ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ ΑΠΟΚΕΝΤΡΩΣΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΙΝΣΤΙΤΟΥΤΟ ΕΠΙΜΟΡΦΩΣΗΣ

ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

Επιστημονικός Υπεύθυνος: Δρ. Ηλίας Κ. Μαραγκός

Συγγραφή: Αβραντινής Νικόλαος
Γαβριηλίδης Νικόλαος
Κηπουρός Νικόλαος
Μάγκος Κωνσταντίνος
Δρ. Μαυρομμάτης Γεώργιος
Παπαπάνος Ιωάννης
Σχαλέκης Νικόλαος

Αθήνα
2010

ΠΕΡΙΕΧΟΜΕΝΑ

10.4 Τύποι ACLs

11. Μεταγωγείς (switches)

11.1 Εισαγωγή στους μεταγωγείς
11.2 Bridging & Switching
11.3 Το Spanning Tree protocol (STP) σε δίκτυα μεταγωγέων
11.4 Βασική ρύθμιση μεταγωγέα
11.5 VLANs και ρύθμιση τους σε μεταγωγείς
11.6 Το πρωτόκολλο VTP
11.7 Παράδειγμα ρύθμισης μεταγωγέα σε δίκτυο

12. Μετάφραση Διεύθυνσης

12.1 Μετάφραση Διεύθυνσης Δικτύου (NAT).
12.2 Μετάφραση Θύρας Διεύθυνσης Δικτύου (PAT).
12.3 Διαμόρφωση NAT & PAT

13. Dynamic Host Configuration Protocol (DHCP).

14. Τεχνολογίες WAN (Wide Area Networks).

14.1 Είδη Συνδέσεων.

15. Point-to-Point Protocol (PPP).

15.1 Πιστοποίηση PPP.
15.2 Επαλήθευση, Εύρεση Λαθών Πιστοποίησης (Troubleshooting Authentication).

16. Δίκτυα ISDN

16.1 Πλεονεκτήματα και εγκατάσταση του ISDN
16.2 Ρύθμιση ενός ISDN router

1. Εισαγωγή στα Δίκτυα

1.1 Σύνδεση Υπολογιστή στο Δίκτυο

Το Internet είναι σήμερα το μεγαλύτερο δίκτυο δεδομένων που υπάρχει επιτρέποντας την απομακρυσμένη επικοινωνία και μεταφορά δεδομένων μεταξύ υπολογιστών. Μπορεί να θεωρηθεί σαν ένα μεγάλο σύννεφο όπου διάφορες δικτυακές συσκευές συνδέονται μεταξύ τους επιτρέποντας την διακίνηση πληροφορίας με αδιαφανή προς τον χρήστη τρόπο.

Για να μπορέσει ένας υπολογιστής να συνδεθεί σε ένα δίκτυο και κατ' επέκταση στο Internet απαιτούνται τρία βασικά στοιχεία:

A) Φυσική Σύνδεση
B) Λογική Σύνδεση
C) Εφαρμογές που μεταφράζουν και παρουσιάζουν την διακινούμενη πληροφορία.

Α) Η Φυσική Σύνδεση έχει να κάνει με τα μηχανικά μέρη της σύνδεσης και τα μέσα που χρησιμοποιούνται για την δικτύωσή τους. Έτσι για έναν τυπικό υπολογιστή θα πρέπει να γίνει σύνδεση μεταξύ της κάρτας δικτύου του (**NIC – Network Interface Card**) μέσω ενός Ethernet καλωδίου με ένα switch ή hub, ή μέσω ενός τηλεφωνικού καλωδίου σύνδεση μεταξύ ενός εσωτερικού modem και της πρίζας τηλεφώνου. Αν το modem είναι εξωτερικό τότε απαιτείται και ένα σειριακό καλώδιο μεταξύ του υπολογιστή και του modem.

Η κάρτα δικτύου - NIC (Network Interface Card)

Όπως αναφέρθηκε παραπάνω ένας υπολογιστής συνήθως συνδέεται στο Internet είτε μέσω μιας κάρτας δικτύου (NIC) είτε μέσω ενός modem. Η κάρτα δικτύου χρησιμοποιείται για την σύνδεση του υπολογιστή στο τοπικό δίκτυο (LAN) ενώ το modem για την σύνδεση του υπολογιστή στο δίκτυο του παρόχου μέσα από το τηλεφωνικό δίκτυο.

Μια κάρτα δικτύου (εικόνα 1.1) είναι ένα ολοκληρωμένο κύκλωμα που είτε είναι ενσωματωμένο πάνω στην μητρική πλακέτα είτε βρίσκεται πάνω σε μια ξεχωριστή πλακέτα επέκτασης (PCI ή ISA για destop PCs ή PCMCIA για laptops). Η NIC είναι αυτή που στέλνει και λαμβάνει δεδομένα σε ψηφιακή μορφή και αποτελεί για τον υπολογιστή ένα interface με το ανάλογο μέσω δικτύωσης (καλώδιο).

Εικόνα 1.1: Η κάρτα δικτύου (NIC)

Η εγκατάσταση μιας NIC στον υπολογιστή, όπως και σχεδόν κάθε άλλης συσκευής απαιτεί κάποιο IRQ και κάποια διεύθυνση μνήμης καθώς και το κατάλληλο πρόγραμμα οδήγησης (driver) για να μπορεί να είναι ορατή από το σύστημα και να λειτουργεί σωστά. Συνήθως τα παραπάνω δεν απαιτούν κάποια παρέμβαση από τον χρήστη και ρυθμίζονται αυτόματα από το λειτουργικό σύστημα με την

διαδικασία του Plug and Play. Πριν γίνει αγορά μιας κάρτας δικτύου ο χρήστης πρέπει να λάβει υπόψη του τα παρακάτω:

- Το είδος του δικτύου στο οποίο θα συνδεθεί (Ethernet, Token Ring) και τα πρωτοκολλά που θα χρησιμοποιηθούν (TCP/IP, CSMACD).

- Το είδος του μέσου που θα συνδεθεί στην κάρτα, όπως Twisted Pair (συνεστραμμένο ζεύγος – το κοινό UTP, Coaxial (ομοαξονικό), Fiber optics (οπτικές ίνες), Wireless (Ασύρματο).

- Ο τύπος του bus που συνδέεται η κάρτα στο PC (PCI, ISA, USB)

Μία τυπική NIC σήμερα μπορεί να επιτρέψει την μεταφορά δεδομένων μέχρι και 1 Gbps.

Το modem (modulator – demodulator)

Το modem συνδέει τον υπολογιστή στο αναλογικό τηλεφωνικό δίκτυο. Αυτό μπορεί να είναι εσωτερικό (εικόνα 1.2) και να συνδέεται σαν κάρτα επέκτασης (ISA ή PCI) στην μητρική πλακέτα του υπολογιστή, αλλά μπορεί να είναι και εξωτερικό (εικόνα 1.3) το οποίο συνήθως συνδέεται με ένα σειριακό καλώδιο σε μια COM πόρτα του υπολογιστή. Η δουλειά του είναι να μετατρέψει τα ψηφιακά σήματα που στέλνει ο υπολογιστής σε αναλογικά ώστε να περάσουν πάνω από τις τηλεφωνικές γραμμές, όπως και η φωνή στην κλασσική τηλεφωνία. Αντίστροφα όταν τα δεδομένα καταφθάνουν στον υπολογιστή το modem μετατρέπει τα αναλογικά σήματα σε ψηφιακά ώστε να μπορούν να αποκωδικοποιηθούν από τον υπολογιστή.

Εικόνα 1.2: Εσωτερικό modem

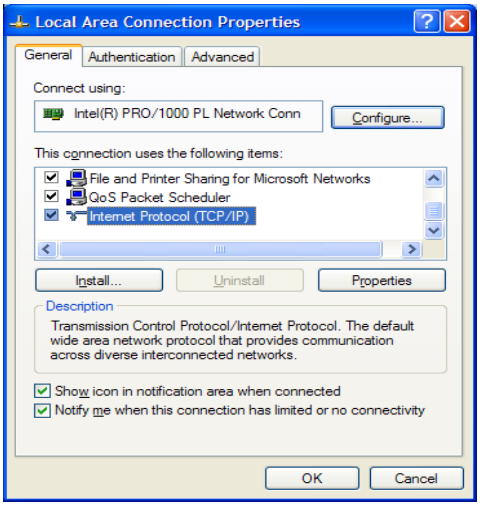
Εικόνα 1.3: Εξωτερικό modem

Τα κλασσικά modem για τις dialup γραμμές υποστηρίζουν ταχύτητες μέχρι και 56 kbps, ενώ με την εμφάνιση των DSL γραμμών σήμερα η ταχύτητα είναι σχεδόν 200 φορές μεγαλύτερη, 10 Mbps και άνω.

Β) Η Λογική Σύνδεση υλοποιείται μέσω πρωτοκόλλων. Ένα πρωτόκολλο είναι μία συλλογή από κανόνες και standards που καθορίζουν τον τρόπο με τον οποίο οι συσκευές σε ένα δίκτυο πρέπει να επικοινωνούν. Μία σύνδεση στο Internet απαιτεί την χρήση διαφόρων πρωτοκόλλων και συνήθως είναι αυτά που ανήκουν στην οικογένεια του TCP/IP.

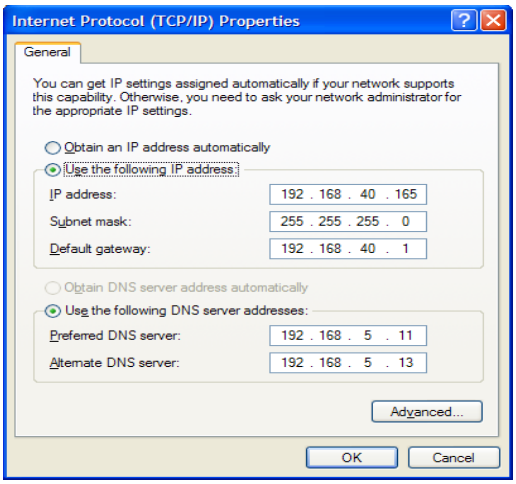
Ρυθμίσεις TCP/IP

Αφού ολοκληρωθεί η φυσική σύνδεση και η εγκατάσταση της κάρτας δικτύου στον υπολογιστή πρέπει να γίνουν οι κατάλληλες ρυθμίσεις του TCP/IP. Στην εικόνα 1.4 εμφανίζεται η καρτέλα ιδιοτήτων σύνδεσης τοπικού δικτύου σε ένα τυπικό Windows XP μηχάνημα. Με αυτές τις ρυθμίσεις ο υπολογιστής θα μπορέσει να συνδεθεί αρχικά στο τοπικό δίκτυο ώστε να μπορεί να επικοινωνεί με τις υπόλοιπους υπολογιστές που ανήκουν σε αυτό, καθώς και με την συσκευή που θα παρέχει την σύνδεση στο Internet.



Εικόνα 1.4: Καρτέλα ιδιοτήτων σύνδεσης τοπικού δικτύου

Όπως φαίνεται στην εικόνα 1.4 η κάρτα δικτύου που χρησιμοποιείται για την σύνδεση έχει ήδη αναγνωριστεί από το σύστημα (Intel Pro /1000 PL), και έχει επιλεχθεί να γίνει ρύθμιση του TCP/IP.

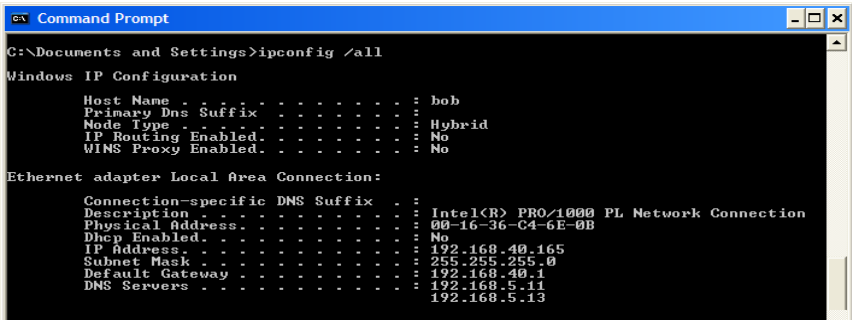


Εικόνα 1.5: Καρτέλα ιδιοτήτων TCP/IP

Η επιλογή για την ρύθμιση των ιδιοτήτων του TCP/IP εμφανίζει την καρτέλα στην εικόνα 1.5. Εδώ αρχικά πρέπει να οριστεί εάν ο υπολογιστής θα πάρει αυτόματα τις απαιτούμενες ρυθμίσεις από έναν DHCP server ή αν θα οριστούν από τον χρήστη. Στην εικόνα 1.5 έχει γίνει χειροκίνητη ρύθμιση, όπου ο χρήστης έχει δηλώσει την IP διεύθυνση (IP address) και την μάσκα υποδικτύου (Subnet Mask) του

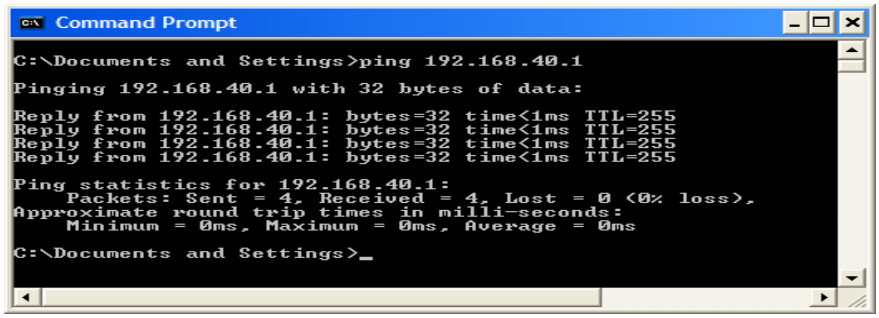
υπολογιστή τα οποία θα προσδιορίζουν μονοσήμαντα τον συγκεκριμένο υπολογιστή στο δίκτυο. Επίσης έχει δηλωθεί και η IP διεύθυνση για το default geteway που είναι η δικτυακή συσκευή στην οποία ο υπολογιστής θα στέλνει τα δεδομένα όταν χρειάζεται να επικοινωνήσει με κάποιον εκτός του τοπικού δικτύου. Τέλος έχει δηλωθεί η IP διεύθυνση του πρωτεύων (primary) και εναλλακτικού (alternate) DNS (Domain Naming Sytem) server. Αυτό είναι το μηχάνημα που θα κάνει αντιστοίχηση μεταξύ IP διευθύνσεων και ονομάτων προορισμών για το συγκεκριμένο δίκτυο.

Αφού γίνουν οι παραπάνω ρυθμίσεις απομένει να γίνει έλεγχος και δοκιμή της σύνδεσης. Για τον σκοπό αυτό θα χρησιμοποιηθεί μία κονσόλα DOS (Start -> Run -> cmd). Εδώ αφού εκτελεστεί η εντολή **ipconfig /all** εμφανίζονται όλες οι ρυθμίσεις δικτύου που γίνανε παραπάνω καθώς και άλλες πληροφορίες που έχουν να κάνουν με υπηρεσίες του δικτύου που έχουν ρυθμιστεί στον υπολογιστή. Η έξοδος μετά την εκτέλεση της παραπάνω εντολής παρουσιάζεται στην εικόνα 1.6.



Εικόνα 1.6: Έλεγχος ρυθμίσεων δικτύου από κονσόλα DOS

Αφού επιβεβαιωθούν οι σωστές ρυθμίσεις δικτύου η επόμενη κίνηση είναι να γίνει έλεγχος της σύνδεσης προσπαθώντας να γίνει επικοινωνία με έναν άλλο υπολογιστή του δικτύου. Για αυτή την λειτουργία θα χρησιμοποιηθεί η εντολή **ping** η οποία στέλνει κάποια πακέτα στον υπολογιστή που θα της δοθεί σαν όρισμα και εάν η επικοινωνία είναι δυνατή ο απομακρυσμένος υπολογιστής στέλνει πίσω με την σειρά του κάποια πακέτα ως απάντηση. Στην εικόνα 1.7 παρουσιάζεται η έξοδος της εκτέλεσης του ping με όρισμα το μηχάνημα που έχει δηλωθεί σαν default gateway.



Εικόνα 1.7: 'Εξοδος της εντολής ping με όρισμα το default gateway

Όπως φαίνεται στην εικόνα στάλθηκαν τέσσερα πακέτα-ερώτησης στο μηχάνημα με την IP διεύθυνση 192.168.40.1 (το default gateway), το οποίο με τη σειρά του απάντησε με τέσσερα πακέτα-απάντησης. Αυτό επιβεβαιώνει ότι οι δύο υπολογιστές μπορούν να επικοινωνούνε δικτυακά μεταξύ τους.

C) Οι Εφαρμογές είναι αυτές που υλοποιούν κάποια από τα πρωτόκολλα για να στείλουν και να λάβουν δεδομένα μετά από αίτηση του χρήστη και να παρουσιάσουν τα αποτελέσματα σε αυτόν. Ο

web browser είναι ίσως η πιο γνωστή και συχνότερα χρησιμοποιούμενη δικτυακή εφαρμογή. Η λειτουργία του είναι μετά από αίτημα του χρήστη να συνδέεται και να συλλέγει κάποιες πληροφορίες από έναν web server και στην συνέχεια να τις παρουσιάζει στην οθόνη του χρήστη με την κατάλληλη μορφή. Η μορφή αυτή είναι η **HTML - Hypertext Markup Language** (και άλλες πιο εξελιγμένες μορφές όπως XML) ή οποία είναι μια γλώσσα που κωδικοποιεί web σελίδες. Σήμερα οι δύο πιο διαδεδομένοι browsers είναι ο Internet Explorer της Microsoft και ο Mozilla Firefox του Mozilla Project. Ενώ στην βασική της μορφή η HTML μπορεί να εμφανίσει κείμενο, εικόνα και βίντεο, μέσω διάφορων plug-gins οι browsers μπορούν να αναπαράγουν αρχεία flash, quicktime, pdf, realaudio κ.α κάνοντας την περιήγηση στο Internet αρκετά πιο ενδιαφέρον και διασκεδαστική.
Έτσι η σύνδεση ενός υπολογιστή στο Internet απαιτεί την εγκατάσταση των φυσικών συσκευών και μέσων, την ρύθμιση των κατάλληλων πρωτοκόλλων και την εγκατάσταση των κατάλληλων εφαρμογών.

1.2 Συστήματα Αρίθμησης στα Δίκτυα

Το Δεκαδικό Σύστημα

Το δεκαδικό σύστημα αρίθμησης (ή βάσης 10) είναι το κοινό αριθμητικό σύστημα που χρησιμοποιούμε στην καθημερινή μας ζωή. Αυτό αποτελείται από δέκα αριθμητικά σύμβολα τα 0,1,2,3,4,5,6,7,8,9 και το 10 θεωρείται η βάση του συστήματος. Κάθε ποσότητα (πχ. 235) στο δεκαδικό σύστημα παριστάνεται από μια διάταξη των παραπάνω συμβόλων/ψηφίων και μπορεί να αποτελείται από μονάδες, δεκάδες, εκατοντάδες, χιλιάδες κλπ.

Ο υπολογισμός της τιμής μιας τέτοιας συμβολοσειράς γίνεται προσθέτοντας τις επιμέρους τιμές που προκύπτουν από το γινόμενο του κάθε ψηφίου με την ύψωση της βάσης (του 10) στην δύναμη της θέσης που βρίσκεται το ψηφίο αυτό. Η αρίθμηση της θέσης του κάθε ψηφίου ξεκινά από το 0 από δεξιά προς τ' αριστερά.

Παράδειγμα

$1325 = 1\cdot\ 10^3 + 3\cdot\ 10^2 + 2\cdot\ 10^1 + 5\cdot\ 10^0 = 1\cdot\ 1000 + 3\cdot\ 100 + 2\cdot\ 10 + 5\cdot\ 1 = 1000 + 300 + 20 + 5$

Με αυτόν τον υπολογισμό γίνεται αντιληπτό πως στον παραπάνω αριθμό προκύπτουν οι χιλιάδες, οι εκατοντάδες, οι δεκάδες και οι μονάδες.

Ενώ γενικότερα δεν συνηθίζεται, ο παραπάνω αριθμός μπορεί να γραφτεί δηλώνοντας και την βάση του ως δείκτη στο τέλος του αριθμού ως εξής: 1325_{10}

Το Δυαδικό Σύστημα

Ενώ το δεκαδικό σύστημα θεωρείται κατάλληλο για την αναπαράσταση και χρήση αριθμών στην καθημερινή μας ζωή, δεν μπορεί να χρησιμοποιηθεί με αποτελεσματικότητα για την έκφραση ποσοτήτων σε ηλεκτρονικά μέσα, όπως τα ηλεκτρονικά κυκλώματα και κατ' επέκταση οι ηλεκτρονικοί υπολογιστές. Ένα ηλεκτρονικό κύκλωμα μπορεί να βρίσκεται σε δύο πιθανές καταστάσεις: ON και OFF. Έτσι δύο και μόνο σύμβολα/ψηφία, το 0 και το 1 μπορούν να εκφράσουν τις καταστάσεις αυτές. Αυτά ονομάζονται δυαδικά ψηφία ή bits.

Έτσι ένα ξεχωριστό αριθμητικό σύστημα που αποτελείται από αυτά τα δύο ψηφία είναι απαραίτητο. Αυτό είναι το δυαδικό σύστημα του οποίου η βάση είναι το 2 (αντίστοιχα με το 10 για το δεκαδικό). Κάθε ποσότητα στο δυαδικό σύστημα αποτελείται από μία διάταξη από 0 και 1.

Παράδειγμα

0000_2, 011001_2, 1111111_2, 00011000_2

Ο δείκτης 2 στο τέλος του κάθε αριθμού υποδηλώνει ότι είναι ένας δυαδικός αριθμός δηλαδή έχει ως βάση το 2.

Οι ηλεκτρονικοί υπολογιστές χρησιμοποιούν εσωτερικά αποκλειστικά τέτοιου είδους συμβολοσειρές για να αναπαραστήσουν τα δεδομένα που επεξεργάζονται και αποθηκεύουν. Ένα bit θεωρείται η μικρότερη μονάδα αποθήκευσης σε έναν ηλεκτρονικό υπολογιστή. Για παράδειγμα ο χαρακτήρας 'A' εσωτερικά σε έναν υπολογιστή έχει την μορφή 01000010 (στην αναπαράσταση ASCII).

Διαφορετικές συμβολοσειρές από bits μπορούν να αναπαραστήσουν οποιαδήποτε πληροφορία, όπως ο χαρακτήρας 'A' παραπάνω. Ο αριθμός των bits που απαιτούνται για να αναπαραστήσουν μία πληροφορία εξαρτάται από τις διαφορετικές τιμές που μπορεί να πάρει αυτή η πληροφορία. Για παράδειγμα με ένα bit μπορούμε να αναπαραστήσουμε μόνο 2 διαφορετικές τιμές το 0 και το 1. Με 2 bits μπορούμε να αναπαραστήσουμε 4 τιμές που προκύπτουν από όλους τους διαφορετικούς συνδυασμούς αυτών των 2 bits μεταξύ τους: 00, 01, 10, 11. Γενικά με N bits μπορούμε να αναπαραστήσουμε 2^N διαφορετικές τιμές. Για παράδειγμα αν κάποιος ήθελε να αναπαραστήσει με bits 8 διαφορετικά χρώματα θα έπρεπε να χρησιμοποιήσει 3 bits ($2^3 = 8$) για το κάθε χρώμα και να κάνει την παρακάτω αντιστοιχία:

000	Άσπρο
001	Κόκκινο
010	Μπλε
011	Κίτρινο
100	Πράσινο
101	Πορτοκαλί
110	Καφέ
111	Μαύρο

Πίνακας 1.1: Αναπαράσταση χρωμάτων με δυαδικούς αριθμούς

Μονάδες Μέτρησης Στο Δυαδικό Σύστημα

Όπως αναφέρθηκε παραπάνω ένα bit είναι η μικρότερη μονάδα αποθήκευσης σε έναν ηλεκτρονικό υπολογιστή. Μία συλλογή από 8 bits αποτελεί 1 **byte**. Με ένα byte μπορούν να εκφραστούν $2^8 = 256$ διαφορετικές καταστάσεις. Μεγαλύτερες συλλογές από bits αντιστοιχούν στις μονάδες μέτρησης που εμφανίζονται στον παρακάτω πίνακα:

Μονάδα	**Συμβολισμός**	**Αντιστοιχία**
Bit	b	Ένα δυαδικό ψηφίο 0 ή 1
Byte	B	8 **bits**
Kilobyte	KB	1024 **Bytes** 1.048.576 **bits**
Megabyte	MB	1024 **Kilobytes** 1.048.576 **Bytes**
Gigabyte	GB	1024 **Megabytes**

		1.048.576	**Kilobytes**
		1.073.741.824	**Bytes**
Terabyte	TB	1024	**Gigabytes**
		1.048.576	**Megabytes**
		1.073.741.824	**Kilobytes**
		1.099.511.627.778	**Bytes**

Πίνακας 1.2: Μονάδες μέτρησης στο δυαδικό

Μετατροπή Δυαδικού σε Δεκαδικό

Ενώ το δυαδικό σύστημα είναι απόλυτα κατανοητό από τα ηλεκτρονικά κυκλώματα είναι κάπως ξένο στην ανθρώπινη λογική που είναι συνηθισμένη στο δεκαδικό σύστημα. Η μετατροπή ενός αριθμού από το δυαδικό στο δεκαδικό ακολουθεί την ίδια λογική που παρουσιάστηκε παραπάνω για τον υπολογισμό ενός δεκαδικού αριθμού. Δηλαδή το άθροισμα των επιμέρους γινομένων που προκύπτουν από τον πολλαπλασιασμό του κάθε ψηφίου με την ύψωση της βάσης (του 2) στη δύναμη που καθορίζεται από την θέση του ψηφίου.

Παράδειγμα

$1011_2 = 1\cdot\ 2^3 + 0\cdot\ 2^2 + 1\cdot\ 2^1 + 1\cdot\ 2^0 = 1\cdot\ 8 + 0\cdot\ 4 + 1\cdot\ 2 + 1\cdot\ 1 = 8+ 0 + 2 + 1 = 11_{10}$

Ο υπολογισμός ξεκινάει πάντα από τα δεξιά όπου το πρώτο bit βρίσκεται στην θέση 0 το δεύτερο στην θέση 1 κτλ.

Μετατροπή Δεκαδικού σε Δυαδικό

Μέθοδος 1η - διαδοχική διαίρεση

Με αυτή τη μέθοδο ο δεκαδικός αριθμός αρχικά και στην συνέχεια το πηλίκο που προκύπτει κάθε φορά διαιρείται διαδοχικά με τη βάση του 2. Το υπόλοιπο της διαίρεσης που προκύπτει σε κάθε βήμα αποτελεί και ένα ψηφίο του τελικού δυαδικού αριθμού. Η διαδικασία τερματίζει όταν το πηλίκο γίνει 0.

Παράδειγμα

Σε αυτό το παράδειγμα ο δεκαδικός αριθμός 69 θα μετατραπεί στον αντίστοιχο δυαδικό.

Διαίρεση	**Πηλίκο**	**Υπόλοιπο**	**Αποτέλεσμα**
69:2	34		
34 : 2	17	**0**	
17 : 2	8	**1**	
8 : 2	4	**0**	

4 : 2	2	**0**	**1 0 0 0 1 0 1**
2 : 2	1	**0**	
1 : 2	0	**1**	

Το αποτέλεσμα της παραπάνω διαδικασίας είναι ο αριθμός 1000101_2 που είναι ο δεκαδικός 69_{10}.

Μέθοδος 2η

Βήμα 1

Αρχικά υπολογίζονται τα λιγότερα δυνατά bits που απαιτούνται για να εκφράσουν τον δεκαδικό αριθμό. Για παράδειγμα για τον αριθμό 69 απαιτούνται τουλάχιστον 7 bits, καθώς 2^6=64 ενώ 2^7=128. Τα 6 bits θα μπορούσαν να μας δώσουν το περισσότερο 64 διαφορετικούς αριθμούς (0 ... 63) κάτι που δεν θα ήταν αρκετό για τον αριθμό 69. Αντιθέτως το 7 bits μπορούν να μας δώσουν μέχρι και 128 αριθμούς (0...127) και κάποιος συνδυασμός από αυτά τα 7 bits θα αντιστοιχεί στον αριθμό 69.

Βήμα 2

Γράφουμε σε κάθε θέση τον αριθμό που προκύπτει αν υψωθεί το 2 (η βάση) στην δύναμη που εκφράζεται από την θέση αυτή. Έτσι στην 7η θέση (6) γράφουμε την τιμή 64 (2^6), στην 6η θέση γράφουμε την τιμή 32 (2^5) κτλ. Στην πρώτη γραμμή του πίνακα του παραδείγματος παρακάτω αναγράφονται οι τιμές και των 7 θέσεων για τον αριθμό των 7 bits που θα εκφράσει τον δεκαδικό 69.

Βήμα 3

Στη συνέχεια πρέπει να βρούμε ένα ένα τα 7 αυτά bits ξεκινώντας από αριστερά (το πιο σημαντικό ψηφίο). Γίνεται σύγκριση του αριθμού με την τιμή της θέσης:

- Αν ο αριθμός είναι **μεγαλύτερος ή ίσος** με την τιμή της θέσης τότε το παραγόμενο bit είναι **1** και ο αριθμός μειώνεται παίρνοντας τιμή που ισούται με την διαφορά της τιμής θέσης από τον αριθμό. Η επόμενη σύγκριση θα γίνει μεταξύ του νέου αυτού αριθμού και της τιμής της επόμενης θέσης.
- Αν ο αριθμός είναι **μικρότερος** της τιμής θέσης τότε το παραγόμενο bit είναι **0** και ο αριθμός παραμένει ίδιος για σύγκριση με την τιμή της επόμενης θέσης.

(Θέση) Τιμή	(6) **64**	(5) **32**	(4) **16**	(3) **8**	(2) **4**	(1) **2**	(0) **1**
Αριθμός	**69**	69-64= **5**	**5**	**5**	**5**	5-4 = **1**	**1**
Σύγκριση	69 > 64	5 < 32	5 < 16	5 < 8	5 > 4	1 < 2	1 = 1

Bits	**1**	**0**	**0**	**0**	**1**	**0**	**1**

Παραπάνω παρουσιάζεται η μετατροπή του δεκαδικού 69 στον δυαδικό 1000101. Αρχικά ο αριθμός 69 συγκρίνεται με το 64 (τιμή της θέσης 6) και καθώς είναι μεγαλύτερος το παραγόμενο bit είναι 1. Από αυτή τη διαδικασία ο αρχικός αριθμός μειώνεται από 69 σε 5 (69-64). Στη συνέχεια το 5 συγκρίνεται με το 32 (τιμή της θέσης 5). Καθώς το 5 είναι μικρότερο το παραγόμενο bit είναι 0. Ακολούθως το 5 συγκρίνεται διαδοχικά με το 16 και το 8 και παράγει δύο 0 bits καθώς είναι μικρότερο από αυτές τις τιμές. Η επόμενη σύγκριση του 5 με το 4 (τιμή της θέσης 2) παράγει το bit 1 αφού 5 > 4, και η τιμή του μειώνεται από 5 σε 1 (5-4). Η τελευταία σύγκριση του αριθμού 1 με το 1 (τιμή της θέσης 0) παράγει το bit 1 αφού οι δύο αριθμοί είναι ίσοι.

Στον παρακάτω πίνακα παρουσιάζονται οι δεκαδικοί αριθμοί από το 0_{10} ως το 16_{10} και οι αντίστοιχοι δυαδικοί τους.

Δυαδικός	**Δεκαδικός**	**Δυαδικός**	**Δεκαδικός**
0100	0	1100	8
0101	1	1101	9
0110	2	1110	10
0111	3	1111	11
0000	4	1000	12
0001	5	1001	13
0010	6	1010	14
0011	7	1011	15

Πίνακας 1.3: Οι δεκαέξι πρώτοι δυαδικοί και δεκαδικοί αριθμοί

Δυαδική Λογική – Πράξεις με bits

NOT		Το λογικό NOT αντιστρέφει την τιμή του bit. Έτσι αν ο τελεστής είναι **0** το αποτέλεσμα του NOT θα δώσει **1** και αντίστοιχα αν ο τελεστής είναι **1** το αποτέλεσμα του NOT θα είναι **0**. Το αποτέλεσμα ονομάζεται αντίστροφος ή συμπλήρωμα του αρχικού αριθμού.
0	**1**	
1	**0**	

Παράδειγμα:

Ο αντίστροφος του 01100110 είναι ο 10011001

AND			Το λογικό AND μπορεί να θεωρηθεί ως το αντίστοιχο του πολλαπλασιασμού στο δεκαδικό σύστημα. Το αποτέλεσμα του AND μεταξύ δύο bits μπορεί να είναι **1** μόνο όταν και τα δύο bits τελεστές έχουν την τιμή **1**. Σε όλες τις άλλες περιπτώσεις το αποτέλεσμα είναι **0.**
0	0	**0**	
0	1	**0**	
1	0	**0**	
1	1	**1**	

Παράδειγμα:

X:	0	1	1	0	1
Y:	0	0	1	1	0
Αποτέλεσμα AND:	**0**	**0**	**1**	**0**	**0**

OR			
0	0	**0**	Το λογικό OR μεταξύ δύο bits δίνει ως αποτέλεσμα 0 μόνο όταν και οι δύο τελεστές είναι **0**. Σε όλες τις άλλες περιπτώσεις δίνει ως αποτέλεσμα το **1**. Υπάρχει μια σχετική αντιστοιχία με την πρόσθεση στο δεκαδικό σύστημα.
0	1	**1**	
1	0	**1**	
1	1	**1**	

Παράδειγμα

X:	0	1	1	0	1
Y:	0	0	1	1	0
Αποτέλεσμα OR:	**0**	**1**	**1**	**1**	**1**

Οκταδικό και Δεκαεξαδικό σύστημα

Άλλα αριθμητικά συστήματα εκτός του δεκαδικού και δυαδικού που αναφέρθηκαν παραπάνω είναι είναι το οκταδικό και το δεκαεξαδικό.

Το οκταδικό σύστημα έχει ως βάση του το 8 και αποτελείται από τα ψηφία 0, 1, 2, 3, 4, 5, 6, 7. Ο αριθμός 3_8 είναι ένας οκταδικός αριθμός που αντιστοιχεί στον δεκαδικό 3_{10} ($3 \cdot 8^0$), ενώ ο οκταδικός αριθμός 12_8 αντιστοιχεί στον δεκαδικό 10_{10} ($1 \cdot 8^1 + 2 \cdot 8^0$). Ένας οκταδικός αριθμός μπορεί να γραφτεί είτε με τον δείκτη 8 στο τέλος του αριθμού (πχ. 11_8) είτε βάζοντας το 0 ως πρόθεμα του αριθμού (πχ. 011).

Το δεκαεξαδικό σύστημα έχει ως βάση του το 16 και αποτελείται από τα σύμβολα 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Ο αριθμός 5_{16} αντιστοιχεί στον αριθμό 5_{10} στο δεκαδικό, ενώ ο αριθμός A_{16} αντιστοιχεί στον αριθμό 10_{10} στο δεκαδικό. Ένας δεκαεξαδικός αριθμός μπορεί να γραφτεί είτε με τον δείκτη 16 στο τέλος του αριθμού (πχ. $1F_{16}$) είτε με το λεκτικό '0x' ως πρόθεμα του αριθμού (πχ. 0x1F).

Δεκαδικός	**Δυαδικός**	**Οκταδικός**	**Δεκαεξαδικός**
0	000**0**	**0**	**0**
1	000**1**	**1**	**1**
2	0010	**2**	**2**
3	0011	**3**	**3**
4	0100	**4**	**4**

5	0101	**5**	**5**
6	0110	**6**	**6**
7	0111	**7**	**7**
8	1000	10	**8**
9	1001	11	**9**
10	1010	12	**A**
11	1011	13	**B**
12	1100	14	**C**
13	1101	15	**D**
14	1110	16	**E**
15	1111	17	**F**

Πίνακας 1.4: Οι δεκαέξι πρώτοι δεκαδικοί, δυαδικοί, οκταδικοί και δεκαεξαδικοί αριθμοί

Παρατηρείστε ότι απαιτούνται τουλάχιστον 3 bits για εκφραστούν όλα τα πιθανά σύμβολα ενός οκταδικού αριθμού με δυαδικές τιμές, ενώ απαιτούνται τουλάχιστον 4 bits για να εκφραστούν όλα τα πιθανά σύμβολα ενός δεκαεξαδικού αριθμού με δυαδικές τιμές. Πάνω σε αυτή την παρατήρηση στηρίζεται και η μετατροπή ενός οκταδικού ή δεκαεξαδικού αριθμού σε δυαδικό.

Για παράδειγμα ο οκταδικός 1352_8 έχει τέσσερα ψηφία και έτσι απαιτούνται τουλάχιστον 15 bits για τον αντίστοιχο δυαδικό, 3 bits για το κάθε οκταδικό ψηφίο. Με αντιστοίχηση των ψηφίων από τον πίνακα 1.4 ο δυαδικός που παράγεται είναι ο παρακάτω.

Οκταδικός	1	3	5	2
Δυαδικός	001	011	101	010

οπότε ο 1352_8 = 001011101010.

Ένα ακόμα παράδειγμα για την μετατροπή του δεκαεξαδικού $2B3F_{16}$ στον αντίστοιχο δυαδικό. Αυτός ο δεκαεξαδικός αριθμός αποτελείται από τέσσερα ψηφία όποτε ο αντίστοιχος δυαδικός θα αποτελείται από τουλάχιστον 16 bits (4 bits για το κάθε δεκαεξαδικό ψηφίο. Η αντιστοίχηση των δεκαεξαδικών και δυαδικών ψηφίων από τον πίνακα 1.4 δίνει την παρακάτω μετατροπή.

Δεκαεξαδικός	2	B	3	F
Δυαδικός	0010	1011	0011	1111

Οπότε ο $2B3F_{16}$ = 0010101100111111.

Ο πίνακας 1.4 είναι πολύ σημαντικός καθώς αποτελεί έναν γρήγορο οδηγό για αντιστοίχηση μεταξύ αριθμών διαφορετικών συστημάτων.

1.3 IP Διευθύνσεις και Υποδίκτυα

IP Διευθύνσεις

Κάθε υπολογιστής που συνδέεται στο Internet έχει και μία μοναδική IP διεύθυνση. Αυτή είναι απαραίτητη για να μπορεί ο υπολογιστής να επικοινωνήσει με άλλους υπολογιστές μέσω δικτύου. Κάθε IP διεύθυνση αποτελείται από 32 bits τα οποία είναι χωρισμένα σε 4 ομάδες των 8 bits (1 byte ή octet). Για παράδειγμα η **11000011 11001000 01100100 00000101** είναι μία IP διεύθυνση όπως αυτή αναπαριστάται εσωτερικά σε έναν ηλεκτρονικό υπολογιστή. Ενώ αυτή η αναπαράσταση είναι άμεσα κατανοητή σε έναν υπολογιστή δεν ισχύει το ίδιο και για την ανθρώπινη λογική. Για αυτό το σκοπό οι IP διευθύνσεις συνηθίζεται να αναπαριστούνται με δεκαδικούς αριθμούς όπως **195.200.100.5**. Η μορφή αυτή ονομάζεται **Dotted Decimal Notation**, και αποτελείται από τέσσερις δεκαδικούς αριθμούς που διαχωρίζονται μεταξύ τους με μία τελεία (.). Κάθε δεκαδικός αντιστοιχεί και σε μία από τις τέσσερις ομάδες των 8 bits της IP διεύθυνσης στην δυαδική της μορφή.

IP Διεύθυνση				
Δυαδική μορφή	11000011	11001000	01100100	00000101
Δεκαδική μορφή	195	200	100	5

Ενώ η δεκαδική μορφή των IP διευθύνσεων προσφέρει μεγάλη ευκολία στην χρήση και ρύθμιση τους είναι πολλές φορές απαραίτητο να γίνονται μετατροπές από τη μία μορφή στην άλλη. Οι μετατροπές αυτές ακολουθούν τους κανόνες μετατροπής μεταξύ δυαδικών και δεκαδικών αριθμών που παρουσιάστηκαν σε προηγούμενες ενότητες. Στη περίπτωση των IP διευθύνσεων οι μετατροπές περιορίζονται μεταξύ 8-bit δυαδικών αριθμών και το πολύ 3-ψήφιων δεκαδικών αριθμών, καθώς 8 bit μπορούν να αποδώσουν το πολύ $2^8 = 256$ διαφορετικούς αριθμούς οι οποίοι όλοι αποτελούνται από το πολύ 3 δεκαδικά ψηφία. Έτσι για τον υπολογισμό της παραπάνω IP διεύθυνσης:

11000011 = $1\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0$ = 128+64+0+0+0+0+2+1 = **195**

11001000 = $1\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 0\cdot 2^0$ = 128+64+0+0+8+0+0+0 = **200**

01100100 = $0\cdot 2^7 + 1\cdot 2^6 + 1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 0\cdot 2^0$ = 0+64+32+0+0+4+0+0 = **100**

00000101 = $0\cdot 2^7 + 0\cdot 2^6 + 0\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0$ = 0+0+0+0+0+4+0+1 = **5**

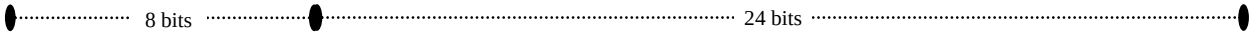
Η αποστήθιση του πίνακα 1.5 παρακάτω θα αποτελέσει ένα χρήσιμο εργαλείο για την γρήγορη μετατροπή μεταξύ των δύο μορφών IP διευθύνσεων καθώς αρκεί κάποιος να προσθέσει τις τιμές των θέσεων των bits που έχουν την τιμή **1** για να προκύψει ο αντίστοιχος δεκαδικός αριθμός για το κάθε byte.

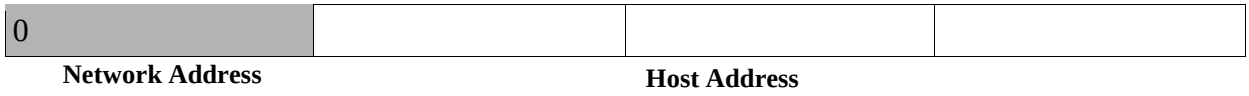
Θέση Bit	7	6	5	4	3	2	1	0
Τιμή	128	64	32	16	8	4	2	1

Πίνακας 1.5: Οι δεκαδικές τιμές των πρώτων 8 bits

Οι IP διευθύνσεις χρησιμοποιούν ένα ιεραρχικό μοντέλο σύμφωνα με το οποίο κατατάσσονται σε διάφορες κλάσεις.

Class A





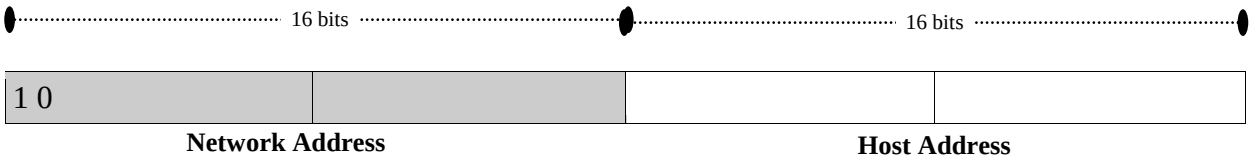
Το 1ο octet αποτελεί την διεύθυνση δικτύου ενώ τα υπόλοιπα τρία octets την διεύθυνση υπολογιστή.

Οι δυαδικές και δεκαδικές τιμές που μπορούν να πάρουν τα octets για τον σχηματισμό μιας class A διεύθυνσης είναι:

Octet	1 (net)	2 (host)	3 (host)	4 (host)
Δυαδικές Τιμές	00000000 ... 01111111	00000000 ... 11111111	00000000 ... 11111111	00000000 ... 11111111
Δεκαδικές Τιμές	0 ... 127	0 ... 255	0 ... 255	0 ... 255

Αυτό σημαίνει ότι συνολικά μπορούν να υπάρχουν μέχρι και 128 διαφορετικά class A δίκτυα (126 καθώς τα δυο class A δίκτυα που ξεκινάνε από 0 και 127 δεν χρησιμοποιούνται) από τα οποία το καθένα μπορεί αποδώσει συνολικά μέχρι και 256· 256· 256 = 16.777.216 IP διευθύνσεις. Από αυτές όλες εκτός της πρώτης και της τελευταίας μπορούν να αποδοθούν σε δικτυακές συσκευές. Η πρώτη χρησιμοποιείται για την διεύθυνση του δικτύου ενώ η τελευταία για broadcast διεύθυνση που απευθύνεται σε όλους τους hosts.

Class B



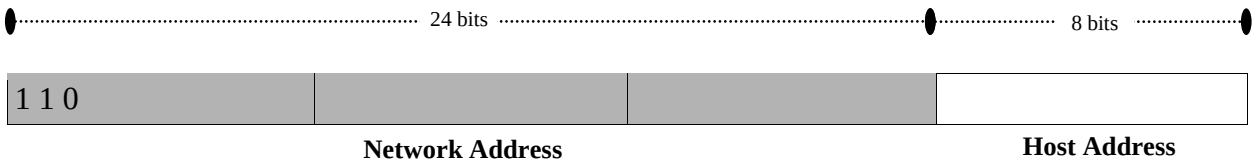
Τα δύο πρώτα octets αποτελούν την διεύθυνση δικτύου ενώ τα υπόλοιπα δύο octets την διεύθυνση υπολογιστή (host).

Οι δυαδικές και δεκαδικές τιμές που μπορούν να πάρουν τα octets για τον σχηματισμό μιας class B διεύθυνσης είναι:

Octet	1(net)	2(net)	3(host)	4(host)
Δυαδικές Τιμές	10000000 ... 10111111	00000000 ... 11111111	00000000 ... 11111111	00000000 ... 11111111
Δεκαδικές Τιμές	128 ... 191	0 ... 255	0 ... 255	0 ... 255

Αυτό σημαίνει ότι συνολικά μπορούν να υπάρχουν μέχρι και 64· 256 = 16.384 διαφορετικά class B δίκτυα από τα οποία το καθένα μπορεί αποδώσει συνολικά μέχρι και 256· 256 = 65.536 IP διευθύνσεις. Από αυτές όλες εκτός της πρώτης και της τελευταίας μπορούν να αποδοθούν σε δικτυακές συσκευές. Η πρώτη χρησιμοποιείται για την διεύθυνση του δικτύου ενώ η τελευταία για broadcast διεύθυνση που απευθύνεται σε όλους τους hosts.

Class C



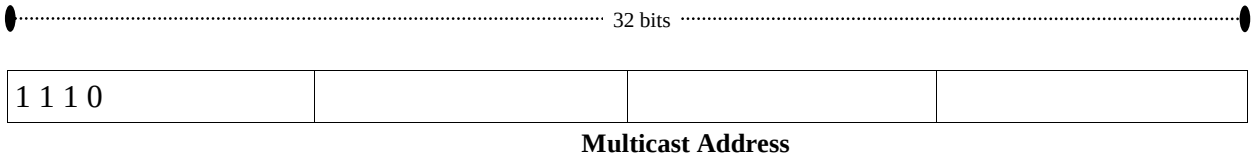
Τα τρία πρώτα octets αποτελούν την διεύθυνση δικτύου ενώ το τελευταίο octet την διεύθυνση υπολογιστή (host).

Οι δυαδικές και δεκαδικές τιμές που μπορούν να πάρουν τα octets για τον σχηματισμό μιας class C διεύθυνσης είναι:

Octet	1(net)	2(net)	3(net)	4(host)
Δυαδικές Τιμές	10000000 ... 10111111	00000000 ... 11111111	00000000 ... 11111111	00000000 ... 11111111
Δεκαδικές Τιμές	192 ... 223	0 ... 255	0 ... 255	0 ... 255

Αυτό σημαίνει ότι συνολικά μπορούν να υπάρχουν μέχρι και 32· 256· 256 = 2.097.152 διαφορετικά class C δίκτυα από τα οποία το καθένα μπορεί αποδώσει συνολικά μέχρι και 256 IP διευθύνσεις. Από αυτές όλες εκτός της πρώτης και της τελευταίας μπορούν να αποδοθούν σε δικτυακές συσκευές. Η πρώτη χρησιμοποιείται για την διεύθυνση του δικτύου ενώ η τελευταία για broadcast διεύθυνση που απευθύνεται σε όλους τους hosts.

Class D

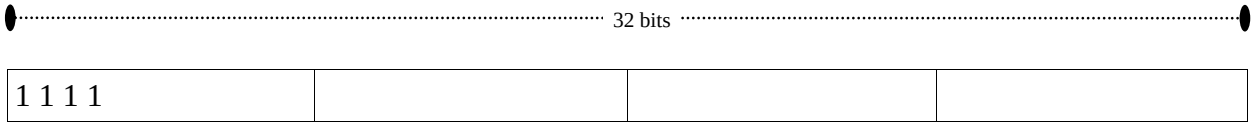


Οι διευθύνσεις αυτές απευθύνονται σε ομάδες από hosts. Δεδομένα που στέλνονται σε μία multicast διεύθυνση λαμβάνονται ταυτόχρονα από μία προκαθορισμένη ομάδα παραληπτών.

