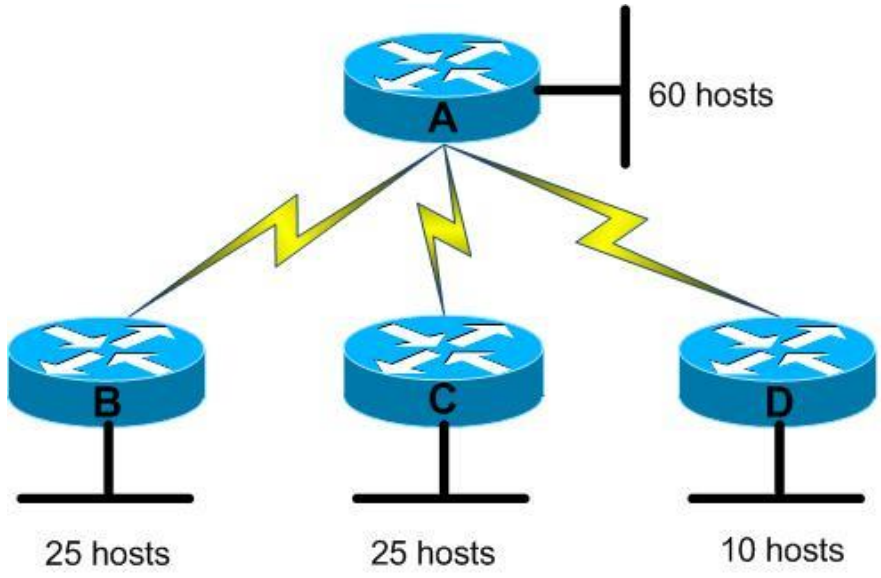
4.3 Διευθύνσεις δικτύου και ευρυεκπομπής

Όταν το μήκος του τμήματος υπολογιστή (*host part*) ενός IP αριθμού είναι n, τότε οι διαθέσιμοι συνδυασμοί είναι ασφαλώς 2^n. Μπορούν να χρησιμοποιηθούν όλοι αυτοί οι IP αριθμοί για να διευθυνσιοδοτήσουν πραγματικούς *hosts* μέσα στο υποδίκτυο; Όταν όλα τα *host bits* είναι ίσα με μηδέν ή ένα, τότε οι αριθμοί που προκύπτουν είναι δεσμευμένοι και δε μπορούν να ρυθμιστούν σε ένα πραγματικό μηχάνημα. Ο πρώτος λέγεται διεύθυνση δικτύου (*network address*), και χρησιμοποιείται για την περιγραφή ολόκληρου του δικτύου, μαζί ασφαλώς με τη μάσκα υποδικτύου. Ο δεύτερος λέγεται διεύθυνση ευρυεκπομπής (*broadcast address*) και αναφέρεται στο σύνολο των *hosts* του δικτύου. Άρα, με n δανεισμένα *bits* το πλήθος των προς χρήση IP διευθύνσεων είναι ίσο με 2^n-2.

Παραδείγματα και αριθμητικά προβλήματα υποδικτύωσης (*subnetting*) δίνονται στο Παράρτημα Α.

4.4 Υποδικτύωση με μάσκες διαφορετικού μήκους

Στην τοπολογία της **Εικόνας 4.1** έχουν σημειωθεί οι απαιτήσεις σε πλήθος διευθύνσεων για κάθε τοπικό δίκτυο. Όσο για τις WAN συνδέσεις, κάθε μία απαιτεί ασφαλώς ένα δίκτυο με τουλάχιστο δύο IP αριθμούς.



Εικόνα 4.1 VLSM

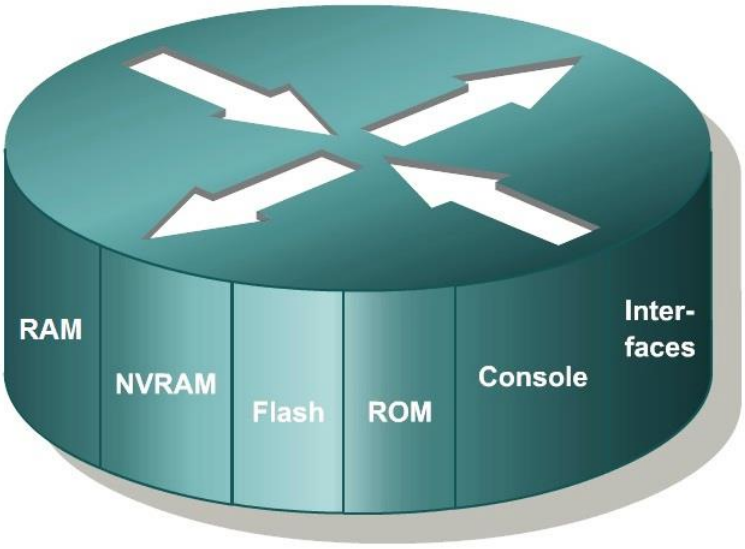
Σε ένα περιβάλλον χωρίς δυνατότητα υποδικτύωσης (*classfull addressing*) θα απαιτούνταν 7 διαφορετικές κλάσεις C, με 254 προς χρήση διευθύνσεις η καθεμία! Ένας πολύ μεγάλος αριθμός από IP διευθύνσεις (πόσες ακριβώς;) δε χρησιμοποιούνται, αλλά δεσμεύονται, χωρίς να μπορούν να διευθυνσιοδοτήσουν υπολογιστές σε άλλα δίκτυα. Στο ίδιο συμπέρασμα, αν και με μικρότερη έκταση, καταλήγουμε εάν υποθέσουμε ότι διαθέτουμε μόνο /26 υποδίκτυα (να υπολογιστεί και εδώ ακριβώς η σπατάλη των IP διευθύνσεων).

Η υποδικτύωση με μάσκες διαφορετικού μήκους (VLSM, *Variable Length Subnet Mask*) δίνει τη λύση σε αυτό το πρόβλημα, προτείνοντας διαφορετικές μάσκες, ανάλογα με το μέγεθος του προς διευθυνσιοδότηση δικτύου.

5 Εισαγωγή στους δρομολογητές

5.1 Ο δρομολογητής είναι ένας υπολογιστής

Είδαμε ότι ο δρομολογητής (*router*) είναι μία ενδιάμεση δικτυακή συσκευή που λειτουργεί στο 3^{ο} Επίπεδο του OSI με σκοπό την εύρεση της καλύτερης διαδρομής και την προώθηση των IP πακέτων. Πιο πρακτικά, ο δρομολογητής ενώνει IP δίκτυα μεταξύ τους. Κατασκευαστικά και λειτουργικά ένας δρομολογητής δε διαφέρει από ένα οποιοδήποτε υπολογιστικό σύστημα. Διαθέτει επεξεργαστή, λειτουργικό σύστημα, μόνιμη και πτητική μνήμη και είσοδο / έξοδο. Πιο συγκεκριμένα, και με αναφορά στην **Εικόνα 5.1**:



Εικόνα 5.1 Τα μέρη ενός δρομολογητή

Η **RAM** είναι η γρήγορη πτητική μνήμη στην οποία φορτώνεται το λειτουργικό σύστημα όταν εκκινεί ο δρομολογητής και φιλοξενεί όλους τους πίνακες που αυτός χρησιμοποιεί για τη λειτουργία του.

Η **NVRAM** είναι η μη-πτητική μνήμη που φιλοξενεί το αρχείο των ρυθμίσεων (*configuration file*).

Η **flash** είναι μία μόνιμης αποθήκευσης μνήμη τεχνολογίας EEPROM που αναλαμβάνει τη φύλαξη του λειτουργικού συστήματος.

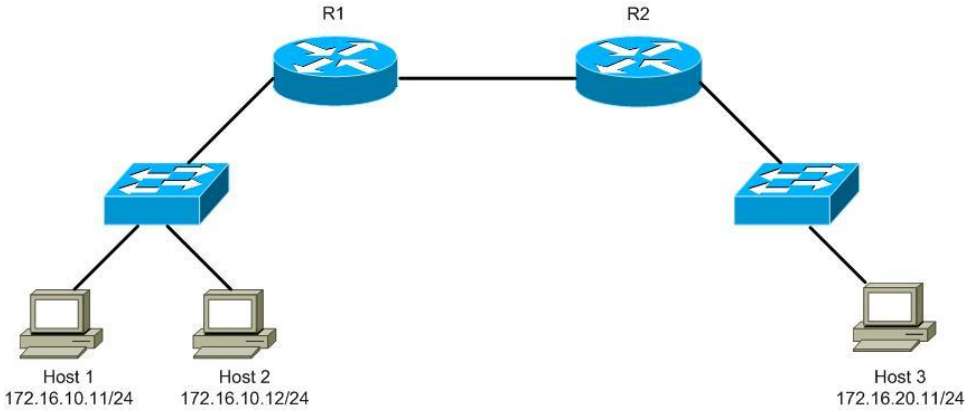
Το **λειτουργικό σύστημα** ενός δρομολογητή είναι ουσιαστικά ένα *embedded software* που 'συντονίζει' το υλικό και εκτελεί τις εντολές. Το λειτουργικό σύστημα, π.χ. ενός δρομολογητή Cisco καλείται IOS (*Internetworking Operating System*).

Η μνήμη **ROM** είναι σε μορφή ολοκληρωμένου πάνω στη μητρική και κρατά αποθηκευμένες τις εντολές για το αρχικό POST (*Power-On Self Test*) καθώς και το πρόγραμμα bootstrap.

Τέλος, ο δρομολογητής μπορεί να μη διαθέτει ο ίδιος ποντίκι, πληκτρολόγιο ή οθόνη, έχει όμως μία σειρά από **διεπαφές (*interfaces*)** που παρέχουν πρόσβαση στις εντολές του λειτουργικού συστήματος είτε μέσω γραμμής εντολών είτε μέσω γραφικού περιβάλλοντος.

5.2 Μεταφέροντας πακέτα από άκρο σε άκρο

Στην **Εικόνα 5.2** ας θεωρήσουμε την επικοινωνία από τον Υπολογιστή 1 (στο εξής Host 1) προς στον Υπολογιστή 2 (Host 2).



Εικόνα 5.2 Η ζωή ενός πακέτου

- Το IP πακέτο που ξεκινά από τον Host 1 έχει IP διεύθυνση αφετηρίας την 172.16.10.11 και προορισμού την 172.16.20.11. Με χρήση της μάσκας υποδικτύωσης ο Host 1 εξάγει το δίκτυο προορισμού και αντιλαμβάνεται ότι το πακέτο απευθύνεται σε ένα δίκτυο διαφορετικό από το δικό του, άρα το προωθεί στην προεπιλεγμένη πύλη του (default gateway). [Για την ακρίβεια κάνει αναφορά στον πίνακα δρομολόγησης που διαθέτει και διαλέγει την εγγραφή που ταιριάζει καλύτερα, (βλ. αντίστοιχη ενότητα)].
- Η κάρτα δικτύου του Host 1 είναι λοιπόν υποχρεωμένη να δημιουργήσει ένα Ethernet πλαίσιο με MAC διεύθυνση προορισμού αυτή του τοπικού interface του R1. Για να γίνει αυτό, ο Host 1 πρέπει να βρει τη διεύθυνση MAC του R1, κάτι που κάνει παράγοντας ένα ARP request για την IP του R1. Η απάντηση θα είναι ένα ARP reply με τη MAC του R1, την οποία βάζει σαν διεύθυνση προορισμού του πλαισίου Ethernet.
- Το Ethernet πλαίσιο φθάνει στο δρομολογητή R1.
- Ο R1 αφαιρεί τη Layer 2 πληροφορία και διαβάζει την IP διεύθυνση προορισμού του πακέτου. Αφού παραλήπτης στο IP δεν είναι ο ίδιος ο δρομολογητής (είναι ο Host 3), κάνει αναφορά στον δικό του πίνακα

δρομολόγησης και αποφασίζει να το προωθήσει στο άλλο του interface (προς τα δεξιά), δηλαδή προς τον R2.

- Για να προωθηθεί μέχρι τον R2 το πακέτο θα πρέπει να ενθυλακωθεί σε ένα πλαίσιο που να ταιριάζει με την τεχνολογία της διασύνδεσης ανάμεσα στους δύο δρομολογητές. Ανάλογα με το πρωτόκολλο, μπορεί να υπάρχει ή όχι διεύθυνση προορισμού σε αυτό. Για παράδειγμα αν η σύνδεση είναι PPP, τότε δεν υπάρχει, ενώ αν είναι Frame Relay, υπάρχει ένα αναγνωριστικό σύνδεσης, όχι προορισμού.
- Σε αυτό το σημείο μπορεί να γίνει κατακερματισμός (fragmentation) του πακέτου, εφόσον το μέγεθός του δεν χωρά στο μέγιστο μέγεθος εκπομπής (Maximum Transmission Unit – MTU) του πρωτοκόλλου του δικτύου. Εφόσον αυτό απαιτηθεί, το IP διαθέτει τα κατάλληλα πεδία στην κεφαλίδα του, έτσι ώστε όταν τα τεμάχια φτάσουν στον τελικό αποδέκτη να μπορούν να ανασυντεθούν στο αρχικό πακέτο που κατακερματίστηκε.
- Ο R2 λαμβάνει το πλαίσιο (π.χ. PPP), αφαιρεί τη Layer 2 πληροφορία και με τη σειρά του διαβάζει την IP διεύθυνση προορισμού (παραμένει η 172.16.20.11) και αποφασίζει να το προωθήσει προς τα δεξιά, στο τοπικό του δίκτυο.
- Για να μπει το IP πακέτο στο τοπικό δίκτυο του R2, αυτός είναι υποχρεωμένος να δημιουργήσει ένα Ethernet πλαίσιο με MAC διεύθυνση προορισμού αυτή του Host 3. Και πάλι, ο R2 πρέπει να ανακαλύψει τη διεύθυνση MAC του Host 3, κάτι που κάνει με χρήση του πρωτοκόλλου ARP.
- Ο Host 3 λαμβάνει το πλαίσιο και με τη διαδικασία της αποθυλάκωσης (decapsulation) το επεξεργάζεται, ανεβάζοντάς το στο λειτουργικό σύστημα και τις εφαρμογές του.
- Η επικοινωνία είναι πάντα αμφίδρομη, δηλαδή ο Host 3 επικοινωνεί στην αντίθετη κατεύθυνση με τον Host 1 για να στείλει απαντήσεις κτλ.

Παρατηρούμε λοιπόν ότι στο Layer 2 τα πλαίσια (άρα και οι φυσικές διευθύνσεις) αλλάζουν ανάλογα με το μέσο (*media dependent*). Αντίθετα, οι λογικές διευθύνσεις του Layer 3 (δηλαδή οι IP διευθύνσεις αφετηρίας και προορισμού) παραμένουν από άκρο σε άκρο. Για αυτό λέμε ότι στο Τρίτο Επίπεδο του OSI υλοποιείται *host-to-host* επικοινωνία, με τους δρομολογητές να αναλαμβάνουν ενδιάμεσα την προώθηση των πακέτων προς τον προορισμό.

Σημειώνουμε επίσης τα ακόλουθα:

α) Οι δρομολογητές παίζουν το ρόλο του ενδιάμεσου, όχι της πηγής ή του αποδέκτη.

β) Οι δρομολογητές παίρνουν την απόφαση για το που θα μετάγουν την πληροφορία ανεξάρτητα, χωρίς να συνεργάζονται.

γ) Τα πακέτα IP διαθέτουν μόνο πληροφορία διεύθυνσης αποστολέα-παραλήπτη, όχι του δρόμου που πρέπει να ακολουθήσουν (εξαίρεση αποτελεί στο source routing). Οι δρομολογητές παίρνουν τις αποφάσεις, όχι μόνο ανεξάρτητα, αλλά πιθανώς και δυναμικά, ανάλογα με τις συνθήκες του δικτύου και κάθε πακέτο IP δρομολογείται με τον καλύτερο δυνατό τρόπο (best effort) και ανεξάρτητα από τα υπόλοιπα, ακόμα και αν ανήκει στην ίδια ομάδα/αρχείο.

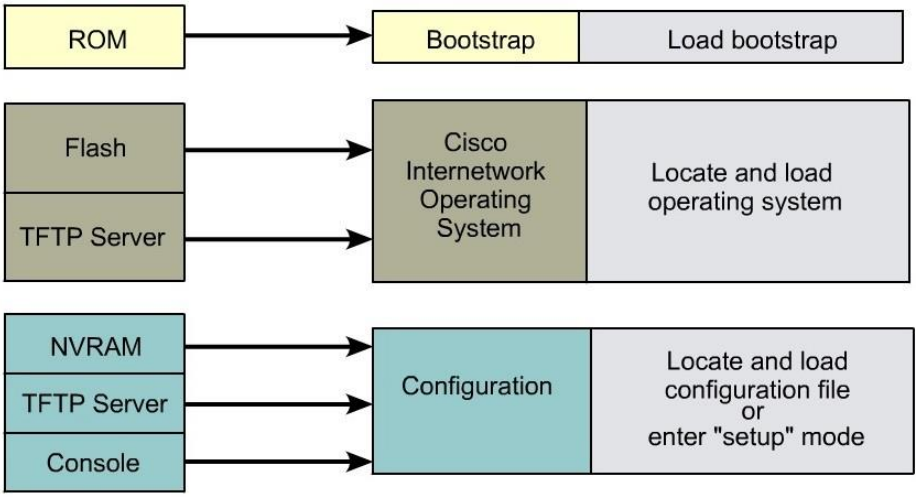
δ) Οι δρομολογητές μετάγουν τα πακέτα από τη διεπαφή εισόδου στη διεπαφή εξόδου, διαβάζοντας δεδομένα που βρίσκονται στην κεφαλίδα IP (3^{ου} επιπέδου δικτύου) του πακέτου, κάνουν δηλαδή μεταγωγή 3^{ου} επιπέδου, η οποία περιλαμβάνει και τη λειτουργία της δρομολόγησης (αναφορά στον πίνακα δρομολόγησης).

5.3 Εκκίνηση του δρομολογητή

Για να μπορέσει ένας δρομολογητής να λειτουργήσει ως τέτοιος, τρία είναι τα βήματα που πρέπει να ολοκληρωθούν με επιτυχία:

- Όλα τα υποσυστήματα του υλικού λειτουργούν σωστά.
- Εύρεση του λειτουργικού συστήματος και φόρτωσή του στη RAM.
- Εύρεση και φόρτωση του αρχείου των ρυθμίσεων ή εκκίνηση σε 'setup mode'.

Πιο αναλυτικά, η **Εικόνα 5.3** παρουσιάζει την εκκίνηση ενός δρομολογητή Cisco.



Εικόνα 5.3 Εκκίνηση δρομολογητή

- Εκτελείται το πρόγραμμα bootstrap από τη ROM. Πρόκειται για μία σειρά από εντολές που ελέγχουν το υλικό και αρχικοποιούν το λειτουργικό σύστημα.
- Το λειτουργικό σύστημα εντοπίζεται, προεπιλεγμένα στη μνήμη flash ή εναλλακτικά σε έναν εξυπηρετητή TFTP, και φορτώνεται στη RAM, όπως περίπου συμβαίνει στον προσωπικό μας υπολογιστή όταν τα Windows φορτώνονται από το σκληρό δίσκο στη RAM.
- Εάν υπάρχει αρχείο ρυθμίσεων εκκίνησης (*startup configuration file*) τότε αυτό φορτώνεται στη RAM. Εάν όχι, τότε λέμε ότι το μηχάνημα είναι *out-of-the-box* και ο μόνος τρόπος να κάνουμε τις αρχικές ρυθμίσεις (*initial configuration*) είναι μέσω της σύνδεσης Console.

Αμέσως παρακάτω φαίνεται η εκκίνηση ενός δρομολογητή Cisco μέσα από τη γραμμή εντολών του IOS.

```
Self decompressing the image :
#############System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :
###########################################################################
[OK]
              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco  IOS  Software,  1841  Software  (C1841-ADVIPSERVICESK9-M),  Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
Image text-base: 0x60080608, data-base: 0x6270CD50


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found
at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
```

```
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team


         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

5.3 Βασική ρύθμιση δρομολογητή

Λέγοντας βασικές ρυθμίσεις δρομολογητή (*basic router configuration*) εννοούμε την ασφάλιση (*hardening*) της συσκευής και την ανάθεση IP διευθύνσεων στις λειτουργικές διεπαφές (*interfaces*).

Αρχικά ας δώσουμε όνομα στο δρομολογητή μας:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RTKY2
RTKY2(config)#
```

Από εδώ και στο εξής, μετά τη ρύθμιση του ονόματος, μπορούμε να γνωρίζουμε σε ποιο ακριβώς μηχάνημα εργαζόμαστε. Θυμίζουμε ότι σε ένα εταιρικό δίκτυο τα ονόματα των συσκευών και υπολογιστών ακολουθούν συνήθως κάποιους κανόνες, όπως στο παράδειγμά μας, όπου πρόκειται για το δεύτερο δρομολογητή της κεντρικής υπηρεσίας (RTKY2).

Όπως γνωρίζουμε, η ασφάλιση μίας συσκευής, είτε είναι ένα δικτυακό μηχάνημα, είτε ένας εξυπηρετητής, είτε ο προσωπικός μας υπολογιστής, περιλαμβάνει τον έλεγχο της πρόσβασης και την απενεργοποίηση υπηρεσιών και διαδικασιών που δε χρησιμοποιούνται. Μία στοιχειώδης ασφάλιση για ένα δρομολογητή απαιτεί την

προστασία του *privileged mode* και των γραμμών κονσόλας και εικονικού τερματικού. Πιο συγκεκριμένα:

```
RTKY2(config)#
RTKY2(config)#enable password clearpass
RTKY2(config)#enable secret encryptpass
RTKY2(config)#
```

Το `clearpass` είναι μη-κρυπτογραφημένο (*clear text*) ενώ το `encryptpass` έχει ισχυρή κατά md5 κρυπτογράφηση. Προσοχή: Στην περίπτωση ρύθμισης και των δύο κυριαρχεί το δεύτερο.

```
RTKY2(config)#
RTKY2(config)#line console 0
8RTKY2(config-line)#password myclass
RTKY2(config-line)#login
RTKY2(config-line)#exit
RTKY2(config)#
RTKY2(config)#line vty 0 15
RTKY2(config-line)#password myremote
RTKY2(config-line)#login
RTKY2(config-line)#exit
```

Το password `myclass` χρησιμοποιείται για τη σύνδεση κονσόλας στο δρομολογητή μας ενώ το `myremote` για την απομακρυσμένη διαχείριση μέσω `telnet`.

Ο δρομολογητής, ως δικτυακή συσκευή του 3^{ου} Επιπέδου του OSI, 'ενώνει' ή 'χωρίζει' IP δίκτυα, ανάλογα με το εάν θα δούμε τη λειτουργία του από τη σκοπιά του *routing* ή από τη σκοπιά του L3 *segmentation*. Σε κάθε περίπτωση, κάθε *interface* του δρομολογητή ανήκει σε διαφορετικό IP *subnet*. Οι παρακάτω εντολές του Cisco IOS χρησιμοποιούνται για τη διευθυνσιοδότηση και ενεργοποίηση των IP διεπαφών του *router* μας.

```
RTKY2(config)#interface fastethernet 0/0
RTKY2(config-if)#ip address 172.16.10.33 255.255.255.224
RTKY2(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

RTKY2(config-if)#exit
RTKY2(config)#interface fastethernet 0/1
RTKY2(config-if)#ip address 172.16.10.65 255.255.255.224
RTKY2(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

RTKY2(config-if)#exit
RTKY2(config)#interface serial 0/0/0
%Invalid interface type and number
RTKY2(config)#interface serial 0/1/0
RTKY2(config-if)#ip address 172.16.10.241 255.255.255.252
RTKY2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
RTKY2(config-if)#
```

Όπως συμβαίνει και με ένα έγγραφο που έχουμε ανοικτό, έτσι και με τις ρυθμίσεις, αυτές βρίσκονται προσωρινά στη RAM και εάν ο δρομολογητής σβήσει χωρίς να έχουν αποθηκευθεί, θα χαθούν. Η αποθήκευση των *working* ρυθμίσεων από τη RAM στην NVRAM γίνεται ως εξής:

```
RTKY2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RTKY2#
```

Το σύνολο των ρυθμίσεων του δρομολογητή δεν είναι παρά ένα μικρό *text* αρχείο, που μπορεί να αποθηκευθεί σε έναν απομακρυσμένο TFTP server και να κρατηθεί ως αντίγραφο ασφαλείας (*backup*). Σε περίπτωση αστοχίας υλικού ή απώλειας του `startup-config` το αρχείο των ρυθμίσεων μπορεί να φορτωθεί από τον TFTP server πίσω στο δρομολογητή μας. Για να είναι δυνατή αυτή η μεταφορά αρχείων από / προς τον TFTP server είναι ασφαλώς απαραίτητη η κατά TCP/IP επικοινωνία

ανάμεσα στα δύο μηχανήματα. Η εντολή που χρησιμοποιείται για την αντιγραφή στον TFTP server είναι η `copy startup-config tftp` και για το κατέβασμα των ρυθμίσεων από τον server η `copy tftp startup-config`:

```
RTTHE1#
RTTHE1#copy startup-config tftp
Address or name of remote host []? 172.16.12.22
Destination filename [RTTHE1-confg]?
Writing startup-config...!!
[OK - 426 bytes]

426 bytes copied in 0 secs
RTTHE1#
```

Τέλος, εκτός από το αρχείο με τις ρυθμίσεις (`startup-config`) ενδείκνυται και η αποθήκευση σε TFTP server του λειτουργικού συστήματος (IOS) του δρομολογητή μας. Χρησιμοποιούμε την εντολή `copy flash tftp`:

```
RTTHE1#copy flash tftp
Source filename []? c1841-ipbase-mz.123-14.T7.bin
Address or name of remote host []? 172.16.12.22
Destination filename [c1841-ipbase-mz.123-14.T7.bin]?
Writing c1841-ipbase-mz.123-
14.T7.bin!!!
```

```
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-advipservicesk9-mz.124-15.T1.bin"
… παράβλεψη τμήματος της εξόδου της εντολής …
A summary of U.S. laws governing Cisco cryptographic products may be found
at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

Συνοπτική εμφάνιση πληροφοριών για τις διεπαφές:

```
RTKY2#show ip interface brief
Interface          IP-Address      OK? Method Status                Protocol

FastEthernet0/0    172.16.10.33    YES manual up                      up

FastEthernet0/1    172.16.10.65    YES manual up                      up

Modem0/0/0         unassigned      YES unset  administratively down down

Modem0/0/1         unassigned      YES unset  administratively down down

Serial0/1/0        172.16.10.241   YES manual down                    down

Serial0/1/1        unassigned      YES unset  administratively down down

Vlan1              unassigned      YES unset  administratively down down
```

Εμφάνιση των τρεχουσών ρυθμίσεων στη RAM:

```
RTKY2#show running-config
Building configuration...

Current configuration : 915 bytes
!
version 12.4
… παράβλεψη τμήματος της εξόδου της εντολής …!
hostname RTKY2
!
!
!
enable secret 5 $1$mERr$A.sOoXbEVX5l7ayFFh/Uk0
enable password clearpass
!
… παράβλεψη τμήματος της εξόδου της εντολής …!
!
interface FastEthernet0/0
 ip address 172.16.10.33 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.10.65 255.255.255.224
 duplex auto
 speed auto
!
interface Modem0/0/0
 no ip address
 shutdown
!
interface Modem0/0/1
 no ip address
 shutdown
!
interface Serial0/1/0
 ip address 172.16.10.241 255.255.255.252
 clock rate 2000000
!
… παράβλεψη τμήματος της εξόδου της εντολής …!
!
line con 0
 password myclass
 login
line vty 0 4
 password myremote
 login
```

```
line vty 5 15
 password myremote
 login
!
!
!
end
RTKY2#
```

Αναλυτική εμφάνιση πληροφοριών για την κατάσταση μίας διεπαφής:

```
RTKY2#show interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0010.11b5.5801 (bia 0010.11b5.5801)
  Internet address is 172.16.10.33/27
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
RTKY2#
```

6 Δρομολόγηση

6.1 Τι είναι η δρομολόγηση

Μπορούμε να περιγράψουμε τη δρομολόγηση σαν μία συλλογή από κατευθύνσεις (*routes*) ώστε ένα πακέτο να φθάσει σε ένα δίκτυο προορισμού (*destination network*). Αυτές οι κατευθύνσεις μπορούν να δοθούν στο δρομολογητή είτε δυναμικά, από γειτονικά μηχανήματα είτε στατικά, από το χέρι του διαχειριστή του δικτύου.

Ένα *route* (διαδρομή) περιλαμβάνει το δίκτυο προορισμού (με μάσκα), το *interface* (διεπαφή) εξόδου και μία έκφραση κόστους. Λέγοντας *interface* εξόδου εννοούμε το *interface* που θα χρησιμοποιήσει ο δρομολογητής για να προωθήσει το πακέτο. Θυμόμαστε εδώ ότι το *router* λειτουργεί στο 3^{ο} Επίπεδο του OSI και απλά 'σπρώχνει' το πακέτο έξω από το κατάλληλο *interface*, κάνει δηλαδή *best effort delivery*. Συμπληρωματικά το *route* μπορεί να έχει κάποιον *timer*, εάν πρόκειται για *route* που έχει μαθευτεί δυναμικά, καθώς και τη διεύθυνση IP του *interface* του επόμενου προς τον προορισμό δρομολογητή (*next-hop router*).

Το σύνολο των *routes* που ο δρομολογητής συντηρεί στη RAM ονομάζεται πίνακας δρομολόγησης (*routing table)*. Αμέσως παρακάτω φαίνεται ένας τυπικός πίνακας δρομολόγησης σε δρομολογητή Cisco.

```
R1#show 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

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.1/32 is directly connected, Loopback0
O       10.10.10.0/24 [110/1172] via 192.168.10.6, 00:00:10, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.16/28 is directly connected, FastEthernet0/0
O       172.16.1.32/29 [110/391] via 192.168.10.6, 00:00:20, Serial0/0/1
     172.30.0.0/30 is subnetted, 1 subnets
C       172.30.1.0 is directly connected, Serial0/1/0
     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
```

```
O       192.168.10.8 [110/1171] via 192.168.10.6, 00:00:20, Serial0/0/1
R1#
```

Ας γνωρίσουμε την ανατομία ενός route, δηλαδή μίας γραμμής ή καταχώρησης του πίνακα δρομολόγησης:

```
O       172.16.1.32/29 [110/391] via 192.168.10.6, 00:00:20, Serial0/0/1
```

Στην πρώτη στήλη '`O`' φαίνεται ο τρόπος με τον οποίο έχει μαθευτεί το route. Στην περίπτωσή μας πρόκειται για το πρωτόκολλο δυναμικής δρομολόγησης OSPF. Στη δεύτερη στήλη βρίσκεται το δίκτυο προορισμού με την αντίστοιχη μάσκα υποδικτύου. Ακολουθούν δύο αριθμοί, `[110/391]`. Ο πρώτος είναι το Administrative Distance του *route* και ο δεύτερος το κόστος του. Ο αριθμός `192.168.10.6` είναι η IP διεύθυνση του επόμενου προς τον προορισμό δρομολογητή, ενώ μετά το timer αναφέρεται το *interface* εξόδου. Κάθε πακέτο λοιπόν που θα μπει στο *router* μας και θα έχει προορισμό το δίκτυο `172.16.1.32/29` θα εξέρχεται από το `Serial0/0/1`.

Πριν προχωρήσουμε, είναι αναγκαία σε αυτό το σημείο η αντιπαραβολή της δρομολόγησης (*routing*) με τη μεταγωγή (*switching*). Η βασική διαφορά τους είναι ότι το *switching* συμβαίνει στο 2^{ο} ενώ το *routing* στο 3^{ο} Επίπεδο του OSI. Οι δύο δηλαδή διαδικασίες χρησιμοποιούν διαφορετική πληροφορία για τη μεταφορά δεδομένων από την πηγή στον προορισμό. Στην πρώτη περίπτωση διακινούνται πλαίσια (*frames*) με βάση τη MAC διεύθυνση ενώ στη δεύτερη πακέτα (*packets*) με βάση την IP διεύθυνση. Στην Ενότητα της Πολυεπίπεδης Μεταγωγής (Ενότητα 16) θα μας δοθεί και πάλι η ευκαιρία να συζητήσουμε τις δύο λειτουργίες.

6.2 Στατικοί δρόμοι

Ένας δρομολογητής μπορεί να 'μάθει' απομακρυσμένα δίκτυα με δύο τρόπους:

- Χειροκίνητα, από στατικούς δρόμους (*static routes*) που ρυθμίζει ο διαχειριστής του δικτύου.
- Αυτόματα, από ένα πρωτόκολλο δυναμικής δρομολόγησης.

Συγκρίνοντας τα στατικά με τα δυναμικά routes, τα πρώτα έχουν τα παρακάτω πλεονεκτήματα:

- Απλότητα και αμεσότητα στην κατανόηση και λειτουργία τους.
- Ασφάλεια, αφού δεν ανταλλάσσονται μηνύματα μεταξύ των δρομολογητών.
- Δε δαπανούν πόρους του δρομολογητή, μνήμη και κύκλους επεξεργαστή.
- Λειτουργούν άριστα σε πολύ μικρά δίκτυα.

Στα μειονεκτήματα του στατικού *routing* αναφέρουμε:

- Δε μπορεί να ανταποκριθεί σε αλλαγές στην τοπολογία του δικτύου.
- Δε μπορεί να λειτουργήσει σωστά καθώς το δίκτυό μας μεγαλώνει, δεν είναι, όπως λέμε, κλιμακοθέσιμα ή επεκτάσιμα (*not scalable*).

Τρία είναι τα βήματα για την επιτυχή ρύθμιση ενός στατικού *route*:

- Ο διαχειριστής του δικτύου ρυθμίζει την εντολή `(config)#ip route`.
- Το στατικό *route* εγκαθίσταται στο *routing table*.
- Το στατικό *route* χρησιμοποιείται για τη δρομολόγηση πακέτων.

Η σύνταξη της εντολής ip route, σε global configuration mode είναι:

```
(config)#ip route{destination network & mask} {exit interface}
```

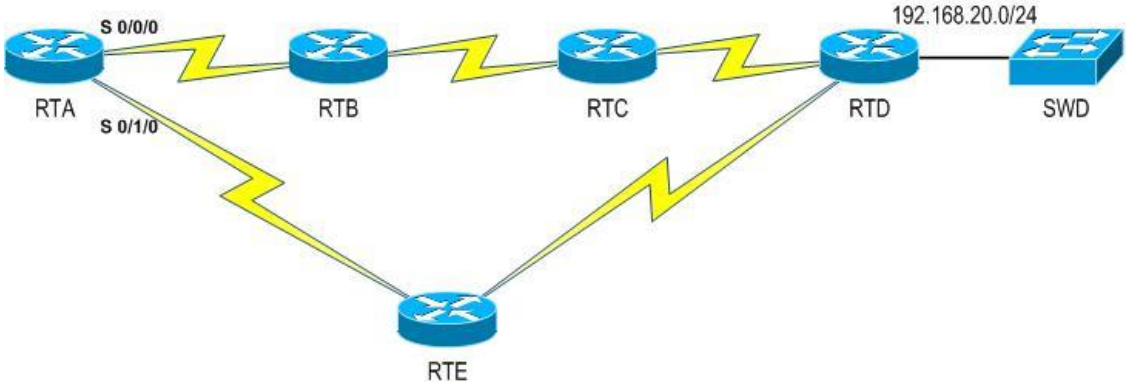
ή

```
(config)#ip route {destination network with mask}
{next hop ip address}
```

Στην **Εικόνα 6.1**, με την εντολή:

```
RTA(config)#ip route 192.168.20.0 255.255.255.0 serial 0/1/0
```

ο δρομολογητής RTA θα προωθήσει το IP πακέτο με διεύθυνση προορισμού στο δίκτυο 192.168.20.0/24 προς τα κάτω, χρησιμοποιώντας το interface **s 0/1/0** χωρίς να ενδιαφέρεται ούτε για την τύχη του πακέτου στις επόμενες ενδιάμεσες συσκευές, ούτε για την επιστροφή. Αυτό είναι και το νόημα του *best effort delivery*.



Εικόνα 6.1 Για τη στατική δρομολόγηση

Μία ειδική περίπτωση στατικής δρομολόγησης, με μεγάλη πρακτική αξία, είναι το προεπιλεγμένο route (*default route*). Πρόκειται για ένα *route* που θα χρησιμοποιηθεί από το δρομολογητή όταν δε γίνει ταίριασμα σε καμία από τις γραμμές του πίνακα δρομολόγησης. Η σύνταξη ενός *default route* είναι:

```
(config)#ip route 0.0.0.0 0.0.0.0 {exit interface}
```

ή

```
(config)#ip route 0.0.0.0 0.0.0.0 {next hop ip address}
```

Επειδή ακριβώς ένα πακέτο με προορισμό χωρίς συγκεκριμένο ταίριασμα θα 'φύγει' από το *default route*, το τελευταίο θα το συναντήσουμε και ως *gateway of last resort*. Παρακάτω φαίνεται τμήμα ενός τυπικού πίνακα δρομολόγησης με διαδρομή *default*:

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0


     172.15.0.0/30 is subnetted, 1 subnets
C       172.15.100.8 is directly connected, Serial0/0/0
```

```
     172.25.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.25.10.0/24 is directly connected, FastEthernet0/0
R       172.25.30.0/24 [120/1] via 172.25.100.6, 00:00:19, Serial0/0/1
C       172.25.100.4/30 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/1/0
```

Για την επαλήθευση της σωστής ρύθμισης και λειτουργίας ενός στατικού δρόμου μπορούμε να χρησιμοποιήσουμε τις εντολές:

```
#show running-config
#show ip route
```

6.3 Δυναμική δρομολόγηση και Πρωτόκολλα

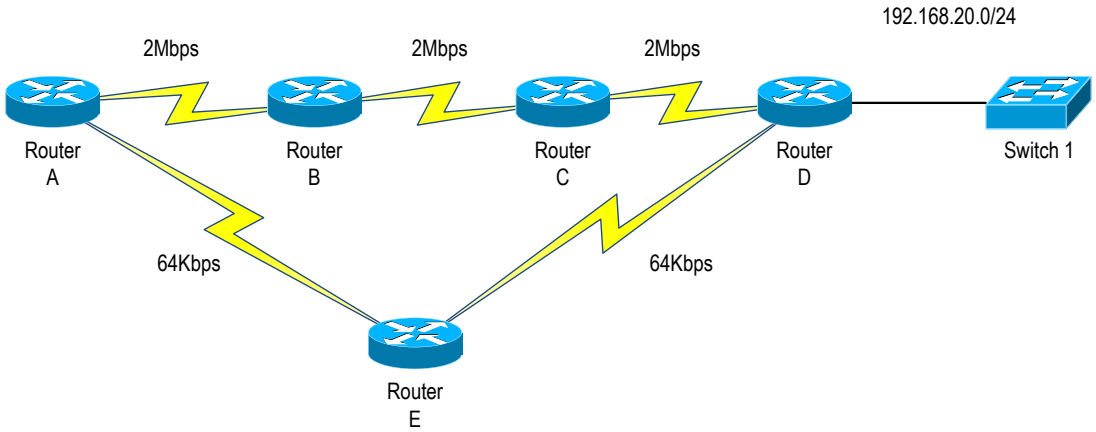
Ένα πρωτόκολλο δυναμικής δρομολόγησης, *dynamic routing protocol*, στηρίζεται στην επιλογή της καλύτερης διαδρομής για ένα δίκτυο προορισμού με βάση πληροφορίες που ανταλλάσσουν οι δρομολογητές μεταξύ τους. Οι πληροφορίες αυτές λέγονται *routing updates* και χρησιμοποιούνται για τη δημιουργία και τη συντήρηση του πίνακα δρομολόγησης στη RAM. Ένα δρομολογούμενο, *routed*, πρωτόκολλο είναι μία διαδικασία του 3^{ου} Επιπέδου του OSI που αναλαμβάνει τη λογική διευθυνσιοδότηση και το σχηματισμό πακέτων, ώστε τα πακέτα αυτά να μπορούν να μεταβαίνουν από ένα *host* σε ένα άλλο. Το γνωστό μας IP είναι ένα *routed* πρωτόκολλο. Λιγότερο πιθανό είναι να συναντήσουμε τα Internetwork Packet Exchange (IPX) και AppleTalk. Άρα το *routing* πρωτόκολλο υποστηρίζει το *routed*, παρέχοντας μηχανισμούς για την ανταλλαγή πληροφοριών δρομολόγησης από *router* σε *router*, με σκοπό τη συντήρηση πινάκων, ώστε το *router* να εκπληρώνει τις λειτουργίες του. Παραδείγματα routing πρωτοκόλλων είναι το *Routing Information Protocol* (RIP) ή το *Open Shortest Path First* (OSPF).

Πριν προχωρήσουμε σε μία αρχική συζήτηση για τα πρωτόκολλα δρομολόγησης, θυμίζουμε ότι ένας δρομολογητής πραγματοποιεί δύο βασικές εργασίες:

- Συντηρεί τον πίνακα δρομολόγησης και ενημερώνει άλλους δρομολογητές για αλλαγές στην τοπολογία του δικτύου, με χρήση ενός *routing* πρωτοκόλλου.
- Όταν ένα πακέτο φθάνει σε ένα *interface*, το *router* ανατρέχει στο *routing table* για να αποφασίσει από πού θα 'βγάλει' το πακέτο. Το προωθεί προς το κατάλληλο *interface* εξόδου, κατασκευάζει το κατάλληλο πλαίσιο (*frame*) και τελικά 'διώχνει' το πακέτο.

Για την επιλογή της βέλτιστης διαδρομής το *router* χρησιμοποιεί το *routing metric* (θα το αποδώσουμε ως 'μετρική'). Πρόκειται για μία τιμή που δηλώνει πόσο επιθυμητή είναι μία διαδρομή. Το πλήθος των επόμενων routers (*hop count*), το εύρος ζώνης (*bandwidth*), η καθυστέρηση (*delay*) ή η αξιοπιστία (*reliability*) μίας γραμμής είναι μεγέθη που μπορούν να χρησιμοποιηθούν ως *metrics*. Ας θεωρήσουμε το δρομολογητή RTA στην παρακάτω τυπική τοπολογία, με δίκτυο προορισμού το 192.168.20.0. Εάν ως *metric* χρησιμοποιείται μόνο το *hop count*, τότε η βέλτιστη διαδρομή είναι σαφώς μέσω του δρομολογητή RTE. Εάν όμως ο υπολογισμός του

metric στηρίζεται στο αθροιστικό εύρος ζώνης (*cumulative bandwidth*) τότε ο δρομολογητής RTA θα στείλει το πακέτο με προορισμό το δίκτυο 192.168.20.0 προς τον RTB.



Εικόνα 6.2 Για το *metric*

Όπως θα δούμε αναλυτικά παρακάτω, με τον πρώτο τρόπο λειτουργούν πρωτόκολλα όπως το RIP, ενώ με το δεύτερο πρωτόκολλα όπως το OSPF.

Τα πρωτόκολλα δρομολόγησης μπορούν να διακριθούν σε:

Εσωτερικά και **εξωτερικά**, ανάλογα με την εμβέλειά τους. Ένα εσωτερικό πρωτόκολλο (**IGP**, ***Interior Gateway Protocol***) συνδέει δικτυακές συσκευές που βρίσκονται στο ίδιο 'Αυτόνομο Σύστημα'. Με τον όρο αυτό, *Autonomous System* (AS) δηλώνουμε μία συλλογή από δρομολογητές που βρίσκονται υπό την ίδια διαχείριση, είναι όπως λέμε *self-contained and under a common administration*, για παράδειγμα το δίκτυο μίας τράπεζας ή ενός παρόχου υπηρεσιών διαδικτύου. Τα πρωτόκολλα που θα μελετήσουμε είναι όλα εσωτερικά, IGPs. Ένα εξωτερικό πρωτόκολλο (EGP, *Exterior Gateway Protocol*) συνδέει διαφορετικά ASs μεταξύ τους, όπως το BGP (*Border Gateway Protocol*).

Distance vector και ***link state***, ανάλογα με τον τρόπο με τον οποίο οι δρομολογητές αλληλεπιδρούν ανταλλάσσοντας *routing updates*. Σε ένα δρομολογητή που 'τρέχει' ένα *distance vector* πρωτόκολλο, προσδιορίζεται για κάθε δίκτυο προορισμού η κατεύθυνση και η απόσταση (*hop count*), ενώ στέλνεται στους γειτονικούς δρομολογητές περιοδικά ολόκληρο ή μέρος του πίνακα δρομολόγησης (*routing table)* ακόμα και εάν δεν υπάρχει αλλαγή στην τοπολογία. Ο δρομολογητής που δέχεται την ενημέρωση επιβεβαιώνει τα υφιστάμενα *routes* και επικαιροποιεί τον πίνακα δρομολόγησης κατά περίπτωση. Η εικόνα που έχει ο δρομολογητής για το δίκτυο είναι αυτή που του δίνει ο γείτονάς του, χωρίς να είναι δυνατή μία συνολική χαρτογράφηση της τοπολογίας. Για το λόγο αυτό η δρομολόγηση με distance vector πρωτόκολλα λέγεται και *routing by rumor*.

Η μέθοδος που χρησιμοποιούν τα *distance vector* πρωτόκολλα για τον υπολογισμό των καλύτερων διαδρομών είναι ο αλγόριθμος Bellman – Ford. Τα *distance vector*

πρωτόκολλα είναι απλά στην κατανόηση και τη ρύθμιση (*configuration*) αλλά και πολύ 'ελαφρά' ως προς τους απαιτούμενους πόρους υλικού. Έχουν όμως προβλήματα με την ταχύτητα και την αξιοπιστία της σύγκλισης, ειδικά όταν το δίκτυό μας μεγαλώνει.

Ένα *link-state* πρωτόκολλο αντίθετα, δημιουργεί *routing updates* μόνο όταν αυτό είναι απαραίτητο, δηλαδή όταν συμβεί μία αλλαγή στην τοπολογία. Ο δρομολογητής που 'τρέχει' ένα τέτοιο πρωτόκολλο μπορεί να έχει συνολική εικόνα της τοπολογίας, όπως πάνω-κάτω εμείς που διαβάζουμε το γράφημα του δικτύου. Η σύγκλιση είναι γρήγορη και αξιόπιστη, και το πρωτόκολλο λειτουργεί σωστά και για μεγάλα δίκτυα, είναι δηλαδή όπως λέμε *scalable*. Το σημαντικότερο *link-state* πρωτόκολλο είναι το OSPF, *Open Shortest Path First*. Στις επόμενες ενότητες, η κατά περίπτωση μελέτη των πρωτοκόλλων δυναμικής δρομολόγησης θα μας επιτρέψει να αντιληφθούμε καλύτερα τη λειτουργία, τη χρήση, τα πλεονεκτήματα και μειονεκτήματά τους.

Classful και ***classless***, ανάλογα με τη δυνατότητα διαχείρισης του σχήματος διευθυνσιοδότησης του δικτύου στο οποίο 'τρέχουν'. Ένα *classful* πρωτόκολλο δε μεταφέρει πληροφορία μάσκας μέσα στις ενημερώσεις δρομολόγησης (*routing updates)* ενώ δεν υποστηρίζει τοπολογίες με μάσκες μεταβλητού μήκους (VLSM). Τέτοια πρωτόκολλα είναι το RIPv1 και το IGRP και θεωρούνται εκτός χρήσης (*obsolete*) στα σημερινά δίκτυα. Αντίθετα, ένα *classless* πρωτόκολλο υποστηρίζει VLSM, CIDR (*Classless Interdomain Routing*) και *discontiguous* τοπολογίες. Πρακτικά όλα τα πρωτόκολλα που ρυθμίζονται σήμερα είναι *classless*, όπως το RIPv2, το OSPF ή το EIGRP.

7. Πρωτόκολλα δρομολόγησης RIP, OSPF και EIGRP

Σε αυτό το κεφάλαιο θα παρουσιάσουμε στοιχεία για τα τρία από τα πιο γνωστά και διαδεδομένα πρωτόκολλα δρομολόγησης, τις δύο εκδόσεις του RIP, το EIGRP και το OSPF. Όποιο όμως πρωτόκολλο και αν χρησιμοποιήσουμε θα πρέπει να πραγματοποιήσουμε δύο βασικά βήματα για την αρχική ρύθμισή του:

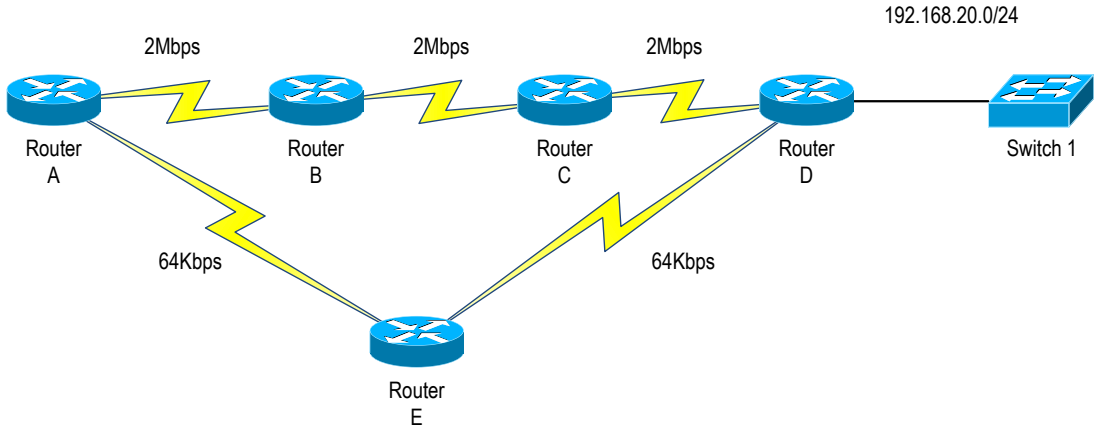
- Να ενεργοποιήσουμε το πρωτόκολλο δρομολόγησης.
- Να ενεργοποιήσουμε τα *interfaces* που θα συμμετάσχουν στη διαδικασία δρομολόγησης ή ισοδύναμα να ορίσουμε τα δίκτυα που ο δρομολογητής θα διαφημίζει μέσω του πρωτοκόλλου.

7.1 Χαρακτηριστικά του πρωτοκόλλου RIP

Το πρωτόκολλο RIP (*Routing Information Protocol*) μπορεί να θεωρηθεί ο τυπικός εκπρόσωπος της οικογένειας των *distance vector* δυναμικών πρωτοκόλλων δρομολόγησης. Έχει υλοποιηθεί σε δύο εκδόσεις: RIPv1 και RIPv2. Το RIPv1 είναι αμιγώς πρωτόκολλο *distance vector* ενώ το RIPv2 είναι ενσωματώνει μία σειρά από βελτιώσεις (*enhancements*). Επιχειρώντας μία παρουσίαση των δύο εκδόσεων έχουμε:

RIPv1

Το RIPv1 χρησιμοποιεί τοπικά *broadcasts* προκειμένου να διαμοιράσει περιοδικά την πληροφορία της δρομολόγησης (*routing updates*). Η περίοδος είναι 30 δευτερόλεπτα. Η μετρική που χρησιμοποιείται είναι το *hop count*, δηλαδή το πλήθος των συσκευών δρομολόγησης που παρεμβάλλονται από την αφετηρία έως τον προορισμό. Ας θεωρήσουμε την τοπολογία της **Εικόνας 7.1**, με τους δρομολογητές μας να τρέχουν το πρωτόκολλο RIP:



Εικόνα 7.1 Για τη μετρική του RIP

Ο Α, προκειμένου να προωθήσει ένα πακέτο προς το δίκτυο 192.168.20.0/24 θα επιλέξει τη διαδρομή μέσω του δρομολογητή Ε (προς τα κάτω) και όχι μέσω του Β. Είναι όμως αυτή η πραγματικά καλύτερη διαδρομή; Με δεδομένες τις ταχύτητες των γραμμών, μήπως η προώθηση προς τον Β στείλει το πακέτο '*πιο γρήγορα*' στον προορισμό του; Μήπως ένα δυναμικό πρωτόκολλο που θα μπορούσε να επιλέξει αυτή τη δεύτερη διαδρομή λειτουργούσε '*καλύτερα*'; Σε αυτόν ακριβώς τον προβληματισμό απαντά το *Administrative Distance* (AD) ενός πρωτοκόλλου δρομολόγησης.

Πρόκειται για έναν αριθμό που δηλώνει την αξιοπιστία των διαδρομών που προτείνει το πρωτόκολλο. Μεγαλύτερη τιμή σημαίνει μικρότερη αξιοπιστία. Ανάμεσα σε δύο διαφορετικά *routes* που προτείνουν δύο πρωτόκολλα, ο δρομολογητής θα επιλέξει αυτό με το μικρότερο AD. Το AD παίρνει ακέραιες τιμές από 0 έως 255. Στον παρακάτω πίνακα φαίνονται οι προεπιλεγμένες τιμές για τα Administrative Distances στατικών διαδρομών και πρωτοκόλλων.

Πηγή του *route*	**Administrative Distance**
Συνδεδεμένη διεπαφή (interface)	0
Στατική διαδρομή	1
Σύνοψη EIGRP	5
Εξωτερικό BGP	20
EIGRP	90
OSPF	110
IS-IS	115
RIP (version 1 και version 2)	120
Εξωτερικό EIGRP	170
Εσωτερικό BGP	200

Στην περίπτωσή μας, το RIP έχει *Administrative Distance* ίσο με 120. Εάν στην τοπολογία της **Εικόνας 7.1** οι δρομολογητές τρέχουν και OSPF (που έχει μικρότερο AD) οι διαδρομές που θα προτείνει θα προτιμηθούν έναντι αυτών του RIP.

Ως προς την επεκτασιμότητά του (*scalability*), το RIP δε μπορεί να λειτουργήσει σωστά σε δίκτυα όπου το *hop count* ξεπερνά το 15. Κάθε δίκτυο με μετρική ίση με 16 θεωρείται μη προσβάσιμο (*unreachable*). Για το λόγο αυτό σε μεγάλα εταιρικά δίκτυα χρησιμοποιούνται άλλα, πιο εξελιγμένα *routing* πρωτόκολλα.

Το RIPv1 είναι *classful* πρωτόκολλο. Αυτό πρακτικά σημαίνει ότι δε μπορεί να υποστηρίξει τοπολογίες με μάσκες υποδικτύωσης διαφορετικού μήκους (VLSM, *Various Length Subnet Masks*).

Επιπλέον το RIPv1 υποστηρίζει από 4 (*default*) έως 6 (μέγιστο) ίσου κόστους διαδρομές για τον ίδιο προορισμό (*equal cost load balancing*). Όλα τα ίσου κόστους μονοπάτια θα τοποθετηθούν στον πίνακα δρομολόγησης και η κίνηση θα διαμοιραστεί εξίσου ανάμεσα τους. Το *load balancing* είναι γενικά επιθυμητό γιατί:

- Ο δρομολογητής εκμεταλλεύεται καλύτερα τη χωρητικότητα των γραμμών σύνδεσης (*links*) μοιράζοντας την κίνηση ανάμεσά τους.
- Η σύγκλιση είναι γρηγορότερη αφού αν μια διαδρομή πάψει να υπάρχει τότε η πληροφορία δρομολογείται από τις υπόλοιπες ίσου κόστους διαδρομές, χωρίς να απαιτείται επανυπολογισμός και χωρίς καθυστέρηση.

RIPv2

Το RIPv2 είναι *distance-vector* με βελτιώσεις (*enhancements*) και χρησιμοποιείται αποτελεσματικά σε πολλά σημερινά δίκτυα μικρής-μεσαίας κλίμακας. Αντίθετα με το RIPv1, δε χρησιμοποιεί τοπικά *broadcasts* για τη μετάδοση των ενημερώσεων δρομολόγησης αλλά *multicasts*, στη διεύθυνση 224.0.0.9. Επιπλέον το RIPv2 χρησιμοποιεί κατά περίπτωση ενημερώσεις όταν υπάρχει κάποια αλλαγή στην τοπολογία (*event-triggered updates*).

Ως προς τα σχήματα διευθυνσιοδότησης, το RIPv2 είναι *classless*, άρα υποστηρίζει μάσκες υποδικτύου μεταβλητού μήκους (VLSM), μεταφέροντας μέσα στις ενημερώσεις και πληροφορία μάσκας του δικτύου που διαφημίζεται.

Το RIPv2 παρέχει επίσης τη δυνατότητα για πιστοποίηση ταυτότητας (*authentication*) ανάμεσα σε δύο δρομολογητές, ώστε να εξασφαλιστεί ότι οι ενημερώσεις δε θα φθάσουν σε ξένη κακόβουλη συσκευή.