Οι δυαδικές και δεκαδικές τιμές που μπορούν να πάρουν τα octets για τον σχηματισμό μιας class D διεύθυνσης είναι:

Octet	1(host)	2(host)	3(host)	4(host)
Δυαδικές Τιμές	11100000 ... 11101111	00000000 ... 11111111	00000000 ... 11111111	00000000 ... 11111111
Δεκαδικές Τιμές	224 ... 239	0 ... 255	0 ... 255	0 ... 255

Class E



Μελλοντική Χρήση

Οι διευθύνσεις που ανήκουν στο E class χρησιμοποιούνται μόνο για ερευνητικούς σκοπούς και δεν αποδίδονται σε συστήματα παραγωγής στο Internet.

Οι δυαδικές και δεκαδικές τιμές που μπορούν να πάρουν τα octets για τον σχηματισμό μιας class E διεύθυνσης είναι:

Octet	1(host)	2(host)	3(host)	4(host)
Δυαδικές Τιμές	10000000 ... 10111111	00000000 ... 11111111	00000000 ... 11111111	00000000 ... 11111111
Δεκαδικές Τιμές	240 ... 254	0 ... 255	0 ... 255	0 ... 255

Μάσκες Υποδικτύου (Subnet Masks)

Η τεράστια εξάπλωση του Internet οδήγησε στην εξάντληση των διαθέσιμων IP διευθύνσεων. Το γεγονός αυτό καθώς και η αδυναμία των δρομολογητών να μπορούν να διατηρούν πολύ μεγάλους πίνακες με τις IP διευθύνσεις που πρέπει να δρομολογούν οδήγησε στην καθιέρωση των subnet masks (μάσκες υποδικτύου). Μία subnet mask αποτελείται και αυτή από 32 bits, και στόχος της είναι να δηλώνει πόσα bits μιας IP διεύθυνσης ανήκουν στην διεύθυνση δικτύου και πόσα στην διεύθυνση του host. Αυτό υλοποιείται εκφράζοντας το network κομμάτι της IP διεύθυνσης με bits που έχουν την τιμή 1 και με bits που έχουν την τιμή 0 το host κομμάτι της IP διεύθυνσης. Έτσι μια subnet mask αποτελείται από έναν αριθμό συνεχόμενων 1 ακολουθούμενων από μία σειρά συνεχόμενων 0 bits. Ο πίνακας 1.6 εμφανίζει τις default subnet masks (βασικές μάσκες υποδικτύου) για τις τρεις κύριες κλάσεις IP διευθύνσεων:

Class	**Network**	**Host**	**Default Subnet Mask (Δυαδική μορφή)**	**Default Subnet mask (Δεκαδικη μορφή)**	**Συντόμευση**
Class A	1 octet	3 octets	11111111 00000000 00000000 00000000	255.0.0.0	/8
Class B	2 octets	2 octets	11111111 11111111 00000000 00000000	255.255.0.0	/16
Class C	3 octets	1 octet	11111111 11111111 11111111 00000000	255.255.255.0	/24

Πίνακας 1.6: Default subnet masks

Οι μάσκες υποδικτύου μας επιτρέπουν να χωρίσουμε ένα δίκτυο σε πολλά μικρότερα ή ακόμα και να ομαδοποιήσουμε πολλά μικρά δίκτυα σε ένα μεγαλύτερο. Για παράδειγμα έστω ότι μία εταιρία στην Αθήνα χρειάζεται να συνδέσει τους υπολογιστές της στο Internet. Στα γραφεία της εταιρίας υπάρχουν συνολικά 125 υπολογιστές και όπως είναι προφανές θα χρειαστεί ένα class C δίκτυο που προσφέρει συνολικά μέχρι και 254 IP διευθύνσεις για hosts. Έστω ότι το class C δίκτυο που της διατίθεται είναι το 195.224.64.0. Η εταιρία αναθέτει τις πρώτες 125 πρώτες διευθύνσεις 195.224.64.1 έως 192.168.64.125 στους υπολογιστές της. Οι υπόλοιπες (192.168.64.126 έως 192.168.64.254) μένουν αχρησιμοποίητες ενώ η τελευταία 192.168.64.255 είναι η broadcast διεύθυνση του δικτύου. Μετά από λίγο καιρό η εταιρεία αυτή ανοίγει άλλο ένα παράρτημα με 125 υπολογιστές στην Θεσσαλονίκη και θέλει να συνδέσει και αυτούς στο Internet. Μία επιλογή θα ήταν η εταιρία να αγοράσει άλλο ένα class

C δίκτυο για το νέο παράρτημα. Μια άλλη επιλογή είναι η εταιρία να χρησιμοποιήσει τις αχρησιμοποίητες IP's απο το 192.168.64.0 δίκτυο που της ανήκει ήδη. Καθώς όμως το παράρτημα στη Θεσσαλονίκη χρειάζεται το δικό του δίκτυο, θα πρέπει το class C δίκτυο που έχει να χωριστεί σε μικρότερα δίκτυα ή υποδίκτυα. Αυτό είναι δυνατό με την χρήση μιας subnet mask.

Η default subnet mask του class C δικτύου της εταιρίας είναι η

11111111 11111111 11111111 00000000 ή 255.255.255.0 ή 192.168.64.0 /24

όπου τα 24 πρώτα 1 bits δηλώνουν το Network κομμάτι της διεύθυνσης του δικτύου ενώ τα 8 τελευταία 0 bits δηλώνουν το Host κομμάτι. Αν τα 0 bits αντί για 8 ήταν 7 σε αριθμό τότε τα 7 hosts bits θα δήλωναν ότι οι διαθέσιμες IP's για hosts είναι $2^7 = 128$ και η subnet mask θα ήταν:

11111111 11111111 11111111 10000000 ή 255.255.255.128 ή 192.168.64.0 /25

Μία τέτοια subnet mask θα έσπαγε το δίκτυο της εταιρίας σε δύο μικρότερα υποδίκτυα όπου τα καθένα θα μπορούσε να έχει από 128-2=126 συνδεδεμένους hosts. Κάτι τέτοιο θα ήταν ιδανικό για την παραπάνω εταιρία καθώς καλύπτει έστω και οριακά της ανάγκες για τα δύο γραφεία της σε Αθήνα και Θεσσαλονίκη. Έτσι τα γραφεία στην Αθήνα θα ανήκαν στο δίκτυο 192.168.64.0 με μάσκα 255.255.255.128 και broadcast address 192.168.64.127 ενώ τα γραφεία στην Θεσσαλονίκη θα άνηκαν στο δίκτυο 192.168.64.128 με μάσκα 255.255.255.128 και broadcast address 192.168.64.255.

Όπως φάνηκε απο το παραπάνω παράδειγμα αλλάζοντας την default μάσκα του δικτύου είναι δυνατό να σπάσουμε ένα δίκτυο σε μικρότερα υποδίκτυα. Αυτό επιτυγχάνεται "δανείζοντας" μερικά bits από το Host κομμάτι στο Network κομμάτι της IP διεύθυνσης. Όσο περισσότερα bits δανείζουμε τόσα περισσότερα υποδίκτυα δημιουργούμε μειώνοντας όμως τον συνολικό αριθμό από hosts που μπορεί να έχει το κάθε υποδίκτυο.

Ο πίνακας 1.7 δίνει τις πιθανές μάσκες για ένα class C δίκτυο αναγράφοντας τον αριθμό υποδικτύων και διαθέσιμων host IPs που δημιουργούνται σε κάθε περίπτωση.

Subnet mask (Συντόμευση)	**Subnet mask (Δεκαδική μορφή)**	**Subnet mask (Δυαδική μορφή)**	**Πλήθος Subnets**	**Πλήθος Hosts / Subnet**
24	255.255.255.0	11111111 11111111 11111111 00000000	$2^0 = 1$	$2^8 = 256$
25	255.255.255.128	11111111 11111111 11111111 10000000	$2^1 = 2$	$2^7 = 128$
26	255.255.255.192	11111111 11111111 11111111 11000000	$2^2 = 4$	$2^6 = 64$
27	255.255.255.224	11111111 11111111 11111111 11100000	$2^3 = 8$	$2^5 = 32$
28	255.255.255.240	11111111 11111111 11111111 11110000	$2^4 = 16$	$2^4 = 16$
29	255.255.255.248	11111111 11111111 11111111 11111000	$2^5 = 32$	$2^3 = 8$
30	255.255.255.252	11111111 11111111 11111111 11111100	$2^6 = 64$	$2^2 = 4$

Πίνακας 1.7: Πιθανές μάσκες για ένα C class δίκτυο

Για τον παραπάνω πίνακα αξίζει να αναφερθεί ότι η τελευταία στήλη αναφέρεται στις συνολικές αλλά όχι και στις ελεύθερες για χρήση Host IP addresses που προκύπτουν. Ο αριθμός των αποτελεσματικών

IP διευθύνσεων είναι αυτός που αναφέρεται στον πίνακα μείον 2, καθώς η πρώτη από όλες τις διευθύνσεις είναι η διεύθυνση του ίδιου του υποδικτύου, ενώ η τελευταία είναι η broadcast διεύθυνση που χρησιμεύει στην μαζική αποστολή πακέτων σε όλους τους hosts του δικτύου.

Ο υπολογισμός της κατάλληλης μάσκας που πρέπει να τεθεί σε ένα δίκτυο έχει πάντα σαν γνώμονα το συνολικό αριθμό των hosts που θέλουμε να διευθυνσιοδοτήσουμε σε κάθε ένα από τα παραγόμενα υποδίκτυα. Η μασκά που απαιτείται για το δίκτυο με τους περισσότερους hosts είναι αυτή που πρέπει να χρησιμοποιηθεί για το subneting. Στην συνέχεια βρίσκουμε την μικρότερη δυνατή δύναμη του 2 που θα μας δώσει αυτόν τον αριθμό (συν 2 αν υπολογίσουμε και την διεύθυνση υποδικτύου και την broadcast) και δανείζουμε τόσα bits στο Network κομμάτι της διεύθυνσης. Τα συνολικά υποδίκτυα που θα δημιουργηθούν θα είναι $2^{\text{δανειζόμενα bits}}$.

Ο πίνακας 1.8 δείχνει τα παραγόμενα subnets που προκύπτουν από το subneting της class C 195.64.224.0 χρησιμοποιώντας την μάσκα 255.255.255.224 που δανείζεται 3 bits από το host κομμάτι δίνοντας $2^3 = 8$ subnets με $2^5 = 32$ hosts το καθένα.

Subnet	Host IP range	Broadcast address
195.64.224.0	.1 - .30	195.64.224.31
195.64.224.32	.33 - .62	195.64.224.63
195.64.224.64	.65 - .94	195.64.224.95
195.64.224.96	.97 - .126	195.64.224.127
195.64.224.128	.129 - .158	195.64.224.159
195.64.224.160	.161 - .190	195.64.224.191
195.64.224.192	.193 - .222	195.64.224.223
195.64.224.224	.225 - .254	195.64.224.255

Πίνακας 1.8: Αποτέλεσμα subneting με μάσκα /27

Ευρεση των subnets ANDing

Στην περίπτωση που γνωρίζουμε την IP διεύθυνση και την μάσκα ενός Host και θέλουμε να βρούμε σε πιο υποδίκτυο ανήκει αρκεί να γράψουμε την μάσκα κάτω από την IP σε δυαδική μορφή να να εκτελέσουμε ένα λογικό AND μεταξύ των δύο. Για παράδειγμα ο Host με την IP 195.64.224.130 και μάσκα 255.255.255.224.

```
195.64.224.130      ----> 11000011 01000000 11100000 10000010
255.255.255.224     ----> 11111111 11111111 11111111 11100000
AND                       11000011 01000000 11100000 10000000  ---> 195.64.224.128
```

Το αποτέλεσμα αυτό επιβεβαιώνεται και από τον πίνακα 1.8 όπου η 195.64.224.130 βρίσκεται στο 5ο subnet.

2. Συσκευές και Τύποι Δικτύωσης

2.1 Συσκευές Δικτύωσης

Ένα δίκτυο αποτελείται από διάφορες δικτυακές συσκευές που διασυνδέονται μεταξύ τους για την μεταφορά δεδομένων. Αυτές μπορεί να είναι συσκευές του τελικού χρήστη (end-user devices) όπως προσωπικοί υπολογιστές, δικτυακοί εκτυπωτές κ.α, ή συσκευές δικτύωσης όπως repeaters, hubs, switches, routers κ.α. Που διασυνδέουν μεταξύ τους πολλές end-user συσκευές επεκτείνοντας έτσι το εύρος του δικτύου.

Κάρτα Δικτύου (Network Interface Card - NIC)

Η κάρτα δικτύου είναι ο εξοπλισμός που συνδέει μια end-user συσκευή όπως έναν υπολογιστή στο δίκτυο, και πιο συγκεκριμένα στο τοπικό δίκτυο (LAN) του χρήστη. Είναι ένα ολοκληρωμένο κύκλωμα το οποίο παρέχει όλες τις απαραίτητες λειτουργίες για την μετάδοση των δεδομένων του χρήστη και την διασύνδεση της end-user συσκευής στο φυσικό μέσο του δικτύου. Κάθε NIC έχει μία MAC διεύθυνση η οποία είναι 48 bits και παρέχεται από τον κατασκευαστή, ενώ είναι παγκοσμίως μοναδική. Οι NICs μπορεί να είναι είτε ενσωματωμένες πάνω στην μητρική πλακέτα του υπολογιστή, είτε να υλοποιούνται σε πλακέτες επέκτασης (PCI ή ISA για desktops και PCMCIA για laptops). Τελευταία έχουν εμφανιστεί και εξωτερικές NICs που συνδέονται σε USB θύρα του υπολογιστή. Τέλος οι NICs μπορεί να είναι είτε ενσύρματες είτε ασύρματες.

Εικόνα 2.2: Ενσύρματη PCI κάρτα δικτύου

Εικόνα 2.1: Ασύρματη PCMCIA κάρτα δικτύου

Repeater

Οι Repeaters είναι συσκευές δικτύωσης, οι οποίες διασυνδέουν τμήματα (segments) δικτύου επεκτείνοντας έτσι το συνολικό εύρος του δικτύου. Αυτό είναι απαραίτητο όταν το δίκτυο απλώνεται σε μεγάλη περιοχή καθώς το σήμα εξασθενεί για να φτάσει από το ένα άκρο στο άλλο. Στην ουσία θεωρούνται 'χαζές' συσκευές καθώς το μόνο που κάνουν είναι να ενισχύσουν το σήμα, που τους έρχεται από το ένα segment και να το προωθήσουν στο επόμενο, χωρίς να χρειαστεί να κάνουν άλλες ενέργειες που έχουν να κάνουν με δρομολόγηση πακέτων ή επιλογή βέλτιστης διαδρομής που εκτελούν άλλες συσκευές δικτύωσης όπως οι routers. Οι λειτουργίες των repeaters ανήκουν στο πρώτο επίπεδο του OSI. Η πιο συνήθης χρήση τους είναι η επέκταση ενός LAN ώστε να απλώνεται πάνω από 100 μέτρα. Σήμερα σπάνια χρησιμοποιούνται repeaters καθώς οι λειτουργίες τους έχουν ενσωματωθεί σε άλλες πιο προηγμένες συσκευές δικτύωσης.

Hub

Τα hubs είναι συσκευές που συγκεντρώνουν πολλές δικτυακές συνδέσεις σε ένα segment δικτύου. Έχουν πολλαπλές πόρτες πάνω στις οποίες συνδέονται τελικές συσκευές δικτύου όπως, PCs, εκτυπωτές και άλλα hubs. Στην ουσία το hub υλοποιεί εσωτερικά ένα μικρό LAN στο οποίο παίρνουν μέρος όλες οι συσκευές που συνδέονται στις πόρτες του. Όταν μια συσκευή που συνδέεται σε κάποια

πόρτα του hub στείλει δεδομένα στο δίκτυο, το hub αναπαράγει το σήμα από την πόρτα που το δέχτηκε και το στέλνει σε όλες τις άλλες πόρτες του από όπου θα το λάβει ένας ή περισσότεροι παραλήπτες. Αυτό σημαίνει ότι όσοι είναι συνδεδεμένοι πάνω στο Hub μπορούν να βλέπουν την κίνηση του δικτύου και μάλιστα όλοι μοιράζονται το προσφερόμενο bandwidth.

Εικόνα 2.3: Το Hub

Η λειτουργία των hubs είναι αρκετά παρόμοια με αυτή των repeaters με την μόνη διαφορά ότι οι repeaters έχουν συνήθως μόνο δύο πόρτες για να διασυνδέσουν δύο segments δικτύου, ενώ τα hubs έχουν πολλαπλές πόρτες για να διασυνδέσουν πολλές συσκευές πάνω σε ένα segment. Και τα hubs εκτελούν λειτουργίες του πρώτου επιπέδου του OSI, ενώ και αυτά πλέον σήμερα έχουν αντικατασταθεί από τα switches.

Bridge

Όπως οι repeaters έτσι και τα bridges δίνουν την δυνατότητα επέκτασης ενός δικτύου μόνο που τα bridges είναι αρκετά πιο έξυπνες συσκευές και κυρίως χρησιμοποιούνται είτε για να συνδέσουν δύο LANs μεταξύ τους τα οποία μπορεί να είναι και διαφορετικού τύπου, είτε για να κατατμήσουν ένα μεγάλο LAN σε μικρότερα βελτιώνοντας έτσι την επίδοση και την λειτουργικότητα του δικτύου. Αυτό συμβαίνει καθώς τα bridges απομονώνουν την δικτυακή κίνηση αλλά και το bandwidth ανά το κάθε LAN που διασυνδέουν και αποτρέπουν την διαρροή πακέτων από το ένα LAN στο άλλο. Έτσι οι συσκευές στο ένα LAN επικοινωνούν απευθείας μεταξύ τους ενώ επικοινωνούν μέσω του bridge με συσκευές που ανήκουν σε άλλο LAN. Για να συμβεί αυτό τα bridges εκτός από το να αναπαράγουν το σήμα περνώντας το από το ένα LAN στο άλλο, εκτελούν και λειτουργίες switching καθώς εξετάζουν την φυσική διεύθυνση του αποστολέα και του παραλήπτη των πακέτων και τα δρομολογούν στο κατάλληλο LAN. Για αυτό το σκοπό τα bridges χρησιμοποιούν εσωτερικά κάποιους πίνακες (τα bridging tables) που περιέχουν αντιστοιχήσεις μεταξύ των πορτών του και των φυσικών διευθύνσεων MAC των συσκευών του δικτύου.

Το bridge εκτελεί λειτουργίες του δεύτερου επιπέδου του OSI καθώς σε αυτό το επίπεδο τα data είναι οργανωμένα σε frames τα οποία με την σειρά τους χαρακτηρίζονται από τις φυσικές διευθύνσεις του αποστολέα και του παραλήπτη τις οποίες χρησιμοποιεί το bridge για την λειτουργία του.

Συνοπτικά η λειτουργία του bridge έχει ως εξής:

Όταν φτάσει ένα πακέτο σε μια πόρτα του bridge τότε ελέγχεται η φυσική διεύθυνση προορισμού του πακέτου για το αν ο παραλήπτης είναι γνωστός δηλαδή αν υπάρχει κάποια αντιστοιχία στο bridging table της διεύθυνσης αυτής με κάποια πόρτα στο bridge. Εάν υπάρχει και ο παραλήπτης είναι στο ίδιο

segment με τον αποστολέα τότε το bridge απλώς αγνοεί το πακέτο, εάν όμως ο παραλήπτης είναι γνωστός και ανήκει σε άλλο segment τότε το bridge αναπαράγει το πακέτο στην πόρτα όπου είναι συνδεδεμένο το segment του παραλήπτη. Στην περίπτωση που το bridge δεν ξέρει πως να προωθήσει το πακέτο στον παραλήπτη καθώς δεν υπάρχει στο bridging table, τότε μεταδίδει το πακέτο σε όλες τις πόρτες του και κατά συνέπεια σε όλα τα semgnets. Σε αυτή την περίπτωση όταν ο παραλήπτης στείλει με την σειρά του απάντηση στον αποστολέα το bridge θα μάθει που βρίσκεται αυτός και θα μπορεί πλέον να του προωθεί τα πακέτα απευθείας στο σωστό segment.

Switch

Τα switches όπως και τα bridges κάνουν **segmentation** του δικτύου καθώς και διαχωρισμό των **collision domains**. Δηλαδή έχουν την ικανότητα να διασπάσουν ένα μεγάλο δίκτυο σε μικρότερα segments και να περιορίζουν την κίνηση στο κάθε segment ώστε να μην επηρεάζει τα άλλα segments. Αυτό επιφέρει αφιερωμένο bandwidth για το κάθε segment καθώς και περιορισμό των συγκρούσεων (collisions) μόνο στο segment που συμβαίνουν και όχι στα γειτονικά segments. Η κύρια διαφορά τους με τα bridges είναι ότι τα switches είναι γενικά πιο 'έξυπνες' συσκευές καθώς έχουν πολλαπλές πόρτες και την ικανότητα να διασυνδέσουν πολλά segments σε ένα κεντρικό σημείο αναλαμβάνοντας την βέλτιστη μεταγωγή των πακέτων από segment σε segment.

Εικόνα 2.4: Ένα switch με 24 πόρτες

Σε γενικές γραμμές τα switches έχουν αντικαταστήσει τα hubs και είναι αυτά που χρησιμοποιούνται σήμερα για την διασύνδεση πολλών συσκευών στο LAN αλλά και για την διασύνδεση των LANs μεταξύ τους. Τα switches σε αντίθεση με τα hubs για κάθε επικοινωνία μεταξύ δύο συσκευών που συνδέονται στο switch δημιουργούν ένα ιδεατό κύκλωμα με αφιερωμένο bandwidth για την επικοινωνία μεταξύ των δύο.

Router

Οι routers είναι συσκευές δικτύωσης που περιλαμβάνουν τις λειτουργίες όλων των παραπάνω συσκευών. Δηλαδή, αναπαράγουν το σήμα από τη μία πόρτα τους σε μία άλλη, κάνουν segmentation του δικτύου, διατηρούν ξεχωριστά collision domains, δρομολογούν τα πακέτα στο σωστό προορισμό με βάση την διεύθυνση αποστολέα και είναι οι συσκευές που κατά βάση προσφέρουν WAN συνδέσεις για την διασύνδεση LANs σε μεγάλες αποστάσεις. Σε αντίθεση με τα switches οι routers λειτουργούν στο τρίτο επίπεδο του OSI και αντί για φυσικές διευθύνσεις χρησιμοποιούν λογικές διευθύνσεις για την δρομολόγηση των πακέτων. Ένα άλλο πολύ σημαντικό χαρακτηριστικό του router είναι ότι μπορεί να περιορίζει τα broadcasts στο δίκτυο από όπου προέρχονται και δεν τα προωθεί στα δίκτυα που είναι συνδεδεμένα στις άλλες πόρτες του. Αυτό έχει σαν αποτέλεσμα την καλύτερη απόδοση του δικτύου, την πιο εύκολη διαχείρισή του και αυξημένη ασφάλεια.

Εικόνα 2.5: Το πίσω μέρος ενός router

Από τις συσκευές δικτύωσης που εξετάστηκαν παραπάνω οι repeaters και τα hubs θεωρούνται παθητικές (passive) συσκευές ενώ τα bridges, τα switches και οι routers θεωρούνται ενεργητικές (active) συσκευές. Ο διαχωρισμός τους βασίζεται στον τρόπο με τον οποίο διαχειρίζονται την δικτυακή κίνηση και έτσι ενώ τα hubs και οι repeaters απλά ενισχύουν και αναμεταδίδουν το ηλεκτρικό σήμα σε όλες τις πόρτες τους, οι άλλες συσκευές επεξεργάζονται τα πακέτα και παίρνουν έξυπνες αποφάσεις για την σωστή δρομολόγησή τους και την μετάδοσή τους πάνω στο μέσο διασύνδεσης.

2.2 Τύποι Δικτύων

Μερικά από τα κριτήρια κατηγοριοποίησης των δικτύων σήμερα είναι η γεωγραφική τους εξάπλωση, ο σκοπός που εξυπηρετούν και η πρόσβαση που προσφέρουν.

LAN – Local Area Network (Τοπικά Δίκτυα)

Τα τοπικά δίκτυα χαρακτηρίζονται κυρίως από την μικρή γεωγραφική τους κάλυψη που μπορεί να είναι μερικά μέτρα έως και μερικά χιλιόμετρα (σχεδόν μέχρι 2 χλμ). Ένα LAN συνήθως καλύπτει έναν όροφο κτιρίου, ένα ολόκληρο κτίριο ή και μερικά κτίρια που βρίσκονται σε μικρή απόσταση μεταξύ τους. Τα LANs διασυνδέουν πολλαπλές, σχετικά κοντινές μεταξύ τους δικτυακές συσκευές και προσφέρουν αρκετά μεγάλες ταχύτητες μεταφοράς δεδομένων (10Mbps – 1Gbps) ενώ λειτουργούν σε συνεχή βάση. Οι κυριότερες συσκευές δικτύωσης που χρησιμοποιούνται στα LANs είναι NICs, Hubs, Repeaters, Switches και Routers, ενώ μερικές από τις πιο γνωστές τεχνολογίες LANs είναι το Ethernet και το Token Ring.

WAN – Wide Area Network (Δίκτυο Ευρείας Περιοχής)

Τα WANs συνήθως χρησιμοποιούνται για να διασυνδέσουν δύο ή περισσότερα LANs που απέχουν μεγάλες μεταξύ τους αποστάσεις. Αυξάνουν σημαντικά την απόσταση διασύνδεσης προσφέροντας όμως συνήθως μικρότερες ταχύτητες μετάδοσης δεδομένων μεταξύ των LANs. Η λειτουργία ενός WAN μπορεί να είναι συνεχής ή κατά απαίτηση και μερικές από τις πιο συνήθεις WAN τεχνολογίες είναι:

1. Frame Relay
2. DSL
3. ISDN
4. E1, T1, E3, T3
5. Modems – PSTN

MAN – Metropolitan Area Network (Μητροπολιτικό Δικτυο)

Ένα MAN είναι συνήθως ένα δίκτυο που καλύπτει μία πόλη και που συνδέει δύο ή περισσότερα LANs που ανήκουν στον ίδιο οργανισμό. Τα MANs προσφέρουν μικρές έως μεσαίες ταχύτητες μεταφοράς δεδομένων και παραδοσιακά υλοποιούνταν με τεχνολογίες όπως ATM, FDDI και SMDS οι οποίες πλέον αντικαθιστούνται από το Ethernet και από ασύρματες τεχνολογίες. Οι δικτυακές συσκευές που χρησιμοποιούνται στα MANs είναι ίδιες με αυτές των WANs.

SAN – Storage Area Network

Ένα SAN είναι ένα δίκτυο υψηλών επιδόσεων αφιερωμένο αποκλειστικά για μετακίνηση δεδομένων μεταξύ servers συστημάτων και συσκευών αποθήκευσης. Η υψηλές ταχύτητες που επιτυγχάνονται σε ένα SAN οφείλονται κυρίως στο ότι η κίνηση του δικτύου περιορίζεται ανάμεσα σε servers με συσκευές αποθήκευσης, συσκευή αποθήκευσης με συσκευή αποθήκευσης, server με server. Όλη αυτή η κίνηση διαχωρίζεται από την δικτυακή κίνηση που οφείλεται σε δραστηριότητα των χρηστών του δικτύου.

Τα κυριότερα χαρακτηριστικά των SANs είναι:

- **Υψηλές Επιδόσεις:** Επιτρέπουν ταυτόχρονη και σε υψηλές ταχύτητες πρόσβαση σε δίσκους και συστοιχίες από μαγνητικές ταινίες από δύο ή περισσότερους servers.
- **Διαθεσιμότητα:** Έχουν την δυνατότητα να παίρνουν αντίγραφα ασφαλείας σε διαφορετικές τοποθεσίες που μπορεί να απέχουν μέχρι και 10 χλμ. μεταξύ τους.
- **Επεκτασιμότητα:** Μπορούν να χρησιμοποιούν διαφορετικές τεχνολογίες ταυτόχρονα και έτσι να επεκταθούν με σχετική ευκολία χωρίς να επηρεάζονται οι υπηρεσίες που προσφέρουν.

Δεν πρέπει να γίνεται σύγχυση των SANs τα οποία προσφέρουν πρόσβαση σε απομακρυσμένες συσκευές αποθήκευσης σε επίπεδο 'blocks' με τα πιο συνήθη πρωτόκολλα remote sharing (SMB, NFS) που προσφέρουν πρόσβαση σε επίπεδο αρχείων ή filesytem.

VPN – Virtual Private Network

Το VPN είναι ένα ιδεατό ιδιωτικό δίκτυο υλοποιημένο πάνω από ένα δίκτυο με ευρεία δημόσια πρόσβαση όπως το Internet. Ο στόχος του είναι να διαχωρίσει και να απομονώσει συγκεκριμένη δικτυακή κίνηση από το δημόσιο δίκτυο δημιουργώντας ένα ιδεατό δίκτυο στο οποίο τις περισσότερες των περιπτώσεων η διακίνηση των δεδομένων γίνεται με ασφαλή τρόπο μέσω κρυπτογράφησης, ενώ η πρόσβαση σε αυτό απαιτεί πρώτα αυθεντικοποίηση των χρηστών.

Είδη VPNs:

Access VPNs

Επιτρέπουν την απομακρυσμένη σύνδεση ενός ή περισσοτέρων υπαλλήλων ή οικιακών γραφείων στο εσωτερικό δίκτυο της εταιρίας. Για παράδειγμα ένας υπάλληλος μπορεί να εργάζεται από το σπίτι του αφού έχει συνδεθεί μέσω Internet με μία dial-up γραμμή και modem στο εσωτερικό δίκτυο της εταιρίας. Αυτός θα έχει πρόσβαση στους ίδιους πόρους όπως αν βρισκόταν σε έναν υπολογιστή μέσα στην εταιρία.

Intranet VPNs

Προσφέρουν απομακρυσμένη διασύνδεση ενός ή περισσοτέρων παραρτημάτων μιας εταιρίας με το εσωτερικό δίκτυο των κεντρικών γραφείων της εταιρείας.

Extranet VPNs

Προσφέρουν απομακρυσμένη διασύνδεση ενός ή περισσοτέρων γραφείων συνεργατών μιας εταιρίας στο εσωτερικό δίκτυο της εταιρίας. Ενώ στα Intranet VPNs μόνο υπάλληλοι της εταιρίας έχουν δικαίωμα σύνδεσης στο εσωτερικό δίκτυο, στα Extranet VPNs η σύνδεση επιτρέπει και σε εξωτερικούς συνεργάτες να έχουν πρόσβαση στο εσωτερικό δίκτυο της εταιρίας.

Σε γενικές γραμμές τα VPNs προσφέρουν μία οικονομική και ασφαλή λύση για διασύνδεση μεταξύ απομακρυσμένων sites, καθώς δεν υλοποιούνται με φυσικές αφιερωμένες γραμμές μεταξύ των δύο σημείων αλλά χρησιμοποιούν το δημόσιο Internet και ειδικό λογισμικό.

Intranet vs. Extranet

Κάθε δίκτυο χωρίζεται σε δύο μέρη. Το **Intranet** (**Εσωτερικό Δίκτυο**) και το **Extranet** (**Εξωτερικό Δίκτυο**). Ο πιο συνήθης τρόπος που διαχωρίζονται αυτά τα δύο μέρη είναι με ένα Firewall. Το Intranet αφορά τους εσωτερικούς χρήστες του δικτύου και τον τρόπο που αυτοί διασυνδέονται και επικοινωνούν μεταξύ τους και με τους κοινούς πόρους του δικτύου όπως με εκτυπωτές και servers. Το Extranet έχει να κάνει με την διασύνδεση και την επικοινωνία απομακρυσμένων χρηστών (που βρίσκονται εκτός του εσωτερικού δικτύου) με τις υπηρεσίες, τους χρήστες και τους πόρους του εσωτερικού δικτύου. Συγκεκριμένες πολιτικές ασφάλειας καθορίζουν τον τρόπο που οι χρήστες από τα δύο μέρη του δικτύου μπορούν να έχουν πρόσβαση στις υπηρεσίες και τους πόρους του δικτύου και συνήθως οι χρήστες του Extranet έχουν πολύ λιγότερα δικαιώματα από τους χρήστες του Intranet.

2.3 Μοντέλα Αναφοράς Δικτύωσης

OSI Networking Reference Model

Το **OSI** (**Open Systems Interconnection**) αναπτύχθηκε το 1982 από τον οργανισμό International Organization for Standardization (ISO) και είναι ένα μοντέλο αναφοράς δικτύωσης που χωρίζεται σε επτά επίπεδα (layers). Ο στόχος του ήταν να δημιουργήσει πρότυπα ώστε να περιορίσει την ασυμβατότητα που προέκυπτε από την διαφορετική υλοποίηση δικτύων και πρωτοκόλλων δικτύωσης από τους διάφορους κατασκευαστές όπου καθένας χρησιμοποιούσε τους δικούς του κανόνες και τρόπους υλοποίησης. Η δημιουργία πρωτοκόλλων και η υλοποίηση δικτύων που συμφωνούν σε ένα κοινό μοντέλο τυποποίησης επιτρέπει δίκτυα διαφορετικών εταιριών να μπορούν να επικοινωνούν μεταξύ τους.

Τα επτά επίπεδα του OSI φαίνονται στο παρακάτω σχήμα.

7	**Application** (Επίπεδο Εφαρμογής)
6	**Presentation** (Επίπεδο Παρουσίασης)

5	**Session** (Επίπεδο Συνόδου)
4	**Transport** (Επίπεδο Μεταφοράς)
3	**Network** (Επίπεδο Δικτύου)
2	**Data Link** (Επίπεδο Ζεύξης Δεδομένων)
1	**Physical** (Φυσικό Επίπεδο)

Σχήμα 2.1: Τα 7 επίπεδα του OSI

Το μοντέλο OSI περιγράφει τις ενέργειες που απαιτούνται για να μπορέσει η πληροφορία να ταξιδέψει μεταξύ δύο διασυνδεδεμένων συστημάτων. Κάθε επίπεδο εκτελεί συγκεκριμένες λειτουργίες που είναι ανεξάρτητες από τις λειτουργίες των άλλων επιπέδων και προσφέρει κάποιες υπηρεσίες στο αμέσως από πάνω επίπεδο. Η διάσπαση της όλης διαδικασίας σε επτά επίπεδα όπου το καθένα έχει συγκεκριμένες και ανεξάρτητες από τα άλλα επίπεδα λειτουργίες έχει ως συνέπεια την απομόνωση των προβλημάτων στο κάθε επίπεδο και προσφέρει ευελιξία καθώς αλλαγές σε ένα επίπεδο δεν επηρεάζουν τα άλλα επίπεδα. Είναι σημαντικό να τονιστεί ότι υπάρχει κάθετη και οριζόντια λογική διασύνδεση μεταξύ των επιπέδων. Στην κάθετη διασύνδεση το κάθε επίπεδο μεταφέρει δεδομένα στο αμέσως από κάτω του και το αμέσως από πάνω του. Με αυτόν τον τρόπο μπορεί το κάθε επίπεδο να προσφέρει κάποιες υπηρεσίες στο αμέσως από πάνω του. Στην οριζόντια διασύνδεση το κάθε επίπεδο συνδέεται λογικά με το αντίστοιχο επίπεδο του άλλου άκρου με το οποίο επικοινωνεί. Τα δεδομένα μεταξύ των επιπέδων μεταφέρονται από τα αντίστοιχα πρωτόκολλα μέσα σε ειδικές για το κάθε επίπεδο μονάδες μεταφοράς που ονομάζονται **PDUs** (**Protocol Data Units**). Αυτές ανάλογα με το επίπεδο μπορεί να είναι απλά **Data**, **Segments**, **Packets**, **Frames** που καταλήγουν σε **bits** τα οποία θα μεταδοθούν μέσα από το φυσικό μέσο. Στην πλευρά του αποστολέα καθώς το PDU του επιπέδου **N** μεταφέρεται στο επίπεδο **N-1** από κάτω, προστίθεται σε αυτό ένας **header** και ίσως και κάποιος **trailer** που περιέχουν πληροφορίες ελέγχου του επιπέδου N-1. Αντίστοιχα στην πλευρά του παραλήπτη καθώς τα δεδομένα φτάνουν στο N-1 επίπεδο αυτό επεξεργάζεται την πληροφορία που το αφορά, αφαιρεί τον δικό του header και trailer και προκύπτει το PDU του N επιπέδου στο οποίο και παραδίδεται.

Physical Layer
Αποστολή bits πάνω από το φυσικό μέσο. Το επίπεδο αυτό ασχολείται με τα καλώδια, τους τύπους connectors, τα σήματα μετάδοσης, τον συγχρονισμό μεταξύ των δύο συσκευών, τις ηλεκτρικές τάσεις κ.α.

Data Link Layer
Καθορίζει τα λειτουργικά χαρακτηριστικά για να αποκατασταθεί, να υποστηριχτεί και να τερματιστεί μία σύνδεση μεταξύ των δύο άκρων μιας γραμμής. Μεταφέρει **frames** από το ένα άκρο στο άλλο χρησιμοποιώντας φυσικές διευθύνσεις και με αξιόπιστο τρόπο εκτελώντας ανίχνευση και διόρθωση σφαλμάτων και έλεγχο ροής δεδομένων.

Network Layer

Μεταφέρει **packets** μεταξύ δύο ακραίων σταθμών σε ένα μεγάλο δίκτυο, χρησιμοποιώντας λογικές διευθύνσεις για να προσδιορίσει το κάθε άκρο και να δρομολογήσει τα πακέτα από κάθε ενδιάμεσο κόμβο. Κάνει ταξινόμηση και αρίθμηση πακέτων ενώ θεωρείται *best-effort delivery service*.

Transport Layer
Προσφέρει από άκρη σε άκρη αξιόπιστη μεταφορά δεδομένων σε μορφή **segments**, εκτελώντας έλεγχο και αποκατάσταση σφαλμάτων, έλεγχο ροής και αρίθμηση δεδομένων.

Session Layer
Ασχολείται με την καθίδρυση, την διαχείριση, την αποκατάσταση και τον τερματισμό διαλόγου μεταξύ των εφαρμογών των δύο ακραίων σημείων.

Presentation Layer
Ασχολείται με την παρουσίαση των δεδομένων που ανταλλάσσονται μεταξύ των εφαρμογών των δύο ακραίων σημείων ώστε να είναι κατανοητή και από τους δύο και να μπορεί η μία εφαρμογή να επικοινωνεί με την άλλη. Εδώ μπορεί να πραγματοποιούνται διαδικασίες όπως κρυπτογράφηση και συμπίεση δεδομένων, μετατροπή κωδικοσελίδων κλπ.

Application Layer
Εδώ παρέχεται ο τρόπος με τον οποίο μπορεί να επικοινωνεί η μία εφαρμογή με την άλλη και είναι κυρίως κάτω από τον έλεγχο του χρήστη.

Όπως φαίνεται και στο σχήμα 2.2 κάθε επίπεδο χρησιμοποιεί το δικό του PDU. Τα PDUs ενσωματώνονται (encapsulated) μέσα στα PDUs του αμέσως από κάτω επιπέδου στην πλευρά του αποστολέα μέχρις ότου μεταδοθούν με την μορφή bits από το φυσικό μέσο. Στην πλευρά του παραλήπτη το κάθε επίπεδο αποσπά (decapsulate) από το PDU του την πληροφορία που το αφορά και με την οποία επικοινωνεί με το πρωτόκολλο του αντίστοιχου επιπέδου της απέναντι πλευράς και παραδίδει τα δεδομένα στο παραπάνω επίπεδο που πλέον έχουν την μορφή του δικού του PDU.

Το μοντέλο TCP/IP

Το μοντέλο **TCP/IP** δημιουργήθηκε από το US DoD (Department of Defence) ως κομμάτι του ARPANET σαν πρότυπο μοντέλο για την δημιουργία δικτύων που θα μπορούσαν να λειτουργήσουν κάτω από οποιεσδήποτε συνθήκες και κυρίως εν καιρό πολέμου όπου έπρεπε οι επικοινωνίες να είναι δυνατές ακόμα και αν ένα μέρος του δικτύου καταστρεφόταν.

Το TCP/IP είναι υλοποιημένο σαν ένα ανοιχτό πρότυπο (open standard) που σημαίνει ότι οποιοσδήποτε μπορεί να το χρησιμοποιήσει, να δημιουργήσει πρωτόκολλα και να χτίσει δίκτυα βασισμένα σε αυτό. Το γεγονός αυτό καθώς και το ότι το TCP/IP προϋπήρχε του OSI, το έκαναν το πιο αποδεκτό και διαδεδομένο μοντέλο αναφοράς και είναι αυτό πάνω στο οποίο έχει χτιστεί το σημερινό Internet.

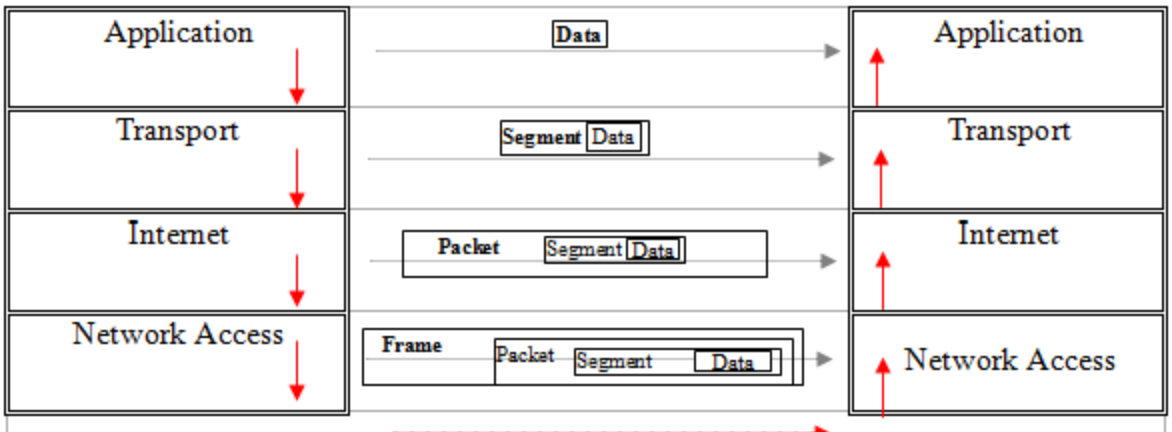
Όπως και το OSI έτσι και το TCP/IP αποτελείται από επίπεδα (layers) με τη διαφορά ότι έχει τέσσερα επίπεδα αντί για εφτά, όπως φαίνεται και στο σχήμα 2.3.

Το **Application layer** είναι αντίστοιχο με αυτό του OSI μόνο που εδώ ενσωματώνει και τα layers Presentation και Session.

Το **Transport layer** είναι αυτό που ασχολείται με την από άκρο σε άκρο επικοινωνία μεταξύ δύο σταθμών με αξιόπιστο τρόπο κάνοντας ανίχνευση και διόρθωση λαθών καθώς και έλεγχο ροής των δεδομένων. Το πιο χαρακτηριστικό πρωτόκολλο του επιπέδου αυτού είναι το **TCP (Transmission Control Protocol)**. Το TCP είναι ένα *connection oriented* πρωτόκολλο οπού προκειμένου για τα δύο άκρα να επικοινωνήσουν θα πρέπει πρώτα να εγκαθιδρύσουν μία λογική σύνδεση μεταξύ τους. Στη συνέχεια καθώς τα δύο άκρα ανταλλάσσουν μεταξύ τους δεδομένα ο αποστολέας αριθμεί τα segments που στέλνει και ο παραλήπτης για κάθε μέρος των δεδομένων που λαμβάνει επιβεβαιώνει την λήψη τους στον αποστολέα. Σε περίπτωση που ο αποστολέας δεν λάβει την επιβεβαίωση μέσα σε κάποιο προκαθορισμένο χρόνο υποθέτει ότι τα δεδομένα δεν έφτασαν στον προορισμό τους και τα ξαναστέλνει. Επίσης όσο διαρκεί η ανταλλαγή δεδομένων ο παραλήπτης έχει την δυνατότητα να ενημερώνει τον αποστολέα για τον όγκο των δεδομένων που μπορεί να δεχτεί σε κάθε δοσοληψία και έτσι να ρυθμίζουν μεταξύ τους την ροή των δεδομένων.

Το **Internet layer** είναι παρόμοιο με το Network Layer του OSI και είναι υπεύθυνο για την διευθυνσιοδότηση και μεταφορά των πακέτων μεταξύ των δύο ακραίων σταθμών. Η δουλειά του Internet layer είναι να παραλάβει τα segments από το Transport layer και να τα μεταφέρει μέσα σε packets στο άλλο άκρο από μία ή περισσότερες διαδρομές. Το πιο χαρακτηριστικό πρωτόκολλο του επιπέδου αυτού είναι το **IP (Internet Protocol)**, το οποίο μπορεί να θεωρηθεί σαν το μέσο μεταφοράς των segments του Transport layer. Το IP είναι **conectionless** δηλαδή δεν απαιτεί την αποκατάσταση λογικής σύνδεσης μεταξύ των δύο άκρων και δεν απαιτεί επιβεβαίωση των πακέτων που στέλνονται. Επίσης κάνει αρίθμηση των πακέτων ώστε να εξασφαλίσει ότι φτάνουν με την σωστή σειρά, και κάνει κατακερματισμό (fragmentation) και επανασυγκόλληση (reassembly) των μεγάλων πακέτων.

Το **Network Access layer** είναι το κατώτερο επίπεδο και στην ουσία ενσωματώνει το Data Link layer και το Physical layer του OSI. Το επίπεδο αυτό ασχολείται με όλα τα λογικά και φυσικά κομμάτια της σύνδεσης που απαιτούνται για να μεταφερθούν τα δεδομένα πάνω από ένα φυσικό μέσο. Παραλαμβάνει τα πακέτα από το Internet layer και τα διαμορφώνει ώστε να μπορέσουν να διαδοθούν πάνω από μία LAN ή WAN γραμμή.



Σχήμα 2.3: Επικοινωνία μεταξύ δύο σταθμών στο OSI

Μερικά από τα πιο γνωστά πρωτόκολλα του TCP/IP περιέχονται στον πίνακα 2.1 αναφέροντας και το επίπεδο στο οποίο ανήκουν.

Επίπεδο	**Πρωτόκολλο**
Application	HTTP, FTP, SMTP, DNS, TELNET, SSH, SNMP
Transport	TCP, UDP
Internet	ICMP, RIP, OSPF, BGP, EIGRP IP ARP, RARP
Network Access	X.25, HDLC, PPP, IEEE 802.3

Πίνακας 2.1: Πρωτόκολλα του TCP/IP

Παρόλο που το TCP/IP και το OSI είναι δύο διαφορετικά μοντέλα, έχουν αρκετά κοινά μεταξύ τους και το ένα δεν αναιρεί το άλλο. Το OSI είναι ένα πιο γενικό μοντέλο και είναι κυρίως θεωρητικό που χρησιμοποιείται σαν οδηγός για την μελέτη δικτύων και πρωτοκόλλων. Το TCP/IP είναι πιο πρακτικό μοντέλο και σε αυτό εξάλλου είναι χτισμένο το Internet. Όπως φάνηκε και από την παραπάνω παρουσίαση τα επίπεδα του TCP/IP μπορούν να αντιστοιχηθούν με αυτά του OSI και το ίδιο ισχύει για τα πρωτόκολλα. Είναι κοινό να λέγεται για παράδειγμα ότι το FTP ανήκει στο επίπεδο 7 (Application layer) του OSI ή ότι το IEEE 802.3 καλύπτει τα δύο πρώτα επίπεδα του OSI.

3. Μέσα Δικτύωσης

Τα μέσα δικτύωσης έχουν να κάνουν με τις φυσικές συνδέσεις που χρησιμοποιούνται για να διασυνδεθούν δικτυακές συσκευές μεταξύ τους. Αυτά μπορεί να είναι καλώδια με σύρματα χαλκού ή οπτικές ίνες ή ακόμα και ασύρματες ζεύξεις.

3.1 Ενσύρματα Μέσα Δικτύωσης

Καλώδια χαλκού

Τα καλώδια χαλκού είναι αυτά που χρησιμοποιούνται στις περισσότερες εγκαταστάσεις τοπικών δικτύων LAN. Ο χαλκός είναι ένα από τα πιο φθηνά στοιχεία της φύσης που είναι καλός αγωγός ηλεκτρικού ρεύματος. Δηλαδή επιτρέπει την διέλευση ηλεκτρονίων από το ένα άκρο στο άλλο. Καθώς τα ηλεκτρικά σήματα μπορούν να χρησιμοποιηθούν για την αναπαράσταση και μεταφορά δεδομένων, ο χαλκός αποτελεί ένα από τα πιο διαδεδομένα μέσα επικοινωνίας δεδομένων για πολλά χρόνια. Υπάρχουν διάφορες υλοποιήσεις καλωδίων χαλκού οι οποίες διαφέρουν μεταξύ τους κυρίως όσο αναφορά το αν μεταφέρουν δεδομένα σε αναλογική ή ψηφιακή μορφή, την ταχύτητα μετάδοσης και την απόσταση μετάδοσης του σήματος. Τα καλώδια χαλκού που θα εξεταστούν παρακάτω είναι το coaxial, το UTP, το STP και ScTP.

Coaxial Cable (ομοαξονικό καλώδιο)

Το **coaxial cable** αποτελείται από ένα χάλκινο αγωγό στο κέντρο του, ο οποίος καλύπτεται από ένα

ελαστικό πλαστικό περίβλημα. Με την σειρά του αυτό περιβάλλεται από ένα πλεχτό χάλκινο στρώμα που λειτουργεί σαν δεύτερος αγωγός για τον σχηματισμό κυκλώματος. Το διαχωριστικό περίβλημα μεταξύ των δύο αγωγών είναι στην ουσία ένα διηλεκτρικό μονωτικό υλικό για τον διαχωρισμό των σημάτων μεταξύ των δύο αγωγών, ενώ ο εξωτερικός αγωγός λειτουργεί και σαν ασπίδα στις ηλεκτρομαγνητικές παρεμβολές για τον εσωτερικό αγωγό. Τέλος, όλη η παραπάνω κατασκευή περιβάλλεται από ένα χοντρό και σχετικά εύκαμπτο κάλυμμα το οποίο προστατεύει το καλώδιο από φυσικές φθορές.

Εικόνα 3. 1: Το ομοαξονικό καλώδιο

Εικόνα 3. 2: Ο T-connector

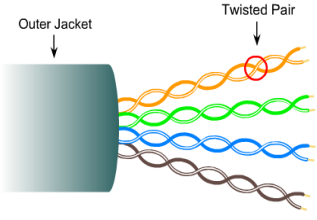
Μερικά από τα πλεονεκτήματα του μέσου αυτού είναι ότι προσφέρει καλή προστασία από εξωτερικούς θορύβους που μπορεί να βλάψουν το σήμα και ότι μπορεί να μεταφέρει δεδομένα σε μεγάλες αποστάσεις (σχεδόν 500 μέτρα) χωρίς να εξασθενεί το σήμα.

Τα μειονεκτήματα του coaxial είναι ότι είναι σχετικά δύσχρηστο καθώς είναι χοντρό και όχι πολύ εύκαμπτο με αποτέλεσμα να είναι δύσκολη και ακριβή η εγκατάστασή του.

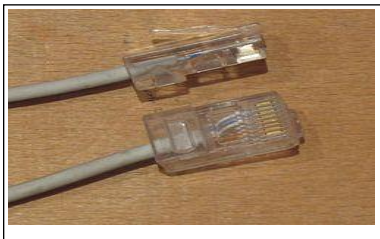
Το coaxial ήταν από τα πρώτα καλώδια που χρησιμοποιήθηκαν για εγκαταστάσεις Ethernet LANs και προσφέρονταν σε δύο τύπους. Το 10BASE5 για Thicknet δίκτυα και το 10BASE2 για Thinnet δίκτυα. Στον πρώτο τύπο το καλώδιο ήταν πιο χοντρό ενώ υποστήριζε ταχύτητες μέχρι 10 Mbps και απόσταση μετάδοσης χωρίς ενίσχυση τα 500 μέτρα. Το Thinnet χρησιμοποιούσε πιο λεπτό και εύκαμπτο καλώδιο που υποστήριζε ταχύτητες μέχρι και 10 Mbps αλλά το σήμα χρειαζόταν ενίσχυση μετά τα 200 μέτρα.

UTP (Unshielded Twisted Pair) cable

Το **UTP** είναι ένα από τα πιο ευρέως διαδεδομένα μέσα που χρησιμοποιούνται για διάφορες δικτυακές συνδέσεις. Αποτελείται από τέσσερα ζεύγη αγωγών που είναι καλυμμένοι από ένα μονωτικό περίβλημα. Οι αγωγοί του κάθε ζεύγους είναι συνεστραμμένοι μεταξύ τους σε ελικοειδή σχηματισμό. Αυτό έχει σαν αποτέλεσμα ο θόρυβος που παράγεται από τον ένα αγωγό του ζεύγους να αλληλοεξοντώνεται με αυτόν που παράγεται από τον άλλο αγωγό. Επίσης επιλέγοντας οι συστροφές του ενός ζεύγους να είναι διαφορετικές (να έχουν διαφορετικό μήκος έλικα συστροφής) με ενός διπλανού αντιμετωπίζονται και οι παρεμβολές μεταξύ γειτονικών ζευγών. Τέλος όλα τα ζεύγη περιβάλλονται από ένα εξωτερικό, σχετικά εύκαμπτο κάλυμμα για προστασία από τις φυσικές φθορές και τις εξωτερικές παρεμβολές.



Εικόνα 3.3: Η δομή του UTP



Εικόνα 3.4: UTP και RJ-45 connector

Τα UTP καλώδια είναι αρκετά φθηνά και εύκολα στην εγκατάστασή τους καθώς είναι αρκετά εύκαμπτα. Μπορούν να μεταδώσουν σήμα χωρίς ενίσχυση μέχρι και τα 100 μέτρα ενώ ανάλογα με την κατηγορία του καλωδίου αποδίδουν ταχύτητες μετάδοσης 10 Mbps, 100 Mbps και 1000 Mbps.

Η σύνδεση του καλωδίου στην τελική συσκευή γίνεται με ένα RJ-45 connector, στον οποίο τερματίζονται οι αγωγοί του καλωδίου στα δύο άκρα. Επίσης ανάλογα με τις συσκευές που συνδέονται στα δύο άκρα του καλωδίου, ο τερματισμός διαφέρει έτσι ώστε να είναι δυνατό οι δύο συσκευές να επικοινωνήσουν. Στον πίνακα 3.1 παρουσιάζονται οι τρεις τύποι UTP καλωδίου που υπάρχουν ανάλογα με τον τερματισμό στα δύο άκρα, καθώς και το είδος των συσκευών που διασυνδέονται με τον κάθε τύπο.

Τύπος UTP	**Συνδεσμολογία**	**Διασυνδεόμενες Συσκευές**
Straight-through	1 -------- 1 2 -------- 2 3 -------- 3 4 -------- 4 5 -------- 5 6 -------- 6 7 -------- 7 8 -------- 8	• PC με Hub • PC με Switch • Switch με Router • Hub με Router
Crossover	**1** -------- **3** **2** -------- **6** **3** -------- **1** 4 -------- 4 5 -------- 5 **6** -------- **2** 7 -------- 7 8 -------- 8	6. PC με PC 7. PC με Router 8. Switch με Hub 9. Hub με Hub 10. Switch με Switch 11. Router με Router
Rollover	1 -------- 8 2 -------- 7 3 -------- 6 4 -------- 5 5 -------- 4 6 -------- 3 7 -------- 2 8 -------- 1	• PC (COM) με PC (COM) • PC (COM) με Router (Console) Για την COM ή την Console θύρα συνήθως απαιτείται μετατροπέας από RJ-45 σε DB-9.

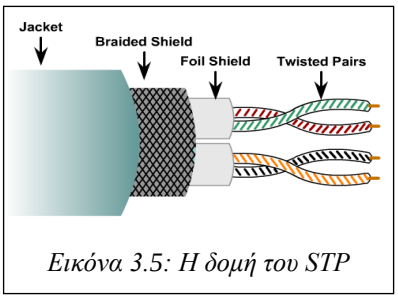
Πίνακας 3.1: Διάφοροι τύποι συνδέσεων UTP καλωδίου

Γενικά οι ακροδέκτες 1 και 2 χρησιμοποιούνται για την εκπομπή δεδομένων ενώ οι 3 και 6 για την λήψη. Έτσι αν πρέπει να συνδεθούν δύο PC's μεταξύ τους μέσω ενός UTP καλωδίου και τις κάρτες δικτύου τους θα πρέπει να χρησιμοποιηθεί ένα crossover UTP ώστε αυτά που στέλνει ο ένας να καταφθάνουν στα σωστά pins λήψης στον άλλον.

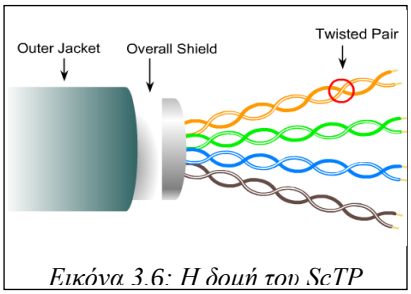
STP (Shielded Twisted Pair) και ScTP (Screened Twisted Pair)

Όπως το UTP έτσι και οι δύο αυτοί τύποι καλωδίων χρησιμοποιούν συνεστραμμένα ζεύγη μονωμένων αγωγών για την εξάλειψη της παραδιαφωνίας (crosstalk) και άλλων θορύβων. Σε αντίθεση όμως με το UTP, τα καλώδια αυτά έχουν επιπρόσθετη θωράκιση για ακόμα αποδοτικότερη αντιμετώπιση των θορύβων, κάτι που τα κάνει πιο αξιόπιστα από τα UTP αλλά συγχρόνως λιγότερο εύκαμπτα και ακριβότερα.

Στο **STP** το κάθε ζεύγος επίσης περιβάλλεται από ένα μεταλλικό κάλυμμα για καλύτερη προστασία θορύβου μεταξύ των ζευγών και επίσης όλα τα ζεύγη μαζί προστατεύονται από άλλο ένα μεταλλικό αγώγιμο πλέγμα για προστασία από εξωτερικές παρεμβολές. Το πλέγμα αυτό απορροφάει και γειώνει τις εξωτερικές παρεμβολές και ταυτόχρονα αποτρέπει την διαρροή ηλεκτρομαγνητικής ακτινοβολίας από το καλώδιο.



Εικόνα 3.5: Η δομή του STP



Εικόνα 3.6: Η δομή του ScTP

Το **ScTP** είναι μια ενδιάμεση στο UTP και STP υλοποίηση, καθώς είναι σαν το STP άλλα δεν περιλαμβάνει ξεχωριστή επικάλυψη για το κάθε ζεύγος. Και αυτό το καλώδιο είναι ακριβότερο από το UTP και πιο δύσκολο στην εγκατάστασή του.

Οπτικές Ίνες (Fiber Optics)

Οι οπτικές ίνες είναι το πιο συχνό μέσο διασύνδεσης για μεγάλες αποστάσεις, όπως στις WAN συνδέσεις, αλλά και σε δίκτυα κορμού (backbones) επιτρέποντας μεταδόσεις σε υψηλές ταχύτητες. Τα δεδομένα μεταδίδονται με την διάδοση φωτός μέσα από λεπτές ίνες γυαλιού ή πλαστικού. Φυσικά τα δεδομένα πριν μεταδοθούν μέσα από την ίνα θα πρέπει πρώτα ο πομπός να μετατρέψει τα ηλεκτρικά σήματα σε σήματα φωτός και ο δέκτης με την σειρά του θα πρέπει να μετατρέψει τα σήματα φωτός πίσω σε ηλεκτρικά σήματα για να αποκωδικοποιήσει τα δεδομένα.

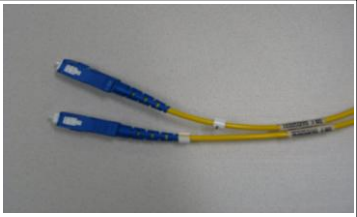
Όπως είναι γνωστό το φως είναι και αυτό ένα είδος ηλεκτρομαγνητικής ενέργειας όπως και τα μικροκύματα ή τα ραδιοκύματα. Επιπρόσθετα το φως έχει την ικανότητα να ταξιδεύει με ταχύτητα περίπου 300.000 χλμ/δευτερόλεπτο σε σωλήνα κενού αέρα (η λεγόμενη ταχύτητα του φωτός) και μάλιστα με πολύ μικρή εξασθένηση για μεγάλες αποστάσεις. Τα παραπάνω χαρακτηριστικά κάνουν το φως ένα ιδανικό μέσο για την γρήγορη μεταφορά δεδομένων μεταξύ δύο απομακρυσμένων σημείων.

Ένα καλώδιο οπτικής ίνας αποτελείται από τον **πυρήνα** (**core**) ο οποίος είναι συνήθως από γυαλί, την **επίστρωση** (**cladding**) που είναι φτιαγμένη από σιλικονούχο υλικό και το **εξωτερικό κάλυμμα** (**Coating**) που είναι συνήθως πλαστικό και προστατεύει το καλώδιο από εξωτερικές φθορές.

Όταν μία δέσμη φωτός ταξιδεύει μέσα στην γυάλινη ίνα μπορεί να φτάσει στην άλλη άκρη ακολουθώντας είτε μία ευθεία πορεία είτε με συνεχείς ανακλάσεις στα τοιχώματα του εσωτερικού της ίνας. Φυσικά για να συμβεί οποιοδήποτε από τα δύο η δέσμη φωτός θα πρέπει να εισαχθεί στην ίνα με τις κατάλληλες προϋποθέσεις και κυρίως με την σωστή γωνία έτσι ώστε οι πιθανές ανακλάσεις με τα τοιχώματα να μην προκαλέσουν απώλεια ενέργειας.

Υπάρχουν δύο κατηγορίες οπτικών ινών. Οι **single-mode** και οι **multimode**. Οι single-mode έχουν μικρότερη διάμετρο στο εσωτερικό (core) και επιτρέπουν μόνο μία διαδρομή που μπορεί να ακολουθήσει η δέσμη φωτός που συνήθως είναι υπεριώδες laser. Λόγω του σχεδιασμού αυτού οι single-mode προσφέρουν μεταδόσεις σε μεγαλύτερες ταχύτητες και αποστάσεις από ότι οι multimode οι οποίες έχουν μεγαλύτερης διαμέτρου core μέσα στον οποίο η φωτεινή δέσμη μπορεί να ακολουθήσει διάφορες πολλαπλές διαδρομές. Για τις single-mode οπτικές ίνες χρησιμοποιούνται ST connectors για την προσαρμογή σε μία συσκευή όπως ο router ενώ για τις multimode χρησιμοποιούνται οι SC connectors.

Εικόνα 3.7: Ο ST connector



Εικόνα 3.8: Ο SC connector

3.2 Ασύρματες Ζεύξεις

Σε αντίθεση με τα ενσύρματα δίκτυα όπου τα δεδομένα μεταφέρονται μέσω ενός καλωδίου με την μορφή ηλεκτρικών σημάτων, στα ασύρματα δίκτυα χρησιμοποιούνται πομποί και δέκτες και τα δεδομένα μεταφέρονται μέσω του αέρα. Ο πομπός μετατρέπει τα δεδομένα από ηλεκτρικά σήματα σε ραδιοκύματα τα οποία εκπέμπει από μία κεραία ενώ ο δέκτης αφού παραλάβει αυτά τα ραδιοκύματα τα μετατρέπει πάλι σε ηλεκτρικά σήματα για να μπορέσει να γίνει αποκωδικοποίηση των δεδομένων.

Πρότυπα

Σήμερα υπάρχουν συγκεκριμένα πρότυπα ορισμένα από την IEEE για την λειτουργία των ασύρματων δικτύων.

802.11

Αυτό είναι το πρώτο πρότυπο που δημιουργήθηκε το οποίο λειτουργεί στη μπάντα συχνοτήτων των 2.4 GHz και επιτυγχάνει ταχύτητες μέχρι και 2 Mbps.

802.11b

Αυτό το πρότυπο καθώς και όλα τα μεταγενέστερα του θεωρούνται πιστοποιημένα ως **Wi-Fi.** Λειτουργεί στην μπάντα συχνοτήτων των 2.4 GHz την οποία χωρίζει σε 14 διαφορετικά κανάλια. Το πρότυπο αυτό επιτυγχάνει θεωρητικές ταχύτητες μέχρι και 11 Mbps και είναι συμβατό με το απλό 802.11.

802.11a

Το πρότυπο αυτό επιτυγχάνει ταχύτητες που φτάνουν τα 54 Mbps και είναι λιγότερο ευάλωτο σε παρεμβολές. Λειτουργεί στην μπάντα των 5 GHz κάτι που το κάνει ασύμβατο με το 802.11b

και χρησιμοποιεί μέχρι και 8 διαφορετικά κανάλια.

802.11g

Το πρότυπο αυτό είναι μία βελτίωση του 802.11b καθώς λειτουργεί στην μπάντα των 2.4 GHz με 14 διαφορετικά κανάλια αλλά επιτυγχάνει ταχύτητες που φτάνουν τα 54 MHz. Το πρότυπο αυτό είναι συμβατό με το 802.11b αλλά όχι και με το 802.11a.

Ασύρματα Δίκτυα και Συσκευές

Οι συσκευές που χρησιμοποιούνται για την υλοποίηση ασύρματων δικτύων διαφέρουν από αυτές για τα ενσύρματα δίκτυα καθώς πρέπει να είναι ικανές να κάνουν μετατροπές μεταξύ ηλεκτρικών σημάτων και ραδιοκυμάτων και να μπορούν να τα εκπέμπουν και να τα λαμβάνουν μέσω του αέρα. Τα πιο απλά ασύρματα δίκτυα είναι τα **ad-hoc** δίκτυα. Αυτά αποτελούνται κυρίως από δύο υπολογιστές όπου ο ένας συνδέεται στον άλλο μέσω της ασύρματης κάρτας δικτύου που έχει εγκατεστημένη ο καθένας από αυτούς. Τέτοια δίκτυα σπάνια υλοποιούνται σήμερα καθώς δεν είναι επεκτάσιμα, προσφέρουν ελάχιστη ασφάλεια και μικρές ταχύτητες, ενώ η επιτυχής λειτουργία ενός τέτοιου δικτύου προϋποθέτει να υπάρχει συμβατότητα μεταξύ των κατασκευαστών των δύο καρτών.

Η πιο συνήθης τοπολογία ενός ασύρματου δικτύου απαλλαγμένη από τα προβλήματα των 'ad-hoc' δικτύων είναι αυτή με την χρήση ενός ή περισσοτέρων **access points**. Το access point είναι εφοδιασμένο με μία ή περισσότερες κεραίες και λειτουργεί σαν ένα hub (με περισσότερες όμως λειτουργίες) για το ασύρματο LAN. Ένας ή περισσότεροι υπολογιστές με την χρήση ασύρματων NICs συνδέονται στο access point παίρνοντας έτσι μέρος στο ασύρματο LAN.

Εικόνα 3.9: Ασύρματη κάρτα δικτύου

Για να μπορέσει κάποιος υπολογιστής να συνδεθεί στο ασύρματο LAN πρέπει πρώτα να εντοπίσει αν υπάρχει κάποιο access point που προσφέρει αυτή τη δυνατότητα. Η διαδικασία εντοπισμού access point ονομάζεται **scanning** και μπορεί να είναι είτε **active** είτε **passive**. Στο **active scanning** ο υπολογιστής εκπέμπει μία αίτηση για συμμετοχή σε κάποιο ασύρματο δίκτυο. Σε αυτή την αίτηση περιλαμβάνει και την ταυτότητα (**SSID – Service Set Identifier**) του ζητούμενου access point. Εάν το ζητούμενο access point είναι διαθέσιμο τότε απαντάει σε αυτή την αίτηση και αν υπάρχουν οι σωστές ρυθμίσεις τότε ο υπολογιστής συνδέεται στο ασύρματο δίκτυο.

Με το **passive scanning** ο υπολογιστής 'ακούει' μέσω της ασύρματης κάρτας του για πιθανά **beacons.** Αυτά είναι κάποια πακέτα που εκπέμπονται από τα access points ανά τακτά χρονικά διαστήματα και περιέχουν κάποιες πληροφορίες, όπως το SSID, για το διαθέσιμο ασύρματο δίκτυο. Μόλις λάβει αυτή την πληροφορία ο υπολογιστής μπορεί να κάνει μία αίτηση για να πραγματοποιήσει την σύνδεση.

Εικόνα 3.10: Wireless access point

Ένα access point μπορεί να έχει εμβέλεια μέχρι και 150 μέτρα δημιουργώντας έτσι ένα **cell.** Περισσότερα του ενός access point είναι δυνατό να δημιουργήσουν μια ομάδα από cells επιτρέποντας έτσι την εξάπλωση του ασύρματου δικτύου δίνοντας έτσι και την δυνατότητα για μετακίνηση του χρήστη (roaming) από cell σε cell χωρίς να χάνεται ή σύνδεση με το ασύρματο δίκτυο.

Δύο σημαντικά θέματα που εμποδίζουν την ευρεία εξάπλωση των ασύρματων δικτύων είναι η αξιοπιστία και η ασφάλεια. Όσο αναφορά το πρώτο τα ραδιοκύματα επηρεάζονται από διάφορες πηγές που προκαλούν παρεμβολές όπως οικιακές συσκευές (φούρνος μικροκυμάτων), ασύρματα οικιακά τηλέφωνα, από φυσικά εμπόδια όπως τοίχους και δέντρα ή ακόμα και από καιρικά φαινόμενα όπως ομίχλη ή εκτεταμένη υγρασία και κεραυνούς όπου καθώς αλλάζει η ατμόσφαιρα μπορούν να αλλάξουν και οι διαδρομές που ακολουθούν τα ραδιοκύματα.

Το ζήτημα της ασφάλειας είναι επίσης σημαντικό καθώς πλέον τα δεδομένα δεν μεταδίδονται μέσα από κάποιο καλώδιο όπου υπάρχει σχετικός έλεγχος πρόσβασης σε αυτό, άλλα από τον αέρα που είναι προσβάσιμος από όλους. Έτσι χωρίς τις κατάλληλες προφυλάξεις μπορεί κάποιος χωρίς εξουσιοδότηση να έχει πρόσβαση στα μεταδιδόμενα σήματα και κατ' επέκταση στα δεδομένα που αυτά μεταφέρουν. Τεχνολογίες όπως το WEP και το μεταγενέστερο WPA, το MAC filtering καθώς και τα VPNs και οι authentication servers είναι κάποιες από τις πιο σημαντικές τεχνικές ασφάλισης των ασύρματων δικτύων που συνήθως χρησιμοποιούνται σε συνδυασμό μεταξύ τους.

4. Έλεγχος καλωδίωσης και τύποι ελέγχων

Η έλεγχος σφαλμάτων σε μία εγκατάστασή δικτύου ξεκινάει στις περισσότερες των περιπτώσεων από το κατώτερο επίπεδο που είναι η φυσικές συνδέσεις. Συνήθως προβλήματα που έχουν να κάνουν με την φυσική καλωδίωση είναι δύσκολο να εντοπιστούν καθώς τα καλώδια διέρχονται από σημεία που είναι δύσκολο να ελεγχθούν. Για το λόγο αυτό, ο έλεγχος των καλωδίων πριν την εγκατάστασή τους καθώς και του χώρου που αυτά διέρχονται είναι ένα πολύ σημαντικό και πρωταρχικό βήμα για στήσιμο ενός δικτύου.

Όσο αναφορά την ορθή λειτουργία ενός καλωδίου πρέπει τα δεδομένα που στέλνει ο πομπός από την μία άκρη να διαδοθούν στην άλλη άκρη όπου ο δέκτης θα μπορέσει σε πρώτη φάση να τα λάβει και στη συνέχεια να τα αποκωδικοποιήσει σωστά. Τα δεδομένα είναι μία ακολουθία από bits, όπου το κάθε bit αναπαριστάται στα καλώδια χαλκού σαν ηλεκτρική τάση και στις οπτικές ίνες σαν ένταση φωτός.

Η **εξασθένηση** του σήματος (**attenuation**) είναι η μείωση της έντασης του σήματος καθώς αυτό μεταδίδεται κατά μήκος του καλωδίου και έχει άμεση σχέση τόσο με το μήκος του καλωδίου όσο και με την υψηλή συχνότητα μετάδοσης του σήματος. Υπάρχουν διάφοροι παράγοντες που προκαλούν την εξασθένηση του σήματος. Κατά πρώτον η φυσική αντίσταση των στοιχείων του καλωδίου μετατρέπει ένα μέρος της ηλεκτρικής ενέργειας σε θερμότητα. Επίσης ένα μέρος της ενέργειας του σήματος διαρρέει από τα τοιχώματα του καλωδίου και γιαυτό κάποια καλώδια χρησιμοποιούν ενισχυμένες μονωτικές επιστρώσεις που καλύπτουν τους εσωτερικούς αγωγούς. Τέλος κάθε πρόσθετος connector μεταξύ δύο καλωδίων προκαλεί απώλεια ενέργειας λόγω της διαφορετικής εμπέδησης η οποία προκαλεί μέρος του σήματος να ανακλάται πίσω στον πομπό.

Ο **θόρυβος** (**noise**) είναι ηλεκτρική ενέργεια από εξωτερικές πηγές που παρεμβάλλεται στο κανονικό σήμα που μεταδίδεται μέσα από το καλώδιο και προκαλεί σύγχυση στην σωστή αποκωδικοποίηση του σήματος από τον δέκτη. Ο θόρυβος μπορεί να προκληθεί από γειτονικά καλώδια ή γεννήτριες ρεύματος ή ακόμα και από πηγές φωτός. Η σωστή απομόνωση των καλωδίων και η καλή εξωτερική θωράκισή τους είναι απαραίτητα για την αντιμετώπιση των θορύβων.

Η **παραδιαφωνία** (**crosstalk**) είναι ένα είδος θορύβου και έχει να κάνει με τις παρεμβολές που προκαλούνται από ηλεκτρικά σήματα που ανήκουν σε γειτονικούς αγωγούς του καλωδίου. Αυτό γιατί οι αγωγοί λειτουργούν σαν κεραίες και 'τραβάνε' την ηλεκτρομαγνητική ενέργεια που εκπέμπεται κατά την μετάδοση σήματος από διπλανούς αγωγούς. Σε υψηλές συχνότητες το crosstalk είναι πιο έντονο. Το φαινόμενο του crosstalk είναι σύνηθες στα καλώδια χαλκού που αποτελούνται από πολλούς αγωγούς (UTP, STP) και αντιμετωπίζεται επιτυχώς με την συστροφή των αγωγών ανά ζεύγη. Με την συστροφή δεν εξαφανίζεται το crosstalk, απλά επειδή είναι το ίδιο και στους δύο αγωγούς, ο θόρυβος που προκαλείται μπορεί να εντοπιστεί από τον δέκτη και να αντιμετωπιστεί. Καθώς όμως περισσότερα του ενός ζεύγους αγωγών είναι πιθανό να υπάρχουν σε ένα καλώδιο, το crosstalk μπορεί να υπάρχει και μεταξύ γειτονικών ζευγών. Σε αυτή την περίπτωση αντιμετωπίζεται με την χρήση διαφορετικού αριθμού συστροφών ανά ζεύγος, δηλαδή έχουν διαφορετικό μήκος έλικα συστροφής.

Σε ένα UTP καλώδιο υπάρχουν διάφοροι έλεγχοι που πρέπει να γίνουν για να επιβεβαιώσουν την σωστή λειτουργία του. Μερικοί από τους πιο σημαντικούς ελέγχους είναι:

Wire Map

Έχει να κάνει με τον σωστό τερματισμό του UTP καλωδίου στα δύο άκρα. Δηλαδή ότι και στους δύο ακραίους RJ-45 connectors, όλοι οι αγωγοί έχουν τοποθετηθεί στα σωστά pins. Κατά τον έλεγχο αυτό μπορεί να βρεθεί ότι υπάρχει ένα **ανοιχτό κύκλωμα** (**open circuit**), δηλαδή ότι ένας αγωγός είναι συνδεδεμένος μόνο στη μία άκρη, ένα **βραχυκύκλωμα** (**short circuit**) όπου ένας αγωγός έχει επαφή με κάποιον γειτονικό του, μία **αντιστροφή ζευγών** (**reserved pairs**) όπου ένα ζεύγος έχει συνδεθεί σωστά στη μία άκρη αλλά στη θέση κάποιου άλλου στην άλλη, και τέλος μπορεί να υπάρχει ένα **split-pair** όπου ένας αγωγός από κάποιο ζεύγος έχει συνδεθεί με αγωγό ενός άλλου ζεύγους.

Return loss

Αυτή είναι η μέτρηση του επιστρεφόμενου σήματος, το οποίο εκφράζει την εξασθένηση του σήματος λόγω απώλειας ενέργειας που προκύπτει από την ανάκλαση του σήματος σε υλικά με διαφορετική εμπέδηση όπως διάφοροι connectors.

Propagation Delay

Είναι η καθυστέρηση που παρουσιάζεται κατά την διάδοση του σήματος από το ένα άκρο του καλωδίου στο άλλο. Η καθυστέρηση αυτή εξαρτάται κυρίως από το μήκος του καλωδίου καθώς και από την κατασκευή του καλωδίου και τις διάφορες ηλεκτρικές ιδιότητες που έχει.

Crosstalk (Παραδιαφωνία)
Ο τερματισμός του καλωδίου πρέπει να γίνει σωστά και στα δύο άκρα για αποφυγή του φαινομένου crosstalk. Το καλώδιο πρέπει να τερματιστεί με σωστό τρόπο στον RJ-45 connector ώστε να μην χαλάσει η συστροφή των αγωγών.

Όλοι οι παραπάνω έλεγχοι μπορούν να γίνουν με ειδική συσκευή προορισμένη για αυτή την δουλειά, τον **cable tester**. Η συσκευή αυτή προσαρμόζεται στα δύο άκρα του καλωδίου και δίνει αναλυτικές μετρήσεις που αποκαλύπτουν κάποιο από τα παραπάνω φαινόμενα και βοηθούν στον εντοπισμό του προβλήματος.

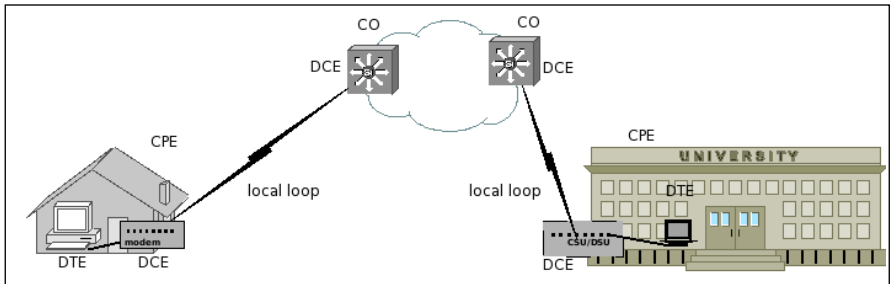
Εικόνα 4.1: Ο cable tester

Όσο αναφορά τις οπτικές ίνες, αυτές είναι σε γενικές γραμμές λιγότερο επιρρεπείς στον θόρυβο αλλά και στην εξασθένηση του σήματος από ότι τα καλώδια χαλκού. Παρόλα αυτά θέλει πολύ προσοχή ο τερματισμός τους καθώς και η ένωση δύο οπτικών ινών. Για αυτή την δουλεία απαιτείται ειδικός μηχανισμός καθώς ο γυάλινος πυρήνας των δύο καλωδίων πρέπει να θερμανθεί και να κολληθεί με απόλυτη ευθυγράμμιση στο σημείο τομής των δύο καλωδίων.
Η συσκευή που ελέγχει ασυνέχειες και διάφορες ανωμαλίες σε ένα καλώδιο οπτικής ίνας ονομάζεται **Optical Time Domain Reflectometer**.

Εικόνα 4.2: Optical Domain Reflectrometer

5. Καλωδίωση WANs: συνδέσεις Serial, BRI, DSL, cable, console.

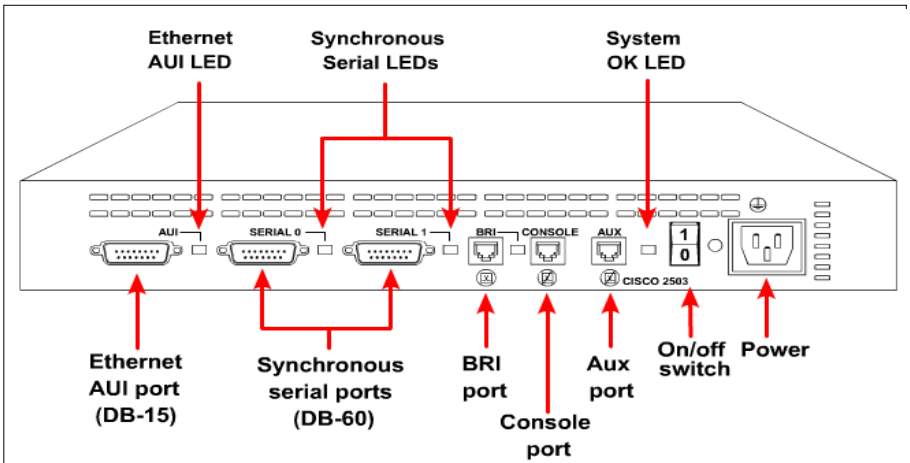
Τα **WANs** (**Wide Area Networks**) είναι δίκτυα που εκτείνονται σε ευρεία περιοχή και στην ουσία συνδέουν μεταξύ τους LANs σχηματίζοντας έτσι ένα δίκτυο από δίκτυα. Σε αντίθεση με τις LAN, οι WAN συνδέσεις συνήθως απαιτούν μία εταιρεία ή ένας οργανισμός να εγγραφεί στην υπηρεσία που προσφέρει κάποιος πάροχος/φορέας, ώστε να μπορέσουν να μεταφέρουν δεδομένα μέσα από το WAN δίκτυο του φορέα. Οι WAN γραμμές που προσφέρει κάποιος φορέας επιτρέπουν την σύνδεση με το Internet, την διασύνδεση απομακρυσμένων σημείων ενός οργανισμού, την σύνδεση με απομακρυσμένα σημεία άλλων οργανισμών και την διασύνδεση απομακρυσμένων χρηστών. Οι WAN συνδέσεις γενικά χρησιμοποιούνται για την μεταφορά διαφόρων τύπων δικτυακής κίνησης όπως φωνή, δεδομένα και βίντεο, ενώ οι υπηρεσίες τηλεφώνου και δεδομένων είναι οι πιο κοινές.



Εικόνα 5.1: Τυπική σύνδεση WAN

Οι συσκευές που βρίσκονται στις εγκαταστάσεις του πελάτη ονομάζονται **CPE** (**Customer Premises Equipment**) και συνδέονται στο άλλο άκρο με κάποια συσκευή στις εγκαταστάσεις του φορέα, στο **CO** (**Central Office**). Αυτή η σύνδεση μεταξύ των δύο σημείων είναι το λεγόμενο l**ocal loop**. Στην πλευρά του πελάτη μία ή περισσότερες **DTE** (**Data Terminal Equipment**) συσκευές, που μπορεί να είναι ένα PC ή ακόμα και ένας router, στέλνουν τα προς μετάδοση δεδομένα σε μία συσκευή **DCE** (**Data Curcuit-Terminating Equipment**) η οποία μετατρέπει τα δεδομένα σε μορφή κατάλληλη για να μεταδοθούν μέσα από το local loop. Στην ουσία το DCE προσφέρει ένα interface για το DTE στην WAN γραμμή και συνήθως είναι ή ένα **modem** (για αναλογικές γραμμές) ή ένα **CSU/DSU** (για ψηφιακές γραμμές). Οι DTE και DCE συσκευές συνδέονται συνήθως μεταξύ τους με ένα σειριακό καλώδιο και καθώς τα δεδομένα στέλνονται σειριακά ένα ένα bit πρέπει να υπάρχει κάποιος συγχρονισμός μεταξύ των δύο συσκευών που συνήθως δίνεται από το DCE.

Οι συσκευές που κυρίως χρησιμοποιούνται για την υλοποίηση των WANs είναι οι routers. Οι routers θα πρέπει να έχουν τα κατάλληλα interfaces ώστε να μπορούν σε αυτούς να συνδεθούν τόσο LANs όσο και WANs και συνήθως προσφέρουν μια ποικιλία από interfaces για να μπορέσουν να υποστηρίξουν την τεχνολογία καλωδίωσης που θα χρησιμοποιηθεί.



Εικόνα 5.2: Το πίσω μέρος ενός router

Σειριακές WAN συνδέσεις

Τα είδη των WAN συνδέσεων ποικίλουν ανάλογα με την απόσταση της σύνδεσης, την ταχύτητα και τον τύπο των δεδομένων που πρέπει να μεταφερθούν. Οι απλές σειριακές συνδέσεις ξεκινούν από τα 24 Kbps για τις **dial-up** γραμμές που χρησιμοποιούν το κοινό τηλεφωνικό δίκτυο για την μετάδοση δεδομένων σε αναλογική μορφή. Τον ρόλο του DCE παίζει το modem το οποίο κατά την αποστολή δεδομένων μετατρέπει τα σήματα από ψηφιακή σε αναλογική μορφή για να μεταδοθούν μέσα από το local loop, και αντίστροφα κατά την λήψη μετατρέπει τα σήματα από αναλογική σε ψηφιακή μορφή ώστε να τα λάβει σωστά η DTE συσκευή (πχ. ένα PC).

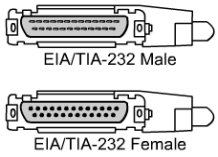
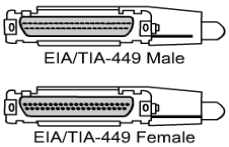
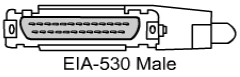
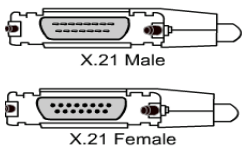
Οι **αφιερωμένες γραμμές** είναι δεσμευμένα κυκλώματα που προσφέρονται από τον πάροχο στον πελάτη και προσφέρουν σταθερό bandwidth και επικοινωνία χωρίς καθυστέρηση. Οι ταχύτητες (πίνακας 5.2) μπορεί να είναι στα 1,544 Mbps στις **T1** γραμμές (Αμερικάνικο πρότυπο) ή τα 2,048 Mbps στις **E1** γραμμές (Ευρωπαϊκό πρότυπο) ενώ οι πιο ακριβές αφιερωμένες γραμμές μπορεί να φτάνουν και τις ταχύτητες των 2,5 Gbps.

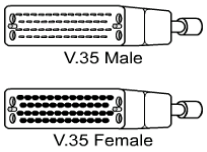
Τύπος Γραμμής	Ταχύτητα
54	56 Kbps
64	64 Kbps
T1	1,544 Mbps
E1	2,048 Mbps
E3	34,064 Mbps
J1	2,048 Mbps
T3	44,736 Mbps
OC-1	51,84 Mbps
OC-3	155,54 Mbps

OC-9	466,56 Mbps
OC-12	622,08 Mbps
OC-18	933,12 Mbps
OC-24	1244,16 Mbps
OC-36	1866,24 Mbps
OC-48	2488,32 Mbps

Πίνακας 5. 1: Τύποι αφιερωμένων γραμμών και bandwidth

Τα πρότυπα που παρουσιάζονται στον πίνακα 5.2 αφορούν την φυσική σύνδεση και το μηχανικό μέρος αυτής που έχει να κάνει με την σηματοδοσία, τον συγχρονισμό και γενικά τον τρόπο με τον οποίο τα bits θα μεταδοθούν πάνω από το φυσικό μέσο. Σε πιο υψηλό επίπεδο, στο Data Link Layer του OSI, υπάρχουν διάφορα πρωτόκολλα που ασχολούνται με την αποστολή των δεδομένων σε frames, τον έλεγχο λαθών και τον έλεγχο ροής των δεδομένων. Μερικά από τα πρωτόκολλα αυτά είναι τα HDLC, PPP, Frame Relay, X.25, ATM.

WAN Standard	**Connectors**	**Περιγραφή**
EIA/TIA-232		Επιτρέπει σχετικά μικρές ταχύτητες μέχρι 64 Kbps σε μικρές αποστάσεις. Χρησιμοποιεί έναν 25-pin D connector ενώ παλιότερα ήταν γνωστό σαν RS-232.
EIA/TIA-449		Είναι μία πιο γρήγορη έκδοση του EIA/TIA-232 που επιτρέπει ταχύτητες μέχρι και 2 Mbps ενώ μπορεί να χρησιμοποιηθεί και για συνδέσεις μεγαλύτερων αποστάσεων. Χρησιμοποιεί έναν 36 pin D connector. Είναι επίσης γνωστό ως RS-422 και RS-423.
EIA-530		Παρόμοιο με το EIA/TIA-449.
EIA-613		Το HSSI (High Speed Serial Interface) χρησιμοποιεί έναν 60 pin connector και επιτρέπει ταχύτητες μέχρι και 52 Mbps.
X.21		Είναι πρότυπο της ITU-T και χρησιμοποιεί έναν 15 pin D connector για σύγχρονες ψηφιακές συνδέσεις.

V.35		Επίσης πρότυπο της ITU-T για σύγχρονες συνδέσεις μέχρι 48 Kbps. Χρησιμοποιεί έναν 34 pin connector.

Πίνακας 5.2: πρότυπα WAN

ISDN (Intergrated Services Digital Network)

Οι **ISDN** είναι ένα είδος dial-on-demand ψηφιακές συνδέσεις οι οποίες προσφέρονται σε δύο τύπους, τις BRI και τις PRI. Οι **BRI** (**Basic Rate Interface**) ISDN γραμμές αποτελούνται από δύο B κανάλια των 64 Kbps το καθένα, που χρησιμοποιούνται για την αποστολή δεδομένων και ένα D κανάλι των 16 Kbps, που χρησιμοποιείται για σήματα ελέγχου της γραμμής. Οι **PRI** (**Primary Rate Interface**) ISDN γραμμές αποτελούνται είτε από 23 B κανάλια των 64 Kbps και ένα D κανάλι των 64 Kbps για τα Αμερικάνικα πρότυπα, είτε από 30 B κανάλια των 64 Kbps και ένα D κανάλι των 64 Kbps για τα Ευρωπαϊκά πρότυπα. Η σύνδεση μιας ISDN γραμμής στην πλευρά του πελάτη, σύμφωνα με τα Ευρωπαϊκά πρότυπα, γίνεται με την σύνδεση από το **BRI S/T** interface του router σε μία **NT1** συσκευή η οποία παρέχεται και είναι υπό την επίβλεψη του παρόχου. Λειτουργία αυτής της συσκευής είναι να μετατρέψει την τετρασύρματη γραμμή σε δυσύρματη ώστε να γίνει η σύνδεση με το local loop. Στην περίπτωση που ο router δεν έχει BRI interface τότε απαιτείται ένας **Terminal Adapter** (TA) ανάμεσα στις δύο συσκευές. Σε αυτή την περίπτωση η σύνδεση του router με τον TA γίνεται με σειριακό καλώδιο (EIA/TIA-232, V.35, X.21).

DSL (Digital Subscriber Line)

Το **DSL** που έχει διαδοθεί ευρέως τα τελευταία χρόνια χρησιμοποιεί την υπάρχουσα υποδομή του τηλεφωνικού δικτύου για να προσφέρει broadband ψηφιακές συνδέσεις που φτάνουν ταχύτητες υψηλότερες και από τις κλασσικές E1/T1 γραμμές. Υπάρχουν δύο κύριες κατηγορίες DSL συνδέσεων οι **ADSL** και οι **SDSL**. Οι πρώτες είναι ασύμμετρες με την έννοια ότι επιτρέπουν διαφορετικές ταχύτητες για upload και download. Με τα σημερινά δεδομένα μία ADSL σύνδεση μπορεί να προσφέρει μέχρι και 24 Mbps για download και 2 Mbps για upload. Οι SDSL είναι συμμετρικές συνδέσεις που προσφέρουν ίδιες ταχύτητες για upload και download που δεν ξεπερνούν όμως τα 2 Mbps. Η σύνδεση μιας DSL γραμμής γίνεται με κλασσικό τηλεφωνικό καλώδιο όπου η μία του άκρη συνδέεται στο DSL port του router με RJ-11 connector και η άλλη άκρη του στην τηλεφωνική πρίζα πάλι με RJ-11 connector. Στην πλευρά του παρόχου πολλαπλές DSL γραμμές από διάφορους πελάτες συγκεντρώνονται σε ένα **DSLAM** όπου γίνεται πολυπλεξία σε μία μεγάλης χωρητικότητας γραμμή στο εσωτερικό δίκτυο του παρόχου.

Cable

Η **καλωδιακές συνδέσεις** προσφέρονται από κάποιο πάροχο καλωδιακής τηλεόρασης και μεταφέρουν δεδομένα μέσα από το κλασσικό σύστημα της κεραίας και του ομοαξονικού καλωδίου της τηλεόρασης. Καλωδιακές συνδέσεις μπορούν να φτάσουν ταχύτητες παρόμοιες ή ακόμα και μεγαλύτερες από το DSL (μέχρι και 40 Mbps). Για την σύνδεση μιας cable γραμμής το ομοαξονικό καλώδιο που έρχεται από την κεραία συνδέεται σε έναν **F-connector** στον router ενώ υπάρχει και ένας **splitter** για τον διαχωρισμό του σήματος τηλεόρασης από τα δεδομένα του δικτύου. Οι καλωδιακές

συνδέσεις είναι σπάνιες στην Ελλάδα.

Συνδέσεις κονσόλας (console connections)

Η διαχείριση ενός router (και άλλων δικτυακών συσκευών) μπορεί να γίνεται είτε τοπικά είτε απομακρυσμένα. Όμως η αρχική εγκατάσταση καθώς και άλλες συγκεκριμένες λειτουργίες σε έναν router μπορούν να γίνουν μόνο τοπικά με σύνδεση κονσόλας. Η σύνδεση αυτή γίνεται μεταξύ της σειριακής πόρτας (COM) ενός τερματικού (πχ. ένα PC) με την console port του router χρησιμοποιώντας ένα **rollover** καλώδιο. Το καλώδιο αυτό συνήθως έχει στις άκρες του RJ-45 connectors και για την σύνδεση στην COM πόρτα του PC απαιτείται ένας μετατροπέας από RJ-45 σε DB-9 ή DB-25 connector.

Το λογισμικό που απαιτείται για την σύνδεση αυτή είναι ένας **προσομοιωτής τερματικού** (**terminal emulation**) που πρέπει να είναι εγκατεστημένος στο PC. Τέτοιου είδους εφαρμογές είναι το **Hyper Terminal** για Windows ή το **minicom** για Linux.

Αφού γίνει η φυσική σύνδεση μεταξύ των δύο συσκευών, πρέπει να γίνει έναρξη του προγράμματος και μέσα από αυτό να δοθούν οι παρακάτω ρυθμίσεις για την COM πόρτα:

2. Bits/sec: 9600 bps
3. Data bits: 8 data bits
4. Parity: no parity
5. Stop Bits: 1 stop bit
6. Flow Control: no flow control

Αν η σύνδεση είναι επιτυχής τότε στην οθόνη του υπολογιστή θα εμφανίζεται το output του router.

Η **AUX** πόρτα στον router μπορεί να χρησιμοποιηθεί για τον ίδιο σκοπό με την console πόρτα, μόνο που αφορά απομακρυσμένες συνδέσεις μέσω modem.

6. Εισαγωγή στο TCP / IP
6.1 Τρόπος λειτουργίας του TCP / IP

Το κλειδί για την κατανόηση λειτουργίας των δικτύων που βασίζονται στο μοντέλο αυτό είναι η ανάλυση των πρωτοκόλλων των δύο ενδιάμεσων στρωμάτων, συγκεκριμένα των Transport και Internet.

Transport Layer

Το στρώμα αυτό είναι υπεύθυνο για τη λογική σύνδεση μεταξύ δύο συσκευών. Επιτρέπει τη δυνατότητα αξιόπιστης σύνδεσης και ελέγχου ροής. Σε κάθε σύνδεση χρησιμοποιείται ένα από τα δυο διαθέσιμα πρωτόκολλα TCP ή UDP τα οποία θα αναλυθούν παρακάτω. Η πληροφορία σε αυτό το επίπεδο χωρίζεται σε segments

TCP (Transmission Control Protocol)

Χρησιμοποιείται στην περίπτωση που απαιτούμε αξιόπιστη σύνδεση μεταξύ δυο συσκευών. Φυσικά ένας υπολογιστής (ή άλλη συσκευή) μπορεί να επικοινωνεί ταυτόχρονα με πολλές άλλες. Για τη διαφοροποίηση μεταξύ των συνδέσεων χρησιμοποιούνται οι θύρες (ports). Μία τοπική εφαρμογή

χρησιμοποιεί μια τοπική θύρα (ένας αριθμός από 1 ως 65535) και συνδέεται με μια απομακρυσμένη θύρα που αντιστοιχεί στην εφαρμογή της απομακρυσμένης συσκευής. Έτσι εξασφαλίζεται η μοναδικότητα και διαχωρισμός ταυτόχρονων συνδέσεων. Οι θύρες από 1 ως 1023 έχουν ειδική σημασία και θεωρούνται «ευρέως γνωστές» (well known ports). Σχετίζονται άμεσα με συγκεκριμένες εφαρμογές. Πχ, ένας υπολογιστής που τρέχει εφαρμογή ftp server «ακούει» στη θύρα 21. Περιμένει δηλαδή άλλες συσκευές να ξεκινήσουν επικοινωνία με αυτόν μέσω της συγκεκριμένης θύρας. Όταν ένας υπολογιστής που τρέχει ftp client προσπαθήσει να επικοινωνήσει με τον ftp server, το λειτουργικό του σύστημα (στον client) θα επιλέξει μια τυχαία αχρησιμοποίητη θύρα (από τις μη γνωστές) τοπικά και τη θύρα 21 ως προορισμό. Επομένως όταν το segment φτάσει στον προορισμό, θα μπορεί παραλήπτης να αναγνωρίσει ότι πρόκειται για επικοινωνία που αφορά την εφαρμογή ftp server. Όπως είναι προφανές, οι θύρες αποτελούν και το συνδετικό κρίκο μεταξύ του Transmission και του Application Layer.

Η αξιοπιστία των συνδέσεων εξασφαλίζεται μέσω μιας διαδικασίας αρχικοποίησης συνδέσεων που ονομάζεται τριπλή χειραψία (3 way handshake). Εξασφαλίζει τη δυνατότητα αναγνώρισης χαμένων segments αλλά και αναδιάταξης αυτών σε περίπτωση που παραληφθούν με λανθασμένη σειρά. Η διαδικασία συνοπτικά είναι η εξής:

1. Η πηγή (η συσκευή που ξεκινάει τη σύνδεση) στέλνει το SYN, ένα ειδικό segment συγχρονισμού με έναν αρχικό αριθμό ακολουθίας (sequence number)
2. Όταν αυτό φτάσει στον προορισμό, η απομακρυσμένη συσκευή στέλνει το SYN/ACK segment. Αυτό περιλαμβάνει αναγνώριση ότι έλαβε το πρώτο segment καθώς και ένα καινούριο SYN με το δικό του sequence number.
3. Η πρώτη συσκευή στέλνει αναγνώριση (ACK) ότι έλαβε το SYN segment.