7.2 Ρύθμιση του πρωτοκόλλου RIP

Η ρύθμιση του πρωτοκόλλου RIP γίνεται ως εξής:

```
Router(config)# router rip
Router(config-router)# network <διεύθυνση δικτύου>
```

Παρότι το RIPv1 είναι *classful* ενώ το RIPv2 είναι *classless*, η ρύθμιση της εντολής `network` παραμένει και στα δύο *classful*! Το μόνο που χρειάζεται να εισάγουμε ως παράμετρο είναι η διεύθυνση δικτύου αφού πρώτα την ανάγουμε στην αντίστοιχη κλάση (θα το συναντήσουμε και ως *major network*). Έτσι, αν τα *interfaces* του δρομολογητή μας έχουν ως διευθύνσεις π.χ. 192.168.1.1/26, 10.1.1.1/19 και 172.16.1.1/18 οι ρυθμίσεις για το RIPv1 έχουν ως εξής:

```
Router(config)# router rip
Router(config-router)# network 192.168.1.0
Router(config-router)# network 172.16.0.0
Router(config-router)# network 10.0.0.0
```

Ενώ για το RIPv2 θα είναι όπως παρακάτω:

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.1.0
Router(config-router)# network 172.16.0.0
```

```
Router(config-router)# network 10.0.0.0
```

ΠΡΟΣΟΧΗ: Στην περίπτωση που επιθυμούμε κάποιο *interface* να μη διαφημίζει ενημερώσεις του πρωτοκόλλου RIP (συνεχίζουν να λαμβάνονται) χρησιμοποιούμε την παρακάτω εντολή:

```
Router(config)# router rip
Router(config-router)# passive-interface fa0/0
```

Προβληματισμός: σε ποια περίπτωση απαιτείται η χρήση της εντολής `passive-interface` για λόγους ασφάλειας, ώστε τα *routing updates* να μην επικοινωνούνται σε πιθανώς κακόβουλα μηχανήματα που δεν τα χρειάζονται;

7.3 Έλεγχος ορθής λειτουργίας του RIP

Μερικές εντολές που μπορούμε να χρησιμοποιήσουμε για να ελέγξουμε την ορθή λειτουργία του RIP (*verification* και *troubleshooting*) είναι οι παρακάτω:

- `clear ip route`
- `show ip route`
- `show ip protocols`
- `debug ip rip`

`clear ip route`

Η εντολή **`clear ip route *`** 'καθαρίζει' και κατασκευάζει από την αρχή τον πίνακα δρομολόγησης. Κάθε φορά που αλλάζουμε κάτι σε ένα δυναμικό πρωτόκολλο μπορούμε να εισάγουμε αυτή την εντολή. Καθαρίζει μόνο τις διαδρομές που ο δρομολογητής έχει 'μάθει' δυναμικά μέσω ενός πρωτοκόλλου ενώ οι στατικές διαδρομές καθώς και οι συνδεδεμένες παραμένουν. Οι στατικές αφαιρούνται με χρήση της εντολής **`no ip route`** ενώ οι άμεσα συνδεμένες μόνο αν κλείσουμε το αντίστοιχο *interface*.

`show ip route`

Με αυτή την εντολή εμφανίζονται τα περιεχόμενα του πίνακα δρομολόγησης, δηλαδή οι καλύτερες διαδρομές για κάθε προορισμό, όπως 'πιστεύει' ο δρομολογητής βάσει των αλγορίθμων που χρησιμοποιεί ή / και των ρυθμίσεων που έχει πραγματοποιήσει ο διαχειριστής (στατικές διαδρομές). Ένα παράδειγμα δίνεται αμέσως 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
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
```

```
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 192.168.5.2, 00:00:17, Serial0/0/0
R    192.168.3.0/24 [120/2] via 192.168.5.2, 00:00:17, Serial0/0/0
                    [120/2] via 192.168.8.1, 00:00:09, Serial0/0/1
R    192.168.4.0/24 [120/1] via 192.168.8.1, 00:00:09, Serial0/0/1
C    192.168.5.0/24 is directly connected, Serial0/0/0
R    192.168.6.0/24 [120/1] via 192.168.5.2, 00:00:17, Serial0/0/0
R    192.168.7.0/24 [120/1] via 192.168.8.1, 00:00:09, Serial0/0/1
C    192.168.8.0/24 is directly connected, Serial0/0/1
```

Στον πίνακα δρομολόγησης εμφανίζονται δύο είδη διαδρομών. Με το γράμμα `C` εμφανίζονται τα άμεσα συνδεμένα (*directly connected*) δίκτυα ενώ με `R` όσα δίκτυα έχουν γίνει γνωστά στο δρομολογητή μέσω του πρωτοκόλλου RIP. Για τις εγγραφές του RIP παρατηρούμε δύο τιμές μέσα σε άγκιστρα π.χ. `[120/2]`. Η πρώτη τιμή είναι το γνωστό μας *administrative distance* του πρωτοκόλλου, ενώ η δεύτερη είναι η τιμή της μετρικής για τη συγκεκριμένη καταχώρηση (το *hop count*). Στη συνέχεια ακολουθεί η IP διεύθυνση της διεπαφής που έστειλε την ενημέρωση, πριν πόση ώρα έγινε η λήψη της, καθώς και το τοπικό *interface* εξόδου.

show ip protocols

Η εντολή αυτή παρουσιάζει όλα τα πρωτόκολλα δρομολόγησης που εκτελούνται στο δρομολογητή. Ακολουθεί ένα παράδειγμα αυτής της εντολής, όταν στο δρομολογητή εκτελείται το πρωτόκολλο RIP.

```
Router#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 18 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface             Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0       2     2
  Serial0/0/0           2     2
  Serial0/0/1           2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
       192.168.1.0
       192.168.5.0
       192.168.8.0
Passive Interface(s):
Routing Information Sources:
       Gateway         Distance      Last Update
       192.168.5.2          120      00:00:25
```

```
      192.168.8.1          120      00:00:22
Distance: (default is 120)
```

Στο παραπάνω παράδειγμα τρέχει το πρωτόκολλο RIPv2 (`Default version control: send version 2, receive 2`), οι ενημερώσεις στέλνονται κάθε `30` δευτερόλεπτα, ενώ η επόμενη ενημέρωση θα σταλεί σε `18` δευτερόλεπτα. Συμμετέχουν τρία *interfaces* στο πρωτόκολλο (στέλνουν και λαμβάνουν ενημερώσεις), τα `FastEthernet0/0`, `Serial0/0/0` και `Serial0/0/1`. Τα δίκτυα που έχουν προσδιοριστεί μέσω εντολών `network` είναι τα: `192.168.1.0`, `192.168.5.0` και `192.168.8.0` ενώ οι γειτονικοί δρομολογητές είναι οι: `192.168.5.2` και `192.168.8.1` από τους οποίους έχουμε λάβει ενημερώσεις πριν από `25` και `22` δευτερόλεπτα αντίστοιχα. Τέλος το *administrative distance* είναι ίσο με `120`.

debug ip rip

Οι εντολές `#debug` λειτουργούν δυναμικά και συμπληρώνουν τις εντολές `show` που παρουσιάζουν στατικά αποτελέσματα. Μας δίνουν τη δυνατότητα να εντοπίζουμε λάθη στις ρυθμίσεις μας ή / και στη δρομολόγηση, αλλά πρέπει να τις χρησιμοποιούμε προσεκτικά σε παραγωγικούς δρομολογητές επειδή είναι πολύ απαιτητικές σε πόρους του μηχανήματος. Ένα παράδειγμα της εξόδου της εντολής `#debug ip rip` που παρουσιάζει τις ενημερώσεις που στέλνει και λαμβάνει ένας δρομολογητής εμφανίζεται παρακάτω:

```
Router#debug ip rip
RIP protocol debugging is on
Router#RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (192.168.5.1)
RIP: build update entries
      192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
      192.168.4.0/24 via 0.0.0.0, metric 2, tag 0
      192.168.7.0/24 via 0.0.0.0, metric 2, tag 0
      192.168.8.0/24 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (192.168.8.2)
RIP: build update entries
      192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
      192.168.2.0/24 via 0.0.0.0, metric 2, tag 0
      192.168.5.0/24 via 0.0.0.0, metric 1, tag 0
      192.168.6.0/24 via 0.0.0.0, metric 2, tag 0
Router#RIP: received v2 update from 192.168.5.2 on Serial0/0/0
      192.168.2.0/24 via 0.0.0.0 in 1 hops
      192.168.3.0/24 via 0.0.0.0 in 2 hops
      192.168.6.0/24 via 0.0.0.0 in 1 hops
      192.168.7.0/24 via 0.0.0.0 in 2 hops
Router#RIP: received v2 update from 192.168.8.1 on Serial0/0/1
      192.168.3.0/24 via 0.0.0.0 in 2 hops
      192.168.4.0/24 via 0.0.0.0 in 1 hops
      192.168.6.0/24 via 0.0.0.0 in 2 hops
      192.168.7.0/24 via 0.0.0.0 in 1 hops
```

Σε αυτό το παράδειγμα ο δρομολογητής έστειλε ενημερώσεις μέσω του πρωτόκολλου RIPv2 (`sending v2 update to 224.0.0.9`) σε δύο διαφορετικά *interfaces*, ενώ έλαβε ενημερώσεις από δύο διαφορετικούς γείτονες. Προσοχή θα πρέπει να δοθεί στις ενημερώσεις που στέλνει ή λαμβάνει και προσδιορίζουν πόσα *hops* απέχει κάθε δίκτυο. Όταν ο δρομολογητής λάβει ένα *route* για κάποιο δίκτυο, αυξάνει την τιμή της μετρικής κατά 1 και το τοποθετεί στον πίνακα δρομολόγησης, εφόσον συνιστά την καλύτερη διαδρομή.

7.4 Χαρακτηριστικά του πρωτοκόλλου EIGRP

Το EIGRP (*Enhanced Interior Gateway Routing Protocol*) είναι ένα πρωτόκολλο δρομολόγησης της Cisco (*proprietary*), που μπορεί να χρησιμοποιηθεί αποτελεσματικά σε μεγάλα εταιρικά δίκτυα. Τα κυριότερα χαρακτηριστικά του είναι:

- Πετυχαίνει γρήγορη σύγκλιση, με κατά περίπτωση (*triggered*) ενημερώσεις όταν συμβαίνουν αλλαγές στην τοπολογία.
- Υποστηρίζει μάσκες υποδικτύου μεταβλητού μήκους (VLSM), είναι δηλαδή ένα *classless* πρωτόκολλο.
- Χρησιμοποιεί *multicasting* για τη μετάδοση των ενημερώσεων.
- Υποστηρίζει πολλαπλά πρωτόκολλα Επιπέδου 3 (*routed* πρωτόκολλα).
- Υποστηρίζει διαμοιρασμό της κίνησης σε έως έξι μονοπάτια, με ίσα ή και με διαφορετικά κόστη.
- Χρησιμοποιεί μία σύνθετη μετρική που περιγράφει με μεγαλύτερη ακρίβεια τα χαρακτηριστικά των διαδρομών.

Στον υπολογισμό της μετρικής (metric) του EIGRP συμμετέχουν οι εξής παράμετροι: χωρητικότητα (*bandwidth*), καθυστέρηση (*delay*), φόρτος (*load*), αξιοπιστία (*reliability*) και το μέγιστο μέγεθος μετάδοσης (MTU). Προεπιλεγμένα χρησιμοποιούνται μόνο οι δύο πρώτες (χωρητικότητα και καθυστέρηση) αλλά μπορούν να ρυθμιστούν και οι υπόλοιπες από το διαχειριστή.

Το EIGRP χρησιμοποιεί τον αλγόριθμο DUAL (*Diffusing Update Algorithm*) για να ενημερώσει τον πίνακα δρομολόγησης, αποθηκεύοντας την πληροφορία που μαθαίνει από τους γείτονες σε έναν πίνακα τοπολογίας (*topology table*). Έτσι αν μια κύρια διαδρομή που βρίσκεται στον πίνακα δρομολόγησης πάψει να υπάρχει, τότε ο δρομολογητής ανασύρει μια δευτερεύουσα διαδρομή (αν αυτή υπάρχει) από τον πίνακα τοπολογίας επιτυγχάνοντας έτσι σχεδόν άμεση σύγκλιση.

7.5 Λειτουργία του EIGRP

Ένας EIGRP δρομολογητής ενημερώνεται από τους απευθείας συνδεμένους γειτονικούς δρομολογητές. Χρησιμοποιεί πακέτα *hello* για να ανακαλύψει τους γείτονες, να διατηρήσει ενεργές τις σχέσεις γειτονίας και να μοιραστεί την πληροφορία δρομολόγησης. Αυτή την πληροφορία αποθηκεύει στον πίνακα γειτονίας

και τον πίνακα τοπολογίας. Χρησιμοποιεί τη διεύθυνση *multicast* 224.0.0.10 για τις ενημερώσεις δρομολόγησης και τα μηνύματα *hello*. Τα τελευταία στέλνονται κάθε 5 δευτερόλεπτα σε τοπικά δίκτυα και σε συνδέσεις *point-to-point* και *multipoint* με ταχύτητες τουλάχιστο ίσες με T1/E1. Διαφορετικά στέλνονται κάθε 60 δευτερόλεπτα. Ο *dead interval* χρόνος, δηλαδή ο χρόνος που ένας γείτονας θεωρείται ότι δεν υπάρχει πια, είναι ίσος με τρεις φορές το χρόνο του *hello interval*.

Η σύνθετη μετρική του EIGRP

Οι μετρικές (*metrics*) είναι μαθηματικές ποσότητες που χρησιμοποιούνται ώστε ένα πρωτόκολλο να επιλέξει μια διαδρομή. Όσο μεγαλύτερη αριθμητικά είναι μια μετρική που συνδέεται με μια διαδρομή, τόσο λιγότερο επιθυμητή είναι αυτή η διαδρομή. Η μετρική που χρησιμοποιεί το πρωτόκολλο EIGRP δημιουργείται από τον αλγόριθμο DUAL, χρησιμοποιώντας τον παρακάτω τύπο:

$$\left[\left(K_1 \cdot \mathrm{Bandwidth}_E + \frac{K_2 \cdot \mathrm{Bandwidth}_E}{256 - \mathrm{Load}} + K_3 \cdot \mathrm{Delay}_E\right) \cdot \frac{K_5}{K_4 + \mathrm{Reliability}}\right] \cdot 256$$

Αυτός ο τύπος χρησιμοποιεί τις εξής ποσότητες:

- Χωρητικότητα (*Bandwidth*): είναι η μικρότερη χωρητικότητα των συνδέσεων κατά μήκος ενός μονοπατιού προς ένα δίκτυο.
- Καθυστέρηση (*Delay*): είναι το άθροισμα όλων των καθυστερήσεων σε όλες τις συνδέσεις κατά μήκος ενός μονοπατιού προς ένα δίκτυο.
- Φόρτος (*Load*) : Ο μεγαλύτερος φόρτος κατά μήκος ενός μονοπατιού, βάση του packet rate και της χωρητικότητας που έχει ρυθμιστεί στα interfaces.
- Αξιοπιστία (*Reliability*): Η χαμηλότερη αξιοπιστία των συνδέσεων κατά μήκος ενός μονοπατιού, που υπολογίζεται με βάση τα *keepalives*.

Σταθερές: K1, K2, K3, K4, K5. Οι προεπιλεγμένες τιμές είναι K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0.

Με τις προεπιλεγμένες τιμές των σταθερών K, προκύπτει ότι:

Μετρική = χωρητικότητα + καθυστέρηση

Όπως γίνεται κατανοητό, τροποποίηση των τιμών των σταθερών επηρεάζει τους παράγοντες που επιδρούν στον υπολογισμό της μετρικής. Για αυτό το λόγο και οι σταθερές θα πρέπει να τροποποιούνται μόνο μετά από προσεκτικό σχεδιασμό, διότι η αλλαγή τους μπορεί να επηρεάσει τη σύγκλιση του δικτύου.

Σχέσεις γειτονίας

Ένας δρομολογητής που εκτελεί το πρωτόκολλο EIGRP αποθηκεύει τους γείτονες ώστε να μπορεί να προσαρμοστεί γρήγορα σε αλλαγές στο δίκτυο. Έτσι αν πάψει να υπάρχει η κατάλληλη διαδρομή στον πίνακα δρομολόγησης ενώ δεν υπάρχει ούτε η κατάλληλη εναλλακτική (backup) διαδρομή στον πίνακα τοπολογίας, το EIGRP θα

απευθύνει ερωτήματα στους γείτονες προκειμένου να ανακαλύψει μια εναλλακτική διαδρομή. Πώς όμως γίνονται γείτονες δύο δρομολογητές;
Για να γίνουν γείτονες δύο δρομολογητές που εκτελούν το πρωτόκολλο EIGRP θα πρέπει να ταυτίζονται στα *hello* πακέτα τους τα παρακάτω:

- Ο αριθμός του αυτόνομου συστήματος (AS).
- Οι τιμές K που ενεργοποιούν ή απενεργοποιούν τις διάφορες συνιστώσες στη σύνθετη μετρική του EIGRP.

Δε χρειάζεται να ταυτίζονται όμως οι χρόνοι των *hello* και *hold-down* χρονιστών για να χτιστεί η σχέση γειτονίας. Η διαδικασία έχει ως εξής:

- Ο πρώτος δρομολογητής στέλνει ένα μήνυμα *hello*.
- Αν η πληροφορία ταυτίζεται με του απέναντι δρομολογητή (αριθμός του αυτόνομου συστήματος και τιμές K) τότε αυτός στέλνει πίσω ένα μήνυμα *Update* με την τοπική πληροφορία τοπολογίας.
- Ο πρώτος δρομολογητής στέλνει ένα μήνυμα ACK (*Acknowledge*), επιβεβαιώνοντας τη λήψη της πληροφορίας δρομολόγησης.
- Ο πρώτος δρομολογητής στέλνει την δική του τοπική πληροφορία τοπολογίας στο δεύτερο δρομολογητή μέσω ενός μηνύματος *Update*.
- Ο απέναντι δρομολογητής επιστρέφει ένα μήνυμα ACK.

Σε αυτό το σημείο οι δύο δρομολογητές έχουν γίνει γείτονες, και είναι πλέον σε θέση να ανταλλάσσουν EIGRP μηνύματα. Τα είδη των μηνυμάτων είναι:

- Ενημέρωση (*update*): περιέχει μια ενημέρωση δρομολόγησης.
- Ερώτηση (*query*): περιέχει ερώτηση προς ένα γείτονα για επικύρωση πληροφορίας δρομολόγησης.
- Απάντηση (*reply*): περιέχει την απάντηση σε μία ερώτηση (*query*).

Επιλογή Διαδρομών

Το EIGRP για να υπολογίσει τις βέλτιστες διαδρομές που θα τοποθετήσει στον πίνακα δρομολόγησης χρησιμοποιεί τον αλγόριθμο DUAL. Αρχικά κατασκευάζει τον πίνακα τοπολογίας (*topology table*), όπου αποθηκεύει τις διαδρομές που μαθαίνει από τους γείτονες με τις αποστάσεις που εκείνοι του διαφημίζουν (*advertised distances*) καθώς και τις αποστάσεις που θα προκύψουν με αφετηρία τον ίδιο (*feasible distances*). Από αυτό τον πίνακα τοπολογίας θα επιλέξει τις βέλτιστες διαδρομές (*successor routes*) και θα τις τοποθετήσει στον πίνακα δρομολόγησης.

Αυτό που κάνει το EIGRP ξεχωριστό είναι η δυνατότητα επιλογής δευτερευουσών διαδρομών (*Feasible Successors*) για έναν προορισμό. Απαραίτητη προϋπόθεση είναι να ισχύει το εξής κριτήριο: θα πρέπει η απόσταση που διαφημίζει ο γείτονας (που είναι υποψήφιος για *Feasible Successor*) για το δίκτυο προορισμού να είναι αυστηρά μικρότερη από την τρέχουσα βέλτιστη απόσταση[1]. Έτσι, αν για κάποιο λόγο πάψει να υπάρχει η βέλτιστη διαδρομή και υπάρχει δευτερεύουσα διαδρομή στον πίνακα τοπολογίας, τότε ο δρομολογητής την επιλέγει άμεσα και την τοποθετεί στον πίνακα

[1] Η συνθήκη αυτή αναφέρεται και ως *Feasability Condition*.

δρομολόγησης. Με αυτό τον τρόπο δεν υπάρχει διακοπή στη δρομολόγηση σε περίπτωση αστοχίας στο δίκτυο. Στην αντίθετη περίπτωση, δηλαδή όταν δεν υπάρχει δευτερεύουσα διαδρομή στον πίνακα τοπολογίας, τότε η διαδρομή σημειώνεται ως ενεργή (*active*) και παράγεται ένα πακέτο ερώτησης από τον δρομολογητή προς τους γείτονες του. Αν εκείνοι δε γνωρίζουν εναλλακτική διαδρομή τότε και εκείνοι με τη σειρά τους παράγουν πακέτα ερωτήσεων προς τους γείτονες τους.

7.6 Ρύθμιση και έλεγχος του EIGRP

Η βασική ρύθμιση για το EIGRP είναι απλή:

```
Router(config)# router eigrp 100
Router(config-router)#       network <διεύθυνση δικτύου>
                             [μάσκα wildcard]
```

Αρχικά δηλαδή ενεργοποιείται το πρωτόκολλο εισάγοντας τον αριθμό του αυτόνομου συστήματος που θα πρέπει να συμπίπτει για όλους τους δρομολογητές. Στη συνέχεια εισάγουμε τα *classful* δίκτυα που υπάρχουν στα interfaces του δρομολογητή, παρότι το πρωτόκολλο είναι *classless*. Είναι δυνατή η δήλωση των διεπαφών / υποδικτύων ατομικά (*individual network statements*) με χρήση *wildcard* μασκών.

Έτσι, αν τα *interfaces* του δρομολογητή μας έχουν τις διευθύνσεις π.χ. 192.168.1.1/26, 10.1.1.1/24 και 172.16.1.1/24 οι ρυθμίσεις για το EIGRP έχουν ως εξής:

```
Router(config)# router eigrp 100
Router(config-router)# network 192.168.1.0
Router(config-router)# network 172.16.0.0
Router(config-router)# network 10.0.0.0
```

Οι δηλώσεις network με χρήση μασκών γίνονται:

```
Router(config)# router eigrp 100
Router(config-router)# network 192.168.1.0 0.0.0.63
Router(config-router)# network 172.16.1.0 0.0.0.255
Router(config-router)# network 10.1.1.0 0.0.0.255
```

Μερικές εντολές που μπορούμε να χρησιμοποιήσουμε για να ελέγξουμε την ορθή λειτουργία του EIGRP είναι:

- `show ip protocols`
- `show ip route`
- `show ip eigrp neighbors`
- `show ip eigrp topology`
- `show ip eigrp traffic`
- `debug ip eigrp`

- `debug ip eigrp packets`

show ip protocols

Η εντολή αυτή παρουσιάζει όλα τα πρωτόκολλα δρομολόγησης που εκτελούνται στο δρομολογητή. Ακολουθεί ένα παράδειγμα αυτής της εντολής, όταν στο δρομολογητή εκτελείται το πρωτόκολλο EIGRP.

```
Router#sh ip protocols

Routing Protocol is "eigrp  100 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 100
  Automatic network summarization is in effect
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
     192.168.2.0
     192.168.5.0
     192.168.6.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.5.1     90            122034
    192.168.6.2     90            159899
  Distance: internal 90 external 170
```

Στην έξοδο της εντολής μπορούμε να δούμε ότι εκτελείται το πρωτόκολλο EIGRP στο αυτόνομο σύστημα `100` (`Routing Protocol is "eigrp 100"`). Αφού μόνο τα K1 και K3 είναι ίσα με 1, η σύνθετη μετρική λαμβάνει υπόψη της μόνο τη χωρητικότητα (*bandwidth*) και την καθυστέρηση (*delay*). Υπάρχουν δύο γειτονικοί δρομολογητές, αυτοί είναι οι `192.168.5.1` και `192.168.6.2`. Τα δίκτυα που συμμετέχουν στο EIGRP είναι τα: `192.168.2.0`, `192.168.5.0` και `192.168.6.0`. Τέλος το *Administrative Distance* του πρωτοκόλλου είναι ίσο με `90` (`Distance: internal 90`). Παρατηρείστε ότι είναι μικρότερο από του RIP (120). Ποιο λοιπόν πρωτόκολλο ο δρομολογητής θα θεωρήσει πιο αξιόπιστο;

show ip route

Είναι η εντολή που εμφανίζει τα περιεχόμενα του πίνακα δρομολόγησης (*routing table*). Ένα παράδειγμα δίνεται αμέσως 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
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

D  192.168.1.0/24 [90/2172416] via 192.168.5.1, 00:56:45, Serial0/0/1
C  192.168.2.0/24 is directly connected, FastEthernet0/0
D  192.168.3.0/24 [90/2172416] via 192.168.6.2, 00:56:07, Serial0/0/0
D  192.168.4.0/24 [90/2684416] via 192.168.6.2, 00:55:36, Serial0/0/0
                  [90/2684416] via 192.168.5.1, 00:55:34, Serial0/0/1
C  192.168.5.0/24 is directly connected, Serial0/0/1
C  192.168.6.0/24 is directly connected, Serial0/0/0
D  192.168.7.0/24 [90/2681856] via 192.168.6.2, 00:56:05, Serial0/0/0
D  192.168.8.0/24 [90/2681856] via 192.168.5.1, 00:56:45, Serial0/0/1
```

Οι διαδρομές που χαρακτηρίζονται με το γράμμα `D`, έχουν γίνει γνωστές μέσω του πρωτοκόλλου EIGRP. Η πρώτη διαδρομή για το δίκτυο `192.168.1.0/24` έχει γίνει γνωστή από τον `192.16.5.1`, έχει ληφθεί μια ενημέρωση πριν από 56 λεπτά ενώ για να φτάσουμε σε αυτό το δίκτυο θα πρέπει να χρησιμοποιηθεί το *interface* `serial0/0/0`. Για τους αριθμούς μέσα στα άγκιστρα `[90|2172416]`, ο πρώτος είναι το *Administrative Distance* του πρωτοκόλλου ενώ ο δεύτερος είναι η τιμή της μετρικής (λέγεται και *Feasible Distance*). Θα πρέπει να σημειωθεί ότι για το δίκτυο `192.168.4.0/24` υπάρχουν δύο διαδρομές με την ίδια μετρική, γεγονός που συνεπάγεται ότι ο δρομολογητής θα πραγματοποιήσει ισότιμη διαμοίραση του φόρτου ανάμεσα στα δύο διαφορετικά μονοπάτια (το γνωστό μας *equal-cost load balancing*).

show ip eigrp neighbors

Εμφανίζει τους δρομολογητές με τους οποίους έχει συναφθεί σχέση γειτονίας:.

```
Router#sh ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address       Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                 (sec)          (ms)        Cnt  Num
0   192.168.5.1   Se0/0/1        10   01:09:55  40     1000  0   15
1   192.168.6.2   Se0/0/0        13   01:09:17  40     1000  0   15
```

Πολύ συνοπτικά θα αναφέρουμε ότι φαίνονται ο αριθμός του αυτόνομου συστήματος (`process 100`), η IP διεύθυνση του κάθε γείτονα, το *interface* μέσω του οποίου συνδεόμαστε στο γείτονα, ο χρόνος πριν θεωρήσουμε το γείτονα 'πεθαμένο' (δηλαδή ότι δεν είναι πλέον ενεργή η επικοινωνία μαζί του) και ο χρόνος που η επικοινωνία αυτή είναι ενεργή (`uptime`). Οι υπόλοιπες πληροφορίες αφορούν στο χρόνο που ο δρομολογητής θα περιμένει πριν αναμεταδώσει ένα πακέτο στο γείτονα σε περίπτωση που το προηγούμενο χαθεί (`RTO`) και στο χρόνο που απαιτείται για να μεταδοθεί ένα πακέτο και να ληφθεί ένα μήνυμα επιβεβαίωσης λήψης του πακέτου `ACK` (`SRTT – Smooth Round-Trip Time`).

show ip eigrp topology

Εμφανίζει τις βέλτιστες και τις εναλλακτικές διαδρομές:

```
Router#show ip eigrp topology
IP-EIGRP Topology Table for AS 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 192.168.2.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 192.168.5.0/24, 1 successors, FD is 2169856
         via Connected, Serial0/0/1
P 192.168.1.0/24, 1 successors, FD is 2172416
         via 192.168.5.1 (2172416/28160), Serial0/0/1
P 192.168.8.0/24, 1 successors, FD is 2681856
         via 192.168.5.1 (2681856/2169856), Serial0/0/1
P 192.168.6.0/24, 1 successors, FD is 2169856
         via Connected, Serial0/0/0
P 192.168.3.0/24, 1 successors, FD is 2172416
         via 192.168.6.2 (2172416/28160), Serial0/0/0
P 192.168.7.0/24, 1 successors, FD is 2681856
         via 192.168.6.2 (2681856/2169856), Serial0/0/0
P 192.168.4.0/24, 2 successors, FD is 2684416
         via 192.168.6.2 (2684416/2172416), Serial0/0/0
         via 192.168.5.1 (2684416/2172416), Serial0/0/1
```

Σε κάθε διαδρομή που γνωρίζει ο δρομολογητής παρατηρούμε σε παρενθέσεις δύο αριθμούς, ο πρώτος είναι το *Feasible Distance*, δηλαδή η συνολική βέλτιστη απόσταση προς έναν προορισμό από το δρομολογητή μας, ενώ ο δεύτερος είναι το *Advertised Distance*, δηλαδή η απόσταση από τον προορισμό που μας διαφημίζει ο γείτονας για τον εαυτό του (το *Advertised Distance* θα το συναντήσουμε και ως *Reported Distance*). Όλες οι διαδρομές είναι *passive* (P) δηλαδή λειτουργικές και σταθερές. Τέλος για το δίκτυο 192.168.4.0/24 υπάρχουν δύο εναλλακτικά μονοπάτια με την ίδια μετρική (2684416).

show ip eigrp traffic

Προκειμένου να δούμε στατιστικά κίνησης για το πρωτόκολλο EIGRP χρησιμοποιούμε την ακόλουθη εντολή:

```
Router#show ip eigrp traffic
IP-EIGRP Traffic Statistics for process 100
  Hellos sent/received: 3327/2207
  Updates sent/received: 12/16
  Queries sent/received: 0/0
  Replies sent/received:  0/0
  Acks sent/received:  16/11
  Input queue high water mark 1, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
```

Όπως παρατηρούμε ο δρομολογητής μας στέλνει και λαμβάνει μηνύματα *hello* στους γείτονες ενώ μοιράζεται πληροφορία δρομολόγησης χρησιμοποιώντας *Updates* και *Queries*.

7.7 Χαρακτηριστικά του πρωτοκόλλου OSPF

Το OSPF είναι ένα πρωτόκολλο *link-state* που αναπτύχθηκε ως ένα ανοικτό πρότυπο (OSPFv2 RFC 2328) προκειμένου να αντιμετωπιστούν οι περιορισμοί που το RIP επιβάλλει σε μεγάλα εταιρικά δίκτυα. Έχει αρκετά πλεονεκτήματα όπως:

- Είναι βασισμένο σε ανοικτό πρότυπο (*open standard*) και εκτελείται σε δρομολογητές διάφορων κατασκευαστών (*multi-vendor*).
- Είναι *link-state*, *classless*, επιτρέχει ιεραρχική δόμηση του δικτύου με χρήση περιοχών (areas[1]), υποστηρίζει υποδίκτυα με μάσκες μεταβλητού μήκους (VLSM) αλλά και συνόψεις (*summarization*).
- Υλοποιεί τον αλγόριθμο SPF (*Shortest-Path First*) του Dijkstra, παρέχοντας έτσι τη δυνατότητα αποφυγής βρόχων (*loops*) στην τοπολογία.
- Χρησιμοποιεί μια απλή μετρική, **το κόστος**, που είναι αντίστροφα ανάλογο της χωρητικότητας (*bandwidth*) ενός *interface*, ή ενός *link*.

Έχει όμως και μειονεκτήματα όπως:

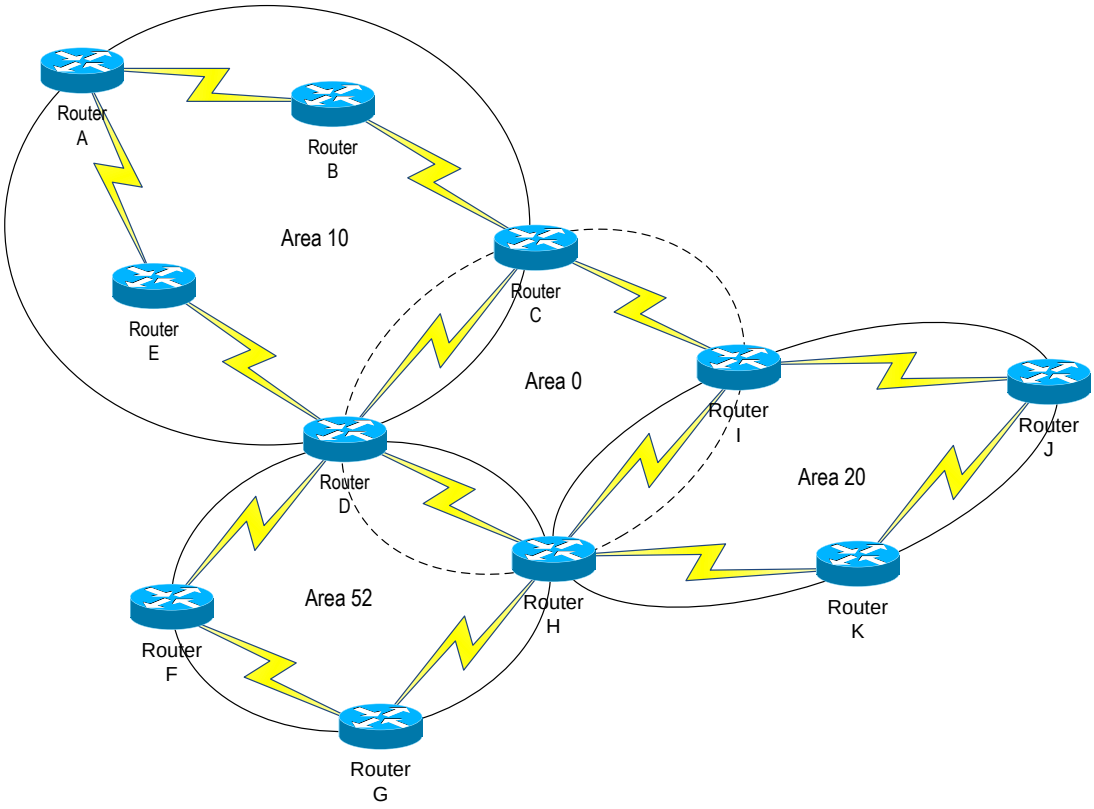
- Καταναλώνει αρκετή μνήμη στο δρομολογητή για την αποθήκευση του πίνακα γειτονίας (*adjacency table*), της τοπολογίας (*topology database*) καθώς και του πίνακα δρομολόγησης.
- Χρησιμοποιεί περισσότερη μνήμη RAM για να εκτελέσει τον αλγόριθμο SPF, ειδικά όταν οι δρομολογητές εκκινούν και κατασκευάζουν από την αρχή τους πίνακες γειτονίας και τοπολογίας.
- Είναι πιο σύνθετο τόσο στη ρύθμιση όσο και στην επίλυση τυχόν προβλημάτων.
- Πρέπει να γίνει προσεκτικός σχεδιασμός, δεδομένου ότι το πρωτόκολλο χρησιμοποιεί περιοχές, ώστε να γίνει ορθή κατάτμηση του δικτύου σε περιοχές που να καλύπτουν ορθά τις επιχειρησιακές λειτουργίες και το δικτυακό φόρτο.

Το OSPF χρησιμοποιεί τις περιοχές (OSPF *areas*) για ταχύτερη σύγκλιση και σταθερότερη λειτουργία σε μεγάλα δίκτυα. Μια περιοχή είναι ένα σύνολο από συνεχή IP δίκτυα, τμήματα δηλαδή ενός ευρύτερου δικτύου, που μπορούν να συνοψιστούν σε μεγαλύτερα δίκτυα. Με αυτό τον τρόπο επιτρέπουν τον καλύτερο έλεγχο των ενημερώσεων (*routing updates*) που μπορούν να περνούν από μια περιοχή σε μια άλλη, περιορίζοντας έτσι τις ενημερώσεις από άσκοπη διάχυση. Μία αλλαγή που πραγματοποιείται σε μια περιοχή δε μεταδίδεται υποχρεωτικά στις άλλες.

Το OSPF υποστηρίζει μια ιεραρχία δύο επιπέδων: υπάρχει μια περιοχή κορμού που ονομάζεται περιοχή 0 (area 0) στην οποία πρέπει να συνδέονται υποχρεωτικά όλες οι υπόλοιπες. Ο σκοπός αυτής της σχεδίασης είναι τα δίκτυα κάθε περιοχής να μπορούν να συνοψιστούν στα όρια των περιοχών οπότε οι ενημερώσεις να είναι μικρές σε μέγεθος, μικραίνοντας έτσι και τους πίνακες δρομολόγησης. Για παράδειγμα στην

[1] Η αναλυτική συζήτηση για το multi-area OSPF ξεφεύγει από τους σκοπούς του εγχειριδίου.

τοπολογία της **Εικόνας 7.2**, σε κάθε περιοχή αντιστοιχούμε ένα δίκτυο κλάσης Α ή κλάσης Β. Έτσι, αν στους δρομολογητές που συνδέουν τις περιοχές υλοποιήσουμε προσεκτικά συνόψεις, οι αλλαγές που θα συμβαίνουν μέσα σε μια περιοχή δε θα ανακοινώνονται στις άλλες περιοχές, δημιουργώντας σταθερότητα στη δρομολόγηση.



Εικόνα 7.2 Τοπολογία OSPF με πολλές περιοχές

Με αυτό τον τρόπο, κάθε εσωτερικός δρομολογητής σε μια περιοχή γνωρίζει μόνο τις διαδρομές που βρίσκονται μέσα στην περιοχή καθώς και τις συνόψεις των άλλων περιοχών. Για μεγάλα εταιρικά δίκτυα απαιτείται πιο σύνθετος σχεδιασμός.

Το OSPF χρησιμοποιεί ως μετρική το κόστος, που είναι αντίστροφα ανάλογο της χωρητικότητας μιας γραμμής (*bandwidth*). Με αυτό τον τρόπο όσο πιο γρήγορη είναι μια γραμμή τόσο μικρότερο κόστος έχει. Θα πρέπει να δοθεί όμως ιδιαίτερη προσοχή στο ότι τα σειριακά interfaces έχουν προεπιλεγμένα ονομαστική χωρητικότητα 1.544 Kbps, οπότε και με χρήση της εντολής `(config-if)#banwidth` θα πρέπει να ρυθμίζουμε κατά περίπτωση. Με αυτό τον τρόπο και επειδή το OSPF έχει την ικανότητα να διαμοιράσει το φόρτο προεπιλεγμένα σε 4 μονοπάτια ίσου κόστους (έως 16 μετά από ρύθμιση) αποφεύγουμε τη λανθασμένη δρομολόγηση σε άνισου κόστους διαδρομές.

7.8 Λειτουργία του OSPF

Στο OSPF κάθε δρομολογητής έχει ένα μοναδικό RID (Router ID). Αυτό περιλαμβάνεται σε όλα τα μηνύματα που στέλνει ο δρομολογητής και ορίζεται διαδοχικά ως εξής:

- Ο αριθμός που προσδιορίζεται από το διαχειριστή μέσω της εντολής `router-id`.
- Η μεγαλύτερη IP διεύθυνση από τα loopback *interfaces*.
- Η μεγαλύτερη IP διεύθυνση από τα ενεργά φυσικά *interfaces*.

Επειδή αν δεν υπάρχουν ενεργά *interfaces* τότε η διεργασία του OSPF δεν τρέχει από το δρομολογητή, κρίνεται τις περισσότερες φορές απαραίτητο να ορίσουμε ένα loopback interface, ώστε πάντα να υπάρχει ένα RID.

Αρχικά ο δρομολογητής συνάπτει σχέσεις γειτονίας (*adjacencies*) με τους γειτονικούς δρομολογητές ανταλλάσοντας πληροφορία δρομολόγησης με τη χρήση *link state advertisements* (LSAs). Προκειμένου να γίνει αυτό στέλνει μηνύματα *hello* κάθε 10 δευτερόλεπτα. Εάν δε λάβει κάποιο μήνυμα *hello* από ένα συγκεκριμένο γείτονα για τουλάχιστο 40 δευτερόλεπτα, τότε τον κηρύσσει 'πεθαμένο' (*dead-interval time*).

Σε αντίθεση με το EIGRP, δύο OSPF δρομολογητές δημιουργούν σχέση γειτονίας εφόσον ισχύουν τα παρακάτω:

- Βρίσκονται στην ίδια περιοχή.
- Οι χρόνοι αποστολής *hello* μηνυμάτων αλλά και ο *dead-interval* χρόνος συμπίπτουν.

Designated και Backup-Designated Routers

Στην περίπτωση που περισσότεροι από δύο OSPF δρομολογητές (ας δεχθούμε N-το πλήθος) βρίσκονται σε δίκτυο πολλαπλής πρόσβασης, για παράδειγμα ένα Ethernet δίκτυο (*multi-access broadcast network*), τότε σχηματίζονται N(N-1)/2 adjacencies. Όταν κάθε δρομολογητής χρειαστεί να στείλει ένα μήνυμα, θα το κάνει *multicast* σε όλους τους άλλους. Αυτό έχει ως αποτέλεσμα μεγάλη κίνηση μέσα στο multi-access δίκτυο εξαιτίας των ενημερώσεων του OSPF. Για την αποφυγή αυτού του προβλήματος το πρωτόκολλο υλοποιεί μία διαδικασία εκλογής ενός '*αρχηγού*' και ενός '*υπαρχηγού*' που επωμίζονται τη συγκέντρωση και την προώθηση των updates.

Ο δρομολογητής που αναλαμβάνει το ρόλο του '*αρχηγού*' λέγεται DR (*Designated Router*) και ο '*υπαρχηγός*' λέγεται BDR (*Backup-Designated Router*). Οι υπόλοιποι δρομολογητές που συνδέονται μέσα στο δίκτυο που συμβαίνει η εκλογή αναλαμβάνουν το ρόλο του DROTHER. Στις τοπολογίες σημείου-προς-σημείο (*point-to-point*) δεν πραγματοποιείται εκλογή DR και BDR.

Έτσι όταν ένας δρομολογητής ξεκινά και ένα *interface* του συνδέεται σε ένα Ethernet δίκτυο, τότε σε αυτό το *interface* σχηματίζει σχέσεις γειτονίας μόνο με τον DR και τον BDR. Κάθε φορά που γίνεται ανταλλαγή πληροφορίας δρομολόγησης αυτή

γίνεται με τον DR και τον BDR και εκείνοι στη συνέχεια ενημερώνουν τους υπόλοιπους δρομολογητές που βρίσκονται στο ίδιο τμήμα δικτύου. Προκειμένου να γίνει αυτή η διαδικασία εφικτή, όταν ένας δρομολογητής επικοινωνεί με τους DR και BDR χρησιμοποιεί τη διεύθυνση 224.0.0.6, ενώ όταν ο DR και ο BDR ενημερώνουν τους υπόλοιπους δρομολογητές χρησιμοποιούν τη διεύθυνση 224.0.0.5.

Ποιος όμως εκλέγεται DR και BDR; Ο δρομολογητής που συμμετέχει με την υψηλότερη προτεραιότητα (*OSPF priority value*) στο αντίστοιχο τμήμα δικτύου. Στην περίπτωση που υπάρξει ισοπαλία, τότε εκλέγεται ο δρομολογητής με το μεγαλύτερη RID, που υπενθυμίζεται ότι πρέπει να είναι μοναδικό σε ολόκληρο το δίκτυο. Προεπιλεγμένα κάθε δρομολογητής έχει προτεραιότητα ίση με 1. Στην ειδική περίπτωση που ένας δρομολογητής έχει προτεραιότητα ίση με 0 δε συμμετέχει στη διαδικασία εκλογής (αυτό είναι θεμιτό και συμβαίνει σε συγκεκριμένες τοπολογίες). Προκειμένου να ρυθμιστεί η προτεραιότητα σε ένα δρομολογητή χρησιμοποιείται η εντολή `(config-if)#ip ospf priority`.

Προσοχή: Όταν εκλεγεί ο DR και ο BDR, διατηρούν αυτούς τους ρόλους ακόμα και αν συνδεθεί στο ίδιο τμήμα δικτύου δρομολογητής με υψηλότερη προτεραιότητα και συνάψουν σχέσεις γειτονίας. Επανεκλογή DR ή BDR θα συμβεί μόνο αν δεν υπάρχει καθόλου DR ή BDR ή αυτοί σβήσουν ξαφνικά.

7.9 Ρύθμιση και έλεγχος του OSPF

Για τη ρύθμιση του OSPF είναι απαραίτητη η αναλυτική δήλωση όλων των διεπαφών (*interfaces*) που θα συμμετέχουν, με την κατάλληλη wildcard μάσκα:

```
Router(config)# router ospf <αριθμός διεργασίας>
Router(config-router)#       network <διεύθυνση δικτύου>
                             <wildcard μάσκα> area <περιοχή>
```

Ο αριθμός διεργασίας είναι σημαντικός μόνο για το δρομολογητή και διαφοροποιεί πολλαπλές διεργασίες που εκτελούνται στον ίδιο δρομολογητή. Επομένως αυτοί οι αριθμοί δεν είναι απαραίτητο να ταυτίζονται σε γειτονικούς *routers*. Στη συνέχεια για να προσδιορίσουμε τα *interfaces* που θα συμμετέχουν σε μια περιοχή του OSPF χρησιμοποιούμε, όπως πάντα, την εντολή `(config-router)#network`.

Έτσι, αν τα *interfaces* του δρομολογητή μας έχουν τις διευθύνσεις 192.168.1.1/26, 10.1.1.1/30 και 172.16.1.1/24 η βασική ρύθμιση του OSPF θα είναι:

```
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.63 area 0
Router(config-router)# network 172.16.1.0 0.0.0.255 area 0
Router(config-router)# network 10.1.1.0 0.0.0.3 area 0
```

Επιπλέον ένα παράδειγμα ρύθμισης ενός loopback interface είναι όπως παρακάτω:

```
Router(config)# interface loopback 0
```

```
Router(config-if)# ip address 192.168.5.1 255.255.255.0
```

Τα loopback *interfaces* είναι ένας χρήσιμος τρόπος για να αναθέσουμε ένα RID (Router IP) για το πρωτόκολλο OSPF σε ένα δρομολογητή, ή για δοκιμαστικούς λόγους να ελέγξουμε ένα δίκτυο και να επιλύσουμε προβλήματα, ή ακόμα για να τερματίσουμε συνδέσεις όπως είναι τα GRE ή IPSec τούνελ. Σε ένα δρομολογητή μπορούμε να δημιουργήσουμε όσα loopback *interfaces* επιθυμούμε χρησιμοποιώντας τους αριθμούς από 0 έως 2147483647. Μετά τη δημιουργία του μπορεί να χρησιμοποιηθεί με τον ίδιο τρόπο όπως και ένα φυσικό *interface*.

Μερικές εντολές που μπορούμε να χρησιμοποιήσουμε για να ελέγξουμε την ορθή λειτουργία του OSPF (verification και troubleshooting) είναι οι παρακάτω:

- `show ip protocols`
- `show ip route`
- `show ip ospf neighbor`
- `show ip ospf interface`
- `debug ip ospf adj`
- `debug ip ospf events`
- `debug ip ospf packet`

`show ip protocols`

Η εντολή αυτή παρουσιάζει όλα τα πρωτόκολλα δρομολόγησης που εκτελούνται στο δρομολογητή. Ακολουθεί ένα παράδειγμα αυτής της εντολής, όταν στο δρομολογητή εκτελείται το πρωτόκολλο OSPF.

```
Router#show ip protocols


Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.16.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.1.0 0.0.0.63 area 0
    172.16.1.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.1.1.2             110      00:00:54
    172.16.1.1           110      00:00:54
    192.168.1.1          110      00:01:29
    192.168.10.1         110      00:00:54
    200.200.200.200      110      00:00:54
  Distance: (default is 110)
```

Σε αυτό το παράδειγμα μπορούμε να δούμε ότι το Router ID του δρομολογητή μας είναι 172.16.1.1. Δύο *interfaces* συμμετέχουν στο OSPF και βρίσκονται στην περιοχή

0. Άλλοι τέσσερις δρομολογητές υπάρχουν στο δίκτυο ενώ το *administrative distance* του πρωτοκόλλου είναι ίσο με `110 (Distance: (default is 110)`. Συγκρίνετε με τα Administrative Distances του RIP και του OSPF. Τι παρατηρείτε;

show ip route

Είναι η εντολή που εμφανίζει τις καταχωρήσεις του πίνακα δρομολόγησης. Ένα παράδειγμα δίνεται αμέσως παρακάτω:

```
Router#show 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 172.16.1.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, FastEthernet0/0
     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/0/0
O    192.168.1.0/24 [110/196] via 172.16.1.2, 00:02:28, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.16.1.2, 00:02:28, Serial0/0/0
```

Σε αυτό το παράδειγμα ο δρομολογητής γνωρίζει δύο διαδρομές από το πρωτόκολλο OSPF. Η πρώτη έχει *administrative distance* `110` και κόστος `196` και προέρχεται από την ίδια περιοχή (έχει το πρόθεμα `O`), ενώ η δεύτερη έχει *administrative distance* `100` και κόστος `1` και είναι *default* διαδρομή που οδηγεί έξω από το αυτόνομο σύστημα (έχει το πρόθεμα `O*E2`). Και στις δύο περιπτώσεις στα δίκτυα αυτά μπορούμε να οδηγηθούμε μέσω του γείτονα `172.16.1.2`.

show ip ospf neighbor

Προκειμένου να δούμε τους δρομολογητές με τους οποίους έχει συναφθεί σχέση γειτονίας εκτελούμε την εντολή **#show ip ospf neighbor**.

```
Router#show ip ospf neighbor

Neighbor ID       Pri  State         Dead Time   Address    Interface
200.200.200.200   1    FULL/DR       00:00:39    10.1.1.1   FastEthernet0/0
172.16.1.1        1    FULL/BDR      00:00:39    10.1.1.3   FastEthernet0/0
192.168.10.1      0    2WAY/DROTHER  00:00:39    10.1.1.4   FastEthernet0/0
```

Σε αυτό το παράδειγμα παρατηρούμε ότι τρεις δρομολογητές συνδέονται στο `interface FastEthernet0/0` με τις εξής ιδιότητες:

- Ο δρομολογητής με RID: 200.200.200.200 είναι DR
- Ο δρομολογητής με RID: 172.16.1.1 είναι BDR
- Ο δρομολογητής με RID: 192.168.10.1 είναι DROTHER

Θα πρέπει να σημειωθεί ότι ο δρομολογητής από τον οποίο εκτελέσαμε την εντολή θα είναι DROTHER, και η σχέση του με τους DR και BDR είναι FULL, δηλαδή με αυτούς μοιράζεται πληροφορία δρομολόγησης. Σε αντίθεση με τον άλλο DROTHER δρομολογητή η σχέση του είναι 2WAY οπότε και δε θα μοιραστεί πληροφορία δρομολόγησης απευθείας παρά μόνο μέσω των DR και BDR.

show ip ospf interface

Ένας δρομολογητής διατηρεί πληροφορία για το πρωτόκολλο OSPF για κάθε *interface* και συγκεκριμένα την περιοχή που αυτό ανήκει αλλά και τους συνδεμένους γείτονες. Αυτή την πληροφορία μπορούμε να δούμε χρησιμοποιώντας την εντολή **#show ip ospf interface**.

```
Router#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.1.1.3/24, Area 0
  Process ID 1, Router ID 172.16.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 200.200.200.200, Interface address 10.1.1.1
  Backup Designated Router (ID) 172.16.1.1, Interface address 10.1.1.3
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 3, Adjacent neighbor count is 3
    Adjacent with neighbor 10.1.1.2
    Adjacent with neighbor 192.168.10.1
    Adjacent with neighbor 200.200.200.200  (Designated Router)
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 172.16.1.1/30, Area 0
  Process ID 1, Router ID 172.16.1.1, Network Type POINT-TO-POINT, Cost: 195
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
```

```
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.1
  Suppress hello for 0 neighbor(s)
```

Σε αυτό το παράδειγμα το RID του δρομολογητή είναι `172.16.1.1`, στο interface `FastEthernet0/0` η κατάσταση του είναι `BDR`, ο `DR` έχει RID ίσο με `200.200.200.200`, ενώ έχει τρεις γείτονες και τρεις σχέσεις γειτονίας (`adjacent neighbor count is 3`) επειδή έχει το ρόλο του `BDR`. Στην περίπτωση που είχε το ρόλο του DROTHER θα είχε σχέσεις γειτονίας μόνο με τον DR και τον BDR.

Στο interface Serial0/0/0, ο τύπος της σύνδεσης είναι `POINT-TO-POINT`, και για αυτό το λόγο δε γίνεται εκλογή DR και BDR. Σε αυτή την περίπτωση συνάπτει σχέσεις γειτονίας με τον μοναδικό δρομολογητή με τον οποίο συνδέεται και ο οποίος έχει RID ίσο με `192.168.1.1`.

debug ip ospf adj

Προκειμένου να δούμε τι συμβαίνει κατά τη διαδικασία δημιουργίας σχέσεων γειτονίας μπορούμε να εκτελέσουμε την εντολή debug ip ospf adj. Για να παρουσιάσει αυτή η εντολή κάποιο output θα πρέπει να πραγματοποιηθεί κάποια εκλογή DR και BDR. Στο συγκεκριμένο παράδειγμα την προκαλούμε εμείς με το σβήσιμο ενός δρομολογητή:

```
Router#debug ip ospf adj

OSPF: Build router LSA for area 0, router ID 172.16.1.1
OSPF: DR/BDR election on FastEthernet0/0
OSPF: Elect BDR 10.1.1.2
OSPF: Elect DR 172.16.1.1
DR: 172.16.1.1 (Id)   BDR: 10.1.1.2 (Id)
```

Μετά το σβήσιμο του δρομολογητή που εκτελούσε χρέη DR, πραγματοποιήθηκε εκλογή νέου DR, με τον BDR να έχει προτεραιότητα λόγω του ρόλου του. Έτσι άμεσα προβιβάστηκε σε DR ο 172.16.1.1 ενώ εκλέχθηκε νέος BDR ο 10.1.1.2.

debug ip ospf events

Για να έχουμε μια πιο λεπτομερειακή εικόνα για τη λειτουργία του OSPF μπορούμε να εκτελέσουμε την εντολή debug ip ospf events. Υπό κανονικές συνθήκες το μόνο που θα δούμε είναι τα μηνύματα hello που ανταλλάσσονται μεταξύ των δρομολογητών. Σε περίπτωση όμως εκλογής DR και BDR θα έχουμε μια πιο σύνθετη εικόνα που απεικονίζεται στο επόμενο παράδειγμα (τμήμα της εξόδου της εντολής έχει παραλειφθεί):

```
Router#debug ip ospf events
OSPF events debugging is on
OSPF: Rcv hello from 192.168.1.1 area 0 from Serial0/0/0 172.16.1.2
OSPF: End of hello processing
```

```
OSPF: Rcv hello from 200.200.200.200 area 0 from FastEthernet0/0 10.1.1.1
OSPF: 2 Way Communication to 200.200.200.200 on FastEthernet0/0, state 2WAY
OSPF: Send DBD to 200.200.200.200 on FastEthernet0/0 seq 0x4418 opt 0x00
flag 0x7 len 32
OSPF: End of hello processing
OSPF: Neighbor change Event on interface FastEthernet0/0
OSPF: DR/BDR election on FastEthernet0/0
OSPF: Elect BDR 10.1.1.2
OSPF: Elect DR 172.16.1.1
DR: 172.16.1.1 (Id)   BDR: 10.1.1.2 (Id)
OSPF: Rcv DBD from 200.200.200.200 on FastEthernet0/0 seq 0x6d7d opt 0x00
flag 0x7 len 32  mtu 1500 state EXSTART
OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: Send DBD to 200.200.200.200 on FastEthernet0/0 seq 0x6d7d opt 0x00
flag 0x2 len 212
OSPF: Rcv DBD from 200.200.200.200 on FastEthernet0/0 seq 0x6d7e opt 0x00
flag 0x3 len 172  mtu 1500 state EXCHANGE
OSPF: Send DBD to 200.200.200.200 on FastEthernet0/0 seq 0x6d7e opt 0x00
flag 0x0 len 32
OSPF: Rcv DBD from 200.200.200.200 on FastEthernet0/0 seq 0x6d7f opt 0x00
flag 0x1 len 32  mtu 1500 state EXCHANGE
OSPF: Send DBD to 200.200.200.200 on FastEthernet0/0 seq 0x6d7f opt 0x00
flag 0x0 len 32
Exchange Done with 200.200.200.200 on FastEthernet0/0
Synchronized with 200.200.200.200 on FastEthernet0/0, state FULL
%OSPF-5-ADJCHG: Process 1, Nbr 200.200.200.200 on FastEthernet0/0 from
LOADING to FULL, Loading Done
OSPF: Send DBD to 200.200.200.200 on FastEthernet0/0 seq 0x6d7f opt 0x00
flag 0x0 len 32
```

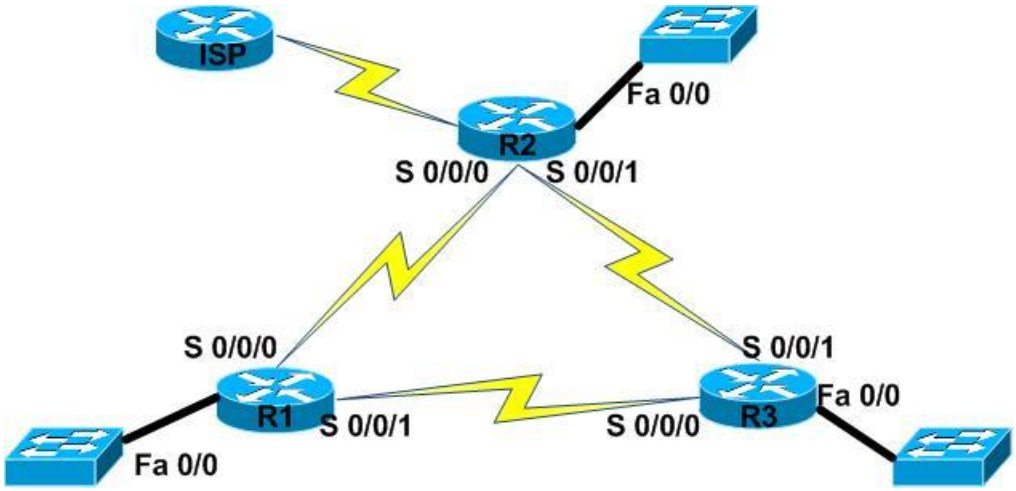
Θα πρέπει να σημειωθεί ότι εκτός από την εκλογή DR και BDR πραγματοποιείται και συγχρονισμός των βάσεων για το πρωτόκολλο OSPF που διατηρούν οι δρομολογητές με την ανταλλαγή DBDs (Database Descriptor μηνυμάτων).

7.10 Εργαστηριακή Άσκηση EIGRP

Ας θεωρήσουμε την τοπολογία της **Εικόνας 7.3**. Η διευθυνσιοδότηση (*addressing*) φαίνεται στον παρακάτω πίνακα:

Συσκευή	Interface	IP διεύθυνση	Μάσκα Subnet
R1	Fa 0/0	172.16.1.1	255.255.255.0
	S 0/0/0	172.16.3.1	255.255.255.252
	S 0/0/1	192.168.10.5	255.255.255.252
R2	Fa 0/0	172.16.2.1	255.255.255.0
	S 0/0/0	172.16.3.2	255.255.255.252
	S 0/0/1	192.168.10.9	255.255.255.252
	S 0/1/0	10.1.1.1	255.255.255.252
R3	Fa 0/0	192.168.1.1	255.255.255.0
	S 0/0/0	192.168.10.6	255.255.255.252
	S 0/0/1	192.168.10.10	255.255.255.252
ISP	S 0/0/0	10.1.1.2	255.255.255.252

Οι δρομολογητές R1, R2 και R3 συγκροτούν το Αυτόνομο Σύστημα 1 (AS=1). Όλες οι WAN συνδέσεις είναι E1 (2048 bps).



Εικόνα 7.3 Για τις εργαστηριακές ασκήσεις

Ζητούνται τα εξής:

α) Με εξαίρεση το S 0/1/0 του R2, να ενεργοποιηθεί το πρωτόκολλο EIGRP με ατομικά *network statements* με χρήση *wildcard* μασκών.
β) Να ρυθμιστεί ένα *default route* στο S 0/1/0 του R2.
γ) Με την κατάλληλη εντολή, το *default route* του R2 να διαδοθεί '*προς τα πίσω*' σε όλους τους EIGRP δρομολογητές.
δ) Να επιβεβαιωθούν οι σχέσεις γειτονίας για όλους τους δρομολογητές.
ε) Να επιβεβαιωθούν οι πίνακες δρομολόγησης.
στ) Το bandwidth στο link ανάμεσα στους R1 και R3 να γίνει 1024 bps. Τι παρατηρείτε;

7.11 Εργαστηριακή Άσκηση OSPF

Για την τοπολογία και τις διευθύνσεις της **Εικόνας 7.3** ζητούνται:

α) Με εξαίρεση το S 0/1/0 του R2, να ενεργοποιηθεί το πρωτόκολλο OSPF σε μία περιοχή (*single area*) με αριθμό διεργασίας 100.
β) Να ρυθμιστεί ένα *default route* στο S 0/1/0 του R2.
γ) Με την κατάλληλη εντολή, το *default route* του R2 να διαδοθεί '*προς τα πίσω'* σε όλους τους OSPF δρομολογητές.
δ) Να επιβεβαιωθούν οι σχέσεις γειτονίας για όλους τους δρομολογητές.
ε) Να επιβεβαιωθούν οι πίνακες δρομολόγησης.
στ) Το bandwidth στο link ανάμεσα στους R1 και R3 να γίνει 1024 bps. Τι παρατηρείτε;

8. Λίστες ελέγχου πρόσβασης

Οι λίστες ελέγχου πρόσβασης (*Access Control Lists*, ACLs) μπορούν να θεωρηθούν ένας μηχανισμός κατηγοριοποίησης πακέτων με βάση μία σειρά κριτηρίων που εξετάζονται με τη σειρά, το ένα μετά το άλλο. Η πιο βασική εφαρμογή τους είναι η λειτουργία τους ως φίλτρα πακέτων που εισέρχονται ή εξέρχονται από μία διεπα*φή (interface*). Χρησιμοποιούνται όμως και για άλλους σκοπούς όπως είναι ο περιορισμός της απομακρυσμένης πρόσβασης (*virtual type terminal access*) σε μια συσκευή δρομολόγησης ή μεταγωγής, η ανάθεση προτεραιότητας σε πακέτα με χρήση ουρών, το φιλτράρισμα πληροφορίας δρομολόγησης, η πρόκληση τηλεφωνικών συνδέσεων με χρήση *dial-on-demand* ή ο καθορισμός της κίνησης που θα προστατευθεί από ένα IPSec VPN.

8.1 Ανασκόπηση των λιστών ελέγχου πρόσβασης

Μία λίστα ελέγχου πρόσβασης είναι ένα σύνολο από εντολές (*statements*), ομαδοποιημένες σύμφωνα με έναν αριθμό ή ένα όνομα, που χρησιμοποιούνται για να ελέγξουν τη ροή της κίνησης που εισέρχεται ή εξέρχεται σε ένα interface. Οι εντολές αυτές καθορίζουν με αυστηρό τρόπο την κίνηση που επιτρέπεται ή απαγορεύεται. Τις εισάγουμε σε *Global Configuration Mode* και τις εφαρμόζουμε σε *interface* ή *sub-interface mode*. Όταν εφαρμόζουμε μια λίστα ελέγχου πρόσβασης, πρέπει να καθορίσουμε την κατεύθυνση της κίνησης θα φιλτραριστεί[1]:

- **Εισερχόμενη (*inbound*):** σε αυτή την περίπτωση η κίνηση εισέρχεται σε ένα *interface* από μια εξωτερική πηγή.
- **Εξερχόμενη (*outbound*):** η κίνηση ελέγχεται πριν εξέλθει από ένα *interface*.

Στην περίπτωση που μια λίστα ελέγχου πρόσβασης εφαρμόζεται στην εισερχόμενη κίνηση, τότε η συσκευή ελέγχει την κίνηση προτού αυτή μεταφερθεί από ένα *interface* σε ένα άλλο. Αντίθετα όταν εφαρμόζεται στην εξερχόμενη κίνηση, το πακέτο εισέρχεται από ένα *interface*, γίνεται η δρομολόγηση, το πακέτο μεταφέρεται στο *interface* εξόδου και τότε ελέγχονται οι κανόνες της λίστας.

Σημαντικές οδηγίες για τη ρύθμιση

Μερικά πολύ σημαντικά ζητήματα για την υλοποίηση, επεξεργασία και συντήρηση των λιστών ελέγχου πρόσβασης είναι τα παρακάτω:

- Η επεξεργασία των εντολών (*statements*) μιας λίστας ελέγχου πρόσβασης, γίνεται από επάνω προς τα κάτω, από την πρώτη προς την τελευταία εντολή, μέχρι να γίνει ταίριασμα του πακέτου. Όταν αυτό συμβεί, τότε εκτελείται η εντολή της λίστας και δεν πραγματοποιούνται επιπλέον έλεγχοι στο πακέτο.

[1] Θα αντιμετωπίσουμε εδώ τις ACLs απλά ως φίλτρα της κίνησης από / προς μία διεπαφή, δηλαδή ως μία διαδικασία επιλογής ανάλογα με τα κριτήρια που διατυπώνονται στα *statements* της λίστας.

- Η σειρά με την οποία εισάγουμε τις εντολές σε μια λίστα ελέγχου πρόσβασης είναι σημαντική: οι πιο περιοριστικές εντολές (αυτές που αναφέρονται σε πιο συγκεκριμένα δίκτυα), πρέπει να τοποθετούνται στην κορυφή της λίστας, ενώ οι λιγότερο περιοριστικές τοποθετούνται στο κατώτερο μέρος της. Ενδείκνυται δηλαδή η διάταξη των εντολών από το ειδικό στο γενικό.
- Στο τέλος κάθε λίστας τοποθετείται αυτόματα μια εντολή που δεν εμφανίζεται αλλά έμμεσα απαγορεύει οποιοδήποτε τύπο κίνησης που δεν έχει ήδη επιτραπεί με κάποια από τις προηγούμενες εντολές (*implicit deny*)**.**
- Οι λίστες ελέγχου πρόσβασης δε μπορούν να φιλτράρουν την κίνηση που ξεκινά από τον ίδιο τον δρομολογητή, στον οποίο έχουν εφαρμοστεί.
- Σε κάθε διεπαφή (*interface*) μπορούμε να τοποθετήσουμε μία λίστα ελέγχου πρόσβασης ανά κατεύθυνση και ανά πρωτόκολλο του Επιπέδου 3.
- Αν εφαρμόσουμε μια κενή, δηλαδή χωρίς κανένα *statement*, λίστα ελέγχου πρόσβασης σε ένα *interface*, τότε όλη η κίνηση θα επιτρέπεται να περάσει! Το *implicit deny* τοποθετείται στο τέλος μιας λίστας μόνο όταν αυτή έχει τουλάχιστο μία άλλη εντολή.

Υπάρχουν δύο βασικοί τύποι λιστών: οι βασικές (*standard*) και οι εκτεταμένες (*extended*). Οι *standard* φιλτράρουν λαμβάνοντας υπόψη τους μόνο την IP διεύθυνση της αφετηρίας ενός πακέτου, ενώ οι *extended* μπορούν να φιλτράρουν λαμβάνοντας υπόψη τους τόσο τις IP διευθύνσεις αφετηρίας και προορισμού, το πρωτόκολλο (TCP, UDP, ICMP …) καθώς και πληροφορίες του πρωτοκόλλου (όπως είναι οι TCP και UDP θύρες ή οι τύποι των ICMP μηνυμάτων).

Μια άλλη διάκριση των λιστών ελέγχου πρόσβασης γίνεται αναφορικά με τον τρόπο αναφοράς τους. Έτσι υπάρχουν οι αριθμημένες (*numbered*) λίστες και οι λίστες με όνομα (*named*). Μία αριθμημένη λίστα μπορεί να είναι *standard* ή *extended*. Το ίδιο συμβαίνει και με μία λίστα με όνομα (και πάλι μπορεί να είναι είτε *standard* είτε *extended*).

8.2 Βασική ρύθμιση

Προκειμένου να δημιουργήσουμε μια αριθμημένη λίστα ελέγχου πρόσβασης χρησιμοποιούμε την παρακάτω σύνταξη:

```
Router(config)# access-list <αριθμός> permit | deny <συνθήκη>
```

Ανάλογα με τον αριθμό που αναθέτουμε στη λίστα, αυτή θα είναι είτε *standard* είτε *extended*. Όπως φαίνεται και από τον παρακάτω πίνακα, το πλήθος των αριθμημένων λιστών πρόσβασης που μπορούμε να δημιουργήσουμε είναι περιορισμένος. Στις λίστες με όνομα δεν υπάρχει αντίστοιχος περιορισμός.

Τύπος λίστας ελέγχου πρόσβασης	**Αριθμοί**
Standard IP	1 - 99, 1300 - 1999
Extended IP	100 – 199, 2000 - 2699

Η συνθήκη μετά το `perimit / deny` περιγράφει στο δρομολογητή ποια περιεχόμενα του πακέτου θα πρέπει να ελέγξει προκειμένου να επιτρέψει ή να απαγορεύσει τη διέλευσή του. Η συνθήκη μπορεί να περιλαμβάνει τον έλεγχο διευθύνσεων IP και πρωτοκόλλου. Όταν υπάρχει ταίριασμα (*match*) τότε εκτελεί την εντολή και δεν συνεχίζει τον έλεγχο της λίστας, ενώ αν δεν υπάρχει ταίριασμα συνεχίζει τον έλεγχο στην επόμενη εντολή, μέχρι το τέλος της λίστας.

Μάσκες *Wildcard* (μπαλαντέρ)

Οι μάσκες *wildcard* χρησιμοποιούνται στις λίστες ελέγχου πρόσβασης προκειμένου να περιγράψουν μία συγκεκριμένη συσκευή, ένα δίκτυο, ή ένα τμήμα δικτύου. Τις συναντήσαμε στη ρύθμιση του OSPF, αλλά και του EIGRP. Όπως και οι μάσκες υποδικτύου έτσι και οι μάσκες *wildcard* αποτελούνται από 32 bits. Όταν η μάσκα *wildcard* έχει την τιμή 0 σε μια θέση, τότε η αντίστοιχη θέση στη διεύθυνση της λίστας ελέγχου πρόσβασης πρέπει να ταιριάξει ακριβώς. Τα μηδενικά στη wildcard μάσκα λέγονται και *do-care bits*, με την έννοια ότι δηλώνουν τα *bits* στη διεύθυνση της λίστας ελέγχου πρόσβασης που πρέπει να ταυτίζονται με τα αντίστοιχα *bits* στο πακέτο που ελέγχεται από τη λίστα.

Παράδειγμα 1
Εάν έχουμε το συνδυασμό `172.16.0.0/20`, ξεκινάμε γράφοντας στο δυαδικό σύστημα τη μάσκα υποδικτύωσης `255.255.240.0`:

`11111111.11111111.11110000.00000000`

και αντιστρέφοντας τα ψηφία:

`00000000.00000000.00001111.1111 1111`

Οπότε η μάσκα wildcard είναι: `0.0.15.255`

Παράδειγμα 2
Εάν θεωρήσουμε το `172.17.4.0/22`, δηλαδή με μάσκα υποδικτύωσης `255.255.252.0` ξεκινάμε γράφοντας τη και πάλι στο δυαδικό σύστημα:

`11111111.11111111.11111100.00000000`

και αντιστρέφοντας τα ψηφία:

`00000000 00000000.00000011.1111 1111`

Οπότε η μάσκα wildcard είναι: `0.0.3.255`

Ειδικές μάσκες *wildcard*:

Υπάρχουν δύο ειδικές μάσκες *wildcard*: η **`0.0.0.0`** και η **`255.255.255.255`**. Η πρώτη (**`0.0.0.0`**) προσδιορίζει ότι και τα 32 bits της διεύθυνσης της εντολής της λίστας ελέγχου πρόσβασης πρέπει να ταυτίζονται με εκείνα που υπάρχουν στο προς εξέταση IP πακέτο προκειμένου να πραγματοποιηθεί η ενέργεια που περιγράφεται (*permit* ή *deny*). Η μάσκα αυτή είναι γνωστή και ως μάσκα συσκευής (*host mask*). Ένα παράδειγμα είναι το **`192.168.1.10 0.0.0.0`** όπου ο δρομολογητής εξετάζει αν το πακέτο περιέχει ακριβώς τη διεύθυνση **`192.168.1.10`**. Στην περίπτωση που δεν την περιέχει τότε προχωρά στην εξέταση της επόμενης εντολής της λίστας

ελέγχου πρόσβασης. Το παραπάνω παράδειγμα μπορεί να γραφεί και ως **`host 192.168.1.10`**.

Η δεύτερη μάσκα (**`255.255.255.255`**) προσδιορίζει ότι δεν έχει σημασία τι περιέχεται στο πακέτο που εξετάζεται από την αντίστοιχη εντολή της λίστας ελέγχου πρόσβασης. Ένα παράδειγμα είναι το **`0.0.0.0 255.255.255.255`** που μπορεί να γραφεί και ως **`any`**.

Αμέσως παρακάτω δίνονται παραδείγματα συνδυασμών IP Διεύθυνσης και Wildcard Μάσκας, μαζί με τη λειτουργία τους:

IP Διεύθυνση	**Μάσκα Wildcard**	**Επεξήγηση**
`0.0.0.0`	`255.255.255.255`	Γίνεται ταίριασμα οποιασδήποτε διεύθυνσης (μπορεί να αντικατασταθεί με τη λέξη **`any`**)
`192.168.1.10`	`0.0.0.0`	Γίνεται ταίριασμα ακριβώς με την IP διεύθυνση 192.168.1.10 Μπορεί να αντικατασταθεί με το **`host 192.168.1.10`**
`192.168.1.0`	`0.0.0.255`	Γίνεται ταίριασμα με τις διευθύνσεις που βρίσκονται στο διάστημα 192.168.1.1 – 192.168.1.255
`172.30.0.0`	`0.0.255.255`	Γίνεται ταίριασμα με τις διευθύνσεις που βρίσκονται στο διάστημα 172.30.0.0 – 172.30.255.255
`10.0.0.0`	`0.255.255.255`	Γίνεται ταίριασμα με τις διευθύνσεις που βρίσκονται στο διάστημα 10.0.0.0 – 10.255.255.255

Ενεργοποίηση μιας λίστας ελέγχου πρόσβασης

Μια λίστα ελέγχου πρόσβασης δεν κάνει τίποτα έως ότου τοποθετηθεί σε ένα *interface*. Η εντολή που την ενεργοποιεί είναι η παρακάτω:

```
Router(config)# interface <ονομασία interface>
Router(config-if)# ip access-group <αριθμός ACL> in | out
```

Αρχικά εισερχόμαστε στο *interface* που θα ρυθμίσουμε τη λίστα και στη συνέχεια την ενεργοποιούμε είτε με τον αριθμό είτε με το όνομά της προσέχοντας την κατεύθυνση που θα χρησιμοποιήσουμε: **`in`** αν επιθυμούμε να ελέγχεται η κίνηση εισερχόμενη στο interface ή **`out`** αν επιθυμούμε να ελέγχεται η κίνηση όταν εξέρχεται από το *interface*. Λέμε επίσης ότι η λίστα '*γκρουπάρεται*' στο *interface*.

Προσοχή: Μπορούμε να εφαρμόσουμε **μόνο μία λίστα** ανά πρωτόκολλο, ανά *interface* και ανά κατεύθυνση, δηλαδή για το πρωτόκολλο IP μπορούμε να εφαρμόσουμε μόνο μία λίστα με κατεύθυνση in ή out σε ένα *interface*.

8.3 Τύποι λιστών ελέγχου πρόσβασης

***Standard* λίστες ελέγχου πρόσβασης:** είναι οι πιο απλές λίστες και φιλτράρουν μόνο με βάση τη διεύθυνση αφετηρίας ενός πακέτου (*source IP address*). Για να δημιουργηθούν χρησιμοποιούμε την παρακάτω εντολή:

```
Router(config)# access-list 1-99 | 1300-1999 permit | deny <IP διεύθυνση
                πηγής> <μάσκα wildcard> [log]
```

Σε μια *standard* λίστα ελέγχου πρόσβασης μπορούμε να χρησιμοποιήσουμε τους αριθμούς 1-99 και 1300-1999, να περιγράψουμε την ενέργεια που θα πραγματοποιηθεί (*permit* ή *deny*) και τη διεύθυνση αφετηρίας του πακέτου. Στο τέλος της εντολής, προαιρετικά, τοποθετείται η επιλογή `log` που δίνει τη δυνατότητα, αν υπάρξει ταίριασμα κάποιου πακέτου, να εμφανιστεί ανάλογο μήνυμα στην κονσόλα ή σε κάποιον syslog εξυπηρετητή.

***Extended* λίστες ελέγχου πρόσβασης:** Οι *extended* λίστες ελέγχου πρόσβασης είναι πιο ευέλικτες από τις *standard* δίνοντας τη δυνατότητα να γίνει ταίριασμα ενός πακέτου με βάση τα παρακάτω χαρακτηριστικά:

- IP διεύθυνση αφετηρίας ή IP διεύθυνση προορισμού
- Πρωτόκολλο (TCP, UDP, ICMP, IP)
- Θύρα Υπηρεσίας για το TCP και UDP, ή τύπος μηνύματος για το ICMP

Για να δημιουργηθούν χρησιμοποιούμε την παρακάτω εντολή:

```
Router(config)# access-list 100-199|2000-2699 permit | deny
                <πρωτόκολλο>
                <IP διεύθυνση πηγής> <μάσκα wildcard> <πληροφορία
                πρωτοκόλλου>
                <IP διεύθυνση προορισμού> <μάσκα wildcard>
                <πληροφορία πρωτοκόλλου> [log]
```

Σε μια *extended* λίστα ελέγχου πρόσβασης μπορούμε να χρησιμοποιήσουμε τους αριθμούς **`100-199`** και **`2000-2699`**, να περιγράψουμε την ενέργεια που θα πραγματοποιηθεί (**`permit`** ή **`deny`**), το πρωτόκολλο, τη διεύθυνση αφετηρίας του πακέτου και τη μάσκα *wildcard* αλλά και τη διεύθυνση προορισμού του πακέτου και τη μάσκα *wildcard*. Στο τέλος της εντολής και πάλι προαιρετικά τοποθετείται η επιλογή **`log`** που δίνει τη δυνατότητα, αν υπάρξει ταίριασμα κάποιου πακέτου με τη λίστα, να εμφανιστεί ανάλογο μήνυμα στην κονσόλα ή σε κάποιον syslog εξυπηρετητή.

Τα πρωτόκολλα που μπορούν να περιγραφούν από την extended λίστα ελέγχου πρόσβασης περιλαμβάνουν τα **`tcp`**, **`udp`**, **`ip`**, **`icmp`**, **`gre`**, **`eigrp`**, **`igmp`**, **`ospf`** κ.α. Σε περίπτωση που επιθυμούμε να φιλτράρονται όλα τα πρωτόκολλα χρησιμοποιούμε το **`ip`**.

Επομένως υπάρχουν δύο μεγάλες προσθήκες σε σχέση με τις *standard* λίστες ελέγχου πρόσβασης. Η πρώτη είναι η χρήση του πρωτοκόλλου που προσδιορίζει κάποιον συγκεκριμένο τύπο κίνησης ενώ η δεύτερη είναι ότι μπορούν να καθορίζονται τόσο η διεύθυνση πηγής όσο και η διεύθυνση προορισμού.

Extended λίστες ελέγχου πρόσβασης για τα πρωτόκολλα TCP και UDP

Για να δημιουργήσουμε μια λίστα ελέγχου πρόσβασης για το TCP ή UDP χρησιμοποιούμε το παρακάτω συντακτικό:

```
Router(config)# access-list 100-199|2000-2699 permit | deny
                tcp | udp
                <IP διεύθυνση πηγής> <μάσκα wildcard> <τελεστής θύρα>
                <IP διεύθυνση προορισμού> <μάσκα wildcard> <τελεστής θύρα >
                [established][log]
```

Σε αυτές τις λίστες χρησιμοποιούμε τον προσδιοριστή **`permit`** ή **`deny`** και στη συνέχεια το πρωτόκολλο **`tcp`** ή **`udp`**. Περιγράφουμε τις διευθύνσεις αφετηρίας και προορισμού συνοδευόμενες από τις κατάλληλες μάσκες *wildcard*, αλλά τοποθετούμε και από ποια θύρα γίνεται εκκίνηση της συνομιλίας καθώς και σε ποια θύρα απευθύνεται η συνομιλία (προσδιορίζοντας έτσι την αντίστοιχη υπηρεσία). Οι τελεστές που μπορούν να χρησιμοποιηθούν παρουσιάζονται στον παρακάτω πίνακα:

Τελεστής	Επεξήγηση
`eq`	Ίσο με
`neq`	Όχι ίσο με
`range`	Διάστημα αριθμών θυρών
`gt`	Μεγαλύτερο από
`lt`	Μικρότερο από

Επιπλέον μπορούμε να προσδιορίσουμε την υπηρεσία ή τη θύρα που αντιστοιχεί σε αυτή. Μερικές από αυτές απεικονίζονται στον παρακάτω πίνακα:

Υπηρεσία	Εντολή	Αριθμός θύρας
ftp data	`ftp-data`	20
ftp control	`ftp`	21
Secure Shell	`Ssh`	22
Telnet	`telnet`	23
Smtp	`Smtp`	25
DNS	`Domain`	53
TFTP	`Tftp`	69
HTTP	`www`	80
POP3	`pop3`	110
SNMP	`Snmp`	161

Τέλος η λέξη `established` αναφέρεται σε συνδέσεις TCP. Αυτή αφορά κίνηση που έχει ξεκινήσει από το εσωτερικό μέρος του δικτύου και φιλτράρεται από τη λίστα ελέγχου πρόσβασης κατά την επιστροφή της στο δίκτυο. Έτσι απαγορεύει ή επιτρέπει, ανάλογα εάν έχει τοποθετηθεί `permit` ή `deny` στην εντολή, την κίνηση που έχει ενεργοποιημένα συγκεκριμένα *flags* στην προμετωπίδα (*header*) του TCP *segment*.

Extended λίστες ελέγχου πρόσβασης για το πρωτόκολλο ICMP

Για να δημιουργήσουμε μια λίστα ελέγχου πρόσβασης για το πρωτόκολλο ICMP χρησιμοποιούμε το παρακάτω συντακτικό:

```
Router(config)# access-list 100-199|2000-2699 permit | deny icmp
                <IP διεύθυνση πηγής> <μάσκα wildcard>
                <IP διεύθυνση προορισμού> <μάσκα wildcard>
                [μήνυμα ICMP][log]
```

Σε αντίθεση με το TCP και UDP, το πρωτόκολλο ICMP δε χρησιμοποιεί θύρες αλλά τύπους μηνυμάτων, όπως είδαμε σε προηγούμενη ενότητα. Στον παρακάτω πίνακα εμφανίζονται τα πιο συχνά χρησιμοποιούμενα μηνύματα τα οποία μπορούμε να εισάγουμε είτε με το όνομα τους ή τον αριθμό τους. Στην περίπτωση που δεν περιληφθεί ο τύπος μηνύματος τότε η εντολή προσδιορίζει όλους τους τύπους μηνυμάτων.

Τύπος μηνύματος	Περιγραφή Μηνύματος
echo	Χρησιμοποιείται από το Ping για να ελέγξει έναν προορισμό
echo-reply	Είναι η απάντηση σε ένα echo μήνυμα
host-unreachable	Δεν ανταποκρίνεται μια συγκεκριμένη συσκευή
net-unreachable	Δεν ανταποκρίνεται ένα δίκτυο
traceroute	Ελέγχει την πληροφορία του traceroute

Ονοματισμένες λίστες ελέγχου πρόσβασης (Named ACLs):

Οι ονοματισμένες λίστες ελέγχου πρόσβασης μας επιτρέπουν να ξεπεράσουμε τον περιορισμό του πλήθους των αριθμημένων λιστών που μπορούμε να δημιουργήσουμε σε μια συσκευή. Επιπλέον, σε αντίθεση με τις αριθμημένες λίστες, στις ονοματισμένες μπορούμε να σβήσουμε ή να προσθέσουμε μία εντολή χωρίς να σβηστεί ολόκληρη η λίστα (είναι όπως λέμε *editable*).

Για να δημιουργήσουμε μια ονοματισμένη λίστα ελέγχου πρόσβασης ακολουθούμε την παρακάτω σύνταξη:

```
Router(config)#    ip access-list standard | extended <όνομα>
```

Αρχικά προσδιορίζουμε τον τύπο της λίστας, δηλ. `standard` ή `extended`. Δηλώνουμε ένα μοναδικό όνομα και μεταφερόμαστε σε ACL *subconfiguration mode*.

```
Router(config-std-acl)#
```

ή

```
Router(config-ext-acl)#
```

Έτσι, για μια `standard` ονοματισμένη λίστα ελέγχου πρόσβασης μπορούμε να εισάγουμε τα παρακάτω:

```
Router(config)#     ip access-list standard <όνομα>
Router(config-std-acl)# permit | deny
                        <IP διεύθυνση πηγής> <μάσκα wildcard>
```

Ενώ για μια `extended` ονοματισμένη λίστα ελέγχου πρόσβασης μπορούμε να εισάγουμε τα παρακάτω:

```
Router(config)#     ip access-list extended <όνομα>
Router(config-std-acl)# permit | deny
                        <IP διεύθυνση πηγής> <μάσκα wildcard>
                        [πληροφορία πρωτοκόλλου]
                        <IP διεύθυνση προορισμού> <μάσκα wildcard>
                        [πληροφορία πρωτοκόλλου] [log]
```

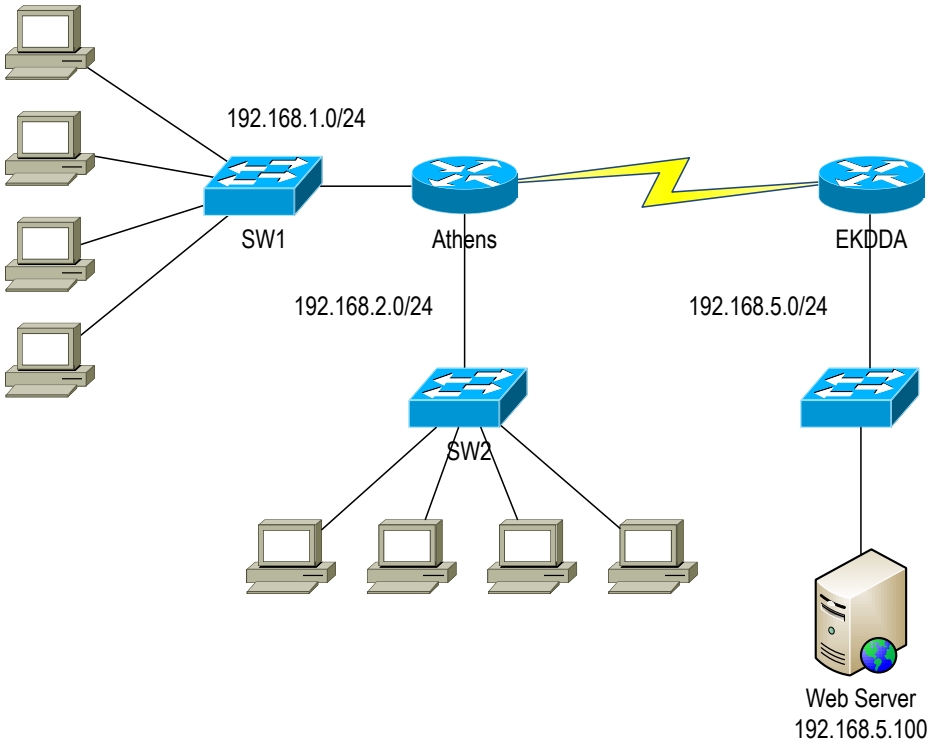
8.4 Τοποθέτηση και παραδείγματα χρήσης των λιστών ελέγχου πρόσβασης

Σαν έναν πρόχειρο κανόνα θα πρέπει να θυμόμαστε ότι:

- Οι *standard* λίστες ελέγχου πρόσβασης θα πρέπει να τοποθετούνται όσο πιο κοντά στον προορισμό (*closer to the destination*) ενώ,
- Οι *extended* λίστες ελέγχου πρόσβασης θα πρέπει να τοποθετούνται όσο πιο κοντά στην αφετηρία (*closer to the source*).

Παράδειγμα 1

Στην τοπολογία της **Εικόνας 8.1** επιθυμούμε να απαγορεύσουμε την πρόσβαση του δικτύου 192.168.1.0/24 στο Web Server που βρίσκεται στο εσωτερικό δίκτυο του δρομολογητή EKDDA (για όλες τις υπηρεσίες που φιλοξενούνται σε αυτό τον *server*), δηλαδή στη διεύθυνση 192.168.5.100.



Εικόνα 8.1 Για τα Παραδείγματα 1, 2

Θα υλοποιήσουμε μια *standard* λίστα ελέγχου πρόσβασης με τις παρακάτω εντολές:

```
R(config)#access-list 10 deny 192.168.1.0 0.0.0.255 host 192.168.5.100
R(config)#access-list 10 permit any
```

Αυτή η λίστα επιτρέπει σε όλους να συνδεθούν στον Web Server (permit any) αλλά απαγορεύει την πρόσβαση σε όσους βρίσκονται στο δίκτυο 192.168.1.0/24. Πού θα την εφαρμόσουμε όμως; Αν την εφαρμόσουμε στο δρομολογητή Athens τότε όντως θα αποτρέψουμε τις συσκευές από το δίκτυο 192.168.1.0/24 να επικοινωνήσουν με τον Web Server, αλλά θα τις αποτρέψουμε και από το να επικοινωνήσουν με οποιονδήποτε άλλο προορισμό.

Για να επιτύχουμε το στόχο μας, θα την εφαρμόσουμε στο FastEthernet *interface* του δρομολογητή EKDDA με κατεύθυνση `out`. Θα μπορούσε βέβαια κάποιος πολύ ορθά να προτείνει να την εφαρμόσουμε στο σειριακό interface του δρομολογητή EKDDA με κατεύθυνση in. Αυτό όμως θα δημιουργούσε προβλήματα σε τυχόν μελλοντική επέκταση του δικτύου. Σκεφτείτε αν στο δρομολογητή EKDDA συνδέσουμε ένα δεύτερο Ethernet *interface*. Τότε αν είχαμε εφαρμόσει τη *standard* λίστα ελέγχου πρόσβασης στο σειριακό interface, οι συσκευές από το δίκτυο 192.168.1.0/24 δε θα μπορούσαν να επικοινωνήσουν και με το νέο αυτό δίκτυο.

Σε κάθε περίπτωση όμως, ας σκεφτούμε τι συμβαίνει όταν ένα πακέτο ξεκινήσει με αφετηρία μία συσκευή με διεύθυνση 192.168.1.10 με προορισμό τον Web Server. Θα περάσει από το δρομολογητή Athens, θα φτάσει στο δρομολογητή EKDDA, αυτός θα εξετάσει τη διεύθυνση προορισμού και θα το μεταφέρει από το σειριακό του *interface*

στο FastEthernet *interface*. Εκεί θα το εξετάσει η *standard* λίστα ελέγχου πρόσβασης και θα το απορρίψει. Δηλαδή το πακέτο, θα ταξιδέψει σε ολόκληρο το δίκτυο μας μέχρι να απορριφθεί πολύ κοντά στον προορισμό. Αυτό επιβαρύνει τόσο τη γραμμή όσο και τους πόρους των δρομολογητών.

Παράδειγμα 2

Προκειμένου να ξεπεράσουμε τους περιορισμούς από τη χρήση της *standard* λίστας ελέγχου πρόσβασης του προηγούμενου παραδείγματος, θα κατασκευάσουμε μια *extended* λίστα που θα τοποθετήσουμε κοντά στην αφετηρία των πακέτων. Αυτή θα αποτρέψει τα πακέτα από το να ταξιδέψουν άσκοπα στο δίκτυό μας πριν απορριφθούν, επιτυγχάνοντας τα ίδια αποτελέσματα με μεγαλύτερη ακρίβεια.

Η λίστα ελέγχου πρόσβασης θα είναι:

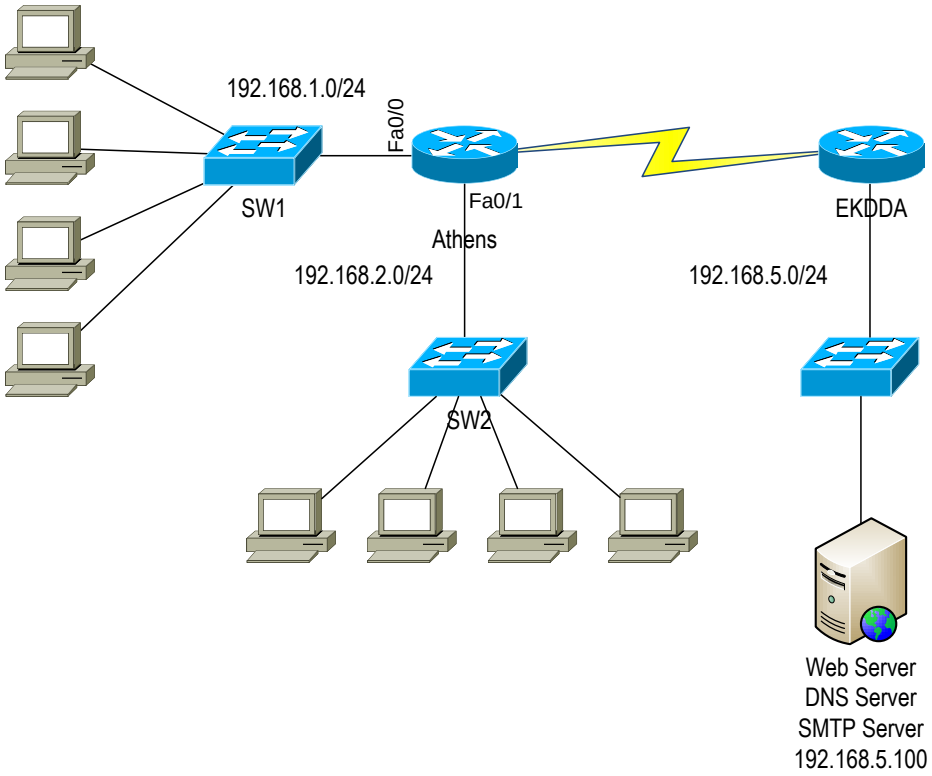
```
R(config)#access-list 100 deny ip 192.168.1.0 0.0.0.255 host 192.168.5.100
R(config)#access-list 100 permit ip any any
```

Σε αυτή την περίπτωση θα τοποθετήσουμε τη λίστα όσο πιο κοντά στην πηγή δηλαδή στο FastEthernet *interface* του δρομολογητή Athens που συνδέεται απευθείας με το δίκτυο 192.168.1.0/24 και με κατεύθυνση `in`. Μετά την εφαρμογή της λίστας τα πακέτα που έχουν αφετηρία οποιαδήποτε διεύθυνση στο δίκτυο 192.168.1.0/24 και προορισμό τον Web Server (192.168.5.100) θα απορρίπτονται κατά την είσοδο τους στο FastEthernet *interface* του δρομολογητή. Αν όμως απευθύνονται σε οποιαδήποτε άλλη IP διεύθυνση δε θα ταυτίζονται με την πρώτη εντολή της λίστας ελέγχου πρόσβασης αλλά με τη δεύτερη (`permit ip any any`) οπότε και θα τους επιτρέπεται η είσοδος.

Παράδειγμα 3

Ας εμπλουτίσουμε λίγο όμως το παράδειγμα μας. Το ΕΚΔΔΑ αποφάσισε να εγκαταστήσει στον Web Server και δύο άλλες υπηρεσίες, η μία είναι το DNS (Domain Name Service) και η άλλη είναι το SMTP (έναν εξυπηρετητή αλληλογραφίας), όπως φαίνεται στην **Εικόνα 8.2**. Τώρα το ζητούμενο είναι το εξής:

1. Οι τελευταίες 32 (τριάντα δύο) διευθύνσεις του δικτύου 192.168.1.0/24, δηλαδή οι διευθύνσεις 192.168.1.224 – 192.168.1.255 να μπορούν να συνδεθούν με την υπηρεσία Web του εξυπηρετητή 192.168.5.100 και με την υπηρεσία DNS αλλά όχι με την υπηρεσία SMTP.
2. Όλες οι υπόλοιπες διευθύνσεις από το δίκτυο 192.168.1.0/24 να μπορούν να συνδεθούν με την υπηρεσία SMTP αλλά όχι με τις υπηρεσίες DNS και Web.
3. Όλες οι διευθύνσεις από το δίκτυο 192.168.2.0/24 να μπορούν να συνδεθούν σε όλες τις υπηρεσίες της συσκευής 192.168.5.100.
4. Να απαγορεύεται οποιαδήποτε άλλη κίνηση.



Εικόνα 8.2 Για τα Παραδείγματα 3, 4

Μία απάντηση θα μπορούσε να είναι η παρακάτω:

```
R(config)#access-list 100 permit tcp 192.168.1.224 0.0.0.31 host 192.168.5.100 eq www
R(config)#access-list 100 permit udp 192.168.1.224 0.0.0.31 host 192.168.5.100 eq dns
R(config)#access-list 100 deny tcp 192.168.1.224 0.0.0.31 host 192.168.5.100 eq smtp
R(config)#access-list 100 deny tcp 192.168.1.0 0.0.0.255 host 192.168.5.100 eq www
R(config)#access-list 100 deny udp 192.168.1.0 0.0.0.255 host 192.168.5.100 eq dns
R(config)#access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 192.168.5.100 eq smtp
R(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 host 192.168.5.100
R(config)#access-list 100 deny ip any any
```

Οι δύο πρώτες εντολές επιτρέπουν στο δίκτυο 192.168.1.224/27, δηλαδή στις τελευταίες 32 διευθύνσεις να έχουν πρόσβαση στις υπηρεσίες WWW (πρωτόκολλο TCP και θύρα 80) και DNS (πρωτόκολλο UDP και θύρα 53) που λειτουργούν στη συσκευή με διεύθυνση 192.168.5.100. Η Τρίτη εντολή απαγορεύει στο δίκτυο 192.168.1.224/27 την πρόσβαση στην υπηρεσία SMTP (πρωτόκολλο TCP και θύρα 25) που λειτουργεί στη συσκευή με διεύθυνση 192.168.5.100.

Οι εντολές 4, 5 και 6 απαγορεύουν στο δίκτυο 192.168.1.0/24, την πρόσβαση στις υπηρεσίες WWW και DNS που λειτουργούν στη συσκευή με διεύθυνση 192.168.5.100 ενώ επιτρέπουν την πρόσβαση στην υπηρεσία SMTP.

Η 7η εντολή επιτρέπει στο δίκτυο 192.168.2.0/24 να έχει πρόσβαση σε όλες τις υπηρεσίες που εκτελούνται στον εξυπηρετητή με διεύθυνση 192.168.5.100.

Τέλος η 8η εντολή απαγορεύει οποιαδήποτε άλλη κίνηση να περάσει. Σε περίπτωση που δεν τοποθετήσουμε αυτή την εντολή, θα εισαχθεί από το λειτουργικό σύστημα αυτόματα όταν ολοκληρώσουμε τη λίστα (implicit deny). Τώρα όμως θα έχουμε τη δυνατότητα να με χρήση της εντολή show access-lists na παρατηρήσουμε αν υπάρχει κίνηση που δεν ταυτίζεται με κάποια από τις προηγούμενες εντολές και φιλτράρεται από την απαγορευτική εντολή (deny ip any any).

Στη συνέχεια όμως πού θα εφαρμοστεί αυτή τη λίστα; Για να μπορεί να φιλτράρει τα δίκτυα 192.168.1.0/24 και 192.168.2.0/24 και να είναι όσο το δυνατό πιο κοντά στην αφετηρία θα πρέπει να τοποθετηθεί στο σειριακό *interface* του δρομολογητή Athens με κατεύθυνση `out`. Δηλαδή:

```
Athens(config)# int Serial 0/0/0
Athens(config-if)# ip access-group 100 out
```

Παράδειγμα 4

Ο διαχειριστής του δρομολογητή Athens αποφάσισε να περιορίσει την πρόσβαση μέσω απομακρυσμένης σύνδεσης (με χρήση telnet ή SSH) στο δρομολογητή. Συγκεκριμένα θα επιτρέψει στις διευθύνσεις 192.168.1.10 και 192.168.2.30 να μπορούν να συνδεθούν στο δρομολογητή. Για να το πετύχει αυτό κατασκευάζει μια standard λίστα ελέγχου πρόσβασης που επιτρέπει αυτές τις διευθύνσεις:

```
Athens(config)#access-list 15 permit host 192.168.1.10
Athens(config)#access-list 15 permit host 192.168.2.30
```

Στη συνέχεια όμως πού θα εφαρμόσει αυτή τη λίστα; Αυτή είναι μια ειδική λίστα και εφαρμόζεται στις γραμμές VTY του δρομολογητή. Αυτό το επιτυγχάνουμε με τις παρακάτω εντολές:

```
Athens(config)# line vty 0 4
Athens(config-line)# access-class 15 in
```

Παρατηρούμε ότι χρησιμοποιείται η εντολή `access-class` για να εφαρμόσουμε τη standard λίστα ελέγχου πρόσβασης στις γραμμές VTY.

9. Εισαγωγή στους μεταγωγείς

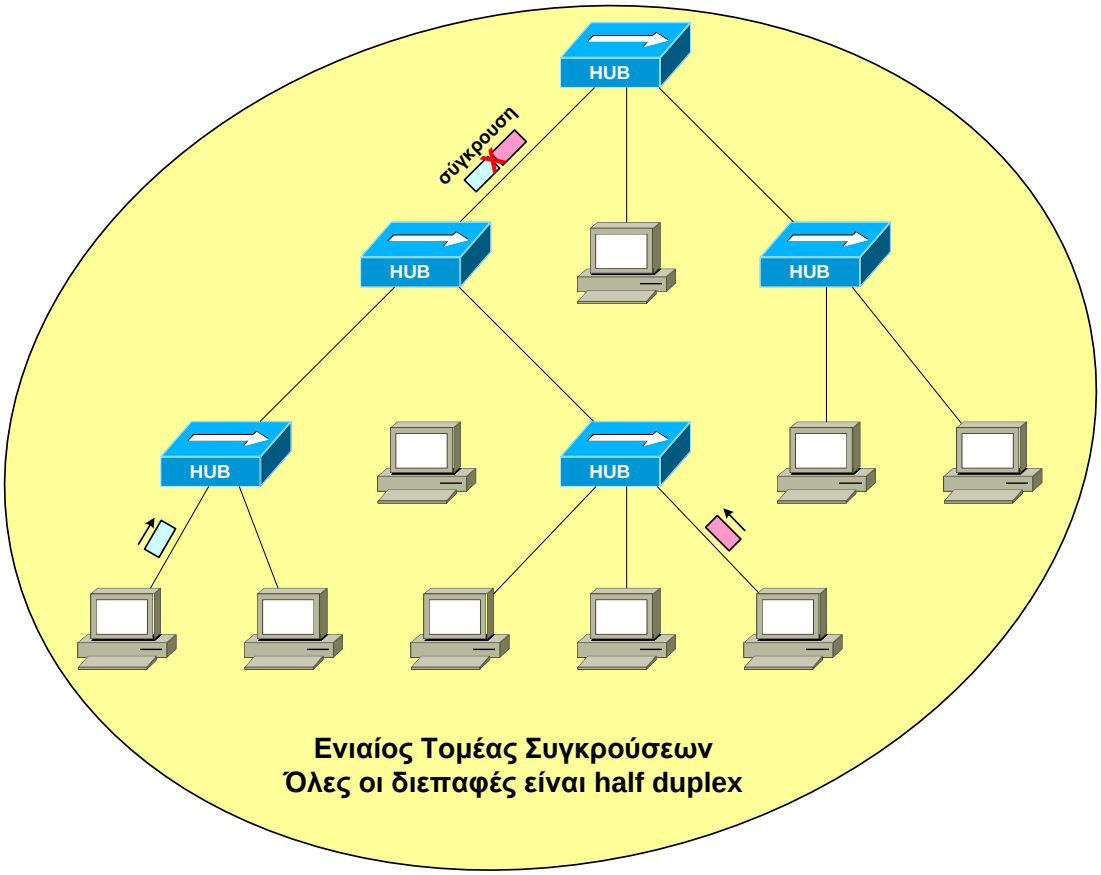
9.1 Από τα hubs, στις γέφυρες, στους μεταγωγείς

Το Ethernet είχε δύο βασικά προβλήματα στην ανάπτυξη μεγάλων δικτύων. Την απόσταση και τις συγκρούσεις. Με τη χρήση δομημένης καλωδίωσης καλωδίων UTP, η μέγιστη δυνατή απόσταση διαμορφώθηκε στα 100 μέτρα, λόγω της απορρόφησης σήματος και των παρεμβολών από μαγνητικά πεδία. Μια λύση ήταν η χρήση ενός επαναλήπτη φυσικού επιπέδου (*repeater*) για την αναγέννηση του σήματος. Στην περίπτωση της καλωδίωσης UTP αυτός έπαιρνε τη μορφή μιας CSMA/CD πλήμνης (*hub*). Ένα *hub* είναι μια συσκευή πρώτου επιπέδου δικτύου, με πολλές διεπαφές RJ-45, η οποία λαμβάνει ένα σήμα σε μια θύρα και την αναγεννά σε όλες τις άλλες. Ωστόσο, εάν το σήμα που εισέρχεται είναι κακό, ή το πλαίσιο είναι κατεστραμμένο, το *hub* επαναλαμβάνει το ίδιο ακριβώς.

Επιπλέον, η χρήση του CSMA/CD ως πρωτόκολλου δικτύου ενέχει και την ύπαρξη συγκρούσεων. Μια κοινή περιοχή δικτύου, αυτή που αποτελείται από όλα τα καλώδια και τους επαναλήπτες, αποτελεί ένα ενιαίο μέσο (δίκτυο) για τη χρήση του οποίου ανταγωνίζονται (*contention-based access*) όλοι οι υπολογιστές που θέλουν να το χρησιμοποιήσουν ώστε να μεταφέρουν πληροφορία πάνω από το δίκτυο. Το πρωτόκολλο CSMA/CD αποτελεί ένα τρόπο διαχείρισης αυτού του κοινού μέσου, υπό το οποίο όταν ένας σταθμός θέλει να εκπέμψει ακολουθεί την διαδικασία:

α) ‘Ακούει’ το μέσο για να δει αν το χρησιμοποιεί κανείς (ανίχνευση φέροντος σήματος – *carrier sense* – το CS στα αρχικά του ονόματος του πρωτοκόλλου).
β) Αν δεν ανιχνεύσει χρήση αρχίζει να εκπέμπει και ταυτόχρονα να ‘ακούει’ πως ‘ακούγεται’ στο μέσο η εκπομπή του.
γ) Αν ανιχνεύσει σύγκρουση (ότι αυτό που ακούει δεν είναι αυτό που εκπέμπει) υποθέτει ότι συγκρούστηκε με άλλον που άρχισε να εκπέμπει (προφανώς πριν φτάσει σε αυτόν το σήμα του), παράγει ένα σήμα συμφόρησης (*jam*) και περιμένει ένα τυχαίο χρονικό διάστημα μέχρι να αρχίσει τη διαδικασία από την αρχή (*back-off*).

Αυτή η τοπική περιοχή δικτύου, εντός της οποίας ένας σταθμός που εκπέμπει μπορεί να συγκρουστεί με έναν άλλο ονομάζεται τομέας ή περιοχή συγκρούσεων (*collision domain*). Στην **Εικόνα 9.1** φαίνεται ένας τομέα συγκρούσεων σε ένα δίκτυο που χρησιμοποιεί *hubs*.



Εικόνα 9.1 Τομέας συγκρούσεων σε δίκτυο με *hubs*

Το πρόβλημα με το παραπάνω πρωτόκολλο είναι ότι όσο μεγαλύτερη είναι η τοπική περιοχή δικτύου και όσο μεγαλύτερη είναι η χρήση του δικτύου (άρα όσο περισσότεροι είναι οι σταθμοί και όσο μεγαλύτερη είναι η χρήση του από τις εφαρμογές), τόσο μεγαλύτερη είναι η πιθανότητα της σύγκρουσης. Τελικά σε μεγάλη χρήση δικτύου, οι σταθμοί αναλώνουν το μεγαλύτερο μέρος του χρόνου τους για να ανακάμπτουν από συγκρούσεις, αντί να εκπέμπουν χρήσιμα δεδομένα.

Για την αντιμετώπιση αυτών των προβλημάτων χρησιμοποιήθηκαν αρχικά οι γέφυρες (*bridges*). Οι γέφυρες είναι συσκευές 2^{ου} Επιπέδου, οι οποίες εισήχθησαν αρχικά για τη μετατροπή μεταξύ διαφορετικών πρωτοκόλλων 1^{ου} και 2^{ου} Επιπέδου (π.χ. μεταξύ Ethernet 802.3 και WiFi 802.11). Μια γέφυρα απομονώνει τις διεπαφές της σε διαφορετικούς τομείς συγκρούσεων (δεν περνά τις συγκρούσεις). Επιπλέον, πριν επανεκπέμψει ένα πλαίσιο ελέγχει το πεδίο ελέγχου πλαισίου (FCS, *Frame Check Sequence*) και μόνο εάν αυτό είναι έγκυρο επανεκπέμπει το πλαίσιο. η γέφυρα κάνει τα διαφορετικά φυσικά τμήματα δικτύου να φαίνονται ένα. Παράλληλα περνά τις ευρυεκπομπές, οι οποίες θέλουμε να περνούν. Δηλαδή μια γέφυρα δεν χωρίζει το δίκτυο σε διαφορετικές περιοχές ευρυεκπομπής (*broadcast domains*).

Τις λειτουργίες αυτές μια γέφυρα τις επιτελεί με λογισμικό, αποφασίζοντας για τη θύρα εξόδου βάσει των δεδομένων των κεφαλίδων 2^{ου} Επιπέδου, μέσα σε ένα πλαίσιο και βασικά τη διεύθυνση MAC παραλήπτη. Μια γέφυρα κατασκευάζει έναν πίνακα

διευθύνσεων MAC στον οποίο αντιστοιχεί θύρες εξόδου σε MAC διευθύνσεις υπολογιστών, όπως ο ακόλουθος:

MAC Address	**Θύρα Εξόδου**
AA:00:CC:00:00:01	1
BB:00:CC:00:00:02	2

Όταν ένα πλαίσιο εισέρχεται σε μια θύρα, η γέφυρα διαβάζει τη διεύθυνση MAC παραλήπτη (αφού εξετάσει το FCS) και βάσει του πίνακα MAC αποφασίζει ποια θα είναι η θύρα εξόδου. Αν βρει τη διεύθυνση παραλήπτη / προορισμού στον πίνακα MAC, αναπαράγει το πλαίσιο μόνο στη θύρα εξόδου που αναφέρει. Αν δεν τη βρει, 'πλημμυρίζει' (*flood*) το πλαίσιο σε όλες τις θύρες της. Αν η διεύθυνση παραλήπτη είναι αντιστοιχισμένη με την ίδια θύρα που μπήκε το πλαίσιο, τότε το πετάει (θεωρεί ότι το πλαίσιο έχει ήδη φτάσει στον παραλήπτη).

Ο πίνακας MAC κατασκευάζεται δυναμικά, διαβάζοντας τις διευθύνσεις MAC αποστολέα. Δηλαδή όταν μια γέφυρα 'δει' ένα πλαίσιο σε μια θύρα της, τη διεύθυνση αποστολέα την περνά στον πίνακα MAC, βάζοντας τιμή θύρας τη θύρα που μπήκε το πλαίσιο. Έτσι η γέφυρα 'μαθαίνει' και εμπλουτίζει (*populate*) τον πίνακα MAC με 'δυναμικές' εγγραφές (είναι δυνατός ο εμπλουτισμός του και με 'στατικές' εγγραφές που βάζει ο διαχειριστής της γέφυρας προγραμματιστικά). Οι εγγραφές αυτές έχουν χρόνο ζωής (*aging time*), με την παρέλευση του οποίου σβήνονται και ξαναμαθαίνονται. Η μόνη διεύθυνση που δεν μαθαίνεται (δεν τοποθετείται ποτέ στον πίνακα MAC), είναι η διεύθυνση ευρυεκπομπής FF:FF:FF:FF:FF:FF και πλαίσια με τέτοια διεύθυνση παραλήπτη αναπαράγονται εξ' ορισμού σε όλες τις θύρες (εκτός από αυτήν που ήρθαν).

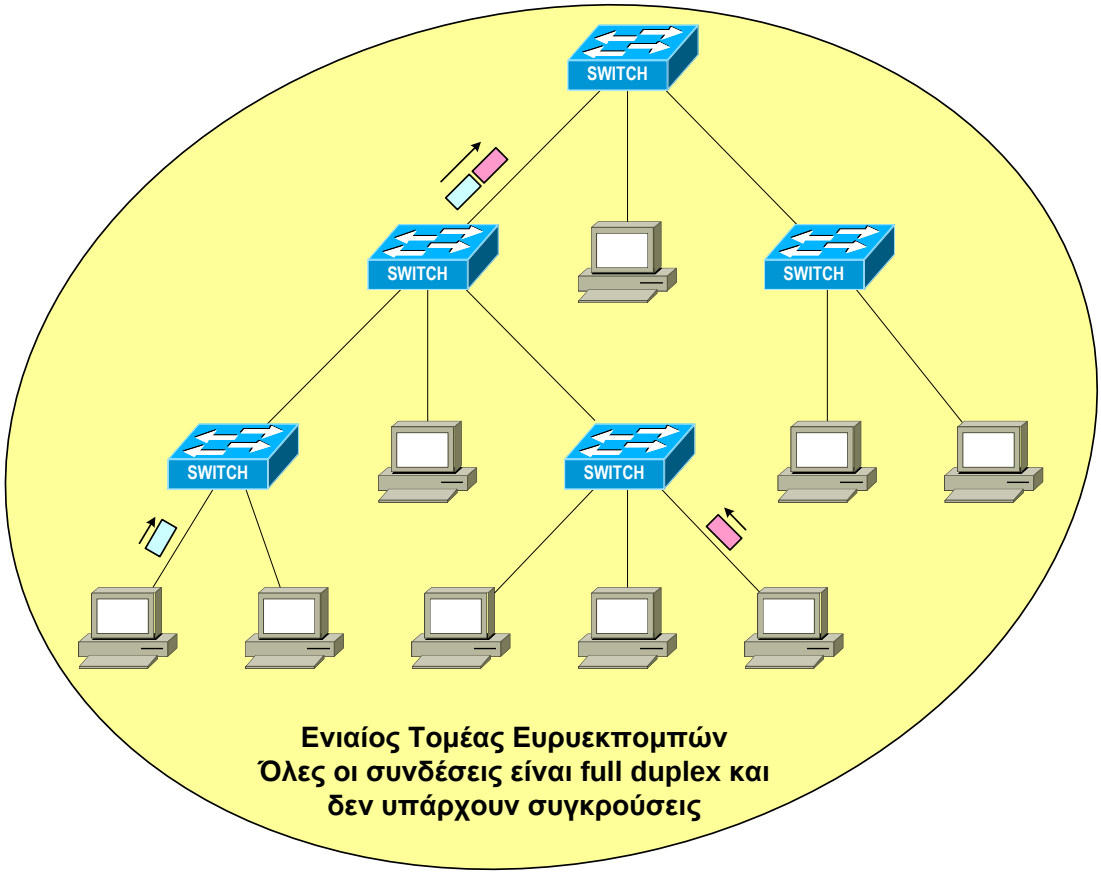
Αυτή η μεταγωγή λέγεται μεταγωγή 2^{ου} Επιπέδου και οι γέφυρες επιτελούν αυτή τη διαδικασία στον κεντρικό τους επεξεργαστή. Οι μεταγωγείς (*switches*) από την άλλη μεριά αποτελούν νεότερη τεχνολογία που έγινε δυνατή με τη μείωση του κόστους των ολοκληρωμένων κυκλωμάτων. Οι μεταγωγείς ήρθαν να ικανοποιήσουν την ανάγκη για μεγαλύτερη ταχύτητα μεταγωγής και μεγαλύτερη πυκνότητα διεπαφών (*port density*). Οι γέφυρες, αν και 'έξυπνες' συσκευές, δεν είναι κατάλληλες για τη δημιουργία μεγάλων δικτύων, ώστε να αντικαταστήσουν τα hubs. Οι γέφυρες δίνουν έμφαση στην αποτελεσματική μετατροπή μεταξύ πρωτοκόλλων 2^{ου} Επιπέδου και διαθέτουν τυπικά λίγες θύρες.

Ωστόσο, με την αύξηση του μεγέθους και της χρήσης των τοπικών δικτύων, χρειαζόταν μια συσκευή με όλα τα προτερήματα των γεφυρών, αλλά με τα ακόλουθα επιπρόσθετα χαρακτηριστικά:

α) Γρήγορη μεταγωγή όσο το δυνατό σε ταχύτητα μέσου, με ελάχιστη καθυστέρηση.
β) Μεγάλη πυκνότητα διεπαφών Ethernet, έτσι ώστε να υποστηρίζονται μεγάλα δίκτυα, όσον αφορά τον αριθμό των σταθμών εργασίας.
γ) Χωρισμό του δικτύου σε διαφορετικούς τομείς σύγκρουσης. Ή δυνατόν κάθε σταθμός θα ήταν συνδεμένος στη δική του 'αποκλειστική' θύρα ενός

μεταγωγέα. Αυτό θα είχε το αποτέλεσμα της κατάργησης των hubs και μαζί τους την κατάργηση του CSMA/CD σαν πρωτόκολλο διαχείρισης κοινού μέσου μετάδοσης, στο οποίο μια συσκευή ή μπορεί να εκπέμπει, ή μπορεί να λαμβάνει (λειτουργία *half-duplex*). Οι σταθμοί θα επικοινωνούν με τον μεταγωγέα σε λειτουργία *full duplex*, έχοντας δηλαδή τη δυνατότητα να εκπέμπουν και να λαμβάνουν ταυτόχρονα, χωρίς συγκρούσεις και με διπλασιασμό της ταχύτητας (π.χ. 10 Mbps προς και άλλα 10 Mbps από τη γέφυρα).

Η απάντηση στα παραπάνω ήταν οι μεταγωγείς (*switches*). Στην **Εικόνα 9.2** φαίνεται πώς διαμορφώνεται το δίκτυο της **Εικόνας 9.1** με μεταγωγείς.



Εικόνα 9.2 Δίκτυο με μεταγωγείς

9.2 Βασικές λειτουργίες μεταγωγέων

Για να επιτύχουν τα παραπάνω (και πολλά άλλα ακόμα), οι μεταγωγείς υλοποιούν τη μεταγωγή 2^{ου} Επιπέδου στο υλικό (*in hardware*) και ο επεξεργαστής τους κάνει απλώς τη διαχείριση. Ο δε πίνακας MAC, δεν υλοποιείται σε απλή RAM (*Random Access Memory* – μνήμη τυχαίας πρόσβασης), αλλά σε CAM (*Content Addressable Memory* – Μνήμη Προσβάσιμη μέσω Περιεχομένου), η οποία λειτουργεί σαν βάση δεδομένων, με τις διευθύνσεις MAC να παίζουν το ρόλο του *Index*.

Σαν αποτέλεσμα παρέχουν ταχύτητες μεταγωγής πολύ μεγαλύτερες από αυτές των γεφυρών (και των περισσοτέρων άλλων δικτυακών συσκευών), της τάξης των εκατομμυρίων (έως και εκατοντάδων εκατομμυρίων) πλαισίων το δευτερόλεπτο.

Οι μεταγωγείς παρέχουν τρεις βασικές μεθόδους μεταγωγής:

α) Αποθήκευση-και-προώθηση (*store-and-forward*). Αποτελεί τη βασική μορφή μεταγωγής και αυτή που υλοποιούν οι περισσότεροι φθηνοί και μη διαχειρίσιμοι (που δεν παραμετροποιούνται) μεταγωγείς. Με αυτήν ο μεταγωγέας, πρώτα διαβάζει ολόκληρο το εισερχόμενο πλαίσιο, μετά ελέγχει την εγκυρότητα του πεδίου ελέγχου (FCS) και αν το πλαίσιο είναι ακέραιο αποφασίζει (με αναφορά στον πίνακα MAC) για τη θύρα εξόδου και το εκπέμπει. Η μέθοδος αυτή έχει το καλό ότι δεν επανεκπέμπονται κατεστραμμένα πλαίσια. Έχει όμως το μειονέκτημα ότι, επειδή ο μεταγωγέας πρέπει να διαβάσει πρώτα όλο το πλαίσιο και να υπολογίσει πάλι το FCS, η μεταγωγή εισάγει καθυστέρηση (*latency*) στη μετάδοση των πλαισίων.

β) Άμεση (*cut-through*). Παρέχεται από διαχειρίσιμους μεταγωγείς (που παραμετροποιούνται). Σε αυτή τη μέθοδο, μόλις ο μεταγωγέας διαβάσει τη διεύθυνση MAC του παραλήπτη από την κεφαλίδα του Ethernet (που είναι στην αρχή του πλαισίου, αμέσως μετά το πεδίο του *preamble*), αποφασίζει αμέσως για τη θύρα εξόδου (με αναφορά στον πίνακα MAC) και αρχίζει να το εκπέμπει, ενόσω συνεχίζει τη λήψη του. Η μέθοδος αυτή έχει το καλό ότι δεν εισάγει καθυστέρηση στη μεταγωγή. Όμως δεν διασφαλίζει τη μη εκπομπή κατεστραμμένων πλαισίων, αφού ο μεταγωγέας δεν έχει διαβάσει (και ελέγξει) το FCS του πλαισίου, πριν ξεκινήσει την επανεκπομπή του. Οι περισσότεροι κατασκευαστές μεταγωγέων αντιμετωπίζουν αυτό το πρόβλημα ελέγχοντας εκ των υστέρων το FCS και ενημερώνοντας ένα μετρητή της θύρας για κάθε κατεστραμμένο πλαίσιο που λαμβάνουν. Μόλις ο αριθμός περάσει ένα όριο, αλλάζουν τη μέθοδο στην αποθήκευση-και-προώθηση.

γ) Ελεύθερη θραυσμάτων (*fragment-free*). Ενώ στη μέθοδο άμεσης μεταγωγής ο μεταγωγέας διαβάζει μέχρι το πεδίο διεύθυνσης αποστολέα πριν ξεκινήσει να το μετάγει, σε αυτή τη μέθοδο περιμένει να λάβει τα πρώτα 64 bytes, το ελάχιστο νόμιμο μέγεθος των πλαισίων Ethernet. Με αυτό τον τρόπο κόβονται τα ‘κολοβά’ πλαίσια (*runts*), σύνηθες αποτέλεσμα προβληματικών συνδέσεων με συγκρούσεις. Η μέθοδος αυτή δεν προστατεύει από κατεστραμμένα πλαίσια και έτσι οι κατασκευαστές μεταγωγέων υλοποιούν μεθόδους όπως αυτή της προηγούμενης παραγράφου.

Επιπλέον οι μεταγωγείς μπορούν τυπικά να διαχειριστούν πολλαπλές ταχύτητες (πρότυπα) Ethernet στις θύρες τους. Έτσι οι ηλεκτρικές θύρες (RJ-45) μπορεί να τρέχουν στα 10 Mbps (10BaseT), στα 100 Mbps (100BaseT), στα 1000 Mbps (1000BaseT), ή ακόμα και στα 10 Gbps (10GbaseT). Επιπλέον οι θύρες μπορεί να αλλάζουν δυναμικά την πολικότητά τους (Auto-MDIX), έτσι ώστε να υποστηρίζουν είτε μεταγωγείς, είτε τελικούς σταθμούς.

Οι θύρες των μεταγωγέων είναι είτε ηλεκτρικές με βύσματα RJ-45, οι οποίες δέχονται καλώδια συνεστραμμένων ζευγών (U/UTP, U/FTP, F/UTP S/FTP και SF/UTP) κατηγοριών Cat5 έως Cat6a, είτε οπτικές, οι οποίες με βύσματα LC ή SC δέχονται καλώδια οπτικών ινών, μονότροπων (*single mode*) ή πολύτροπων (*multi mode*). Πολλοί μεταγωγείς ταχύτητας από 1 Gbps και πάνω υποστηρίζουν μεταβλητές συνδέσεις τύπου είτε GBIC είτε SFP, οι οποίες με το κατάλληλο δομοστοιχείο (*module*), μπορούν να υποστηρίξουν τόσο ηλεκτρικά καλώδια, όσο και οπτικές ίνες.

Όπως αναφέρθηκε σε προηγούμενη παράγραφο, ένας μεταγωγέας μπορεί να υλοποιήσει επικοινωνία *full duplex* με άλλους μεταγωγείς, δρομολογητές, σταθμούς και συσκευές. Η *full duplex* επικοινωνία αφιερώνει ξεχωριστά κανάλια για την εκπομπή και τη λήψη, έτσι ώστε να είναι δυνατές και οι δύο ταυτόχρονα, διπλασιάζοντας τη συνολική ταχύτητα και καταργώντας τον αλγόριθμο διαχείρισης κοινού μέσου CSMA/CD και τις συγκρούσεις. Η μόνη περίπτωση για να μην ισχύει αυτό είναι αν σε ένα μεταγωγέα συνδεθεί ένα *hub* (εκτός από την περίπτωση προβλημάτων).

Τυπικά μία ηλεκτρική θύρα ενός μεταγωγέα που ανιχνεύει φέρον σήμα – σύνδεση με άλλη συσκευή, εκκινεί διαδικασία διαπραγμάτευσης (*negotiation*) έτσι ώστε να επιτευχθεί το καλύτερο επίπεδο επικοινωνίας που υποστηρίζεται και από τις δύο συσκευές η συσκευή που είναι συνδεδεμένη πάνω της, όσον αφορά το duplex (*full* ή *half*), την ταχύτητα και την πολικότητα.

Στην αγορά, οι μεταγωγείς χωρίζονται σε κατηγορίες, ανάλογα με το αν είναι διαχειριζόμενοι (*managed*) ή όχι και με το αν είναι σταθερής ή μεταβλητής διαμόρφωσης (*fixed / modular configuration*).

α) Μη διαχειριζόμενοι σταθερής διαμόρφωσης. Είναι οι πιο φθηνοί. Έχουν συγκεκριμένες διεπαφές (τυπικά 4 – 24 ηλεκτρικές θύρες RJ-45 ταχύτητας 10 – 1000 Mbps) και δεν μπορούν να παραμετροποιηθούν. Έχουν ρυθμίσεις που διασφαλίζουν την πιο σταθερή και αξιόπιστη λειτουργία. Στην **Εικόνα 9.3** φαίνονται τέτοιοι μεταγωγείς.

Εικόνα 9.3 Οικογένεια Cisco Small Business 100

β) Διαχειριζόμενοι σταθερής διαμόρφωσης. Έχουν από χαμηλό έως μεσαίο κόστος, ανάλογα με τις δυνατότητές τους. Μπορούν να παραμετροποιηθούν και υποστηρίζουν ευρεία γκάμα δυνατοτήτων, από απλές μέχρι ιδιαίτερα πολύπλοκες. Έχουν συγκεκριμένο αριθμό διεπαφών, οι περισσότερες

ηλεκτρικές (τυπικά 4 – 40 θύρες RJ-45), λίγες (2 – 4) μεταβλητές, είτε GBIC, είτε SFP. Στην **Εικόνα 9.4** φαίνονται τέτοιοι μεταγωγείς. Οι μεταγωγείς αυτοί χρησιμοποιούνται σε όλα τα επίπεδα δικτύου (βλ. ενότητα «Σύγχρονες Αρχιτεκτονικές Δικτύου»).

Εικόνα 9.4 Οικογένεια Cisco Catalyst 2960

γ) Διαχειριζόμενοι σταθερής διαμόρφωσης στοιβάσιμοι (*stackable*). Σε σύγκριση με τους προηγούμενους, έχουν το επιπλέον προσόν ότι μπορεί να συνδεθεί το οπισθεπίπεδό τους (*backplane*), έτσι ώστε πολλοί μαζί να αποτελούν μία μονάδα. Με αυτό τον τρόπο είναι επεκτάσιμοι, χωρίς να αυξάνεται το διαχειριστικό φορτίο. Βέβαια αυτό αυξάνει αρκετά το κόστος μονάδας, εξακολουθούν όμως να είναι πιο φθηνοί από την επόμενη κατηγορία. Στην **Εικόνα 9.5** φαίνονται τέτοιοι μεταγωγείς.

Εικόνα 9.5 Οικογένεια Cisco Catalyst 3750

δ) Διαχειριζόμενοι μεταβλητής διαμόρφωσης. Έχουν τυπικά υψηλό κόστος. Μπορούν να παραμετροποιηθούν και υποστηρίζουν ευρεία γκάμα δυνατοτήτων, από απλές μέχρι ιδιαίτερα πολύπλοκες. Διαθέτουν ένα σασί-περίβλημα, το οποίο δέχεται τροφοδοτικά ισχύος, κεντρικούς επεξεργαστές και διεπαφές διαφόρων τύπων μέσω μεγάλων υποδοχών καρτών γραμμής (*line cards*), συχνά με δυνατότητες πλεονασμού (εφεδρικά υποσυστήματα για βλαβοαντοχή), όπως διπλά τροφοδοτικά και επεξεργαστές. Κάθε κάρτα μπορεί να έχει διεπαφές που αντιστοιχούν σε ένα μεταγωγέα σταθερής διαμόρφωση (6 – 48, ηλεκτρικές ή οπτικές). Οι μεταγωγείς αυτοί έχουν τις μεγαλύτερες δυνατότητες και τη μεγαλύτερη πυκνότητα διεπαφών. Χρησιμοποιούνται τυπικά στο επίπεδο διανομής, πυρήνα ή πρόσβασης εξυπηρετητών (βλ.

ενότητα ‘Σύγχρονες Αρχιτεκτονικές Δικτύου’). Στην **Εικόνα 9.6** φαίνονται τέτοιοι μεταγωγείς.

Εικόνα 9.6 Οικογένεια Cisco Catalyst 6500

Οι διαφορές ενός *hub*, μιας γέφυρας και ενός μεταγωγέα συνοψίζονται στον ακόλουθο πίνακα:

Λειτουργία	**HUB**	**ΓΕΦΥΡΑ**	**ΜΕΤΑΓΩΓΕΑΣ**
Λειτουργεί στο επίπεδο του μοντέλου OSI	1	2	2
Δυνατότητα διαχείρισης	Συνήθως όχι	ΝΑΙ	ΝΑΙ
Έμφαση στην	Ποιότητα σήματος	Αποτελεσματική μετατροπή πρωτοκόλλων	Ταχύτητα μεταγωγής
Πυκνότητα διεπαφών	Μικρή ιδίου τύπου, τυπικά ~4-16	Μικρή διαφορετικών τύπων, τυπικά 2-4	Μεγάλη ιδίου τύπου, τυπικά 5-48
Συνδέσεις καλωδίων	Ηλεκτρικά	Ηλεκτρικά και οπτικά	Ηλεκτρικά και οπτικά
Μεταβλητές συνδέσεις ηλεκτρικές/οπτικές	ΟΧΙ	Συνήθως όχι	ΝΑΙ GBIC ή SFP
Δομοστοιχειωτός	ΟΧΙ	Συνήθως όχι	ΝΑΙ
Ταχύτητες (Mbps)	10	10-1000	10-10000
Duplex	Half	Half/Full	Half/Full
Διαπραγμάτευση συνδέσεων	ΟΧΙ	ΝΑΙ	ΝΑΙ
Auto-MDIX	ΟΧΙ	ΝΑΙ	ΝΑΙ
Εκμάθηση διευθύνσεων MAC δικτύου	ΟΧΙ	ΝΑΙ, πίνακας MAC σε RAM	ΝΑΙ, πίνακας MAC σε CAM

Επίπεδο OSI μεταγωγής	ΟΧΙ	2	2 - 3
Τρόποι μεταγωγής 2ου επιπέδου	Απλή επανάληψη	Store and forward	Store and forward, cut through, fragment free
Χωρισμός δικτύου σε τομείς σύγκρουσης	ΟΧΙ	ΝΑΙ	ΝΑΙ
Χωρισμός δικτύου σε τομείς ευρυεκπομπής	ΟΧΙ	ΟΧΙ	ΟΧΙ

9.3 Εκκίνηση Μεταγωγέα

Σε αντίθεση με ένα συνηθισμένο υπολογιστή, οι μεταγωγείς δε διαθέτουν πληκτρολόγιο και οθόνη για να παρέχουν κάποια σύνδεση προκειμένου να παραμετροποιηθούν ή/και να επισκοπηθεί η κατάστασή τους. Αντίθετα οι διαχειρίσιμοι μεταγωγείς επιτρέπουν τη ρύθμισή τους είτε μέσω τοπικής ή απομακρυσμένης κονσόλας, είτε μέσω ιστοσελίδας (*web-based*). Αν όμως δεν είναι διαχειρίσιμοι δεν παρέχουν καμία δυνατότητα για ρύθμιση.

Για την πρόσβαση σε σειριακή κονσόλα, όπως και στους δρομολογητές συνδέουμε ένα σειριακό καλώδιο (στη Cisco είναι γαλάζιο *rollover* καλώδιο από σειριακό DB-9 σε σειριακό RJ-45) από τη σειριακή θύρα ενός υπολογιστή (αν δεν υπάρχει σειριακή θύρα θα χρειαστούμε ένα μετατροπέα από USB σε σειριακή) στη θύρα κονσόλας του μεταγωγέα (στη Cisco έχει τη μορφή υποδοχής RJ-45 όπως το Ethernet, αλλά είναι μαρκαρισμένη με γαλάζιο χρώμα). Στη συνέχεια, εκκινούμε ένα πρόγραμμα τερματικού (*terminal emulation*) όπως είναι το Hyperterminal, το TeraTerm, ή το PuTTy, συνδεόμαστε στη σειριακή θύρα με ρυθμίσεις που αναφέρει ο κατασκευαστής (τυπικά 9600,N,8,1) και βλέπουμε τη διεπαφή εντολών γραμμής (*Command Line Interface* – CLI) του μεταγωγέα.

Αν αυτό το κάνουμε πριν τον ανοίξουμε βλέπουμε τη διαδικασία εκκίνησης. Πραγματοποιείται έλεγχος της μνήμης FLASH, εντοπίζεται το λειτουργικό σύστημα, αποσυμπιέζεται και φορτώνεται στη μνήμη του μεταγωγέα. Αναλυτικά η διαδικασία για μεταγωγείς Cisco έχει ως εξής:

1. Αρχικά εκτελείται ο έλεγχος εκκίνησης (POST, *Power-On Self Test*), ο οποίος ελέγχει ότι όλα τα μέρη του μεταγωγέα είναι λειτουργικά. Το POST είναι ένα μικροπρόγραμμα, που είναι αποθηκευμένο στη ROM.
2. Στη συνέχεια ο μεταγωγέας εκτελεί το πρόγραμμα bootstrap, επίσης ένα μικροπρόγραμμα αποθηκευμένο στη ROM, που ξεκινά τον μεταγωγέα και προσπαθεί να εντοπίσει το IOS στην εσωτερική μνήμη FLASH. Αν το bootstrap δεν εντοπίσει έγκυρο λειτουργικό σύστημα IOS στη FLASH, τότε θα προσπαθήσει να φορτώσει το IOS είτε από έναν TFTP εξυπηρετητή, είτε από τη ROM. Σε περίπτωση που το IOS δεν βρεθεί ούτε στη FLASH, ούτε από έναν TFTP εξυπηρετητή, τότε το bootstrap φορτώνει το Rx-boot image από τη ROM (θα πρέπει να σημειωθεί ότι το Rx -boot image είναι ένα είδος ελαττωμένου λειτουργικού συστήματος). Όταν συμβεί αυτό τότε εμφανίζεται

στην οθόνη το prompt `(boot)>`, όπου μπορούμε να εισάγουμε εντολές ελέγχου της διαδικασίας εκκίνησης, όπως για παράδειγμα να προσδιορίσουμε την τοποθεσία από όπου μπορεί να φορτωθεί ένα λειτουργικό σύστημα IOS.

3. **Φόρτωση του λειτουργικού συστήματος.** Το λειτουργικό σύστημα φορτώνεται στη RAM, αποσυμπιέζεται και εκτελείται.
4. **Φορτώνεται το startup configuration**. Αφού εκτελεστεί το λειτουργικό σύστημα, προσπαθεί να εντοπίσει τη διαμόρφωση εκκίνησης (*startup configuration*) στην NVRAM και να το φορτώσει στη RAM, μετασχηματίζοντας το έτσι στη λεγόμενη διαμόρφωση λειτουργίας (*running configuration*).

Σε αυτό το σημείο ολοκληρώνεται η διαδικασία εκκίνησης και ο μεταγωγέας είναι πλήρως λειτουργικός.

9.4 Βασική ρύθμιση μεταγωγέα

Προκειμένου να μπορούμε να διαχειριστούμε ένα μεταγωγέα 2^{ου} Επιπέδου απομακρυσμένα θα πρέπει να του αναθέσουμε διεύθυνση IP. Για παράδειγμα, για να μπορέσουμε να συνδεθούμε μέσω telnet ή SSH, μέσω ενός Web browser, ή ενός σταθμού για διαχείριση μέσω του πρωτοκόλλου SNMP. Στους μεταγωγείς της Cisco αυτό γίνεται με ανάθεση διεύθυνσης IP στο προκαθορισμένο VLAN vlan1 (για περισσότερες πληροφορίες για τα VLAN, βλ. την αντίστοιχη ενότητα).

Για να αναθέσουμε για παράδειγμα τη διεύθυνση 192.168.1.2/24, οι εντολές που δίνουμε σε Cisco CLI είναι οι ακόλουθες:

```
Switch(config)#interface vlan 1
Switch(config-vlan)#ip address 192.168.1.2 255.255.255.0
Switch(config-vlan)#no shutdown
Switch(config-vlan)#exit
```

Στη συνέχεια θα δείξουμε σειρά βασικών ρυθμίσεων, μέσω ενός συνολικού παραδείγματος σε Cisco CLI.

Παράδειγμα ρύθμισης μεταγωγέα

```
Switch(config)#hostname Central
Central(config)#line console 0
Central(config-line)# password linepass
Central(config-line)#login
Central(config-line)#exec-timeout 5 0
Central(config-line)#exit
Central(config)#line vty 0 15
Central(config-line)#password linepass
Central(config-line)#login
Central(config-line)#exec-timeout 5 0
```

```
Central(config-line)#exit
Central(config)#enable secret secpass
Central(config)#service password-encryption
Central(config)#banner motd $Unauthorized use will be prosecuted$
Central(config)#interface vlan 1
Central(config-if)#ip address 10.1.1.2 255.255.255.0
Central(config-if)#no shutdown

%LINK-5-CHANGED: Interface Vlan1, changed state to up

Central(config-if)#exit
Central(config)#ip default-gateway 10.1.1.1
Central(config)#clock timezone EET 2
Central(config)#clock summer-time EEST recurring last Sun Mar 3:00 last
sun Oct 4:00
Central(config)#service timestamps debug datetime localtime show-
timezone
Central(config)#service timestamps log datetime localtime show-timezone
Central(config)#logging buffered 16384 notifications
Central(config)#logging rate-limit console 20
Central(config)#end

%SYS-5-CONFIG_I: Configured from console by console

Central#clock set 12:00:00 24 Nov 2013
Central#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Central#
```

Στην παραπάνω διαμόρφωση, παραμετροποιήσαμε τα ακόλουθα:

α) Με την εντολή **`hostname`** αναθέσαμε στον μεταγωγέα το όνομα **`Central`**.

β) Με την εντολή **`password`** αναθέσαμε κωδικό **`linepass`** για σύνδεση μέσω της σειριακής κονσόλας (**`console 0`**) και μέσω δικτύου με telnet (**`vty 0 15`**).

γ) Αναθέσαμε κωδικό **`secpass`** για τη διαμόρφωση προνομίων (privileged mode) με την εντολή **`enable secret`**.

δ) Ενεργοποιήσαμε υπηρεσία για την κρυπτογράφηση των κωδικών εντός του running-configuration (**`service password-encryption`**).

ε) Ενεργοποιήσαμε την εμφάνιση μηνύματος καλωσορίσματος προς όποιον συνδέεται στο μεταγωγέα (**`login banner motd`**).

στ) Αναθέσαμε IP διεύθυνση και default gateway, ώστε να μπορούμε να συνδεθούμε μέσω του δικτύου απομακρυσμένα.

ζ) Ρυθμίσαμε την τοπική ώρα ζώνης με όνομα EET (Eastern European Time) και διαφορά ώρας από UTC +2 (**`clock timezone EET 2`**).

η) Ρυθμίσαμε την θερινή ώρα με όνομα EEST (Eastern European Summer Time) για να αλλάζει κάθε τελευταία Κυριακή του Μαρτίου στις 03:00 και του Οκτωβρίου στις 04:00 (**`clock summer-time EEST recurring last Sun Mar 3:00 last sun Oct 4:00`**).

θ) Ενεργοποιήσαμε υπηρεσία να εμφανίζει στις καταγραφές (logs) και στις αναφορές αποσφαλμάτωσης (debug) την ώρα, αντί για το χρόνο που είναι ανοικτός ο μεταγωγέας (**`service timestamps debug datetime localtime show-timezone`** και **`service timestamps log datetime localtime show-timezone)`**.

ι) Θέσαμε τον εσωτερικό χώρο καταγραφών στα 16 Kbytes (**`logging buffered 16384 notifications)`** και περιορίσαμε το ρυθμό αναφοράς των μηνυμάτων της κονσόλας σε 20/δευτερόλεπτο, για να την προστατέψουμε από υπερφόρτωση (**`logging rate-limit console 20`**).

ια) Ρυθμίσαμε το εσωτερικό ρολόι του μεταγωγέα στις 12:00:00 της 24 Νοεμβρίου 2013 (**`clock set 12:00:00 24 Nov 2013`**). Σημειώνεται ότι αυτό το ρολόι είναι λογισμικού και χάνεται όταν επανεκκινηθεί ο μεταγωγέας. Προτείνεται ο συγχρονισμός με δικτυακό ρολόι με το πρωτόκολλο NTP.

ιβ) Αποθηκεύσαμε όλες τις ρυθμίσεις στην NVRAM (**`copy running-config startup-config`**), ώστε να μην χαθούν με την επανεκκίνηση του μεταγωγέα.

Κατά την εισαγωγή των εντολών ενδέχεται να εμφανιστούν μηνύματα κατάστασης (*syslog messages*), όπως αυτά που φαίνονται παραπάνω.

9.5 Έλεγχος λειτουργίας μεταγωγέα

Για να δούμε την κατάσταση των θυρών ενός μεταγωγέα σε Cisco CLI δίνουμε την εντολή `show interfaces status`. Ένα παράδειγμα της εντολής φαίνεται στον παρακάτω πίνακα, όπου για κάθε θύρα φαίνεται η κατάστασή της (**`connected/not connected`**), το VLAN που ανήκει, η κατάστασή της όσον αφορά το *duplex* (**`a-full, a-half, full, half`**), η ταχύτητα που τρέχει και ο τύπος της θύρας. Το *duplex* και η ταχύτητα είναι είτε αποτέλεσμα διαπραγμάτευσης με τη συσκευή που είναι συνδεδεμένη (a-xxx, όπου xxx το ανώτερο κοινό χαρακτηριστικό που υποστηρίζουν οι δύο συσκευές), είτε ρυθμισμένα από το διαχειριστή της.

```
Switch#show interfaces status

Port     Name         Status       Vlan     Duplex     Speed     Type
Fa0/0                 connected    1        a-full     a-100     10/100BaseTX
Fa0/1                 notconnect   1        auto       auto      10/100BaseTX
Fa0/2                 notconnect   1        auto       auto      10/100BaseTX
Fa0/3                 notconnect   1        auto       auto      10/100BaseTX
Fa0/4                 connected    1        a-full     a-100     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                 connected    1        a-full     a-100     10/100BaseTX
```

Μία από τις κυριότερες λειτουργίες ενός μεταγωγέα είναι να μαθαίνει τις MAC διευθύνσεις των συσκευών που συνδέονται στις θύρες του. Αυτή η πληροφορία αποθηκεύεται σε έναν πίνακα διευθύνσεων, που είναι γνωστός είτε ως *mac address table* είτε ως *content addressable memory* (CAM). Ένα παράδειγμα σε Cisco CLI εμφανίζεται στον παρακάτω πίνακα:

```
Central>show mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0001.c94d.c485    DYNAMIC     Fa0/5
   1    0003.e49e.aa33    DYNAMIC     Fa0/10
   1    0004.9a2c.145e    DYNAMIC     Fa0/2
   1    0050.0fb8.a5e4    DYNAMIC     Fa0/4
   1    0060.5c28.892b    DYNAMIC     Fa0/3
   1    00d0.d3ca.23b5    STATIC      Fa0/1
```

Σε αυτό το παράδειγμα όλες οι διευθύνσεις έχουν εγγραφεί δυναμικά στη μνήμη του μεταγωγέα εκτός από την τελευταία που είναι στατική. Προκειμένου να καθαριστούν οι δυναμικές εγγραφές από το *mac address table* μπορούμε να εκτελέσουμε την εντολή **`#clear mac-address-table`** από το Privilege EXEC.

Σαν βασική λειτουργία, ο μεταγωγέας καταγράφει στον πίνακα διευθύνσεων MAC (*mac address table*) τις διευθύνσεις MAC των αποστολέων των πλαισίων που εισέρχονται στις θύρες του. Υπάρχουν όμως περιπτώσεις στις οποίες ο διαχειριστής μπορεί να επιθυμεί να περάσει κάποιες διευθύνσεις MAC με στατικό τρόπο, για παράδειγμα για λόγους ασφαλείας (βλ. παρακάτω `port-security`).

Σε αντίθεση με τις δυναμικές εγγραφές, οι στατικές εγγραφές δε 'γερνούν', δηλαδή δε διαγράφονται απ' τον πίνακα MAC μετά από κάποιο χρόνο (π.χ. σε έναν μεταγωγέα Cisco 2960 αυτός ο χρόνος είναι 300 sec). Οι στατικές εγγραφές δε διαγράφονται ακόμα και όταν πραγματοποιηθεί επανεκκίνηση του μεταγωγέα (εφόσον οι ρυθμίσεις έχουν αποθηκευθεί στην NVRAM). Θα πρέπει να δοθεί όμως ιδιαίτερη προσοχή στο γεγονός ότι αν δημιουργήσουμε μία στατική εγγραφή για μία συσκευή που είναι συνδεμένη σε μία θύρα του μεταγωγέα, τότε αν μετακινήσουμε τη συσκευή σε μια διαφορετική θύρα, η στατική εγγραφή δε θα επιτρέψει στο μεταγωγέα να μάθει τη διεύθυνση MAC της συσκευής στη νέα θύρα που τη συνδέσαμε.

Προκειμένου να δημιουργήσουμε μια στατική εγγραφή στον πίνακα MAC ενός μεταγωγέα χρησιμοποιούμε την εντολή:

```
Switch(config)#mac-address-table static 00d0.d3ca.23b5 vlan 1 interface fa0/6
```

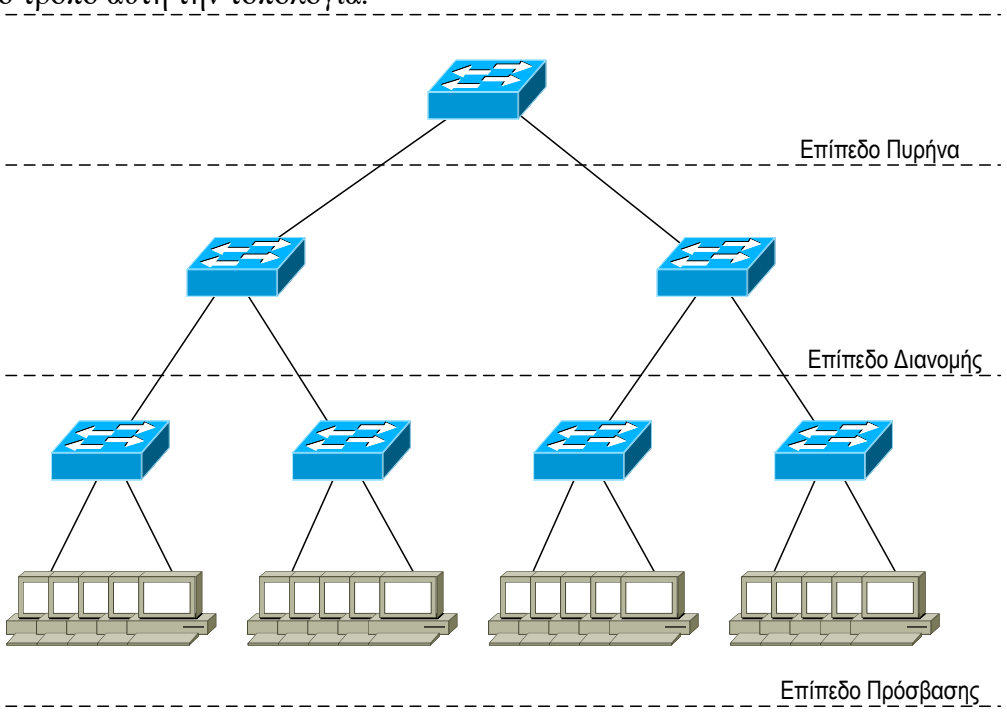
Σε αυτή την εντολή προσδιορίζουμε τη MAC διεύθυνση της συσκευής, π.χ. **00d0.d3ca.23b5**, το vlan στο οποίο ανήκει, π.χ. **vlan 1**, και τη θύρα στην οποία συνδέεται, π.χ. **fa0/6**. Στη συνέχεια χρησιμοποιούμε την εντολή **#show mac-address-table** για να δούμε τις νέες εγγραφές, ενώ για να αφαιρέσουμε μια στατική εγγραφή εισάγουμε την ίδια εντολή όπως παραπάνω ξεκινώντας με τη λέξη **no**.

10. Σύγχρονες αρχιτεκτονικές δικτύου

10.1 Ιεραρχικά Δίκτυα

Στις παραδοσιακές (*legacy*) αρχιτεκτονικές δικτύου ήταν κοινός τόπος η τοποθέτηση των δικτυακών συσκευών στο κέντρο του δικτύου και των χρηστών στην περιφέρεια. Ωστόσο, την τελευταία δεκαετία έχουν αλλάξει πολλά, όπως η εξέλιξη στις εφαρμογές (οι οποίες έγιναν πιο 'βαριές' για το δίκτυο), η δημιουργία γραφικών περιβαλλόντων εργασίας (*Graphical User Interfaces*, GUIs), η ευρεία διάδοση εφαρμογών πολυμέσων και κοινωνικής δικτύωσης και άλλα. Όλα αυτά έχουν αλλάξει σε πολύ μεγάλο βαθμό τη χρήση του δικτύου από τους σταθμούς εργασίας και τους εξυπηρετητές και έχουν αυξήσει την εξάρτηση από την υψηλή απόδοση αυτού δραματικά. Στην προσπάθεια λοιπόν για πιο 'πλούσια' και 'βαριά' δίκτυα, έχουν εξελιχθεί πιο μοντέρνες αρχιτεκτονικές δικτύου, οι οποίες είναι δομημένες στη βάση μιας ιεραρχίας.

Έτσι λοιπόν, το ιεραρχικό μοντέλο αρχιτεκτονικής δικτύου διακρίνει τρία βασικά επίπεδα: τον πυρήνα (*core*), τη διανομή (*distribution*) και την πρόσβαση (*access*), **Εικόνα 10.1**. Ένα σύγχρονο καλοσχεδιασμένο δίκτυο εφαρμόζει με τον ένα ή τον άλλο τρόπο αυτή την τοπολογία.



Εικόνα 10.1 Ιεραρχικό δίκτυο με διακριτά επίπεδα πρόσβασης, διανομής και πυρήνα

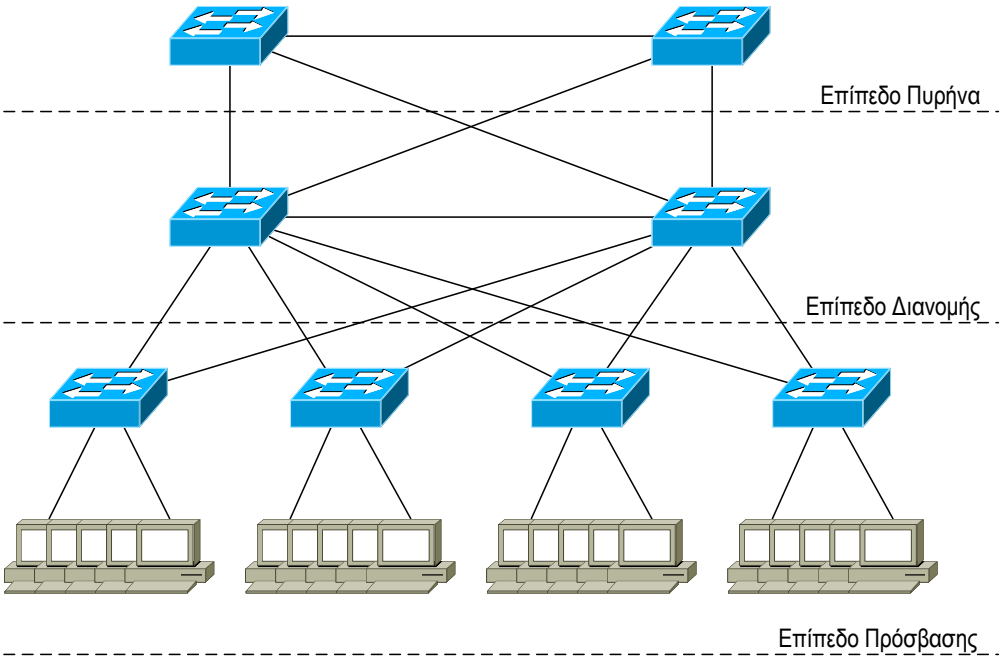
Τα πλεονεκτήματα της ιεραρχικής δομής είναι τα ακόλουθα:

- Κλιμακοθεσιμότητα (*scalability*). Λόγω του δομοστοιχειωτού (*modular*) χαρακτήρα τους, τα ιεραρχικά δίκτυα μεγαλώνουν εύκολα και μπορούν να υποστηρίξουν πιο απαιτητικές εφαρμογές. Για παράδειγμα, διαθέτοντας δύο

μεταγωγείς διανομής των εικοσιτεσσέρων θυρών, μπορεί κανείς να προσθέτει από έναν μέχρι και εικοσιτέσσερις μεταγωγείς πρόσβασης, ανάλογα με τις ανάγκες, χωρίς ουσιαστική αλλαγή στην τοπολογία του δικτύου. Επιπλέον, βασιζόμενα στη δομημένη καλωδίωση, τα ιεραρχικά δίκτυα παρέχουν πολύ καλή ευελιξία και αξιοπιστία.

- Πλεοναστικότητα (*redundancy*). Με την αύξηση του μεγέθους του δικτύου και της εξάρτησης των οργανισμών από αυτό για τη λειτουργία τους, η ανάγκη για τη διαθεσιμότητά του αυξάνει αντίστοιχα. Τα ιεραρχικά δίκτυα παρέχουν μεγάλες δυνατότητες πλεοναστικής διαμόρφωσης, με πολλαπλούς μεταγωγείς και διασυνδέσεις, τόσο στο επίπεδο διανομής, όσο και στο επίπεδο πυρήνα, **Εικόνα 10.2**. Κάθε μεταγωγέας πρόσβασης συνδέεται σε δύο τουλάχιστον μεταγωγείς διανομής και κάθε μεταγωγέας διανομής σε δύο τουλάχιστον μεταγωγείς πυρήνα. Έτσι, εάν ένας από αυτούς (ή μια σύνδεση προς αυτούς) αποτύχει, το δίκτυο συνεχίζει να δουλεύει.
- Απόδοση (*performance*). Σε ένα καλοσχεδιασμένο ιεραρχικό δίκτυο αποφεύγονται οι καθυστερήσεις και τα σημεία συμφόρησης (*bottlenecks*). Η μετάδοση από τους μεταγωγείς πρόσβασης στο επίπεδο διανομής γίνεται συνήθως με διασφάλιση επαρκούς αριθμού ανερχόμενων συνδέσεων (*uplinks*) και με συνάθροιση συνδέσεων (*link aggregation*). Οι μεταγωγείς διανομής και πυρήνα μεταγάγουν συνήθως σε ταχύτητα καλωδίου (*wire speed*). Οι μεταγωγείς διανομής δρομολογούν την κίνηση με βέλτιστο τρόπο και συχνά πάνω από πολλαπλές διαδρομές ταυτόχρονα. Το αποτέλεσμα είναι μεγάλη απόδοση, ακόμα και σε υψηλό φορτίο.
- Ασφάλεια (*security*). Η ασφάλεια βελτιώνεται και η διαχείρισή της γίνεται πιο εύκολη. Οι μεταγωγείς πρόσβασης μπορούν να διαμορφωθούν με διάφορες επιλογές ασφάλειας θυρών, έτσι ώστε να υπάρχει έλεγχος στο ποιες συσκευές και χρήστες μπορούν να συνδεθούν και σε ποιες περιοχές του δικτύου έχουν πρόσβαση. Στο επίπεδο διανομής μπορούν να εφαρμοστούν ακόμα πιο πολύπλοκες πολιτικές ασφαλείας, καθορίζοντας κανόνες διακριτικής πρόσβασης με βάση τα πρωτόκολλα δευτέρου έως και εβδόμου επιπέδου του δικτύου. Έτσι π.χ. το δίκτυο μπορεί να χωριστεί σε ζώνες, στις οποίες οι ροές από και προς αυτές ελέγχονται (π.χ. μόνο οι εξυπηρετητές εφαρμογής και οι διαχειριστές να έχουν πρόσβαση στους εξυπηρετητές βάσεων δεδομένων).
- Διαχειρισιμότητα (*manageability*). Η διαχείριση είναι σχετικά απλή σε ένα ιεραρχικό δίκτυο, καθώς κάθε επίπεδο επιτελεί συγκεκριμένες λειτουργίες που είναι ομοιόμορφες σε όλο το επίπεδο. Για παράδειγμα μια αλλαγή πολιτικής πρόσβασης στο δίκτυο εφαρμόζεται εύκολα και ενιαία σε ολόκληρο το επίπεδο πρόσβασης, χωρίς να επηρεάσει άλλο επίπεδο. Επίσης, η τοποθέτηση νέων μεταγωγέων σε ένα επίπεδο απλοποιείται λόγω της ομοιομορφίας που υπάρχει εντός του ιδίου επιπέδου και έτσι μπορεί να αντιγραφεί η διαμόρφωση. Επιπλέον, η ομοιομορφία βοηθά την αντιμετώπιση προβλημάτων και τη γρήγορη ανάκαμψη.
- Συντηρησιμότητα (*maintainability*). Επειδή τα ιεραρχικά δίκτυα έχουν δομοστοιχειωτή φύση και είναι πολύ κλιμακοθέσιμα, η συντήρησή τους είναι πιο εύκολη. Σε άλλες αρχιτεκτονικές η συντήρηση γίνεται προοδευτικά πολύ δύσκολη με την αύξηση του μεγέθους του δικτύου. Σε ορισμένες περιπτώσεις

μάλιστα υπάρχει όριο στο πόσο μπορεί να μεγαλώσει το δίκτυο προτού να καταστεί ασύμφορη, πρακτικά και οικονομικά, η συντήρησή του. Στο ιεραρχικό δίκτυο όμως, οι λειτουργίες των μεταγωγέων είναι συγκεκριμένες και καθορισμένες σε κάθε επίπεδο, κάνοντας την επιλογή του κατάλληλου μεταγωγέα πιο εύκολη. Επιπλέον, προκειμένου ένα δίκτυο πλήρους πλέγματος (*full mesh*) να έχει βέλτιστη απόδοση, πρέπει όλοι οι μεταγωγείς να είναι υψηλής απόδοσης. Αντίθετα, στο ιεραρχικό μοντέλο, ένας μεταγωγέας που θα προστεθεί πρέπει απλώς να έχει την απόδοση και τις λειτουργίες του επιπέδου που θα τοποθετηθεί. Και καθότι η πλειονότητα των μεταγωγέων βρίσκεται στο επίπεδο πρόσβασης, μπορούν αυτοί να είναι χαμηλού κόστους, μειώνοντας έτσι το συνολικό κόστος του δικτύου και βελτιώνοντας σημαντικά την συντηρησιμότητά του.



Εικόνα 10.2 Πλεοναστικότητα στο επίπεδο διανομής και πυρήνα

Επίπεδο Πρόσβασης

Το επίπεδο πρόσβασης (*access layer*), όπως δηλώνει το όνομά του, αποτελεί τον εξωτερικό 'φλοιό' του δικτύου, την περιφέρεια αυτού και παρέχει πρόσβαση σε όλες τις συσκευές 'πελάτες' του δικτύου, όπως σταθμούς εργασίας χρηστών, δικτυακούς εκτυπωτές, IP τηλέφωνα κτλ. Η πρόσβαση παρέχεται είτε από μεταγωγείς Ethernet, είτε από ασύρματα σημεία πρόσβασης (*access points*), τα γνωστά Wi-Fi.

Στο επίπεδο αυτό δίνεται σημασία (και γίνεται υλοποίηση) στα ακόλουθα:

- Μεγάλη πυκνότητα διεπαφών των (ενσύρματων) μεταγωγέων που συνδέουν τις συσκευές στο δίκτυο, έτσι ώστε να υποστηρίζονται όσο το δυνατόν περισσότερες συνδέσεις 'εισόδου' στο δίκτυο σε μικρό χώρο. Όταν πρόκειται για ασύρματα σημεία πρόσβασης, δίνεται σημασία στην επαρκή χωρική

κάλυψη του δικτύου και στη δυνατότητα εξυπηρέτησης της αναμενόμενης χωρικής πυκνότητας σταθμών.

- Μικρό κόστος ανά διεπαφή με δυνατότητα απλής μεταγωγής 2^{ου} Επιπέδου (*L2 Switching*).
- Μία διεπαφή ανά συσκευή, καθώς οι περισσότεροι σταθμοί εργασίας διαθέτουν μία μόνο.
- Μηχανισμοί ασφάλειας στην πρόσβαση, έτσι ώστε να μην μπορεί να συνδεθεί στο δίκτυο οποιαδήποτε συσκευή. Αυτό αποκτά ιδιαίτερη σημασία για την ασύρματη πρόσβαση, η οποία γίνεται πάνω από ένα ελεύθερο και μη περιορίσιμο μέσο (αέρας). Στην περίπτωση αυτή παρέχονται τυπικά τόσο μηχανισμοί επαλήθευσης ταυτότητας (*authentication*) σταθμού ή / και χρήστη, όσο και κρυπτογράφηση της επικοινωνίας.
- Μηχανισμοί διαχείρισης ταχύτητας επικοινωνίας και ουριοδότησης (*queuing*), έτσι ώστε να διασφαλίζεται η ορθή λειτουργία συσκευών πολυμέσων (IP τηλέφωνα, IP *videoconferencing* κλπ).
- Πρόβλεψη επαρκούς εύρους (ταχύτητας) πρόσβασης στο επόμενο επίπεδο (επίπεδο διανομής, βλ. παρακάτω), έτσι ώστε να εξυπηρετούνται όλες οι συσκευές που συνδέονται σε αυτό, όσον αφορά την επικοινωνία τους με τα υπόλοιπα μέρη του δικτύου και ιδίως το επίπεδο πρόσβασης εξυπηρετητών (βλ. παρακάτω), με ικανοποιητική ταχύτητα για τις εφαρμογές που τρέχουν.
- Πολλαπλές συνδέσεις με το επίπεδο διανομής, έτσι ώστε να διασφαλίζεται βλαβοαντοχή (*fault tolerance*), στην περίπτωση απώλειας σύνδεσης ή απώλειας συσκευής δικτύου του επιπέδου διανομής.
- Υποστήριξη συνάθροισης συνδέσεων στις ανερχόμενες συνδέσεις προς το επίπεδο διανομής, ώστε να αποφεύγονται σημεία συμφόρησης.
- Οι μεταγωγείς του επιπέδου πρόσβασης μπορεί να παρέχουν ρεύμα πάνω από το καλώδιο δικτύου (*Power over Ethernet*, PoE). Αυτό είναι ιδιαίτερα χρήσιμο για IP τηλέφωνα και δυσπρόσιτα access points, πρέπει όμως να υποστηρίζεται αυτό τόσο από τους μεταγωγείς, όσο και από τις συσκευές και αυξάνει αρκετά το κόστος. Συνήθεις συσκευές που μπορούν να τροφοδοτηθούν μέσω PoE είναι *access points*, IP τηλέφωνα, κάμερες και μεταγωγείς.

Στο επίπεδο πρόσβασης αντίθετα δε δίνεται σημασία στα ακόλουθα:

- Πολλαπλές συσκευές πρόσβασης (μεταγωγής). Η απώλεια ενός μεταγωγέα σε αυτό το επίπεδο δεν επηρεάζει μεγάλη περιοχή δικτύου, μόνο τους σταθμούς εργασίας που είναι συνδεδεμένα πάνω σε αυτόν. Στην περίπτωση που θέλουμε να αποφύγουμε ακόμα και αυτό το ενδεχόμενο, απλώς κάνουμε πρόβλεψη για την προμήθεια επιπλέον μεταγωγέων πρόσβασης, είτε σε αναμονή, είτε υπό μορφή στοίβας (*stack*).
- Πολλαπλές συνδέσεις από τις συσκευές προς το επίπεδο πρόσβασης. Έτσι κι αλλιώς οι συσκευές πρόσβασης (σταθμοί εργασίας κτλ), διαθέτουν τυπικά μόνο μία διεπαφή δικτύου.
- Πολυεπίπεδη μεταγωγή (*multilayer switching*) ή μεταγωγή τρίτου επιπέδου (*L3 switching*), βλ. παρακάτω.

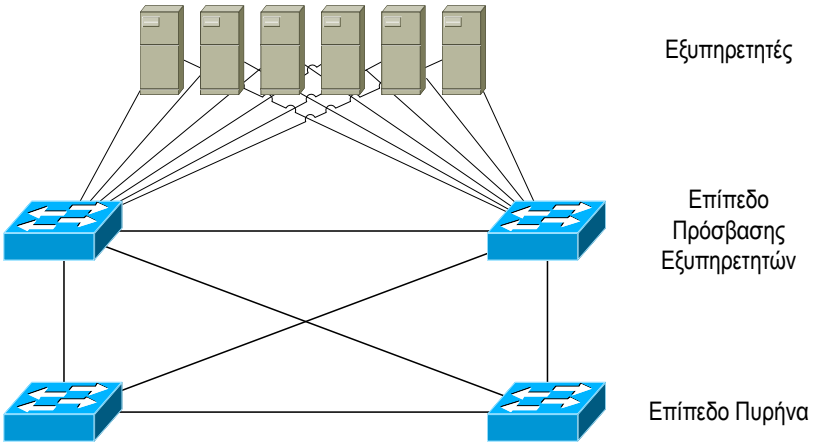
- Πρωτόκολλα δρομολόγησης. Έτσι κι αλλιώς οι συσκευές που βρίσκονται σε αυτό το επίπεδο (σταθμοί εργασίας κτλ) δεν τρέχουν πρωτόκολλα δρομολόγησης και δεν υπάρχουν πολλαπλοί δρόμοι από αυτές προς το δίκτυο (μονές συνδέσεις).
- Υψηλής απόδοσης μεταγωγείς και μεγάλος αριθμός ανερχόμενων συνδέσεων. Προκειμένου να μειωθεί το κόστος τους, οι μεταγωγείς του επιπέδου πρόσβασης δεν διαθέτουν οπισθεπίπεδο (*backplane*) υψηλής απόδοσης. Τυπικά γίνεται υπερκάλυψη της ταχύτητάς του από το άθροισμα της ταχύτητας των θυρών πρόσβασης, κάνοντας την υπόθεση ότι η πιθανότητα να κάνουν υψηλή χρήση του δικτύου ταυτόχρονα όλοι οι σταθμοί είναι μικρή. Κατά τον ίδιο τρόπο το άθροισμα της ταχύτητας των ανερχόμενων συνδέσεων είναι αρκετά μικρότερο από το άθροισμα της ταχύτητας των θυρών πρόσβασης (π.χ. 4 Gbps *uplinks* για 20 θύρες των 1 Gbps, αναλογία 1 προς 5).

Επίπεδο Πρόσβασης Εξυπηρετητών

Μια ειδική περίπτωση του επιπέδου πρόσβασης είναι το επίπεδο πρόσβασης εξυπηρετητών (*server access layer*). Διακρίνεται από το απλό επίπεδο πρόσβασης, τόσο για εκπαιδευτικούς λόγους, όσο (κυρίως) για λειτουργικούς λόγους. Το επίπεδο πρόσβασης εξυπηρετητών, επειδή προσφέρει πρόσβαση στο δίκτυο στους εξυπηρετητές (ή ανάποδα πρόσβαση προς τους εξυπηρετητές για το υπόλοιπο δίκτυο) έχει ιδιαίτερη σημασία, αν σκεφτεί κανείς ότι στα σύγχρονα δίκτυα και εφαρμογές το 90% της κίνησης (όσον αφορά τον όγκο κυρίως) κινείται από και προς αυτούς.

Για το επίπεδο πρόσβασης των εξυπηρετητών ισχύει ότι και για το απλό επίπεδο πρόσβασης, με τις ακόλουθες σημαντικές διαφορές:

Στο επίπεδο πρόσβασης εξυπηρετητών δίνεται έμφαση στην βλαβοαντοχή μέσω πλεοναστικότητας. Εκμεταλλευόμενοι το γεγονός ότι οι εξυπηρετητές διαθέτουν πολλαπλές διεπαφές δικτύου (τυπικά από 2 έως 8), κάθε εξυπηρετητής συνδέεται σε δύο τουλάχιστον μεταγωγείς, έτσι ώστε αν χαθεί ο ένας (ή κοπεί η σύνδεση προς τον εξυπηρετητή ή προς το ανώτερο επίπεδο) να μην χαθεί η σύνδεση του εξυπηρετητή με το δίκτυο. Συχνά οι μεταγωγείς εξυπηρετητών είναι σε μορφή στοίβας (*stack*), κάτι που αυξάνει εκτός από τη βλαβοαντοχή και τη διαχειρισιμότητά τους. Επιπλέον, οι μεταγωγείς πρόσβασης των εξυπηρετητών συνδέονται με πολλαπλές συνδέσεις με διαφορετικούς μεταγωγείς του ανώτερου επιπέδου (είτε διανομής εξυπηρετητών, είτε πυρήνα), για τους ίδιους λόγους, **Εικόνα 10.3**.

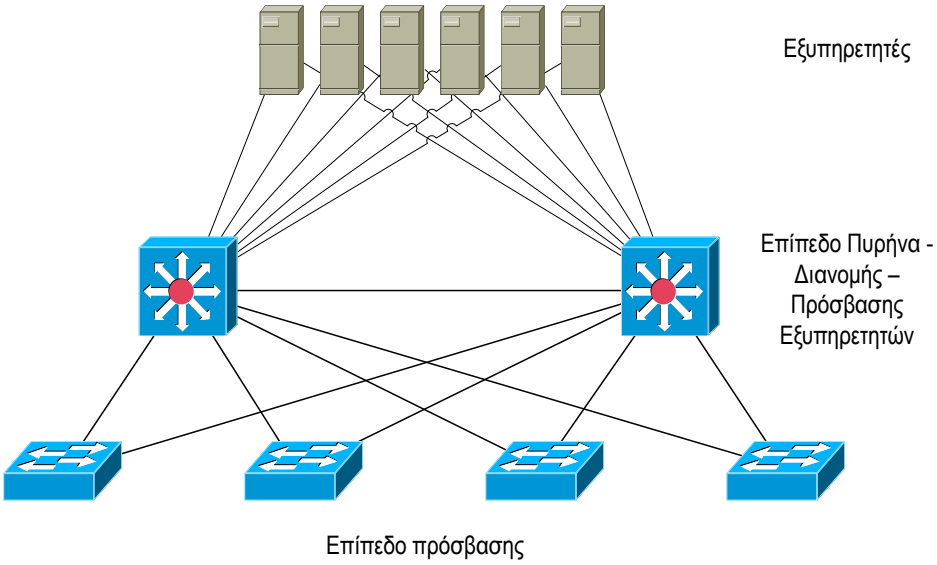


Εικόνα 10.3 Επίπεδο πρόσβασης εξυπηρετητών με διπλές συνδέσεις προς τους εξυπηρετητές και το ανώτερο επίπεδο

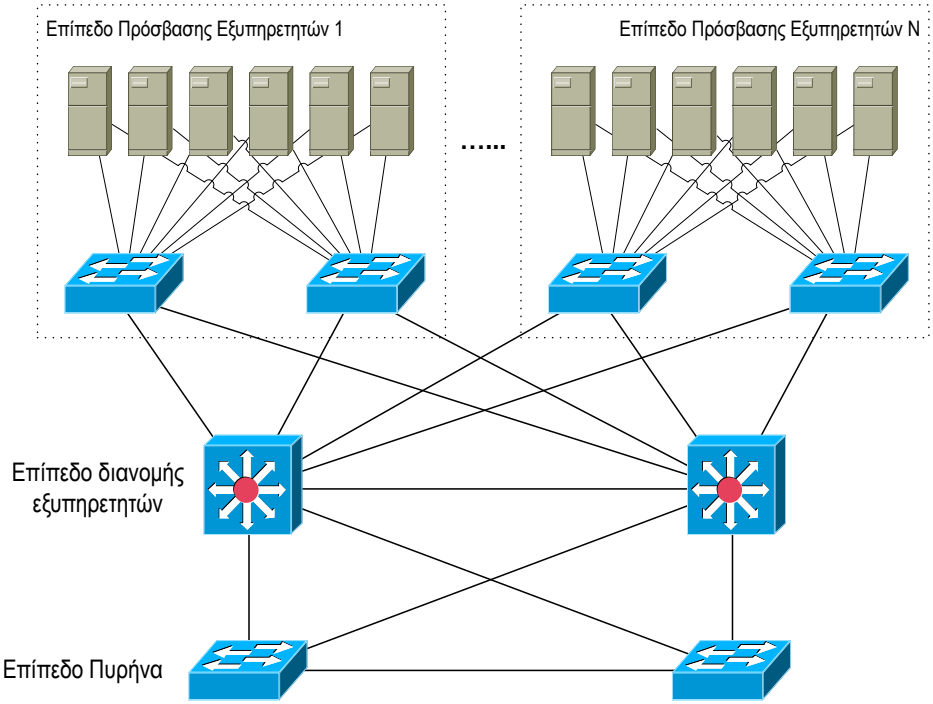
Οι μεταγωγείς πρόσβασης εξυπηρετητών είναι τυπικά μεγαλύτερης απόδοσης από τους απλούς μεταγωγείς πρόσβασης (έχουν μεγαλύτερη ταχύτητα οπισθεπίπεδου), ώστε να μπορούν να αντιμετωπίσουν την αυξημένη χρήση δικτύου των εξυπηρετητών. Επιπλέον, επειδή το μεγαλύτερο ποσοστό της κίνησης δικτύου κατευθύνεται από και προς τους εξυπηρετητές, η αναλογία κατερχόμενων (*downlinks*) και ανερχόμενων (*uplinks*) θυρών είναι καλύτερη για την αποφυγή συμφόρησης. Ιδιαίτερη σημασία αποκτούν τα παραπάνω όταν πρόκειται για μεταγωγείς κορυφής ικριώματος (*Top of Rack*, ToR).

Οι μεταγωγείς πρόσβασης εξυπηρετητών συνδέονται συχνά κατευθείαν στον πυρήνα του δικτύου για λόγους ταχύτητας. Σε σχετικά μικρά δίκτυα, μπορεί οι εξυπηρετητές να συνδέονται κατευθείαν πάνω στους μεταγωγείς πυρήνα, **Εικόνα 10.4**. Μόνο σε μεγάλα δίκτυα με μεγάλο αριθμό εξυπηρετητών και σε αυτά που χρησιμοποιούν μεταγωγείς TOR συναντώνται μεταγωγείς διανομής εξυπηρετητών, **Εικόνα 10.5**.

Σε πολλές περιπτώσεις οι μεταγωγείς πρόσβασης εξυπηρετητών είναι μεταγωγείς τρίτου επιπέδου (*L3 switches*), πολυεπίπεδοι μεταγωγείς (*multilayer switches*), μεταγωγείς σύγκλισης (*convergence switches*), κατανεμημένοι μεταγωγείς (*distributed switches*), ή ακόμα και μεταγωγείς εφαρμογής (*application switches*). Αυτά για να υποστηριχθούν επιπλέον ανάγκες που εισάγουν οι εξυπηρετητές, όπως ιδεατικοποίηση (*virtualization*), δίκτυα αποθήκευσης (*storage networks*), κατανομή φορτίου (*load balancing*), επιτάχυνση κρυπτογραφίας (*cryptographic accelerators*), επιτάχυνση εφαρμογών (*application accelerators*) κά. Αυτές οι δυνατότητες μπορεί να αυξήσουν το κόστος ενός μεταγωγέα κατακόρυφα, αλλά είναι αναγκαίες για την υποστήριξη μεσαίων και μεγάλων κέντρων μηχανογράφησης.



Εικόνα 10.4 Δίκτυο όπου οι εξυπηρετητές συνδέονται κατευθείαν στο επίπεδο πυρήνα

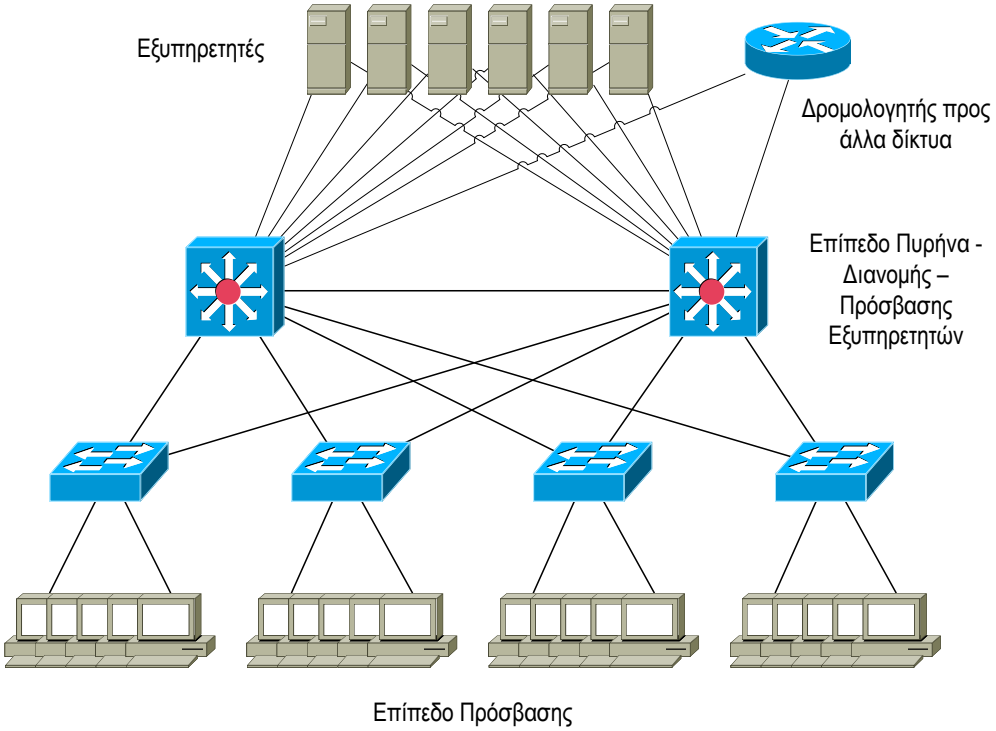


Εικόνα 10.5 Δίκτυο με επίπεδο πρόσβασης και διανομής εξυπηρετητών.

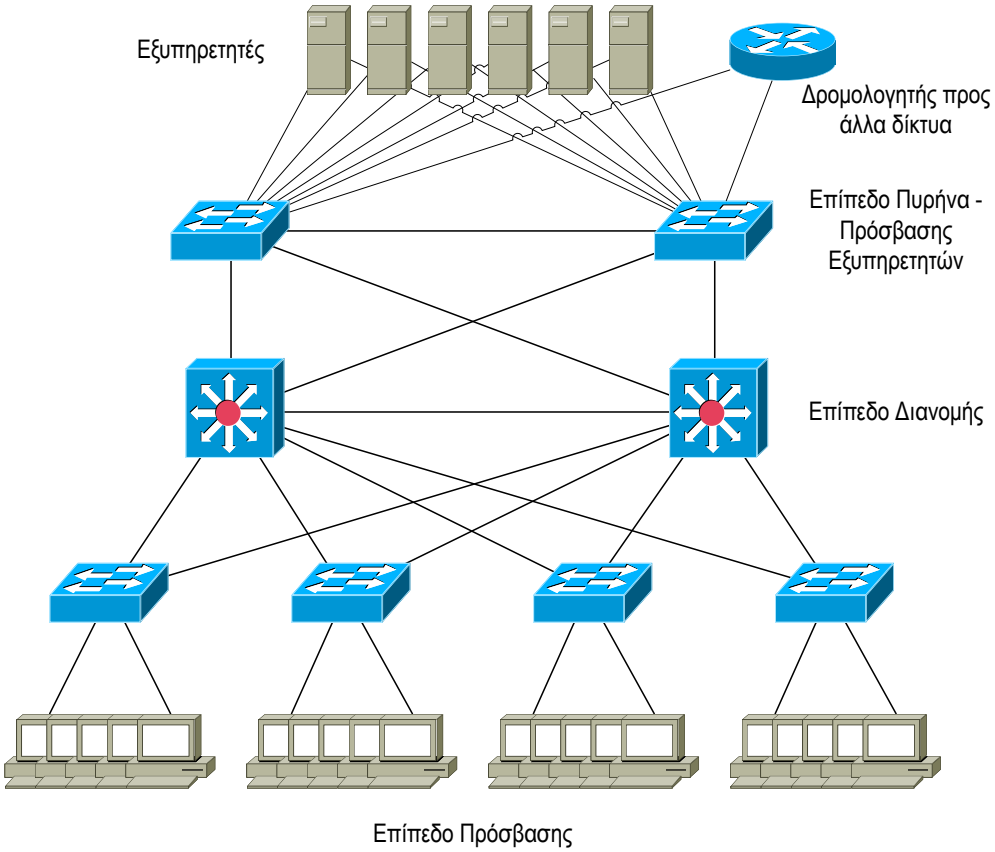
Επίπεδο Διανομής

Το επίπεδο διανομής (*distribution layer*) διασυνδέει τους μεταγωγείς πρόσβασης και, όπως λέει το όνομά του, διανέμει την πληροφορία με τον βέλτιστο τρόπο μεταξύ των διαφορετικών περιοχών πρόσβασης. Το βασικό πλεονέκτημα που παρέχει είναι η δυνατότητα ανάπτυξης του επιπέδου πρόσβασης σε μεγάλο μέγεθος, προσθέτοντας επιπλέον περιοχές πρόσβασης, **Εικόνα 10.7**. Σε μικρότερα δίκτυα που δεν χρειάζεται να έχουν μεγάλο μέγεθος διανομής, το επίπεδο αυτό μπορεί να ταυτίζεται με το

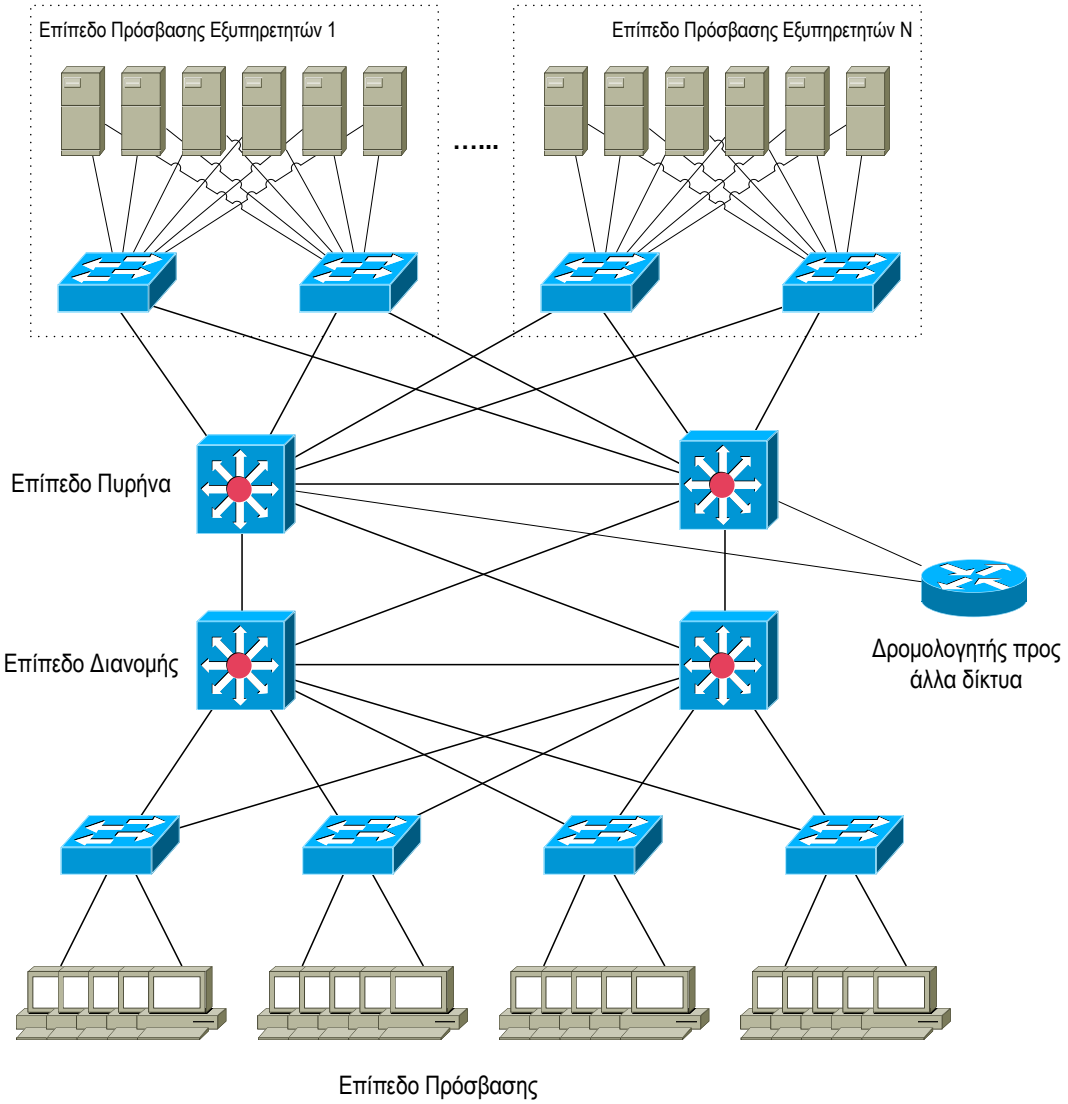
επίπεδο πυρήνα, **Εικόνα 10.6**. Σε ένα τέτοιο δίκτυο, αν οι εξυπηρετητές δεν είναι πολλοί και δεν χρειάζονται ξεχωριστό επίπεδο πρόσβασης εξυπηρετητών, μπορούν να συνδέονται κατευθείαν πάνω στο ενιαίο επίπεδο διανομής/πυρήνα, **Εικόνα 10.6**, διαφορετικά μπορεί να διαθέτουν ξεχωριστό επίπεδο πρόσβασης εξυπηρετητών, **Εικόνα 10.8**.



Εικόνα 10.6 Δίκτυο με ενοποιημένο επίπεδο πυρήνα, διανομής και πρόσβασης εξυπηρετητών (δύο επίπεδα)



Εικόνα 10.7 Δίκτυο με ξεχωριστά επίπεδα διανομής και πυρήνα, όπου οι εξυπηρετητές συνδέονται πάνω στον πυρήνα (τρία επίπεδα)



Εικόνα 10.8 Δίκτυο με ξεχωριστά επίπεδα διανομής, πυρήνα και πρόσβασης εξυπηρετητών (τέσσερα επίπεδα)

Εφόσον περιλαμβάνει μεταγωγείς τρίτου επιπέδου (*Layer 3 switches*), το επίπεδο διανομής μπορεί να επιτελεί και άλλες λειτουργίες όπως:

- Να χωρίζει το δίκτυο σε διαφορετικούς τομείς ευρυεκπομπών (*broadcast domains*).
- Να δρομολογεί μεταξύ διαφορετικών ιδεατών δικτύων (VLAN) και διαφορετικών (σαν αποτέλεσμα) υποδικτύων (*subnets*).
- Να διανέμει πληροφορία υποδικτύων σε όλο το δίκτυο μέσω πρωτοκόλλων δρομολόγησης.
- Να ελέγχει τη ροή της πληροφορίας βάση συγκεκριμένων πολιτικών πρόσβασης και ποιότητας των ροών.

Στο επίπεδο διανομής δίνεται σημασία στα ακόλουθα:

- Υποστήριξη μεταγωγής σε ταχύτητα σύρματος (*wire-speed switching*).
- Επαρκής ταχύτητα οπισθεπίπεδου των μεταγωγέων με όσο το δυνατό κάλυψη ταυτόχρονης μέγιστης χρήσης όλων των διεπαφών.

- Επαρκής αριθμός διεπαφών για τη διασύνδεση όλων των μεταγωγέων επιπέδου πρόσβασης.
- Επαρκής αναλογία κατερχόμενων συνδέσεων (*downlinks*) προς το επίπεδο πρόσβασης και ανερχόμενων συνδέσεων (*uplinks*) προς το επίπεδο πυρήνα, έτσι ώστε να αποφεύγονται σημεία συμφόρησης.
- Υποστήριξη συνάθροισης συνδέσεων στις κατερχόμενες και στις ανερχόμενες συνδέσεις, ώστε να αποφεύγονται σημεία συμφόρησης.
- Βλαβοαντοχή με πολλαπλούς μεταγωγείς διανομής (τουλάχιστον δύο) και πολλαπλές συνδέσεις προς κάθε μεταγωγέα πρόσβασης και πυρήνα.

Επίπεδο Πυρήνα

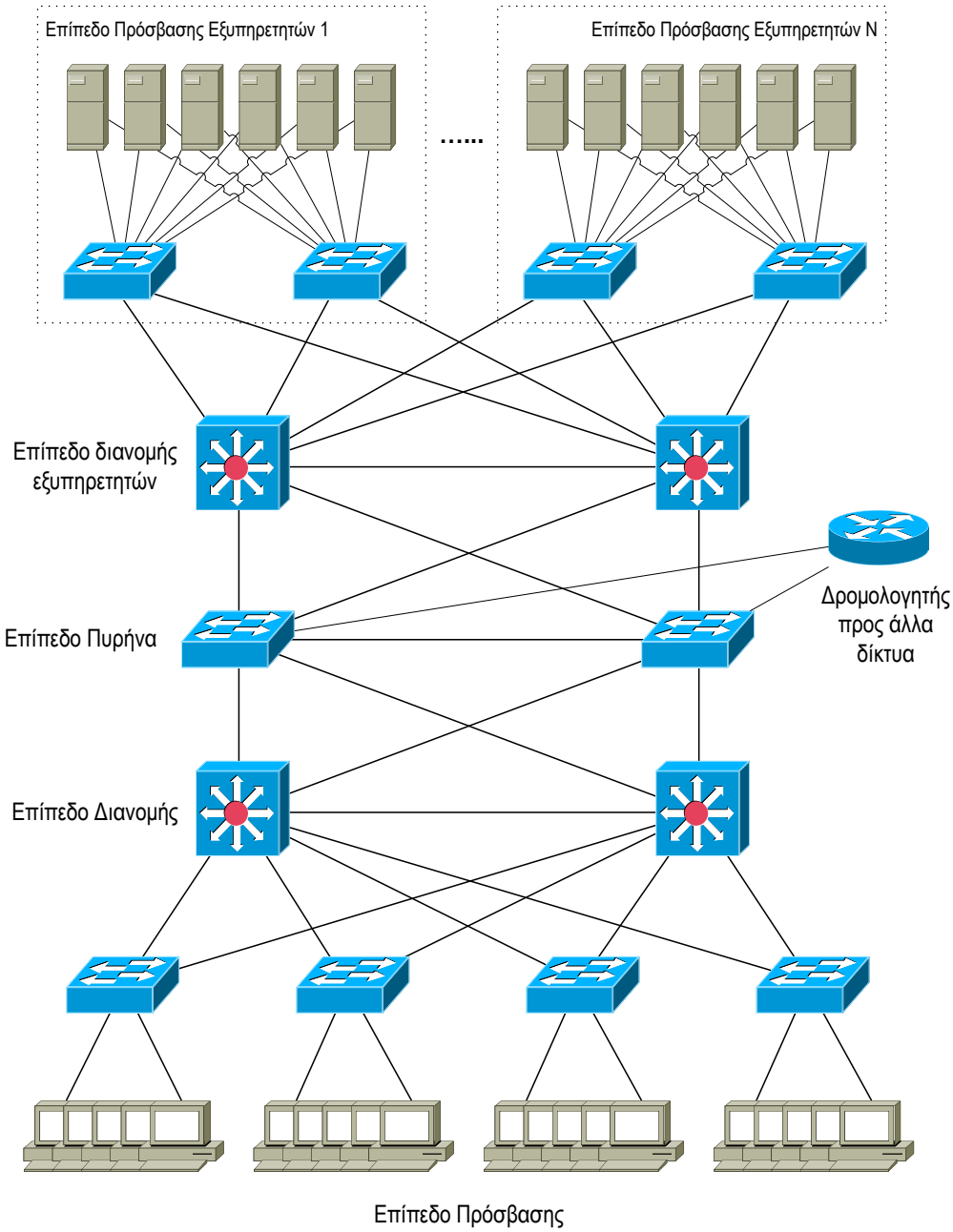
Το επίπεδο πυρήνα, όπως λέει και το όνομά του, αποτελεί τον πυρήνα του δικτύου, τον κορμό αυτού. Σαν αποτέλεσμα είναι ίσως και το σημαντικότερο δομοστοιχείο αυτού, με αποτέλεσμα να απαιτείται η μεγαλύτερη δυνατή ταχύτητα και αξιοπιστία.

Το επίπεδο πυρήνα διασυνδέει τα διαφορετικά δομοστοιχεία (μεταγωγείς) του επιπέδου διανομής. Πάνω σε αυτό συνδέονται τυπικά και οι εξυπηρετητές, είτε κατευθείαν, αν δεν είναι πολλοί (βλ. **Εικόνα 10.6**), είτε μέσω κάποιου επιπέδου πρόσβασης εξυπηρετητών (βλ. **Εικόνα 10.8**), είτε ακόμα και (αν υπάρχουν πολλά και διεσπαρμένα επίπεδα πρόσβασης εξυπηρετητών προς τα οποία πρέπει να γίνει βέλτιστη δρομολόγηση από μεγάλο αριθμό επιπέδων πρόσβασης σταθμών) μέσω κάποιου επιπέδου διανομής εξυπηρετητών (βλ. **Εικόνα 10.9**). Τυπικά όμως, για λόγους διατήρησης της υψηλότερης δυνατής ταχύτητας, το επίπεδο πυρήνα δεν διαθέτει τις δυνατότητες του επιπέδου διανομής (π.χ. δρομολόγηση) και είναι σύνηθες να αποτελείται από απλούς (αλλά ταχύτατους και αξιόπιστους) μεταγωγείς 2^{ου} Επιπέδου (*L2 switches*).

Στο επίπεδο πυρήνα δίνεται σημασία στα ακόλουθα:

- Υποστήριξη μεταγωγής σε ταχύτητα σύρματος (*wire-speed switching*), με την μικρότερη δυνατή καθυστέρηση (*delay*).
- Επαρκής ταχύτητα οπισθεπίπεδου των μεταγωγέων με 100% κάλυψη μέγιστης χρήσης όλων των διεπαφών.
- Επαρκής αριθμός διεπαφών για τη διασύνδεση όλων των μεταγωγέων επιπέδου διανομής.
- Επαρκής αναλογία κατερχόμενων συνδέσεων (*downlinks*) προς το επίπεδο διανομής, έτσι ώστε να αποφεύγονται σημεία συμφόρησης.
- Δυνατότητα υποστήριξης συνάθροισης συνδέσεων στις κατερχόμενες συνδέσεις προς το επίπεδο διανομής, ώστε να αποφεύγονται σημεία συμφόρησης.
- Βλαβοαντοχή με πολλαπλούς μεταγωγείς (τουλάχιστον δύο) και πολλαπλές συνδέσεις προς κάθε μεταγωγέα διανομής.

Τυπικά πάνω στους μεταγωγείς επιπέδου πυρήνα συνδέονται και οι δρομολογητές προς άλλα δίκτυα ή το Διαδίκτυο (*Internet*).



Εικόνα 10.9 Δίκτυο με ξεχωριστά επίπεδα πρόσβασης, διανομής, πυρήνα, διανομής και πρόσβασης εξυπηρετητών (πέντε επίπεδα)

10.2 Συγκεκλιμένα Δίκτυα

Στα παραδοσιακά δίκτυα, υπήρχε διαφορετική καλωδίωση για τους υπολογιστές, τα τηλέφωνα και τις οπτικοακουστικές συσκευές (τηλεοράσεις, σταθμούς τηλεδιάσκεψης κλπ). Η εξέλιξη όμως της τεχνολογίας των δικτύων και η μείωση του κόστους των οπτικοακουστικών συσκευών οδήγησε στην ενοποίηση των ξεχωριστών δικτύων πάνω από την ίδια δομημένη καλωδίωση και τα ίδια πρωτόκολλα δικτύωσης, όπως είναι το Ethernet και το IP.

Έτσι υπάρχουν πια τηλεφωνικές συσκευές, τηλεοράσεις, σταθμοί τηλεδιάσκεψης, κάμερες, συστήματα ελέγχου κτηρίων (*Building Management Systems*, BMS) και πολλά άλλα, που συνδέονται κατευθείαν πάνω στο δίκτυο των υπολογιστών και χρησιμοποιούν αυτό για όλη τη μεταφορά ήχου, εικόνας και δεδομένων που επιτελούν.

Αντίστοιχα, τα δίκτυα υπολογιστών και τα πρωτόκολλα που τα υλοποιούν έχουν εξελιχθεί ώστε να μπορούν να υποστηρίξουν τις νέες συσκευές και εφαρμογές εικόνας, ήχου και δεδομένων που τρέχουν πάνω από αυτά. Οι συσκευές που τα υλοποιούν, μεταγωγείς, δρομολογητές κτλ. υποστηρίζουν νέα πρωτόκολλα και ποιότητα υπηρεσίας (*quality of service*), ώστε να κάνουν δυνατή αυτή τη νέα λειτουργικότητα των δικτύων, με καλή ταχύτητα και αξιοπιστία, παράλληλα με την (ολοένα και αυξανόμενη) χρήση του δικτύου για μεταφορά δεδομένων. Λαμβάνοντας παράλληλα υπόψη ότι οι υπολογιστές έχουν μεταβληθεί σε μεγάλο βαθμό από καθαρά υπολογιστικές μηχανές σε μηχανές διακίνησης πληροφορίας.

Τα δίκτυα που υποστηρίζουν, αρχιτεκτονικά, λειτουργικά και ποιοτικά τέτοιες εφαρμογές και χρήσεις ονομάζονται συγκεκλιμένα δίκτυα (*converged networks*). Οι λειτουργίες και τα πρωτόκολλα που απαιτεί ένα τέτοιο δίκτυο απλώνονται σε όλα τα επίπεδα δικτύου (πρόσβασης, διανομής, πυρήνα) και σε όλες τις δικτυακές συσκευές (μεταγωγείς, δρομολογητές, τείχη προστασίας, γέφυρες, εξυπηρετητές, συσκευές και σταθμούς εργασίας) και τα πρωτόκολλα δικτύου (Ethernet, IP κτλ). Το κόστος ενός συγκεκλιμένου δικτύου είναι ελαφρά αυξημένο, ωστόσο κερδίζουμε σημαντικά σε λειτουργικότητα, ευελιξία, συντηρησιμότητα, διαχειρισιμότητα και ευκολότερη εγκατάσταση.

11. Ιδεατά Δίκτυα (*Virtual LANs*)

11.1 Εισαγωγή στα VLANs

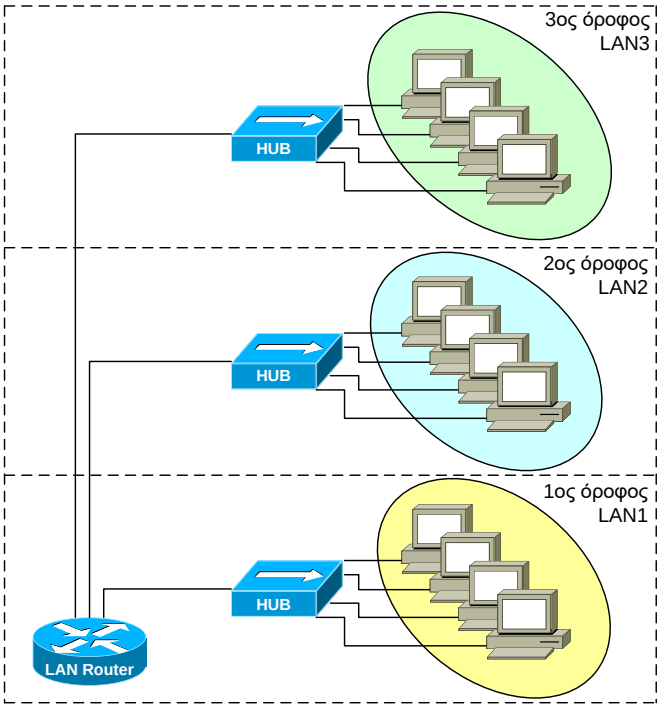
Από την ώρα που τα δίκτυα αυξήθηκαν τόσο σε μέγεθος (αριθμός δικτυακών σταθμών), όσο και στον όγκο δεδομένων που διακινούν (περισσότερες και 'βαρύτερες' εφαρμογές δικτύου), έγινε επιτακτική η αντιμετώπιση των ακόλουθων προβλημάτων.

- Το δίκτυο 'υπέφερε' από πολλές συγκρούσεις (*collisions*) και έπρεπε να περιοριστεί το μέγεθος των περιοχών σύγκρουσης (*collision domains*).
- Το δίκτυο 'υπέφερε' από πολλές ευρυεκπομπές και έπρεπε να περιοριστεί το μέγεθος των περιοχών ευρυεκπομπών (*broadcast domains*).
- Το δίκτυο έπρεπε να χωριστεί σε πολλαπλά υποδίκτυα (*subnets*), για την υλοποίηση των παραπάνω.
- Με τη χρήση της δομημένης καλωδίωσης έγινε μεγάλη η ανάγκη δυναμικής τοποθέτησης των σταθμών εργασίας σε συγκεκριμένα υποδίκτυα, όχι ανάλογα με τη φυσική τους θέση, αλλά ανάλογα με άλλες παραμέτρους (λειτουργικότητα, διεύθυνση, χρήστης κλπ).

Για την αντιμετώπιση του πρώτου προβλήματος, αναπτύχθηκαν οι μεταγωγείς, με την χρήση των οποίων καταργήθηκαν οι συγκρούσεις, το πρωτόκολλο CSMA/CD και η λειτουργία σε *half duplex*. Τώρα κάθε σταθμός συνδέεται αποκλειστικά σε μια θύρα μεταγωγέα, λειτουργώντας σε *full duplex*, διπλασιάζοντας την ταχύτητα και χωρίς να υπάρχει πιθανότητα σύγκρουσης με άλλον (εκτός και αν στη θύρα μεταγωγέα συνδέσουμε επαναλήπτη, *hub*, κάτι που δεν προτείνεται).

Για την αντιμετώπιση του δεύτερου και του τρίτου προβλήματος, παλαιότερες αρχιτεκτονικές δικτύου που χρησιμοποιούσαν ακόμα *hubs* (οι μεταγωγείς δεν υπήρχαν ακόμα ή ήταν πολύ ακριβοί), χώριζαν το δίκτυο σε διαφορετικούς τομείς σύγκρουσης, ευρυεκπομπών και αντίστοιχα υποδίκτυα, με τη χρήση αργών δρομολογητών τοπικού δικτύου (LAN *routers*), όπως στην **Εικόνα 11.1**.

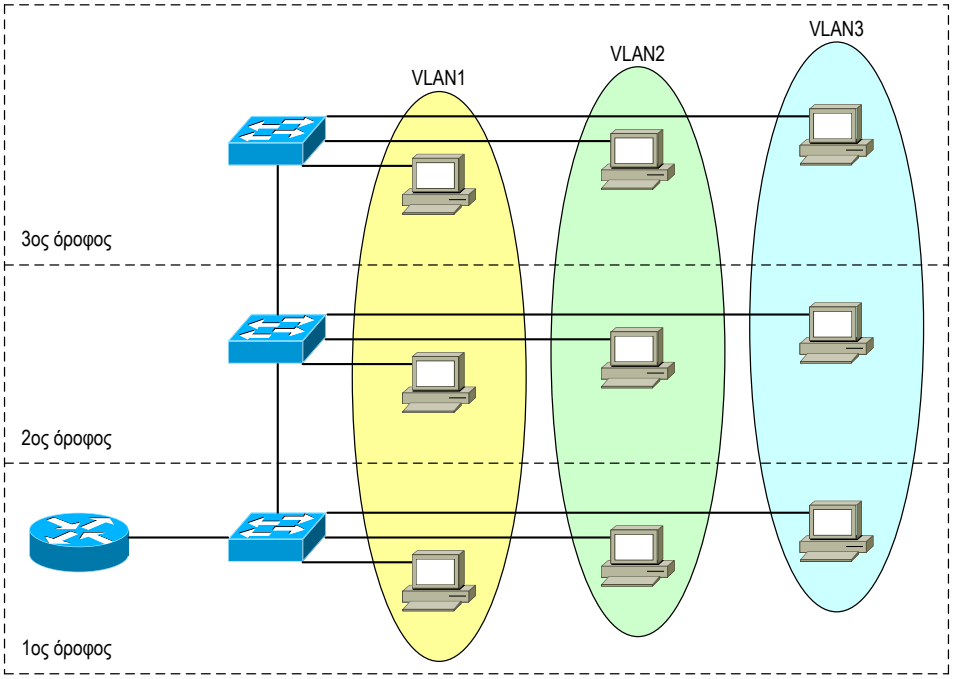
Ωστόσο αυτή η αρχιτεκτονική δεν διέθετε καλή κλιμακοθεσιμότητα (*scalability*) διότι οι LAN routers είχαν χαμηλή ταχύτητα μεταγωγής και λίγες θύρες (2-8), με αποτέλεσμα οι τομείς σύγκρουσης να μην περιορίζονται πολύ σε μέγεθος και το δίκτυο να μην μπορεί να μεγαλώσει πολύ χωρίς μεγάλη πτώση της ταχύτητας. Κυρίως όμως αυτή η αρχιτεκτονική δεν κάλυπτε το τέταρτο ζητούμενο. Έτσι, και με την εξέλιξη της τεχνολογίας των μεταγωγέων, αναπτύχθηκαν τα ιδεατά δίκτυα (*Virtual LAN*).



Εικόνα 11.1 Παλαιά αρχιτεκτονική δικτύου με LAN router

Ένα VLAN είναι μια λογική συνάθροιση δικτυακών συσκευών (για την ακρίβεια δικτυακών διεπαφών) που βρίσκονται εντός της ίδιας περιοχής ευρυεκπομπής, η οποία όμως μπορεί να απλώνεται σε πολλαπλά και ασύνδετα μεταξύ τους φυσικά τμήματα δικτύου. Κάθε συσκευή μπορεί να επικοινωνήσει με οποιαδήποτε άλλη εντός του ιδίου VLAN, όπου και αν είναι η φυσική της θέση, χρησιμοποιώντας ευρυεκομπές (*broadcasts*), πολυεκπομπές (*multicasts*) ή μονοεκπομπές (*unicasts*) Ethernet. Τα VLAN υλοποιούνται από το υλικό των μεταγωγέων και η σύνδεση μεταξύ των (ασύνδετων) τμημάτων γίνεται μόνο από μεταγωγείς, χωρίς την παρεμβολή δρομολογητών (τα VLAN δεν υποστηρίζονται από επαναλήπτες, *hubs*). Έτσι, ενώ οι μεταγωγείς κανονικά δεν κόβουν το δίκτυο σε πολλαπλούς τομείς ευρυεκπομπής, με την υλοποίηση των VLAN από αυτούς, το δίκτυο κόβεται σε πολλαπλούς τομείς ευρυεκπομπής, μία για κάθε VLAN.

Τονίζεται ότι ο διαχωρισμός των VLAN διασφαλίζεται από το υλικό των μεταγωγέων και δεν είναι δυνατή η υπερπήδηση VLAN (*VLAN hopping*). Κάθε VLAN αποτελεί ξεχωριστή περιοχή δικτύου από τα άλλα, με όρια που δεν μπορούν να υπερβληθούν με πρωτόκολλα 2^{ου} Επιπέδου. Δηλαδή το Ethernet και τα άλλα πρωτόκολλα 2^{ου} Επιπέδου δικτύου (και οι αντίστοιχες συσκευές, μεταγωγείς και γέφυρες) δεν μπορούν να μετάγουν μεταξύ VLAN. Για να γίνει αυτό και να είναι δυνατή η επικοινωνία μεταξύ διαφορετικών VLAN, πρέπει η επικοινωνία να 'ανέβει επίπεδο' και να δρομολογηθεί στο 3^{ο} Επίπεδο δικτύου, να γίνει δηλαδή δρομολόγηση από συσκευή (δρομολογητή) και πρωτόκολλο (IP) που μπορεί να το κάνει αυτό. Σαν αποτέλεσμα κάθε VLAN πρέπει να αποτελεί και ένα ξεχωριστό υποδίκτυο (*subnet*). Μια πιο σύγχρονη αρχιτεκτονική δικτύου με VLAN και δρομολογητή για τη διασύνδεση μεταξύ των VLAN φαίνεται στην **Εικόνα 11.2**.



Εικόνα 11.2 Νεότερη αρχιτεκτονική δικτύου με VLAN και δρομολογητή

Τα VLAN υλοποιούνται από τους μεταγωγείς με επέκταση της λειτουργίας της προώθησης πλαισίων μέσω του πίνακα διευθύνσεων MAC (*MAC address table*). Στους μεταγωγούς Cisco η διαμόρφωση των VLAN αποθηκεύεται σε ειδικό αρχείο με όνομα vlan.dat, που βρίσκεται στη μνήμη flash των μεταγωγέων και όχι στο startup-configuration, αποτελεί δε τη λεγόμενη βάση δεδομένων VLAN (VLAN *database*). Γνωρίζοντας σε ποιο VLAN ανήκει ένα εισερχόμενο σε μια θύρα πλαίσιο (βλ. παρακάτω για το πώς αποκτά τη γνώση αυτή), ο μεταγωγέας το προωθεί μόνο προς θύρες πρόσβασης που ανήκουν στο ίδιο VLAN, είτε σε αυτήν που αντιστοιχεί στη διεύθυνση MAC παραλήπτη (όπως την βρίσκει από την αναζήτηση στον πίνακα MAC), είτε σε όλες (αν δεν γνωρίζει αυτόν τον παραλήπτη). Το προωθεί επίσης σε όλες τις θύρες κορμού από τις οποίες περνάει αυτό το VLAN (βλ. παρακάτω για θύρες κορμού).

Η υλοποίηση των VLAN παρέχει τα ακόλουθα πλεονεκτήματα:

- Εύκολη προσθήκη και μετακίνηση σταθμών από υποδίκτυο σε υποδίκτυο. Δεν ισχύει ο περιορισμός της τοποθέτησης σε υποδίκτυο ανάλογα με τη φυσική θέση του σταθμού. Η προσθήκη / μετακίνηση γίνεται απλώς με προγραμματισμό των μεταγωγέων, ή αυτόματα με προ-ορισμένα κριτήρια που έχουν προγραμματιστεί στους μεταγωγείς.
- Ευκολότερη αλλαγή της λογικής τοπολογίας του δικτύου, χωρίς αλλαγές στην καλωδίωση.
- Έλεγχος των ευρυεκπομπών (*broadcast containment*). Το δίκτυο χωρίζεται σε ξεχωριστούς τομείς ευρυεκπομπής, μία για κάθε VLAN, μειώνοντας έτσι το μέγεθός τους και την επίπτωσή τους σε ολόκληρο το δίκτυο.
- Αποδοτικότερη χρήση του εξοπλισμού. Δεν χρειάζονται πια επιπλέον μεταγωγείς για την υλοποίηση διαφορετικών υποδικτύων.

- Καλύτερη κλιμακοθεσιμότητα. Με τα VLAN είναι δυνατό να δημιουργήσουμε μεγαλύτερα δίκτυα χωρίζοντάς τα σε διαφορετικούς τομείς ευρυεκπομπής. Μια τυπική σύσταση για τον αριθμό των συσκευών ανά VLAN είναι 500. Αυτό μπορεί να διαφοροποιηθεί σημαντικά βέβαια, ανάλογα με τις εφαρμογές που τρέχουν.
- Μεγαλύτερη ασφάλεια. Είναι δυνατό να τοποθετηθούν κανόνες διακριτικής πρόσβασης στις συσκευών που θα δρομολογούν μεταξύ των VLAN (δρομολογητές ή τείχη προστασίας).
- Επειδή τα VLAN υλοποιούνται από το υλικό των μεταγωγέων δεν εισάγουν επιπλέον καθυστέρηση στο δίκτυο (για την επικοινωνία εντός του ιδίου VLAN).

Η υλοποίηση των VLAN παρέχει τα ακόλουθα μειονεκτήματα:

- Πιο πολύπλοκη διαμόρφωση των μεταγωγέων και μεγαλύτερο κόστος κτήσης τους (πρέπει να είναι διαχειρίσιμοι μεταγωγείς).
- Επιπλέον διαχειριστικός φόρτος, εφόσον δεν υπάρχει αυτόματη τοποθέτηση σταθμών στα VLAN. Οι διαχειριστές πρέπει να διατηρούν πίνακες με αντιστοιχίσεις μεταξύ πριζών πρόσβασης, συνδέσεων σε κατανεμητή (*patch panel*), θυρών μεταγωγέων και VLAN.
- Αυξημένη καθυστέρηση για την επικοινωνία μεταξύ των VLAN λόγω ανάγκης δρομολόγησης της επικοινωνίας αυτής από το 3° Επίπεδο δικτύου (δρομολόγηση).
- Πιθανή δημιουργία σημείων συμφόρησης σε γραμμές από τις οποίες διέρχονται πολλά VLAN (βλ. παρακάτω, γραμμές κορμού).

11.2 VLAN και τύποι κίνησης

Τα VLAN χρησιμοποιούνται και για το διαχωρισμό κίνησης ανάλογα με τον τύπο της (όχι μόνο ανάλογα με τους υπολογιστές που τη διακινούν), προκειμένου να κρατηθεί χωριστή από άλλα είδη και να τύχει διαφορετικής αντιμετώπισης, όσον αφορά την διασφάλιση ποιότητας και ασφάλειας. Έτσι κίνηση διαχειριστική, φωνής (*Voice over IP*), πολυεκπομπής (*multicast*) και δικτυακής αποθήκευσης (*storage network*), μπορεί να τοποθετείται σε ξεχωριστά VLAN από την απλή κίνηση δικτύου. Για παράδειγμα κίνηση φωνής ή εικόνας έχει τυπικά ιδιαίτερες απαιτήσεις περιορισμού της μεταβλητότητας της καθυστέρησης και η ανάμιξή της με κίνηση δεδομένων μπορεί να δημιουργεί προβλήματα στον ήχο ή στην εικόνα.

Πολλοί μεταγωγείς υποστηρίζουν ειδικό είδος VLAN που ονομάζεται VLAN φωνής (*voice VLAN*), στο οποίο μπορούν να τοποθετούν αυτόματα συσκευές που παράγουν τέτοια κίνηση, διασφαλίζοντας παράλληλα με ειδικούς αλγόριθμους ουριοδότησης (*queuing*) στην μεταγωγή την ποιότητα (QoS) που απαιτείται γι’ αυτή την κίνηση.

11.3 Τοποθέτηση σε VLAN

Βασικό πρόβλημα για ένα μεταγωγέα στον οποίο έχουν οριστεί πολλαπλά VLAN είναι το να καθορίσει σε ποιο από αυτά ανήκει ένα εισερχόμενο σε μια θύρα πλαίσιο. Ο καθορισμός αυτός μπορεί να γίνει με τρεις βασικούς τρόπους:

- Στατικά. Με αυτό τον τρόπο ορίζεται σε μια θύρα ότι ένα εισερχόμενο πλαίσιο Ethernet ανήκει σε συγκεκριμένο VLAN, το οποίο ονομάζεται VLAN θύρας (port VLAN). Στη γλώσσα της Cisco, αυτή είναι θύρα πρόσβασης (βλ. παρακάτω) και 'ανήκει' σε αυτό το VLAN.
- Δυναμικά. Με αυτό τον τρόπο ορίζεται ότι ένα εισερχόμενο σε μια θύρα πλαίσιο ανήκει σε ένα VLAN ανάλογα με κανόνες που εφαρμόζονται πάνω στις κεφαλίδες $2^{ου}$, $3^{ου}$, ή $4^{ου}$ Επιπέδου ή ακόμα και στα δεδομένα εφαρμογής ($7^{ου}$ Επιπέδου) που βρίσκονται εντός του πλαισίου. Έτσι μπορεί για παράδειγμα να καθοριστεί ότι ένα εισερχόμενο πλαίσιο ανήκει σε ένα VLAN ανάλογα με τη διεύθυνση MAC, ή τη διεύθυνση IP του αποστολέα, ή το πρωτόκολλο συνεδρίας που ενθυλακώνει. Γι' αυτό το σκοπό, ο μεταγωγέας μπορεί να συμβουλευτεί ένα εξυπηρετητή πολιτικής ιδιότητας μέλλους VLAN (*VLAN membership policy server*), ο οποίος παρέχει αντιστοίχιση ανάμεσα στην πληροφορία-κριτήριο (π.χ. MAC διευθύνσεις) και τα VLAN.
  Μια άλλη επιλογή είναι να χρησιμοποιηθεί επαλήθευση ταυτότητας θύρας (*port authentication*) βασισμένη στο πρωτόκολλο 802.1x, το οποίο μπορεί να χρησιμοποιηθεί για την επαλήθευση της ταυτότητας του χρήστη ενός σταθμού που συνδέεται σε ένα μεταγωγέα ή ένα ασύρματο σημείο πρόσβασης (*wireless Access Point*). Και πάλι ο μετατωγέας συμβουλεύεται έναν εξυπηρετητή ελέγχου πρόσβασης (*Access Control Server*), ο οποίος μπορεί να ορίζει το VLAN στο οποίο θα τοποθετούνται τα πλαίσια που παράγονται από το σταθμό, γι' αυτό το χρήστη, βάση των διαπιστευτηρίων (όνομα / κωδικός) που παρείχε.
  Τα δυναμικά VLAN έχουν ένα βασικό πλεονέκτημα έναντι των στατικών. Ενέχουν πολύ μικρότερο διαχειριστικό φόρτο και υποστηρίζουν κινητικότητα των σταθμών. Ο διαχειριστής δεν χρειάζεται πια να διατηρεί πίνακες αντιστοιχίσεων μεταγωγέων-θυρών-VLAN και ένας σταθμός μπορεί να μετακινηθεί σε άλλη θύρα/μεταγωγέα χωρίς επίπτωση. Από την άλλη όμως, απαιτούν την ύπαρξη εξυπηρετητή και ειδικού λογισμικού (τα οποία έχουν κάποιο κόστος), υποστήριξη από το υλικολογισμικό (*firmware*) του μεταγωγέα και πιο πολύπλοκη διαμόρφωση (προγραμματισμό) αυτού.
- Φωνής. Σε VLAN φωνής τοποθετούνται αυτόματα τα πλαίσια τα οποία παράγονται από συσκευές φωνής. Τα πλαίσια αυτά διαθέτουν τυπικά ειδική σήμανση στις κεφαλίδες $2^{ου}$ ή $3^{ου}$ Επιπέδου που τα χαρακτηρίζει ως πλαίσια φωνής. Ακόμα και αν στη θύρα του μεγαγωγέα είναι συνδεδεμένος, εκτός από το IP τηλέφωνο και σταθμός εργασίας (πολλά IP τηλέφωνα ενσωματώνουν ένα μικρό μεταγωγέα με μια ανερχόμενη και μια κατερχόμενη σύνδεση, έτσι ώστε μια θέση εργασίας να μην χρειάζεται δύο θύρες πρόσβασης, μια για δεδομένα και μια για τηλεφωνία), ο μεταγωγέας μπορεί να ξεχωρίσει τα πλαίσια φωνής από τα πλαίσια δεδομένων και να τα τοποθετήσει στο voice VLAN.

11.4 Συνδέσεις VLAN

Σε κάποιους κατασκευαστές μεταγωγέων όπως η Cisco, μια θύρα χαρακτηρίζεται είτε ως θύρα πρόσβασης (*access port*), είτε ως θύρα κορμού (*trunk port*). Σε άλλους κατασκευαστές δεν υπάρχει αυτός ο διαχωρισμός (μάλιστα *trunk* ονομάζεται η συνάθροιση συνδέσεων, *link aggregation*). Σε αυτή την περίπτωση η θύρα ονομάζεται γενικού τύπου (*generic port*).

Θύρες Πρόσβασης

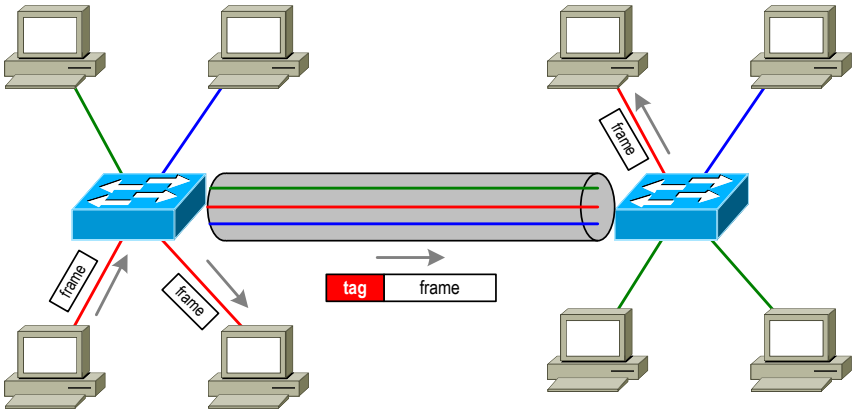
Μια θύρα πρόσβασης είναι αυτή που συνδέεται σε ένα τμήμα δικτύου στο οποίο 'τρέχει' το κανονικό Ethernet (802.3), στα πλαίσια του οποίου δεν υπάρχει πληροφορία για το VLAN που ανήκουν. Μια τέτοια θύρα (η οποία είναι τυπικά και portfast – βλ. STP), σχετίζεται με ένα μόνο VLAN (είτε στατικά, είτε δυναμικά) και μια συσκευή που είναι συνδεδεμένη σε αυτή ανήκει σε αυτό το συγκεκριμένο VLAN.

Για τον μεταγωγέα, κάθε εισερχόμενο σε αυτή τη θύρα πλαίσιο Ethernet ανήκει σε αυτό το VLAN. Αν στη θύρα συνδεθούν παραπάνω της μιας συσκευής (π.χ. με χρήση ενός *hub* ή ενός μη διαχειρίσιμου μεταγωγέα), τότε όλες θα ανήκουν σ' αυτό το VLAN. Αν υπάρχει ανάγκη οι συσκευές να ανήκουν σε πολλαπλά VLAN, θα πρέπει να συνδεθεί στη θύρα ένας διαχειρίσιμος μεταγωγέας και η θύρα να προγραμματιστεί ως θύρα κορμού (βλ. παρακάτω). Τα πλαίσια που εισέρχονται και εξέρχονται από τη θύρα αυτή λέμε ότι είναι *μη επισηματοθετημένα (untagged)*, επειδή δεν διαθέτουν τη σήμανση του ποιο VLAN ανήκουν.

Θύρες Κορμού

Αντίθετα, μια θύρα κορμού δεν ανήκει σε συγκεκριμένο VLAN. Οι θύρες κορμού είναι *απαραίτητες* για τη διασύνδεση μεταγωγέων στους οποίους έχουν οριστεί VLAN. Χωρίς αυτές τα διεσπαρμένα σε διαφορετικούς μεταγωγείς φυσικά τμήματα ενός VLAN δεν θα ενώνονταν. Δηλαδή οι συσκευές που θα βρίσκονταν στο ίδιο VLAN αλλά θα ήταν συνδεδεμένες σε διαφορετικούς μεταγωγείς δεν θα επικοινωνούσαν.

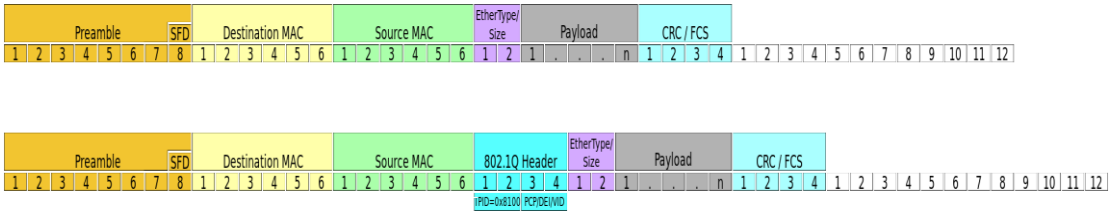
Από μια θύρα κορμού περνάνε είτε όλα, είτε κάποια από τα VLAN (αυτό μπορεί να καθοριστεί στατικά με τη λειτουργία *allowed VLANs*, προτερόθετα περνάνε όλα τα VLAN). Όταν ένας μεταγωγέας εκπέμπει ένα πλαίσιο σε μια θύρα κορμού, πρέπει να συμπεριλάβει την πληροφορία του VLAN στο οποίο ανήκει το πλαίσιο, αλλιώς ο μεταγωγέας που θα το παραλάβει από την άλλη μεριά δεν θα ξέρει σε ποιο VLAN ανήκει, αφού η θύρα που το λαμβάνει δεν ανήκει σε κάποιο VLAN και το απλό πρωτόκολλο Ethernet δεν περιλαμβάνει πληροφορία VLAN (βλ. παρακάτω, πρωτόκολλο dot1q), **Εικόνα 11.3**.



Εικόνα 11.3 Θύρες κορμού για την επικοινωνία μεταξύ μεταγωγέων με VLANs.

Για να είναι δυνατά τα παραπάνω, χρειαζόμαστε ένα αναγνωριστικό για τα VLAN, που το ονομάζουμε VLAN ID (VID). Επιπλέον χρειαζόμαστε ένα πρωτόκολλο που θα τρέχει στις θύρες κορμού το οποίο θα περιλαμβάνει στην κεφαλίδα του την πληροφορία VID (κάτι που δεν κάνει το Ethernet). Το πρωτόκολλο που έχει επικρατήσει είναι το 802.1q (συνήθως το γράφουμε *dot1q*). Αποτελεί πρότυπο της IEEE και υποστηρίζεται από τους μεταγωγείς όλων των κατασκευαστών.

Το dot1q υποστηρίζει VIDs μήκους 12 bits, με τιμές από 1 έως 4095 (τιμές 0 και 4096 είναι αποκλεισμένες), υποστηρίζονται δηλαδή θεωρητικά 4094 διαφορετικά VLAN (βέβαια κάποιος συγκεκριμένος μεταγωγέας μπορεί να υποστηρίζει λιγότερα). Την πληροφορία αυτή το dot1q την τοποθετεί σε μια νέα κεφαλίδα που εισάγει στο Ethernet, το *dot1q header* (από πολλούς αυτή η κεφαλίδα ονομάζεται ετικέτα – tag). Επομένως το dot1q *δεν* είναι Ethernet και ένας μεταγωγέας που μετάγει ένα πλαίσιο Ethernet από μια θύρα πρόσβασης σε μια θύρα κορμού *πρέπει* να το μετασχηματίσει σε dot1q, εισάγοντας τη νέα κεφαλίδα και υπολογίζοντας ξανά το πεδίο ελέγχου του πλαισίου (FCS). Η μορφή ενός πλαισίου dot1q φαίνεται στην **Εικόνα 11.4**[1].



Εικόνα 11.4 Σύγκριση πλαισίων Ethernet και Dot1q

Η αρίθμηση είναι σε bytes. Η κεφαλίδα dot1q (802.1q Header) έχει συνολικό μήκος 4 bytes. Από αυτά, τα 12 τελευταία bits αποτελούν το VID.

Αυτός ο μετασχηματισμός πλαισίων ονομάζεται επισηματοθέτηση (*tagging*) και γι' αυτό λέμε ότι το dot1q είναι ένα πρωτόκολλο που εισάγει ετικέτες (*tagging protocol*). Η επισηματοθέτηση γίνεται από το υλικό του μεταγωγέα, έτσι ώστε να μην δημιουργείται καθυστέρηση στη μεταγωγή. Μια θύρα που θα λάβει ένα πλαίσιο dot1q και δεν τρέχει dot1q (π.χ. μια θύρα ενός σταθμού εργασίας ή μια θύρα

[1] Bill Stafford, Wikipedia

πρόσβασης ενός μεταγωγέα), δεν θα το καταλάβει και θα το πετάξει. Επίσης, ένας μεταγωγέας μπορεί να κάνει και την αντίστροφη διαδικασία, να μετασχηματίσει δηλαδή ένα πλαίσιο dot1q σε Ethernet, προκειμένου να το μεταγάγει από μια θύρα κορμού σε μια θύρα πρόσβασης.

Σε μια θύρα κορμού ορίζεται επίσης ένα εντόπιο VLAN (*native* VLAN), στο οποίο ένας μεταγωγέας θεωρεί ότι ανήκει ένα μη επισηματοθετημένο πλαίσιο που λαμβάνεται στη θύρα αυτή. Αντίστροφα, τα πλαίσια που ανήκουν στο εντόπιο VLAN εκπέμπονται στη θύρα αυτή προτερόθετα χωρίς επισηματοθέτηση (για λόγους ασφαλείας είναι δυνατόν να οριστεί ότι ακόμα και τα πλαίσια του εντόπιου VLAN θα εκπέμπονται επισηματοθετημένα). Προτερόθετα, το εντόπιο VLAN είναι το VLAN1, όπως αυτό μπορεί να αλλάξει με ειδική ρύθμιση. Είναι σημαντικό το εντόπιο VLAN και των δύο θυρών που μετέχουν σε μια σύνδεση δικτύου μεταξύ δύο μεταγωγέων να είναι το ίδιο, αλλιώς θα συμβεί ανάμιξη των VLAN. Σημειώνεται εδώ ότι η τελευταία έκδοση του 802.1q-2004 δεν περιλαμβάνει την έννοια των γραμμών κορμού ή του εντόπιου VLAN (βλ. παρακάτω, γενικού τύπου θύρες). Σαν μέτρο ασφαλείας, το πρωτόκολλο CDP (*Cisco Discovery Protocol*), το οποίο είναι προτερόθετα ενεργό στους μεταγωγείς της Cisco, παράγει μηνύματα λάθους εφόσον ανιχνεύσει ότι οι δύο θύρες που μετέχουν σε μια σύνδεση κορμού έχουν διαφορετικό εντόπιο VLAN.

Συσκευές που υποστηρίζουν θύρες κορμού (ή γενικότερα θύρες που τρέχει το πρωτόκολλο dot1q) δεν είναι μόνο μεταγωγείς. Dot1q υποστηρίζουν σε διεπαφές Ethernet και δρομολογητές και εξυπηρετητές. Οι πρώτοι το κάνουν για να μπορούν να δρομολογούν μεταξύ VLAN μέσα από την ίδια διεπαφή (βλ. δρομολόγηση μεταξύ VLAN), χωρίς να χρειάζονται μία φυσική διεπαφή ανά VLAN. Οι εξυπηρετητές το υποστηρίζουν είτε για να μπορούν να συνδέονται σε όλα τα VLAN (έτσι ώστε να είναι προσβάσιμοι από όλα, χωρίς ανάγκη χρήσης δρομολογητή, μια διασύνδεση που είναι μάλλον ασυνήθιστη στα σύγχρονα δίκτυα, όπου προτιμάται η δρομολόγηση με χρήση μεταγωγέων 3^{ου} Επιπέδου), είτε για να υποστηρίζουν ιδεατούς μεταγωγείς (*virtual switches*), στα πλαίσια μιας ιδεατής υποδομής (*virtual infrastructure*).

Σημειώνεται ότι υπάρχει και νεότερο πρότυπο πρωτόκολλο επισηματοθέτησης, το IEEE 802.1ad με επιπλέον δυνατότητες όπως διπλές ετικέτες (QinQ).

Γενικού Τύπου Θύρες

Στις γενικού τύπου θύρες ορίζεται ρητά τι γίνεται με τα εκπεμπόμενα πλαίσια (αν επισηματοθετούνται ή όχι) και τι γίνεται με τα πλαίσια που λαμβάνονται (τι αντιμετώπιση θα έχουν αν δεν έχουν επισηματοθέτηση).

Για την εκπομπή των πλαισίων, ορίζεται τα πλαίσια ποιων VLAN θα επισηματοθετούνται και ποιών δεν θα επισηματοθετούνται. Τυπικά τα πλαίσια όλων των VLAN εκτός από ένα επισηματοθετούνται (είναι δυνατό να επισηματοθετούνται όλα τα πλαίσια όλων των VLAN για λόγους ασφαλείας). Το VLAN του οποίου τα πλαίσια δεν επισηματοθετούνται αντιστοιχεί στο εντόπιο VLAN της προηγούμενης παραγράφου.

Για τη λήψη των πλαισίων, ορίζεται σε ποιο VLAN, το ονομαζόμενο VLAN θύρας, θα θεωρείται ότι ανήκει ένα εισερχόμενο πλαίσιο που δεν διαθέτει επισηματοθέτηση (αν διαθέτει, απλά ανήκει στο VLAN που ορίζει η κεφαλίδα του dot1q). Ο ορισμός του VLAN θύρας μπορεί να είναι είτε δυναμικός, είτε στατικός, όπως αναλύεται στην παράγραφο 'Τοποθέτηση σε VLAN'.

Όπως και στην περίπτωση του εντόπιου VLAN, όταν έχουμε δύο μεταγωγείς που είναι συνδεδεμένοι μεταξύ τους με ένα καλώδιο, καλό είναι οι δύο θύρες να έχουν το ίδιο VLAN ορισμένο ως VLAN θύρας, διαφορετικά θα έχουμε μίξη της κίνησης διαφορετικών VLAN, κάτι που είναι κανονικά ανεπίτρεπτο (υπάρχουν περιπτώσεις, όμως τα ασυμμετρικά VLAN που θέλουμε κάτι τέτοιο και μάλιστα για περισσότερα των δύο VLAN, καλό είναι όμως να αποφεύγεται αν δεν γνωρίζουμε καλά τις επιπτώσεις αυτού).

Dynamic Trunking Protocol

Η Cisco έχει αναπτύξει ένα πρωτόκολλο δυναμικής ενεργοποίησης κατάστασης κορμού στις θύρες των μεταγωγέων, το οποίο ονομάζεται DTP και είναι προτερόθετα ενεργό στους μεταγωγείς της. Αν ένας μεταγωγέας ανιχνεύσει ότι υποστηρίζεται από τον απέναντι μεταγωγέα που είναι συνδεδεμένος, τότε το DTP μπορεί να ενεργοποιήσει το dot1q γι' αυτή τη θύρα, τοποθετώντας τη σε κατάσταση κορμού.

Το DTP ορίζει τις ακόλουθες ρυθμίσεις για μια θύρα που έχει οριστεί ως θύρα κορμού (αν μια θύρα έχει οριστεί ως πρόσβασης, τότε δεν τρέχει DTP):

- On. Σε αυτή τη διαμόρφωση η θύρα είναι ρυθμισμένη ως θύρα κορμού στατικά. Ότι και αν είναι η απέναντί της, αυτή θα τρέχει dot1q. Όμως στέλνει διαφημίσεις DTP στην απέναντι, έτσι ώστε αν τις καταλαβαίνει να μπορεί να αλλάξει κι αυτή αντίστοιχα σε λειτουργία κορμού.
- Dynamic Auto. Σε αυτή τη διαμόρφωση η θύρα διαφημίζει τη δυνατότητά της να γίνει θύρα κορμού, αλλά δεν το επιδιώκει. Η θύρα γίνεται κορμού μόνο αν η απέναντι θύρα το ζητήσει (dynamic desirable) ή αν είναι ήδη σε διαμόρφωση κορμού (on). Αν και οι δύο θύρες είναι σε ρύθμιση dynamic auto, τότε δεν γίνονται κορμού. Αν η απέναντι θύρα δεν απαντήσει (δεν μπορεί να διαπραγματευτεί με DTP), τότε η θύρα γίνεται θύρα πρόσβασης (δεν σηκώνει dot1q). Η διαμόρφωση αυτή είναι η προτερόθετη διαμόρφωση των θυρών σε μεταγωγείς Cisco.
- Dynamic Desirable. Σε αυτή την κατάσταση η θύρα διαφημίζει την επιθυμία να γίνει θύρα κορμού. Αν η απέναντι θύρα είναι on, dynamic auto, ή dynamic desirable, η θύρα γίνεται κορμού. Αν η απέναντι θύρα δεν μπορεί να διαπραγματευτεί με DTP, τότε η θύρα γίνεται θύρα πρόσβασης (δεν σηκώνει dot1q).

Ο ακόλουθος πίνακας συνοψίζει τα παραπάνω για μια σύνδεση μεταξύ δύο θυρών. Στην πρώτη γραμμή είναι η ρύθμιση της μιας θύρας και στην πρώτη

στήλη η ρύθμιση της απέναντι θύρας. Στα κελιά η κατάσταση που διαμορφώνεται τελικά η σύνδεση (και οι θύρες) από το DTP.

	Dynamic Auto	**Dynamic Desirable**	**Trunk**	**Access**
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Λάθος
Access	Access	Access	Λάθος	Access

Είναι δυνατό να απενεργοποιηθεί το DTP, οπότε οι θύρες διαμορφώνονται είτε ως κορμού, είτε ως πρόσβασης στατικά. Άλλοι κατασκευαστές μεταγωγέων δεν υποστηρίζουν το DTP και η ρύθμιση γίνεται στατικά.

11.5 VLAN Διαχείρισης

Το VLAN διαχείρισης είναι ένα VLAN που παρέχει τη δυνατότητα να διαχειριστεί κανείς τον μεταγωγέα. Σε αυτό το VLAN τοποθετείται η λογική διεπαφή (logical interface) 3^{ου} Επιπέδου και η διεύθυνση IP πάνω στα οποία συνδεόμαστε με πρωτόκολλο απομακρυσμένης κονσόλας (telnet, ssh) ή σε διαχειριστική ιστοσελίδα (*web-based* GUI). Για να γίνει αυτό δημιουργείται, όπως αναφέραμε, μια λογική διεπαφή, αφού ο τυπικός μεταγωγέας είναι συσκευή 2^{ου} Επιπέδου δικτύου και οι φυσικές του διεπαφές 'καταλαβαίνουν' και μετάγουν μόνο Ethernet και όχι IP.

Προτερόθετα, το διαχειριστικό VLAN είναι το VLAN1 και η λογική διεπαφή για τη διαχείριση είναι το vlan1 (για να τα ξεχωρίζουμε τα γράφουμε σε αυτό το κείμενο το ένα με κεφαλαία και το άλλο με μικρά, όμως στην πράξη η γραφή δεν έχει σημασία). Τονίζεται ότι εννοιολογικά το πρώτο είναι αντικείμενο 2^{ου} Επιπέδου (Virtual LAN), ενώ το δεύτερο είναι αντικείμενο 3^{ου} Επιπέδου (διεπαφή IP). Όμως συνδέονται αυτόματα και όταν τοποθετηθεί διεύθυνση IP στο vlan1 και 'σηκωθεί' η διεπαφή, ο μεταγωγέας δέχεται συνδέσεις σε αυτή πάνω από το δίκτυο, εντός της περιοχής ευρυεκπομπών που αποτελεί το VLAN1.

Είναι δυνατό το διαχειριστικό VLAN να αλλάξει και να οριστεί κάποιο άλλο, απλά ορίζοντας μια άλλη λογική διεπαφή (π.χ. vlan100) και τοποθετώντας διεύθυνση IP σε αυτήν, αντί του vlan1. Τονίζεται ότι ο τυπικός μεταγωγέας επιδέχεται μόνο μία τέτοια λογική διεπαφή ενεργή, διότι είναι συσκευή 2^{ου} Επιπέδου και όχι 3^{ου} (δρομολογητής). Αν προσπαθήσουμε να σηκώσουμε δεύτερη λογική διεπαφή δίνοντας σε αυτή διεύθυνση IP, τότε η πρώτη απενεργοποιείται αυτόματα. Τονίζεται επίσης ότι του ορισμού της νέας λογικής διεπαφής, *πρέπει* να προηγηθεί ο ορισμός του αντίστοιχου VLAN, διαφορετικά η νέα διεπαφή θα 'μείνει' στον αέρα, χωρίς σύνδεση σε VLAN (κάποιοι μεταγωγείς δημιουργούν αυτόματα και το αντίστοιχο VLAN).

11.6 Ρυθμίσεις VLAN σε μεταγωγείς με Cisco CLI

Για τον ορισμό ενός νέου VLAN:

```
Switch(config)# vlan vlan#
```

Για παράδειγμα για τον ορισμό του VLAN 2 δίνουμε:

```
Switch(config)# vlan 2
```

Αφού οριστεί ένα VLAN, μπορεί προαιρετικά να δοθεί ένα όνομα σ' αυτό. Το όνομα ισχύει μόνο γι' αυτόν τον μεταγωγέα και έχει καθαρά πληροφοριακό ρόλο, δεν έχει σημασία για τη διαμόρφωση των VLAN. Η εντολή είναι:

```
Switch(config-vlan)# name vlan_name
```

Παράδειγμα:

```
Switch(config-vlan)# name red
```

Για να δούμε τα VLAN που είναι ορισμένα μέσα στη VLAN database δίνουμε:

```
Switch# show vlan [brief | vlan# | summary]
```

Παράδειγμα:

```
Switch# show vlan brief
```

Με το **brief** η εντολή παράγει πίνακα που δείχνει όλα τα προορισμένα VLAN, όλα αυτά που έχουμε ορίσει, καθώς και ποιες θύρες του μεταγωγέα ανήκουν σε αυτά. Με το *VLAN#* δείχνει πληροφορίες μόνο για το συγκεκριμένο VLAN. Με το **summary** δείχνει στατιστικά για όλα τα VLAN.

Για να ορίσουμε μια θύρα ως **access** και να την τοποθετήσουμε στατικά σε ένα VLAN πρέπει να δώσουμε (αφού πρώτα έχουμε ορίσει το ζητούμενο VLAN, ως παραπάνω):

```
Switch(config)# interface type [slot#]/port#
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan vlan#
```

Παράδειγμα:

```
Switch(config)# interface fastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
```

Για να ορίσουμε μια θύρα ως `trunk` και να ορίσουμε το `native vlan` της δίνουμε:

```
Switch(config)# interface type [slot#]/port#
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan vlan#
```

Παράδειγμα:

```
Switch(config)# interface gigabitEthernet1/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 99
```

Για να καθορίσουμε ποια VLAN επιτρέπονται να περνάνε σε μια `trunk` θύρα δίνουμε:

```
Switch(config-if)# switchport trunk allowed vlan [vlan_list | all | add
vlan_list | except vlan_list | none | remove vlan_list]
```

Παράδειγμα:

```
Switch(config-if)# switchport trunk allowed vlan 1-10
```

Με την παράμετρο *vlan_list* καθορίζουμε ποια VLAN θα περνάνε, θα προστεθούν σε αυτά που περνάνε, θα εξαιρούνται ή θα αφαιρεθούν από αυτά που περνάνε, αντίστοιχα. Με την `all` ορίζουμε να περνάνε όλα. Με την ακόλουθη εντολή γυρνάμε τη διαμόρφωση της θύρας, όσον αφορά τα VLAN που περνάνε, στην κανονική (περνάνε όλα τα VLAN):

```
Switch(config-if)# no switchport trunk allowed vlan
```

Σημειώνεται ότι το `allowed vlan` είναι διαφορετική ρύθμιση από το `vlan pruning` που θα δούμε ποιο κάτω.

Για να απενεργοποιήσουμε το DTP σε μια θύρα δίνουμε:

```
Switch(config-if)# switchport nonnegotiate
```

Για να δούμε την κατάσταση μιας θύρας, όσον αφορά τις παραμέτρους μεταγωγής (αν είναι trunk ή access, σε ποιο VLAN ανήκει αν είναι `access`, ποιο είναι το Native VLAN της αν είναι `trunk`, το voice VLAN και ποια VLAN είναι `allowed`) δίνουμε:

```
Switch# show interfaces type [slot#]/port# switchport
```

Στην παραγόμενη από αυτή την εντολή πληροφορία, ως `administrative mode` αναφέρεται τι έχουμε καθορίσει στη διαμόρφωση του μεταγωγέα και ως `operational mode` αναφέρεται τι έχει καταφέρει να ενεργοποιήσει ο μεταγωγέας (πως δουλεύει αυτή τη στιγμή η θύρα). Η διαφορά μεταξύ των δύο οφείλεται τυπικά στο DTP. Αν παραλείψουμε το όνομα του *interface*, βλέπουμε τη διαμόρφωση για όλες τις θύρες του μεταγωγέα, μια σελίδα ανά θύρα. Με την εντολή:

```
Switch# show interfaces trunk
```

βλέπουμε συνοπτική πληροφορία για όλες τις θύρες που είναι σε διαμόρφωση trunk. Συγκεκριμένα βλέπουμε σε τι DTP διαμόρφωση είναι, ποιο είναι το πρωτόκολλο tagging (dot1q), σε τι κατάσταση είναι (`trunk` ή `access`), ποιο είναι το native VLAN, ποια VLAN επιτρέπονται και ποια VLAN είναι ενεργά σε αυτές.

Για να ορίσουμε το διαχειριστικό VLAN και να του δώσουμε διεύθυνση IP δίνουμε:

```
Switch(config)# interface vlan VLAN#
Switch(config-if)# ip address ip_address subnet_mask
Switch(config-if)# no shutdown
```

Για παράδειγμα, για να ορίσουμε ως διαχειριστικό VLAN το VLAN100 και να του δώσουμε τη διεύθυνση IP 192.168.100.250/24 δίνουμε:

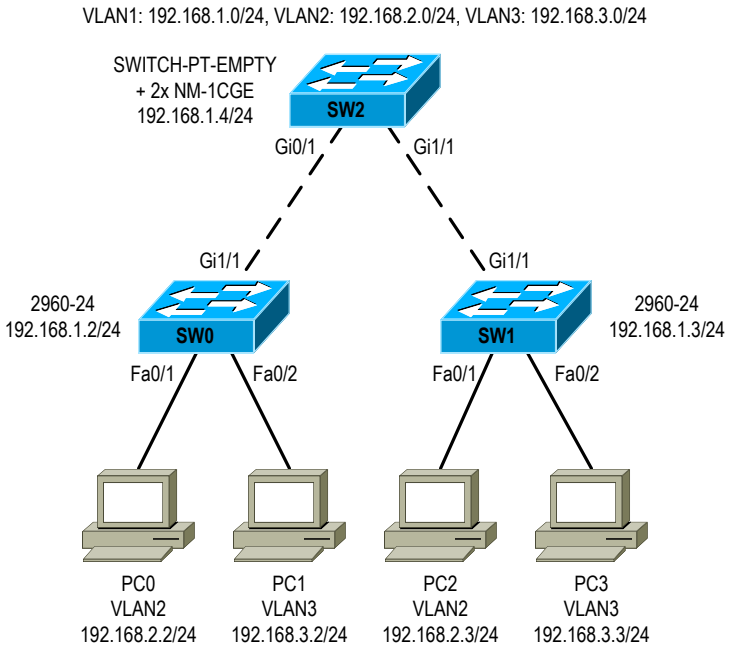
```
Switch(config)# interface vlan100
Switch(config-if)# ip address 192.168.100.250 255.255.255.0
Switch(config-if)# no shutdown
```

Για να δούμε ποιο είναι το διαχειριστικό VLAN του μεταγωγέα και τη διεύθυνση IP αυτού δίνουμε:

```
Switch# show ip interface
```

11.7 Εργαστηριακή άσκηση

Στην άσκηση αυτή θα παραμετροποιηθούν τρεις μεταγωγείς και τέσσερεις σταθμοί εργασίας, προκειμένου να δημιουργηθεί ένα δίκτυο με τρία VLAN, το VLAN1, το VLAN2 και το VLAN3. Στο ακόλουθο διάγραμμα δικτύου (**Εικόνα 11.5**) φαίνονται οι συνδέσεις των συσκευών, τα VLAN και οι διευθύνσεις δικτύου αυτών, οι διευθύνσεις IP των σταθμών εργασίας και οι διαχειριστικές διευθύνσεις IP των μεταγωγέων. Η άσκηση θα γίνει με το λογισμικό προσομοίωσης Cisco Packet Tracer και με εντολές στο Cisco CLI.



Εικόνα 11.5 Διάγραμμα δικτύου για την εργαστηριακή άσκηση **11.7**

Αφού γίνουν οι συνδέσεις, ζητούνται:

α) Σε κάθε μεταγωγέα να οριστούν το *hostname*, τα VLAN και η IP διεύθυνση διαχείρισης. Το VLAN διαχείρισης να παραμείνει το vlan1 και οι συνδέσεις των μεταγωγέων να είναι κορμού (*trunk*), ενώ οι συνδέσεις με τους σταθμούς να είναι πρόσβασης (*access*) και στο οριζόμενο VLAN. Οι συνδέσεις access να είναι portfast.

β) Σε κάθε σταθμό εργασίας να οριστεί η διεύθυνση δικτύου (δεν χρειάζεται *default gateway*).

γ) Θα πρέπει σταθμοί εργασίας που βρίσκονται στο ίδιο VLAN να κάνουν ping μεταξύ τους.

δ) Θα πρέπει οι μεταγωγείς να κάνουν ping μεταξύ τους.

ε) Θα πρέπει οι σταθμοί εργασία να κάνουν telnet στους μεταγωγείς.

12. Το Πρωτόκολλο VTP

12.1 Εισαγωγή

Τα VLAN αποτελούν πολύ σημαντική διαμόρφωση για ένα δίκτυο. Απώλεια ενός VLAN ισοδυναμεί με απώλεια ολόκληρης περιοχής σε ένα συμβατικό δίκτυο. Ανάλογα, διαφορές στη διαμόρφωση των VLAN στους μεταγωγείς μπορούν να δημιουργήσουν σοβαρά προβλήματα λειτουργίας και ασφάλειας. Επιπλέον, ο σωστός προγραμματισμός και συντήρηση όλων των VLAN σε όλους τους μεταγωγείς μπορεί να αποτελεί σοβαρό φόρτο για τους διαχειριστές ενός μεγάλου δικτύου. Για παράδειγμα σε ένα δίκτυο με 80 μεταγωγείς και 20 VLAN, απαιτούνται 80 x 20 = 1600 εντολές να δοθούν με το χέρι σε όλους τους μεταγωγείς, χωρίς να υπολογιστούν οι εντολές εισόδου στη διαμόρφωση των μεταγωγέων. Και η προσθήκη ενός VLAN σε αυτό το δίκτυο απαιτεί τουλάχιστον 40 εντολές.

Για την αποτελεσματική αντιμετώπιση των παραπάνω, η Cisco έχει αναπτύξει το VLAN *Trunking Protocol*. Αντίθετα με αυτό που υποδηλώνει το όνομά του, το VTP δεν είναι ένα πρωτόκολλο για τη δημιουργία των γραμμών κορμού. Είναι ένα πρωτόκολλο που τρέχει πάνω από γραμμές κορμού και βασικός σκοπός του είναι να συγχρονίζει τη διαμόρφωση των VLAN (τη VLAN *database*) σε όλους τους μεταγωγείς, έτσι ώστε να διασφαλίζεται ενιαία διαμόρφωση και να αποφεύγονται προβλήματα από ασυμφωνίες στη διαμόρφωση των VLAN. Επιπλέον, όταν προστίθεται ή αφαιρείται ένα VLAN στο δίκτυο, φροντίζει για την ανάλογη διαμόρφωση των γραμμών κορμού ώστε αυτό να περνά. Το VTP τρέχει πάνω από το dot1q, χρησιμοποιεί πλαίσια πολυεκπομπής (*multicast*) και κόβεται από τους δρομολογητές.
Συνοψίζοντας, το VTP βοηθάει στα ακόλουθα:

- Διαχείριση – Μεταφορά της διαμόρφωσης των VLAN σε όλους τους μεταγωγείς (ελαχιστοποίηση διαχειριστικού φόρτου).
- Διαχείριση – Μοντέλο πελάτη / εξυπηρετητή με δυνατότητα για πολλαπλούς εξυπηρετητές.
- Ασφάλεια – Προστασία από λάθη και ανομοιομορφία στη διαμόρφωση των VLAN.
- Ασφάλεια – Προστασία από την εμφάνιση ‘ξένου’ μεταγωγέα με διαφορετική διαμόρφωση VLAN που θα μπορούσε να δημιουργήσει προβλήματα στο δίκτυο.

Όπως ειπώθηκε, το VTP υπάρχει μόνο σε μεταγωγείς Cisco. Άλλοι κατασκευαστές μεταγωγέων έχουν υιοθετήσει το Multiple VLAN Registration Protocol (MVRP), που αποτελεί το πρότυπο IEEE 802.1ak (το οποίο υποστηρίζεται και από τη Cisco).

12.2 Λειτουργικά χαρακτηριστικά VTP

Το VTP ορίζει τις ακόλουθες έννοιες:

- **VTP Domain.** Είναι ένα σύνολο από συνδεδεμένους μεταγωγείς που τελούν υπό ενιαία διαχείριση και οι οποίοι επικοινωνούν μεταξύ τους με το VTP προκειμένου να ανταλλάσουν πληροφορία διαμόρφωσης VLANs (να συγχρονίζουν δηλαδή τη VLAN database). Το VTP Domain έχει ένα αλφαριθμητικό όνομα, το οποίο προτερόθετα είναι κενό (*null*). Εφόσον οι μεταγωγείς είναι συνδεδεμένοι με γραμμές κορμού, ο πρώτος μεταγωγέας που θα αποκτήσει VTP domain θα το μεταδώσει αυτόματα στους άλλους, εντός της ίδιας περιοχής δικτύου 2^{ου} Επιπέδου.
- **VTP Domain Password.** Ένα domain μπορεί να διαθέτει και ένα κωδικό ασφαλείας, έτσι ώστε μεταγωγείς που δεν τον διαθέτουν να μην μπορούν να επικοινωνήσουν (όσον αφορά το VTP) με τους υπολοίπους. Με αυτό τον τρόπο προστατεύεται η VLAN database των μεταγωγέων που μετέχουν σε ένα domain από μη εξουσιοδοτημένη επικοινωνία και αλλαγές. Ο κωδικός κρυπτογραφεί μόνο την επικοινωνία VTP και δεν επηρεάζει τα πακέτα δεδομένων. Προτερόθετα ο κωδικός είναι κενός και η επικοινωνία VTP είναι ελεύθερη.
- **VTP Modes.** Όσον αφορά το VTP, ένας μεταγωγέας μπορεί να έχει το ρόλο του εξυπηρετητή (server), του πελάτη (client), ή να είναι διάφανος (transparent).

  Οι VTP servers αποθηκεύουν την VLAN database στη flash και την διανέμουν στους άλλους μεταγωγείς που τρέχουν VTP. Σε αυτούς μπορούν να προστεθούν, να αφαιρεθούν ή να μετονομαστούν VLAN. Παράγουν και αναδιανέμουν VTP advertisements (βλ. παρακάτω). Πρέπει να υπάρχουν τουλάχιστον δύο server σε κάθε domain για λόγους βλαβοαντοχής. Αυτή η διαμόρφωση είναι προτερόθετα ενεργή στους μεταγωγείς της Cisco, δηλαδή όλοι οι μεταγωγείς είναι αρχικά VTP servers.

  Οι VTP clients δουλεύουν όπως οι servers, αλλά δεν μπορούν να κάνουν αλλαγές στην VLAN database και δεν την αποθηκεύουν. Οι clients ανακτούν τα VLAN από τους servers του domain όταν ανοίγουν και φροντίζουν να αναδιανέμουν τα VTP advertisements σε άλλους μεταγωγείς (servers ή clients). Η διαμόρφωση client πρέπει να ρυθμιστεί.

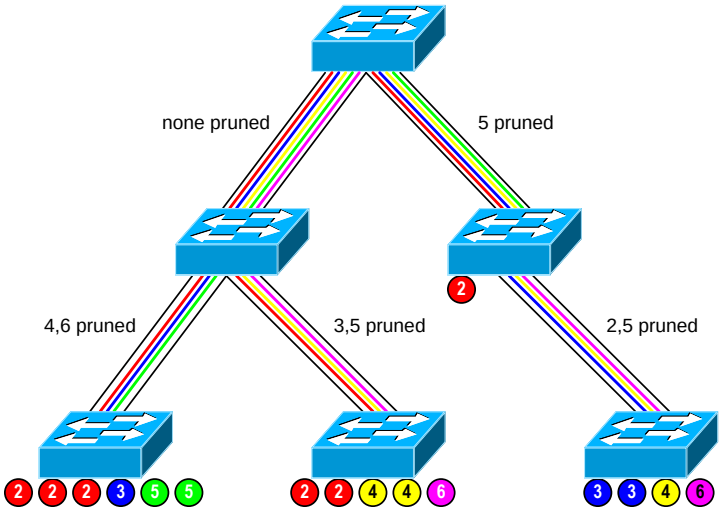
  Στη διαμόρφωση VTP Transparent ένας μεταγωγέας αναδιανέμει τα VTP advertisements, αλλά δεν μετέχει με άλλο τρόπο στην ανταλλαγή στοιχείων μέσω VTP. Αυτός ο μεταγωγέας διατηρεί (και αλλάζει) τη δική του VLAN database στη flash. Η διαμόρφωση transparent πρέπει να ρυθμιστεί.
- **VTP Messages.** Το VTP χρησιμοποιεί μια ιεραρχία από μηνύματα για τη διανομή και συγχρονισμό της VLAN database σε όλους τους μεταγωγείς που μετέχουν στο ίδιο VTP Domain. Τα μηνύματα αυτά μπορεί να είναι:

  Advertisement requests. Αποτελεί μήνυμα που στέλνει ένας client για να λάβει την VLAN database από ένα server.

  Subset advertisement. Είναι το μήνυμα που στέλνει ένας server σε απάντηση του request ενός client. Περιλαμβάνει αναλυτική πληροφορία για τη διαμόρφωση των VLAN, όμως VIDs, ονόματα, τύπους κα.

  Summary advertisement. Τα μηνύματα αυτά στέλνονται προτερόθετα κάθε πέντε λεπτά από ένα μεταγωγέα και όταν συμβεί κάποια αλλαγή στη VLAN database. Περιλαμβάνουν περιληπτική πληροφορία για τα VLAN.

- **VTP Version.** Υπάρχουν τρεις εκδόσεις του VTP, η 1, η 2 και η 3. Οι μεταγωγείς ενός domain πρέπει να τρέχουν την ίδια έκδοση VTP. Η προτερόθετη έκδοση είναι η 1. Οι τρεις εκδόσεις διαφέρουν μεταξύ τους σε αρκετές λεπτομέρειες, με σημαντικότερη το ότι η 1 υποστηρίζει πολλαπλά domains ενώ η 2 μόνο ένα.
- **VTP Revision Number.** Κάθε μεταγωγέας που τρέχει VTP διατηρεί ένα αριθμό ενημέρωσης, ο οποίος προτερόθετα είναι 0. Κάθε φορά που γίνεται μια αλλαγή στη VLAN database (με την προσθήκη, αφαίρεση ή αλλαγή ενός VLAN), ο αριθμός αυτός αυξάνει κατά 1. Με αυτόν τον τρόπο οι μεταγωγείς καταλαβαίνουν αν έχουν την τελευταία έκδοση της database ή όχι και ενημερώνονται. Αλλαγή στο όνομα του domain μηδενίζει τον αριθμό αυτό. Αν ένας server λάβει ένα μήνυμα VTP από άλλον με μικρότερο revision number, θα του απαντήσει με ένα μήνυμα με το δικό του revision number. Ο πρώτος θα καταλάβει έτσι ότι δεν διαθέτει την πιο ενημερωμένη VLAN database και θα την ζητήσει από τον server που την έχει. Κατά αυτή την έννοια το VTP revision number μοιάζει λίγο με το sequence number του TCP.
- **VTP Pruning.** Το VTP pruning είναι μια δυνατότητα των μεταγωγέων Cisco με την οποία μπορούν να προσθαφαιρούν VLANs από γραμμές κορμού (προτερόθετα όλα τα VLAN περνούν από μια γραμμή κορμού). Το VTP δίνει τη δυνατότητα στους μεταγωγείς να γνωρίζουν ποια VLAN είναι ενεργά στην κατεύθυνση μιας σύνδεσης κορμού και έτσι κίνηση που ανήκει σε VLAN που δεν είναι ενεργά να μην την προωθούν, μειώνοντας έτσι το φόρτο των γραμμών κορμού και την πιθανότητα να αποτελέσουν αυτές σημείο συμφόρησης στο δίκτυο (βλ. **Εικόνα 12.1**). Διαφορετικά ένας μεταγωγέας πρέπει να αναμεταδίδει ευρυεκπομπές, πολυεκπομπές και μονοεκπομπές άγνωστου παραλήπτη σε όλες τις συνδέσεις κορμού, ακόμα και αν ο διπλανός μεταγωγέας τελικά τα απορρίψει. Επιπλέον, το pruning μειώνει το μέγεθος του Spanning Tree και το φορτίο που βάζει το PVST ή Rapid-PVST, καθώς δεν δημιουργούνται δομές και δεν εκπέμπονται BPDUs για μη ενεργά VLAN.
  Το VTP pruning είναι προτερόθετα ενεργό για όλα τα VLAN (εκτός του VLAN1 το οποίο δεν μπορεί να γίνει prune), μπορεί όμως τα περιοριστεί σε κάποια από αυτά (δηλαδή κάποια να μην γίνονται ποτέ prune). Κάθε μεταγωγέας μεταδίδει τα ενεργά του VLAN στους γειτονικούς (και αυτοί στους δικούς τους). Αν γίνει αλλαγή (π.χ. ένα VLAN τοποθετηθεί για πρώτη φορά σε μια θύρα), τα ξαναμεταδίδει. Οι γειτονικά μεταγωγείς «κόβουν» τα μη-ενεργά VLAN από τις γραμμές κορμού προς αυτόν. Σημειώνεται ότι η ενεργοποίηση/απενεργοποίηση του VTP pruning σε ένα VTP server ενός domain, το ενεργοποιεί/απενεργοποιεί σε όλους τους μεταγωγείς του domain αυτού.



Εικόνα 12.1 Αποτελέσματα VTP Pruning

Για τη λειτουργία του VTP απαραίτητες προϋποθέσεις είναι τα εξής:

- Οι μεταγωγείς πρέπει να συνδέονται με γραμμές κορμού (trunk).
- Το VTP μεταδίδει την πληροφορία του μέσα από το VLAN1. Επομένως το VLAN1 πρέπει να υπάρχει και να περνάει μέσα από όλες τις γραμμές κορμού, που είναι και η κανονική λειτουργία.
- Πρέπει να είναι ορισμένο το VTP Domain και να είναι κοινό σε όλους τους μεταγωγείς. Αν υπάρχει VTP password πρέπει επίσης να είναι κοινό.
- Πρέπει να υπάρχει τουλάχιστον ένας VTP server. Για λόγους βλαβοαντοχής προτείνεται να έχουν οριστεί τουλάχιστον δύο.
- Ένας μεταγωγέας που υποστηρίζει το VTP v2 μπορεί να λειτουργήσει στο ίδιο domain με έναν μεταγωγέα που υποστηρίζει v1 μόνο αν απενεργοποιηθεί το v2.

12.3 Ενεργοποίηση VTP

Για την ενεργοποίηση του VTP σε ένα νέο δίκτυο, προτείνονται τα ακόλουθα βήματα:

α) Ενεργοποιούμε το VTP <u>πριν</u> ορίσουμε VLANs και <u>αφού</u> ορίσουμε τις θύρες διασύνδεσης των μεταγωγέων ως κορμού.

β) Εγκαθιστούμε τον πρώτο μεταγωγέα που θα έχει το ρόλο του VTP server, ορίζουμε σ’ αυτό το VTP domain/password/version/pruning. Επιλέγουμε ποια VLAN θα συμμετέχουν στο VTP pruning (αν δεν μετέχουν όλα).

γ) Εγκατάσταση του δεύτερου μεταγωγέα που θα έχει το ρόλο ο VTP server, ορισμός σ’ αυτό του VTP password/version (το domain το έχει πάρει αυτόματα).

δ) Εγκατάσταση των υπολοίπων μεταγωγέων, ορισμός VTP σε αυτούς σε client mode και του password/version (το domain το έχουν πάρει αυτόματα).

Για την ενεργοποίηση του VTP σε ένα παλαιό δίκτυο, προτείνονται τα ακόλουθα βήματα. Σημειώνεται ότι όλοι οι μεταγωγείς είναι προτερόθετα σε server mode.

α) Ενεργοποιούμε το VTP πριν ορίσουμε VLANs και αφού ορίσουμε τις θύρες διασύνδεσης των switches ως κορμού. Αν υπάρχουν ήδη VLANs, συγχρονίζουμε πρώτα με το χέρι όλα τα VLAN σε όλους τους μεταγωγείς.
β) Στον πρώτο μεταγωγέα που θα είναι server ορίζουμε το VTP domain (αυτόματα όλα τα switches παίρνουν το νέο domain) και το password, version και pruning.
γ) Στον δεύτερο μεταγωγέα που θα είναι server, ορίζουμε password, version.
δ) Στους υπόλοιπους μεταγωγείς, ορίζουμε client mode, password, version.

Σημειώνεται ότι στην περίπτωση που προσθέσουμε σε ένα δίκτυο μεταγωγέα που ήταν πριν ενεργός σε άλλο, η εκκαθάριση της nvram δεν σβήνει την VLAN database και αν το revision number αυτού του μεταγωγέα είναι μεγαλύτερο από του υπόλοιπου δικτύου θα μπορούσε να αλλάξει τα VLAN των υπολοίπων. Γι' αυτό είναι καλό να σβήνουμε την VLAN database (vlan.dat) ενός μεταγωγέα που προσθέτουμε σε ένα δίκτυο, να του δίνουμε το σωστό VTP domain και password και μετά να τον συνδέουμε.

12.4 Ρυθμίσεις VTP σε μεταγωγείς με Cisco CLI

Για τον καθορισμό του vtp mode:

```
Switch(config)# vtp mode {off | client | server | transparent }
```

Υπενθυμίζεται ότι server είναι η προτερόθετη ρύθμιση. Για παράδειγμα, για να μπει σε client mode ένας μεταγωγέας δίνουμε:

```
Switch(config)# vtp mode client
```

Για τον καθορισμό του ονόματος του VTP domain δίνουμε:

```
Switch(config)# vtp domain name
```

Για παράδειγμα:

```
Switch(config)# vtp domain d1
```

Για την ενεργοποίηση του VTP v2, ανάλογα με την έκδοση του μεταγωγέα:

```
Switch(config)# vtp v2-mode
```

ή σε κάποιους μεταγωγείς:

```
Switch(config)# vtp version 2
```

Για τον ορισμό του VTP password δίνουμε:

```
Switch(config)# vtp password password
```

Για παράδειγμα:

```
Switch(config)# vtp password p1
```

Για τη γενική ενεργοποίηση του VTP pruning δίνουμε:

```
Switch(config)# vtp pruning
```

Για επιλογή των VLAN που θα γίνονται prune ανά γραμμή κορμού:

```
Switch(config-if)# switchport trunk pruning vlan vlan-list
```

Για επισκόπηση της κατάστασης του VTP και στατιστικά:

```
Switch# show vtp status
Switch# show vtp counters
```

Για επισκόπηση των VLAN που γίνονται prune:

```
Switch# show interface type [slot#]/port# switchport
Switch# show interfaces trunk
```

12.5 Εργαστηριακή άσκηση

Σε αυτή την εργαστηριακή άσκηση θα γίνει διαμόρφωση του VTP στο δίκτυο της εργαστηριακής άσκησης 11.7. Η άσκηση θα γίνει με το λογισμικό προσομοίωσης Cisco Packet Tracer και με εντολές στο Cisco CLI. Ζητούμενο είναι να ρυθμιστεί ως VTP server ο μεταγωγέας SW2, ενώ οι μεταγωγείς SW0 και SW1 ως clients (υπενθυμίζεται ότι σε ένα πραγματικό δίκτυο είναι θεμιτό να υπάρχουν τουλάχιστον δύο VTP servers, για λόγους βλαβοαντοχής). Συγκεκριμένα ζητείται:

α) Ο μεταγωγέας SW2 να ρυθμιστεί ως VTP server με VTP domain «d1» και VTP password «p1» (χωρίς τα εισαγωγικά).
β) Οι μεταγωγείς SW0 και SW1 να ρυθμιστούν ως VTP clients, στο ίδιο domain και με το ίδιο password.
γ) Η έκδοση του VTP να είναι v2.
δ) Να είναι ενεργό το VTP pruning σε όλο το δίκτυο.
ε) Να επιδειχθεί η σωστή λειτουργία του VTP με την προσθαφαίρεση του vlan 3 και την επισκόπηση της προσθήκης του και της αφαίρεσής του από τη VLAN database των μεταγωγέων.
στ) Να επιδειχθεί η λειτουργία του VTP pruning προσθέτοντας το vlan 3, κάνοντας επισκόπηση των ενεργών VLAN στις θύρες κορμού των μεταγωγέων, βάζοντας

στη θύρα fa0/3 του μεταγωγέα SW0 ένα σταθμό εργασίας στο vlan 3 και κάνοντας επισκόπηση για το pruning ή μη του vlan 3 στις θύρες κορμού.

13. Δρομολόγηση μεταξύ VLAN

13.1 Εισαγωγή

Όπως έχει επανειλημμένα αναφερθεί στις προηγούμενες ενότητες, η εισαγωγή των VLAN στο δίκτυο το κατακερματίζει σε ξεχωριστούς τομείς ευρυεκπομπής (broadcast domains), οι οποίες δεν επικοινωνούν μεταξύ τους στο 2^{ο} Επίπεδο δικτύου (Ethernet), σαν να είναι πραγματικά ξεχωριστά δίκτυα. Για να γίνει δυνατή η επικοινωνία μεταξύ αυτών, πρέπει να γίνει δρομολόγηση στο τρίτο επίπεδο δικτύου με χρήση δρομολογητών. Παρά την αυξημένη πολυπλοκότητα και καθυστέρηση στη μεταγωγή που εισάγει αυτό, είναι θεμιτό για πολλούς λόγους:

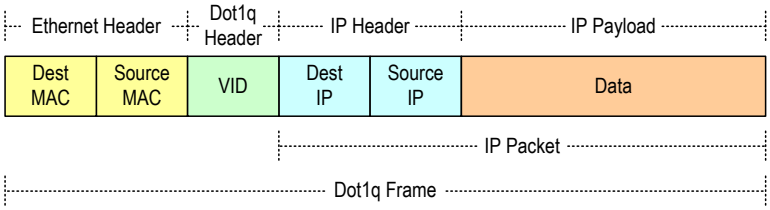
- Η μεταγωγή γίνεται πια από δρομολογητές στο 3^{ο} επίπεδο του δικτύου και έτσι έχουμε περιορισμό του εύρους των ευρυεκπομπών και μεγαλύτερη κλιμακοθεσιμότητα (το δίκτυο μπορεί να γίνει μεγαλύτερο, με περισσότερος σταθμούς).
- Τα VLAN γίνονται ξεχωριστά *subnets*. Αυτό προσφέρει τα ακόλουθα πλεονεκτήματα:
    - Μπορούμε να δομήσουμε το δίκτυό μας στο 3ο επίπεδο, δημιουργώντας δίκτυα, υποδίκτυα (*subnets*) και υπερδίκτυα (*supernets*), έχοντας τη δυνατότητα να αναφερόμαστε σε πολλαπλά δίκτυα με μία διεύθυνση δικτύου.
    - Μπορούμε να εισάγουμε κανόνες διακριτικής πρόσβασης μεταξύ των υποδικτύων, με κανόνες διευθύνσεων ή/και πρωτοκόλλων 3^{ου}, 4^{ου}, έως και 7^{ου} Επίπεδου δικτύου.
    - Μπορούμε να χρησιμοποιήσουμε πρωτόκολλα δρομολόγησης για την επικοινωνία μεταξύ των υποδικτύων. Τα πρωτόκολλα δρομολόγησης εισάγουν σημαντική ‘εξυπνάδα’ στο δίκτυο, καθιστώντας δυνατή τη χρήση πολλαπλών διαδρομών, με δυνατότητες βλαβοαντοχής, κατανομής φορτίου και δυναμικής απόκρισης στο φορτίο του δικτύου.

Στην πραγματικότητα, η μεταγωγή στο 3^{ο} Επίπεδο προηγήθηκε των VLAN και όχι το ανάποδο. Όπως είδαμε σε προηγούμενη ενότητα, πρώτα χρειάστηκε να χωρίσουμε το δίκτυο σε πολλαπλούς τομείς ευρυεκπομπής και υποδίκτυα, έτσι ώστε να το μεγαλώσουμε και μετά εμφανίστηκαν τα VLAN.

Αρχικά η δρομολόγηση μεταξύ των διαφορετικών υποδικτύων του δικτύου μας γινόταν με LAN routers, όπου ο δρομολογητής διέθετε μία διεπαφή (και IP διεύθυνση), ανά φυσικό υποδίκτυο. Με την εισαγωγή των ιδεατών υποδικτύων (VLAN), η ανάγκη αυτή δεν αλλάζει. Ο δρομολογητής πρέπει να διαθέτει διαφορετική διεπαφή (και διεύθυνση IP) για κάθε VLAN. Σε αντίθεση όμως με την παλαιά αρχιτεκτονική, τώρα το δίκτυό μας μπορεί να διαθέτει δεκάδες ή και εκατοντάδες VLAN, αν λάβουμε υπόψη ότι τα δημιουργούμε και για πολλούς άλλους λόγους πέραν της ανάγκης να περιορίσουμε τις ευρυεκπομπές (βλ. ενότητα ‘Εισαγωγή στα VLAN’). Επομένως ένας δρομολογητής που θα διέθετε μία διεπαφή

για κάθε VLAN θα έπρεπε να διαθέτει δεκάδες ή και εκατοντάδες διεπαφές, κάτι που θα τον καθιστούσε πολύ ακριβό.

Πιο καλή ιδέα θα ήταν να εκμεταλλευτούμε τη δυνατότητα των δρομολογητών να τρέξουν σε μια διεπαφή τους πρωτόκολλο κορμού dot1q. Με τη χρήση αυτού, ένας δρομολογητής μπορεί να γνωρίζει σε ποιο VLAN ανήκει ένα εισερχόμενο σε μια διεπαφή του πακέτο IP, από την κεφαλίδα 2^{ου} Επιπέδου του dot1q, **Εικόνα 13.1**. Άρα, αυτό που μένει για να μπορεί να δρομολογεί μεταξύ των VLAN, είναι ένας τρόπος να «αντιστοιχίσει» μεταξύ των VLAN και της διεύθυνσης IP που πρέπει να διαθέτει για καθένα από αυτά.



Εικόνα 13.1 IP μέσα σε dot1q

Δηλαδή η διεπαφή αυτή που τρέχει dot1q θα πρέπει να διαθέτει πολλαπλές διευθύνσεις από πολλαπλά υποδίκτυα διαφορετικών περιοχών ευρυεκπομπής, κάτι που δεν είναι δυνατό σε μια και μοναδική φυσική διεπαφή. Για να ξεπεραστεί αυτό το εμπόδιο, οι δρομολογητές μπορούν να δημιουργήσουν πολλαπλές 'λογικές υποδιεπαφές' (*logical subinterfaces*) στο λογισμικό, όλες συνδεδεμένες με την ίδια φυσική διεπαφή, μία για κάθε VLAN που θέλουμε να δρομολογούμε. Αυτές έχουν τα ακόλουθα χαρακτηριστικά:

α) Μπορούν να δημιουργηθούν όσες χρειάζονται, ανάλογα με τον αριθμό των VLAN.

β) Κάθε μία συνδέεται με ένα μόνο VLAN και η συσχέτιση γίνεται με το VID, το οποίο ορίζεται στα χαρακτηριστικά της. Οι λογικές «ιδεατές» υποδιεπαφές δηλαδή συνδέονται με τα ιδεατά δίκτυα (VLAN), ένα προς ένα.

γ) Για να φαίνεται ότι όλες οι λογικές υποδιεπαφές σχετίζονται με την ίδια φυσική διεπαφή, το όνομά τους έχει συνήθως τη μορφή 'όνομα φυσικής διεπαφής'.'αριθμός λογικής υποδιεπαφής'. Για παράδειγμα για την διεπαφή g0/0 ενός δρομολογητή, δύο λογικές διεπαφές θα μπορούσαν να ονομάζονται:

g0/0.1 και **g0/0.2**

Αν και δεν είναι υποχρεωτικό, συνηθίζεται ο αριθμός υποδιεπαφής να είναι ίδιος με το VID του VLAN που σχετίζεται.

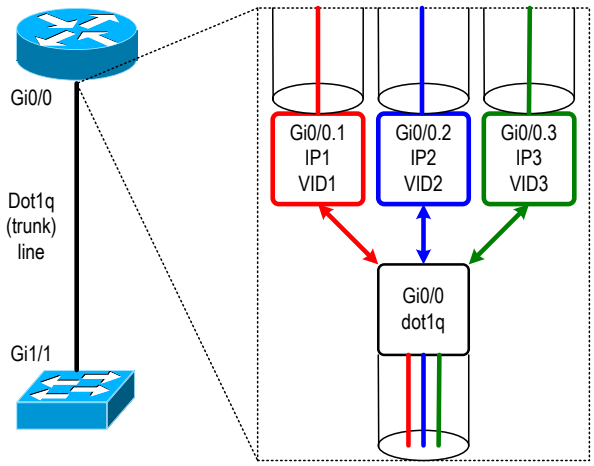
δ) Η «μαμά» φυσική διεπαφή τρέχει dot1q, όχι Ethernet.

ε) Οι λογικές υποδιεπαφές μιας φυσικής διεπαφής σηκώνονται μόλις σηκωθεί πρωτόκολλο dot1q στη φυσική διεπαφή.

στ) Κάθε λογική υποδιεπαφή διαθέτει διεύθυνση IP εντός του subnet (network ID) του VLAN με το οποίο σχετίζεται.

ζ) Η δρομολόγηση και μεταγωγή ενός εισερχόμενου πλαισίου dot1q σε μια διεπαφή κορμού γίνεται ως ακολούθως:

i) Διαβάζεται το VID που αναφέρεται στην κεφαλίδα dot1q.
ii) Αποθυλακώνεται (*decapsulation*) το πακέτο IP που βρίσκεται μέσα και προωθείται στη λογική υποδιεπαφή που σχετίζεται με αυτό το VID, σαν να επρόκειτο για πραγματική φυσική διεπαφή, **Εικόνα 13.2**. Αν το πακέτο IP δεν προορίζεται για τον ίδιο τον δρομολογητή, γίνεται δρομολόγηση με αναφορά στον πίνακα δρομολόγησης και αποφασίζεται η διεπαφή εξόδου.



Εικόνα 13.2 Λογικές υποδιεπαφές και φυσικές διεπαφές

iii) Εφόσον η διεπαφή εξόδου είναι μια από τις λογικές υποδιεπαφές, το πακέτο IP ενθυλακώνεται σε Dot1q με το VID της υποδιεπαφής εξόδου και μέσα από τη φυσική διεπαφή εκπέμπεται στο δίκτυο.

η) Από την άποψη του υπόλοιπου δικτύου, η μόνη διαφορά με το να είχε ο δρομολογητής πολλαπλές φυσικές διεπαφές, μία για κάθε VLAN, είναι ότι ο δρομολογητής εμφανίζεται με την ίδια διεύθυνση MAC σε όλα τα υποδίκτυα, αυτή που έχει η φυσική του διεπαφή (δηλαδή οι λογικές υποδιεπαφές δεν διαθέτουν δική τους MAC διεύθυνση – προφανώς αφού πρόκειται και οντότητες 3ου επιπέδου δικτύου).
θ) Η θύρα του μεταγωγέα στον οποίο συνδέεται πρέπει να ρυθμιστεί ως θύρα κορμού (να τρέχει dot1q δηλαδή). Κανονικά, σε μια απλή σύνδεση ο δρομολογητής αντιμετωπίζεται από τους μεταγωγείς όπως οι σταθμοί πρόσβασης, δηλαδή η θύρα του μεταγωγέα που συνδέεται είναι θύρα πρόσβασης (access) και τρέχει απλό Ethernet. Άρα θα πρέπει να γίνει η αντίστοιχη ρύθμιση στον μεταγωγέα ώστε η θύρα να γίνει θύρα κορμού στατικά (οι δρομολογητές δεν υποστηρίζουν DTP).

Όταν ένας δρομολογητής έχει μία μόνο διεπαφή κορμού με το δίκτυο, μέσα από την οποία μπαίνει και βγαίνει όλη η κίνηση μεταξύ VLAN, λέμε ότι ο δρομολογητής είναι συνδεδεμένος ως '*router on-a-stick*' (από την αγγλική έκφραση *bird on-a-stick*). Προφανώς μια τέτοια διεπαφή αποτελεί για το δίκτυο τόσο σημείο συμφόρησης (για υψηλή κίνηση μεταξύ VLAN), όσο και μοναδικό σημείο αδυναμίας (στην περίπτωση που χαθεί η σύνδεση), όπως άλλωστε συμβαίνει και για ολόκληρο το δρομολογητή. Για τους λόγους αυτούς (και άλλους), έχουν αναπτυχθεί νεότερες αρχιτεκτονικές και

τεχνολογίες δικτύου που βασίζονται στην πολυεπίπεδη μεταγωγή (βλ. επόμενο κεφάλαιο).

13.2 Ρύθμιση Inter-VLAN Routing σε δρομολογητές με Cisco CLI

Για να δημιουργηθεί μια λογική υποδιεπαφή σε μια φυσική διεπαφή ενός δρομολογητή δίνουμε:

```
Router(config)# interface type port#.subinterface# [point | multipoint]
Router(config-subif)#
```

Ο αριθμός *subinterface#* μπορεί να είναι από 0 έως 2^{32} και δεν έχει κάποια λειτουργική σημασία. Χρησιμοποιείται μόνο για το διαχωρισμό των υποδιεπαφών. Ωστόσο, συνηθίζεται να είναι ίδιος με το VID του VLAN με το οποίο θα σχετίζεται η υποδιεπαφή. Η παράμετρος [**point** | **multipoint**] χρησιμοποιείται μόνο για σειριακές συνδέσεις και παραλείπεται για Ethernet συνδέσεις. Στη συνέχεια πρέπει να ρυθμιστεί η ενθυλάκωση σε dot1q και το VID του VLAN:

```
Router(config-subif)# encapsulation dot1q VID#
```

Για παράδειγμα, για να ορίσουμε δύο υποδιεπαφές στη φυσική θύρα **fa0/0** ενός δρομολογητή, μία στο **VLAN10** και μία στο **VLAN20**, με διευθύνσεις IP αντίστοιχα **172.16.1.1/24** και **172.16.2.1/24**, δίνουμε:

```
Router(config)# interface fa0/0
Router(config-if)# no shutdown
Router(config)# interface fa0/0.10
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# ip address 172.16.1.1 255.255.255.0
Router(config-subif)# interface fastethernet0/0.20
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# ip address 172.16.2.1 255.255.255.0
```

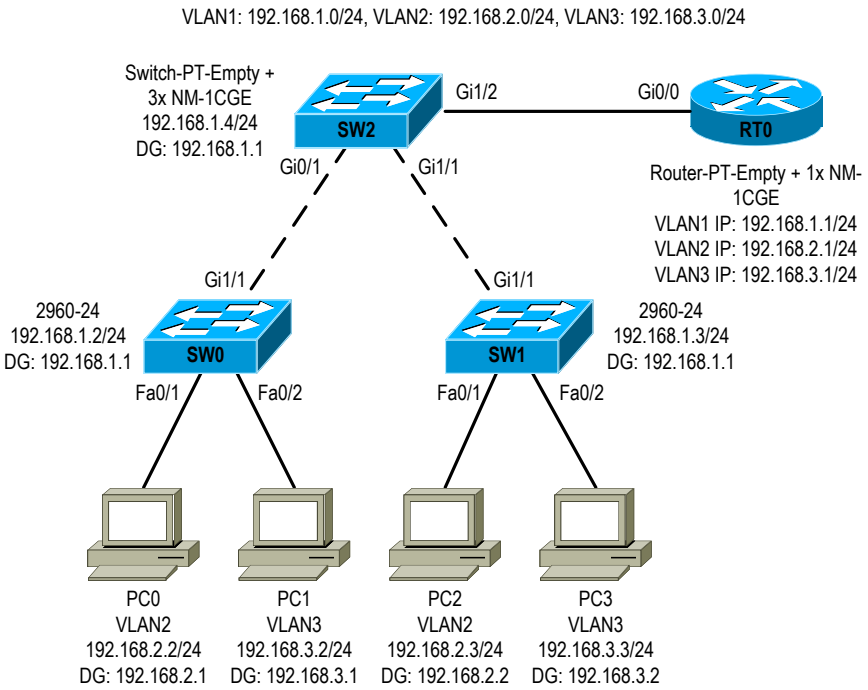
Υπενθυμίζεται ότι η θύρα του μεταγωγέα στον οποίο συνδέεται ο δρομολογητής θα πρέπει να έχει ρυθμιστεί ως θύρα κορμού (trunk) και ότι οι δρομολογητές τυπικά δεν υποστηρίζουν DTP. Σημειώνεται επίσης ότι όσον αφορά το STP οι δρομολογητές θεωρούνται τερματικοί σταθμοί, δηλαδή δεν παράγουν BPDUs και στη θύρα του μεταγωγέα μπορεί ενεργοποιηθεί portfast (βλ. ενότητα 'Ρυθμίσεις PVST+ και RPVST').

13.3 Εργαστηριακή άσκηση

Σε αυτή την άσκηση θα βελτιωθεί το δίκτυο της άσκησης 11.7 με την προσθήκη δρομολογητή, έτσι ώστε τα VLAN να επικοινωνούν μεταξύ τους μέσω αυτού (inter-VLAN routing). Ο δρομολογητής θα είναι συνδεδεμένος με σύνδεση κορμού στον

μεταγωγέα διανομής (SW2), θα διαθέτει τρεις διευθύνσεις IP, μία για κάθε ένα από τα τρία VLAN και όλοι οι σταθμοί εργασίας και οι μεταγωγείς θα έχουν ορισμένη τη διεύθυνση του δρομολογητή στο VLAN τους ως default gateway, έτσι ώστε όλοι να επικοινωνούν με όλους. Η άσκηση θα γίνει με το λογισμικό προσομοίωσης Cisco Packet Tracer και με εντολές στο Cisco CLI.

Το διάγραμμα δικτύου διαμορφώνεται όπως στην **Εικόνα 13.3**



Εικόνα 13.3 Διάγραμμα δικτύου για την εργαστηριακή άσκηση **13.3**

Επιπλέον των ζητουμένων των ασκήσεων 12.7 και 13.5, θα πρέπει:

α) Να προστεθεί μία κάρτα NM-1CGE στον μεταγωγέα SW2, στην οποία θα συνδεθεί ο δρομολογητής και να ρυθμιστεί η διεπαφή ως κορμού (trunk).

β) Να συνδεθεί ο δρομολογητής και να δημιουργηθούν και να παραμετροποιηθούν οι λογικές υποδιεπαφές της φυσικής διεπαφής του ώστε να τρέχουν dot1q και να έχουν τις οριζόμενες διευθύνσεις IP.

γ) Να ρυθμιστούν οι σταθμοί εργασίας και οι μεταγωγείς έτσι ώστε να έχουν ως default gateway τη διεύθυνση IP που έχει ο δρομολογητής στο VLAN τους.

δ) Όλες οι συσκευές (σταθμοί, μεταγωγείς και δρομολογητής) θα πρέπει να επικοινωνούν μεταξύ τους (να κάνουν ping ο ένας τον άλλο) και οι σταθμοί εργασίας να κάνουν telnet στους μεταγωγείς και τον δρομολογητή.

14. Ασφάλιση θυρών μεταγωγέα

Η τεχνολογία *port security* επιτρέπει να κλειδώσουμε τις θύρες ενός μεταγωγέα ως προς τις διευθύνσεις MAC που σχετίζονται με τη θύρα, εμποδίζοντας έτσι τη μη επιτρεπόμενη πρόσβαση στο τοπικό δίκτυο. Έτσι, αν μια διεύθυνση MAC, π.χ. **`00d0.d3ca.23b5`** θα έπρεπε να εμφανίζεται στη θύρα **`fa0/6`** και εμφανιστεί στη θύρα **`fa0/14`** τότε αυτό θεωρείται παραβίαση ασφαλείας. Επιπλέον παραβίαση ασφαλείας, θεωρείται και η εμφάνιση περισσότερων διευθύνσεων MAC σε μια θύρα από αυτές που περιμένουμε να συνδεθούν σε αυτή τη θύρα.

Ο διαχειριστής του μεταγωγέα έχει τη δυνατότητα να ελέγξει τι θα συμβεί στην περίπτωση παραβίασης ασφαλείας, όπως π.χ. την αποστολή ειδοποίησης σχετικά με την παραβίαση, τη διακοπή της αποστολής πλαισίων σε αυτή τη θύρα ή ακόμα και το κλείσιμο της θύρας (*port shutdown*). Θα πρέπει να σημειωθεί ότι το *port security* δεν μπορεί να εφαρμοστεί σε θύρες που είναι σε κατάσταση *trunk* (βλέπε κεφάλαιο VLAN).

14.1 Ρύθμιση του Port Security

Η ρύθμιση του port security γίνεται για κάθε μία θύρα ξεχωριστά χρησιμοποιώντας την εντολή `switchport`. Μια ενδεικτική διαμόρφωση είναι η παρακάτω:

```
Central#configure terminal
Central(config)#interface fa0/6
Central(config-if)#switchport mode access
Central(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
Central(config-if)#switchport port-security
Central(config-if)#switchport port-security maximum 1
Central(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
Central(config-if)#switchport port-security violation shutdown
Central(config-if)#switchport port-security mac-address ?
  H.H.H   48 bit mac address
  sticky  Configure dynamic secure addresses as sticky
Central(config-if)#switchport port-security mac-address sticky
Central(config-if)#end
Central#
%SYS-5-CONFIG_I: Configured from console by console

Central#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
```

```
                (Count)       (Count)        (Count)
-----------------------------------------------------------------
        Fa0/6        1          0                 0         Shutdown
        Fa0/8        2          2                 0         Restrict
-----------------------------------------------------------------
Central#
```

Επεξήγηση

Στο παραπάνω παράδειγμα αρχικά ρυθμίζουμε τη θύρα `fa0/6` έτσι ώστε να ανήκει στο `vlan 10`, δηλαδή να είναι access θύρα και όχι trunk (βλέπε κεφάλαιο VLAN). Στη συνέχεια με την εντολή `switchport port-security` ενεργοποιούμε το port security. Με την επιλογή `switchport port-security maximum` καθορίζουμε το μέγιστο αριθμό των συσκευών που μπορούν να σχετιστούν με μία θύρα. Με την ενεργοποίηση του port security αυτό αυτόματα γίνεται ίσο με 1, δηλαδή μόνο μία συσκευή μπορεί να σχετιστεί με μία θύρα.

Μία πολύ σημαντική εντολή είναι η `switchport port-security violation`. Η εντολή αυτή καθορίζει τι γίνεται αν σε μια θύρα εμφανιστεί πλαίσιο που δεν είναι σύμφωνο με το port security. Παρέχονται οι εξής επιλογές:

α) `Protect:` Αν επιλεγεί, τότε όταν ο αριθμός των διευθύνσεων που μαθαίνει ένας μεταγωγέας σε μια θύρα φτάσει το μέγιστο αριθμό των διευθύνσεων που έχουν καθοριστεί με την επιλογή `maximum,` οι επιπλέον διευθύνσεις δεν καταγράφονται στον πίνακα MAC του μεταγωγέα. Απαιτεί τη χρήση της επιλογής `sticky` που θα εξηγήσουμε παρακάτω. Τέλος, συνεχίζουν να προωθούνται τα πλαίσια από τις MAC διευθύνσεις που επιτρέπονται, ενώ απορρίπτονται τα πλαίσια από άλλες MAC διευθύνσεις.

β) `Restrict:` Σε αυτή την περίπτωση ο μεταγωγέας δημιουργεί ένα προειδοποιητικό μήνυμα ασφαλείας (syslog μήνυμα) και αυξάνει τον μετρητή παραβιάσεων (violation counter).

γ) `Shutdown:` Ο μεταγωγέας δημιουργεί ένα προειδοποιητικό μήνυμα ασφαλείας (syslog μήνυμα) και κλείνει τη θύρα. Προκειμένου η θύρα να γίνει πάλι λειτουργική, θα πρέπει ο διαχειριστής του να εισάγει την εντολή `no shutdown`. Στην περίπτωση που δεν προσδιοριστεί μία από τις παραπάνω επιλογές (`protect, restrict`) τότε η ενεργοποίηση του port security έχεις ως προεπιλογή το `shutdown`.

Σημείωση: Στην περίπτωση που συμβεί κάποια παραβίαση ασφαλείας όταν είναι ενεργοποιημένο το port security, μπορούμε να κάνουμε reset τη θύρα χρησιμοποιώντας την εντολή `errdisable recovery cause psecure-violation.`

Με την εντολή `switchport port-security mac-address` έχουμε δύο επιλογές: είτε να προσδιορίσουμε με στατικό τρόπο τη MAC διεύθυνση που επιτρέπεται να συσχετιστεί με μία θύρα, είτε να επιτρέψουμε στον μεταγωγέα να μάθει δυναμικά αυτή τη διεύθυνση και στη συνέχεια μόνος του να τη μετατρέψει σε στατική. Το τελευταίο επιτυγχάνεται με την επιλογή `sticky`, οπότε με την

αποθήκευση του `running-config` στο `startup-config`, οι διευθύνσεις που έχουν γίνει γνωστές δυναμικά ως **`sticky`**, εμφανίζονται σαν να έχουν ανατεθεί στατικά. Με αυτό τον τρόπο ο διαχειριστής μπορεί να καταγράψει με δυναμικό τρόπο τις MAC διευθύνσεις των συσκευών που ενώνονται με τον μεταγωγέα χωρίς να τις καταγράψει μία μία.

Αφού ολοκληρώσουμε την εισαγωγή του port security μπορούμε να εξετάσουμε τα αποτελέσματα των ρυθμίσεων μας με την εντολή **`show port-security`** που δείχνει σε μορφή πίνακα συνοπτικά τις ρυθμίσεις ανά θύρα.

14.2 Έλεγχος λειτουργίας του port-security

Για να ελέγξουμε την ορθή λειτουργία του port-security σε μια θύρα χρησιμοποιούμε την παρακάτω εντολή:

```
Central#show port-security interface fa0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0001.C94D.C485:10
Security Violation Count   : 0
```

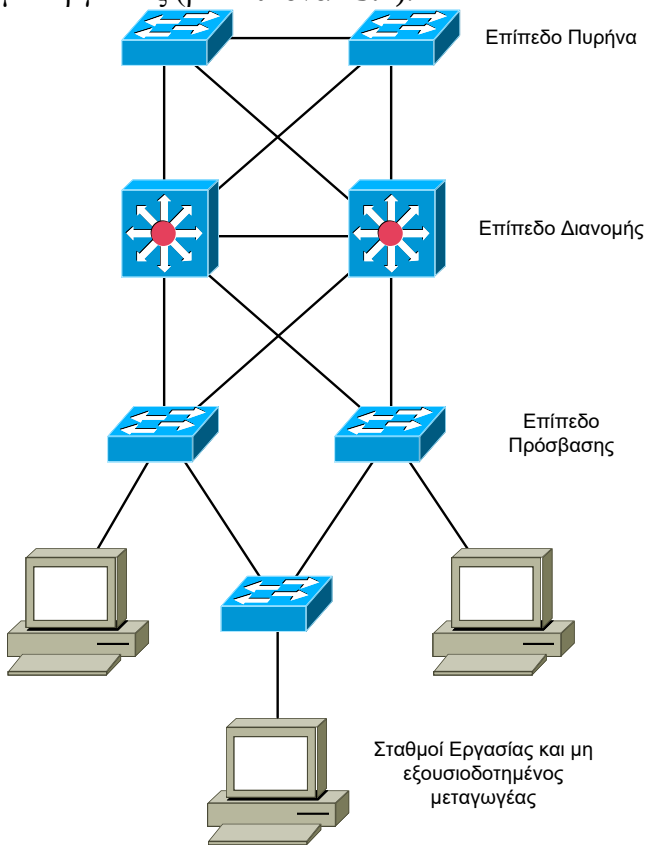
Σε αυτό το παράδειγμα, έχει ενεργοποιηθεί το port-security (`Secure-up`), η επιλογή σε μορφή παραβίασης ασφαλείας είναι `shutdown`, ο μέγιστος αριθμός MAC διευθύνσεων που μπορεί να μάθει ο μεταγωγέας είναι 1, αυτή τη στιγμή γνωρίζει τη διεύθυνση `0001.C94D.C485:10` στη θύρα, ενώ δεν υπάρχουν παραβιάσεις στην πόρτα (`Security Violation Count`).

15. Spanning Tree Protocol

15.1 Εισαγωγή

Όπως φαίνεται από τα παραπάνω, βασικό συστατικό των αξιόπιστων αρχιτεκτονικών δικτύου είναι οι πολλαπλές διαδρομές μεταξύ μεταγωγέων. Οι διαδρομές αυτές προκαλούν βρόχους στη διασύνδεση των δικτύων, είναι όμως απαραίτητες για τη βλαβοαντοχή σε περίπτωση απώλειας μεταγωγέα ή σύνδεσης. Οι βρόχοι μπορούν να σχηματιστούν στα ακόλουθα σημεία:

- Μεταξύ των μεταγωγέων του επιπέδου πρόσβασης και του επιπέδου διανομής. Στα σημείο αυτό δημιουργούνται συνήθως από την αρχιτεκτονική του δικτύου, είτε όταν κάθε μεταγωγέας πρόσβασης συνδέεται σε περισσότερους του ενός μεταγωγέων διανομής, είτε όταν ένας μεταγωγέας συνδέεται με έναν άλλο με πολλαπλές συνδέσεις, **Εικόνα 15.1**.
- Μεταξύ του επιπέδου διανομής και του επιπέδου πυρήνα. Στα σημείο αυτό δημιουργούνται συνήθως από την αρχιτεκτονική του δικτύου, είτε όταν κάθε μεταγωγέας διανομής συνδέεται σε περισσότερους του ενός μεταγωγέων πυρήνα, είτε όταν ένας μεταγωγέας συνδέεται με έναν άλλο με πολλαπλές συνδέσεις (βλ. **Εικόνα 15.1**).
- Μεταξύ μεταγωγέων που βρίσκονται στο επίπεδο πρόσβασης. Αυτό συμβαίνει συνήθως από λάθος, όταν π.χ. οι χρήστες συνδέσουν 'αυθαίρετα' στο δίκτυο ένα μεταγωγέα σε πολλαπλές θύρες πρόσβασης όπου κανονικά συνδέονται μόνο σταθμοί εργασίας (βλ. **Εικόνα 15.1**).



Εικόνα 15.1 Βρόχοι στα επίπεδα πρόσβασης, διανομής και πυρήνα

Οι βρόχοι αυτοί, αν και συνήθως απαραίτητοι, μπορούν να δημιουργήσουν σοβαρά προβλήματα στο δίκτυο, αν δεν υπάρχει ειδική πρόβλεψη γι' αυτούς. Συγκεκριμένα μπορεί να προκαλέσουν:

- Θύελλα ευρυεκπομπών (*broadcast storm*). Πρόκειται για συνεχή επανεκομπή πλαισίων ευρυεκπομπής (*broadcasts*) σε όλες τις θύρες των μεταγωγέων. Με την ύπαρξη ενός βρόχου τα πλαίσια αυτά πολλαπλασιάζονται εκθετικά καθώς επανεκπέμπονται συνεχώς κατά μήκος του, με αποτέλεσμα την υπερπλήρωση του δικτύου και τη διακοπή της λειτουργίας του.
- Θύελλα αγνώστων μονοεκπομπών (*unknown unicast storm*). Πρόκειται για συνεχή επανεκπομπή πλαισίου με παραλήπτη που δεν είναι γνωστός (δεν τον έχει ξαναδεί και δεν υπάρχει στον πίνακα MAC) από ένα μεταγωγέα. Το πλαίσιο αυτό αντιμετωπίζεται από τον μεταγωγέα όπως μία ευρυεκπομπή, δηλαδή μετάγεται σε όλες τις θύρες του. Με την ύπαρξη ενός βρόχου, το πλαίσιο αυτό εμφανίζεται να εισέρχεται από πολλαπλές θύρες των μεταγωγέων, με αποτέλεσμα την κατάρρευσή τους λόγω υπερβολικού φορτίου συνεχών αλλαγών στον πίνακα MAC (αστάθεια πίνακα MAC).
- Στα πλαίσια Ethernet δεν υπάρχει πεδίο χρόνου ζωής (TTL), όπως συμβαίνει στα πακέτα IP. Ένα πλαίσιο που δεν φτάνει ποτέ στον προορισμό του, έτσι ώστε να αφαιρεθεί από το δίκτυο, συνεχίζει να κυκλοφορεί επ' αόριστο, με αποτέλεσμα τελικά την κατάρρευση του δικτύου.

15.2 Spanning Tree Protocol

Το STP είναι ένα πρωτόκολλο (και αντίστοιχος αλγόριθμος *Spanning Tree Algorithm*) που τρέχει κατευθείαν πάνω από το Ethernet. Αποτελεί το πρότυπο IEEE 802.1d και είναι ενεργό αυτόματα στους περισσότερους διαχειριζόμενους μεταγωγείς (*managed switches*). Το STP έχει τους ακόλουθους στόχους:

- Να μετατρέψει ένα δίκτυο από δίκτυο με βρόχους σε δίκτυο δενδροειδούς μορφής χωρίς βρόχους. Η μετατροπή αυτή γίνεται με αποκοπή συγκεκριμένων συνδέσεων μεταγωγέων, έτσι ώστε να διακόπτονται οι βρόχοι.
- Να αντιδρά σε αλλαγές της τοπολογίας του δικτύου (λόγω απώλειας μεταγωγέα ή διασύνδεσης), έτσι ώστε να αποκαθίσταται η επικοινωνία, με την ενεργοποίηση θυρών που έχουν αποκοπεί.
- Τα παραπάνω να γίνονται αυτόματα και στο μικρότερο δυνατό χρόνο, έτσι ώστε η διακοπή επικοινωνίας να ελαχιστοποιείται.

Το STP χρησιμοποιεί ειδικά πλαίσια που ονομάζονται *Bridge Protocol Data Units* (BPDU), τα οποία στέλνονται ως πολυκεπομπές (*multicasts*) και τα οποία λαμβάνουν μόνο άλλοι μεταγωγείς ή γέφυρες (*bridges*). Τα BPDU χρησιμοποιούνται για να 'μάθουν' οι μεταγωγείς την τοπολογία του δικτύου: ποιοι μεταγωγείς συνδέονται σε ποιους και αν υπάρχουν βρόχοι ή όχι. Αν βρεθούν βρόχοι οι μεταγωγείς θα αποκόψουν μια ή περισσότερες θύρες για να τους διακόψουν. Η επιλογή των θυρών γίνεται χρησιμοποιώντας τον αλγόριθμο STP. Οι θύρες αυτές δεν κλείνουν τελείως, αλλά τοποθετούνται σε ειδική κατάσταση αποκοπής (βλ. καταστάσεις θυρών STP). Έτσι το δίκτυο μετατρέπεται σε δίκτυο χωρίς βρόχους και ένα πλαίσιο μπορεί να

ακολουθήσει μία μόνο διαδρομή από τον αποστολέα έως τον παραλήπτη του. Αν συμβεί κάποια αλλαγή στο δίκτυο (χαθεί ένας μεταγωγέας ή μία διασύνδεση) οι μεταγωγείς μοιράζονται μεταξύ τους αυτή την πληροφορία, ο αλγόριθμος STP ξανατρέχει και παράγεται μια νέα τοπολογία χωρίς βρόχους, πιθανώς με ενεργοποίηση κάποιας θύρας που πριν είχε αποκοπεί.

Προτερόθετα (*by default*), τα BPDU στέλνονται κάθε 2 δευτερόλεπτα (ο χρόνος αυτός ονομάζεται *hello time*), κάτι που επιταχύνει τη σύγκλιση (*convergence*). Σύγκλιση ονομάζεται η διαδικασία που ακολουθείται ώστε το δίκτυο να επανέλθει σε σταθερή κατάσταση, μετά από μια αλλαγή στην τοπολογία. Όσο μικρότερος είναι ο χρόνος σύγκλισης, τόσο μικρότερη είναι η διακοπή στη λειτουργία του δικτύου.

Τα BPDU περιέχουν πολλή πληροφορία έτσι ώστε να είναι δυνατή η λειτουργία του STP. Η πιο βασική είναι το Bridge ID, που αποτελεί το χαρακτηριστικό ταυτότητας του κάθε μεταγωγέα για το STP. Το BID είναι ένα σύνθετο νούμερο μήκους 64 bits, που αποτελείται από την αλληλουχία του *Bridge Priority* (τα ανώτερα 16 bits) και τη MAC διεύθυνση του μεταγωγέα (τα κατώτερα 48 bits). Όπως και η διεύθυνση MAC, γράφεται στο δεκαεξαδικό σύστημα, αλλά με 16 ψηφία. Το BID χρησιμοποιείται από το STP, τόσο για την αναγνώριση των μεταγωγέων μεταξύ τους, όσο και για τη δημιουργία της δενδροειδούς τοπολογίας χωρίς βρόχους.

BID = Bridge Priority && Bridge MAC

<u>Παράδειγμα</u>

Αν Bridge Priority = 32768 και Bridge MAC = 00e0.8f73.d31d, τότε

BID = 8000 && 00e0.8f73.d31d = 8000.00e0.8f73.d31d

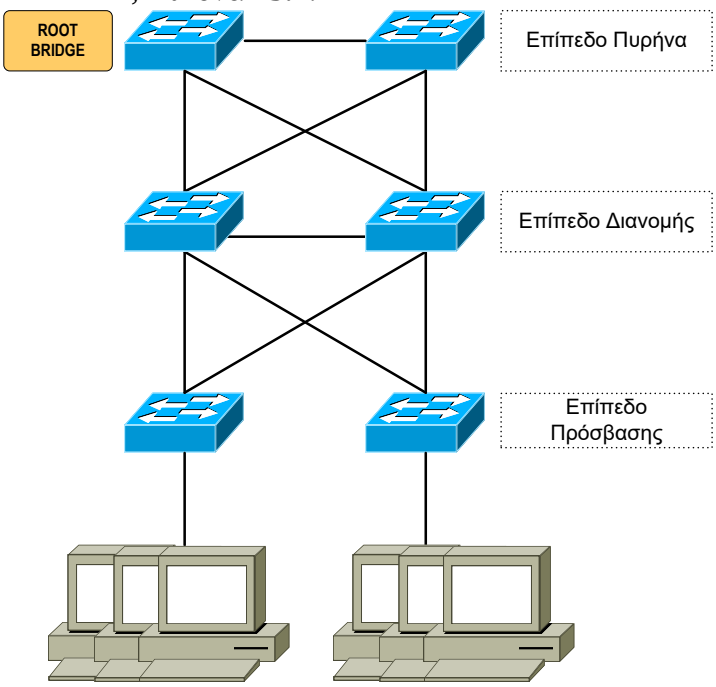
Ο Αλγόριθμος STP

Για τη μετατροπή ενός δικτύου που περιέχει βρόχους, σε μια δενδροειδή μορφή χωρίς βρόχους, απαραίτητη προϋπόθεση είναι ο ορισμός ενός μεταγωγέα ο οποίος θα παίξει το ρόλο του 'μεταγωγέα ρίζας' (*root switch*), την αρχή του ανάποδου δέντρου (κάθε δέντρο πρέπει να διαθέτει μια ρίζα). Ο ορισμός αυτός είναι ιδεατός, δεν θα γίνει κάποια αλλαγή στη φυσική τοπολογία του δικτύου. Όμως με τον καθορισμό της ρίζας, είναι δυνατό να βρεθούν τα πιο 'σύντομα' μονοπάτια προς αυτή από κάθε σημείο του δικτύου και να απενεργοποιηθούν οι συνδέσεις που βρίσκονται «πιο μακριά», έτσι ώστε να διαμορφωθεί το χωρίς βρόχους δέντρο.

Η ρίζα εκλέγεται μεταξύ των μεταγωγέων με ανταλλαγή μηνυμάτων BPDU. Αρχικά κάθε μεταγωγέας θεωρεί ότι είναι ο ίδιος η ρίζα και διαφημίζει αυτή του την ιδιότητα (μαζί με το BID του) στους άλλους μεταγωγείς. Το ίδιο όμως κάνουν και οι άλλοι. Όμως, όταν ένας μεταγωγέας βλέπει διαφημιστικό μήνυμα ενός άλλου ο οποίος έχει μικρότερο αριθμητικά BID, 'υποχωρεί στην ανωτερότητά του' διαφημίζοντας από κει και πέρα αυτόν ως ρίζα. Με αυτόν τον τρόπο, και επειδή όλοι οι μεταγωγείς χρησιμοποιούν τον ίδιο αλγόριθμο, φτάνουν τελικά στο ίδιο συμπέρασμα σχετικά με το ποιος θα είναι ο μεταγωγέας ρίζα, αυτός που έχει το μικρότερο αριθμητικά BID.

Επειδή είναι θέμα τύχης το ποιος μεταγωγέας θα έχει την μικρότερη MAC στο δίκτυο και επειδή προτερόθετα όλοι οι μεταγωγείς έχουν το ίδιο *bridge priority*, 32768, θα είναι τυχαίος ο μεταγωγέας που θα εκλεγεί ως ρίζα στο δίκτυο. Αυτό όμως δεν είναι καλό διότι η επιλογή της ρίζας έχει άμεση σχέση με το ποιες διασυνδέσεις μεταξύ μεταγωγέων θα αποκοπούν. Γενικά συμφέρει η δενδροειδής δομή του STP να ταιριάζει με το ιεραρχικό μοντέλο αρχιτεκτονικής του δικτύου μας και ο μεταγωγέας ρίζα να βρίσκεται όσο το δυνατό πιο κοντά στον πυρήνα του δικτύου. Επίσης είναι σημαντικό αυτός ο μεταγωγέας να διαθέτει χαρακτηριστικά υψηλής αξιοπιστίας, διότι απώλεια της ρίζας σημαίνει διακοπή του δικτύου μέχρι να εκλεγεί νέα.

Επειδή όμως το *bridge priority* αποτελεί τα ανώτερα 16 bit του BID, όποιος μεταγωγέας έχει το μικρότερο, αυτός θα γίνει ρίζα ανεξάρτητα της MAC διεύθυνσης που έχει. Με αυτό τον τρόπο μας δίνεται η δυνατότητα να επηρεάσουμε την εκλογή, αλλάζοντας την τιμή του priority. Αν μειώσουμε λοιπόν χειροκίνητα το bridge priority σε ένα μεταγωγέα, τότε αυτός θα έχει μικρότερο BID από όλους τους άλλους και έτσι θα εκλεγεί αυτός root bridge. Όπως αναφέρθηκε παραπάνω, προτείνεται να ορίζεται σαν ρίζα ένας αξιόπιστος μεταγωγέας που βρίσκεται όσο πιο κοντά γίνεται στον πυρήνα του δικτύου, **Εικόνα 15.2**.



Εικόνα 15.2 Επιλογή μεταγωγέα ρίζας

Όλοι οι μεταγωγείς περιμένουν να λαμβάνουν μήνυμα από τη ρίζα το πολύ μέχρι τον μέγιστο χρόνο (*maximum age time*), ο οποίος είναι προτερόθετα 20 δευτερόλεπτα. Αν ο χρόνος αυτός περάσει και δεν ληφθεί μήνυμα από τη ρίζα, ξεκινά διαδικασία εκλογής νέας ρίζας.

Αφού ως πρώτο βήμα καθοριστεί ο μεταγωγέας ρίζα, σαν δεύτερο βήμα κάθε μεταγωγέας επιλέγει μια θύρα που θα είναι αυτή που θα οδηγεί στην ρίζα και η οποία ονομάζεται 'θύρα ρίζας' (*root port*). Η επιλογή γίνεται με τα ακόλουθα κριτήρια:

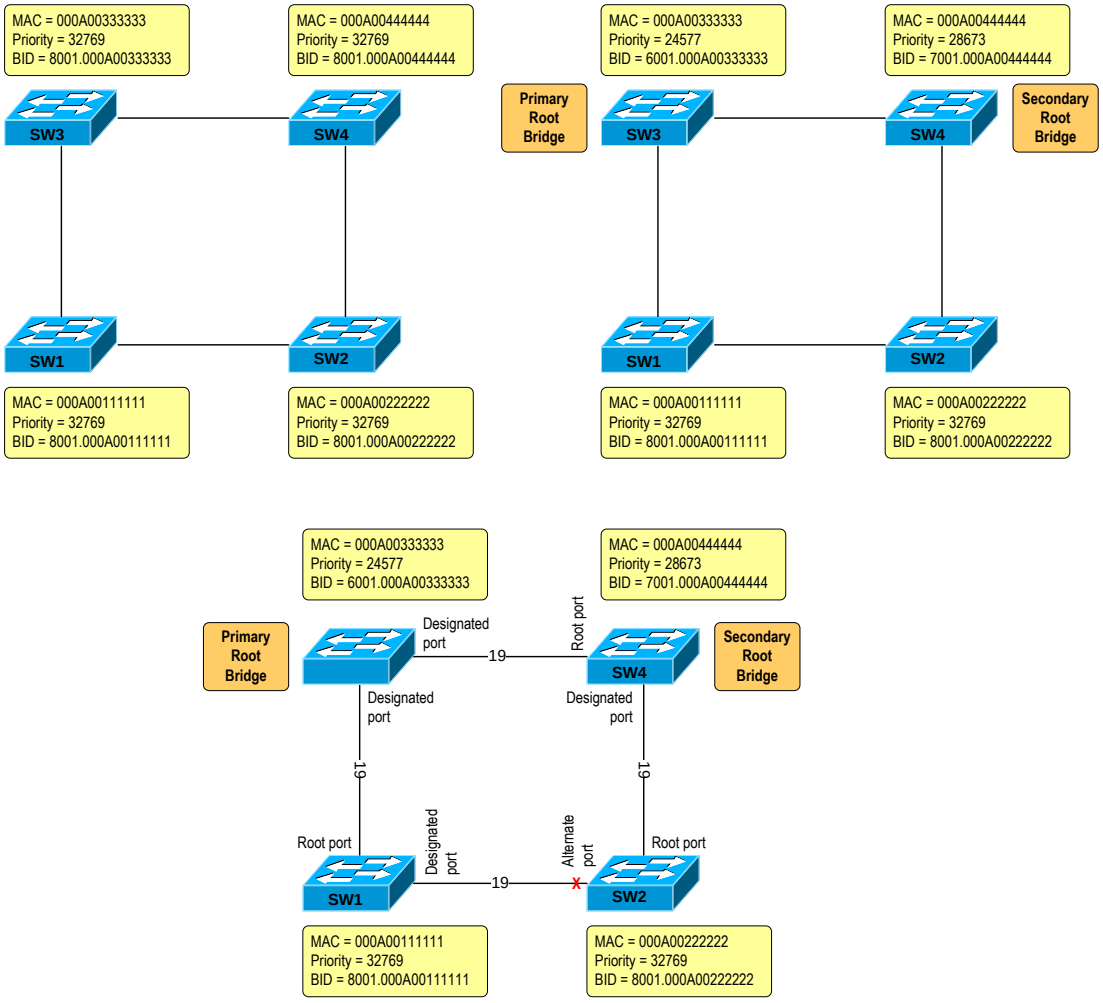
α) Επιλέγεται η θύρα με το μικρότερο κόστος διαδρομής προς τη ρίζα. Το κόστος διαδρομής ορίζεται ως το άθροισμα των κοστών κάθε τμήματος καλωδίου που αποτελεί τη διαδρομή (βλ. παρακάτω για το κόστος τμήματος).
β) Αν υπάρχουν πολλαπλές θύρες με το ίδιο κόστος διαδρομής προς τη ρίζα, επιλέγεται η θύρα που συνδέεται στο γειτονικό μεταγωγέα με το μικρότερο BID.
γ) Αν με αυτό το μεταγωγέα υπάρχουν πολλαπλές συνδέσεις, επιλέγεται η θύρα με την μεγαλύτερη (τη μικρότερη αριθμητικά) προτεραιότητα (προτερόθετα 128).
δ) Αν και πάλι υπάρχει ισοπαλία (δηλαδή οι θύρες έχουν την ίδια προτεραιότητα), επιλέγεται η θύρα που είναι κατασκευαστικά πιο πριν στο μεταγωγέα.

Σαν τρίτο βήμα, σε κάθε τμήμα καλωδίου που βρίσκεται μεταξύ μεταγωγέων πρέπει να εκλεγεί μία και μοναδική θύρα που οδηγεί προς τη ρίζα. Άρα, οι μεταγωγείς που είναι συνδεδεμένοι σε αυτό το τμήμα, εκλέγουν μία από όλες τις συνδέσεις πάνω σε αυτό το τμήμα να είναι η 'προσδιορισμένη θύρα' (*designated port*) γι' αυτό το τμήμα. Μέσα από αυτή τη θύρα οδηγούμαστε στη ρίζα με το μικρότερο δυνατό κόστος. Η επιλογή της προσδιορισμένης θύρας για κάθε τμήμα καλωδίου μεταξύ δύο ή περισσοτέρων μεταγωγέων γίνεται με τα ακόλουθα κριτήρια:

α) Επιλέγεται η θύρα της οποίας ο μεταγωγέας διαφημίζει το μονοπάτι με το μικρότερο συνολικό κόστος προς τη ρίζα.
β) Αν υπάρχει ισοπαλία μεταξύ δύο μεταγωγέων, επιλέγεται ο μεταγωγέας (και η θύρα του), με το μικρότερο BID.
γ) Αν ο μεταγωγέας αυτός τυγχάνει να έχει δύο θύρες συνδεδεμένες πάνω σε αυτό το τμήμα καλωδίου, επιλέγεται η θύρα με τη μεγαλύτερη (μικρότερη αριθμητικά) προτεραιότητα (προτερόθετα 128).
δ) Αν και πάλι υπάρχει ισοπαλία (δηλαδή οι θύρες έχουν την ίδια προτεραιότητα), επιλέγεται η θύρα που είναι κατασκευαστικά πιο πριν στο μεταγωγέα.

Μετά από αυτό το βήμα, κάθε τμήμα καλωδίου δικτύου θα έχει μια και μοναδική προσδιορισμένη θύρα κάποιου μεταγωγέα μέσα από τον οποίο περνάει το βέλτιστο μονοπάτι προς τη ρίζα. Ένας μεταγωγέας μπορεί να είναι συνδεδεμένος σε περισσότερα του ενός τμήματα καλωδίου μέσω διαφορετικών θυρών, όμως μία μόνο απ' αυτές να είναι χαρακτηρισμένη ως προσδιορισμένη (στα άλλα τμήματα καλωδίου η θύρα κάποιου άλλου μεταγωγέα μπορεί να είναι προσδιορισμένη). Εξαίρεση αποτελεί ο μεταγωγέας ρίζα, του οποίου όλες οι ενεργές θύρες είναι προσδιορισμένες στο αντίστοιχο τμήμα τους, κάτι λογικό αφού γι' αυτά τα τμήματα το κόστος της διαδρομής προς τη ρίζα μέσα από την συγκεκριμένη θύρα είναι 0.

Σε κάθε τμήμα καλωδίου, οι θύρες που δεν είναι προσδιορισμένες (*non-designated*) αποκόπτονται. Στην **Εικόνα 15.3** φαίνονται τα αποτελέσματα της διαδικασίας για ένα μικρό δίκτυο.



Εικόνα 15.3 Διαδικασία εκλογής μεταγωγέων και θυρών

Καταστάσεις θυρών

Σε ένα μεταγωγέα που τρέχει STP, οι θύρες μπορεί να βρίσκονται σε μία από τις ακόλουθες καταστάσεις: *αποκοπής (blocking), παρακολούθησης (listening), εκμάθησης (learning), προώθησης (forwarding)* και *απενεργοποίησης (disabled).*

Μια θύρα μπαίνει σε κατάσταση αποκοπής όταν: α) γίνεται εκλογή ρίζας στο δίκτυο, β) ο μεταγωγέας λαμβάνει BPDU που υποδεικνύει μονοπάτι μικρότερου κόστους προς τη ρίζα από άλλη θύρα από αυτή που χρησιμοποιεί, γ) αυτή η θύρα δεν είναι ούτε θύρα ρίζας, ούτε προσδιορισμένη θύρα.

Μια θύρα παραμένει προτερόθετα σε κατάσταση αποκοπής για 20 δευτερόλεπτα (ο χρόνος αυτός ονομάζεται maximum age time) και σε αυτή την κατάσταση λαμβάνει και επεξεργάζεται μόνο πλαίσια BPDU (όλα τα άλλα απορρίπτονται). Σε κατάσταση αποκοπής ο μεταγωγέας προσπαθεί να αποφασίζει ποια θύρα θα είναι η root, ποιες θύρες θα είναι προσδιορισμένες και ποιες θύρες θα παραμείνουν αποκομμένες για την εξουδετέρωση βρόχων.

Με το τέλος του *maximum age time*, μια θύρα ρίζας ή μια προσδιορισμένη θύρα περνάει σε κατάσταση παρακολούθησης. Οι άλλες θύρες παραμένουν σε κατάσταση αποκοπής. Σε κατάσταση παρακολούθησης η θύρα παραμένει προτερόθετα για 15 δευτερόλεπτα (ο χρόνος ονομάζεται *forward delay time*), κατά τη διάρκεια των οποίων επεξεργάζεται τα BPDU και ελέγχει την τοπολογία. Όλα τα άλλα πλαίσια δεδομένων απορρίπτονται.

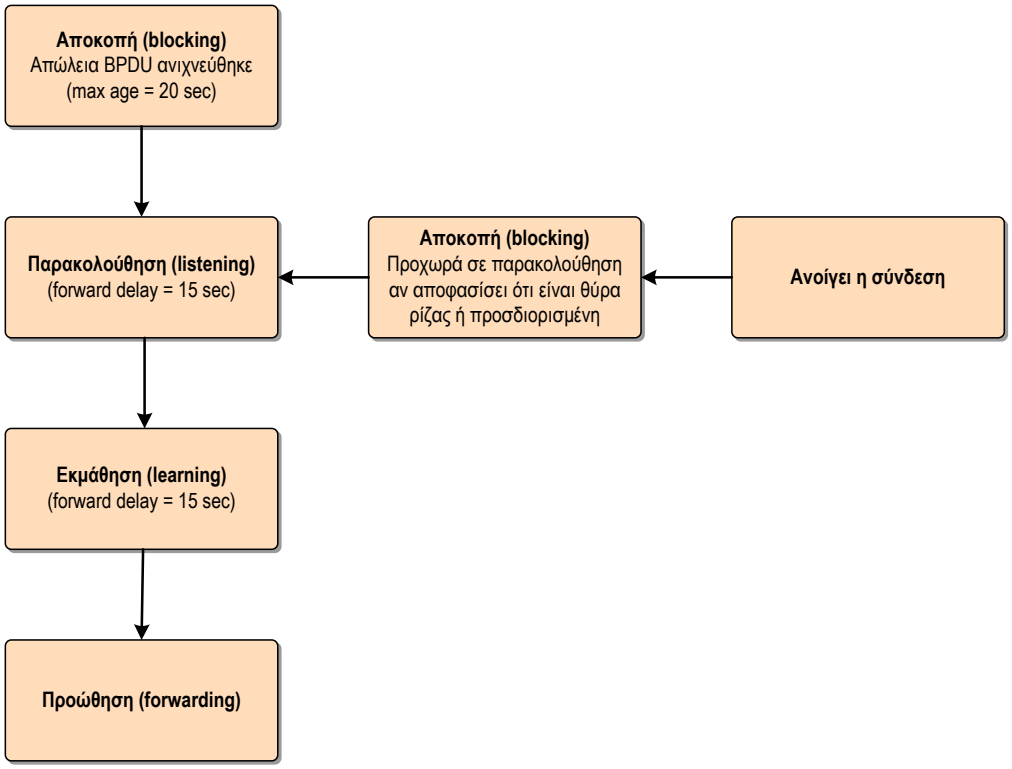
Από την κατάσταση παρακολούθησης, μια θύρα ρίζας ή προσδιορισμένη περνάει σε κατάσταση εκμάθησης, οπότε όχι μόνο επεξεργάζεται BPDU, αλλά παρακολουθεί και τα κανονικά πλαίσια δεδομένων, εμπλουτίζοντας έτσι τον πίνακα MAC διευθύνσεων του μεταγωγέα. Συνεχίζει όμως να μην μετάγει πλαίσια δεδομένων. Ο χρόνος που παραμένει σε αυτή την κατάσταση η θύρα είναι προτερόθετα 15 δευτερόλεπτα (*forward delay time*).

Τελικά η θύρα καταλήγει σε κατάσταση προώθησης, οπότε λειτουργεί κανονικά (και επεξεργάζεται BPDU και προωθεί πλαίσια δεδομένων).

Μια τελευταία κατάσταση θύρας είναι η απενεργοποιημένη. Αυτή είναι μια ειδική κατάσταση στην οποία βρίσκεται μια θύρα διότι α) δεν μετέχει στο STP λόγω διαχειριστικής ρύθμισης, β) είναι κλειστή λόγω ρητής διαχειριστικής ρύθμισης (*shutdown*), γ) είναι μπλοκαρισμένη για λόγους ασφαλείας (*error or security disabled*), δ) δεν υπάρχει σύνδεση δικτύου (*link down or protocol down*).

Ο χρόνος σύγκλισης είναι ο συνολικός χρόνος που περνάει μέχρι να εκλεγεί ένας μεταγωγέας ρίζα, να επιλεγούν οι θύρες ρίζας και οι προσδιορισμένες, να περάσουν αυτές σε κατάσταση προώθησης και οι άλλες θύρες να τοποθετηθούν σε κατάσταση αποκοπής. Αν μια θύρα πρέπει να περάσει από όλες τις καταστάσεις, η σύγκλιση διαρκεί 50”. Αν μια θύρα δεν πρέπει να περάσει από κατάσταση αποκοπής και μπορεί να ξεκινήσει από κατάσταση παρακολούθησης, η σύγκλιση παίρνει 30” (αυτό συμβαίνει όταν ο μεταγωγέας ρίζα δεν έχει χαθεί, αλλά έχει συμβεί κάποια άλλη αλλαγή στο δίκτυο, π.χ. χάσιμο άλλου μεταγωγέα ή σύνδεσης). Υπογραμμίζεται ότι σε αυτό το χρόνο η κίνηση του δικτύου από τη θύρα έχει διακοπεί.

Στην **Εικόνα 15.4** φαίνεται η σχέση καταστάσεων θυρών και χρόνων μεταβάσεων.



Εικόνα 15.4 Σχέση καταστάσεων θυρών και χρόνων μεταβάσεων

Προτείνεται να μη γίνεται ρύθμιση των χρόνων μετάβασης μεταξύ των καταστάσεων θυρών του STP απευθείας (οι χρόνοι έχουν βελτιστοποιηθεί για διάμετρο δικτύου ίση με επτά). Ωστόσο, αν ο διαχειριστής του δικτύου θελήσει να βελτιώσει το χρόνο σύγκλισης για δίκτυο μικρότερης διαμέτρου, μπορεί να το κάνει αλλάζοντας την παράμετρο της διαμέτρου του δικτύου στο μεταγωγέα ρίζα (βλ. Ρυθμίσεις PVST+ και RPVST).

Κόστη θυρών

Κάθε κατασκευαστής μεταγωγέων ορίζει τα δικά του προτερόθετα κόστη για τις θύρες, ανάλογα με το πρότυπο που ακολουθεί και την ταχύτητα που τρέχουν. Στον ακόλουθο πίνακα φαίνονται δύο παραδείγματα:

Ταχύτητα θύρας	Κόστος σύνδεσης IEEE 802.1d-1998	Κόστος σύνδεσης IEEE 802.1d-2004, IEEE 802.1w
10 Mbps	100	2000000
100 Mbps	19	200000
1 Gbps	4	20000
2 Gbps	3	10000
10 Gbps	2	2000

Υπογραμμίζεται ότι σ’ ένα δίκτυο με μεταγωγείς διαφορετικών κατασκευαστών καλό θα είναι τα κόστη των θυρών για τις ίδιες ταχύτητες να είναι ίδια.

15.3 Βελτιώσεις και επεκτάσεις STP

Η όσο το δυνατόν ταχεία σύγκλιση του δικτύου μετά από αλλαγές είναι ιδιαίτερα επιθυμητή, μια και μέχρι να επέλθει το δίκτυο δεν μετάγει χρήσιμη πληροφορία. Γι' αυτό το σκοπό έχουν αναπτυχθεί από τους κατασκευαστές μεταγωγέων επεκτάσεις στο STP. Στη συνέχεια θα δούμε μερικές από αυτές.

Portfast

Οι θύρες μεταγωγέων στις οποίες συνδέονται κανονικά μόνο σταθμοί εργασίας, εξυπηρετητές και δρομολογητές (συσκευές δηλαδή που δεν είναι μεταγωγείς ή γέφυρες), δεν υπάρχει λόγος να περνούν από όλες τις καταστάσεις που προβλέπει το STP και έτσι να καθυστερεί η κανονική τους λειτουργία και να μην περνάνε πλαίσια δεδομένων.

Οι θύρες αυτές μπορούν να τοποθετηθούν σε διαμόρφωση *portfast*, στην οποία μια θύρα περνάει από την κατάσταση απενεργοποίησης (όταν π.χ. η συσκευή που είναι πάνω της είναι κλειστή) κατευθείαν στην κατάσταση προώθησης, χωρίς αναμονή. Έτσι η επικοινωνία π.χ. ενός σταθμού εργασίας που είναι συνδεδεμένος σ' αυτήν αποκαθίσταται άμεσα.

BPDU Guard

Τα παραπάνω είναι καλά, με την προϋπόθεση ότι δεν θα συνδεθεί πάνω σε μια θύρα portfast ένας μεταγωγέας. Αν γίνει αυτό και λόγω της άμεσης ενεργοποίησής της είναι δυνατόν να δημιουργηθεί βρόχος πριν προλάβει το STP να αποκόψει την κατάλληλη θύρα. Το σύνηθες σενάριο είναι αυτό όπου οι χρήστες συνδέουν μεταγωγείς πάνω σε θύρες πρόσβασης επειδή δεν διαθέτουν αρκετές θύρες στο φυσικό τους χώρο. Αν ο μεταγωγέας αυτός συνδεθεί κατά λάθος με περισσότερες της μιας θύρες πρόσβασης θα δημιουργηθεί βρόχος, με αποτέλεσμα την διακοπή της λειτουργίας όλου του δικτύου!

Για να προφυλαχθούμε από το σενάριο αυτό, σε όλες τις θύρες (ή σε κάποιες από αυτές) portfast μπορεί να ενεργοποιηθεί ένας μηχανισμός προφύλαξης από σύνδεση μεταγωγέα, ο οποίος ονομάζεται *BPDU guard*. Με το μηχανισμό αυτό, αν μια θύρα porfast ανιχνεύσει εισερχόμενο BPDU (που σημαίνει ότι έχει συνδεθεί πάνω της ένας διαχειρίσιμος μεταγωγέας ή γέφυρα), η θύρα τοποθετείται σε κατάσταση *error disabled* και σταματά να μετάγει πλαίσια, μέχρι ο διαχειριστής να την ενεργοποιήσει ξανά.
Σημείωση: Ο μηχανισμός BPDU guard προϋποθέτει ότι ο μεταγωγέας που θα συνδεθεί σε guarded θύρα εκπέμπει BPDUs. Αν αυτό δεν ισχύει (π.χ. πρόκειται για μη διαχειρίσιμο μεταγωγέα) τότε το BPDU guard δεν προστατεύει και πρέπει να χρησιμοποιηθεί άλλος μηχανισμός (π.χ. loop detection).

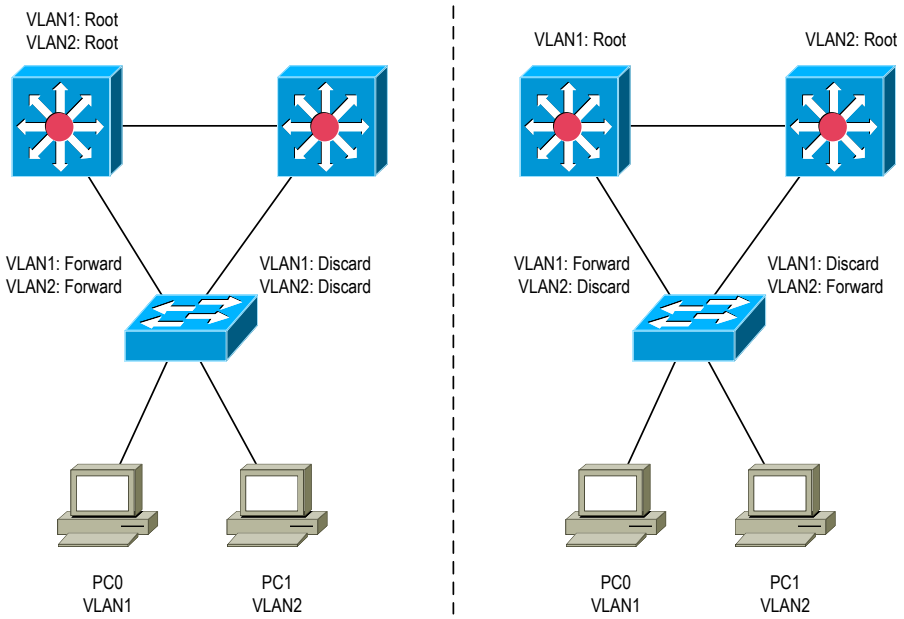
Primary και Secondary Root Bridge

Υπάρχει η δυνατότητα εκτός από την πρωτεύουσα ρίζα (*primary root bridge*) να οριστεί και μια δευτερεύουσα (*secondary root bridge*), η οποία θα αναλάβει το ρόλο της ρίζας στην περίπτωση που η πρωτεύουσα χαθεί. Δευτερεύουσα ρίζα γίνεται ο μεταγωγέας με το δεύτερο μικρότερο BID (αυτός που έχει το μικρότερο γίνεται πρωτεύουσα). Επομένως, βάζοντας τους δύο επιθυμητούς μεταγωγείς να έχουν τη μικρότερη και τη δεύτερη μικρότερη προτεραιότητα, μπορούμε να καθορίσουμε ποιοι θα αναλάβουν αυτούς τους δύο ρόλους.

PVST+

Η Cisco ανάπτυξε το PVST+ (και πολλοί άλλοι κατασκευαστές υιοθέτησαν πολλές από τις λειτουργίες του) έτσι ώστε οι μεταγωγείς να μπορούν να τρέχουν μία ξεχωριστή υπόσταση του STP για κάθε ένα VLAN που υπάρχει στο δίκτυο (για την έννοια του VLAN βλ. το αντίστοιχο κεφάλαιο). Τότε όμως, όλοι οι μεταγωγείς του δικτύου μετέχουν στη σύγκλιση και οι θύρες τους πρέπει να εξυπηρετήσουν το επιπλέον φορτίο των BPDU κάθε μιας υπόστασης του STP.

Με το PVST+ μπορεί να ρυθμιστούν οι παράμετροι του STP έτσι ώστε τα μισά VLAN να προωθούνται από μία και τα άλλα μισά από άλλη ανερχόμενη σύνδεση, **Εικόνα 15.5**. Αυτό γίνεται ρυθμίζοντας ένα μεταγωγέα να είναι ρίζα για τα μισά VLAN και άλλον να είναι ρίζα για τα άλλα μισά. Με αυτό τον τρόπο κατανέμεται στατικά η κίνηση του δικτύου σε παραπάνω της μιας ανερχόμενων συνδέσεων και αυξάνεται και η βλαβοαντοχή.



Εικόνα 15.5 Κατανομή VLANs σε ανερχόμενες συνδέσεις

Στην περίπτωση που υποστηρίζεται πρωτεύουσα και δευτερεύουσα ρίζα, μπορούμε να θέσουμε τον ένα μεταγωγέα ως πρωτεύουσα ρίζα για τα μισά VLAN και δευτερεύουσα για τα άλλα μισά και τον δεύτερο μεταγωγέα ανάποδα.

Επίσης, στο PVST+ το BID αλλάζει ώστε να περιλαμβάνει και το VLAN ID (VID). Έτσι το BID γίνεται:

BID = [Bridge Priority (4 bits) + VID (12 bits)] && Bridge MAC (48 bits)

Παράδειγμα

Αν Bridge Priority = 32768, VLAN ID = 10 και Bridge MAC = 00e0.8f73.d31d, τότε

BID = [8000 + A] && 00e0.8f73.d31d = 800A.00e0.8f73.d31d

Rapid STP

Το STP αναπτύχθηκε σε μια εποχή που η αναμονή 30” ή 50” για να συγκλίνει ένα δίκτυο δεν αποτελούσε σημαντικό πρόβλημα. Όμως σε σύγχρονα δίκτυα με πολυμεσικές εφαρμογές, διακοπές τέτοιου μεγέθους αποτελούν μεγάλο πρόβλημα. Για να βελτιωθούν τα πράγματα, κατασκευαστές μεταγωγέων όπως η Cisco εισήγαγαν επεκτάσεις στο STP, όπως το portfast (βλ. παραπάνω), το uplinkfast και το backbonefast.

Σήμερα ωστόσο, το προτιμούμενο πρωτόκολλο για την προστασία από βρόχους μεταγωγής σε ένα δίκτυο είναι το Rapid STP (RSTP). Όντας εξέλιξη του STP, έχει προτυποποιηθεί ως IEEE 802.1w, υλοποιείται από όλους τους κατασκευαστές μεταγωγέων και αποτελεί την καλύτερη επιλογή, ιδιαίτερα σε δίκτυα με μεταγωγείς από πολλαπλούς κατασκευαστές, έτσι ώστε να διασφαλίζεται η διαλειτουργικότητα. Επιπλέον, οι επεκτάσεις που εισάγει το RSTP δεν απαιτούν ρυθμίσεις και γενικά έχουν καλύτερη απόδοση από τις παλαιότερες ειδικευμένες επεκτάσεις (σημειώνεται ότι ορισμένες επεκτάσεις της Cisco, συγκεκριμένα το uplinkfast και το backbonefast, δεν είναι συμβατές με το RSTP). Παράλληλα το RSTP διατηρεί συμβατότητα προς τα πίσω με το STP, έτσι ώστε να διασφαλίζεται η διαλειτουργικότητα με παλαιούς μεταγωγείς που δεν το υποστηρίζουν. Για παράδειγμα το RSTP εκλέγει ένα μεταγωγέα ρίζα ακριβώς όπως και το STP και χρησιμοποιεί την ίδια δομή BPDU (εκτός από το πεδίο «έκδοση» που παίρνει τιμή 2 για να φαίνεται ότι πρόκειται για RSTP).

Κύριος στόχος του RSTP είναι να επιταχύνει τη διαδικασία σύγκλισης (η οποία στο STP είναι μέχρι και 50”), ενσωματώνοντας πολλές από τις ειδικές επεκτάσεις που είχαν κάνει παλαιότερα κατασκευαστές μεταγωγέων και μειώνοντας το χρόνο σύγκλισης σε ένα καλορυθμισμένο δίκτυο μέχρι και σε δέκατα του δευτερολέπτου.

Το RSTP επανακαθορίζει τις καταστάσεις και τους ρόλους των θυρών. Οι καταστάσεις θυρών είναι τώρα τρεις: απόρριψης (*discarding*), εκμάθησης (*learning*) και προώθησης (*forwarding*). Στο RSTP συνεχίζουν να υπάρχουν οι ρόλοι θυρών ρίζας και προσδιορισμένης, όπως στο STP, ωστόσο το RSTP εισάγει δύο νέους ρόλους, τις ‘αναπληρωματικές’ (*alternate*) και τις ‘εφεδρικές’ (*backup*), οι οποίοι είναι παρόμοιοι με την κατάσταση αποκοπής στο STP. Μια αναπληρωματική θύρα διαθέτει μια ή περισσότερες δευτερεύουσες διαδρομές προς τη ρίζα, αλλά προς το παρόν είναι σε κατάσταση απόρριψης (δεν μετάγει πλαίσια). Μια εφεδρική θύρα από την άλλη, είναι η θύρα ενός τμήματος καλωδίου που θα μπορούσε να οδηγήσει στη

ρίζα, όμως υπάρχει άλλη προσδιορισμένη (*designated*) ενεργή θύρα γι' αυτό το σκοπό. Για να γίνουν αυτά πιο κατανοητά, μπορεί κανείς να φανταστεί την αναπληρωματική θύρα σαν μια δευτερεύουσα θύρα ρίζας, ενώ την εφεδρική σαν μια δευτερεύουσα προσδιορισμένη θύρα. Αν μια θύρα μεταγωγέα έχει τεθεί να είναι αναπληρωματική ή εφεδρική, μπορεί να αλλάξει άμεσα σε κατάσταση προώθησης χωρίς αναμονή. Το RSTP μπορεί να επίσης επιβεβαιώσει ενεργά την ασφαλή μετάβαση μιας θύρας σε κατάσταση προώθησης, χωρίς να βασίζεται σε χρόνους.

Στο STP, αν ένας μεταγωγέας δεν έβλεπε BPDU από τη ρίζα εντός του *maximum age time* (προτερόθετα 20"), γινόταν εκλογή νέας ρίζας και υπολογιζόταν μια νέα τοπολογία χωρίς βρόχους, κάτι πολύ χρονοβόρο. Στο RSTP, αν δεν ληφθεί BPDU εντός τριών περιόδων *hello* (προτερόθετα 3 x 2 = 6" σύνολο) η πληροφορία STP γερνά άμεσα, ο μεταγωγέας θεωρεί το γείτονά του χαμένο και λαμβάνει μέτρα άμεσα.

Επίσης, το RSTP εισάγει την έννοια της θύρας άκρου (*edge ports*), που είναι η ίδια με το portfast, δηλαδή θύρα στην οποία δεν συνδέεται μεταγωγέας. Όμως σε αντίθεση με το portfast, αν ανιχνευτεί BPDU σε μια edge θύρα αυτή χάνει αυτόματα το χαρακτήρα edge. Η Cisco βέβαια διατηρεί την εντολή portfast για τη ρύθμιση του θύρας edge στο RSTP, ενώ άλλοι κατασκευαστές τις χαρακτηρίζουν πιο ορθά ως *edge*.

Επιπλέον, οι θύρες που δεν είναι edge μπορεί να είναι τύπου είτε point-to-point, είτε shared. Οι point-to-point είναι θύρες που λειτουργούν σε full duplex και είναι επίσης υποψήφιες για άμεση μετάβαση σε κατάσταση προώθησης.

Όπως και στο PVST+, όταν υπάρχουν παραπάνω του ενός VLAN, τρέχει μία υπόσταση RSTP ανά VLAN και το πρωτόκολλο ονομάζεται Rapid-PVST.

15.4 Ρυθμίσεις PVST+ και Rapid-PVST σε Cisco CLI

Η διεργασία PVST+ είναι προτερόθετα ενεργοποιημένη στους μεταγωγείς Cisco και δεν χρειάζεται κάποια ρύθμιση για την ενεργοποίησή της.

Για να δει κανείς πληροφορίες που αφορούν το PVST+ ή Rapid-PVST, για ένα ή περισσότερα VLAN, για το ποιος είναι ο μεταγωγέας ρίζα και ποιες θύρες έχουν ποιο ρόλο, η εντολή είναι:

```
Switch# show spanning-tree vlan VLAN# [detail]
```

Παράδειγμα:

```
Switch# show spanning-tree vlan 1
```

Αν δε μπει η παράμετρος **vlan**, θα εμφανιστούν όλες οι υποστάσεις του STP για όλα τα VLAN. Η παράμετρος **detail** δείχνει λίγο περισσότερες πληροφορίες. Για να δούμε πληροφορίες ρυθμίσεων γενικού τύπου των PVST+/Rapid-PVST δίνουμε:

```
Switch# show spanning-tree summary
```

Για να γίνει πλήρης αποσφαλμάτωση (*debugging*) των PVST+/Rapid-PVST, η εντολή είναι:

```
Switch# debug spanning-tree switch all
```

Για να κλείσουμε την αποσφαλμάτωση δίνουμε:

```
Switch# no debug spanning-tree switch all
```

Για να ενεργοποιηθεί το Rapid-PVST αντί του PVST+, η εντολή είναι:

```
Switch(config)# spanning-tree mode rapid-pvst
```

Για να επιστρέψουμε στο PVST+ δίνουμε:

```
Switch(config)# spanning-tree mode pvst
```

Για να αλλαχθεί η προτεραιότητα ενός μεταγωγέα, προκειμένου να αλλαχθεί το BID του, η εντολή είναι:

```
Switch(config)# spanning-tree vlan VLAN# root primary
Switch(config)# spanning-tree vlan VLAN# root secondary
Switch(config)# spanning-tree vlan VLAN# priority priority#
```

Υπενθυμίζεται ότι η προτεραιότητα είναι προτερόθετα 32768 (για την ακρίβεια 32769 στο PVST+ για το VLAN 1). Η πρώτη εντολή μειώνει (αυξάνει) την προτεραιότητα του μεταγωγέα κατά 8192. Η δεύτερη την μειώνει (αυξάνει) κατά 4096. Η τρίτη την θέτει σε ένα συγκεκριμένο νούμερο, πολλαπλάσια του 4096. Αν π.χ. θέλαμε να θέσουμε τον μεταγωγέα A `primary root` για το VLAN 1 και `secondary root` για το VLAN 2, ενώ τον μεταγωγέα B ανάποδα, με πρωτόκολλο Rapid-PVST, τότε θα δίναμε:

```
Switch-A(config)# spanning-tree mode rapid-pvst
Switch-A(config)# spanning-tree vlan 1 root primary
Switch-A(config)# spanning-tree vlan 2 root secondary
Switch-B(config)# spanning-tree mode rapid-pvst
Switch-B(config)# spanning-tree vlan 2 root primary
Switch-B(config)# spanning-tree vlan 1 root secondary
```

Για να ρυθμιστεί στον μεταγωγέα ρίζα η διάμετρος του PVST+/RPVST και έτσι να μειωθούν οι τιμές των χρόνων σύγκλισης, δίνουμε την εντολή:

```
Switch(config)# spanning-tree vlan VLAN# root primary diameter value
```

Για παράδειγμα, για να ρυθμιστεί η παράμετρος της διαμέτρου για ένα δίκτυο με διάμετρο 5 για το VLAN1, δίνουμε:

```
Switch(config)# spanning-tree vlan 1 root primary diameter 5
```

Για να ρυθμιστεί το `portfast` σε όλες τις access θύρες ενός μεταγωγέα:

```
Switch(config)# spanning-tree portfast default
```

Για να γίνει ενεργοποίηση ανά θύρα, η εντολή είναι:

```
Switch(config)# interface type [slot#]/port#
Switch(config-if)# spanning-tree portfast [trunk]
```

Η παράμετρος `trunk` αφορά συνδέσεις κορμού με δρομολογητές και εξυπηρετητές. Για παράδειγμα, για να θέσουμε τις θύρες `fa0/1` έως `fa0/24` ενός μεταγωγέα να είναι `portfast`, δίνουμε:

```
Switch(config)# interface range fa0/1 - 24
Switch(config-if-range)# spanning-tree portfast
```

Για να ρυθμιστεί το `bpduguard` σε όλες τις `access` θύρες ενός μεταγωγέα:

```
Switch(config)# spanning-tree portfast bpduguard default
```

Για να γίνει ενεργοποίηση ανά θύρα, η εντολή είναι:

```
Switch(config)# interface type [slot#]/port#
Switch(config-if)# spanning-tree bpduguard enable
```

Για παράδειγμα, για να θέσουμε `bpduguard` στη θύρα `fa0/1`, δίνουμε:

```
Switch(config)# interface fa0/1
Switch(config-if)# spanning-tree bpduguard enable
```

15.5 Εργαστηριακή άσκηση

Σε αυτή την εργαστηριακή άσκηση θα μελετηθεί μια δι-επίπεδη αρχιτεκτονική δικτύου (επίπεδο πρόσβασης, επίπεδο διανομής), με απλούς μεταγωγείς δευτέρου επιπέδου, η οποία διαθέτει στοιχεία βλαβοαντοχής με πολλαπλές συνδέσεις/διαδρομές μεταξύ των μεταγωγέων πρόσβασης και διανομής. Το πρωτόκολλο που θα χρησιμοποιηθεί για την εξάλειψη των βρόχων μεταγωγής και την

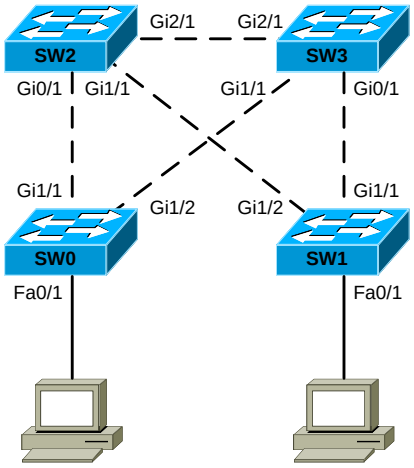
σύγκλιση του δικτύου μετά από πρόβλημα είναι το Rapid-PVST. Η άσκηση θα γίνει με το λογισμικό προσομοίωσης Cisco Packet Tracer και με εντολές στο Cisco CLI.

Τα στοιχεία του δικτύου φαίνονται στον **Πίνακα 15.1**.

Πίνακας 15.1 Δεδομένα συσκευών για την εργαστηριακή άσκηση **15.5**

Α/Α	**Τύπος συσκευής**	**Όνομα (hostname)**	**Διεύθυνση IP**	**Πρωτόκολλα, ρυθμίσεις**
1	PC	PC0	192.168.1.1/24	IP
2	PC	PC1	192.168.1.2/24	IP
3	Switch 2960-24TT	SW0	192.168.1.3/24	IP, RPVST, portfast default, bpduguard default
4	Switch 2960-24TT	SW1	192.168.1.4/24	IP, RPVST, portfast default, bpduguard default
5	Switch PT Empty + 3x NM-1CGE	SW2	192.168.1.5/24	IP, RPVST, primary STP root
6	Switch PT Empty + 3x NM-1CGE	SW3	192.168.1.6/24	IP, RPVST, secondary STP root

Το διάγραμμα δικτύου φαίνεται στην **Εικόνα 15.6**.



Εικόνα 15.6 Διάγραμμα δικτύου για την εργαστηριακή άσκηση 15.5

Ζητούνται:

α) Να ρυθμιστούν οι συσκευές, με τα ονόματα, τα πρωτόκολλα και τις ρυθμίσεις του παραπάνω πίνακα, έτσι ώστε τα PC να κάνουν ping μεταξύ τους και ping και telnet στους μεταγωγείς.

β) Οι θύρες access (fa0/1 – fa0/24) των μεταγωγέων πρόσβασης (sw0, sw1) θα πρέπει να ανοίγουν άμεσα (portfast) και να μην δέχονται σύνδεση μεταγωγέων (bpduguard).

γ) Ο μεταγωγέας sw2 θα πρέπει να είναι primary STP root και ο sw3 secondary STP root, με χρήση πρωτοκόλλου εξάλειψης βρόχων Rapid-PVST.
δ) Αν χαθεί ανερχόμενη σύνδεση από ένα μεταγωγέα πρόσβασης, καθώς και ένας μεταγωγέας διανομής, το δίκτυο θα πρέπει να συγκλίνει στο συντομότερο χρονικό διάστημα. Να βρεθεί προσεγγιστικά ο χρόνος σύνδεσης.

15.6 Εργαστηριακή άσκηση

Σε αυτή την άσκηση, θα γίνει συνδυασμός των λειτουργιών του δικτύου της άσκησης 13.3 με αυτού της άσκησης 15.5. Σκοπός είναι να δημιουργηθεί μια αρχιτεκτονική δικτύου με στοιχεία βλαβοαντοχής, έτσι ώστε απώλεια σύνδεσης, ή μεταγωγέα, ή δρομολογητή να μην προκαλεί μόνιμη δυσλειτουργία στο δίκτυο. Για το σκοπό αυτό, τόσο οι μεταγωγείς διανομής, όσο και οι δρομολογητές θα είναι διπλοί, όπως και οι συνδέσεις μεταξύ των μεταγωγέων επιπέδου πρόσβασης και επιπέδου διανομής. Το διάγραμμα δικτύου φαίνεται στην **Εικόνα 15.7**.

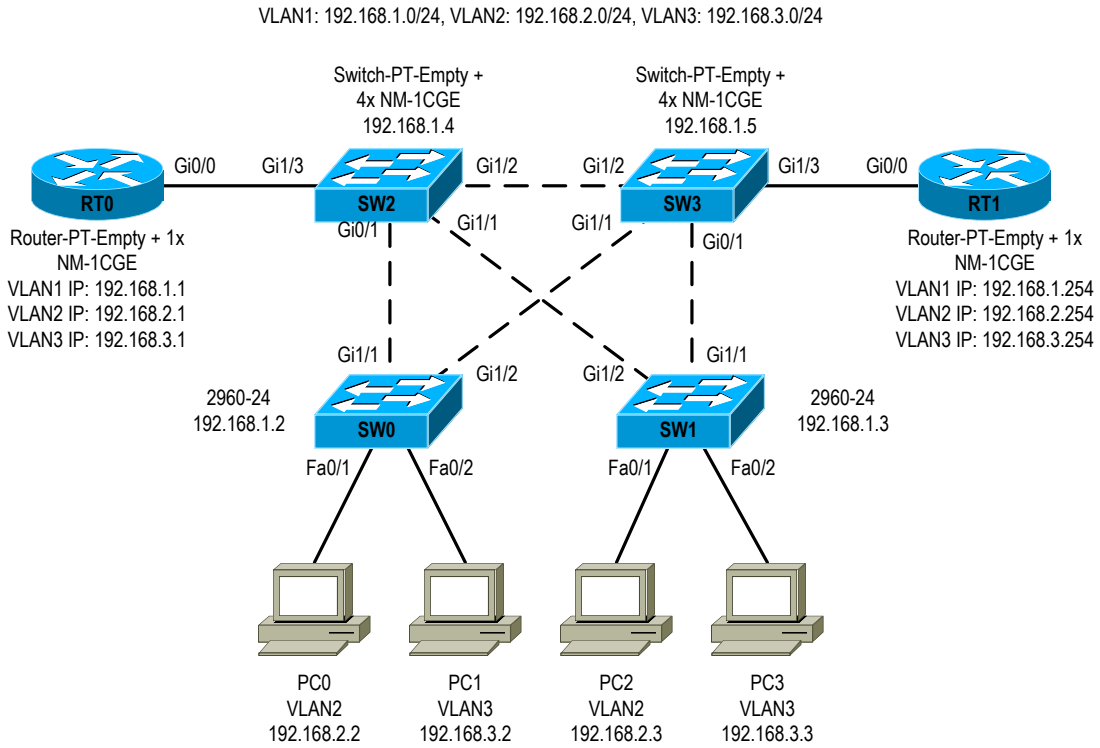
Στο δίκτυο έχουν προστεθεί ένας επιπλέον μεταγωγέας διανομής, ο SW3 και ένας επιπλέον δρομολογητής για το inter-VLAN routing, ο RT1. Στον μεταγωγέα SW2 έχει προστεθεί μια επιπλέον κάρτα NM-1CGE, με μια θύρα Gigabit και ο μεταγωγέας SW3 είναι ίδιος με τον SW2. Επιπλέον ο δρομολογητής RT1 είναι ίδιος με τον RT0. Οι συνδέσεις των συσκευών και οι διευθύνσεις IP είναι όπως στην **Εικόνα 15.7**. Η άσκηση θα γίνει με το λογισμικό προσομοίωσης Cisco Packet Tracer και με εντολές στο Cisco CLI.

Στο δίκτυο αυτό θα υπάρχουν δύο δρομολογητές για κάθε VLAN.Για παράδειγμα για το VLAN2 θα υπάρχει ο 192.168.2.1/24 και ο 192.168.2.254/24. Επειδή όμως οι σταθμοί εργασίας δεν μπορούν να χρησιμοποιήσουν παραπάνω του ενός default gateway, θα εκμεταλλευτούμε τη λειτουργία Proxy-ARP που είναι ενεργή προτερόθετα στους δρομολογητές. Έτσι όλες οι συσκευές δεν θα έχουν ορισμένο default-gateway και θα βασίζονται στο Proxy-ARP των δρομολογητών για να κάνει τη δρομολόγηση.

Συνδυάζοντας τα ζητούμενα των ασκήσεων 13.3 και 15.5, ζητούνται:
α) Να καθοριστεί η μάσκα δικτύου που πρέπει να έχουν οι σταθμοί εργασίας, οι μεταγωγείς και οι δρομολογητές, έτσι ώστε όλοι να κάνουν ping σε όλους. Επιπλέον οι σταθμοί εργασίας θα πρέπει να κάνουν telnet σε μεταγωγείς και δρομολογητές.
β) Οι γραμμές μεταξύ μεταγωγέων να είναι κορμού (trunk), οι γραμμές μεταξύ μεταγωγέων και σταθμών εργασίας να είναι πρόσβασης (access) και portfast, οι γραμμές μεταξύ μεταγωγέων και δρομολογητών να είναι κορμού και portfast.
γ) Να τρέχει Rapid-PVST στους μεταγωγείς, με τον SW2 να είναι primary root και ο SW3 να είναι secondary root. Απώλεια είτε του SW2, είτε του SW3, είτε κάποιας σύνδεσης ανάμεσα σε SW0/SW1 και SW2/SW3 να οδηγεί σε γρήγορη ανάκαμψη (σύγκλιση) του δικτύου. Να βρεθεί πόσος χρόνος (προσεγγιστικά) απαιτείται για τη σύγκλιση.
δ) Να μην τρέχει DTP στις γραμμές κορμού μεταξύ μεταγωγέων.

ε) Οι διεπαφές των δρομολογητών να τρέχουν dot1q, να δημιουργηθούν οι απαιτούμενες υποδιεπαφές και να οριστούν VID και διευθύνσεις IP σε αυτές.

στ) Το δίκτυο να ανακάμπτει από απώλεια δρομολογητή. Να βρεθεί ο χρόνος που απαιτείται για την ανάκαμψη και να αναφερθούν οι τρόποι που μπορεί να επιταχυνθεί αυτός.



Εικόνα 15.7 Διάγραμμα δικτύου για την εργαστηριακή άσκηση **15.6**

16. Πολυεπίπεδη Μεταγωγή

16.1 Εισαγωγή

Όπως ειπώθηκε σε προηγούμενες ενότητες, η εισαγωγή των VLAN και της δρομολόγησης μεταξύ αυτών, ώστε να καλυφθούν οι ανάγκες αύξησης του μεγέθους και της χρήσης των δικτύων, δημιούργησε νέα προβλήματα. Οι δρομολογητές που απαιτούνται για την δρομολόγηση μεταξύ VLAN αποτελούσαν με τη σειρά τους σημεία συμφόρησης και αποτυχίας για το δίκτυο.

Με την εξέλιξη και την μείωση του κόστους της τεχνολογίας, έγινε δυνατή η ενσωμάτωση της λειτουργίας της δρομολόγησης στην ίδια συσκευή με υψηλής ταχύτητας μεταγωγή, η οποία κανονικά συσχετίζεται με μεταγωγείς Ethernet. Η μεταγωγή είναι μια έννοια που έτσι κι αλλιώς βρίσκεται στη βάση της δρομολόγησης, δεδομένου ότι κάθε δρομολογητής πρέπει να κάνει και μεταγωγή, η οποία είναι η διαδικασία μεταβίβασης ενός πλαισίου από μια διεπαφή εισόδου σε μια διεπαφή εξόδου. Ανάλογα με τα κριτήρια που εφαρμόζονται για να ληφθεί η απόφαση της επιλογής της θύρας εξόδου, ανάλογα με το επίπεδο δικτύου που βρίσκονται αυτά, ανάλογα με τις κεφαλίδες που πρέπει να διαβάσει η μηχανή για να πάρει την απόφαση, μπορούμε να πούμε ότι γίνεται και αντίστοιχου επιπέδου μεταγωγή. Έτσι έχουμε:

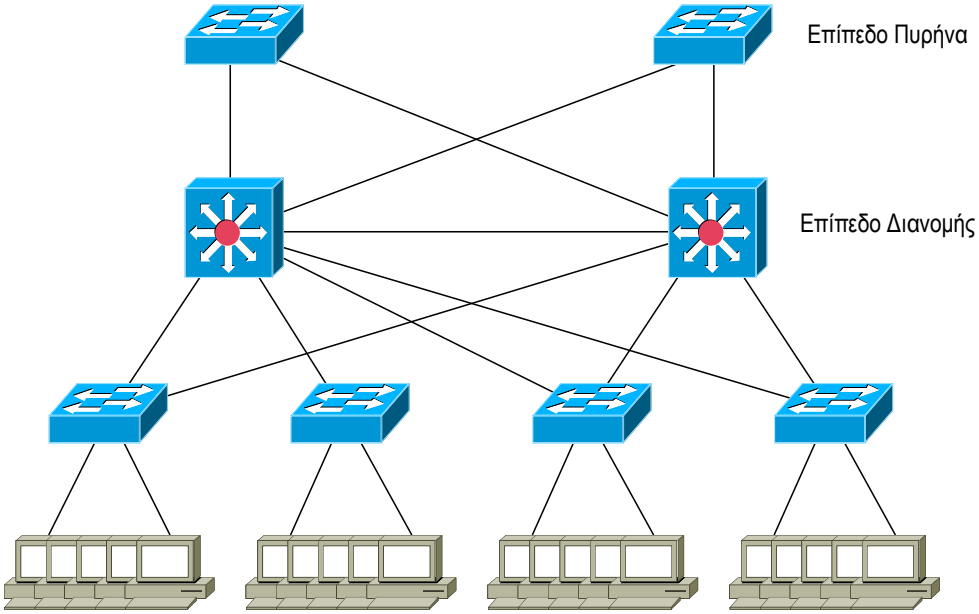
- Μεταγωγή $2^{ου}$ Επιπέδου. Είναι η μεταγωγή που γίνεται με επεξεργασία κεφαλίδων πρωτοκόλλων $2^{ου}$ Επιπέδου δικτύου, όπως το Ethernet. Είναι αυτή που γίνεται από τις κλασικές γέφυρες (*bridges*) και τους μεταγωγείς (*switches*).
- Μεταγωγή $3^{ου}$ Επιπέδου. Είναι η μεταγωγή που γίνεται με επεξεργασία κεφαλίδων πρωτοκόλλων $3^{ου}$ επιπέδου δικτύου, δηλαδή βασικά του IP. Η κλασική έννοια της δρομολόγησης είναι υποσύνολο αυτής της διαδικασίας και αφορά μόνο τις διαδικασίες και τα δεδομένα $3^{ου}$ Επιπέδου (διευθύνσεις IP αποστολέα και παραλήπτη και αναφορά στον πίνακα δρομολόγησης). Η μεταγωγή που γίνεται σε αυτή την περίπτωση αφορά την αποθυλάκωση του πακέτου από το πλαίσιο που ήρθε στην διεπαφή εισόδου και την ενθυλάκωσή του στο πλαίσιο που θα βγει από τη διεπαφή εξόδου. Η επιλογή της διεπαφής εξόδου είναι αποτέλεσμα της δρομολόγησης.

  Είναι σαφές ότι η μεταγωγή $3^{ου}$ Επιπέδου, επειδή ενέχει και δρομολόγηση, είναι πιθανό να εισάγει σημαντική καθυστέρηση. Έτσι οι μεταγωγείς $3^{ου}$ Επιπέδου, χρησιμοποιούν ειδικευμένους μηχανισμούς και υλικό επιτάχυνσης αυτής της διαδικασίας. Οι μεταγωγείς $3^{ου}$ Επιπέδου μπορούν επομένως να θεωρηθούν και ως ειδικευμένοι, υψηλής ταχύτητας δρομολογητές για τοπικά δίκτυα, οι οποίοι διαφέρουν από τους κλασικούς δρομολογητές στο ότι διαθέτουν μεγαλύτερη πυκνότητα διεπαφών Ethernet, λιγότερη ευελιξία σε πρωτόκολλα, μικρότερη πληθώρα τύπων διεπαφών και στο ότι χρησιμοποιούν ειδικό υλικό για την επιτάχυνση της μεταγωγής στο $3^{ο}$ Επίπεδο (ενώ οι δρομολογητές την κάνουν γενικά με τον κεντρικό τους επεξεργαστή).

- Μεταγωγείς 4^{ου} έως και 7^{ου} Επιπέδου. Είναι ειδικές συσκευές που παίρνουν την απόφαση μεταγωγής με δεδομένα πρωτοκόλλων συνόδου (*session*) έως και εφαρμογής (*application*) και χρησιμοποιούνται συνήθως, είτε για κατανομή φορτίου (*load balancing*) σε πολλαπλούς εξυπηρετητές, είτε για επιτάχυνση εφαρμογών (*application acceleration*), είτε και για τα δύο. Χρησιμοποιούνται τυπικά από κέντρα μηχανογράφησης (*data centers*), λειτουργούν με πολύπλοκους κανόνες και πολλές φορές ενέχουν εις βάθος γνώση των εφαρμογών που κατανέμουν/επιταχύνουν. Συχνά ονομάζονται μεταγωγείς υπηρεσιών περιεχομένου (*content services switches*). Παράδειγμα αποτελεί η κατανομή φορτίου ιστοσελίδας που εξυπηρετείται από μία διεύθυνση IP και ένα FQDN, σε πολλές και διαφορετικές ομάδες εξυπηρετητών ιστού (*web servers*) και εφαρμογών (*application servers*), ανάλογα με την ιστο-εφαρμογή που ζητά ο χρήστης.

Λόγω των παραπάνω, η μεταγωγή επιπέδου ανώτερου από το 2^{ο}, ονομάζεται πολλές φορές πολυεπίπεδη μεταγωγή, ιδίως αν χρησιμοποιεί δεδομένα πρωτοκόλλων επιπέδου ανωτέρου από το 3^{ο}. Στην ενότητα αυτή όμως θα εξετάσουμε μόνο τη μεταγωγή 3^{ου} Επιπέδου (*Layer 3 switching*).

Οι μεταγωγείς 3^{ου} Επιπέδου χρησιμοποιούνται κατά κόρον σε σύγχρονες, υψηλής απόδοσης αρχιτεκτονικές δικτύου. Μπορούν να χρησιμοποιηθούν σε οποιοδήποτε επίπεδο δικτύου (πρόσβασης, διανομής, ή πυρήνα), ανάλογα με τις απαιτήσεις και την οικονομική δυνατότητα του κατόχου τους. Διασφαλίζουν μεταγωγή 3^{ου} Επιπέδου, σχεδόν με ταχύτητα καλωδίου (*near wire speed L3 switching*), εισάγοντας κατά μέσο όρο ελαφρά μόνο μεγαλύτερη καθυστέρηση από τους μεταγωγείς 2^{ου} Επιπέδου. Για τη χρήση τους προτείνονται τα ακόλουθα:
α) Η καλύτερη χρήση τους είναι στο επίπεδο διανομής, **Εικόνα 16.1**. Εκεί μπορούν να διανέμουν με βέλτιστο τρόπο μεταξύ των VLAN και των επιπέδων πρόσβασης σταθμών εργασίας και εξυπηρετητών. Με αυτούς είναι δυνατή η ανάπτυξη του δικτύου σε μεγάλα μεγέθη, με υποστήριξη 10άδων VLAN, 1000άδων σταθμών εργασίας και 100άδων εξυπηρετητών. Με τη χρήση πρωτοκόλλων δρομολόγησης, όπως το OSPF, είναι δυνατόν να ανταποκριθούν σε μεταβαλλόμενες συνθήκες δικτύου, όσον αφορά το φορτίο και την αντιμετώπιση βλαβών και να διασφαλίσουν αποτελεσματική δρομολόγηση και κατανομή της κίνησης.

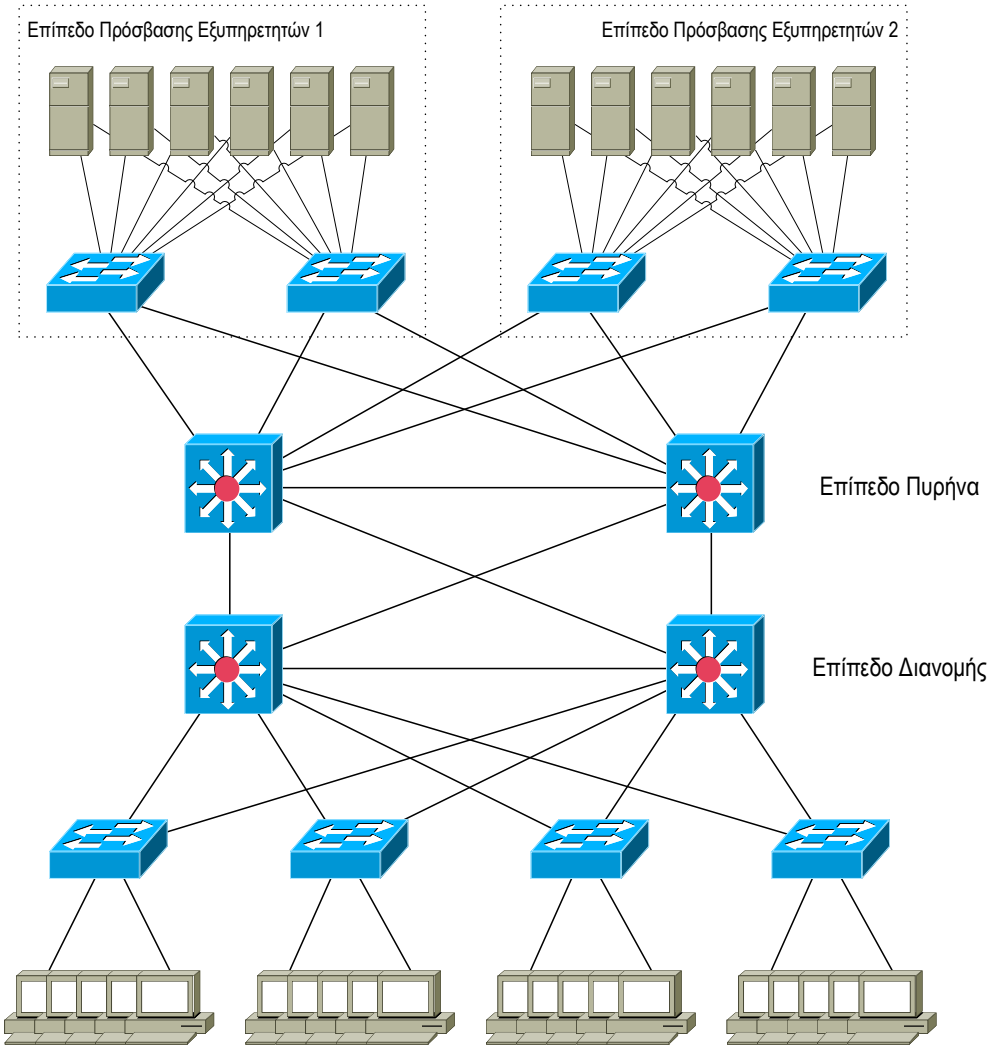


Εικόνα 16.1 Χρήση μεταγωγέων L3 στο επίπεδο διανομής

β) Στο επίπεδο πρόσβασης δεν είναι συνηθισμένη η χρήση μεταγωγέων L3, εκτός από τις περιπτώσεις μεγάλων κέντρων με υποδομές ιδεατών συστημάτων (*virtualization infrastructure*). Οι μεταγωγείς L3 είναι ακόμα αρκετά ακριβή τεχνολογία και στο επίπεδο πρόσβασης, ιδίως αν πρόκειται για επίπεδο πρόσβασης χρηστών, δεν χρειάζεται.

γ) Στο επίπεδο κορμού, εάν πρέπει να χρησιμοποιηθούν μεταγωγείς L3, είναι σημαντικό να είναι υψηλής ταχύτητας (*wire speed*), ώστε να μην εισάγουν καθυστέρηση στη μεταγωγή στον πυρήνα του δικτύου. Γι' αυτό το λόγο, τυπικά στο επίπεδο κορμού χρησιμοποιούνται υψηλής ταχύτητας μεταγωγείς 2^{ου} Επιπέδου. Λόγοι για τη χρήση μεταγωγέων 3^{ου} Επιπέδου στο επίπεδο κορμού μπορεί να είναι:

- Διασύνδεση μεγάλου αριθμού επιπέδων διανομής, σε ένα μεγάλο δίκτυο. Σε αυτή την περίπτωση, μεταγωγείς L3 στο επίπεδο κορμού παρέχουν βέλτιστη δρομολόγηση μεταξύ των εκατοντάδων VLAN που μπορεί να υπάρχουν στο δίκτυο.
- Διασύνδεση πολλών επιπέδων πρόσβασης εξυπηρετητών. Αν για παράδειγμα πρόκειται για ένα δίκτυο μεταξύ κτιρίων και κάθε κτίριο έχει το δικό του επίπεδο διανομής εξυπηρετητών, μεταγωγείς L3 στον κορμό παρέχουν βέλτιστη δρομολόγηση της κίνησης μεταξύ αυτών, **Εικόνα 16.2**.
- Χωρισμός του δικτύου σε ζώνες (σύνολα από VLAN) και υλοποίηση κανόνων διακριτικής πρόσβασης μεταξύ αυτών. Σε αυτή την περίπτωση πρέπει να δοθεί ιδιαίτερη προσοχή, έτσι ώστε η υλοποίηση των κανόνων να μην απενεργοποιεί μηχανισμούς που επιταχύνουν τη μεταγωγή L3 στους μεταγωγείς. Λόγω αυτού, σε πολλές περιπτώσεις, για την υλοποίηση της ως άνω ανάγκης χρησιμοποιούνται ειδικευμένες συσκευές τείχους (*firewalls*), ενσωματωμένες ή μη στους μεταγωγείς.



Εικόνα 16.2 Χρήση μεταγωγέων L3 στο επίπεδο πυρήνα.

Η διαδικασία της μεταγωγής 3^{ου} Επιπέδου δεν διαφέρει στη βάση της από αυτήν που κάνουν οι δρομολογητές. Δηλαδή:

α) Αποθυλακώνεται το πακέτο IP από το πλαίσιο Ethernet (δηλαδή αφαιρείται η κεφαλίδα και το ουραίο).

β) Γίνεται έλεγχος της διεύθυνσης παραλήπτη στην κεφαλίδα IP, αναζητείται η καλύτερη (πιο ειδική) εγγραφή στον πίνακα δρομολόγησης (*routing table*) και βάση αυτής λαμβάνεται η απόφαση για το από ποια διεπαφή πρέπει να βγει το πακέτο.

γ) Μειώνεται κατά ένα το TTL στην κεφαλίδα του IP.

δ) Δημιουργείται ένα νέο πλαίσιο Ethernet με διεύθυνση MAC αποστολέα αυτή του L3 μεταγωγέα και MAC παραλήπτη αυτή του παραλήπτη ή της επόμενης πύλης (γίνεται ARP request αν χρειαστεί) και υπολογίζεται νέο FCS.

Η παραπάνω διαδικασία ονομάζεται μεταγωγή πακέτο-προς-πακέτο (*packet-by-packet switching*) και γίνεται τυπικά από routers (είναι βαριά για τον κεντρικό επεξεργαστή, *CPU intensive*). Οι μεταγωγείς L3 εφαρμόζουν τυπικά πιο γρήγορες

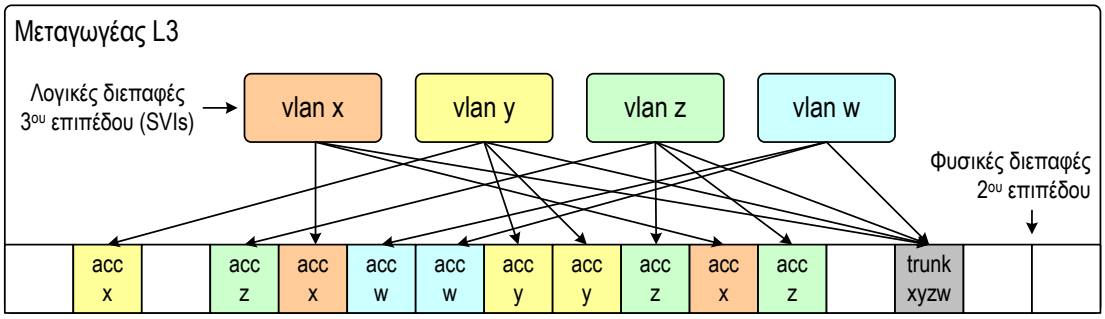
μεθόδους που βασίζονται σε ειδικευμένο κεντρικό ή κατανεμημένο υλικό (CEF, dCEF κτλ.)

16.2 Μεταγωγή 3ου Επιπέδου σε Cisco CLI

Σημείωση: Για την περιγραφή της έννοιας των διεπαφών 3ου Επιπέδου των μεταγωγέων της Cisco, θα χρησιμοποιήσουμε σε αυτό το εγχειρίδιο ως εκπαιδευτικό εργαλείο την ιδέα της 'αναβάθμισης των VLAN στο 3ο επίπεδο'. Αυστηρά τεχνικά ωστόσο, θα αναφερθούμε στη δημιουργία των λεγόμενων ιδεατών διεπαφών μεταγωγής (*switched virtual interfaces*, SVIs).

Για την παραμετροποίηση των μεταγωγέων 3ου Επιπέδου η Cisco χρησιμοποιεί τη μέθοδο της αναβάθμισης των VLAN, από οντότητες 2ου Επιπέδου σε οντότητες 3ου Επιπέδου. Σε προηγούμενη ενότητα είχαμε δει τη δυνατότητα που έχουν οι συμβατικοί μεταγωγείς 2ου Επιπέδου να ορίζουν μία (και μοναδική) διεπαφή 3ου επιπέδου, βάση του διαχειριστικού VLAN (το οποίο προτερόθετα είναι το VLAN1), ώστε να είναι δυνατή η απομακρυσμένη διαχείρισή τους.

Κατά τον ίδιο τρόπο, σε ένα μεταγωγέα 3ου Επιπέδου, αφού οριστεί ένα VLAN ως οντότητα 2ου Επιπέδου, μπορεί να αναβαθμιστεί σε οντότητα 3ου Επιπέδου και να του δοθεί IP. Αυτή η λογική ιδεατή διεπαφή είναι καθόλα εφάμιλλη με τη διεπαφή ενός δρομολογητή και σε αυτήν 'ακούει' ο ενσωματωμένος στον μεταγωγέα δρομολογητής, σε οποιοδήποτε πακέτο απευθυνθεί σε αυτήν (στην διεύθυνση IP της), μέσω του αντίστοιχου VLAN 2ου επιπέδου, δηλαδή είτε μέσω θυρών πρόσβασης που έχουν τοποθετηθεί στο VLAN αυτό, είτε μέσω θυρών κορμού από τις οποίες περνάει, **Εικόνα 15.3**. Δηλαδή η IP της ιδεατής διεπαφής εμφανίζεται στο δίκτυο εντός του VLAN που της αντιστοιχεί και μπορεί να χρησιμοποιηθεί σαν πύλη (gateway) δρομολόγησης, σαν να ήταν μια φυσική διεπαφή. Αν ο μεταγωγέας έχει μία ή περισσότερες φυσικές θύρες (2ου Επιπέδου) σε αυτό το VLAN, τότε αυτή η διεύθυνση ανήκει σε όλες αυτές. Αν όχι, τότε 'απαντά' μέσω των γραμμών κορμού από τις οποίες περνά αυτό το VLAN.



Εικόνα 16.3 Λογικές συνδέσεις διεπαφής 3ου επιπέδου (SVI) και θυρών πρόσβασης και κορμού

Η εντολή με την οποία ορίζεται ένα SVI σε ένα μεταγωγέα 3ου επιπέδου είναι η ίδια με την εντολή που ορίζεται το διαχειριστικό VLAN σε ένα μεταγωγέα 2ου επιπέδου.

Έτσι για να ορίσουμε ένα VLAN 2ου επιπέδου, να δημιουργήσουμε το αντίστοιχο SVI και να του δώσουμε διεύθυνση IP δίνουμε:

```
Switch(config)# vlan VLAN#
Switch(config)# interface vlan VLAN#
Switch(config-if)# ip address ip_address subnet_mask
```

Για παράδειγμα, για να ορίσουμε το VLAN100 και να του δώσουμε τη διεύθυνση IP 192.168.100.250/24 δίνουμε:

```
Switch(config)# vlan 100
Switch(config)# interface vlan100
Switch(config-if)# ip address 192.168.100.250 255.255.255.0
```

Υπενθυμίζεται ότι το VLAN μπορεί να μην χρειάζεται να οριστεί γιατί μπορεί να το έχει μάθει ο μεταγωγέας μέσω του VTP. Για να δούμε όλες τις διεπαφές 3ου Επιπέδου ενός μεταγωγέα, δίνουμε όπως ακριβώς και σε ένα δρομολογητή:

```
Switch# show ip interface
```

Μετά τη δημιουργία των διεπαφών 3ου Επιπέδου, πρέπει να ενεργοποιήσουμε τη δρομολόγηση 3ου Επιπέδου, διαφορετικά ο μεταγωγέας L3 δεν θα δρομολογεί μεταξύ των διεπαφών αυτών και άρα και των VLAN (το αν η λειτουργία αυτή είναι προτερόθετα ανοικτή εξαρτάται από το μοντέλο του μεταγωγέα). Η εντολή είναι:

```
Switch(config)# ip routing
```

Όπως και στους δρομολογητές, μπορούμε να δούμε τον πίνακα δρομολόγησης του L3 μεταγωγέα με την εντολή:

```
Switch# show ip route
```

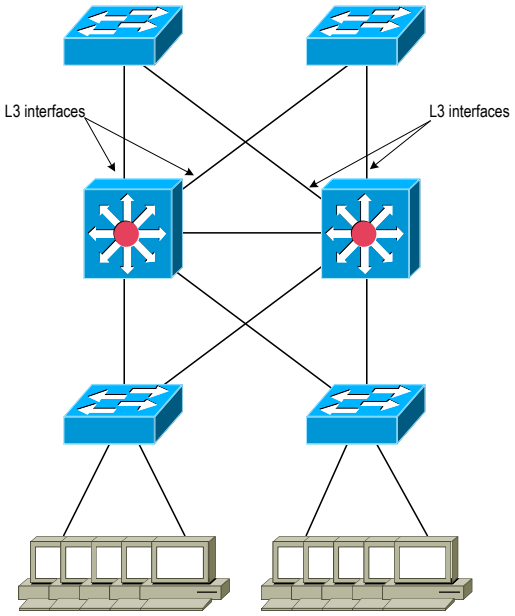
Κανονικά μια φυσική διεπαφή ενός Ethernet μεταγωγέα δεν μπορεί να πάρει IP γιατί αποτελεί οντότητα 2ου Επιπέδου και μετάγει μόνο Ethernet, όχι IP. Σε ένα μεταγωγέα L3 όμως, μια φυσική διεπαφή μπορεί να ρυθμιστεί ως διεπαφή 3ου Επιπέδου και να της δοθεί διεύθυνση IP, σαν να επρόκειτο για μια φυσική διεπαφή δρομολογητή.

Λόγοι για να γίνει αυτό μπορεί είναι:

- Να αποτελεί αυτή η διεπαφή σημείο συνόρου. Με αυτό τον τρόπο μια γραμμή που διαφορετικά θα ήταν γραμμή κορμού μπορεί να χρησιμοποιηθεί για να διακοπεί η μεταγωγή 2ου Επιπέδου, έτσι ώστε περιοριστεί η διανομή των VLAN και το μέγεθος (και το φορτίο) του δέντρου STP. Ένα τέτοιο παράδειγμα φαίνεται στην **Εικόνα 16.4**, όπου οι περιοχές διανομής συνδέονται σε μια περιοχή κορμού, που για λόγους ταχύτητας και οικονομίας χρησιμοποιεί μεταγωγή 2ου Επιπέδου. Άλλη περίπτωση θα μπορούσε να είναι

η σύνδεση μέσω Ethernet με το δίκτυο ενός τρίτου οργανισμού, όπως π.χ. με κάποιο πάροχο σύνδεσης στο Internet.

- Σύνδεση με κάποια συσκευή που δεν υποστηρίζει σύνδεση κορμού, όπως για παράδειγμα ένα *firewall* που δεν υποστηρίζει (ή δεν έχει αδειοδοτηθεί γι' αυτό) VLANs.



Εικόνα 16.4 Σύνδεση L3 μεταγωγέων διανομής στον πυρήνα με διεπαφές 3ου Επιπέδου

Για να ρυθμιστεί μια θύρα μεταγωγέα L3 ως θύρα 3ου Επιπέδου και να της δώσουμε διεύθυνση IP, δίνουμε τις εντολές:

```
Switch(config)# interface type [slot#]/port#
Switch(config-if)# no switchport
Switch(config-if)# ip address ip_address subnet_mask
```

Για παράδειγμα, για να δοθεί η διεύθυνση 192.168.1.10 στη διεπαφή gigabitEthernet0/1 δίνουμε:

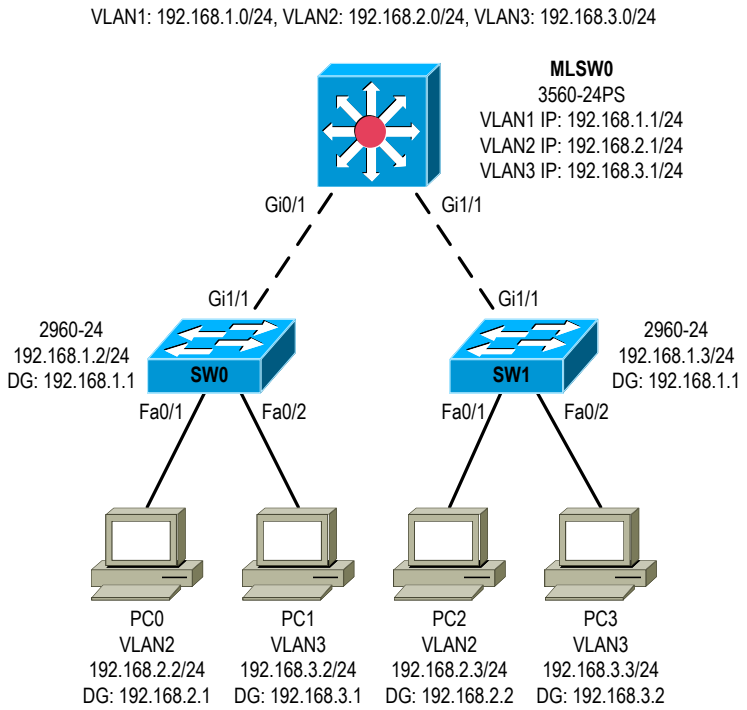
```
Switch(config)# interface gigabitEthernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.1.10 255.255.255.0
```

Κατά τα άλλα, στους μεταγωγείς L3 ισχύει ουσιαστικά ό,τι έχει παρουσιαστεί τόσο για μεταγωγείς 2ου Επιπέδου, όσο και για δρομολογητές. Έτσι οι ρυθμίσεις για το PVST+, Rapid-PVST, VLAN, θύρες πρόσβασης/κορμού, VTP, καθώς και πρωτόκολλα δρομολόγησης είναι οι ίδιες. Τυπικά, τα μόνα που δεν ισχύουν είναι αυτά που αφορούν συνδέσεις WAN, όπως σειριακές, frame relay, ATM κλπ.

Σημειώνεται ότι στην κορυφή των προσφερόμενων από τους κατασκευαστές συσκευών, υπάρχουν μεταγωγείς WAN οι οποίοι δεν διαφέρουν από δρομολογητές (και το αντίστροφο), θολώνοντας τη διαφορά μεταξύ μεταγωγέων και δρομολογητών.

16.3 Εργαστηριακή άσκηση

Στην άσκηση αυτή, θα ενσωματώσουμε τον δρομολογητή της άσκησης **13.3** στον μεταγωγέα διανομής, χρησιμοποιώντας ένα L3 μεταγωγέα. Με αυτό τον τρόπο θα έχουμε όλα τα πλεονεκτήματα της μεταγωγής 3^{ου} επιπέδου και ένα σημείο πιθανής αστοχίας λιγότερο (τον δρομολογητή και τη σύνδεσή του με τον μεταγωγέα). Η άσκηση θα γίνει με το λογισμικό προσομοίωσης Cisco Packet Tracer και με εντολές στο Cisco CLI.
Το διάγραμμα δικτύου φαίνεται στην **Εικόνα 16.5**.



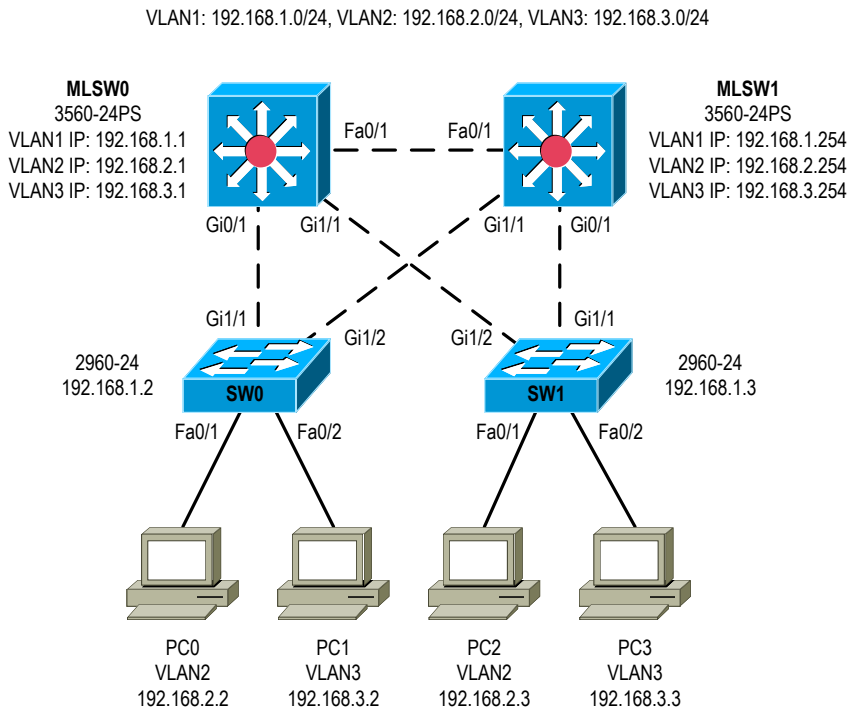
Εικόνα 16.5 Διάγραμμα δικτύου για την εργαστηριακή άσκηση **16.3**

Τα ζητούμενα είναι τα ίδια με την άσκηση **13.3**, απλώς αντί να ρυθμιστεί ο μεταγωγέας SW2 και ο δρομολογητής RT0, πρέπει να ρυθμιστεί ο πολυεπίπεδος μεταγωγέας MLSW0, ο οποίος θα είναι και VTP server για το v2 VTP domain “d1” με VTP password “p1” (χωρίς τα εισαγωγικά).

16.4 Εργαστηριακή άσκηση

Στην άσκηση αυτή, θα ενσωματώσουμε τους δρομολογητές της άσκησης **15.6** στους μεταγωγείς διανομής, χρησιμοποιώντας δύο L3 μεταγωγείς. Η άσκηση θα γίνει με το λογισμικό προσομοίωσης Cisco Packet Tracer και με εντολές στο Cisco CLI.

Το διάγραμμα δικτύου φαίνεται στην **Εικόνα 16.6**.



Εικόνα 16.6 Διάγραμμα δικτύου για την εργαστηριακή άσκηση **15.4**

Τα ζητούμενα είναι τα ίδια με την άσκηση **15.6**, απλώς αντί να ρυθμιστούν οι μεταγωγείς SW2/SW3 και οι δρομολογητές RT0/RT1, πρέπει να ρυθμιστούν οι πολυεπίπεδοι μεταγωγείς διανομής MLSW0/MLSW1, οι οποίοι θα είναι και VTP servers για το v2 VTP domain “d1” με VTP password “p1” (χωρίς τα εισαγωγικά) και Rapid-STR primary και secondary root, αντίστοιχα. Το δίκτυο θα πρέπει να ανακάμπτει από απώλεια μεταγωγέα διανομής ή σύνδεσης μεταξύ των επιπέδων πρόσβασης και διανομής. Θα πρέπει να βρεθεί ο χρόνος που απαιτείται για την ανάκαμψη και να αναφερθούν οι τρόποι που μπορεί να επιταχυνθεί αυτός.

Σημειώνεται ότι επειδή δεν υποστηρίζεται από το Packet Tracer πολυεπίπεδος μεταγωγέας με τρεις θύρες Gigabit Ethernet, η οριζόντια σύνδεση μεταξύ των μεταγωγέων διανομής είναι Fast Ethernet και γι’ αυτό το λόγο διακόπτεται από το STP.

ΠΑΡΑΡΤΗΜΑ Ασκήσεις Υποδικτύωσης

Μετατροπή δυαδικών αριθμών στο δεκαδικό σύστημα

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		**Απάντηση**
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**		
1	1	1	1	1	0	0	0	=	***248***
1	0	0	0	0	0	0	0	=	
1	1	1	0	1	1	1	1	=	
0	0	0	1	1	1	1	1	=	
1	1	1	1	0	0	0	0	=	
1	0	1	0	1	0	1	0	=	
1	1	0	0	1	1	1	1	=	
0	1	0	0	1	1	0	0	=	
1	1	1	0	0	0	0	0	=	
0	1	0	1	0	1	0	1	=	
0	1	1	1	1	1	1	1	=	
0	0	0	1	1	1	1	0	=	
1	1	0	0	0	0	0	0	=	
0	0	1	1	0	1	1	0	=	
0	0	1	1	1	1	1	1	=	
1	1	0	0	1	1	0	0	=	
1	1	1	1	1	1	1	0	=	
0	0	0	0	1	1	0	0	=	
0	0	1	1	0	0	1	1	=	
0	0	0	1	1	0	1	1	=	
1	1	1	1	1	1	1	1	=	

Μετατροπή δεκαδικών αριθμών στο δυαδικό σύστημα

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		**Δεκαδική τιμή**
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**		
1	**0**	**0**	**0**	**0**	**0**	**0**	**1**	=	129
								=	235
								=	127
								=	224
								=	202
								=	123
								=	69
								=	35
								=	170
								=	38
								=	240
								=	199
								=	89
								=	252
								=	159
								=	142
								=	56
								=	15
								=	63
								=	252

= 120

Συμπληρώστε τη σωστή κλάση

Διεύθυνση	Κλάση	Διεύθυνση	Κλάση
178.35.22.7	***B***	127.10.220.3	
12.43.221.6		222.35.22.10	
193.68.76.32		180.199.2.42	
128.169.232.5		192.39.33.123	
224.0.0.10		239.10.105.2	
10.28.57.5		179.202.33.2	
221.0.0.3		124.152.67.43	
169.254.32.25		199.10.45.2	
118.19.20.30		35.47.127.4	
185.45.125.43		201.18.7.25	
198.65.124.233		179.135.98.65	
171.131.254.3		227.35.27.165	
126.5.67.23		223.191.23.7	
132.45.76.132		150.65.47.32	
217.69.75.5		120.32.43.59	
190.32.65.78		242.120.42.231	
203.22.65.123		170.77.128.4	
89.49.165.255		195.123.65.9	
168.56.43.9		124.178.169.35	
128.0.0.2		200.45.32.6	
121.35.48.187		130.15.66.43	
135.169.32.25		119.232.56.89	

Default Μάσκα Υποδικτύωσης

Διεύθυνση	Μάσκα	Διεύθυνση	Μάσκα
221.44.32.5	***255.255.255.0***	124.178.169.35	
185.45.125.43		171.131.254.3	
118.19.20.30		126.5.67.23	
89.49.165.255		221.35.27.165	
132.45.76.132		12.43.221.6	
35.47.127.4		170.77.128.4	
178.35.22.7		179.135.98.65	
127.10.220.3		193.68.76.32	
217.69.75.5		223.191.23.7	
150.65.47.32		179.202.33.2	
192.39.33.123		10.28.57.5	
221.0.0.3		199.10.45.2	
168.56.43.9		198.65.124.233	
169.254.32.25		128.169.232.5	
128.0.0.2		203.22.65.123	
135.169.32.25		119.232.56.89	
180.199.2.42		152.10.105.2	
222.35.22.10		120.32.43.59	
124.152.67.43		121.35.48.187	
210.120.42.231		195.123.65.9	
200.45.32.6		190.32.65.78	
130.15.66.43		201.18.7.25	

Υπολογίστε τη διεύθυνση δικτύου (χρησιμοποιώντας τη μάσκα!!!)

221.44.32.139 255.255.255.240	**221.44.32.128**
124.178.169.35 255.224.0.0	
185.45.125.43 255.255.248.0	
192.39.33.123 255.255.255.224	
128.169.232.5 255.255.224.0	
152.10.105.2 255.255.192.0	
130.15.66.43 255.255.252.0	
201.18.7.25 255.255.255.224	
195.130.75.230 255.255.255.192	
172.17.67.135 255.255.192.0	
10.38.152.3 255.255.128.0	
192.168.37.201 255.255.255.224	
121.35.48.187 255.255.224.0	

Υπολογίστε τη διεύθυνση δικτύου (χρησιμοποιώντας το prefix!!!)

10.122.65.32 /12	**10.112.0.0 /12**
192.168.231.67 /26	
172.19.131.57 /19	
220.35.128.231 /28	
169.253.28.35 /12	
18.131.24.131 /12	
195.130.76.103 /28	
128.129.130.131 /20	
67.70.75.2 /14	
199.35.248.151 /20	
132.37.221.112 /19	
126.199.32.61 /15	
223.152.49.135 /19	

Υποδικτύωση – Παράδειγμα απλής άσκησης

Διεύθυνση Δικτύου	***192.168.35.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***10***
Αριθμός hosts που χρειαζόμαστε	***10***

Default μάσκα υποδικτύωσης	***255.255.255.0***
Δυαδικά ψηφία που δανειζόμαστε	***4***
Προσαρμοσμένη μάσκα υποδικτύωσης	***255.255.255.240***
Αριθμός υποδικτύων	$2^4 = 16$
Αριθμός έγκυρων υποδικτύων	$2^4-2 = 14$
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	$2^4 = 16$
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	$2^4-2 = 14$

Υποδικτύωση – Απλή Άσκηση 1

Διεύθυνση Δικτύου	***172.16.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***1000***
Αριθμός hosts που χρειαζόμαστε	***50***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 2

Διεύθυνση Δικτύου	***10.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***4000***
Αριθμός hosts που χρειαζόμαστε	***4000***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 3

Διεύθυνση Δικτύου	***195.130.75.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***28***
Αριθμός hosts που χρειαζόμαστε	***6***
Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 4

Διεύθυνση Δικτύου	***101.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***200***
Αριθμός hosts που χρειαζόμαστε	***52000***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 5

Διεύθυνση Δικτύου	***220.10.63.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***9***
Αριθμός hosts που χρειαζόμαστε	***12***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 6

Διεύθυνση Δικτύου	***120.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***60***
Αριθμός hosts που χρειαζόμαστε	***150000***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 7

Διεύθυνση Δικτύου	***132.10.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***240***
Αριθμός hosts που χρειαζόμαστε	***190***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 8

Διεύθυνση Δικτύου	***163.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***3***
Αριθμός hosts που χρειαζόμαστε	***7000***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 9

Διεύθυνση Δικτύου	***7.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***120***
Αριθμός hosts που χρειαζόμαστε	***100000***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 10

Διεύθυνση Δικτύου	***192.168.10.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***1***
Αριθμός hosts που χρειαζόμαστε	***60***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 11

Διεύθυνση Δικτύου	***200.32.120.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***57***
Αριθμός hosts που χρειαζόμαστε	***2***
Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 12

Διεύθυνση Δικτύου	***160.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***13***
Αριθμός hosts που χρειαζόμαστε	***3500***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 13

Διεύθυνση Δικτύου	***125.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***8000***
Αριθμός hosts που χρειαζόμαστε	***2000***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 14

Διεύθυνση Δικτύου	***199.23.67.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***2***
Αριθμός hosts που χρειαζόμαστε	***58***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 15

Διεύθυνση Δικτύου	***175.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***57***
Αριθμός hosts που χρειαζόμαστε	***900***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 16

Διεύθυνση Δικτύου	***18.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***15000***
Αριθμός hosts που χρειαζόμαστε	***1000***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 17

Διεύθυνση Δικτύου	***205.102.4.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***5***
Αριθμός hosts που χρειαζόμαστε	***29***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 18

Διεύθυνση Δικτύου	***190.120.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***120***
Αριθμός hosts που χρειαζόμαστε	***2000***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 19

Διεύθυνση Δικτύου	***19.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***30000***
Αριθμός hosts που χρειαζόμαστε	***495***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Απλή Άσκηση 20

Διεύθυνση Δικτύου	***129.23.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***29***
Αριθμός hosts που χρειαζόμαστε	***1900***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	

Υποδικτύωση – Παράδειγμα Σύνθετης Άσκησης

Διεύθυνση Δικτύου	***195.130.75.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***12***
Αριθμός hosts που χρειαζόμαστε	***12***

Default μάσκα υποδικτύωσης	***255.255.255.0***
Δυαδικά ψηφία που δανειζόμαστε	***4***
Προσαρμοσμένη μάσκα υποδικτύωσης	***255.255.255.240***
Αριθμός υποδικτύων	***16***
Αριθμός έγκυρων υποδικτύων	***14***
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	***16***
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	***14***
Ποιο είναι το εύρος του 3ου χρήσιμου υποδικτύου;	***195.130.75.48-195.130.75.63***
Ποια είναι η διεύθυνση δικτύου του 13ου χρήσιμου υποδικτύου;	***195.130.75.208***
Ποια είναι η broadcast διεύθυνση του 6ου υποδικτύου;	***195.130.75.111***
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 10ο χρήσιμο υποδίκτυο;	***195.130.75.161-195.130.75.174***

Υποδικτύωση – Σύνθετη Άσκηση 1

Διεύθυνση Δικτύου	***199.99.99.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***5***
Αριθμός hosts που χρειαζόμαστε	***28***
Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Ποιο είναι το εύρος του 2ου χρήσιμου υποδικτύου;	
Ποια είναι η διεύθυνση δικτύου του 5ου χρήσιμου υποδικτύου;	
Ποια είναι η broadcast διεύθυνση του 4ου υποδικτύου;	
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 3ο χρήσιμο υποδίκτυο;	

Υποδικτύωση – Σύνθετη Άσκηση 2

Διεύθυνση Δικτύου	***172.16.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***28***
Αριθμός hosts που χρειαζόμαστε	***1800***
Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Ποιο είναι το εύρος του 12ου χρήσιμου υποδικτύου;	
Ποια είναι η διεύθυνση δικτύου του 22ου χρήσιμου υποδικτύου;	
Ποια είναι η broadcast διεύθυνση του 8ου υποδικτύου;	
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 29ο χρήσιμο υποδίκτυο;	

Υποδικτύωση – Σύνθετη Άσκηση 3

Διεύθυνση Δικτύου	***10.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***120***
Αριθμός hosts που χρειαζόμαστε	***130.000***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Ποιο είναι το εύρος του 15ου χρήσιμου υποδικτύου;	
Ποια είναι η διεύθυνση δικτύου του 110ου χρήσιμου υποδικτύου;	
Ποια είναι η broadcast διεύθυνση του 80ου υποδικτύου;	
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 72ο χρήσιμο υποδίκτυο;	

Υποδικτύωση – Σύνθετη Άσκηση 4

Διεύθυνση Δικτύου	***192.168.12.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***26***
Αριθμός hosts που χρειαζόμαστε	***4***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Ποιο είναι το εύρος του 10ου χρήσιμου υποδικτύου;	
Ποια είναι η διεύθυνση δικτύου του 7ου χρήσιμου υποδικτύου;	
Ποια είναι η broadcast διεύθυνση του 2ου υποδικτύου;	
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 18ο χρήσιμο υποδίκτυο;	

Υποδικτύωση – Σύνθετη Άσκηση 5

Διεύθυνση Δικτύου	***17.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***800***
Αριθμός hosts που χρειαζόμαστε	***16000***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Ποιο είναι το εύρος του 400ου χρήσιμου υποδικτύου;	
Ποια είναι η διεύθυνση δικτύου του 100ου χρήσιμου υποδικτύου;	
Ποια είναι η broadcast διεύθυνση του 200ου υποδικτύου;	
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 300ο χρήσιμο υποδίκτυο;	

Υποδικτύωση – Σύνθετη Άσκηση 6

Διεύθυνση Δικτύου	***190.50.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***80***
Αριθμός hosts που χρειαζόμαστε	***480***
Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Ποιο είναι το εύρος του 70ου χρήσιμου υποδικτύου;	
Ποια είναι η διεύθυνση δικτύου του 21ου χρήσιμου υποδικτύου;	
Ποια είναι η broadcast διεύθυνση του 39ου υποδικτύου;	
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 48ο χρήσιμο υποδίκτυο;	

Υποδικτύωση – Σύνθετη Άσκηση 7

Διεύθυνση Δικτύου	***23.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***4000***
Αριθμός hosts που χρειαζόμαστε	***4000***
Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Ποιο είναι το εύρος του 15ου χρήσιμου υποδικτύου;	
Ποια είναι η διεύθυνση δικτύου του 38ου χρήσιμου υποδικτύου;	
Ποια είναι η broadcast διεύθυνση του 113ου υποδικτύου;	
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 600ο χρήσιμο υποδίκτυο;	

Υποδικτύωση – Σύνθετη Άσκηση 8

Διεύθυνση Δικτύου	***197.130.63.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***60***
Αριθμός hosts που χρειαζόμαστε	***2***
Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Ποιο είναι το εύρος του 25ου χρήσιμου υποδικτύου;	
Ποια είναι η διεύθυνση δικτύου του 32ου χρήσιμου υποδικτύου;	
Ποια είναι η broadcast διεύθυνση του 13ου υποδικτύου;	
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 51ο χρήσιμο υποδίκτυο;	

Υποδικτύωση – Σύνθετη Άσκηση 9

Διεύθυνση Δικτύου	***135.18.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***58***
Αριθμός hosts που χρειαζόμαστε	***900***
Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Ποιο είναι το εύρος του 31ου χρήσιμου υποδικτύου;	
Ποια είναι η διεύθυνση δικτύου του 29ου χρήσιμου υποδικτύου;	
Ποια είναι η broadcast διεύθυνση του 12ου υποδικτύου;	
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 57ο χρήσιμο υποδίκτυο;	

Υποδικτύωση – Σύνθετη Άσκηση 10

Διεύθυνση Δικτύου	***120.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***2100***
Αριθμός hosts που χρειαζόμαστε	***8050***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Ποιο είναι το εύρος του 210ου χρήσιμου υποδικτύου;	
Ποια είναι η διεύθυνση δικτύου του 420ου χρήσιμου υποδικτύου;	
Ποια είναι η broadcast διεύθυνση του 105ου υποδικτύου;	
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 17ο χρήσιμο υποδίκτυο;	

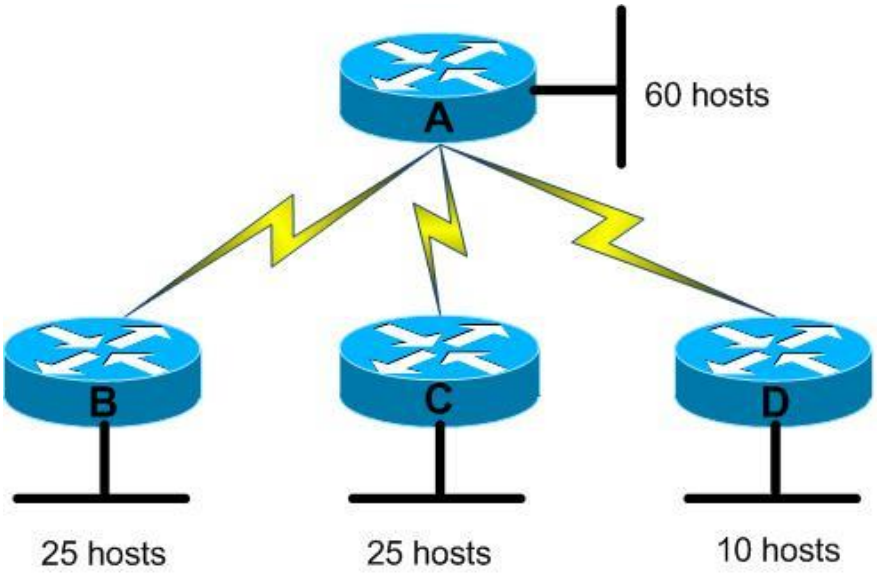
Υποδικτύωση – Σύνθετη Άσκηση 11

Διεύθυνση Δικτύου	***89.0.0.0***
Αριθμός υποδικτύων που χρειαζόμαστε	***490***
Αριθμός hosts που χρειαζόμαστε	***31000***

Default μάσκα υποδικτύωσης	
Δυαδικά ψηφία που δανειζόμαστε	
Προσαρμοσμένη μάσκα υποδικτύωσης	
Αριθμός υποδικτύων	
Αριθμός έγκυρων υποδικτύων	
Αριθμός διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Αριθμός έγκυρων διευθύνσεων διαθέσιμων για Hosts ανά υποδίκτυο	
Ποιο είναι το εύρος του 67ου χρήσιμου υποδικτύου;	
Ποια είναι η διεύθυνση δικτύου του 127ου χρήσιμου υποδικτύου;	
Ποια είναι η broadcast διεύθυνση του 59ου υποδικτύου;	
Ποιες είναι οι διευθύνσεις που μπορούμε να αναθέσουμε σε hosts στο 78ο χρήσιμο υποδίκτυο;	

Υποδικτύωση –Άσκηση με VLSM

Δίνεται η παρακάτω τοπολογία δικτύου:



Με χρήση του κλάσης C αριθμού 195.170.18.0 και μόνο να διευθυνσιοδοτήσετε πλήρως το δίκτυο κάνοντας την ελάχιστη δυνατή σπατάλη διευθύνσεων.

<u>Βήμα 1</u>

1. Πόσοι hosts πρέπει να διευθυνσιοδοτηθούν στο μεγαλύτερο τοπικό δίκτυο ;

2. Πόσα host bits πρέπει να 'δανειστούμε' για το σκοπό αυτό ;

<u>Βήμα 2</u>

Ας υποδικτυώσουμε τώρα το αριθμό 195.170.18.0 ώστε να καλύψουμε το μεγαλύτερο τοπικό δίκτυο.

<u>Βήμα 3</u>

Ας συνεχίσουμε υποδικτυώνοντας τα υποδίκτυα ώστε να καλύψουμε με τον καλύτερο τρόπο τις ανάγκες όλων των τοπικών δικτύων αλλά και των WAN συνδέσεων.

1. Ποια θα είναι η διεύθυνση δικτύου (*Network Address*) και η μάσκα υποδικτύωσης (*Subnet Mask*) για το τοπικό δίκτυο του δρομολογητή A ;

Network Address: _____

Subnet Mask: _____

2. Ποια θα είναι η διεύθυνση δικτύου (*Network Address*) και η μάσκα υποδικτύωσης (*Subnet Mask*) για το τοπικό δίκτυο του δρομολογητή B ;

Network Address: _____

Subnet Mask: _____

3. Ποια θα είναι η διεύθυνση δικτύου (*Network Address*) και η μάσκα υποδικτύωσης (*Subnet Mask*) για το τοπικό δίκτυο του δρομολογητή C ;

Network Address: _____

Subnet Mask: _____

4. Ποια θα είναι η διεύθυνση δικτύου (*Network Address*) και η μάσκα υποδικτύωσης (*Subnet Mask*) για το τοπικό δίκτυο του δρομολογητή D ;

Network Address: _____

Subnet Mask: _____

5. Ποια θα είναι η διεύθυνση δικτύου (*Network Address*) και η μάσκα υποδικτύωσης (*Subnet Mask*) για τη WAN σύνδεση ανάμεσα στους δρομολογητές A και B ;

Network Address: _____

Subnet Mask: _____

6. Ποια θα είναι η διεύθυνση δικτύου (*Network Address*) και η μάσκα υποδικτύωσης (*Subnet Mask*) για τη WAN σύνδεση ανάμεσα στους δρομολογητές A και C ;

Network Address: _____

Subnet Mask: _____

7. Ποια θα είναι η διεύθυνση δικτύου (*Network Address*) και η μάσκα υποδικτύωσης (*Subnet Mask*) για τη WAN σύνδεση ανάμεσα στους δρομολογητές A και D ;

Network Address: _____

Subnet Mask: _____