Παράδειγμα:
1. Πρώτη Συσκευή: Στέλνει SYN με sequence number 1
2. Δεύτερη συσκευή: Στέλνει SYN/ACK με sequence number 10 και αναγνώριση (acknowledgement) 2 (η αναγνώριση είναι το sequence number + 1)
3. Η πρώτη συσκευή στέλνει segment με sequence number 2 (το πρώτο που είχε στείλει ήταν 1) το οποίο περιέχει acknowledgment 11 (αφού η απομακρυσμένη συσκευή ξεκίνησε από 10).

Ο έλεγχος ροής επιτυγχάνεται με το σύστημα windowing. Αν κάθε segment απαιτούσε αναγνώριση οι συνδέσεις θα ήταν πολύ αργές. Για να αυξήσουμε την αποδοτικότητα μπορούμε να αρκεστούμε σε αναγνώριση κάθε x αριθμό segments, (x ο αριθμός segments μεταξύ αναγνωρίσεων, το window size). Αν χαθεί όμως κάποιο segment θα πρέπει να ξανασταλθούν περισσότερα segments (όλα μέχρι την τελευταία αναγνώριση). Το βέλτιστο window size εξαρτάται από συνθήκες όπως η ποιότητα της σύνδεσης και η κίνηση του δικτύου. Το μέγεθος αυτό είναι μεταβλητό κατά τη διάρκεια της σύνδεσης και προσαρμόζεται αυτόματα (το λεγόμενο sliding window).

UDP (User Datagram Protocol)

Εναλλακτικά, αντί για TCP μπορεί να χρησιμοποιηθεί το UDP. Το UDP δεν περιλαμβάνει διαδικασία αρχικοποίησης σύνδεσης, ούτε καμία διαδικασία αναγνώρισης παραλαβής segments. Η μόνη πληροφορία που περιλαμβάνει είναι οι θύρες (source & destination ports), το μέγεθος του segment και ένα checksum για την αναγνώριση λαθών στη μετάδοση. Αυτό το κάνει πιο αποδοτικό σε σχέση με το TCP. Είναι κατάλληλο για τη μεταφορά πληροφορίας που το κόστος (σε απόδοση και ταχύτητα) της αξιοπιστίας της σύνδεσης ξεπερνά τα οφέλη. Πχ σε μετάδοση streaming video ή audio (internet radio

κλπ) ή για συνδέσεις σε πραγματικό χρόνο (online games). Η απώλεια segments θα προκαλέσει κάποιες επιπλοκές αλλά η σύνδεση σε λογική ταχύτητα θα ήταν ασύμφορη έως αδύνατη με TCP. Σε άλλες περιπτώσεις (πχ DNS queries), το μέγεθος της πληροφορίας είναι τόσο μικρό που η αρχικοποίηση σύνδεσης είναι υπερβολή. Η χρήση UDP δεν σημαίνει απαραίτητα ότι η σύνδεση δεν είναι αξιόπιστη, ούτε ότι σύστημα αξιοπιστίας είναι αδύνατον να υλοποιηθεί. Απλώς οποιαδήποτε διαδικασία (πχ acknowledgements) θα πρέπει, αν χρειαστεί, να υλοποιηθεί στο application layer.

Internet Layer

Εδώ γίνεται η δρομολόγηση πακέτων μεταξύ απομακρυσμένων συσκευών με βάση λογικές διευθύνσεις. Το κυριότερο πρωτόκολλο είναι το IP. Άλλα πρωτόκολλα που ανήκουν στο ίδιο στρώμα είναι το ICMP, ARP και RARP. Η πληροφορία εδώ χωρίζεται σε packets

IP (Internet Protocol)

Το IP προσφέρει αναξιόπιστη σύνδεση μεταξύ συσκευών. Οποιαδήποτε αξιοπιστία στη σύνδεση παρέχεται από τα ανώτερα επίπεδα. Τα πακέτα IP μεταφέρουν τα ενθυλακωμένα TCP/UDP segments ή ενδεχομένως αλλά πακέτα πρωτοκόλλων που επίσης ανήκουν στο internet layer αλλά λειτουργούν πάνω από το IP, όπως είναι το ICMP. Το ίδιο το IP πρέπει να γνωρίζει τον τύπο του πρωτοκόλλου των ανώτερων στρωμάτων που εξυπηρετεί. Υπάρχει ειδικό πεδίο στο IP Header για αυτό το σκοπό.
Τα IP πακέτα έχουν περιορισμένο χρόνο ζωής. Το πεδίο TTL (Time to Live) περιλαμβάνει έναν αριθμό που μειώνεται κάθε φορά που το πακέτο περνά από ένα δρομολογητή μέχρι να φτάσει στο 0, όπου δεν δρομολογείται πλέον. Άλλα σημαντικά πεδία είναι οι IP διευθύνσεις (source και destination), το μέγεθος του συνολικού πακέτου και του header και η έκδοση του IP (4 ή 6).

Η τρέχουσα έκδοση του πρωτοκόλλου είναι η IPv4. Σύντομα θα αντικατασταθεί τελείως από την IPv6 (ένας υπολογιστής μπορεί βέβαια να τρέχει ταυτόχρονα και τις δύο εκδόσεις). Η IPv4 χρησιμοποιεί 32 bit για διευθύνσεις, επιτρέποντας ένα θεωρητικό μέγιστο περίπου 4.3δις. (2^32). Πλέον δεν επαρκούν για την κάλυψη των αναγκών του διαδικτύου, λογω της τάσης κάθε συσκευή στον πλανήτη να καταλήξει ενδεχομένως να έχει διεύθυνση IP. Η IPv6 χρησιμοποιεί 128bit για διευθύνσεις και φιλοδοξεί να καλύψει την ανάγκη αυτή για μεγάλο διάστημα αν όχι για πάντα.

Μια τυπική διεύθυνση IPv6 απεικονίζεται στο δεκαεξαδικό και έχει τη μορφή :
A2F1.569B.5642.FBC1.DD22.667F.22AA.99BB
Δηλαδή αποτελείται από οκτώ ομάδες των 16 bit

Σε αντιπαράθεση, μια τυπική διεύθυνση IPv4 απεικονίζεται στο δεκαδικό:
192.168.100.150
Αποτελείται από τέσσερις ομάδες των 8 bit.

Πέρα από αυτό, ο τρόπος λειτουργίας των δύο είναι κατά πολύ παρόμοιος.
Ανάλυση διευθυνσιοδότησης IPv4 περιλαμβάνεται σε ξεχωριστή ενότητα.

ARP (Address resolution Protocol)

Η επικοινωνία μεταξύ συσκευών στο ίδιο υποδίκτυο γίνεται στο πιο χαμηλό στρώμα (Network Access1). Στην περίπτωση δικτύων Ethernet, οι συσκευές έχουν MAC Address (Media Access Control), δηλαδή φυσικές διευθύνσεις, πέρα από τις λογικές διευθύνσεις, όπως IP. Το ARP χρησιμεύει ώστε μια συσκευή, ξέροντας μόνο τη λογική διεύθυνση της συσκευής με την οποία πρέπει να επικοινωνήσει, να μπορεί να μάθει και τη φυσική της διεύθυνση.

Παράδειγμα:

Έστω το PC-A με IP 10.1.1.1 και MAC AAAA.AAAA.AAAA2 και το PC-B με IP 10.1.1.2 και MAC BBBB.BBBB.BBBB
Το A θέλει να επικοινωνήσει με το B, αλλά ξέρει μόνο την IP του B. Οπότε δημιουργεί ένα πακέτο ARP με source IP το 10.1.1.1 και destination το 255.255.255.255, το οποίο χρησιμοποιείται για broadcast σε όλες τις συσκευές. Μέσα στα δεδομένα του ARP πακέτου περιλαμβάνει τη διεύθυνση του B (10.1.1.2). Στο χαμηλότερο στρώμα το πακέτο ενθυλακώνεται σε ένα Ethernet frame με source MAC το AAAA.AAAA.AAAA και destination το FFFF.FFFF.FFFF, το οποίο επίσης είναι ειδική διεύθυνση για broadcast.
Όλες οι συσκευές στο υποδίκτυο θα λάβουν το frame, και όλες επίσης θα εξετάσουν το ARP πακέτο στο ανώτερο στρώμα. Το PC-B μόνο όμως θα απαντήσει αφού η δικιά του διεύθυνση αναφερόταν στα δεδομένα του πακέτου ως αναζητούμενη. Η απάντηση θα σταλθεί αποκλειστικά στο PC-A του οποίου τη διεύθυνση γνωρίζει από το MAC Frame που έλαβε (περιλαμβάνει source MAC).
Για να μην επαναλαμβάνονται διαρκώς τα ίδια ARP requests, οι υπολογιστές διατηρούν πίνακες με αντιστοιχήσεις MAC και IP από τα ARP requests που έχουν ήδη εκπληρώσει.
Το ARP είναι απαραίτητο ακόμα και σε περιπτώσεις που αναζητούμε συσκευή σε άλλο υποδίκτυο. Η επικοινωνία σε αυτήν την περίπτωση γίνεται μέσω ενός δρομολογητή (router), αλλά το ARP χρειάζεται για να μάθουμε τη MAC του δρομολογητή (το μόνο στοιχείο που έχουμε είναι η gateway IP address). Αφού με τη διαδικασία που περιγράφηκε μάθουμε τη MAC του δρομολογητή, μετά μπορεί να ακολουθήσει η δημιουργία κλασικών IP πακέτων με προορισμό την IP της απομακρυσμένης συσκευής. Επειδή ο πρώτος σταθμός αυτών των πακέτων δεν είναι παρά ο δρομολογητής, το destination MAC αυτών είναι αυτό του δρομολογητή. Για την ακρίβεια, αυτός είναι ο μόνος τρόπος να λάβει τα frames ο δρομολογητής και να καταλάβει ότι τα πακέτα που περιέχουν δεν προορίζονται γι αυτόν τον ίδιο αλλά για δρομολόγηση.

[1] Μερικά βιβλία κάνουν διαχωρισμό του Network Access στα επίπεδα data link και physical για πιο πλήρη αντιστοίχηση με το μοντέλο OSI
[2] Οι MAC είναι διευθύνσεις 48bit σε δεκαεξαδικό

6.2 Εισαγωγή στο IP Addressing

Μια διεύθυνση IP συνήθως αναπαριστάται ως τέσσερις δεκαδικοί αριθμοί από το 0 ως το 255, χωρισμένοι με τελείες. Το χωρίζουμε σε τέσσερις ομάδες των 8 bit και αναγράφουμε την κάθε μια με δεκαδικό αριθμό για λόγους ευκολίας στο ανθρώπινο μάτι.

Δυαδική αναπαράσταση

Για να κατανοήσουμε πως λειτουργεί η διευθυνσιοδότηση, πρέπει να εξετάσουμε τις διευθύνσεις στο δυαδικό σύστημα.

Θέση bit	8	7	6	5	4	3	2	1
Δυνάμεις του 2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Δεκαδικός	128	64	32	16	8	4	2	1

Χρησιμοποιώντας τον πίνακα είναι εύκολο να αντιστοιχήσουμε δυαδικούς αριθμούς με δεκαδικούς.
Για παράδειγμα, ο αριθμός: 11011010
Ξεκινώντας από αριστερά προς τα δεξιά έχουμε:
128*1 + 64*1 + 0*32 + 1*16 + 1*8 + 0*4 + 1*2 + 0*1 = 218
Δηλαδή, από τα αριστερά προς τα δεξιά, πολλαπλασιάζουμε το κάθε bit με το δεκαδικό που αντιστοιχεί στην ανάλογη δύναμη του δύο που έχουμε από τον πίνακα.
Για μετατροπή από δεκαδικό σε δυαδικό η λογική παρουσιάζεται στο ακόλουθο παράδειγμα:
Έστω ο αριθμός 181. Για να βρούμε τον αντίστοιχο δυαδικό ξεκινάμε από τα αριστερά του πίνακα και βλέπουμε ποιους από τους δεκαδικούς της τρίτης γραμμής μπορούμε να «χωρέσουμε» (μια φορά) στον αριθμό μας, αφαιρώντας τους από αυτόν. Όποτε αφού το 128 είναι μικρότερο του 181. Το όγδοο bit από αριστερά είναι 1. 181 – 128 = 53. Το 64 είναι μεγαλύτερο του 53 άρα το επόμενο bit παραμένει 0. Το 32 είναι μικρότερο, άρα το τρίτο bit είναι 1 και 53 – 32 = 21. Συνεχίζοντας έτσι βλέπουμε ότι τα bit που αντιστοιχούν στο 16, 4 και 1 γίνονται 1 και τα bit του 8 και του 2 παραμένουν 0. Ο τελικός αριθμός είναι 10110101.
Αυτά θα πρέπει να επαρκούν για μετατροπές ακεραίων ως το 256 (8bit).

Κλάσεις διευθύνσεων IP

Ο αριθμός της διεύθυνσης IP, αν και όπως είπαμε χωρίζεται σε 4 ομάδες των 8bit για λόγους ευκολίας, στην πραγματικότητα ο ουσιαστικός χωρισμός του είναι σε 2 ομάδες μεταβαλλόμενου μεγέθους που δεν αντιστοιχούν απαραίτητα στις ομάδες των 8 bit που συνηθίζουμε να τον αναγράφουμε. Η πρώτη ομάδα αναπαριστά το δίκτυο και η δεύτερη τις συσκευές (hosts).

Οι IP διευθύνσεις χωρίζονται σε πέντε κλάσεις όπως φαίνεται στον πίνακα.

Κλάση	Πρώτη οχτάδα	όρια	Bits δικτύου	Bits συσκευών	Μέγιστο δικτύων	Μέγιστο συσκευών
A	0xxxxxxx	1-126	8	24	126	16.7εκ
B	10xxxxxx	128-191	16	16	65χιλ	65χιλ
C	110xxxxx	192-223	24	8	16.7εκ	254
D	1110xxxx	224-239	-	-	-	-

E	11110xxx	240-254	-	-	-	-

Η δομή της πρώτης οχτάδας καθορίζει την κλάση όπως φαίνεται στον πίνακα. Η επόμενη στήλη δίνει την ίδια πληροφορία σε δεκαδικό. Τα bit δικτύου και συσκευών είναι τα προεπιλεγμένα σε κάθε περίπτωση. Ειδικά για την πρώτη κλάση πρέπει να σημειωθεί ότι δεν υπάρχει διεύθυνση με την πρώτη οχτάδα να είναι 0. Όλο το υποσύνολο των διευθύνσεων αυτών είναι χρεωμένο. Το ίδιο ισχύει για το 127 που χρησιμοποιείται για loopback. Στην κλάση Ε, το δίκτυο 255 είναι επίσης χρεωμένο για γενικό broadcasting προς όλες τις IP διευθύνσεις. Οι κλάσεις Α, Β και C περιλαμβάνουν διευθύνσεις γενικής χρήσης. Αντίθετα η κλάση D χρησιμοποιείται για ειδικές περιπτώσεις όπως για multicasting και η κλάση Ε είναι χρεωμένη και δεν χρησιμοποιείται παρά μόνο για πειραματικούς σκοπούς.

Οι διευθύνσεις των κλάσεων Α, Β και C χωρίζονται σε δημόσιες και ιδιωτικές. Όλες είναι δημόσιες εκτός από τις παρακάτω εξαιρέσεις που είναι ιδιωτικές:

- 10.0.0.0 – 10.255.255.255 - 1 δίκτυο κλάσης Α
- 172.16.0.0 – 172.31.255.255 - 16 δίκτυα κλάσης Β
- 192.168.0.0 – 192.168.255.255 - 256 δίκτυα κλάσης C

Οι ιδιωτικές διευθύνσεις μπορούν να χρησιμοποιηθούν ελεύθερα από οποιονδήποτε στο εσωτερικό του δίκτυο. Δεν μπορούν όμως να δρομολογηθούν έξω από αυτό. Σε αντίθετη περίπτωση δεν θα υπήρχε η απαραίτητη μοναδικότητα των διευθύνσεων στο διαδίκτυο. Όταν ένας υπολογιστής έχει ιδιωτική διεύθυνση και βγαίνει στο διαδίκτυο, εξωτερικά βγαίνει με άλλη, δημόσια διεύθυνση. Η διαδικασία αυτή αναλύεται στο κομμάτι του NAT (Network Address Translation). Η διαχείριση των δημοσίων διευθύνσεων ανά τον κόσμο γίνεται από το διεθνή οργανισμό IANA (Internet Assigned Numbers Authority). Τα δικαιώματα χρήσης διευθύνσεων μπορούν να αποκτηθούν με την καταβολή χρημάτων.

6.3 Subnetting και σχεδιασμός για διευθυνσιοδότηση IP

Οι διευθύνσεις IP συνοδεύονται από τις μάσκες υποδικτύου (subnet masks). Πρόκειται για άλλον ένα 32bit αριθμό που υποδεικνύει ποια bit της IP αποτελούν το κομμάτι του υποδικτύου και ποια θέσεις των hosts. Σε μία διεύθυνση class B, όπως πχ την 172.16.1.100, η default subnet mask είναι 255.255.0.0, δηλαδή τα πρώτα 16bit είναι 1 και τα 16 τελευταία 0. Αυτό επιτρέπει την ύπαρξη 65536 δικτύων (2^16). Τα υπόλοιπα 16bit (με το 0) είναι για θέσεις hosts. Το πρώτο από αυτά είναι η περιγραφή του δικτύου και δεν μπορεί να χρησιμοποιηθεί. Το τελευταίο χρησιμοποιείται για directed broadcast, δηλαδή broadcast σε όλο το συγκεκριμένο υποδίκτυο. Άρα μένουν 2^16 – 2 = 65534 χρησιμοποιήσιμες διευθύνσεις. Για τα class C οι αριθμοί αυτοι είναι περίπου 16.7εκ δίκτυα και 254 hosts ανά δίκτυο.

Όσο μικρότερο το κομμάτι των hosts, τόσο περισσότερες διευθύνσεις χάνονται γιατί υπάρχουν περισσότερα υποδίκτυα και directed broadcast addresses. Ωστόσο, το πρόβλημα με τα μεγάλα υποδίκτυα είναι ότι ποτέ δεν καταλήγουν να χρησιμοποιούν όλες τις διευθύνσεις. Ένα δίκτυο 500 υπολογιστών με διευθύνσεις class B θα κατέληγε να σπαταλάει περιπου 65000 αχρησιμοποίητες διευθύνσεις. Στις αρχές, αυτό δεν φαινόταν πρόβλημα καθώς ελάχιστοι ενδιαφέρονταν για την απόκτηση διευθύνσεων οι οποίες υπήρχαν σε αφθονία. Πλέον δεν ισχύει αυτό. Μια εκ των υστέρων λύση ήταν λοιπόν η δυνατότητα να ανεξαρτητοποιηθούν οι μάσκες από τις κλάσεις των δικτύων και να επιτραπεί ο πλήρης έλεγχος οποιουδήποτε αριθμού bit για δίκτυο ή hosts (και όχι σε οχτάδες όπως αρχικά). Αυτό έχει ως αποτέλεσμα και την ύπαρξη αριθμών στο subnet mask διαφορετικών από το 0 και το 255. Επίσης ένας πιο λιτός τρόπος απεικόνισης του subnet mask είναι με μια κάθετο (/) και τον

αριθμό των bit δικτύου μετά τη διεύθυνση IP. Οπότε πχ η διεύθυνση 192.168.1.1 255.255.255.0 μπορεί να γραφτεί και ως 192.168.1.1 /24.

Ο παρακάτω πίνακας δείχνει όλες τις πιθανές μάσκες σε αντιστοιχία με τον αριθμό bit δικτύου, και τον αριθμό των hosts που προκύπτουν.

Μασκα	Bit δικτύου	Hosts
255.255.255.252	/30	2
255.255.255.248	/29	6
255.255.255.240	/28	14
255.255.255.224	/27	30
255.255.255.192	/26	62
255.255.255.128	/25	126
255.255.255.0	/24	254
255.255.254.0	/23	510
255.255.252.0	/22	1.022
255.255.248.0	/21	2.046
255.255.240.0	/20	4.094
255.255.224.0	/19	8.190
255.255.192.0	/18	16.382
255.255.128.0	/17	32.766
255.255.0.0	/16	65.534
255.254.0.0	/15	131.070
255.252.0.0	/14	252.142
255.248.0.0	/13	524.286
255.240.0.0	/12	1.048.574
255.224.0.0	/11	1.097.150
255.192.0.0	/10	4.194.302
255.128.0.0	/9	8.388.606
255.0.0.0	/8	16.777.216

Σχεδιασμός για διευθυνσιοδότηση IP

Εφόσον, όπως είπαμε, υπάρχει η δυνατότητα ελέγχου του αριθμού των δικτύων και hosts σε ένα δίκτυο, η δομή των διευθύνσεων που θα μοιράσουμε στο τοπικό δίκτυο απαιτεί σχεδιασμό εκ των προτέρων. Συγκεκριμένα, τα ερωτήματα που έχουμε να απαντήσουμε είναι:

1. Ποίες είναι οι απαιτήσεις για αριθμό υποδικτύων και συσκευών ανά υποδίκτυο στον οργανισμό.
2. Τι εύρος διευθύνσεων πρέπει να αποκτήσουμε για να καλυφθούν οι απαιτήσεις? (και ποια μάσκα υποδικτύου του αντιστοιχεί).
3. Αφού απαντήσουμε τα δύο παραπάνω, πρέπει να βρούμε τους αριθμούς περιγραφής δικτύων, τη διεύθυνση για directed broadcast ανά δίκτυο και τις διευθύνσεις hosts ανά δίκτυο.

Φυσικά θα πρέπει να λάβουμε υπόψη πιθανές ανάγκες μελλοντικής επέκτασης στις αρχικές απαιτήσεις.

Παραδείγματα

Ο πιο εύκολος τρόπος να κατανοήσει κανείς τη διαδικασία διευθυνσιοδότησης IP είναι μέσω παραδειγμάτων.

Παράδειγμα 1: Διαθέτουμε το δίκτυο 209.50.1.0 /24. Θέλουμε να το διασπάσουμε σε υποδίκτυα με τουλάχιστον 50 hosts το καθένα.

Η κρίσιμη οχτάδα είναι η τελευταία. Κάποια από τα 8 bit θα μετατραπούν σε bit δικτύου. Όμως πρέπει να διατηρήσουμε αρκετά bit hosts για τουλάχιστον 50 συσκευές. Κοιτώντας στο δυαδικό πίνακα, βλέπουμε ότι το 32 αντιστοιχεί στο 6ο bit και το 64 στο 7ο. Αυτό σημαίνει ότι χρειαζόμαστε 6 bit για να αναπαραστήσουμε αριθμούς μέχρι το 63. Με 5 bit θα φτάναμε μέχρι το 31 που δεν αρκεί. Τα άλλα 2 bit λοιπόν μετατρέπονται σε bit δικτύου. Αυτό μας επιτρέπει να σπάσουμε το αρχικό δίκτυο σε 4 υποδίκτυα με 62 ωφέλιμες διευθύνσεις. Θυμηθείτε ότι η πρώτη και τελευταία διεύθυνση κάθε υποδικτύου δεν μπορούν να χρησιμοποιηθούν για συσκευές. Αν χρειαζόμασταν 64 ή 63 συσκευές ανά δίκτυο, αναγκαστικά θα χρησιμοποιούσαμε 7 bit για hosts και 1 μόνο για δίκτυο.

Οπότε, η νέα μάσκα υποδικτύου είναι 255.255.255.192 (/26). Το επόμενο βήμα είναι να βρούμε τις διευθύνσεις που αντιστοιχούν στο καθένα από τα υποδίκτυα. Στην κρίσιμη οχτάδα της μάσκας, ο δεκαδικός αριθμός είναι το 192. Αφαιρώντας αυτό από το 256 βρίσκουμε με εύκολο τρόπο το «βήμα» με το οποίο προσαυξάνουμε τα υποδίκτυα. Οπότε το βήμα είναι 64. Αφού το πρώτο είναι το 209.50.1.0, το επόμενο θα είναι + 64 στην τελευταία οχτάδα της διεύθυνσης, δηλαδή 209.50.1.64, το επόμενο 209.50.1.128 κοκ. Ο επόμενος πίνακας δείχνει αναλυτικά τις διευθύνσεις που αναλογούν στο καθένα:

Δίκτυο	Bit Δικτύου	Broadcast	Πρώτος host	Τελευταίος
209.50.1.0	/26	209.50.1.63	209.50.1.1	209.50.1.62
209.50.1.64	/26	209.50.1.127	209.50.1.65	209.50.1.126
209.50.1.128	/26	209.50.1.191	209.50.1.129	209.50.1.190
209.50.1.192	/26	209.50.1.255	209.50.1.193	209.50.1.254

Παράδειγμα 2: Έχουμε το Class B δίκτυο 172.16.0.0 και θέλουμε να το διασπάσουμε σε 60 υποδίκτυα.

Το Class B ξέρουμε ότι έχει 16 bit για δίκτυο και 16 για hosts. Πρέπει να βρούμε πόσα από τους hosts θα μετατραπούν σε δικτύου. Χρειαζόμαστε τουλάχιστον 6 bit για να αναπαραστήσουμε 60 αριθμούς (μέγιστο 64). Σε αυτήν την περίπτωση, αντίθετα με το προηγούμενο πρόβλημα, δεν ανησυχούμε για το -2. Θα μπορούσαμε να αναπαραστήσουμε μέχρι και 64 δίκτυα με 6 bit. Η κρίσιμη οχτάδα είναι η 3η. Αν ο αριθμός bit που άλλαζαν ήταν πάνω από 8, η κρίσιμη οχτάδα θα ήταν η 4η καθώς όλα τα bit της 3ης θα άλλαζαν σε άσσους. Με τα 16 + 6 = 22 bit, η μάσκα υποδικτύου για όλα τα υποδίκτυα είναι

255.255.252.0. Το βήμα προσαύξησης είναι 4 (256 – 252, σύμφωνα με το προηγούμενο παράδειγμα). Οπότε τα δίκτυα που σχηματίζονται είναι 172.16.0.0 /22, 172.16.4.0 /22, ... 172.16.252.0 /22, το καθένα από τα οποία περιέχει 1022 διευθύνσεις για hosts. Ο επόμενος πίνακας δίνει ένα δείγμα των πρώτων τριών υποδικτύων.

Δίκτυο	Bit Δικτύου	Broadcast	Πρώτος host	Τελευταίος
172.16.0.0	/22	172.16.3.255	172.16.0.1	172.16.3.254
172.16.4.0	/22	172.16.7.255	172.16.4.1	172.16.7.254
172.16.8.0	/22	172.16.11.255	172.16.8.1	172.16.11.254

Ίσως παρατηρήσετε ότι μέσα στις ωφέλιμες διευθύνσεις περιλαμβάνονται και κάποιες όπως 172.16.2.255 ή 172.16.3.0! Αυτές μπορούν κάλλιστα να χρησιμοποιηθούν με αυτή τη μάσκα υποδικτύου.

6.4 Λήψη Διεύθυνσης IP

Ένας υπολογιστής μπορεί να αποκτήσει διεύθυνση IP με στατική ή δυναμική μέθοδο. Με τη στατική (static addressing), η διεύθυνση χορηγείται σε κάθε μηχάνημα ξεχωριστά από τους διαχειριστές δικτύου, και δεν αλλάζει παρά μόνο με τον ίδιο τρόπο. Μαζί με τη διεύθυνση, ορίζονται επίσης και η μάσκα υποδικτύου καθώς και το default gateway, DNS servers και WINS servers αν υπάρχουν. Αυτή η μέθοδος χρησιμοποιείται κυρίως σε μικρά δίκτυα. Ο φόρτος εργασίας σε μεγάλα δίκτυα το κάνει πολύ δύσκολο και αναγκαζόμαστε να καταφύγουμε σε δυναμικές μεθόδους, συγκεκριμένα στο DHCP.

DHCP (Dynamic Host Configuration Protocol)

Με το DHCP είναι δυνατόν να χρησιμοποιήσουμε έναν η περισσότερους (κατάλληλα ρυθμισμένους) servers που αναλαμβάνουν την ανάθεση διευθύνσεων. Η αναζήτηση ξεκινάει από τον client ο ο οποίος κάνει broadcast ένα πακέτο DHCP Discover. Ο DHCP server θα το λάβει και θα στείλει στον client (με unicast, δηλαδή μόνο σε αυτόν) ένα DHCP Offer, προσφέροντας του μία διαθέσιμη IP από τις διαθέσιμες. Ο client πρέπει να απαντήσει, ζητώντας πλέον τη συγκεκριμένη IP. Αυτό το βήμα είναι απαραίτητο γιατί μπορεί να λάβει πολλά offers από διαφορετικούς servers. Καμία IP δεν δεσμεύεται χωρίς «επίσημη» αίτηση του client. Τέλος ο server απαντάει με acknowledgement και η διαδικασία ολοκληρώνεται.

Ο πιο συνηθισμένος τρόπος ανάθεσης διεύθυνσης στο DHCP είναι ο λεγόμενος dynamic όπου οι διευθύνσεις ενοικιάζονται για περιορισμένο χρονικό διάστημα, πχ 8 ημέρες. Πριν τη λήξη, ο client ζητά ανανέωση της διεύθυνσης, και ξαναπαίρνει την ίδια. Αν δεν προλάβει πριν τη λήξη (πχ γιατί είναι κλειστό το μηχάνημα για πολύ καιρό) πιθανότατα θα πάρει άλλη την επόμενη φορά. Εναλλακτικά το μπορεί να γίνει ρύθμιση στο server οι διευθύνσεις να μην απαιτούν ανανέωση αλλά να ισχύουν για αόριστο χρονικό διάστημα (automatic ή DHCP Reservation).

Κάποια μηχανήματα δεν μας συμφέρει να αποκτούν διεύθυνση δυναμικά, ωστόσο θέλουμε να τους ανατίθεται διεύθυνση από DHCP server. Μπορούμε να ρυθμίσουμε το DHCP server ώστε συγκεκριμένες MAC addresses να παίρνουν πάντα την ίδια IP για να λύσουμε αυτό το πρόβλημα. Εναλλακτικά θα μπορούσαμε απλώς να ορίσουμε στατικά με τον κλασικό τρόπο διευθύνσεις σε αυτά τα μηχανήματα πηγαίνοντας στο καθένα ξεχωριστά. Μέσω DHCP μπορούμε από ένα σημείο να

ρυθμίσουμε όμως έτσι όλες τις αλλαγές.

Bootp (Bootstrap Protocol)

Εκτός από το DHCP, υπάρχει και μία ακόμη, παλαιότερη μέθοδος ανάθεσης IP διευθύνσεων. Χρησιμοποιεί το UDP (θύρες 67 και 68) στο transport layer και το RARP (Reverse ARP) στο network layer, όπως και το DHCP.

Μια σημαντική διαφορά είναι ότι η διαδικασία εξελίσσεται κατά την εκκίνηση της συσκευής ή του υπολογιστή. Παράδειγμα που χρησιμοποιείται το bootp, είναι λογισμικό τύπου Symantec Ghost όπου ξεκινάμε ένα σύστημα από δισκέτα που περιλαμβάνει ένα ελάχιστο λειτουργικό σύστημα για να ξεκινήσει τις υπηρεσίες δικτύου και να πάρει ένα ομοίωμα δίσκου (disk image) από το server ως κομμάτι της διαδικασίας αυτοματοποιημένου deployment. Άλλη περίπτωση είναι ελαχίστων προδιαγραφών δικτυακά τερματικά χωρίς σκληρό δίσκο, τα οποία ήταν κοινά στο παρελθόν αλλά όχι πλέον. Οι σύγχρονες κάρτες δικτύου έχουν ενσωματώσει το πρωτόκολλο στο BIOS τους εξαλείφοντας έτσι ακόμα και την ανάγκη δισκέτας σε ορισμένες περιπτώσεις.

7. Εισαγωγή στους Δρομολογητές

Οι δρομολογητές είναι στην ουσία υπολογιστές με όλα τα βασικά συστατικά ενός κοινού υπολογιστή, όπως CPU, RAM και μονάδες εισόδου/εξόδου. Είναι σχεδιασμένοι όμως να εκτελούν συγκεκριμένες λειτουργίες όπως τη σύνδεση διαφορετικών δικτύων και τη δρομολόγηση πακέτων μεταξύ δικτύων με τον καλύτερο δυνατό τρόπο.

Τα βασικότερα υποσυστήματα του δρομολογητή (router) είναι:

- Η CPU που εκτελεί εντολές για το λειτουργικό σύστημα (IOS – Internetwork Operating System)
- Η RAM που διατηρεί τους πίνακες δρομολόγησης (routing tables) και σβήνεται κάθε φορά που κλείνει η κάνει επανεκκίνηση ο router.
- Η NVRAM (Non Volatile RAM) που κρατάει ένα αντίγραφο του configuration του router ώστε να μην χρειάζεται εκ νέου ρύθμιση κάθε φορά που τον επανεκκινούμε.
- Flash μνήμη για την αποθήκευση του λειτουργικού συστήματος.
- ROM για διαγνωστικά test του hardware κατά τη διαδικασία POST (power on self test)
- System Bus για τη μεταφορά δεδομένων μεταξύ των υποσυστημάτων του router
- Τις διεπαφές για σύνδεση σε δίκτυα LAN ή WAN.

Παρακάτω, θα παρουσιάσουμε τα απαραίτητα βήματα για τη σύνδεση και βασική ρύθμιση ενός δρομολογητή.

7.1 Σύνδεση σε κονσόλα

Την πρώτη φορά που ρυθμίζουμε ένα δρομολογητή, ο μόνος δυνατός τρόπος είναι μέσω της console port. Απαιτεί φυσική πρόσβαση στο δρομολογητή, ένα καλώδιο τύπου rollover και έναν υπολογιστή.

Το καλώδιο έχει εξόδους τύπου RJ-45, σαν Ethernet αν και η συνδεσμολογία διαφέρει. Η μία μεριά πάει στο console port του δρομολογητή και η άλλη στον υπολογιστή, στη σειριακή θύρα. Απαιτείται adapter από RJ-45 σε σειριακή 9 ή 25 ακίδων ανάλογα με τη διαθέσιμη θύρα στον υπολογιστή. Είναι

δυνατόν να φτιαχτεί καλώδιο με RJ-45 στη μία άκρη και σειριακή στην άλλη για να αποφύγουμε την ανάγκη adapter.

Το επόμενο βήμα είναι να ξεκινήσουμε την επικοινωνία με τον υπολογιστή. Στα windows, αυτό μπορεί να γίνει με το HyperTerminal που περιλαμβάνουν. Πρόκειται για ένα απλό πρόγραμμα προσομοίωσης τερματικού, το οποίο είναι απαραίτητο αφού ο δρομολογητής δεν διαθέτει οθόνη και πληκτρολόγιο.
Αφού ξεκινήσουμε το HyperTerminal (Start > Programs > Accessories > Communications > HyperTerminal) και μία νέα σύνδεση με οποιοδήποτε όνομα, επιλέγουμε την COM port, την οποία πρέπει να ξέρουμε, και είναι η σειριακή θύρα στην οποία συνδεθήκαμε. Πλέον οι σύγχρονοι υπολογιστές σπάνια έχουν πάνω από μία, οπότε συνήθως είναι COM1. Οι παράμετροι σύνδεσης πρέπει υποχρεωτικά να είναι οι εξής:

Bits per second	: 9600
Data bits	: 8
Parity	: None
Stop bits	: 1
Flow control	: None

7.2 Διαδικασία εκκίνησης

Εφόσον στο προηγούμενο βήμα εκτελέστηκε χωρίς πρόβλημα, η διαδικασία εκκίνησης, που μπορεί να πάρει κάποιο χρόνο θα ολοκληρωθεί και στην οθόνη θα έχουμε κάτι παρόμοιο με το ακόλουθο:

```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K 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 Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
```

Οι πληροφορίες φυσικά διαφέρουν ανάλογα με την έκδοση του λειτουργικού συστήματος και το διαθέσιμο υλικό.

Απαντάμε no στην ερώτηση για το configuration dialog και πατάμε return για να μας βγάλει στο prompt σε user mode.
Με το ? μπορούμε πάντα να έχουμε βοήθεια για τις επιλογές μας.

```
Router>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
```

Ενώ το ίδιο ισχύει για τις παραμέτρους των βασικών εντολών. Πχ:

```
Router>show ?
  cdp          CDP information
  clock        Display the system clock
  controllers  Interface controllers status
  flash:       display information about flash: file system
  frame-relay  Frame-Relay information
  history      Display the session command history
  hosts        IP domain-name, lookup style, nameservers, and host table
  interfaces   Interface status and configuration
  ip           IP information
  protocols    Active network routing protocols
  sessions     Information about Telnet connections
  tcp          Status of TCP connections
  users        Display information about terminal lines
  version      System hardware and software status
```

Δίνοντας την εντολή **show flash**, παίρνουμε σχετικές πληροφορίες:

```
System flash directory:
File  Length   Name/status
  1   5571584  pt1000-i-mz.122-28.bin
[5571584 bytes used, 26942464 available, 32514048 total]
32768K bytes of processor board System flash (Read/Write)
```

Ενώ δίνοντας τη **show version** παίρνουμε πληροφορίες παρόμοιες με αυτές κατά τη διαδικασία εκκίνησης, αλλά και την τιμή του configuration register που λογικά θα είναι 0x2102. Προς το παρόν, όσον αφορά τον configuration register αρκεί να γνωρίζουμε ότι αναγράφεται στο δεκαεξαδικό και ότι η κανονική του τιμή είναι 2102. Μία συνηθισμένη περίπτωση είναι να θέλουμε να την αλλάξουμε σε 2142, που σημαίνει ότι έτσι αγνοεί όλες τις ρυθμίσεις κατά την εκκίνηση, χωρίς όμως να τις διαγράφει. Αυτό είναι ένα απαραίτητο βήμα για την ανάκτηση ελέγχου του router σε περίπτωση απώλειας των κωδικών πρόσβασης.

7.3 Privileged Mode

Σε user mode, λίγες λειτουργίες είναι διαθέσιμες. Δεν έχουμε δυνατότητα να αλλάξουμε καμία από τις ρυθμίσεις αλλά ούτε και όλες οι επιλογές για απλή απεικόνιση πληροφοριών είναι διαθέσιμες,

Η εντολή **enable** μας επιτρέπει να μπούμε σε privileged mode. Το σύμβολο στο prompt αλλάζει από > σε #.

Ξαναδίνοντας **?**, παρατηρούμε ότι πλέον έχουμε περισσότερες επιλογές

```
Router#?
Exec commands:
  <1-99>      Session number to resume
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  no          Disable debugging informations
  ping        Send echo messages
  reload      Halt and perform a cold restart
  resume      Resume an active network connection
  setup       Run the SETUP command facility
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
  undebug     Disable debugging functions (see also 'debug')
  write       Write running configuration to memory, network, or terminal
```

Το ίδιο ισχύει και για τη **show ?**. Συγκεκριμένα, μας ενδιαφέρει η **show running-config.**

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

Current configuration : 489 bytes
!
version 12.2
no service password-encryption
!
hostname Router
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial2/0
 no ip address
 shutdown
!
interface Serial3/0
 no ip address
 shutdown
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end
```

Παραπάνω φαίνεται το configuration file που έχει αποθηκευμένο στη RAM ο router. Το παράδειγμα δείχνει έναν καινούριο, δηλαδή μη ρυθμισμένο router για χάριν εξοικείωσης με τη μορφή του αρχείου. Καθώς αλλάζουμε τις ρυθμίσεις του router, το running-config αλλάζει. Αν βέβαια δεν αποθηκεύσουμε

τις αλλαγές, αυτές δεν θα ισχύουν μετά από επανεκκίνηση. Η αποθήκευση αλλαγών γίνεται πληκτρολογώντας **copy running-config startup-config** σε privileged mode.
Άλλες χρήσιμες εντολές είναι η **erase startup-config**, με την οποία αφαιρούμε μόνιμα όλες τις αποθηκευμένες ρυθμίσεις και η **reload** η οποία προκαλεί επανεκκίνηση. Σε περίπτωση που έχουμε κάνει αλλαγές στις ρυθμίσεις θα μας ρωτήσει αν θέλουμε να τις αποθηκεύσουμε.
Υπάρχει και η δυνατότητα για **ping** ή **traceroute** σε κάποιο συγκεκριμένο ip address ή hostname, όπως σε συνηθισμένους υπολογιστές.
Για περισσότερα reports, χρήσιμες show εντολές είναι οι ακόλουθες:
show arp
show interfaces
show ip interface brief
show protocols

Για να επιστρέψουμε σε user mode πληκτρολογούμε **disable**.

7.4 Βασικές Ρυθμίσεις I

Σε privileged mode, υπάρχει η εντολή **configure terminal**.

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

Το prompt αλλάζει για να μας δείξει ότι βρισκόμαστε σε configuration mode. Οποιαδήποτε αλλαγή στις ρυθμίσεις είναι προσβασιμη μόνο από αυτό το mode ή τις υποκατηγορίες του.
Η εντολή **hostname** αλλάζει το όνομα του router (και του prompt ως επακόλουθο).

```
Router(config)#hostname athens
athens(config)#
```

Η εντολή **enable password** <password> ενεργοποιεί τον έλεγχο κωδικού πρόσβασης για την είσοδο σε privileged mode.

```
athens(config)#enable password cisco
athens(config)#exit
athens#disable
athens>enable
Password:
athens#
```

Παραπάνω, βάζουμε κωδικό cisco. Με το exit βγαίνουμε από configuration mode (το exit πάντα μας βγάζει ένα mode πιο πάνω). Βγαίνουμε από privileged mode και ξαναμπαίνουμε. Ο κωδικός που εισάγουμε δεν φαίνεται στην οθόνη.

Η εντολή **enable secret** <secret> ενεργοποιεί τον κρυφό κωδικό πρόσβασης, ο οποίος δεν φαίνεται στο configuration file σε text μορφή και έχει προτεραιότητα έναντι του απλού κωδικού. Αυτό δεν είναι το ίδιο με το να χρησιμοποιήσουμε την εντολή **service password-encryption**, το οποίο κρυπτογραφεί με αναστρέψιμη κρυπτογράφηση τον «απλό» κωδικό πρόσβασης. Προτείνεται η χρήση του secret κατά προτίμηση.

Παρακάτω δείχνουμε την ανάθεση κωδικών πρόσβασης για απομακρυσμένη πρόσβαση αλλά και για τοπική μέσω της κονσόλας

```
athens(config)#line console 0
```

```
athens(config-line)#password cisco
athens(config-line)#login
athens(config-line)#exit
athens(config)#line vty 0 4
athens(config-line)#password cisco
athens(config-line)#login
athens(config-line)#exit
athens(config)#
```

Η πρώτη εντολή**, line console 0**, αναφέρεται στην κονσόλα, ώστε να απαιτείται κωδικός ακόμα και για το user mode. Η δεύτερη, **line vty 0 4**, αφορά τα λεγόμενα virtual terminal lines. Πρέπει να υπάρχει κωδικός για να επιτρέπεται η πρόσβαση μέσω telnet. Πέντε διαφορετικά virtual terminals, από 0 ως 4 είναι διαθέσιμα. Αφού δώσουμε κωδικό, πληκτρολογούμε **login** μέσα στο configuration της γραμμής (config-line) ώστε να την ενεργοποιήσουμε. Μερικοί routers έχουν παραπάνω από πέντε terminals. Μπορούμε να ρυθμίσουμε το καθένα ξεχωριστά με άλλο κωδικό αν θέλουμε, ή όλα μαζί όπως παραπάνω

7.5 Βασικές Ρυθμίσεις ΙΙ

Υπάρχει η δυνατότητα να εμφανίζεται ένα συγκεκριμένο μήνυμα σε οποιονδήποτε συνδέεται στο router είτε από κονσόλα είτε απομακρυσμένα, με την εντολή banner **motd** #<message>#, όπως φαίνεται στο παράδειγμα:

```
athens(config)#banner motd #Authorized Access Only#
athens(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
athens#exit



athens con0 is now available

Press RETURN to get started.



Authorized Access Only

athens>
```

Υπάρχει η δυνατότητα για host name resolution τοπικά, με παρόμοιο τρόπο που δουλεύει στα windows pc το c:\windows\system32\drivers\etc\hosts αρχείο. Η εντολή ειναι **ip host** <host> <ip address>. Ετσι μπορει καποιος για παράδειγμα να κάνει ping ή telnet κάποιο host μέσα από το router δίνοντας το όνομα αντί για το ip ακόμα και αν δεν υπάρχει DNS.

Το πιο σημαντικό ειναι η ρύθμιση των interfaces. Οι τυπικοί routers έχουν interfaces για serial και ethernet, τα οποία πρέπει να γνωρίζουμε πως να ρυθμίσουμε. Το όνομα και ο αριθμός του κάθε interface εξαρτάται από τον τύπο router. Μέσα από το configuration terminal, με την εντολή **interface** <type> <number>, Μπαίνουμε σε mode ρύθμισης του συγκεκριμένου interface. Αναθέτουμε διεύθυνση με την εντολή **ip address** <ip address> <subnet mask>, και ενεργοποιούμε το interface με την εντολή **no shutdown.**

Ειδικά για τα serial interfaces υπάρχει η εντολή **clock rate** <number>. Σε μια σύνδεση με serial μεταξύ δυο router, ο ένας ειναι ο DCE (data communications equipment) και ο άλλος ο DTE (data terminal equipment). Ο DCE οφείλει να ορίσει το ρυθμό μετάδοσης οπότε χρειάζεται μια παραπάνω εντολή για

τη ρύθμισή του.

```
athens(config)#interface Serial 2/0
athens(config-if)#ip address 192.168.1.1 255.255.255.0
athens(config-if)#clock rate 56000
athens(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial2/0, changed state to down
athens(config-if)#exit
athens(config)#Interface FastEthernet 0/0
athens(config-if)#ip address 192.168.2.1 255.255.255.0
athens(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
athens(config-if)#exit
athens(config)#
```

Στο παραπάνω παράδειγμα, το serial interface όταν το ανεβάζουμε ξαναπέφτει αμέσως γιατί αντιλαμβάνεται ότι δεν υπάρχει τίποτα στην άλλη μεριά. Άμα ρυθμίζαμε και ένα δεύτερο router στην άλλη άκρη, θα ξανανέβαινε αυτόματα.

Στο IOS σπάνια βλέπει κανείς εντολές για την ακύρωση προηγούμενων ρυθμίσεων, ή εντολές που κάνουν το αντίθετο από άλλες εντολές. Αντ' αυτού, μπορεί να χρησιμοποιηθεί η λέξη **no** μπροστά από υπάρχουσες εντολές. Δεν υπάρχει εντολή για την ενεργοποίηση interface, όποτε η ενεργοποίηση γίνεται με **no shutdown**. Αν θέλουμε να αφαιρέσουμε ip address, πληκτρολογούμε την εντολή για να προσθέσουμε την ip address με ένα no μπροστά. Το ίδιο ισχύει για το clock rate, τα passwords και login κλπ.

Σε αυτό το σημείο θα ήταν χρήσιμη η εντολή **show ip interface brief**.

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

FastEthernet0/0        192.168.2.1     YES manual up                    down

FastEthernet1/0        unassigned      YES manual administratively down down

Serial2/0              192.168.1.1     YES manual down                  down

Serial3/0              unassigned      YES manual administratively down down
```

Η οποία όπως είπαμε δεν πληκτρολογείται στο config αλλά στο καθαρό privileged mode.

7.6 Απομακρυσμένη Σύνδεση

Είναι πολύ χρήσιμο ορισμένες φορές να ελέγχουμε ένα router απομακρυσμένα, μέσω telnet είτε από το PC μας είτε από άλλο συνδεδεμένο router. Τα βασικά για τη σύνδεση telnet θα παρουσιαστούν μέσω παραδείγματος.

Έστω 2 routers συνδεδεμένοι με serial. Ο Athens με ip 192.168.1.1 και ο London με 192.168.1.2 στα serial interfaces τους. Η σύνδεση γίνεται με την εντολή **connect** <ip address> ή **connect** <host>. Φυσικά ο δεύτερος τρόπος λειτουργεί μόνο με την ύπαρξη του ονόματος στο host table όπως δείξαμε προηγουμένως ή αν λειτουργεί DNS. Η λέξη connect μπορεί μάλιστα να παραληφθεί!

```
athens#connect 192.168.1.2
Trying 192.168.1.2 ...

User Access Verification

Password:
london>
```

Για να δουλέψει είναι απαραίτητο να έχουν ρυθμιστεί σωστά τα virtual terminals στον απομακρυσμένο router, με passwords και login όπως δε προηγούμενο παράδειγμα διαφορετικά δεν θα επιτευχθεί η σύνδεση. Αν δεν θέλουμε password, πρέπει να μπούμε σε configuration στο line vty και να δώσουμε την εντολή **no login**, στον απομακρυσμένο router. Ομοίως, για να μπούμε σε privileged mode απομακρυσμένα πρέπει να υπάρχει κωδικός πρόσβασης, αυτή τη φορά υποχρεωτικά.
Κλείνουμε μόνιμα τη σύνδεση με exit. Μπορούμε όμως εναλλακτικά να την κάνουμε suspend πατώντας ctrl-shift-6 και μετά x
Αυτό μας επιτρέπει να έχουμε πολλαπλές telnet συνδέσεις ανοιχτές και να εναλλασσόμαστε μεταξύ τους. Η εντολή **show sessions** μας δείχνει τις ανοιχτές συνδέσεις, και η **disconnect** <number> κλείνει την επιλεγμένη σύνδεση. Ο αριθμός σύνδεσης φαίνεται στον πίνακα συνδέσεων.

```
athens#show sessions
Conn Host               Address             Byte  Idle Conn Name
*  1 192.168.1.2        192.168.1.2            0     0 192.168.1.2
athens#disconnect 1
Closing connection to 192.168.1.2 [confirm]y
athens#
```

Μπορούμε να επαναφέρουμε μια από τις ανοιχτές συνδέσεις με την εντολή **resume** <number>. Εναλλακτικά, αντί για τον αριθμό σύνδεσης μπορούμε να δοκιμάσουμε τις εντολές **disconnect** και **resume** με το ip address ή το όνομα της σύνδεσης.

7.7 CDP (Cisco Discovery Protocol)

Πρόκειται για ένα ιδιωτικό πρωτόκολλο της Cisco που βοηθάει στον εντοπισμό άλλων Cisco συσκευών δικτύου. Οι συσκευές πρέπει να είναι άμεσα συνδεδεμένες, δηλαδή να γειτονεύουν, και φυσικά να είναι Cisco. Αυτό βοηθάει στη γρήγορη χαρτογράφηση ενός υπάρχοντος δικτύου χωρίς να πρέπει να επισκεφθούμε όλες τις συσκευές τοπικά, που στην περίπτωση routers ενωμένων με serial για παράδειγμα οι αποστάσεις μπορεί να είναι μεγάλες. Το αρνητικό είναι η ασφάλεια αφού οι πιο πολλές πληροφορίες είναι διαθέσιμες σε απλό user mode, και γι αυτό υπάρχει η δυνατότητα απενεργοποίησης συνολικά η σε συγκεκριμένα interfaces.
Στο παράδειγμα έχουμε τους routers Athens και London ενωμένους με serial και ένα Ethernet switch ενωμένο στον Athens. Η εντολή **show cdp neighbors** δείχνει τις ενωμένες συσκευές.

```
athens#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
london       Ser 0            175            R       PT1000      Ser 0
Switch       Fas 0/0          175            S       2950        Fas 0/1
```

Η εντολή **show cdp entry** <*deviceID*> δείχνει πληροφορίες για τη συγκεκριμένη συσκευή

```
athens#show cdp entry london
Device ID: london
Entry address(es):
  IP address : 192.168.1.2
Platform: cisco PT1000, Capabilities: Router
Interface: Serial2/0, Port ID (outgoing port): Serial2/0
Holdtime: 160

Version :
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
```

```
advertisement version: 2
Duplex: full
```

Η εντολή show **cdp neighbors detail** είναι ουσιαστικά η ίδια με τη show cdp entry αλλά για όλες τις υπάρχουσες συσκευές, ώστε να μην χρειάζεται να ζητάμε το κάθε entry ξεχωριστά. Η **show cdp interface** <interface> δείχνει πόσο συχνά στέλνει πακέτα cdp το συγκεκριμένο interface και το holdtime. Αν μια γειτονική συσκευή σταματήσει να στέλνει cdp πακέτα, θα παραμείνει στον πίνακα γειτνίασης για χρόνο ίσο με το holdtime σε δευτερόλεπτα.

```
athens#show cdp interface Serial 2/0
Serial2/0 is up, line protocol is up
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

Μπορούμε να καθαρίσουμε τον πίνακα γειτνίασης από απλό privileged mode με την εντολή **clear cdp table**. Η ενεργοποίηση του cdp γίνεται με την εντολή **cdp run** σε configuration mode. Για ενεργοποίηση μόνο σε συγκεκριμένο interface με την εντολή **cdp enable** στο configuration του interface. Η απενεργοποίηση με τη λέξη no μπροστά από τις παραπάνω εντολές. Το cdp είναι by default ενεργοποιημένο στις συσκευές.

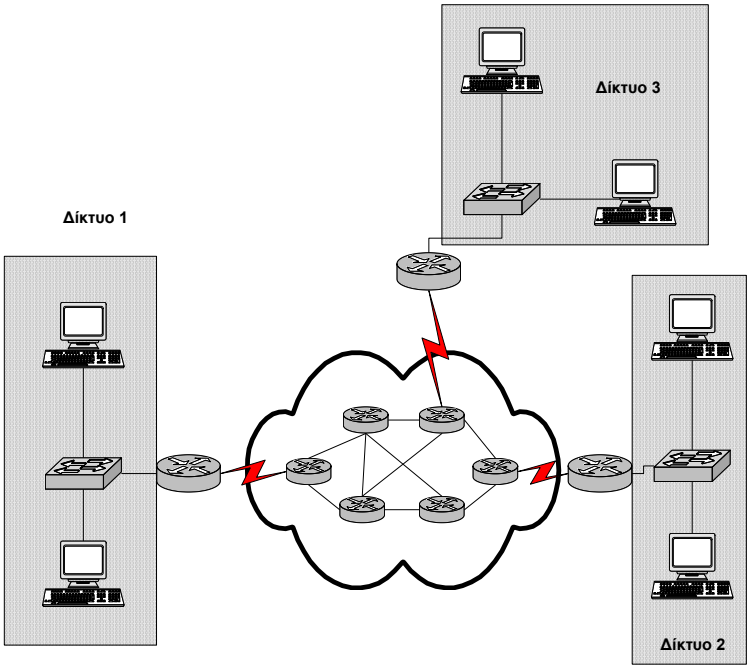
8. Δρομολόγηση

Δρομολόγηση είναι η διαδικασία επιλογής διαδρομών μεταξύ δικτύων ώστε να καταστεί δυνατή η μετάδοση δεδομένων από ένα σημείο (κόμβο) αφετηρίας σε ένα κόμβο προορισμού.

Γιατί χρειάζεται δρομολόγηση σε ένα δίκτυο?

- Γιατί χρειάζεται να εγκατασταθεί μια λογική διαδρομή μεταξύ δύο δικτύων ώστε να καταστεί δυνατή η μεταφορά δεδομένων μεταξύ τους.
- γιατί σε ένα δίκτυο υπάρχουν πολλαπλές πιθανές εναλλακτικές διαδρομές, με διαφορετικές ιδιότητες η καθεμία
- γιατί υπάρχουν πολλές παράμετροι (ταχύτητα, αξιοπιστία, κόστος) οι οποίοι αναδεικνύουν κάποια διαδρομή ως προτιμότερη άλλης

Η δρομολόγηση πακέτων βάσει διεύθυνσης IP είναι λειτουργία 3ου επιπέδου και στα περισσότερα δίκτυα πραγματοποιείται από συσκευές που ονομάζονται δρομολογητές (routers).



Σχήμα 1: Για να επικοινωνήσει ένας υπολογιστής που ανήκει στο δίκτυο 1 με ένα υπολογιστή του δικτύου 2, θα πρέπει να βρεθεί μια διαδρομή που να τους συνδέει, πάνω από την οποία θα περνούν τα πακέτα δεδομένων. Αυτό είναι αρμοδιότητα των δρομολογητών που παρεμβάλλονται μεταξύ των δύο δικτύων.

Εναλλακτικά, η δρομολόγηση μπορεί να πραγματοποιηθεί και από υπολογιστές εξοπλισμένους με περισσότερες από μια κάρτες δικτύου, με τη χρήση κατάλληλου software, όπως π.χ το XORP, το Quagga ή τα Routing & Remote Access Services των Windows Server NT/2003.

Βασική λειτουργία ενός δρομολογητή είναι να συνδέσει δύο ή περισσότερα δίκτυα σε φυσικό επίπεδο ή/και σε επίπεδο IP (Layer 3), χρησιμοποιώντας πολλαπλά (φυσικά ή λογικά) network interfaces και να «ανακαλύψει» πιθανές διαδρομές μεταξύ δικτύων ώστε να μπορέσει στη συνέχεια να μεταφέρει πακέτα δεδομένων από το ένα δίκτυο στο άλλο.

Ένας δρομολογητής μπορεί να μάθει μια νέα διαδρομή με δύο βασικές μεθόδους: στατικά ή δυναμικά.

Οι διαδρομές που μαθαίνει ένας δρομολογητής στατικά είναι σταθερές διαδρομές που μπορούν είτε να οριστούν άμεσα από το διαχειριστή του δικτύου, είτε να εισαχθούν αυτόματα από τον ίδιο το δρομολογητή. Ο δρομολογητής ελέγχει τα ενεργά interfaces που διαθέτει, καθορίζει τα δίκτυα που αντιστοιχούν σε κάθε interface και εισάγει τη σχετική πληροφορία στον πίνακα δρομολόγησης.

Με τη δυναμική, αντίθετα, μέθοδο, οι διαδρομές δημιουργούνται αυτόματα, με τη χρήση διαφόρων τεχνικών οι οποίες υλοποιούνται με πρωτόκολλα δρομολόγησης (routing protocols). Με τη χρήση ενός κοινού πρωτοκόλλου δρομολόγησης, πολλαπλοί δρομολογητές μπορούν να ανταλλάσσουν πληροφορία σχετικά με τα δίκτυα με τα οποία είναι συνδεδεμένοι και να ενημερώνουν ο ένας τον άλλο για διαδρομές μεταξύ δικτύων καθώς και για την προσβασιμότητά τους. Με αυτό τον τρόπο, όλοι οι δρομολογητές που ανήκουν σε μια ευρύτερη περιοχή δικτύου, ενημερώνονται για όλα τα υποδίκτυα που εντάσσονται σε αυτή και τον τρόπο με τον οποίο το ένα μπορεί να επικοινωνήσει με το άλλο.

Έτσι, με τη χρήση είτε στατικών τεχνικών είτε δυναμικών πρωτοκόλλων δρομολόγησης,

ανακαλύπτονται διαδρομές τις οποίες μπορεί να χρησιμοποιήσει ένα δρομολογούμενο πρωτόκολλο (*routed protocol*), όπως π.χ. το IP ή το IPX.

Δρομολογούμενα Πρωτόκολλα	
IP	RIP, IGRP, OSPF, EIGRP, IS-IS (IGP) BGP (EGP)
IPX	RIP, EIGRP, NLSP
AppleTalk	RMTP, AURP, EIGRP

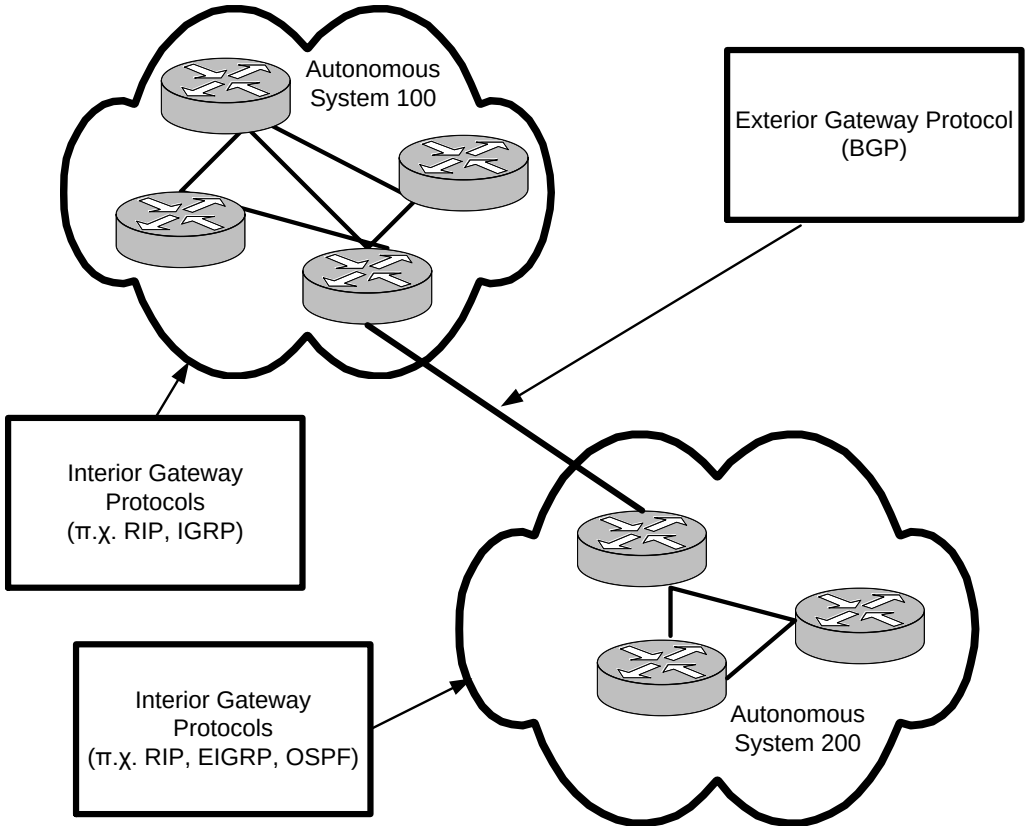
Η δρομολόγηση (όσον αφορά σε δίκτυα IP) μπορεί να γίνει τόσο εντός ενός αυτόνομου συστήματος (Intra-AS) όσο και μεταξύ αυτόνομων συστημάτων (Inter-AS). Διαφορετικά πρωτόκολλα ισχύουν ανά περίπτωση.
Στο παρόν κεφάλαιο θα μας απασχολήσει η δρομολόγηση μόνο εντός ενός αυτόνομου συστήματος

Αυτόνομο σύστημα-η δομική μονάδα του Internet

Το Internet αποτελείται από διασυνδεδεμένα αυτόνομα συστήματα, δηλαδή δίκτυα ή ομάδες δικτύων που εμπίπτουν κάτω από την εποπτεία ενός φορέα (τυπικά, ενός μεγάλου ISP), και υπακούουν σε μια κοινή για όλους, σαφώς ορισμένη πολιτική δρομολόγησης.

Κάθε αυτόνομο σύστημα προσδιορίζεται από ένα μοναδικό αριθμό (AS number), ο οποίος εκχωρείται από την IANA (Internet Assigned Numbers Authority) και χρησιμοποιείται για τη δρομολόγηση μεταξύ αυτόνομων συστημάτων.

Για τη δρομολόγηση μεταξύ αυτόνομων συστημάτων (Inter-AS routing) χρησιμοποιούνται πρωτόκολλα EGP (Exterior Gateway Protocol), σε αντιδιαστολή με τα πρωτόκολλα IGP (Interior Gateway Protocols), τα οποία διαχειρίζονται τη δρομολόγηση εντός ενός αυτόνομου συστήματος.
Σήμερα, στο Internet χρησιμοποιείται πρακτικά μόνο ένα πρωτόκολλο EGP, το BGP (Border Gateway Protocol).
Στο σχήμα που ακολουθεί παρουσιάζονται δύο διασυνδεδεμένα αυτόνομα συστήματα. Το πρώτο οποία χρησιμοποιεί τα πρωτόκολλα RIP και IGRP για την εσωτερική δρομολόγηση, ενώ το δεύτερο τα πρωτόκολλα RIP, EIGRP και OSPF. Η εξωτερική όμως δρομολόγηση (δηλ. η δρομολόγηση μεταξύ των αυτόνομων συστημάτων γίνεται με το πρωτόκολλο BGP.



Για περισσότερες πληροφορίες επισκεφθείτε τις διευθύνσεις ftp://ftp.rfc-editor.org/in-notes/rfc1930.txt και ftp://ftp.rfc-editor.org/in-notes/rfc1786.txt

(Intra-AS routing) και μόνο για το πρωτόκολλο IP.

Πώς λειτουργεί ένας δρομολογητής

- Είδαμε παραπάνω ότι ένας δρομολογητής εκτελεί βασικά δύο λειτουργίες:
- Συνεργάζεται με άλλους δρομολογητές για να βρει μονοπάτια διασύνδεσης μεταξύ δικτύων
- Εκτελεί λειτουργίες που απαιτούνται για την προώθηση πακέτων από ένα πηγαίο κόμβο σε ένα κόμβο προορισμού σε κάποιο άλλο δίκτυο

Η προώθηση πακέτων γίνεται ως εξής:
Κατά την προώθηση πακέτων, ένας router εκτελεί τις εξής διαδικασίες:

- Ο router εξάγει τη destination IP διεύθυνση του πακέτου που παρέλαβε με τις εγγραφές του πίνακα δρομολόγησής του. Συγκεκριμένα, εφαρμοζει τη μάσκα δικτύου της πρώτης εγγραφής του πίνακα δρομολόγησης πάνω στην IP του πακέτου.
  Εάν η διεύθυνση δικτύου της εγγραφής του πίνακα συμπίπτει με το αποτέλεσμα της εφαρμογής της μάσκας στην IP του πακέτου, τότε το πακέτο προωθείται από το interface που αντιστοιχεί στην εγγραφή.
- Εάν το αποτέλεσμα είναι διαφορετικό, τότε συνεχίζεται η ίδια διαδικασία με τις επόμενες εγγραφές μέχρι να βρεθεί ταίριασμα.
- Εάν εξαντληθούν οι εγγραφές και δεν έχει επιτευχθεί match, τότε ελέγχεται εάν υπάρχει default route. Εάν υπάρχει default route, το πακέτο προωθείται σε αυτή, διαφορετικά απορρίπτεται.

8.1 Στατική Δρομολόγηση και προκαθορισμένες διαδρομές

Είδαμε παραπάνω ότι μια στατική διαδρομή είτε αποκτάται αυτόματα από το δρομολογητή, όταν πρόκειται για άμεσα συνδεδεμένα δίκτυα, ή ρυθμίζεται χειροκίνητα από το διαχειριστή του δικτύου.

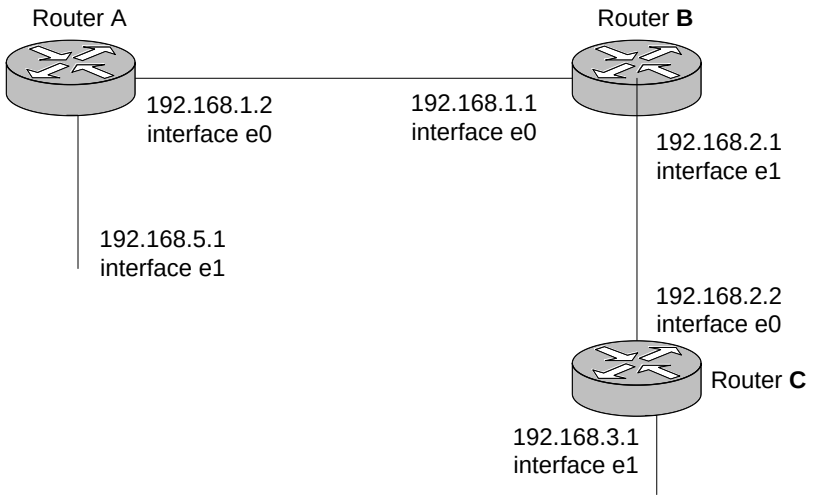
Στην πρώτη περίπτωση, ο δρομολογητής ανιχνεύει τα interfaces με τα οποία είναι εξοπλισμένος, εξετάζει τις διευθύνσεις που έχουν οριστεί στο καθένα από αυτά, εξάγει τις αντίστοιχες διευθύνσεις δικτύου και ενημερώνει τον πίνακα δρομολόγησης με τη σχετική πληροφορία, ορίζοντας έτσι μια συνδεδεμένη διαδρομή (connected route).

Τί είναι ο πίνακας δρομολόγησης

Ένας δρομολογητής, προκειμένου να μπορέσει να προωθήσει σωστά τα πακέτα που λαμβάνει σε ένα από τα interfaces του προς τον τελικό προορισμό τους, διατηρεί εσωτερικά ένα πίνακα ο οποίος περιέχει την εξής πληροφορία:

- **Τύπος διαδρομής** *(καθορίζει εάν η συγκεκριμένη διαδρομή είναι συνδεδεμένη, στατική ορισμένη από το διαχειριστή ή δυναμική, προσδιορίζοντας και το πρωτόκολλο από το οποίο προήλθε)*
- **Διεύθυνση δικτύου προορισμού**
- **Μετρική αξιολόγησης** *(διαφέρει από πρωτόκολλο σε πρωτόκολλο και χρησιμοποιείται για να αποφασίσει ποια διαδρομή είναι προτιμότερη μεταξύ δύο εναλλακτικών)*
- **Interface** *(το interface μέσω του οποίου θα προωθούνται τα πακέτα δεδομένων που απευθύνονται στο συγκεκριμένο δίκτυο)*

Ας θεωρήσουμε για παράδειγμα την ακόλουθη τοπολογία δικτύου (Τοπολογία 1)



Τοπολογία 1

Για το δρομολογητή Α, τα δίκτυα 192.168.1.0 και 192.168.5.0 είναι συνδεδεμένα δίκτυα, με τα interfaces e0 και e1 αντίστοιχα.
Έτσι, ο πίνακας δρομολόγησης του router B θα περιέχει τις εξής εγγραφές:

Learned	Network	Hops	Interface
C	192.168.1.0	0	E0
C	192.168.5.0	0	E1

Τί γίνεται όμως με το δίκτυο 192.168.3.0; Πώς θα μπορούσε ο router A να προωθήσει σωστά τα πακέτα δεδομένων που δέχεται στο interface e1 έτσι ώστε κάποιος υπολογιστής του δικτύου 192.168.5.0 να μπορεί να επικοινωνήσει με κάποιο υπολογιστή στο δίκτυο 192.168.3.0;

Για να γίνει αυτό, τα πακέτα θα πρέπει οπωσδήποτε να φτάσουν στο router C, περνώντας από το router B, για να προωθηθούν στον τελικό αποδέκτη. Ένας τρόπος για να μάθει ο router A πού θα πρέπει να προωθεί πακέτα που προορίζονται για το δίκτυο 192.168.3.0 είναι να ορίσει ο διαχειριστής του δικτύου μια στατική διαδρομή μέσω της οποίας τα πακέτα με Destination IP 192.168.3.* θα προωθούνται μέσω του interface e0 στο router B.

Σε δρομολογητές τύπου Cisco, η εντολή με την οποία είναι εφικτό αυτό είναι η **ip route**, η οποία συντάσσεται με δυο τρόπους:

```
Router(config)# ip route destination_network [subnet_mask]
NextHopNeighbourIPAddress [administrative distance] [permanent]
```

ή εναλλακτικά

```
Router(config)# ip route destination_network [subnet_mask]
exitInterface [administrative distance] [permanent]
```

Διαχειριστική απόσταση ή κόστος (Administrative Distance)

Η διαχειριστική απόσταση είναι μια έννοια που χρησιμοποιούν οι δρομολογητές της Cisco προκειμένου να χαρακτηρίσουν διαδρομές ως περισσότερο ή λιγότερο προτιμητέες, ανάλογα με τον τρόπο με τον οποίο τις πληροφορήθηκε ο δρομολογητής. Για παράδειγμα, εάν ένας δρομολογητής μάθει δύο διαδρομές για το ίδιο δίκτυο, η μια στατική και η άλλη μέσω ενός δυναμικού πρωτοκόλλου, ποιά θα πρέπει να προτιμηθεί;

Η διαχειριστική απόσταση αντιμετωπίζει αυτό το πρόβλημα, αναθέτοντας μια τιμή μεταξύ 0 και 255 σε κάθε διαδρομή. Όσο μικρότερη είναι αυτή η τιμή, τόσο πιο αξιόπιστη θεωρείται η διαδρομή.

Τύπος Διαδρομής	Απόσταση
Συνδεδεμένη	0
Στατική	0 ή 1
EIGRP (εντός του ίδιου αυτόνομου συστήματος)	90
IGRP	100
OSPF	110
RIP	120
EIGRP (από ένα άλλο αυτόνομο σύστημα)	170
Μη έγκυρη-διαδρομή με administrative distance 255 δεν θα χρησιμοποιηθεί από το router.	255

Η πρώτη παράμετρος είναι η διεύθυνση του δικτύου προορισμού. Αυτή ακολουθείται από τη μάσκα υποδικτύου, η οποία όμως μπορεί να παραλειφθεί. Στην περίπτωση που παραλείπεται η μάσκα υποδικτύου, ο δρομολογητής χρησιμοποιεί την προκαθορισμένη μάσκα ανάλογα με την κλάση όπου ανήκει η διεύθυνση δικτύου που δόθηκε σαν πρώτη παράμετρος.
Στη συνέχεια, προσδιορίζεται ο τρόπος με τον οποίο θα φτάσουμε στο δίκτυο προορισμού: είτε δηλώνοντας τη διεύθυνση IP του interface του επόμενου γειτονικού δρομολογητή (πρώτη σύνταξη) ή δηλώνοντας το interface του τρέχοντα δρομολογητή μέσω του οποίου φεύγει το πακέτο.

Η διαχειριστική απόσταση επίσης είναι προαιρετική. Εάν δεν καθοριστεί, τότε παίρνει αυτόματα τιμή 0 ή 1, ανάλογα με το πώς συντάχθηκε η εντολή. Εάν χρησιμοποιείται η σύνταξη NextHopNeighboutIP, τότε παίρνει τιμή 1, ενώ αν δηλώνεται το interface, ο δρομολογητής αντιμετωπίζει τη διαδρομή σαν συνδεδεμένη και της δίνει τιμή 0.

Π.χ. για την τοπολογία 1, την οποία περιγράψαμε παραπάνω, εάν θέλουμε να ορίσουμε μια στατική διαδρομή στο router A προς το δίκτυο 192.168.3.0, μπορούμε να χρησιμοποιήσουμε μια από τις παρακάτω εναλλακτικές:

```
RouterA(config)# ip route 192.168.3.0 255.255.255.0 192.168.1.1
```

ή

```
RouterA(config)# ip route 192.168.3.0 255.255.255.0 e0
```

Στην πρώτη περίπτωση η διαχειριστική απόσταση της διαδρομής θα είναι 1, ενώ στη δεύτερη θα είναι 0

Σημειώνουμε εδώ ότι είναι δυνατόν να οριστούν πολλαπλές στατικές διαδρομές προς τον ίδιο προορισμό, με διαφορετικό administrative distance η καθεμία, όπως για παράδειγμα στην περίπτωση που έχουμε backup routes (οι οποίες θα πρέπει να πάρουν αριθμό μεγαλύτερο από την κύρια, ώστε να έχουν μικρότερη προτεραιότητα).

Η παράμετρος permanent ορίζει ότι η συγκεκριμένη διαδρομή θα πρέπει να παραμείνει μόνιμα στο routing table, ακόμα και αν υπάρχει πρόβλημα στο αντίστοιχο interface. Εάν δεν υπάρχει η παράμετρος permanent και κάποια στιγμή υπάρξει πρόβλημα στο συγκεκριμένο interface, τότε η διαδρομή αυτή θα αφαιρεθεί από τον πίνακα. Η παράμετρος permanent, αντίθετα, θα τη διατηρήσει στον πίνακα, αποτρέποντας τη χρήση κάποιας εναλλακτικής της (χρήσιμο σε ιδιαίτερες περιπτώσεις, όπως π.χ. για λόγους ασφαλείας).

Default Routes (προκαθορισμένες διαδρομές)
Οι προκαθορισμένες διαδρομές χρησιμοποιούνται για να καθορίσουν πού θα προωθούνται πακέτα που περιέχουν διευθύνσεις δικτύου τις οποίες δεν γνωρίζει ο δρομολογητής να προωθήσει με κάποιο άλλο τρόπο. Είναι πολύ σημαντικές, καθώς η τυπική συμπεριφορά ενός δρομολογητή όταν δεν γνωρίζει πού πρέπει να δρομολογηθεί ένα πακέτο είναι να το απορρίψει.

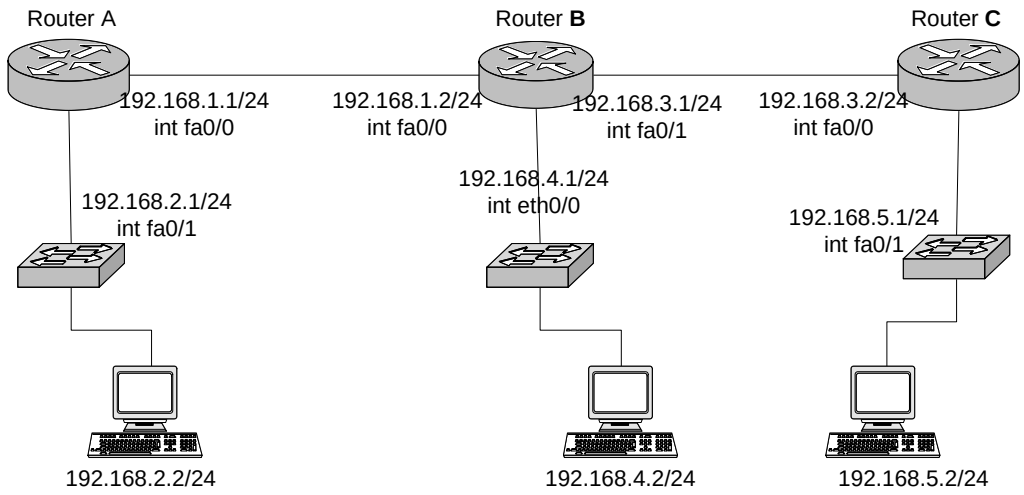
Ένα default route ορίζεται ως εξής:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 NextHopNeighbourIPAddress
```

ή

```
Router(config)# ip route 0.0.0.0 0.0.0.0 exitInterface
```

Συγκεντρωτικό Παράδειγμα:



Με δεδομένη την παραπάνω τοπολογία, θα δούμε πώς ρυθμίζονται και οι τρεις routers χρησιμοποιώντας στατική δρομολόγηση, ώστε όλοι οι υπολογιστές να μπορούν να επικοινωνήσουν ο ένας με τον άλλο.
Θεωρούμε ότι έχουν ήδη γίνει οι βασικές ρυθμίσεις στους δρομολογητές και ότι όλα τα interfaces είναι ενεργά.

Χρησιμοποιώντας αρχικά την εντολή **show ip route** σε καθένα από τους δρομολογητές για να επαληθεύσουμε τα τρέχοντα περιεχόμενα των πινάκων δρομολόγησης παίρνουμε τα ακόλουθα

αποτελέσματα:

```
routerA# 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

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1



routerB#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

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/1
C    192.168.4.0/24 is directly connected, Ethernet1/0

routerC#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

C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.5.0/24 is directly connected, FastEthernet0/1
```

Παρατηρούμε ότι οι τρεις routers ήδη έχουν καταγράψει αυτόματα διαδρομές για τα connected interfaces. Πρέπει λοιπόν τώρα να τους ενημερώσουμε για τα μη άμεσα συνδεδεμένα δίκτυα.

```
routerA#conf term

routerA#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
routerA(config)#ip route 192.168.3.0 255.255.255.0 fa0/0
routerA(config)#ip route 192.168.4.0 255.255.255.0 192.168.1.2
routerA(config)#ip route 192.168.5.0 255.255.255.0 192.168.1.2
routerA(config)#exit
```

Και επαληθεύουμε το configuration με την εντολή show ip route:

```
routerA#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

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
S    192.168.3.0/24 is directly connected, FastEthernet0/0
S    192.168.4.0/24 [1/0] via 192.168.1.2
S    192.168.5.0/24 [1/0] via 192.168.1.2
```

Με τον ίδιο τρόπο συνεχίζουμε με τη ρύθμιση των άλλων δυο routers.

```
routerB#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
routerB(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.1
routerB(config)#ip route 192.168.5.0 255.255.255.0 fa0/1
routerB(config)#exit
```

```
routerB#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

C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 [1/0] via 192.168.1.1
C    192.168.3.0/24 is directly connected, FastEthernet0/1
C    192.168.4.0/24 is directly connected, Ethernet1/0
S    192.168.5.0/24 is directly connected, FastEthernet0/1
```

```
routerC#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
routerC(config)#ip route 192.168.2.0 255.255.255.0 fa0/0
routerC(config)#ip route 192.168.1.0 255.255.255.0 fa0/0
routerC(config)#ip route 192.168.4.0 255.255.255.0 fa0/0
routerC(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
```

```
routerC#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

S    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 is directly connected, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
S    192.168.4.0/24 is directly connected, FastEthernet0/0
C    192.168.5.0/24 is directly connected, FastEthernet0/1
```

Επαλήθευση ρυθμίσεων στατικής δρομολόγησης και ανίχνευση λαθών

Εκτός της εντολής show ip route, την οποία είδαμε στο παράδειγμα, προκειμένου να επαληθεύσουμε την ορθή ρύθμιση ενός router, μπορούμε συμπληρωματικά να χρησιμοποιήσουμε τη γνωστή, πλέον, εντολή show running config. Στο παράδειγμά μας, η χρήση της θα δώσει το εξής αποτέλεσμα:

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

Current configuration : 507 bytes
!
version 12.3
no service password-encryption
!
hostname routerA
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.3.0 255.255.255.0 FastEthernet0/0
ip route 192.168.4.0 255.255.255.0 192.168.1.2
ip route 192.168.5.0 255.255.255.0 192.168.1.2
!
!
```

```
!!
line con 0
line vty 0 4
 login
!
end
```

Το μαρκαρισμένο τμήμα του κειμένου είναι αυτό που αφορά στη στατική δρομολόγηση. Παρατηρούμε ότι έχουν οριστεί χειροκίνητα τρεις διαδρομές, η πρώτη προς το δίκτυο 192.168.3.0 μέσω του interface fa0/0 και οι επόμενες δύο προς τα δίκτυα 4.0 και 5.0 με next hop το 192.168.1.2 (πρακτικά, δηλαδή, μέσω του fa0/0).

Για τον έλεγχο των ρυθμίσεων δρομολόγησης μπορούμε επίσης να χρησιμοποιήσουμε τις εντολές ping και traceroute. Η πρώτη εντολή, της οποίας η χρήση είναι ήδη γνωστή, θα επαληθεύσει κατά πόσον όλοι οι προορισμοί είναι ορατοί μεταξύ τους.

Η εντολή traceroute δίνει περισσότερες πληροφορίες, καθώς εμφανίζει βήμα προς βήμα όλους τους κόμβους που παρεμβάλλονται μεταξύ προορισμού και αφετηρίας, διευκολύνοντας με αυτό τον τρόπο την ανίχνευση του ακριβούς σημείου όπου εμφανίζεται το πρόβλημα. Π.χ. εάν εκτελέσουμε την εντολή traceroute από το routerA με προορισμό τον 192.168.5.1, βλέπουμε η επικοινωνία είναι επιτυχής, με ενδιάμεσα βήματα τους 192.168.1.2 (int fa0/0 στο routerB) και 192.168.3.2 (int fa0/0 στο router C).

```
routerA#traceroute 192.168.5.1
Type escape sequence to abort.
Tracing the route to 192.168.5.1

  1   192.168.1.2     8 msec    5 msec    5 msec
  2   192.168.3.2     8 msec    7 msec    6 msec
```

8.2 Δυναμικά Πρωτόκολλα Δρομολόγησης

Είδαμε στην προηγούμενη ενότητα πώς μπορούν να οριστούν διαδρομές σε ένα δίκτυο με τη χρήση τεχνικών στατικής δρομολόγησης. Μολονότι η ρύθμιση των δρομολογητών είναι σχετικά απλή, απαιτεί αρκετά βήματα και γίνεται εύκολα κατανοητό ότι σε μεγαλύτερα δίκτυα θα ήταν αρκετά σύνθετη και χρονοβόρα εργασία.

Επιπρόσθετα, στην περίπτωση αλλαγών στο δίκτυο (π.χ. προσθήκης ενός νέου δρομολογητή), θα πρέπει να ενημερωθούν χειροκίνητα οι ρυθμίσεις όλων των δρομολογητών.

Προκειμένου να μειωθεί το διαχειριστικό κόστος, ιδιαίτερα για μεγάλα και συχνά μεταβαλλόμενα δίκτυα, χρησιμοποιούνται τεχνικές δυναμικής δρομολόγησης. Με τη χρήση δυναμικών πρωτοκόλλων, οι δρομολογητές μπορούν να ενημερώνονται αυτόματα για αλλαγές στο δίκτυο, ανταλλάσσοντας δεδομένα δρομολόγησης με γειτονικούς δρομολογητές.

Τα δυναμικά πρωτόκολλα δρομολόγησης χωρίζονται γενικά σε τρεις κατηγορίες, ανάλογα με τις τεχνικές που που χρησιμοποιούν για την εύρεση διαδρομών και την ανταλλαγή πληροφορίας μεταξύ δρομολογητών.

Τα πρωτόκολλα της πρώτης κατηγορίας ονομάζονται πρωτόκολλα *διανύσματος απόστασης* (distance vector protocols) και σε αυτήν ανήκουν πρωτόκολλα όπως τα RIP/RIPv2 και IGRP. Η δεύτερη κατηγορία είναι τα πρωτόκολλα κατάστασης συνδέσμου (link state protocols), στην οποία ανήκουν

πρωτόκολλα όπως τα δεύτερη κατηγορία ανήκουν πρωτόκολλα όπως τα OSPF, NLSP. Στην τρίτη κατηγορία εντάσσονται πρωτόκολλα όπως το EIGRP, που συνδυάζουν στοιχεία από τις δυο προηγούμενες κατηγορίες και ονομάζονται *υβριδικά.*

Σε σύνθετα δίκτυα, με πολλαπλές διαδρομές μεταξύ των δρομολογητών, εμφανίζεται το πρόβλημα της επιλογής μιας εξ'αυτών προκειμένου να προωθηθεί ένα πακέτο. Ήδη έχουμε δει ένα τρόπο αντιμετώπισης του προβλήματος, με τη χρήση της έννοιας της διαχειριστικής απόστασης. Η διαχειριστική απόσταση, όμως, εφαρμόζεται μεταξύ διαφορετικών πρωτοκόλλων, δηλαδή για παράδειγμα στην περίπτωση που έχουμε τρεις εναλλακτικές διαδρομές μεταξύ των κόμβων Α και Β και η πρώτη είναι στατική, η δεύτερη έχει γίνει γνωστή μέσω RIP και η τρίτη μέσω IGRP, τότε θα χρησιμοποιηθεί η διαχειριστική απόσταση προκειμένου να επιλεγεί διαδρομή. Η διαχειριστική απόσταση όμως δεν λύνει το πρόβλημα που προκύπτει όταν υπάρχουν δύο εναλλακτικές τις οποίες έχει μάθει ο δρομολογητής μέσω του ίδιου πρωτοκόλλου.
Για να αντιμετωπιστεί η περίπτωση αυτή, τα δυναμικά πρωτόκολλα δρομολόγησης υιοθετούν ένα ή περισσότερα μεγέθη, τα οποία ονομάζονται μετρικές και χρησιμοποιούνται ως μέτρα αξιολόγησης των διαδρομών ώστε να επιλεγεί η προτιμότερη κατά περίπτωση. Στον ακόλουθο πίνακα παρουσιάζονται οι μετρικές που χρησιμοποιούν διάφορα πρωτόκολλα σε IP δίκτυα.

Μετρική	Πρωτόκολλο	Περιγραφή
Εύρος Ζώνης (bandwidth)	EIGRP, IGRP	Χωρητικότητα γραμμής σε Kbps
Κόστος (cost)	OSPF	Παράγωγο μέγεθος βασισμένο στο bandwidth της γραμμής
Καθυστέρηση (delay)	EIGRP, IGRP	Χρόνος που απαιτείται ώστε να φτάσει ένα πακέτο στον προορισμό του
Αριθμός βημάτων (hop count)	RIP (v1,v2)	Αριθμός routers που πρέπει να περάσει το πακέτο μέχρι να φτάσει στον προορισμό
MTU (Maximum Transmission Unit)	IGRP, EIGRP	Η διαδρομή που υποστηρίζει τα μεγαλύτερα μεγέθη πλαισίων
Φόρτος (load)	IGRP, EIGRP	Η διαδρομή με το μικρότερο βαθμό χρήσης
Αξιοπιστία (reliability)	EIGRP, IGRP	Η διαδρομή με το μικρότερο αριθμό λαθών ή το μικρότερο χρόνο εκτός λειτουργίας

8.3 Πρωτόκολλα Distance Vector

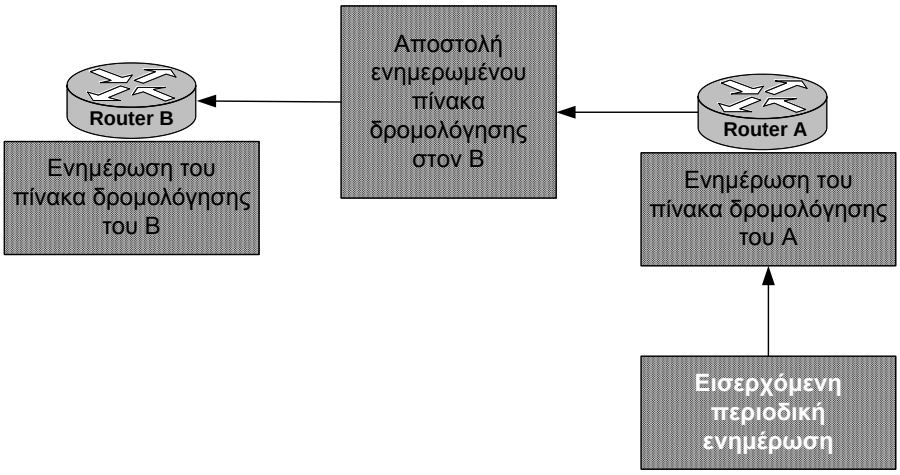
Τα απλούστερα πρωτόκολλα είναι αυτά που υιοθετούν την προσέγγιση distance vector. Αυτά ορίζουν ένα διάνυσμα απόστασης και κατεύθυνσης προκειμένου να ανακαλύψουν μονοπάτια προς

συγκεκριμένους προορισμούς, χρησιμοποιώντας τον αλγόριθμο Bellman-Ford.
Οι δρομολογητές που έχουν οριστεί να λειτουργούν με πρωτόκολλα distance vector μαθαίνουν πληροφορίες δρομολόγησης από τους γειτονικούς τους routers, γι'αυτό και η δρομολόγηση με τεχνικές distance vector είναι επίσης γνωστή ως δρομολόγηση με φήμες (*routing by rumour*).

Τα distance vector πρωτόκολλα είναι σχετικά απλά στη ρύθμιση και τον έλεγχό τους και καταναλώνουν περιορισμένους υπολογιστικούς πόρους. Τα πιο τυπικά distance vector πρωτόκολλα (τα οποία και θα αναλύσουμε στη συνέχεια) είναι τα RIP v1 & v2 και το IGRP.

Βασικές αρχές λειτουργίας

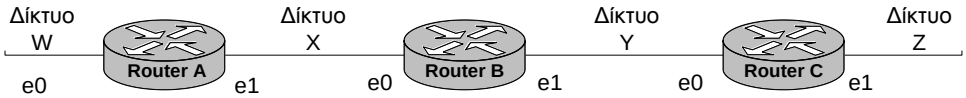
Στα πρωτόκολλα distance vector, κάθε δρομολογητής ανά τακτά χρονικά διαστήματα στέλνει τον πίνακα δρομολόγησής του (ολόκληρο ή τμήματά του, ανάλογα με το πρωτόκολλο και τις εκάστοτε συνθήκες) στους γειτονικούς του routers. Το ίδιο γίνεται και όταν κάποιος δρομολογητής ενημερωθεί για μια αλλαγή στην τοπολογία του δικτύου (π.χ. όταν κάποια σύνδεση είναι νεκρή). Αυτές οι περιοδικές ή κατά περίπτωση ενημερώσεις που προωθεί κάθε δρομολογητής στους γειτονικούς του ονομάζονται routing updates και εκπέμπονται (με διεύθυνση προορισμού 255.255.255.255) σε όλα τα interfaces με τα οποία είναι συνδεδεμένος.



Ας θεωρήσουμε μια περιοχή δικτύου στην οποία ανήκουν πολλοί δρομολογητές. Ο δρομολογητής A στέλνει τον πίνακα δρομολόγησής του στο B, στον οποίο περιέχονται διαδρομές συσχετισμένες με μια μετρική, καθώς και με μια τιμή χρόνου η οποία αντιπροσωπεύει την «ηλικία» της πληροφορίας (δηλ. το χρόνο που έχει περάσει από την απόκτησή της).
Ο B ενημερώνει τη μετρική της διαδρομής (π.χ. στην περίπτωση του πρωτοκόλλου RIP, αυξάνει το hop count κατά 1) και κατόπιν αξιολογεί την πληροφορία για τη διαδρομή προκειμένου να αποφασίσει εάν πρέπει να τη συμπεριλάβει στον πίνακα δρομολόγησής του ή όχι.
Εάν η διαδρομή που περιέχεται στο update είναι καλύτερη (έχει δηλαδή καλύτερη μετρική) από αυτή που περιέχει ο πίνακας του B, τότε αντικαθιστά την υπάρχουσα διαδρομή. Εάν είναι χειρότερη τότε αγνοείται.
Σε περίπτωση που η εισερχόμενη πληροφορία για μια διαδρομή είναι ακριβώς η ίδια με την υπάρχουσα, τότε η τιμή χρόνου για τη συγκεκριμένη διαδρομή μηδενίζεται.

Εάν η εισερχόμενη πληροφορία είναι μια εναλλακτική διαδρομή αλλά με την ίδια μετρική με μια υπάρχουσα, η εναλλακτική διαδρομή προστίθεται στον πίνακα δρομολόγησης ως ισοδύναμη (equal-cost path), και βρίσκει εφαρμογή σε περιπτώσεις εξισορρόπησης φόρτου (load balancing).
Μόλις ολοκληρωθούν οι διαδικασίες αξιολόγησης του update και ενημέρωσης του routing table του B, ο ενημερωμένος πίνακας δρομολόγησης αποστέλλεται ως ένα νέο update προς το router C. Η ίδια διαδικασία επαναλαμβάνεται από κάθε router προς όλους τους γειτονικούς του. Με αυτό τον τρόπο, σταδιακά επιτυγχάνεται η ενημέρωση όλων των δρομολογητών και η σύγκλισή τους σε ένα ενιαίο σύνολο πληροφορίας (τουλάχιστον μέχρι να συμβεί η επόμενη αλλαγή στην τοπολογία του δικτύου). Πρέπει όμως να παρατηρήσουμε ότι η πληροφορία δεν βρίσκεται συγκεντρωμένη σε ένα και μόνο δρομολογητή, παρά είναι κατανεμημένη μεταξύ όλων των δρομολογητών του δικτύου, καθώς κάθε router βλέπει μόνο τους γειτονικούς του.

Ένα απλουστευμένο παράδειγμα



Ας θεωρήσουμε το δίκτυο του σχήματος, το οποίο μόλις έχει τεθεί σε λειτουργία και δεν έχουν ανταλλαγεί routing updates μεταξύ των δρομολογητών, με αποτέλεσμα κάθε router να γνωρίζει μόνο τα άμεσα συνδεδεμένα με αυτόν δίκτυα, τα οποία έχουν μηδενικό hop count.

Όταν ενεργοποιηθούν οι routers, οι πίνακες δρομολόγησης έχουν ως εξής:

Router A			Router B			Router C		
Δίκτυο προορισμού	Interface	Hop Count	Δίκτυο προορισμού	Interface	Hop Count	Δίκτυο προορισμού	Interface	Hop Count
W	e0	0	X	E0	0	Y	e0	0
X	e1	0	Y	E1	0	Z	e1	0

Στο πρώτο βήμα, ο A εκπέμπει ενημέρωση προς το γειτονικό του B, ο C εκπέμπει επίσης ενημέρωση προς το B και ο B εκπέμπει ενημερώσεις προς τον A και το C.
Ο A λαμβάνει την ενημέρωση από το B, η οποία περιέχει τα δίκτυα X και Y. Ο A αυξάνει τις μετρικές των X και Y κατά 1 και στη συνέχεια αγνοεί το δίκτυο X (το οποίο τώρα πια έχει μετρική 1, δηλαδή χειρότερη από την υπάρχουσα εγγραφή στον πίνακα του A) και προσθέτει την εγγραφή για το δίκτυο Y, το οποίο δεν γνωρίζει.
Ο C λαμβάνει επίσης την ενημέρωση, η οποία περιέχει τα δίκτυα X και Y. Ο C αυξάνει τις μετρικές των X και Y κατά 1 και στη συνέχεια αγνοεί το δίκτυο Y (το οποίο τώρα πια έχει μετρική 1, δηλαδή χειρότερη από την υπάρχουσα εγγραφή στον πίνακα του A) και προσθέτει την εγγραφή για το δίκτυο X, το οποίο δεν γνωρίζει.

Ο B δέχεται ενημερώσεις ταυτόχρονα και από τον A και απο το C. Από τον A μαθαίνει για τα δίκτυα W και X και από τον C μαθαίνει για τα δίκτυα Y και Z. Αυξάνει το hop count τους κατά 1 και συγκρίνει τις εγγραφές με τον πίνακά του. Αγνοεί τα X και Y (τα οποία έχουν hop count 1, ενώ οι αντίστοιχες εγγραφές του B έχουν hop count 0) και προσθέτει τα δίκτυα W και Z.

Μετά λοιπόν από αυτό τον κύκλο ανταλλαγών ενημερώσεων, οι πίνακες έχουν ως εξής:

Router A			Router B			Router C		
Δίκτυο προορισμού	Interface	Hop Count	Δίκτυο προορισμού	Interface	Hop Count	Δίκτυο προορισμού	Interface	Hop Count
W	e0	0	X	e0	0	Y	e0	0
X	e1	0	Y	e1	0	Z	e1	0
Y	e1	1	W	e0	1	X	e0	1
			Z	e1	1			

Μόλις έρθει ο χρόνος για την επόμενη περιοδική ενημέρωση, ο κύκλος ανταλλαγής ενημερώσεων ξεκινά ξανά. Σε αυτό το βήμα, ο A μαθαίνει για το δίκτυο Z και ο C για το δίκτυο W. Η πληροφορία που αφορά στα υπόλοιπα δίκτυα αγνοείται, καθώς έχει ήδη καταγραφεί στους πίνακες δρομολόγησης όλων των routers.

Router A			Router B			Router C		
Δίκτυο προορισμού	Interface	Hop Count	Δίκτυο προορισμού	Interface	Hop Count	Δίκτυο προορισμού	Interface	Hop Count
W	e0	0	X	e0	0	Y	e0	0
X	e1	0	Y	e1	0	Z	e1	0
Y	e1	1	W	e0	1	X	e0	1
Z	e1	2	Z	e1	1	W	e0	2

Σε αυτό το βήμα πια έχει ολοκληρωθεί η ανταλλαγή πληροφορίας μεταξύ των routers. Οι επόμενες περιοδικές ενημερώσεις δεν επηρεάζουν τις ρυθμίσεις, καθώς δεν περιέχουν νέα πληροφορία και οι πίνακες θα παραμείνουν αμετάβλητοι, μέχρι τη στιγμή που θα συμβεί κάποια αλλαγή στην τοπολογία του δικτύου.

Προβλήματα της τεχνικής distance vector

Τα πρωτόκολλα distance vector, παρά τα προφανή πλεονεκτήματά τους όσον αφορά στην κατανάλωση υπολογιστικών πόρων και την ευκολία ρύθμισης, χαρακτηρίζονται από δύο μειονεκτήματα: συγκλίνουν πολύ αργά και είναι επιρρεπή σε προβλήματα βρόχου. Τα μειονεκτήματα αυτά αποκτούν ιδιαίτερη σημασία όταν έχουμε να κάνουμε με μεγάλα δίκτυα.

Σύγκλιση

Με τον όρο σύγκλιση (convergence) περιγράφουμε την κατάσταση εκείνη κατά την οποία όλοι οι δρομολογητές είναι ενήμεροι για την τρέχουσα τοπολογία του δικτύου. Η σύγκλιση δεν είναι αυτόματη, αλλά επιτυγχάνεται μετά από αρκετούς κύκλους ενημερώσεων.

Στο προηγούμενο παράδειγμα είδαμε μια τέτοια περίπτωση σύγκλισης σε ένα απλό δίκτυο. Η σύγκλιση απαίτησε δύο κύκλους περιοδικών ενημερώσεων.
Ας θεωρήσουμε ότι οι περιοδικές ενημερώσεις εκπέμπονται κάθε 30 δευτερόλεπτα (τυπικός χρόνος για το πρωτόκολλο RIP). Η πρώτη ενημέρωση εκπέμφθηκε με την ενεργοποίηση των δρομολογητών και η δεύτερη τριάντα δευτερόλεπτα αργότερα. Αυτό σημαίνει ότι η σύγκλιση επιτεύχθηκε λίγο περισσότερο από τριάντα δευτερόλεπτα. Ο χρόνος μπορεί να μη φαίνεται μεγάλος, όμως εξετάζουμε ένα δίκτυο τριών μόλις δρομολογητών. Σε ένα μεγάλο δίκτυο, με δεκάδες ή εκατοντάδες δρομολογητές (π.χ το

δίκτυο ενός ISP), η σύγκλιση μπορεί να απαιτήσει διάστημα αρκετών λεπτών, κατά τη διάρκεια του οποίου η επικοινωνία με μεγάλα τμήματα του δικτύου θα είναι προβληματική.

Υπάρχουν δυο λύσεις που μπορούν να εφαρμοστούν στο πρόβλημα της σύγκλισης Μια λύση είναι η χρήση μικρότερων διαστημάτων για τα περιοδικά updates, π.χ αντί να εκπέμπονται κάθε 30 δεύτερα, να εκπέμπονται κάθε 5. Αυτό θα συντόμευε αρκετά το χρόνο σύγκλισης, όμως για μεγάλα δίκτυα και πάλι ο χρόνος κατά τον οποίο το δίκτυο δεν θα ήταν αξιόπιστο θα ήταν αρκετά μεγάλος. Επιπρόσθετα, αυτή η μέθοδος εισάγει εξαιρετικά μεγάλο φόρτο στο δίκτυο, καθώς πολλαπλασιάζεται ο όγκος των δεδομένων που ανταλλάσσονται (και μάλιστα με τη μορφή broadcasts, τα οποία απασχολούν όλο το δίκτυο).
Μια άλλη λύση είναι η τεχνική των πυροδοτούμενων ενημερώσεων (triggered updates). Αυτές μπορούν να εκπέμπονται συμπληρωματικά προς τις περιοδικές ενημερώσεις. Οι δρομολογητές θα συνεχίσουν να εκπέμπουν περιοδικές ενημερώσεις στα προκαθορισμένα διαστήματα, όταν όμως συμβεί κάποια αλλαγή στις ρυθμίσεις τους, θα παράγουν άμεσα ένα update χωρίς να χρειαστεί να περιμένουν να λήξει το διάστημα.
Αυτή η τεχνική μπορεί να επιταχύνει τη σύγκλιση (κυρίως στην περίπτωση που τεθεί κάποια σύνδεση εκτός λειτουργίας και όχι τόσο στην αρχική εγκατάσταση του δικτύου), κρύβει όμως μια παγίδα: στην περίπτωση που κάποια σύνδεση ανεβοκατεβαίνει, τότε θα παράγονται πολύ πυκνά triggered updates τα οποία θα πλημμυρίζουν το δίκτυο.

Routing Loops (βρόχοι/κύκλοι δρομολόγησης)
Ένα άλλο πρόβλημα των distance vector πρωτοκόλλων είναι οι βρόχοι δρομολόγησης, κυκλικές δηλαδή παραπομπές από ένα router σε ένα άλλο οι οποίες καταλήγουν στο δρομολογητή από όπου ξεκίνησε η διαδικασία.

Ας θεωρήσουμε την παραπάνω τοπολογία δικτύου. Αρχικά, ο routerA στέλνει update που περιέχει διαδρομή για το δίκτυο 192.168.4.0, το οποίο λαμβάνει ο router B. Ο B καταγράφει την πληροφορία στο routing table του και εκπέμπει update προς το C, ο οποίος καταγράφει την πληροφορία στο δικό του routing table. Αμέσως μετά, ο router A τίθεται εκτός λειτουργίας, ενώ ο C στέλνει το ενημερωμένο routing table στο B. Καθώς η διαδρομή που γνώριζε ο B για να φτάσει στο δίκτυο 192.168.4.0 μέσω του A δεν υπάρχει πια, αντικαθίσταται με αυτή που έμαθε από το C. Τα routing tables των B και C εκείνη τη στιγμή έχουν ως εξής:

Router B			Router C		
Δίκτυο προορισμού	Interface	Hop Count	Δίκτυο προορισμού	Interface	Hop Count
192.168.1.0	e0	0	192.168.1.0	e0	1
192.168.2.0	e1	0	192.168.2.0	e0	0
192.168.3.0	e1	2	192.168.3.0	e1	0
192.168.4.0	e1	2	192.168.4.0	e0	2

Ο Β και ο C, όμως, συνεχίζουν να περιλαμβάνουν πληροφορία για το δίκτυο 192.168.4.0, την οποία και στέλνουν με το επόμενο περιοδικό update ο ένας στον άλλο, δημιουργώντας σύγχυση. Ο Β λέει στο C ότι γνωρίζει μια διαδρομή προς το 192.168.4.0 μέσω του C. Ο C λέει στο Β ότι γνωρίζει μια διαδρομή προς το 192.168.4.0 μέσω του Β. Αυτό έχει ως αποτέλεσμα να μην μπορεί να συμπεράνει κανείς τί συμβαίνει με το δίκτυο 192.168.4.0 και το router Α.

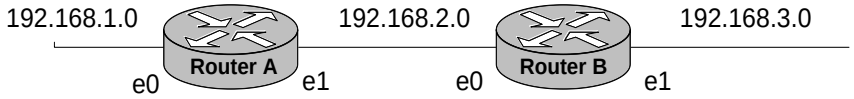
Το πρόβλημα των βρόχων αντιμετωπίζεται με διάφορες τεχνικές, τις οποίες θα δούμε στην πορεία.

Μέγιστος αριθμός βημάτων (Maximum Hop Count)

Όταν σε ένα δίκτυο υπάρχουν τέτοια routing loops, τα πακέτα δεδομένων που αποστέλλονται παγιδεύονται εντός του κύκλου και ταξιδεύουν συνεχώς από τον ένα router στον άλλο, καταναλώνοντας bandwidth και υπολογιστική ισχύ. Το πρόβλημα αντιμετωπίζεται με την εισαγωγή της τιμής TTL (Time To Live) στο header του πακέτου. Η τιμή TTL ξεκινά από ένα προκαθορισμένο ακέραιο αριθμό και με κάθε hop μειώνεται κατά 1. Εάν η τιμή αυτή φτάσει το 0, τότε ο router που θα το παραλάβει με μηδενική τιμή το απορρίπτει και σταματά να το προωθεί.
Βέβαια, η τεχνική αυτή δεν λύνει το πρόβλημα του βρόχου, ο οποίος εξακολουθεί να υφίσταται. Πρόκειται περισσότερο για μια πρόχειρη μέθοδο να αντιμετωπιστούν τα συμπτώματα. Επιπλέον, σε μεγάλα δίκτυα όπου οι διαδρομές είναι μεγάλες, πιθανά να απορρίπτονται και απολύτως έγκυρα πακέτα, εάν ξεπεράσουν το maximum hop count που έχει οριστεί.

Split Horizon

Η τεχνική split horizon ορίζει ότι όταν ένας router λάβει ένα update από ένα δεύτερο, δεν θα του επιστρέψει την πληροφορία με την επόμενη ενημέρωση. Αυτό είναι εφικτό ελέγχοντας το interface από το οποίο προήλθε η ενημέρωση.

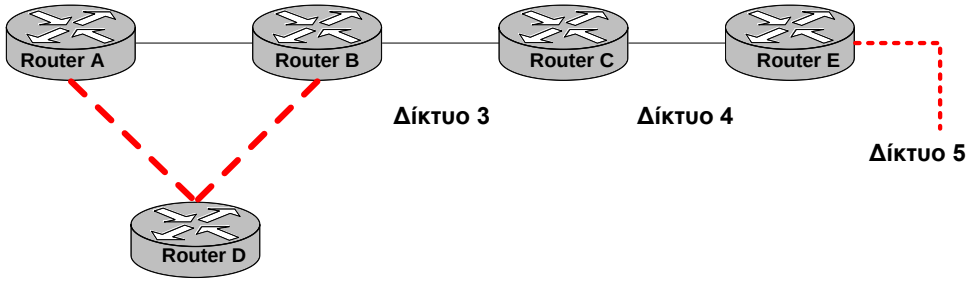


Έστω ότι ο Α στέλνει ενημέρωση για το δίκτυο 192.168.1.0 στο Β από το interface e1. Το interface e0 του Α στη συνέχεια τίθεται εκτός λειτουργίας.
Ο Α λαμβάνει ενημέρωση από το Β, η οποία ορίζει ότι ο Β γνωρίζει ένα μονοπάτι προς το δίκτυο 192.168.1.0 μέσω του interface (b)e0. Προφανώς εδώ το δίκτυο κινδυνεύει να πέσει σε κύκλο.
Με την τεχνική split horizon, η πληροφορία του Β σχετικά με το δίκτυο 192.168.1.0 δεν θα προωθηθεί πίσω στο interface e0 (από όπου και παρελήφθη) και η διαδρομή προς το 192.168.1.0 θα παρουσιάζεται (ορθά) ως εκτός λειτουργίας.

Route Poisoning

Η τεχνική route poisoning ορίζει ότι, όταν ένας router ανιχνεύσει ότι μια από τις άμεσα συνδεδεμένες σε αυτόν διαδρομές έχει πρόβλημα, τότε της αποδίδει μια απείρως μεγάλη μετρική, ώστε να μην επιλέγεται ποτέ (το συγκεκριμένο δίκτυο, δηλαδή, είναι μη προσβάσιμο).
Όταν ένας router στέλνει ενημέρωση που περιέχει «δηλητηριασμένη» διαδρομή στους γείτονές του, τότε οι γείτονες επιστρέφουν την πληροφορία στον αρχικό router, προκειμένου να επιβεβαιωθεί ότι

όλοι οι γείτονες έλαβαν το update για την poisoned route.



Παράδειγμα:
Έστω ότι το δίκτυο 5 τίθεται εκτός λειτουργίας. Μόλις το ανιχνεύσει ο router E, τότε «δηλητηριάζει» τη διαδρομή, ορίζοντάς της απόσταση 16 hops (unreachable) και ενημερώνει το C. Πλέον, τυχόν λανθασμένη πληροφορία διαδρομής σχετικά με το δίκτυο 5 που θα λάβει ο C μέσω του B δεν τον επηρεάζει. Οταν ο C λάβει το route poisoning από τον E, του επιστρέφει ένα update που ονομάζεται poison reverse για να επιβεβαιωθεί ότι η πληροφορία για τη δηλητηριασμένη διαδρομή παρελήφθη

Hold-Down Timers
Προκειμένου να δοθεί αρκετός χρόνος ώστε να προωθηθεί η δηλητηριασμένη διαδρομή και να βεβαιωθεί ότι δεν προκύπτουν βρόχοι για όσο διάστημα διαρκεί η ενημέρωση, οι δρομολογητές υλοποιούν το μηχανισμό hold-down. Αυτό σημαίνει ότι για ένα προκαθορισμένο διάστημα, η διαδρομή αυτή θα παραμείνει ανενεργή (δηλητηριασμένη) στους πίνακες δρομολόγησης. Το διάστημα αυτό συνήθως είναι το τριπλάσιο του διαστήματος περιοδικών ενημερώσεων.
Πώς λειτουργεί ο μηχανισμός hold-down:
Όταν ένας router A παραλάβει ένα update από ένα γείτονα, που ενημερώνει ότι ένα δίκτυο πλέον δεν είναι προσβάσιμο, ο A χαρακτηρίζει τη διαδρομή ως μη προσβάσιμη και ξεκινά το holddown timer.

- Εάν ο router λάβει μια ενημέρωση από **τον ίδιο** γείτονα, που πληροφορεί ότι η διαδρομή είναι ξανά ενεργή, πριν λήξει ο timer, τότε η διαδρομή χαρακτηρίζεται ως προσβάσιμη και ο timer αφαιρείται.
- Εάν φτάσει μια ενημέρωση από ένα άλλο router που έχει καλύτερη μετρική από αυτή της προβληματικής διαδρομής, τότε ο A χαρακτηρίζει τη διαδρομή προσβάσιμη και αφαιρεί τον timer
- Εάν φτάσει μια ενημέρωση από ένα άλλο router με χειρότερη μετρική από αυτή της προβληματικής διαδρομής, αυτή αγνοείται.

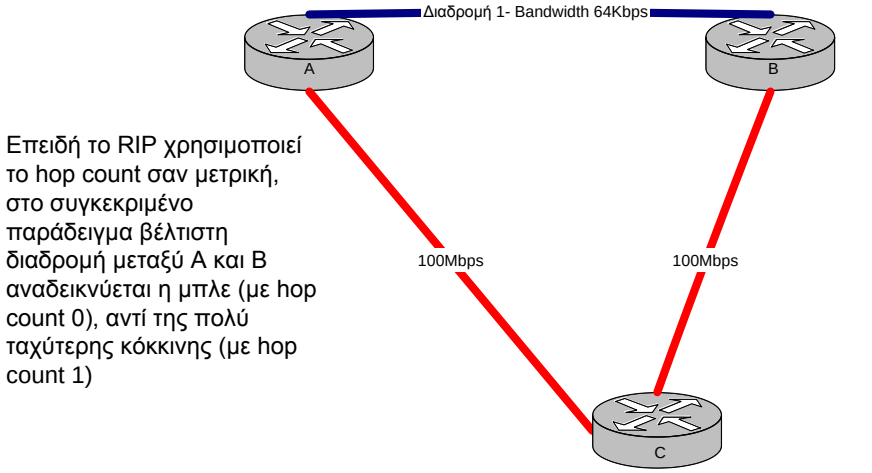
8.4 Το πρωτόκολλο RIP

Το πρωτόκολλο RIP είναι ένα από τα πιο γνωστά πρωτόκολλα IGP. Παρόλο που θεωρείται πια ξεπερασμένο, παραμένει ακόμα δημοφιλές λόγω της ευκολίας ρύθμισής του και λόγω του ότι όλοι πρακτικά οι σύγχρονοι routers το υποστηρίζουν (τουλάχιστον την έκδοση v1).
Είναι πρωτόκολλο distance vector και χρησιμοποιεί σαν μετρική τα hop counts. Υπάρχουν δυο εκδόσεις του, το RIP v1 και RIP v2, των οποίων τις διαφορές θα δούμε στη συνέχεια.

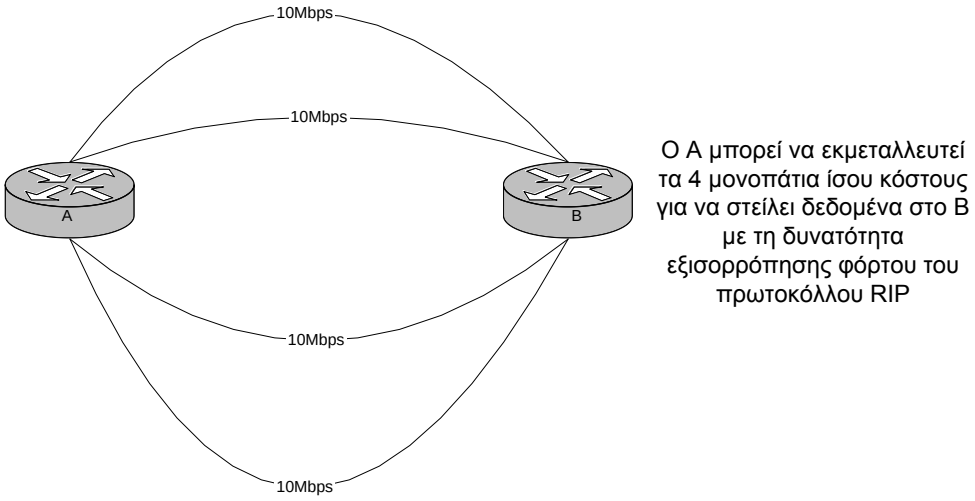
RIP v1
Το RIPv1 λειτουργεί στέλνοντας περιοδικά updates κάθε 30 δευτερόλεπτα, και ενσωματώνει τη μέθοδο split horizon καθώς και hold-down timers με περίοδο 180 δευτερόλεπτα. Τα updates στέλνονται σαν broadcasts στη διεύθυνση 255.255.255.255 (κάτι το οποίο εγκυμονεί τον κίνδυνο

broadcast floods σε περίπτωση προβληματικών συνδέσεων). Δεν υποστηρίζει κάποια μορφή αυθεντικοποίησης.

Χρησιμοποιεί, όπως είπαμε, τα hop counts σαν μετρική, και ορίζει το maximum hop count στα 15 hops και τα 16 hops σαν infinite distance (non-reachable nodes). Η επιλογή του hop count δεν είναι πάντα η καλύτερη δυνατή μετρική, κάτι το οποίο φαίνεται στο ακόλουθο παράδειγμα:



Επίσης, υποστηρίζει load balancing μεταξύ διαδρομών ίσου κόστους (με default 4 και μέγιστο 6 διαδρομές). Αυτό έχει το πλεονέκτημα της βελτιωμένη απόδοση μέσω της εκμετάλλευσης του bandwidth πολλών διαδρομών, καθώς και της ταχύτερης σύγκλισης.



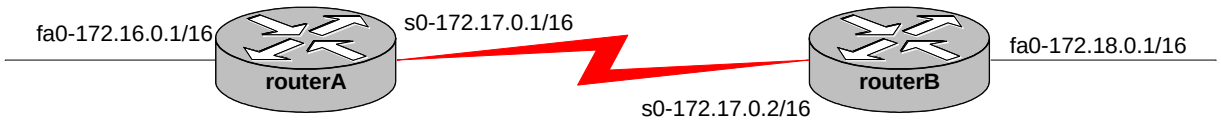
Το RIPv1 είναι ένα classful πρωτόκολλο, λειτουργεί δηλαδή με ολόκληρες κλάσεις διευθύνσεων και όχι με υποδίκτυα. Στα updates του RIPv1 δεν περιέχεται το subnet mask. Δεν δέχεται πολλαπλές μάσκες για το ίδιο δίκτυο και δεν μπορεί να υποστηρίξει σύνθετα σχήματα subnetting ή μάσκες

μεταβλητού μεγέθους3. Θα δούμε πιο αναλυτικά τις ιδιαιτερότητες και τους περιορισμούς που επιβάλλει η classful προσέγγιση του RIPv1 στη συνέχεια, ενώ επίσης θα δούμε πώς το RIPv2 λύνει το πρόβλημα.

Πώς ενεργοποιούμε το πρωτόκολλο RIP

Το πρωτόκολλο RIP είναι απλό στη ρύθμισή του και απαιτεί δύο βασικές εντολές:
την εντολή router rip σε configure terminal mode και την εντολή network IP_Network_Number

Παράδειγμα



Έστω ότι πρέπει να ρυθμίσουμε το παραπάνω δίκτυο προκειμένου να γίνεται δρομολόγηση με το πρωτόκολλο RIPv1. Θεωρούμε ότι ήδη έχουν ρυθμιστεί τα interfaces με τις διευθύνσεις που φαίνονται στο σχήμα.
Η ενεργοποίηση του RIPv1 γίνεται ως εξής:

Αρχικά ορίζουμε στο routerA ότι ρυθμίζουμε το πρωτόκολλο RIP.

```
routerA#configure terminal
routerA(config)#router rip
```

Στη συνέχεια θα πρέπει να δηλώσουμε στο routerA τα δίκτυα για τα οποία θα λαμβάνει και θα στέλνει updates σύμφωνα με το RIP. Αυτά στο παράδειγμά μας είναι το δίκτυο 172.16.0.0 (δηλ. το δίκτυο στο οποίο είναι συνδεδεμένο το int e0) και το δίκτυο 172.17.0.0 (δηλ. το δίκτυο στο οποίο συνδέεται το int s0):

```
routerA(config-router)#network 172.16.0.0
routerA(config-router)#network 172.17.0.0
routerA(config-router)#exit
routerA(config)#exit
```

Στη συνέχεια, αποθηκεύουμε τις ρυθμίσεις στο startup configuration file:

```
routerA#copy running-config startup-config
```

Αντίστοιχες ρυθμίσεις πρέπει να γίνουν και στο routerB:

```
routerB#configure terminal
routerB(config)#router rip
```

[3] Γενικά το RIPv1 βλέπει μόνο τις default μάσκες, εκτός από την περίπτωση όπου έχουμε άμεσα συνδεδεμένα interfaces. Για αυτά, μπορεί να δει τη μάσκα και να τη χρησιμοποιήσει για την προώθηση των πακέτων σε υποδίκτυα, αλλά όχι και να την συμπεριλάβει σε ένα routing update που θα αποστείλει σε κάποιο άλλο router.

```
routerB(config-router)#network 172.17.0.0
routerA(config-router)#network 172.18.0.0
routerB(config-router)#exit
routerB(config)#exit
routerB#copy running-config startup-config
```

Με αυτό το βήμα έχουν ολοκληρωθεί οι υποχρεωτικές ρυθμίσεις προκειμένου να λειτουργήσει το πρωτόκολλο RIP. Όλα τα interfaces που είναι ρυθμισμένα να συμμετέχουν είναι πλέον ενεργά και δέχονται και στέλνουν updates.

Αν δώσουμε την εντολή show ip route θα δούμε το αποτέλεσμα της ενεργοποίησης του RIP στους δυο routers:

```
routerA#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

C    172.16.0.0/16 is directly connected, FastEthernet0/0
C    172.17.0.0/16 is directly connected, Serial0/0
R    172.18.0.0/16 [120/1] via 172.17.0.2, 00:00:03, Serial0/0
```

Οι δυο πρώτες διαδρομές είναι αυτές που δηλώσαμε με την εντολή network στο routerA. Η τρίτη διαδρομή όμως, είναι αυτή που έχει μάθει μέσω του πρωτοκόλλου RIP από το router B. Αναλυτικά η εγγραφή έχει ως εξής:

Protocol	Destination Network	Administrative Distance/Hop Count	Next Hop Interface Address	Time since last update	Forwarding Interface
R *(RIP)*	172.18.0.0/16	120[4]/1	172.17.0.2 *(int s0/0 on routerB)*	00:00:03 *(3 seconds since update received)*	Serial 0/0

Αντίστοιχα αποτελέσματα δίνει η εντολή για το routerB:

```
routerB#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
```

[4] Όπως είδαμε στη σχετική ενότητα στην αρχή του κεφαλαίου, διαδρομές που μαθαίνει ο router μέσω του RIP έχουν default administrative distance 120.

```
       P - periodic downloaded static route

Gateway of last resort is not set

R    172.16.0.0/16 [120/1] via 172.17.0.1, 00:00:05, Serial0/0
C    172.17.0.0/16 is directly connected, Serial0/0
C    172.18.0.0/16 is directly connected, FastEthernet0/0
```

Επιπλέον της εντολής show ip route ο διαχειριστής του δικτύου έχει στη διάθεσή του και την εντολή **show ip protocols**, η οποία δίνει λεπτομερείς πληροφορίες για τα πρωτόκολλα δρομολόγησης που τρέχουν σε ένα router και τις ρυθμίσεις που έχουν.

```
routerA#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 21 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 1, receive any version
  Interface             Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0       1     2 1
  Serial1/0             1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
     172.16.0.0
     172.17.0.0
Passive Interface(s):
Routing Information Sources:
     Gateway         Distance      Last Update
     172.17.0.2           120      00:00:08
Distance: (default is 120)
```

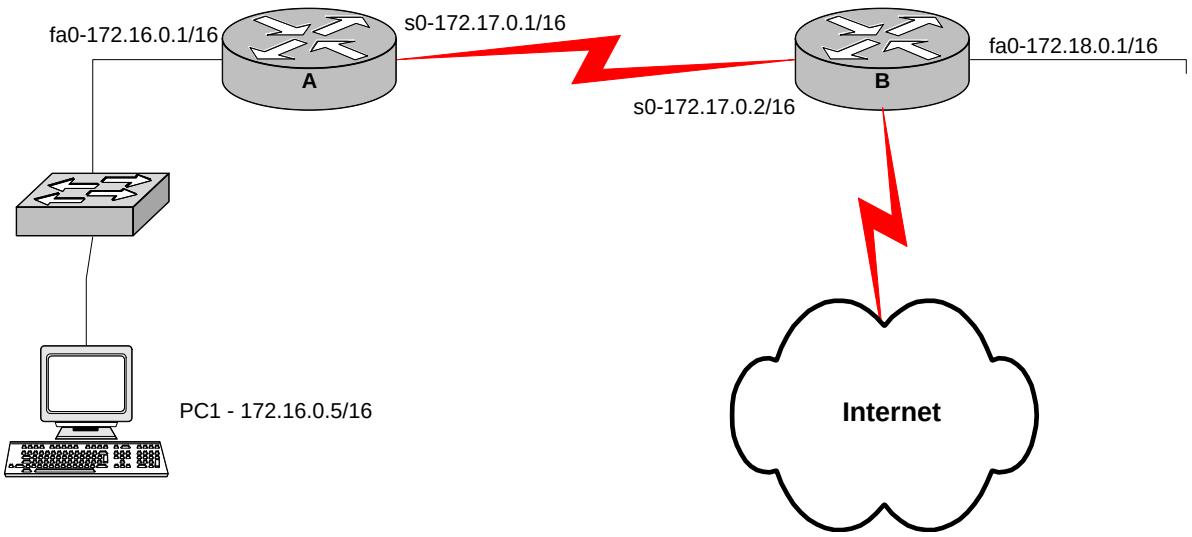
Η εκτέλεση της εντολής στο routerA μας ενημερώνει ότι τρέχει πρωτόκολλο RIP. Ο router αποστέλλει updates σύμφωνα με το RIPv1, δέχεται updates όμως και με το RIPv1 και το v2. Ο hold down timer είναι ρυθμισμένος στα 180 sec, τα περιοδικά updates στέλνονται κάθε 30 sec και το επόμενο update θα γίνει σε 21 sec. Δύο δίκτυα μετέχουν στη δρομολόγηση, το 172.16.0.0 και το 172.17.0.0. Το τελευταίο update που έλαβε ο Α ήταν από τον 172.17.2.0, πριν από 8 δευτερόλεπτα.

Default Routes

Εξετάζοντας ξανά το αποτέλεσμα της εντολής show ip route και στους δυο routers του προηγούμενου παραδείγματος, παρατηρούμε ότι εμφανίζεται το μήνυμα «Gateway of last resort is not set». Τί είναι όμως το gateway of last resort?

Οι δυο routers, μετά από τη ρύθμισή τους και την ανταλλαγή των updates, γνωρίζουν πώς να προωθήσουν δεδομένα σε όλα τα γνωστά δίκτυα. Τί γίνεται όμως όταν κάποιος host που συνδέεται π.χ. μέσω του routerA ζητήσει να στείλει δεδομένα σε κάποιο δίκτυο που ο Α δεν γνωρίζει;

Ας θεωρήσουμε, για παράδειγμα, το ακόλουθο σχήμα, το οποίο τροποποιεί την τοπολογία του προηγούμενου παραδείγματος. Στη συγκεκριμένη τοπολογία, ο routerB είναι και gateway router προς το Internet για όλο το δίκτυο της εταιρείας.



Οι δυο δρομολογητές είναι ρυθμισμένοι με τρόπο παρόμοιο με το προηγούμενο παράδειγμα και η εντολή show ip route δίνει τα εξής αποτελέσματα:

```
routerA#show ip route

... [παραλείπονται στοιχεία] ....

Gateway of last resort is not set

C    172.16.0.0/16 is directly connected, FastEthernet0/0
C    172.17.0.0/16 is directly connected, Serial0/0
R    172.18.0.0/16 [120/1] via 172.17.0.2, 00:00:03, Serial0/0


routerB#show ip route

... [παραλείπονται στοιχεία] ....

Gateway of last resort is not set

R    172.16.0.0/16 [120/1] via 172.17.0.1, 00:00:05, Serial0/0
C    172.17.0.0/16 is directly connected, Serial0/0
C    172.18.0.0/16 is directly connected, FastEthernet0/0
```

Έστω ότι ο host 172.16.0.5 πληκτρολογεί στο web browser του τη διεύθυνση www.dummywebsite.gr, η οποία μεταφράζεται στην IP address 195.251.227.4.
Σύμφωνα με όσα έχουμε δει, ο router A μόλις δεχτεί την αίτηση του host PC1, θα εξετάσει την ip address προορισμού του πακέτου δεδομένων και θα δει ότι δεν απευθύνεται σε κανένα από τα γνωστά του δίκτυα, με αποτέλεσμα να το απορρίψει, με αποτέλεσμα η σελίδα που ζήτησε ο PC1 να μην εμφανιστεί ποτέ. Το ίδιο θα γίνει και για οποιαδήποτε άλλη απόπειρα του host PC1 να αποκτήσει πρόσβαση σε κάποιο υπολογιστή στο διαδίκτυο, καθώς ο A δεν γνωρίζει πως να δρομολογήσει τα πακέτα.

Είναι προφανές ότι δεν είναι δυνατόν να οριστούν όλα τα πιθανά δίκτυα στο internet στα οποία θα μπορούσε να ζητήσει πρόσβαση κάποιος υπολογιστής εντός του δικτύου μας. Προκειμένου να μπορούν να εξυπηρετούνται σωστά παρόμοια αιτήματα, θα πρέπει να οριστεί κάποια προκαθορισμένη διαδρομή την οποία θα ακολουθούν τα πακέτα που απευθύνονται σε άγνωστα δίκτυα. Η διαδρομή αυτή ονομάζεται default route και το next hop interface μέσω του οποίου γίνεται η δρομολόγηση αυτής της διαδρομής ονομάζεται gateway of last resort.
Μια default route μπορεί να μαθευτεί δυναμικά, μέσω κάποιου άλλου router ή να οριστεί χειροκίνητα από το διαχειριστή. (Για να γίνει όμως εφικτή η δυναμική εκμάθησή της, θα πρέπει να έχει οριστεί χειροκίνητα σε ένα από τους router του δικτύου μας).
Η ρύθμιση της προκαθορισμένης διαδρομής είναι εφικτή με την εντολή
ip default-network network_address
ή
ip route 0.0.0.0 0.0.0.0 interface_ip_address [distance]
ή
ip route 0.0.0.0/0 interface_ip_address [distance]
Η εντολή ip default-network είναι classful (δηλαδή εάν οριστεί διαδρομή προς υποδίκτυο, λαμβάνεται υπόψη το κυρίως δίκτυο).
Στο συγκεκριμένο παράδειγμα, η ακόλουθη εντολή θα καθορίσει στο routerA ότι η κίνηση προς δίκτυα που δεν γνωρίζει θα πρέπει να δρομολογείται μέσω του B:

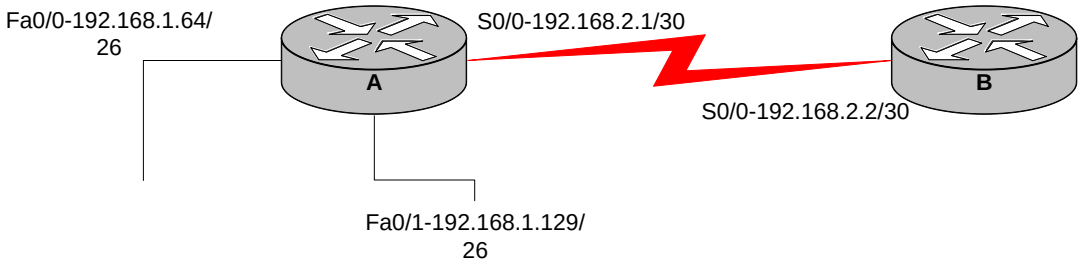
```
routerA(config)#ip route 0.0.0.0. 0.0.0.0 172.17.0.2
```

Η έξοδος της εντολής show ip route τώρα θα περιέχει τη γραμμή

```
Gateway of last resort is 172.17.0.2 to network 0.0.0.0
```

Αυτό υποδηλώνει ότι ο routerA θα δρομολογεί τα πακέτα που απευθύνονται προς δίκτυα που δεν γνωρίζει μέσω του 172.17.0.2

RIP Classful Route Table Construction
Αναφέραμε στα εισαγωγικά του πρωτοκόλλου RIP ότι είναι classful πρωτόκολλο. Αυτό σημαίνει ότι αναγνωρίζει ολόκληρες κλάσεις IP διευθύνσεων (A, B ή C) και όχι υποδίκτυα. Εάν π.χ. το δίκτυό μας είναι το 192.168.1.0/26 (με μάσκα δηλ. 255.255.255.192), άρα τα υποδίκτυά μας είναι τα 192.168.1.0/26, 192.168.1.64/26, 192.168.1.128/26, 192.168.1.192/26, δεν έχει νόημα να δώσουμε 4 φορές την εντολή network για καθένα από τα υποδίκτυα. Αρκεί να δώσουμε τη διεύθυνση του ευρύτερου δικτύου (network 192.168.1.0) και το RIP θα συμπεριλάβει όλα τα υποδίκτυα. Για την ακρίβεια, ακόμη και εάν δώσουμε ξεχωριστά την εντολή για κάθε υποδίκτυο, ο router εσωτερικά θα ανάγει τη διεύθυνση κάθε υποδικτύου σε αυτή του ευρύτερου δικτύου.



Παράδειγμα: Έστω ότι έχουμε το παραπάνω δίκτυο. Η ακόλουθη ρύθμιση δεν έχει νόημα:

```
Router(config-router)#network 192.168.1.64
Router(config-router)#network 192.168.1.128
```

καθώς ο router δεν διακρίνει μεταξύ των εγγραφών 172.16.1.0 και 172.16.2.0. Ο τρόπος με τον οποίο ερμηνεύει ο router τη ρύθμιση είναι σαν να έχουμε δώσει την εντολή:

```
Router(config-router)#network 192.168.1.0
```

Εάν επαληθεύσουμε τις ρυθμίσεις δίνοντας την εντολή show running config, θα πάρουμε το ακόλουθο αποτέλεσμα:

```
Alpha#show run
Building configuration...

Current configuration : 732 bytes
!
version 12.2
no service password-encryption
!
hostname Alpha
!
!
interface FastEthernet0/0
 ip address 192.168.1.65 255.255.255.192
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.129 255.255.255.192
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 192.168.2.1 255.255.255.252
 clock rate 56000
!
!
router rip
 network 192.168.1.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.2.2
!
!
[ παραλείπεται το υπόλοιπο ]
```

Επειδή όμως τα δίκτυα είναι άμεσα συνδεδεμένα στα interfaces του router (και όχι remote networks), ο router μπορεί να διαβάσει την πληροφορία της μάσκας και θα αναγνωρίσει τα υποδίκτυα, όπως μας δείχνει η εντολή show ip route:

```
Alpha#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 192.168.2.2 to network 0.0.0.0

     192.168.1.0/26 is subnetted, 2 subnets
C       192.168.1.64 is directly connected, FastEthernet0/0
C       192.168.1.128 is directly connected, FastEthernet0/1
     192.168.2.0/30 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, Serial0/0
S*   0.0.0.0/0 [1/0] via 192.168.2.2
```

Έτσι, εάν φτάσει στο router Alpha κάποιο πακέτο που προορίζεται για το δίκτυο 192.168.1.128, θα προωθηθεί από το σωστό interface (fa0/1), παρ'όλο που στο running configuration τα δύο δίκτυα εμφανίζονται σαν ένα.

Υπάρχει όμως μια περίπτωση που ο router δεν θα ανταποκριθεί σωστά:
Τί γίνεται εάν κάποιος host (έστω π.χ. ο 192.168.1.25) θελήσει να επικοινωνήσει με κάποιο υποδίκτυο του 192.168.1.0, το οποίο όμως δεν είναι αυστηρά δηλωμένο (π.χ. με το host 192.168.1.196, ο οποίος ανήκει στο δίκτυο 192.168.1.192); Το αναμενόμενο είναι, από τη στιγμή που ο router δεν γνωρίζει ακριβή διαδρομή, να το προωθήσει μέσω του default gateway 192.168.2.2. Αντίθετα όμως με ότι θα περίμενε κανείς, το πακέτο απορρίπτεται.
Αυτό γίνεται γιατί κατά την παραλαβή του πακέτου, ο router ελέγχει τη διεύθυνση προορισμού και βλέπει ότι ανήκει στο class C δίκτυο 192.168.1.0, για το οποίο υπάρχει match στο routing table. Στη συνέχεια εξετάζει τα υποδίκτυα, και βλέπει ότι το πακέτο δεν προορίζεται για κανένα από αυτά, οπότε και το απορρίπτει.
Το πρόβλημα λύνεται με τη χρήση της εντολής ip classless, η οποία δηλώνει στο router ότι κατά τη διαδικασία της πρώθησης πακέτων που προορίζονται για υποδίκτυα θα πρέπει να μην κάνει αναγωγή στην διεύθυνση του ευρύτερου class δικτύου, παρά να αντιμετωπίζει το υποδίκτυο ανεξάρτητα και αν δεν υπάρχει να το προωθεί στο default gateway.

Εδώ πρέπει να επισημάνουμε ότι η εντολή ip classless αφορά μόνο στην προώθηση των πακέτων και όχι στον τρόπο με τον οποίο χτίζεται το routing table και το πώς στέλνονται τα updates, άρα δεν μετατρέπει αυτόματα το RIPv1 σε classless πρωτόκολλο. Classless λειτουργία υποστηρίζεται με το RIPv2 το οποίο θα εξετάσουμε αργότερα.

Επαλήθευση ρυθμίσεων RIP και ανίχνευση λαθών

Έχουμε δει ήδη τις περισσότερες από τις εντολές με τις οποίες μπορούμε να επαληθεύσουμε τις σωστές ρυθμίσεις δρομολόγησης στην ενότητα για τη στατική δρομολόγηση καθώς και στην ενότητα για τη ρύθμιση του RIP. Βασικά εργαλεία είναι οι εντολές:

- Show running config
- Show ip route
- Show ip protocols

Επιπλέον των παραπάνω, για πιο σύνθετη αποσφαλμάτωση και παρακολούθηση βήμα προς βήμα υπάρχει επίσης η εντολή debug ip rip:

```
Router#debug ip rip
Alpha#RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.1.65)
```

```
RIP: build update entries
      network 192.168.1.128 metric 1
RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/1 (192.168.1.129)
RIP: build update entries
      network 192.168.1.64 metric 1

Alpha#RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.1.65)
RIP: build update entries
      network 192.168.1.128 metric 1
RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/1 (192.168.1.129)
RIP: build update entries
      network 192.168.1.64 metric 1
```

Η εντολή debug ip rip «παρακολουθεί» τη λειτουργία του RIP, και όταν υπάρχει κάποιο γεγονός (π.χ. ένα periodic update), εμφανίζει πληροφορίες για το γεγονός στην οθόνη terminal του router. Στο παράδειγμα εμφανίζονται δυο updates, τα οποία έχουν διαφορά χρόνου 30 δευτερόλεπτα το ένα από το άλλο.

Πρόσθετες ρυθμίσεις του RIP

Πέρα από τις ρυθμίσεις τις οποίες έχουμε δει μέχρις στιγμής, υπάρχει ένα σύνολο παραμέτρων στις οποίες ο διαχειριστής μπορεί αν θέλει να επέμβει:

- Μετρικές
- Hold Down Timers
- Periodic update timer
- Έκδοση RIP
- Σύμπτυξη διαδρομών (route summarization)
- Ενεργοποίηση/απενεργοποίηση Split Horizon
- Παράλληλη λειτουργία RIP-IGRP
- Σύνδεση σε WAN

Με την ακόλουθη εντολή ενεργοποιείται/απενεργοποιείται το split horizon, σε περίπτωση που κριθεί αναγκαίο:

```
Router(config-if)#no ip split horizon
```

Ο holddown timer πιθανά να χρειάζεται να ρυθμιστεί, καθώς μπορεί να αυξήσει σημαντικά το χρόνο σύγκλισης. Η default τιμή για το RIP είναι 180 δευτερόλεπτα, όμως μπορεί να μειωθεί, για μικρά δίκτυα, προκειμένου να βελτιωθεί ο χρόνος σύγκλισης του δικτύου. Η ρύθμιση γίνεται με τον εντολή:

```
      Router(config-router)#timers basic holddown [time]
Π.χ   router(config-router)#timers basic holddown 120
```

Ανάλογα ορίζονται και άλλοι χρόνοι. Η εντολή

```
Router(config-router)#timers basic update [time]
```

ορίζει κάθε πότε θα μεταδίδονται τα periodic updates.

Η εντολή

```
Router(config-router)#timers basic invalid [time]
```

ορίζει για πόσο χρονικό διάστημα μπορεί μια διαδρομή να παραμείνει στον πίνακα δρομολόγησης χωρίς να περιλαμβάνεται σε κάποια ενημέρωση. Εάν περάσει το χρονικό διάστημα που ορίζει ο invalid timer (ή expiration timer, ή timeout) χωρίς να ληφθεί κάποιο update που να περιλαμβάνει τη διαδρομή, τότε το hop count της γίνεται 16 και η διαδρομή χαρακτηρίζεται μη προσβάσιμη. Η default τιμή στο RIP είναι 180 δευτερόλεπτα.

Η εντολή

```
Router(config-router)#timers basic flush [time]
```

ορίζει για πόσο χρονικό διάστημα μπορεί μια unreachable διαδρομή να παραμείνει στον πίνακα δρομολόγησης χωρίς να περιλαμβάνεται σε κάποια ενημέρωση. Μια διαδρομή που είναι unreachable δεν διαγράφεται αυτομάτως-αντίθετα, περιλαμβάνεται σε ενημερώσεις με μετρική 16 και παραμένει στον πίνακα δρομολόγησης μέχρι τη λήξη του flush timer (ή garbage collection timer). Η default τιμή είναι 240sec (60 περισσότερο από το invalid timer).

Εάν δεν θέλουμε κάποιος συγκεκριμένος router να αποστέλλει updates προς κάποιο δίκτυο, το αντίστοιχο interface μπορεί να οριστεί ως passive και να δέχεται μόνο updates:

```
      Router(config-router)#passive-interface [interface]
Π.χ   router(config-router)#passive-interface fa0/0
```

Το RIP λειτουργεί με βάση broadcasts. Εάν απαιτείται η ανταλλαγή πληροφορίας δρομολόγησης με δίκτυα που δεν χρησιμοποιούν broadcasts, όπως π.χ. δίκτυα Frame Relay, θα πρέπει να ενημερώσουμε τον αντίστοιχο router ποιος είναι ο γειτονικός του (αφού δεν μπορεί να τον ανακαλύψει):

```
Router(config-router)#neighbor ip [ip address of neighboring interface]
```

Η εντολή maximum paths χρησιμοποιείται για την εξισορρόπηση φόρτου και ορίζει το μέγιστο αριθμό παράλληλων διαδρομών που θα χρησιμοποιηθούν για τη μετάδοση δεδομένων μεταξύ δυο routers:

```
Router(config-router)#maximum-paths [number ]
```

Οι υπόλοιπες εντολές αφορούν στην επιλογή της έκδοσης του πρωτοκόλλου και την επιλογή του τρόπου με τον οποίο θα γίνονται τα updates (κατά RIPv1 και RIPv2):

Με την εντολή

```
Router(config-router)#version {1|2}
```

επιλέγεται η έκδοση RIPv1 (default) ή RIPv2

Με την εντολή

```
Router(config-if)#ip rip send version {1|2|1 2}
```

επιλέγεται αν θα στέλνονται updates σύμφωνα με το RIPv1, το RIPv2 ή με οποιοδήποτε από τα δυο.

Με την εντολή

```
Router(config-if)#ip rip receive version {1|2|1 2}
```

επιλέγεται αν θα λαμβάνονται updates σύμφωνα με το RIPv1, το RIPv2 ή με οποιοδήποτε από τα δυο.

RIP version 2

Είδαμε ότι το RIPv1 μπορεί να καλύψει σχετικά μικρά και όχι ιδιαίτερα σύνθετα δίκτυα επαρκώς. Ορισμένα όμως από τα χαρακτηριστικά του είναι μάλλον απαρχαιωμένα καιο δεν αρκούν για να καλύψουν τα σύγχονα δίκτυα. Για να αντιμετωπιστούν οι ελλείψεις αυτές σχεδιάστηκε η δεύτερη έκδοση του RIP, το RIPv2, το οποίο εισάγει τρεις βασικές διαφορές σε σχέση με το v1:

α) Το RIPv2 αντί για broadcasts για την μετάδοση των updates, χρησιμοποιεί multicasts, επιβάλλοντας πολύ μικρότερο φόρτο στο δίκτυο. Επιπλέον, προκειμένου να επιταχύνει τη σύγκλιση, υποστηρίζει triggered updates
β) Υποστηρίζει ελεγχόμενη συμμετοχή στο πρωτόκολλο και αυθεντικοποίηση με τη χρήση hashed passwords
γ) Η πιο σημαντική διαφορά, είναι ότι το RIPv2 είναι classless πρωτόκολλο. Σε αντίθεση με το RIPv1 που υποστηρίζει μόνο μια μάσκα υποδικτύου για κάθε δίκτυο, το v2 υποστηρίζει μάσκες μεταβλητού μεγέθους (Variable Length Subnet Masks-VLSM) και με αυτό τον τρόπο μπορεί να καλύψει μεγάλα, σύνθετα δίκτυα με πολύ καλύτερη εκμετάλλευση των διαθέσιμων IP διευθύνσεων.

Variable Length Subnet Masks
Οι μάσκες μεταβλητού μεγέθους επιτρέπουν τη χρήση περισσότερων από μιας μάσκας για μια δεδομένη κλάση διευθύνσεων. Αυτό επιτρέπει πολύ πιο αποδοτική χρήση των διαθέσιμων IP διευθύνσεων, καθώς δεν σπαταλώνται διευθύνσεις εκεί που δε χρειάζονται.

Ας θεωρήσουμε π.χ. το ακόλουθο σενάριο: Μια εταιρεία έχει στη διάθεσή της το class C range 192.168.1.0-192.168.1.255. Η εταιρεία έχει τέσσερις μεγάλες ομάδες χρηστών (Διοίκηση, Λογιστήριο, Πωλήσεις, Μηχανοργάνωση) τις οποίες θέλει να χωρίσει σε ανεξάρτητα υποδίκτυα. Η Διοίκηση είναι το πιο δυναμικό σε αλλαγές τμήμα και προβλέπεται να διευρυνθεί αρκετά στο μέλλον, ενώ η Μηχανοργάνωση και το Λογιστήριο είναι τα πιο σταθερά τμήματα από άποψη στελέχωσης. Οι τρέχουσες ανάγκες κάθε ομάδα σε hosts έχουν ως εξής:

Τμήμα	Αρ. Hosts
Διοίκηση	60 hosts
Πωλήσεις	48 hosts
Λογιστήριο	20 hosts
Μηχανοργάνωση	12 hosts

Εάν το πρωτόκολλο routing που χρησιμοποιείται είναι classful, τότε η προφανής λύση για το subnetting είναι να χρησιμοποιηθεί μάσκα 26bit (255.255.255.192) η οποία θα μας δώσει 4 υποδίκτυα των 64 διευθύνσεων (άρα 62 hosts) το καθένα.

Αυτό μπορεί να λύνει το πρόβλημα προς το παρόν, όμως έχει το μειονέκτημα ότι το υποδίκτυο της Διοίκησης έχει ελάχιστα περιθώρια επέκτασης (απομένουν μόνο 2 ελεύθερες διευθύνσεις IP). Από την άλλη, το δίκτυο της Μηχανοργάνωσης ενώ θα μπορούσε κάλλιστα να χωρέσει σε ένα υποδίκτυο 16 διευθύνσεων, καταλαμβάνει τις τετραπλάσιες.

Σε ένα classless πρωτόκολλο όμως, είναι δυνατό να χωριστεί το δίκτυο ως εξής:

Τμήμα	Mask length	Διευθύνσεις	Hosts
Διοίκηση	25	128	126
Πωλήσεις	26	64	62
Λογιστήριο	27	32	30
Μηχανοργάνωση	28	16	14
Unassigned	28	16	14

Είναι ευνόητο ότι η παραπάνω κατανομή εξυπηρετεί πολύ καλύτερα τις ανάγκες της εταιρείας, ενώ επίσης αφήνει περιθώρια προσαρμογής σε μελλοντικές αλλαγές. Το υποδίκτυο της Διοίκησης μπορεί τώρα να υποστηρίξει πολύ περισσότερους hosts και να προσαρμοστεί στις μελλοντικές αλλαγές, ενώ η σπατάλη διευθύνσεων στο Λογιστήριο και τη Μηχανοργάνωση είναι μικρή.

Ας δούμε το μηχανισμό πίσω από τη διευθυνσιοδότηση με VLSM πριν αναλύσουμε περισσότερο το παράδειγμα.

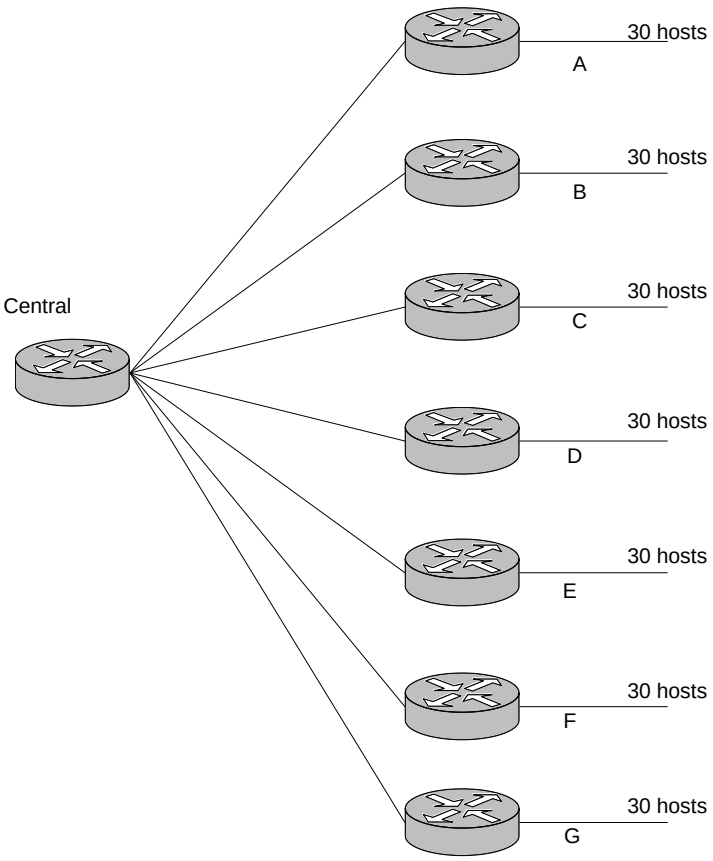
1. Εντοπισμός του segment που απαιτεί το μεγαλύτερο αριθμό διευθύνσεων
2. Επιλογή μιας κατάλληλης μάσκας που να καλύπτει το συγκεκριμένο segment
3. Χωρισμός του class σε υποδίκτυα βάσει του mask που επελέγη
4. Εντοπισμός του αμέσως μεγαλύτερου segment, και επανάληψη της διαδικασίας. Το επόμενο υποδίκτυο θα σταματήσει εκεί που σταμάτησε το προηγούμενο.
5. Για κάθε μικρότερο υποδίκτυο επαναλαμβάνουμε τη διαδικασία.

Ας εφαρμόσουμε την τεχνική στο παράδειγμά μας:
Το segment της Διοίκησης απαιτεί αυτή τη στιγμή 60 hosts και πολύ σύντομα αναμένεται να ξεπεράσει αρκετά αυτό τον αριθμό, συνεπώς καταλληλότερο εύρος για το subnet είναι 128 διευθύνσεις με 25bit μάσκα.
Άρα το πρώτο υποδίκτυο είναι το 192.168.1.0-192.168.1.127
Για το δεύτερο υποδίκτυο 64 διευθύνσεις είναι αρκετές, άρα η καταλληλότερη μάσκα είναι 26bit και το εύρος του υποδικτύου είναι από 192.168.1.128-192.168.1.191
Με τον ίδιο τρόπο χωρίζουμε και το υπόλοιπο class και καταλήγουμε στα εξής υποδίκτυα[5]:

Τμήμα	**Network Address**	**Broadcast Address**	**Subnet Mask**
Διοίκηση	192.168.1.0	192.168.1.127	255.255.255.128
Πωλήσεις	192.168.1.128	192.168.1.191	255.255.255.192
Λογιστήριο	192.168.1.192	192,168.1.223	255.255.255.224
Μηχανοργάνωση	192.168.1.224	192.168.1.239	255.255.255.240
Unallocated (future use)	192.168.1.240	192.168.1.255	255.255.255.240

Ας δούμε τώρα ένα πιο σύνθετο παράδειγμα:

[5] Η συγκεκριμένη κατανομή προϋποθέτει ότι η χρήση του subnet zero είναι αποδεκτή από το δίκτυό μας. Στο παρελθόν, το πρώτο και το τελευταίο υποδίκτυο δεν χρησιμοποιούνταν, προκειμένου να αποφευχθεί σύγχυση μεταξύ της διεύθυνσης του δικτύου και της διεύθυνσης του πρώτου υποδικτύου (που είναι οι ίδιες, με την εξαίρεση της μάσκας). Αργότερα η χρήση του πρώτου υποδικτύου έγινε αποδεκτή και ήταν δυνατή με τη χρήση της εντολής ip subnet-zero. Σήμερα, όλοι οι Cisco Routers υποστηρίζουν εξ'ορισμού το subnet zero



Μας έχει εκχωρηθεί το Class C δίκτυο 192.168.2.0/24. Πρέπει να συνδέσουμε 7 remote sites, το καθένα με 30 hosts, με τον κεντρικό router. Ο αριθμός των hosts δεν θα αλλάξει στο μέλλον. Οι συνδέσεις μεταξύ Central και remote routers είναι point to point συνδέσεις και απαιτούν δυο host addresses (μια για το interface του central και μια για το interface του remote router). Το ζητούμενο είναι να διευθυνσιοδοτηθεί το δίκτυο με τρόπο που να μπορεί να υποστηρίξει αποτελεσματικά τη συγκεκριμένη τοπολογία.

Πρώτο μέλημα είναι η απόδοση διευθύνσεων στα 7 τμήματα των 30 hosts. Για να υποστηριχθούν 30 hosts απαιτούνται 32 διευθύνσεις, άρα το subnet mask είναι 27bit. Η διευθυνσιοδότηση λοιπόν έχει ως εξής:

Subnet	**Network Address**	**Broadcast Address**	**Subnet Mask**
A	192.168.2.0	192.168.2.31	255.255.255.224
B	192.168.2.32	192.168.2.63	255.255.255.224
C	192.168.2.64	192.168.2.95	255.255.255.224
D	192.168.2.96	192.168.2.127	255.255.255.224
E	192.168.2.128	192.168.2.159	255.255.255.224
F	192.168.2.160	192.168.2.191	255.255.255.224
G	192.168.2.192	192.168.1.223	255.255.255.224
Unallocated	192.168.2.224	192.168.2.255	255.255.255.224

Αυτή η κατανομή μας αφήνει ένα μη δεσμευμένο υποδίκτυο 32 διευθύνσεων, στις οποίες θα πρέπει να χωρέσουν 7 υποδίκτυα, που αντιστοιχούν στους συνδέσμους του Central με κάθε Remote Router.
Κάθε σύνδεσμος είδαμε ότι απαιτεί 2 hosts, άρα 4 διευθύνσεις, άρα η μάσκα είναι 30 bit.
Συνεπώς η τελική κατανομή έχει ως εξής:

Subnet	Network Address	Broadcast Address	Subnet Mask
A	192.168.2.0	192.168.2.31	255.255.255.224
B	192.168.2.32	192.168.2.63	255.255.255.224
C	192.168.2.64	192.168.2.95	255.255.255.224
D	192.168.2.96	192.168.2.127	255.255.255.224
E	192.168.2.128	192.168.2.159	255.255.255.224
F	192.168.2.160	192.168.2.191	255.255.255.224
G	192.168.2.192	192.168.1.223	255.255.255.224
A-Central sub-subnet	192.168.2.224	192.168.2.227	255.255.255.252
B-Central sub-subnet	192.168.2.228	192.168.2.231	255.255.255.252
C-Central sub-subnet	192.168.2.232	192.168.2.235	255.255.255.252
D-Central sub subnet	192.168.2.236	192.168.2.239	255.255.255.252
E-Central sub subnet	192.168.2.240	192.168.2.243	255.255.255.252
F-Central sub subnet	192.168.2.244	192.168.2.247	255.255.255.252
G-Central sub subnet	192.168.2.248	192.168.2.251	255.255.255.252
Unallocated	192.168.2.252	192.168.2.255	255.255.255.252

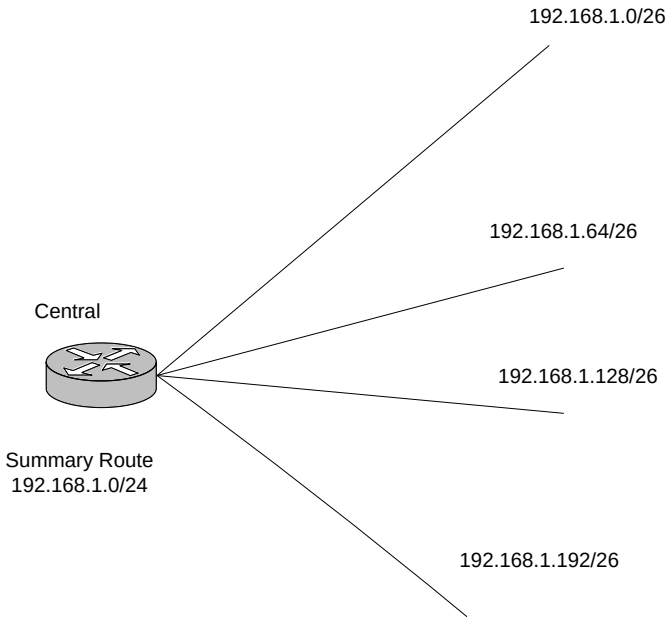
Βλέπουμε εδώ έντονα τη χρήση της μάσκας 30bit (255.255.255.252). Η μάσκα αυτή είναι τυπική για point to point συνδέσεις, γιατί έχει μηδενική σπατάλη διευθύνσεων.
Επισημαίνουμε εδώ ότι κατά τη διευθυνσιοδότηση VLSM πρώτα χωρίζουμε τα μεγαλύτερα υποδίκτυα και προχωράμε σταδιακά προς τα μικρότερα.

Ένα πιο σύνθετο παράδειγμα:

Route Summarization (route aggregation)

Η σύνοψη (ή συγχώνευση) διαδρομών αναφέρεται στη δυνατότητα συνδυασμού ενός ή περισσότερων συνεχόμενων αριθμών δικτύων στον πίνακα δρομολόγησης και την παρουσίασή τους σαν μια ενιαία διαδρομή.
Αυτό επιτρέπει πολύ πιο συμπαγείς πίνακες δρομολόγησης, μειώνοντας την κατανάλωση υπολογιστικών και δικτυακών πόρων, ενώ επίσης επιτρέπει ευκολότερες ρυθμίσεις στους routers.

Παράδειγμα:

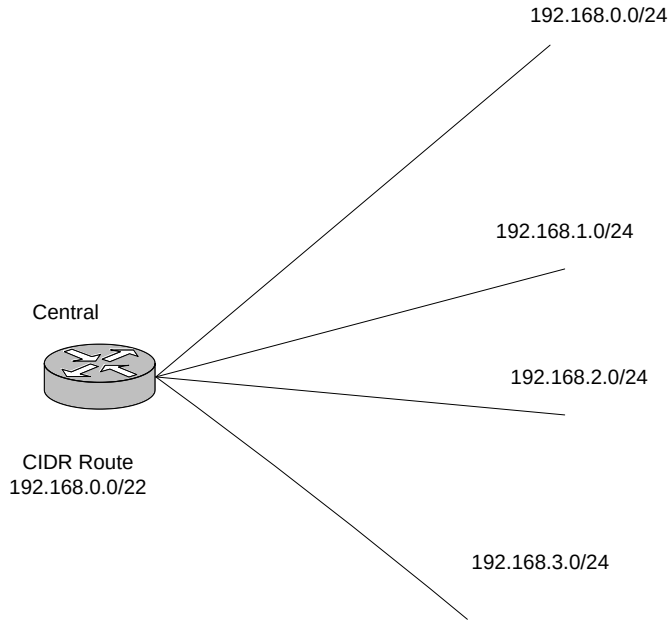


Τα τέσσερα υποδίκτυα του σχήματος μπορούν να συνοψιστούν στη διαδρομή 192.168.1.0/24, η οποία και θα αποστέλλεται με τα routing updates, μειώνοντας τις 4 εγγραφές που θα απαιτούνταν σε 1.

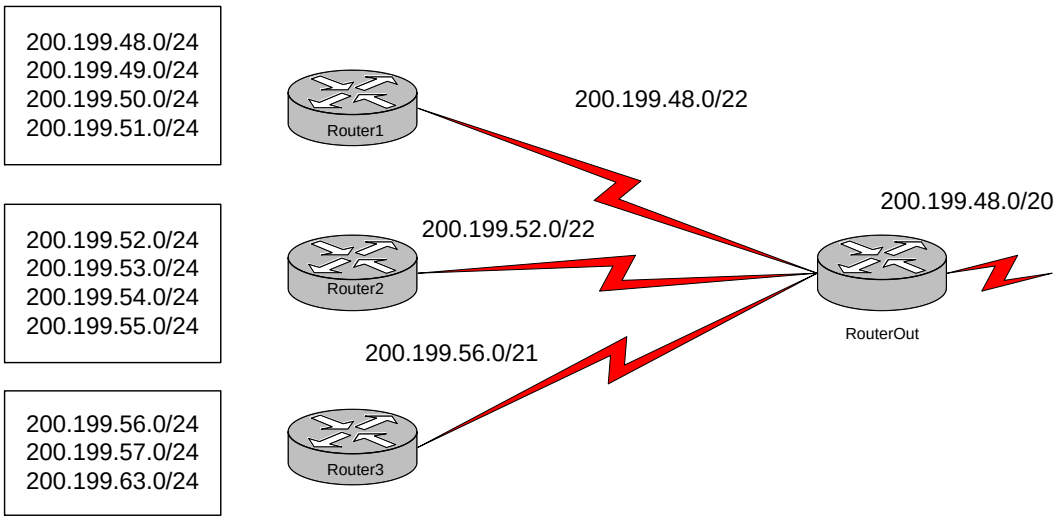
CIDR-Classless InterDomain Routing

Το VLSM Route Summarization είναι η βάση για την τεχνική Classless Interdomain Routing. Με τις VLSM, μπορούμε να συνοψίσουμε διαδρομές μέχρι το όριο της κλάσης τους (π.χ. τέσσερα Class C υποδίκτυα μπορούν να συνοψιστούν σαν ένα δίκτυο C-Class). Το CIDR επεκτείνει αυτή τη λογική και μπορεί να συνδυάσει blocks από A,B ή C-class δίκτυα, τεχνική που είναι γνωστή σαν supernetting.

Παράδειγμα:



Έστω ότι έχουμε την τοπολογία του σχήματος. Τα 4 c-class δίκτυα μπορούν να συνδυαστούν στο CIDR Summary Route 192.168.0.0/22.
Προσέξτε τη μάσκα (255.255.252.0): ορίζει ότι το summary route περιλαμβάνει όλες τις διευθύνσεις από 192.168.0.0 έως 192.168.3.255



Παράδειγμα:

Τα υποδίκτυα στο αριστερό μέρος του σχήματος μπορούν να συνδυαστούν σε summary routes. Το summarization γίνεται βάσει του ip address σε δυαδική μορφή, όπου κρατάμε σαν διεύθυνση summary αυτή που θα προκύψει από το κοινό δυαδικό μέρος των συμμετεχόντων υποδικτύων και μάσκα τόσων bit, όσα είναι τα κοινά bit των υποδικτύων που γίνονται summary.

Η τετράδα π.χ. 200.199.48-51.0/24 σε δυαδική μορφή έχει ως εξής:

11001000. 11000111. 00110000.00000000
11001000. 11000111. 00110001.00000000
11001000. 11000111. 00110010.00000000
11001000. 11000111. 00110011.00000000

Με κόκκινο εμφανίζονται τα κοινά bits (22 συνολικά). Η διεύθυνση που προκύπτει από τα κοινά bits είναι η 200.199.0110000.00000000=200.199.48.0 και η μάσκα είναι 22bit, άρα το aggregate route είναι το 200.199.48.0/22

Περισσότερα για το RIPv2
Είδαμε στα εισαγωγικά του RIPv2 ότι ένα βασικό του πλεονέκτημα έναντι του RIPv1 είναι ότι υποστηρίζει classless routing. Το RIPv2 συμπεριλαμβάνει το subnet mask στην πληροφορία που στέλνει στα updates του και υποστηρίζει τεχνικές VLSM/CIDR κάτι που επιτρέπει να σχεδιάσουμε πολύ αποδοτικότερα δίκτυα.

Η δρομολόγηση βάσει του RIPv2 ενεργοποιείται με τον ακόλουθο τρόπο:

Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network [routednetwork address] [subnet mask]

Η ίδια εντολή (version 2) χρησιμοποιείται και στην περίπτωση που θέλουμε να μετατρέψουμε ένα δίκτυο ήδη ρυθμισμένο να λειτουργεί με RIP σε πρωτόκολλο RIPv2

8.5 Το πρωτόκολλο IGRP

Το πρωτόκολλο IGRP είναι ένα distance vector πρωτόκολλο της εταιρείας Cisco. Το IGRP είναι αρκετά πιο εξελιγμένο από το RIP, καθώς χρησιμοποιεί σύνθετες μετρικές για τον υπολογισμό της βέλτιστης διαδρομής σε ένα δίκτυο.

Βασικά χαρακτηριστικά του IGRP είναι:

- Η δυνατότητα χειρισμού εξαιρετικά σύνθετων τοπολογιών
- Η δυνατότητα χωρισμού του δικτύου σε υποδίκτυα με διαφορετικά χαρακτηριστικά bandwidth και καθυστέρησης
- Η δυνατότητα χειρισμού πολύ μεγάλων δικτύων

Εξ' ορισμού το IGRP χρησιμοποιεί σαν μετρικές το Bandwidth και την καθυστέρηση. Μπορεί όμως να ρυθμιστεί έτσι ώστε να συνδυάζει και άλλες παραμέτρους προκειμένου να σχηματίσει μια σύνθετη μετρική η οποία είναι πολύ πιο ακριβής από το απλό hop count που χρησιμοποιεί το RIP.
Αυτές οι παράμετροι είναι:

- Bandwidth (το εύρος ζώνης μιας διαδρομής)
- Καθυστέρηση (η συνολική καθυστέρηση κατά μήκος μιας διαδρομής)
- Φόρτος (ο φόρτος ενός συνδέσμου μετρούμενος σε bits/sec
- Αξιοπιστία (η αξιοπιστία ενός συνδέσμου όπως καθορίζεται από την ανταλλαγή keepalives)
- MTU (Maximum transmission Unit, αναφέρεται στο μέγεθος του frame που αποστέλλεται.

Το IGRP μπορεί να χρησιμοποιηθεί για τρεις τύπους διαδρομών:

- Εσωτερικές (Interior)
- Εντός Αυτόνομου Συστήματος (System)
- Εξωτερικές (Exterior)

Εσωτερικές Διαδρομές
Οι εσωτερικές διαδρομές είναι διαδρομές μεταξύ υποδικτύων ενός δικτύου συνδεδεμένου σε ένα router interface. Εάν το δίκτυο που είναι συνδεδεμένο στο router δεν είναι υποδικτυωμένο, το IGRP δεν διαφημίζει εσωτερικές διαδρομές.

Διαδρομές Συστήματος
Τα system routes είναι διαδρομές εντός ενός αυτόνομου συστήματος. Το λειτουργικό των Cisco routers έχει τη δυνατότητα να εξάγει διαδρομές system από άμεσα συνδεδεμένα interfaces καθώς και να λάβει system routes που παρέχονται από άλλους IGRP routers ή access servers. Τα system routes δεν

περιέχουν πληροφορία υποδικτύου.

Εξωτερικές διαδρομές
Εξωτερικές ονομάζονται οι διαδρομές προς δίκτυα εκτός του αυτόνομου συστήματος.

Χαρακτηριστικά του IGRP
Αποφυγή routing loops

Το IGRP υποστηρίζει τις ακόλουθες τεχνικές αποφυγής routing loops, τις οποίες έχουμε ήδη παρουσιάσει στο πρωτόκολλο RIP:

- Holddowns
- Split horizons
- Poison reverse updates

Επίσης το IGRP υλοποιεί αρκετούς από τους timers που είδαμε και στο RIP:

- Update timer
- Invalid timer
- Holddown timer
- Flush timer

Ο update timer για το IGRP έχει default τιμή 90 sec.
Η default τιμή για τον invalid timer είναι 3πλάσια του update (270 sec).
Ο holddown timer έχει default τιμή 3 x update_timer + 10 sec (δηλ. 280 sec)
Ο flush timer έχει default τιμή 7πλάσια του update timer (δηλ. 630 sec)

Επιτάχυνση της σύγκλισης
Για να επιτύχει καλύτερους χρόνους σύγκλισης, το IGRP υποστηρίζει triggered updates όταν ανιχνευθεί αλλαγή στο δίκτυο.

Classful Operation
Το IGRP είναι classful πρωτόκολλο και δεν υποστηρίζει VLSMs. Μάσκες μεταβλητού μεγέθους υποστηρίζονται με το Enhanced IGRP, το διάδοχο του IGRP, που όμως είναι hybrid πρωτόκολλο και ενσωματώνει στοιχεία από link-state αλγορίθμους.

Load Balancing
Το IGRP υποστηρίζει τόσο equal όσο και unequal path load balancing, δηλαδή μπορεί να εκτελέσει λειτουργίες εξισορρόπησης φόρτου τόσο μεταξύ συνδέσεων με ίδια μετρική, όσο και μεταξύ συνδέσεων με διαφορετικές μετρικές.

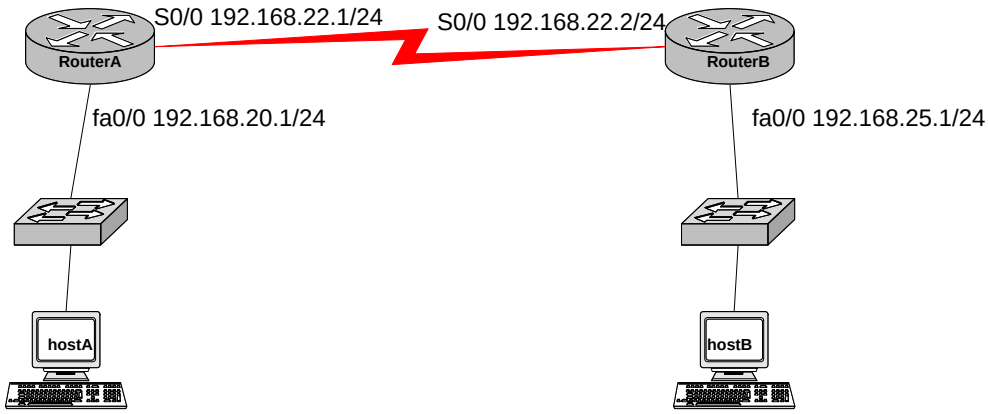
Ρύθμιση του IGRP
Το IGRP ρυθμίζεται σε ένα router ως εξής:

```
Router(config)#router igrp autonomous_system_number
Router(config-router)# network network_address
```

Το IGRP γνωρίζει την έννοια του Autonomous System και απαιτεί τον ορισμό του αριθμού AS[6] για να δρομολογήσει σωστά. Προκειμένου δυο routers να μπορέσουν να ανταλλάξουν routing updates βάσει του IGRP, θα πρέπει να ανήκουν στο ίδιο Autonomous System.
Τα IGRP updates περιέχουν τον αριθμό AS του router που τα στέλνει. Όταν ένας router παραλάβει ένα update, εξετάζει τον αριθμό AS του update και τον συγκρίνει με το δικό του. Εάν δεν ταιριάζουν, ο router απορρίπτει το update.

Η εντολή network λειτουργεί με τον ίδιο τρόπο όπως και στο RIPv1: Αφού το IGRP είναι classful, αρκεί ο ορισμός του class δικτύου. Κάθε interface που η διεύθυνσή του ανάγεται στον αριθμό δικτύου class θα δέχεται και θα στέλνει updates IGRP.

Ας δούμε τις ρυθμίσεις πιο λεπτομερώς με ένα παράδειγμα:



Έστω το δίκτυο που απεικονίζεται στο σχήμα. Μας ζητείται να ρυθμίσουμε τους δυο routers σύμφωνα με τις παραμέτρους που παρουσιάζονται στο σχήμα και στη συνέχεια να ενεργοποιήσουμε το IGRP. Επίσης θα πρέπει να ρυθμίσουμε τους routers με console και telnet password «router» και secret password «router»

Αρχικά ρυθμίζουμε το routerA:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname routerA
routerA(config)#line console 0
routerA(config-line)#password router
routerA(config-line)#login
routerA(config-line)#exit
routerA(config)#line vty 0 4
routerA(config-line)#password router
routerA(config-line)#login
routerA(config-line)#exit
routerA(config)#enable secret router
routerA(config)#int s0/0
routerA(config-if)#ip address 192.168.22.1 255.255.255.0
```

[6] Βλέπε σχετική ενότητα

```
routerA(config-if)#clock rate 56000
routerA(config-if)#no shut
routerA(config-if)#int fa0/0
routerA(config-if)#ip address 192.168.20.1 255.255.255.0
routerA(config-if)#no shut
routerA(config-if)#exit
routerA(config)#exit
routerA#copy run start
```

Αυτό ολοκληρώνει τη βασική ρύθμιση του routerA. Ομοίως για το routerB:

```
Router>enable
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname routerB
routerB(config)#line console 0
routerB(config-line)#password router
routerB(config-line)#login
routerB(config-line)#exit
routerB(config)#line vty 0 4
routerB(config-line)#password router
routerB(config-line)#login
routerB(config-line)#exit
routerB(config)#enable secret router
routerB(config)#int s0/0
routerB(config-if)#ip address 192.168.22.2 255.255.255.0
routerB(config-if)#no shut
routerB(config-if)#int fa0/0
routerB(config-if)#ip address 192.168.25.1 255.255.255.0
routerB(config-if)#no shut
routerB(config-if)#exit
routerB(config)#exit
routerB#copy run start
```

Επιβεβαιώνουμε ότι το serial link λειτουργεί σωστά, κάνοντας ping από τον A στο s0/0 interface του B.

```
routerA#ping 192.168.22.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/11 ms
```

Εάν κάνουμε ping προς το FastEthernet0/0 interface του B, θα δούμε ότι αυτό θα αποτύχει.

```
routerA#ping 192.168.25.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.25.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Το αποτέλεσμα είναι φυσιολογικό, καθώς δεν έχουμε ορίσει διαδρομή για το δίκτυο 192.168.25.0 στο routerA. Η εντολή show ip route επιβεβαιώνει ότι ο A δεν γνωρίζει πώς να προωθήσει πακέτα προς το δίκτυο αυτό.

```
routerA#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

C    192.168.20.0/24 is directly connected, FastEthernet0/0
C    192.168.22.0/24 is directly connected, Serial0/0
```

Στη συνέχεια ενεργοποιούμε το IGRP στο routerA:

```
routerA(config)#router igrp 101
routerA(config-router)#network 192.168.25.0
routerA(config-router)#end
```

και αντίστοιχα για το routerB:

```
routerA(config)#router igrp 101
routerA(config-router)#network 192.168.20.0
routerA(config-router)#end
```

Τώρα έχουμε ενεργοποιήσει το πρωτόκολλο IGRP στους δυο routers, και η εντολή show ip route στο routerA θα μας δώσει τα εξής αποτελέσματα:

```
routerA#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

C    192.168.20.0/24 is directly connected, FastEthernet0/0
C    192.168.22.0/24 is directly connected, Serial0/0
I    192.168.25.0/24 [100/80135] 192.168.22.2, Serial0/0
```

Με αυτό τον τρόπο ολοκληρώνεται η βασική ρύθμιση του IGRP σε μια απλή τοπολογία δύο routers.

Για την επαλήθευση της λειτουργίας του IGRP ισχύουν οι εντολές που έχουμε ήδη δει:

Show ip route
Show ip protocols

Show run
Debug ip igrp events

9. Πρωτόκολλα EIGRP και OSPF

9.1 Το πρωτόκολλο EIGRP

Το Enhanced Interior Gateway Routing Protocol (EIGRP) είναι ένα υβριδικό πρωτόκολλο κατασκευασμένο από την Cisco που συνδυάζει χαρακτηριστικά link-state και distance-vector πρωτοκόλλου. Είναι βασισμένο στο IGRP με πολλές βελτιώσεις ενσωματωμένες. Οι βελτιώσεις αυτές έδωσαν στο EIGRP τα link-state στοιχεία που χρειαζόταν για να μπορεί να αναπτυχθεί σε μεγάλα εταιρικά δίκτυα.

Αρχικά θα γίνει μια σύντομη αντιπαράθεση των δύο EIGRP και IGRP και έπειτα θα αναλυθούν τα πιο αξιόλογα σημεία.

Ομοιότητες:

- Και τα δύο πρωτόκολλα προσφέρουν εξισορρόπηση φορτίου (load balancing) ανάμεσα σε 6 διαφορετικές διαδρομές.
- Έχουν παρόμοια metric που βασίζονται στα ίδια μεγέθη.
- Η λειτουργία και των δύο πρωτοκόλλων βασίζεται στην ανταλλαγή διανυσμάτων απόστασης προς κάθε προορισμό. Δεν ανταλλάσσεται καμία πληροφορία για την τοπολογία του δικτύου. Δηλαδή, ακόμα και το EIGRP στην ουσία είναι πρωτόκολλο distance-vector, ενισχυμένο με κάποια χαρακτηριστικά/τεχνικές από πρωτόκολλα link-state.

Διαφορές:

- Το EIGRP έχει γρηγορότερη σύγκλιση λόγω των προκαλούμενων (triggered) ενημερώσεων και της αποθήκευσης τοπικά των πινάκων δρομολόγησης των γειτόνων.
- Το EIGRP έχει μικρότερη επίδραση στους δικτυακούς πόρους, μια και χρησιμοποιεί προσαυξητικές (incremental) ενημερώσεις.
- Μέρος της επικοινωνίας του EIGRP γίνεται multicast, ενώ στο IGRP όλη η επικοινωνία γίνεται broadcast.
- Οι δρομολογητές στο EIGRP σχηματίζουν σχέσεις γειτονίας μεταξύ τους μέσω μηχανισμού παρόμοιου με τον αντίστοιχο του OSPF. Οι IGRP δρομολογητές δεν συσχετίζονται μεταξύ τους.
- Στο EIGRP χρησιμοποιείται ο αλγόριθμος DUAL για την επιλογή διαδρομών χωρίς loops.
- Στο IGRP, ο μέγιστος αριθμός hops είναι 255. Στο EIGRP ο ίδιος αριθμός είναι 224. Ο αριθμός είναι ικανός για την να εξυπηρέτηση μεγάλων εταιρικών δικτύων.
- Το EIGRP μπορεί να υποστηρίξει την δρομολόγηση πολλαπλών δρομολογούμενων (routed) πρωτοκόλλων.

Τα δύο πρωτόκολλα είναι συμβατά μεταξύ τους. Σε ένα Autonomous System με IGRP και EIGRP δρομολογητές, πληροφορίες δρομολόγησης ανταλλάσσονται αυτόματα μεταξύ τους. Στο παρασκήνιο, οι EIGRP δρομολογητές πραγματοποιούν μετατροπή των metrics, λόγω του διαφορετικού τους μήκους. Συγκεκριμένα, τα metrics των διαδρομών που λαμβάνουν από IGRP δρομολογητές πολλαπλασιάζονται με 256, ενώ τα metrics των διαδρομών που αποστέλλονται στους IGRP δρομολογητές διαιρούνται με 256.

Metric

Τα πρωτόκολλα EIGRP και IGRP χρησιμοποιούν την ίδια δομή στο metric. Τα μεγέθη που χρησιμοποιούν και τα δύο είναι το εύρος ζώνης (bandwidth), η καθυστέρηση (delay), η αξιοπιστία (reliability) και το MTU (Maximum Transfer Unit). Εξ' ορισμού, μόνο τα bandwidth και delay λαμβάνονται υπόψη στον υπολογισμό του metric. Η μόνη διαφορά είναι στο μήκος του metric: το IGRP έχει 24 bit metric, ενώ το EIGRP 32 bit.

Ο μαθηματικός τύπος για τον υπολογισμό του metric στο IGRP είναι:

$$metric = \left[K1 \times bandwidth + \frac{(K2 \times bandwidth)}{(256 - load)} + (K3 \times delay) \right] \times \left[\frac{K5}{(reliability + K4)} \right]$$

όπου εξ' ορισμού, $K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0$.

Και επειδή όταν η παράμετρος K5 είναι μηδέν, το κλάσμα K5/(reliability+K4) αγνοείται (ώστε να μην μηδενίζεται το metric)[7], τελικά ο τύπος ισοδυναμεί με:

$$metric = bandwidth + delay$$

Οι αντίστοιχοι τύποι για το EIGRP είναι:

$$metric = \left[K1 \times bandwidth + \frac{(K2 \times bandwidth)}{(256 - load)} + (K3 \times delay) \right] \times \left[\frac{K5}{(reliability + K4)} \right] \times 256$$

και

$$metric = (bandwidth + delay) \times 256$$

Περιλήψεις Διαδρομών

Σε αντίθεση με το IGRP, το EIGRP υποστηρίζει τόσο αυτόματες όσο και χειροκίνητες περιλήψεις διαδρομών (route summarization). Επειδή κατά βάθος είναι πρωτόκολλο distance-vector, το EIGRP συνοψίζει αυτόματα τις διαδρομές στα όρια των κλάσεων δικτύων A,B και C. Για πιο αποτελεσματικές περιλήψεις πρέπει να απενεργοποιηθεί η αυτόματη περίληψη και να εισαχθούν χειροκίνητα οι επιθυμητές.

Πολλαπλά Δρομολογούμενα Πρωτόκολλα

Το EIGRP υποστηρίζει πολλαπλά Layer 3 πρωτόκολλα: εκτός του IP μπορεί να παρέχει υπηρεσίες δυναμικής δρομολόγησης στα IPX και AppleTalk. Είναι δυνατόν μάλιστα να ανταλλάσει πληροφορίες δρομολόγησης και για τα τρία ταυτόχρονα. Σε δίκτυα που υποστηρίζουν πολλαπλά Layer 3 πρωτόκολλα, το EIGRP είναι ιδανική επιλογή. Η δυνατότητα αυτή του EIGRP οφείλεται στο γεγονός

[7] http://www.cisco.com/warp/public/103/3.html
http://en.wikipedia.org/wiki/EIGRP

ότι σαν πρωτόκολλο transport δεν χρησιμοποιεί το TCP, αλλά πρωτόκολλο της δικής του σουίτας, το EIGRP RTP.

Αλγόριθμος DUAL

Το EIGRP χρησιμοποιεί τον αλγόριθμο DUAL (Diffusing Update Algorithm) για να ενημερώσει το πίνακα δρομολόγησης. Αυτός ο αλγόριθμος προσδίδει στο EIGRP το χαρακτηριστικό της γρήγορης σύγκλισης. Κύρια ευθύνη του είναι η επιλογή των καλύτερων διαδρομών (Successors και Feasible Successors) προς κάθε γνωστό προορισμό και για το σκοπό αυτό αντλεί στοιχεία από τον πίνακα γειτόνων και τον πίνακα τοπολογίας (δες παρακάτω).

Ο αλγόριθμος αποθηκεύει στον πίνακα τοπολογίας τις πληροφορίες δρομολόγησης των γειτόνων. Εάν η πρωτεύουσα διαδρομή για κάποιο προορισμό αποτύχει ο αλγόριθμος DUAL συμβουλεύεται τον πίνακα τοπολογίας για εφεδρική διαδρομή και εάν υπάρχει την τοποθετεί στο πίνακα δρομολόγησης. Με αυτόν τον τρόπο αποφεύγει να μιλήσει με τους γειτονικούς EIGRP δρομολογητές.

Πίνακας Γειτόνων (Neighbor Table)

Κάθε δρομολογητής κρατάει πληροφορίες για την κατάσταση των γειτόνων δρομολογητών σε αυτό τον πίνακα. Τα στοιχεία που καταγράφονται είναι η IP διεύθυνση, η διεπαφή και ο χρόνος HoldTime (δες παρακάτω) του γείτονα. Ο δρομολογητής διατηρεί διαφορετικό πίνακα γειτόνων για κάθε δρομολογούμενο πρωτόκολλο.

Επίσης, ο πίνακας των γειτόνων περιλαμβάνει πληροφορίες απαραίτητες για την λειτουργία του EIGRP RTP, όπως οι σειριακοί αριθμοί που χρησιμοποιούνται για την επιβεβαίωση λήψης των πακέτων. Στον πίνακα καταγράφεται ο τελευταίος σειριακός αριθμός από τα πακέτα κάθε γείτονα, καθώς και κάθε πακέτο που δεν έχει επιβεβαιωθεί ακόμα η παραλαβή του από τους γείτονες. Τα μη επιβεβαιωμένα πακέτα μπαίνουν σε ουρά για αναδιανομή. Τέλος για κάθε γείτονα, υπολογίζονται τα βέλτιστα διαστήματα επανεκπομπής (retransmission interval).

Πίνακας Τοπολογίας (Topology Table)

Ο πίνακας αυτός περιέχει τους προορισμούς που έχουν διαφημιστεί από όλους τους γείτονες. Κάθε καταχώρηση στον πίνακα αναφέρεται σε διαφορετικό προορισμό και περιλαμβάνει τους γείτονες που διαφήμισαν τον προορισμό. Μαζί με κάθε γείτονα αποθηκεύεται το διαφημιζόμενο metric ή Reported Distance (RD) στην ορολογία του EIGRP. Στην καταχώρηση, επίσης, υποδεικνύεται το τελικό metric που θα χρησιμοποιηθεί για τον συγκεκριμένο προορισμό. Το metric αυτό καλείται Feasible Distance (FD) και ισοδυναμεί με το μικρότερο αριθμό που προκύπτει από το άθροισμα του κάθε RD και του αντίστοιχου κόστους πρόσβασης στον γείτονα του RD. Ο γείτονας στον οποίο αντιστοιχεί το FD καλείται Successor. Το FD και ο Successor εισάγονται στον πίνακα δρομολόγησης, ενώ το FD είναι το metric που θα διαφημίζει ο δρομολογητής για τον εν λόγω προορισμό.

Σημαντικός κανόνας των πρωτοκόλλων distance vector είναι ότι τα διαφημιζόμενα metrics αντιστοιχούν σε διαδρομές που χρησιμοποιούν οι ίδιοι οι διαφημιστές-δρομολογητές και άρα βρίσκονται στον πίνακα δρομολόγησης τους.

Successors και Feasible Successors

Διαδρομή (ή δρομολογητής) Successor, όπως περιγράφτηκε προηγουμένως, είναι η διαδρομή (ή ο next-hop δρομολογητής) που επιλέχθηκε από τον αλγόριθμο DUAL σαν η καλύτερη προς δεδομένο προορισμό. Για έναν προορισμό είναι δυνατόν να υπάρχουν έως τέσσερις Successors και εισάγονται όλες στον πίνακα δρομολόγησης.

Οι διαδρομές Successor είναι οι πρωτεύουσες διαδρομές, σε αντίθεση με τις Feasible Successors διαδρομές που θεωρούνται οι εφεδρικές. Οι διαδρομές Feasible Successors δεν εισάγονται στον πίνακα δρομολόγησης, παρά παραμένουν στον πίνακα τοπολογίας. Για να αναδειχθεί κάποιος γείτονας σαν Feasible Successor πρέπει να ικανοποιείται η ακόλουθη συνθήκη (γνωστή σαν Feasibility Condition):

"Το Reported Distance του Feasible Successor πρέπει να είναι μικρότερο από το τρέχων Feasible Distance."

Μια άλλη, πιο απλή διατύπωση, είναι:
"Ο δρομολογητής που μας λέει ότι είναι πιο κοντά στον προορισμό από ότι εμείς, προάγεται σε Feasible Successor."

Η συνθήκη αυτή εξασφαλίζει την χρήση διαδρομών απαλλαγμένων από loops. Η ορθότητα της αποδείχθηκε από τον Dr. J. J. Garcia Luna Aceves. Αξιοσημείωτο είναι ότι αυτή η συνθήκη είναι ικανή αλλά όχι και αναγκαία. Δηλαδή, είναι πιθανό να υπάρχουν και άλλες χωρίς loops διαδρομές προς κάποιο προορισμό, αλλά να μην ικανοποιούν την συνθήκη.

Κατάσταση Προορισμών

Ένας προορισμός μπορεί να βρίσκεται σε είτε κατάσταση Passive, είτε σε κατάσταση Active.

Passive State: Ένας προορισμός θεωρείται ότι βρίσκεται σε αυτήν την κατάσταση όταν ο δρομολογητής δεν εκτελεί υπολογισμό του Successor. Σε περίπτωση που ο Successor αποτύχει και υπάρχει Feasible Successor, δεν χρειάζεται να γίνει εκ νέου υπολογισμός, μεταφέρεται ο Feasible Successor στην θέση του Successor.

Active State: Ένας προορισμός θεωρείται ότι βρίσκεται σε αυτήν την κατάσταση όταν ο δρομολογητής εκτελεί υπολογισμό για νέο Successor, επειδή δεν υπάρχει Feasible Successor (δηλαδή δεν υπάρχει εφεδρική διαδρομή διαθέσιμη στον πίνακα τοπολογίας). Η διαδικασία του υπολογισμού ξεκινάει με την αποστολή πακέτων Query σε όλους του γείτονες. Οι γείτονες πρέπει είτε να απαντήσουν με πληροφορίες για τον εν λόγω προορισμό, είτε να ενημερώσουν ότι δεν έχουν γνώση. Αφού εκτιμηθούν οι απαντήσεις και εφόσον βρεθεί νέος Successor, ο προορισμός ξαναγυρίζει σε κατάσταση Passive.

Είδη Πακέτων/ Μηνυμάτων

Το EIGRP χρησιμοποιεί 5 τύπους πακέτων:

- Hello: Τα πακέτα Hello αποστέλλονται multicast και σκοπός τους είναι η ανακάλυψη νέων γειτόνων και η διατήρηση επαφής με τους υπάρχοντες. Η λήψη τους δεν χρειάζεται επιβεβαίωση.

- Acknowledgement: Ένα άδειο πακέτο Hello αποτελεί ένα πακέτο Acknowledgement (ή απλά Ack). Τα πακέτα Ack στέλνονται unicast και σκοπός τους είναι η επιβεβαίωση λήψης των άλλων τύπων πακέτων. Δηλαδή, η λήψη των πακέτων Update, Query και Reply, υποχρεώνει το δρομολογητή να απαντήσει με ένα Ack στον αποστολέα.

- Updates: Χρησιμοποιούνται για την μεταφορά των περιεχομένων του πίνακα τοπολογίας από δρομολογητή σε δρομολογητή. Τα πακέτα Update προς ένα νέο γείτονα στέλνονται unicast. Στην περίπτωση προκαλούμενων ενημερώσεων, τα Update στέλνονται multicast (στην ίδια διεύθυνση όπως και τα Hello).

- Query: Όταν η κατάσταση ενός προορισμού υπεισέρχεται σε κατάσταση Active, τότε ο δρομολογητής στέλνει πακέτα Query στην multicast διεύθυνση του EIGRP. Εάν σε απάντηση ενός Query σταλθεί άλλο Query τότε το δεύτερο στέλνεται unicast.

- Reply: Ο δρομολογητής που θα λάβει πακέτο Query πρέπει να αποκριθεί, ακόμα και αν δεν έχει να προτείνει κάτι, με ένα πακέτο Reply απ' ευθείας στον αποστολέα του Query (unicast).

Όπως και με το OSPF, με τη χρήση των επιβεβαιώσεων το πρωτόκολλο μεταφοράς εγγυάται αξιόπιστη παράδοση των πακέτων.

Εάν ένας EIGRP δρομολογητής δεν λάβει επιβεβαίωση λήψης για κάποιο από τα παραπάνω μηνύματα, θα επαναλάβει την μετάδοση μηνύματος για συνολικά 16 φορές. Μετά θα ανακηρύξει τον γείτονα εκτός λειτουργίας (dead) και θα τον διαγράψει από γείτονα.

Ετικέτες σε Διαδρομές

Το EIGRP τοποθετεί «ετικέτες» στις διαδρομές που μαθαίνει από το IGRP ή από οποιαδήποτε άλλη πηγή, μαρκάροντας τις σαν εξωτερικές επειδή δεν προέρχονται από EIGRP δρομολογητή. Το IGRP δεν καταλαβαίνει αυτούς τους διαχωρισμούς, γι' αυτό και από τις διαδρομές που διαφημίζονται σε IGRP δρομολογητές αφαιρούνται οι ετικέτες.

Λειτουργία του EIGRP

Neighbor Routers

Το EIGRP χρησιμοποιεί πακέτα Hello για να ανακαλύψει νέους δρομολογητές και να διατηρήσει σχέσεις γειτνίασης με αυτούς. Σε δίκτυα broadcast, point-to-point και point-to-multipoint τα πακέτα Hello αποστέλλονται κάθε 5 δευτερόλεπτα (hello interval). Σε συνδέσεις με ταχύτητες μικρότερες από T1/E1 τα Hello στέλνονται κάθε 60 δευτερόλεπτα. Τα πακέτα Hello στέλνονται στην multicast IP διεύθυνση 224.0.0.10.

Στα πακέτα Hello περιέχεται η παράμετρος HoldTime. Η τιμή της HoldTime ορίζει τον χρόνο μέσα στον οποίο ένας δρομολογητής πρέπει να λάβει πακέτο Hello από τον γείτονα του, ώστε ο γείτονας να παραμείνει ενεργός στον πίνακα γειτόνων του δρομολογητή. Αντιστοιχεί στον χρόνο DeadInterval του OSPF.

Για να γίνουν δύο EIGRP γείτονες πρέπει να ταιριάζουν τα ακόλουθα στοιχεία:

- Ο αριθμός του αυτόνομου συστήματος (AS)
- Οι μεταβλητές K των metric.

Σε αντίθεση με OSPF, χρειάζεται να ταιριάξουν οι ρυθμιστές χρόνου (timers) για να επιτευχθεί γειτνίαση. Η διαδικασία που ακολουθείται κατά την εδραίωση μιας γειτνίασης είναι:

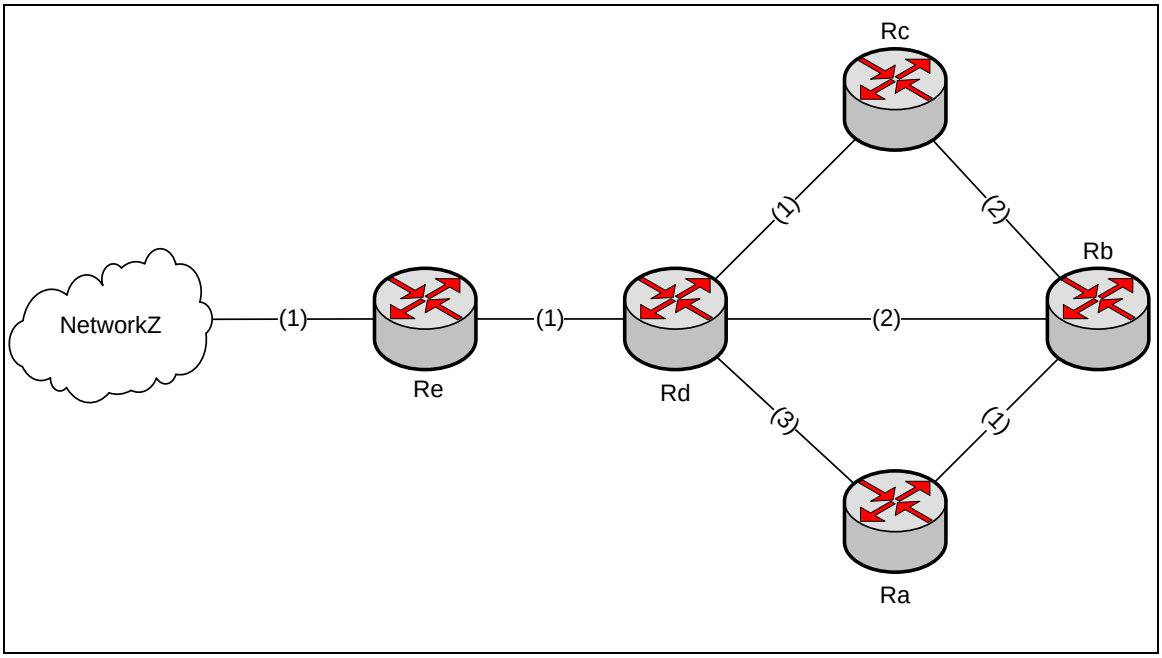
1. Έστω EIGRP δρομολογητής Ra στον οποίο μόλις ξεκίνησε η διεργασία του πρωτοκόλλου. Ο δρομολογητής στέλνει πακέτα Hello από όλες τις διεπαφές που συμμετέχουν στον EIGRP.
2. Δεύτερος EIGRP δρομολογητής Rb λαμβάνει πακέτο Hello από τον Ra. Εάν ταιριάζουν ο αριθμός AS και οι μεταβλητές K, π Rb θα απαντήσει με πακέτο Hello ακολουθούμενο από πακέτο Update. Το τελευταίο περιέχει όλες τις διαδρομές που γνωρίζει ο Rb και μεταδίδεται unicast στον Ra.
3. Ο δρομολογητής Ra θα απαντήσει με πακέτο επιβεβαίωσης (acknowledgement), γνωστοποιώντας έτσι στον Rb την λήψη του πακέτου Rb. Στη συνέχεια θα στείλει στον Rb το δικό του πακέτο Update.
4. Ο δρομολογητής Rb θα απαντήσει με πακέτο acknowledgement.

Σε αυτό το σημείο οι δύο δρομολογητές έχουν συγχρονίσει τις βάσεις τους. Σε αντίθεση με το OSPF, η ανταλλαγή πληροφοριών δρομολόγησης δεν πραγματοποιείται με κάποιον προκαθορισμένο δρομολογητή, αλλά με οποιοδήποτε. Αποτέλεσμα αυτού είναι ότι κάθε neighbor δρομολογητής είναι και adjacent.

Λειτουργία του DUAL

Για να γίνει πιο εύκολα κατανοητή η λειτουργία του DUAL θα εξετάσουμε το δίκτυο της Εικόνας 1 με ζητούμενο την δρομολόγηση από τον Rb προς το δίκτυο NetworkZ.

Θεωρούμε ότι ο Rb έχει χτίσει τον πίνακα τοπολογίας με πληροφορίες δρομολόγησης που έχει πάρει από τους Ra, Rc και Rd κατά την εδραίωση της γειτνίασης. Για τον δίκτυο-προορισμό NetworkZ, ο Rb θα έχει τρεις επιλογές με διαφορετικά Reported Distance.



Εικόνα 1.

Η καταχώρηση στον πίνακα τοπολογίας που αντιστοιχεί στον NetworkZ θα μοιάζει κάπως έτσι:

Destination	***Next-Hop Neighbor***	***RD***	***RD + local metric***	***FD***	***DUAL Result***
NetworkZ					
	via Ra	5	5+1=6		
	via Rc	3	3+2=5		Feasible Successor
	via Rd	2	2+2=4	4	Successor

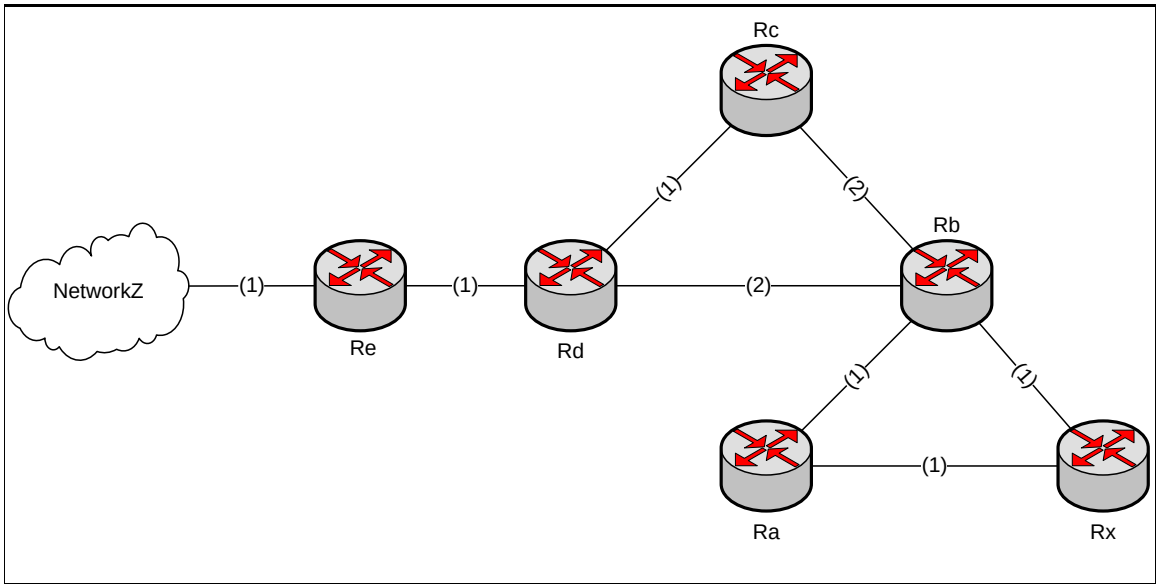
Παρατηρούμε ότι ο Rc ικανοποιεί την συνθήκη RD<FD και προάγεται σε Feasible Successor, αντίθετα από τον Ra ο οποίος δεν ικανοποιεί την συνθήκη και δεν προάγεται. Ο δρομολογητής Rd θα εισαχθεί στον πίνακα δρομολόγησης σαν η καλύτερη διαδρομή για τον προορισμό NetworkZ.

Σε περίπτωση που διακοπεί η σύνδεση Rd-Rb, ο Rb δεν θα χρειαστεί να ξανα-υπολογίσει την καλύτερη διαδρομή προς το δίκτυο NetworkZ. Θα μεταφέρει απλά τον Rc στον πίνακα δρομολόγησης και θα διατηρήσει τον προορισμό σε κατάσταση Passive.

Εάν όμως αποτύχει και η σύνδεση Rc-Rb, τότε ο δρομολογητής Rb θα πρέπει να αλλάξει την κατάσταση του προορισμού NetworkZ σε Active και να προχωρήσει σε εκ νέου υπολογισμό. Αυτό σημαίνει ότι θα μηδενίσει το FD και θα στείλει πακέτα Query. Ο μόνος που θα απαντήσει θα είναι το Ra και συνεπώς θα γίνει ο νέος Successor.

Είναι σαφές ότι λόγω της Feasibility Condition, δεν επιτρέπεται σε μια διαδρομή χωρίς loops να χρησιμοποιηθεί σαν εφεδρική λύση. Βέβαια, στον δεύτερο υπολογισμό αναδεικνύεται στη νέα καλύτερη διαδρομή προς το δίκτυο NetworkZ, άρα συνέπεια εφαρμογής της συνθήκης είναι μόνο ο αυξημένος χρόνος σύγκλισης.

Στο επόμενο παράδειγμα θα εξετάσουμε περίπτωση όπου φαίνεται η αξία του Feasibility Condition. Έστω το δίκτυο της Εικόνας 2.



Εικόνα 2: Αποκλεισμός διαδρομής με loops

Ο δρομολογητής Rx έχει να επιλέξει μεταξύ δύο δρόμων όσον αφορά στο δίκτυο NetworkZ, μέσω του Rb και μέσω του Ra. Το metric μέσω του Rb είναι 5, ενώ μέσω του Ra είναι 6, οπότε επιλέγεται ο Rb σαν Successor του Rx προς το NetworkZ. Ο Rx θα ανακοινώσει στον Ra πρόσβαση στο NetworkZ με metric 6 και ο Ra με την σειρά του θα ανακοινώσει τον εν λόγω προορισμό στον Rb με metric 7.

Ο δρομολογητής Rb θα έχει και πάλι τρεις δυνατότητες για το δίκτυο NetworkZ, μία εκ των οποίων οδηγεί σε loop. Ο πίνακας τοπολογίας θα διαμορφωθεί ως εξής:

Destination	***Next-Hop Neighbor***	***RD***	***RD + local metric***	***FD***	***DUAL Result***
NetworkZ					
	via Ra	7	7+1=8		
	via Rc	3	3+2=5		Feasible Successor
	via Rd	2	2+2=4	4	Successor

Ακολουθώντας την ίδια λογική όπως και στο προηγούμενο παράδειγμα, ο Ra αποκλείεται από ικανή διαδρομή. Ακόμα και αν χαθούν οι άλλες δύο συνδέσεις του Rb, αυτή η προβληματική διαδρομή δεν θα χρησιμοποιηθεί ποτέ, αφού ο Rx δεν θα έχει πια πρόσβαση στο NetworkZ. Αποδεικνύεται, λοιπόν, η σημασία του Feasibility Condition στην επιλογή διαδρομών χωρίς loops.

Παραδείγματα Παραμετροποίησης

Βασικές Εντολές

Η παραμετροποίηση του EIGRP είναι παρόμοια με του IGRP. Η ενεργοποίηση του πρωτοκόλλου σε ένα δρομολογητή Cisco[8] και η προσθήκη διεπαφών στις διαδικασίες του πρωτόκολλου, γίνονται με την παρακάτω ακολουθία εντολών από Global Configuration Mode:

```
Router(config)# router eigrp <autonomous_system_number>
Router(config-router)# network <IP_network>
```

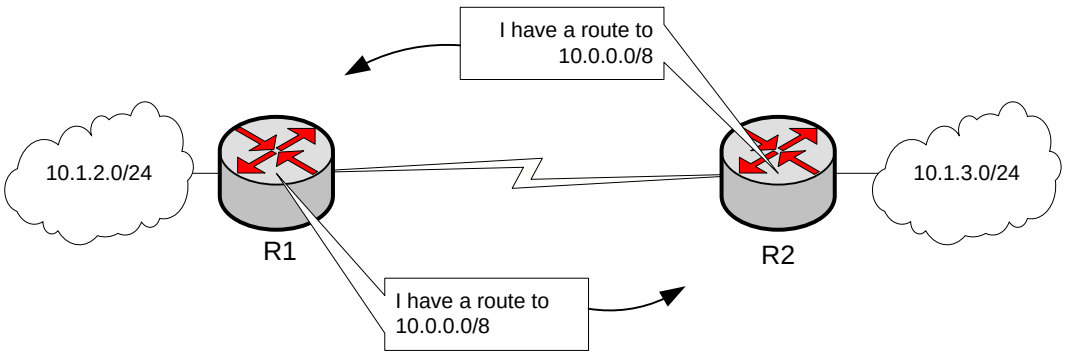
Ο αριθμός του αυτόνομου συστήματος πρέπει να ίδιος σε όλους τους δρομολογητές. Παρόλο που το EIGRP είναι πρωτόκολλο classless, οι αριθμοί των IP δικτύων πρέπει να είναι classful. Για παράδειγμα, σε ένα δρομολογητή στο αυτόνομο σύστημα 100 με δύο διεπαφές Ethernet με διευθύνσεις IP 10.1.2.1 και 10.1.3.1, οι εντολές

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

Περίληψη Διαδρομών

Το EIGRP συμπτύσσει αυτόματα τις διαδρομές στο όριο των κλάσεων. Αυτό σημαίνει ότι ο δρομολογητής R1 στην Εικόνα 3 θα διαφημίσει όλο το κλάσης Α 10.0.0.0/8 δίκτυο, παρόλο που έχει επαφή μόνο με ένα υποδίκτυο αυτού. Η αυτόματη περίληψη του EIGRP βοηθάει στην διατήρηση των πινάκων δρομολόγησης συνεπτυγμένους.

Στις περιπτώσεις μη συνεχόμενων υποδικτύων της ίδιας κλάσης, όπως αυτή της εικόνας 3, η αυτόματη περίληψη δημιουργεί προβλήματα. Οι δρομολογητές διαφημίζουν όλο το δίκτυο κλάσης Α, με αποτέλεσμα ο δρομολογητής που λαμβάνει την διαφήμιση να την απορρίπτει λόγω ότι και ο ίδιος είναι συνδεδεμένος στο ίδιο δίκτυο κλάσης Α.



Εικόνα 3: Αυτόματη περίληψη στο EIGRP

Είναι δυνατόν, για την αποφυγή προβλημάτων δρομολόγησης σε τέτοιες περιπτώσεις, να απενεργοποιηθεί η αυτόματη περίληψη με την παρακάτω εντολή:

[8] Ο δρομολογητής μπορεί να είναι μόνο Cisco, αφού το EIGRP είναι ιδιοκτησία της εν λόγω εταιρίας.

```
router(config-router)# no auto-summary
```

Το EIGRP, όμως, υποστηρίζει και την χειροκίνητη ρύθμιση περιλήψεων. Οι χειροκίνητες περιλήψεις ορίζονται ανά διεπαφή. Η εντολή που θα δοθεί σε Interface Configuration Mode είναι:

```
router(config-if)# ip summary-address eigrp <autonomous_system_number>
                <IP_network> <mask> <administrative_distance>
```

Η περιληπτικές διαδρομές του EIGRP έχουν εξ' ορισμού διαχειριστικό βάρος 5. Προαιρετικά, μπορεί να οριστεί σε νέα τιμή μεταξύ 1 και 255.

Για να απενεργοποιηθούν οι αυτόματες περιλήψεις και να ρυθμιστεί η σωστή περίληψη του διασυνδεόμενου δικτύου στον δρομολογητή R1 της Εικόνας 3, εργαζόμαστε ως εξής:

```
R1(config)# router eigrp 100
R1(config-router)# no auto-summary
R1(config-router)# exit
R1(config)# interface serial 0/0
R1(config-if)# ip summary-address eigrp 100 10.1.2.0 255.255.255.0
```

9.2 Το πρωτόκολλο OSPF

Το OSPF αναλύεται ως "Open Shortest Path First" και είναι ένα link-state πρωτόκολλο που χειρίζεται την δρομολόγηση πακέτων IP. Η δεύτερη έκδοση του περιγράφεται στο RFC2328 και είναι ανοιχτό πρότυπο. Το OSPF βασίζεται στη θεωρία των link-states αλλά εισάγει και μερικά δικά του χαρακτηριστικά.

Το OSPF δημιουργήθηκε στα μέσα της δεκαετίας του 80' με σκοπό να αντιμετωπίσει τις ελλείψεις και κυρίως την αδυναμία χρήσης του RIP σε μεγάλα δίκτυα. Επειδή βασίζεται σε ανοιχτά πρότυπα γρήγορα έγινε ευρέως αποδεκτό και σήμερα χρησιμοποιείται σε πολλά εταιρικά δίκτυα. Τα πλεονεκτήματα του συνοπτικά είναι:

- Μπορεί να τρέξει σε οποιοδήποτε δρομολογητή καθώς βασίζεται σε ανοιχτά πρότυπα και η υλοποίηση του δεν δεσμεύεται από κάποιον κατασκευαστή.
- Παρέχει δρομολόγηση χωρίς loops, χρησιμοποιώντας τον αλγόριθμο SPF.
- Παρέχει γρήγορη σύγκλιση (convergence), κάνοντας χρήση προκαλούμενων (triggered) ενημερώσεων.
- Είναι ένα πρωτόκολλο classless, δηλαδή καταλαβαίνει μάσκες δικτύου και υποδικτύωση (subnetting), και συνεπώς επιτρέπει ιεραρχικό σχεδιασμό στη δρομολόγηση αξιοποιώντας τις τεχνικές VLSM και CIDR.

Το OSPF δεν είναι χωρίς μειονεκτήματα. Αναφέρουμε συνοπτικά:

- Απαιτεί περισσότερη μνήμη καθώς διατηρεί πληροφορίες σε διάφορες βάσεις δεδομένων.
- Απαιτεί περισσότερη υπολογιστική ισχύ για να τρέξει τον αλγόριθμο SPF, ιδιαίτερα κατά την εκκίνηση της διεργασίας του OSPF.
- Είναι πολύπλοκο στην παραμετροποίηση και ακόμα περισσότερο στα μεγάλα δίκτυα όπου απαιτείται προσεκτικός σχεδιασμός για επιτυχημένη ιεραρχική δρομολόγηση.

- Η αποσφαλμάτωση του είναι επίσης δύσκολη διαδικασία.

Βασικές Έννοιες και Ορολογία

Areas

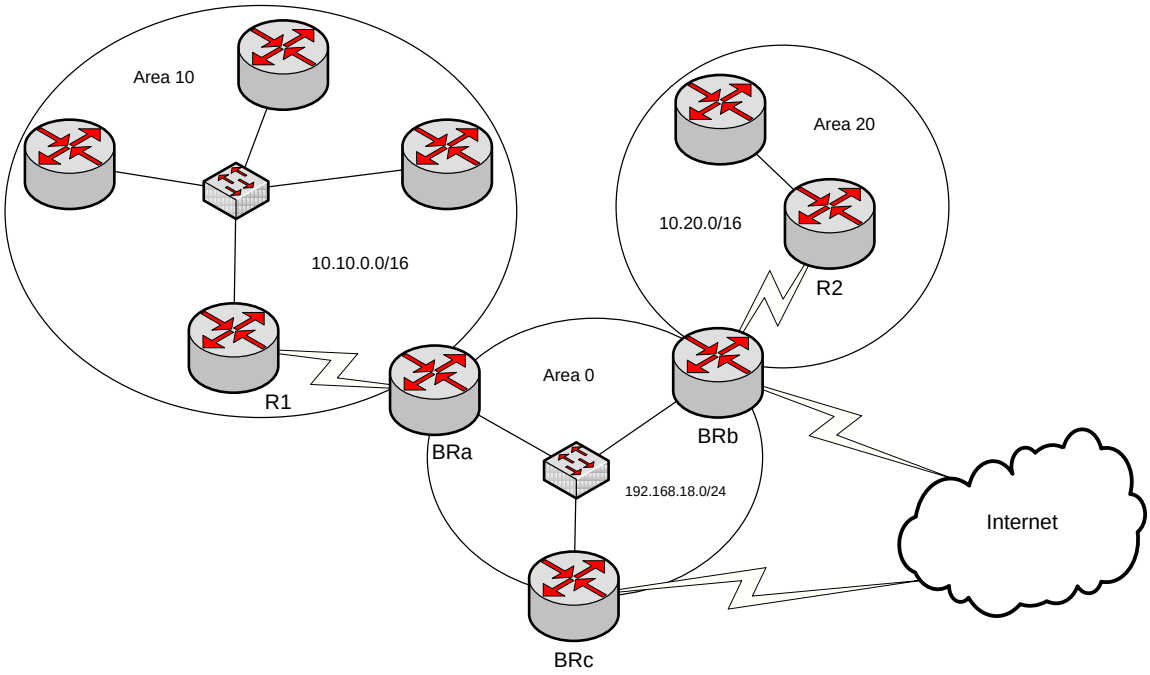
Ένα από τα βασικότερα χαρακτηριστικά του OSPF είναι η ικανότητα του να φέρει εις πέρας τη δρομολόγηση μεγάλων δικτύων που εφαρμόζουν VLSM. Την ικανότητα του αυτή την οφείλει στην υποστήριξη της έννοιας *των αυτόνομων συστημάτων (Autonomous Systems)*, ενώ εισάγει την έννοια των *περιοχών (areas).*
Autonomous system (AS) είναι ένα σύνολο από δίκτυα κάτω από κοινό διαχειριστικό έλεγχο. Σε κάθε Autonomous System αντιστοιχίζεται ένας μοναδικός αριθμός από 1 έως 65,535. Για τον χειρισμό της δρομολόγησης μέσα σε ένα Autonomous System χρησιμοποιούνται τα πρωτόκολλα δρομολόγησης IGP, ενώ για την ανταλλαγή πληροφορίας δρομολόγησης μεταξύ αυτόνομων συστημάτων χρησιμοποιούνται τα πρωτόκολλα EGP.

Μέσα σε ένα AS, τα areas παρέχουν ιεραρχική δρομολόγηση. Χρησιμοποιούνται για τον έλεγχο την ποσότητα της πληροφορίας δρομολόγησης που διακινείται απ' άκρη σ' άκρη στο δίκτυο. Αλλαγές τοπικής σημασίας που συμβαίνουν μέσα στα όρια ενός area είναι δυνατόν να περιοριστούν και να μην ανακοινώνονται στα υπόλοιπα areas. Σε δίκτυα επίπεδου σχεδιασμού, όπως αυτά που προκύπτουν κατά την χρήση του RIP, κάτι τέτοιο δεν είναι εφικτό και όλες οι αλλαγές στην τοπολογία γνωστοποιούνται σε όλους τους δρομολογητές. Για παράδειγμα, ας σκεφτούμε την περίπτωση όπου κάποια διαδρομή για ένα απομακρυσμένο δίκτυο αντικαθίσταται με άλλη λόγω της αστοχίας κάποιου ενδιάμεσου δρομολογητή. Η νέα διαδρομή θα ανακοινωθεί σε όλους τους δρομολογητές που ανήκουν στο ίδιο area. Έκτος, όμως, του εν λόγω area δεν χρειάζεται να ανακοινωθεί τίποτα αφού το απομακρυσμένο δίκτυο εξακολουθεί να είναι προσβάσιμο.

Το OSPF εφαρμόζει ιεραρχία δύο επιπέδων: το area κορμού (backbone) και τα areas εκτός κορμού. Τα areas ταυτοποιούνται με αριθμούς από 0 έως 65,535. Στο backbone area αντιστοιχίζεται πάντα το 0. Όλα τα areas πρέπει να συνδέονται στο backbone area και επικοινωνία μεταξύ των areas γίνεται διαμέσου του backbone.

Το δίκτυο στην Εικόνα 1 περιλαμβάνει το backbone area και ακόμα δύο areas που συνδέονται στο backbone area μέσω των δρομολογητών κορμού BRa και BRb. Υλοποιώντας σωστό σχεδιασμό της IP διευθυνσιοδότησης, είναι δυνατόν η ανταλλαγή πληροφορίας δρομολόγησης μεταξύ των areas να περιοριστεί σε μία μόνο περιληπτική διαδρομή (summary route). Για παράδειγμα, το area 20 δεν χρειάζεται να δώσει στο backbone area περιληπτική περιγραφή των διαδρομών των επιμέρους υποδικτύων (subnets), παρά μόνο μια ανακοίνωση διαμέσου του R2 που περιλαμβάνει το συγκεντρωτικό 10.20.0.0/16.

Στο εσωτερικό ενός area, όμως, όλοι οι δρομολογητές πρέπει να έχουν πλήρη γνώση των διασυνδεόμενων υποδικτύων ώστε να επιτυγχάνεται βέλτιστη δρομολόγηση.



Εικόνα 4: Παράδειγμα τριών διασυνδεόμενων areas.

Η υιοθέτηση της έννοιας των areas αποφέρει τα εξής πλεονεκτήματα: α) λιγότερη πληροφορία στους πίνακες δρομολόγησης και β) τα τοπικά προβλήματα παραμένουν τοπικά και δεν επηρεάζουν την σταθερότητα του υπόλοιπου δικτύου. Σαν αποτέλεσμα, το OSPF δύναται να αναπτυχθεί σε δίκτυα μεγαλύτερα από ότι τα distance-vector πρωτόκολλα, όπως το RIP.

Links και Link-states

Ό όρος link αντιπροσωπεύει την διεπαφή ενός δρομολογητή. Το link-state είναι μια περιγραφή της διεπαφής και της σχέσης της με τους δρομολογητές-γείτονες. Μια τέτοια περιγραφή περιλαμβάνει την IP διεύθυνση της διεπαφής, την μάσκα υποδικτύου (subnet mask), τον τύπο του δικτύου που συνδέεται, τους δρομολογητές που συνδέονται σε αυτό το δίκτυο και άλλα. Τα link-states αποθηκεύονται στην link-state database ή topological database.

Link State Advertisements (LSAs)

Οι βάσεις δεδομένων στο OSPF συντηρούνται από την ανταλλαγή διαφημιστικών ανακοινώσεων γνωστές σαν Link State Advertisements (LSAs). Το LSA είναι ένα σετ δεδομένων που περιγράφουν την κατάσταση ενός δρομολογητή ή ενός δικτύου. Ουσιαστικά είναι διαφημίσεις των link-states ενός δρομολογητή. Ανάλογα με τον τύπο τους (Πίνακας 1) προωθούνται σε μεγαλύτερες ή μικρότερες περιοχές του OSPF δικτύου.

Τύπος	Όνομα LSA	Περιγραφή
1	Router-LSAs	Πλημμυρίζουν μόνο το τοπικό area. Αποστέλλονται από όλους τους

		δρομολογητές του area και περιγράφουν την κατάσταση των διεπαφών που συνδέονται στο εν λόγω area.
2	Network-LSAs	Πλημμυρίζουν μόνο το τοπικό area. Αποστέλλονται από τον Designated Router (βλέπε παρακάτω) και περιέχουν όλους τους δρομολογητές που συνδέονται σε ένα broadcast δίκτυο.
3,4	Summary-LSAs	Πλημμυρίζουν τα γειτονικά area. Αποστέλλονται από τους δρομολογητές που συνδέονται και στα δύο areas (Area Border Routers – ABRs).
5	AS-external-LSAs	Πλημμυρίζουν όλο το Autonomous System και αποστέλλονται από τους δρομολογητές που βρίσκονται στο όριο αυτού (Autonomous System Border Routers – ASBRs).

Πίνακας 1: Οι 5 τύποι LSAs

Metric

Σε αντίθεση με το RIP που χρησιμοποιεί τον αριθμό των hops σαν μέτρο σύγκρισης διαδρομών, το OSPF κάνει χρήση του εύρος ζώνης[9] (bandwidth) μιας σύνδεσης. Για την ακρίβεια χρησιμοποιεί τον όρο *κόστος (cost)* που είναι το αντίστροφο του εύρος ζώνης. Ο μαθηματικός τύπος που σχετίζει τα δύο μεγέθη είναι:

$$COST = \frac{10^8}{(bandwith)}$$

Έτσι, όσο μεγαλύτερη η ταχύτητα μεταφοράς δεδομένων μιας γραμμής, τόσο μικρότερο είναι το κόστος. Το συνολικό κόστος μιας διαδρομής προκύπτει από το άθροισμα των επιμέρους κοστών των φυσικών συνδέσεων που την αποτελούν. Χρησιμοποιώντας το κόστος μιας διαδρομής αντί για το αριθμό των hops, το OSPF επιλέγει διαδρομές πιο έξυπνα.

[9] Εύρος ζώνης είναι γενικότερος όρος της επιστήμης των τηλεπικοινωνιών, ο οποίος στις επικοινωνίες δεδομένων αντιστοιχεί στην ταχύτητα μεταφορά της πληροφορίας.

Μεταξύ δύο διαδρομών προς τον ίδιο προορισμό, το OSPF θα προτιμήσει (και άρα θα τοποθετήσει στον πίνακα δρομολόγησης) αυτήν με το μικρότερο κόστος. Σε περίπτωση διαδρομών με ίδιο κόστος (μέχρι έξι διαδρομές), το OSPF θα μοιράσει τον φόρτο μεταξύ των διαδρομών (load balancing). Είναι σημαντικό, λοιπόν, να ρυθμίζουμε σωστά τα χαρακτηριστικά σύνδεσης μιας διεπαφής.

Router-ID

Κάθε δρομολογητής που συμμετέχει σε ένα OSPF δίκτυο πρέπει να έχει μία μοναδική ταυτότητα που έχει σκοπό να τον ξεχωρίζει από τους υπόλοιπους δρομολογητές. Με αυτήν την ταυτότητα είναι "γνωστός" στο OSPF δίκτυο και συνεπώς, όλες οι διαδρομές που ανακοινώνει συσχετίζονται με την ταυτότητα του. Η ταυτότητα έχει την μορφή μιας IP διεύθυνσης και περιλαμβάνεται σε κάθε OSPF μήνυμα που στέλνει ένας δρομολογητής. Καλείται *Router-ID*.

Η επιλογή του Router-ID γίνεται σύμφωνα με τα παρακάτω κριτήρια:

1. Πρώτα εξετάζονται οι IP διευθύνσεις των loopback διεπαφών και επιλέγεται η μεγαλύτερη.
2. Εάν δεν βρεθεί loopback διεπαφή, επιλέγεται η μεγαλύτερη IP διεύθυνση από τις ενεργές φυσικές διεπαφές.
3. Σε περίπτωση που δεν υπάρχει ενεργή διεπαφή, η διεργασία του OSPF δεν θα ξεκινήσει.

Η βέλτιστη πρακτική είναι η χρήση loopback διεπαφής γιατί είναι πάντα ενεργή και άρα το Router-ID θα είναι πάντα το ίδιο.

Βάσεις Δεδομένων

Οι δρομολογητές σε ένα OSPF δίκτυο διατηρούν δύο βάσεις δεδομένων: την βάση γειτνίασης (adjacency database) και την βάση τοπολογίας (topology ή link-state database).

Η adjacency database ουσιαστικά είναι μια λίστα με όλους του OSPF γείτονες. Δύο OSPF δρομολογητές θεωρούνται γείτονες όταν έχουν εδραιώσει μεταξύ τους αμφίδρομη επικοινωνία (βλέπε παρακάτω). Η λίστα αυτή περιέχει τα Router-ID τους, τις IP διευθύνσεις τους, την διεπαφή με την οποία συνδέονται στο OSPF δίκτυο καθώς και ένα λεκτικό που περιγράφει την κατάσταση ανταλλαγής OSPF πληροφορίας (OSPF state).

Η topology database περιέχει όλους του δρομολογητές και τις διαδρομές, τους προορισμούς και τα κόστη που έχουν ανακοινώσει αυτοί. Στα περιεχόμενα αυτής της βάσης εφαρμόζεται ο αλγόριθμος SPF, τα αποτελέσματα του οποίου τροφοδοτούν τον πίνακα δρομολόγησης.

Αλγόριθμος Shortest Path First

Ο αλγόριθμος Shortest Path First (SPF) είναι η καρδιά του OSPF, αφού είναι υπεύθυνος για τον υπολογισμό των διαδρομών που θα τροφοδοτήσουν τον πίνακα δρομολόγησης, η κύρια εργασία κάθε πρωτόκολλου δρομολόγησης.

Δημιουργός του αλγορίθμου είναι ο Edsger Wybe Dijkstra, ένας Ολλανδός επιστήμονας. Το SPF είναι επίσης γνωστό και σαν αλγόριθμος του Dijkstra.

Σε αυτόν τον αλγόριθμο η καλύτερη διαδρομή είναι αυτή που έχει το μικρότερο κόστος. Ο αλγόριθμος θεωρεί κάθε δίκτυο ένα σύνολο από κόμβος διασυνδεόμενους μεταξύ τους με point-to-point συνδέσεις.

Σε κάθε σύνδεση, ανάλογα με την τεχνολογία που χρησιμοποιείται, αντιστοιχεί διαφορετικό κόστος. Κάθε κόμβος διατηρεί σε βάσεις δεδομένων πλήρη γνώση για την φυσική τοπολογία όλου του area. Οι βάσεις τοπολογίας των δρομολογητών ενός δεδομένου area είναι πανομοιότυπες.

Ο αλγόριθμος SPF εξετάζει τις πληροφορίες από τους γειτονικούς κόμβους και υπολογίζει τις καλύτερες, χωρίς loops διαδρομές προς όλους τους προορισμούς, χρησιμοποιώντας τον κόμβο στον όποιο τρέχει σαν σημείο εκκίνησης. Κατασκευάζει έτσι ένα δένδρο (shortest path tree), όπου τα φύλλα αντιστοιχούν σε απομακρυσμένα δίκτυα-προορισμούς, τα κλαδιά στις κοντινότερες διαδρομές και η ρίζα στον τοπικό κόμβο. Αυτό το δένδρο δίνει ολόκληρη η διαδρομή προς κάθε προορισμό (δίκτυο ή υπολογιστή). Παρόλα αυτά, μόνο ο επόμενος hop χρησιμοποιείται στην διαδικασία προώθησης.

Λειτουργία

Hello Protocol

Είναι επί μέρους πρωτόκολλο του OSPF που χρησιμοποιείται στην εδραίωση και διατήρηση σχέσεων γειτνίασης. Σε δίκτυα broadcast προσφέρει την δυνατότητα ανακάλυψης νέων δρομολογητών δυναμικά. Ο βασικός του στόχος είναι να γεμίσει την adjacency database.

Εξασφαλίζει ότι η επικοινωνία μεταξύ γειτόνων είναι αμφίδρομη. Πακέτα Hello στέλνονται περιοδικά κάθε *HelloInterval* (προκαθορισμένη τιμή 10 δευτερόλεπτα) από όλες τις διεπαφές που συμμετέχουν στο OSPF. Όταν ένας δρομολογητής δει το δικό του Router-ID στα Hello πακέτα ενός γείτονα, αυτό είναι ένδειξη αμφίδρομης επικοινωνίας. Το Hello πρωτόκολλο είναι επίσης υπεύθυνο για την εκλογή του Designated Router.

Σε τοπικά δίκτυα τύπου broadcast (π.χ. Ethernet), κάθε δρομολογητής διαφημίζει τον εαυτό του στέλνοντας περιοδικά πακέτα Hello στην multicast IP διεύθυνση 224.0.0.5 (all-OSPF-routers διεύθυνση). Με αυτόν τον τρόπο είναι δυνατό να ανακαλύπτονται νέοι γείτονες δυναμικά. Τα Hello πακέτα περιέχουν την άποψη του δρομολογητή για το ποιος είναι ο Designated Router και μια λίστα με τους γειτονικούς δρομολογητές από τους οποίους έχει πρόσφατα λάβει Hello πακέτα.

Neighbor Routers

Όταν ένας δρομολογητής ενεργοποιηθεί, η OSPF διεργασία θα αρχίσει να παράγει και να στέλνει από τις διεπαφές που έχουν οριστεί στην OSPF παραμετροποίηση Hello πακέτα. Τα Hello πακέτα, μεταξύ άλλων, μεταφέρουν τα ακόλουθα στοιχεία:
- Τον αριθμό του area,
- Τους ρυθμιστές χρόνου (timers) HelloInterval και DeadInterval (παρακάτω),
- Το OSPF συνθηματικό (εάν έχει ρυθμιστεί πιστοποίηση ταυτότητας)

Για να προχωρήσουν δύο δρομολογητές στο σχηματισμό σχέσης γειτνίασης (neighbors) πρέπει να συμφωνούν στα παραπάνω στοιχεία.

Οι OSPF δρομολογητές περνάνε από τα εξής στάδια μέχρι να γίνουν γείτονες, που συνολικά καλούνται διαδικασία ανταλλαγής (exchange process):

1. ***Down* state:** Ο δρομολογητής Ra δεν έχει ανταλλάξει OSPF μηνύματα με κανένας άλλο δρομολογητή.

2. ***Init* state:** Ο δρομολογητής Ra αρχίζει να στέλνει Hello πακέτα στην IP multicast διεύθυνση 224.0.0.5. Ο δρομολογητής Rb τα λαμβάνει και προσθέτει τον Ra στην λίστα των γειτόνων (εφόσον συμφωνούν τα στοιχεία της παραπάνω παραγράφου με τα δικά του) με την ένδειξη ότι βρίσκεται σε κατάσταση *Init*. Σε αυτό το σημείο η επικοινωνία είναι ακόμα μονόδρομη.
3. ***Two-Way* state:** Ο δρομολογητής Ra λαμβάνει Hello πακέτο από τον δρομολογητή Rb, στο οποίο εντοπίζει το δικό του Router-ID. Ο Ra προσθέτει τον Rb στην δική του λίστα γειτόνων. Και στις δύο λίστες οι δρομολογητές έχουν φτάσει κατάσταση Two-Way. Σε αυτό το σημείο η επικοινωνία είναι αμφίδρομη.

Όταν δύο δρομολογητές φτάσουν στην κατάσταση two-way, τότε θεωρούνται γείτονες.

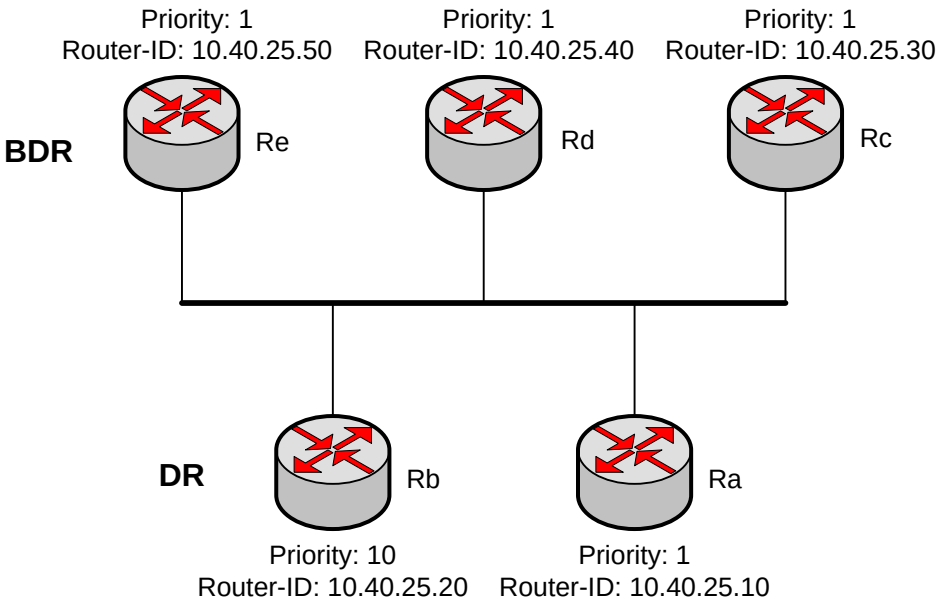
Κάθε OSPF δρομολογητής περιμένει να λάβει πακέτα Hello από τους γείτονες του κάθε *HelloInterval* δευτερόλεπτα. Εάν περάσει χρόνος ίσος με *DeadInterval* (προκαθορισμένη τιμή 40 δευτερόλεπτα) χωρίς να λάβει πακέτο Hello από κάποιο γείτονα, τότε ο γείτονας θεωρείται «νεκρός» και αφαιρείται από την λίστα των γειτόνων. Το γεγονός αυτό γνωστοποιείται στους υπόλοιπους γείτονες μέσω ενός LSA μηνύματος.

Designated Router και Backup Designated Router

Το επόμενο βήμα είναι η ανταλλαγή πληροφοριών δρομολόγησης μεταξύ των γειτόνων. Στο OSPF, όμως, η ανταλλαγή δεν γίνεται μεταξύ όλων των δρομολογητών, γιατί αυτό θα απαιτούσε ν*(ν-1)/2 ανταλλαγές, όπου ν ο αριθμός των δρομολογητών, και συνεπώς αυξημένη κίνηση και χρήση πόρων. Αντίθετα, η ανταλλαγή της πληροφορίας γίνεται μόνο με προκαθορισμένους δρομολογητές.

Για κάθε τοπικό δίκτυο πολλαπλής πρόσβασης εκλέγεται ένας δρομολογητής σαν κεντρικό σημείο συναλλαγής. Ένας δεύτερος δρομολογητής εκλέγεται σαν αντικαταστάτης σε περίπτωση αστοχίας του πρώτου. Οι δρομολογητές αυτοί καλούνται Designated Router (DR) και Backup Designated Router (BDR), αντίστοιχα.

Η εκλογή των DR και BDR γίνεται βάση του αριθμού OSPF προτεραιότητας (priority), ο οποίος εξ' ορισμού είναι 1 (οι τιμές είναι από 0 έως 255). Σε περίπτωση ισοπαλίας, εξετάζεται το Router-ID των δρομολογητών και τα δύο μεγαλύτερα κερδίζουν τον διαγωνισμό. Εάν παρουσιαστεί πρόβλημα στην λειτουργία του DR, τότε ο BDR προβιβάζεται σε DR και κάποιος άλλος δρομολογητής εκλέγεται σαν BDR.



Εικόνα 5: Παράδειγμα εκλογής DR και BDR.

Στην Εικόνα 2 βλέπουμε ότι ο Rb έχει την μεγαλύτερη προτεραιότητα από όλους τους άλλους δρομολογητές και άρα εκλέγεται DR. Οι υπόλοιποι ισοβαθμούν σε προτεραιότητα, οπότε ο BDR κρίνεται βάσει του Router-ID και τελικά εκλέγεται ο Re.

Adjacent Routers

Η διαδικασία ανταλλαγής πληροφοριών δρομολόγησης μεταξύ δύο γειτόνων, αναβαθμίζει την σχέση τους. Δύο neighbor (γείτονες) δρομολογητές που έχουν ανταλλάξει πληροφορίες είναι πλέον adjacent δρομολογητές. Δεν γίνονται όλοι οι neighbors και adjacent, εξαρτάται από τον τύπο του δικτύου (point-to-point, broadcast, NBMA) και τον ρόλο του δρομολογητή στο συγκεκριμένο area (Designated Router ή όχι). Στον Πίνακα 2 παρουσιάζονται οι τύποι δικτύων που αναγνωρίζει το OSPF και πως γίνεται η ανταλλαγή πληροφοριών δρομολόγησης σε καθένα από αυτούς.

Ένας δρομολογητής σε ένα δίκτυο broadcast πολλαπλής πρόσβασης θα γίνει adjacent μόνο με τους DR και BDR. Τα OSPF πακέτα αποστέλλονται στην IP multicast διεύθυνση 224.0.0.6 (all-DRouters διεύθυνση) στην οποία ακούν ο DR και ο BDR. Οι DR και BDR με την σειρά τους, μιλάνε με όλους του γείτονες στην IP multicast διεύθυνση 224.0.05.

Συνεχίζοντας από την κατάσταση two-way που φθάνουν δύο γείτονες, τα επόμενα στάδια προς πλήρη συγχρονισμό των topology databases είναι:

1. ***Exstart* state:** Μεταξύ των Designated Routers (DR και BDR) και του OSPF δρομολογητή, αυτός με το υψηλότερο Router-ID γίνεται *master* και ξεκινάει την διαδικασία ανταλλαγής (δεν είναι σίγουρο ότι θα γίνει master ο DR). Πριν προχωρήσει στο επόμενο βήμα, οι δύο δρομολογητές αποφασίζουν για το αρχικό sequence number των πακέτων (Database Description packets) που θα χρησιμοποιηθούν στον επόμενο βήμα για την περιγραφή της topology database.

2. ***Exchange* state:** Ο master περιγράφει την topology database στον slave, με την μορφή πακέτων Database Description (DDPs). Κάθε DDP περιέχει ένα sequence number και η λήψη επιβεβαιώνεται με LSACK πακέτο. Δεν επιτρέπεται να αναμένουν επιβεβαίωση λήψης παραπάνω από ένα DDP πακέτα. Ο slave συγκρίνει τις πληροφορίες των DDPs με την δική του topology database.

3. ***Loading* state:** Εάν από την σύγκριση που κάνει ο slave προκύψει ότι ο master έχει πιο ενημερωμένη topology database, ο slave θα ζητήσει από τον master τα πιο πρόσφατα LSAs με ένα πακέτο Link State Request (LSR). Ο master θα αποκριθεί με ένα πακέτο Link State Update (LSU) που θα περιέχει τα LSAs που ζήτησε ο slave. Ο slave και πάλι θα επιβεβαιώσει την λήψη των LSUs με ίσο αριθμό LSACKs. Εάν ο slave έχει πιο ενημερωμένη βάση, τότε η διαδικασία γυρίζει στο Exchange state αλλά με αντεστραμμένους τους ρόλους.

4. ***Full* state:** Με το πέρας του Loading state οι δρομολογητές έχουν συγχρονίσει τις topology databases τους και είναι πλήρως adjacent.

Τύπος Δικτύου	**Τεχνολογίες**	**Εκλογή DR**	**Ανταλλαγή Πληροφοριών**
Broadcast multi-access	Ethernet, Token Ring	NAI	με DR
Non-broadcast multi-access (NBMA)	Frame Relay, X.25	NAI	με DR
Point-to-point	PPP, HDLC	OXI	μεταξύ όλων
Point-to-multipoint	Frame Relay, X.25	OXI	μεταξύ όλων

Πίνακας 2: Τύποι δικτύων που αναγνωρίζει το OSPF

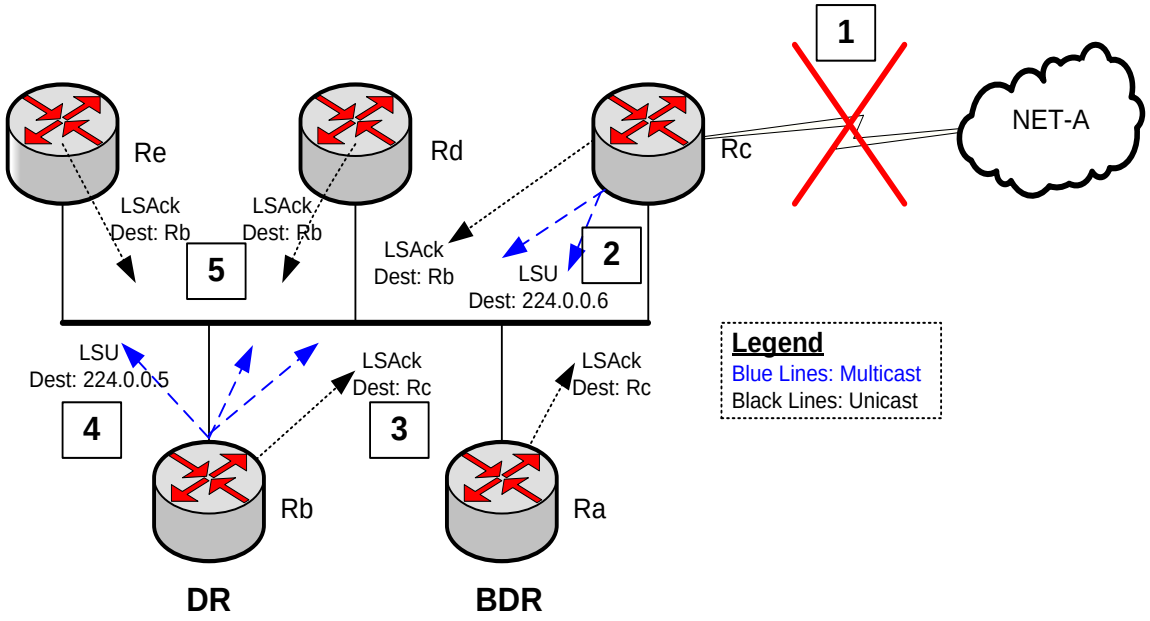
Διάδοση Αλλαγών Δρομολόγησης

Οι δρομολογητές σε Full state με τον DR, χρησιμοποιούν μόνο προσαυξητικές (incremental) ενημερώσεις για περαιτέρω επικοινωνία. Αυτό σημαίνει ότι όταν προκύψουν αλλαγές μέσα σε ένα OSPF area, μόνο αυτές οι μεμονωμένες αλλαγές ανακοινώνονται στον DR, ο οποίος στη συνέχεια θα τις μοιραστεί με τους υπόλοιπους γείτονες του area.

Πιο αναλυτικά, ο δρομολογητής που θα ανιχνεύσει κάποια αλλαγή σε διασυνδεόμενο δίκτυο, θα ετοιμάσει LSU που θα περιέχει LSA με την νέα πληροφορία και θα το στείλει στην multicast IP 224.0.0.6. Οι DR και BDR θα όταν λάβουν το LSU θα αποκριθούν με κατάλληλο unicast LSAck και θα προχωρήσουν στην ενσωμάτωση των νέων δεδομένων στις βάσεις τους. Έπειτα ο DR θα στείλει καινούργιο LSU στην multicast IP 224.0.0.5 ενημερώνοντας με τη σειρά του όλους του δρομολογητές του area για την αλλαγή. Οι δρομολογητές μόλις παραλάβουν το LSU, αποκρίνονται με LSAck, ακόμα και εκείνος που προκάλεσε όλη την ταραχή.

Στην εικόνα 3 βλέπουμε πέντε δρομολογητές που ανήκουν στο ίδιο area. Κάποια στιγμή ο Rc χάνει επαφή με το δίκτυο NET-A. Η πορεία των γεγονότων όπως απεικονίζονται είναι:

1. Διακόπτεται η σειριακή σύνδεση του Rc με το δίκτυο NET-A.
2. Ο Rc στέλνει LSU με προορισμό 224.0.0.6 για να ενημερώσει για την αλλαγή.
3. Οι DR και BDR απαντούν με LSAck.
4. Ο DR στέλνει LSU με προορισμό 224.0.0.5 για να ενημερώσει τους γείτονες.
5. Οι γείτονες αποκρίνονται με LSAck.



Εικόνα 6: Παράδειγμα διάδοσης μιας αλλαγής δρομολόγησης μέσα σε ένα OSPF area.

Παρατηρούμε ότι όλη η επικοινωνία είναι αξιόπιστη παρόλο που χρησιμοποιούνται multicast διευθύνσεις. Σε περίπτωση που κάποιος δρομολογητής δεν ανταποκριθεί με LSAck, τότε ο αποστολέας του LSU πραγματοποιεί unicast επανεκπομπές μέχρι να λάβει επιβεβαίωση ή μέχρι να παρέλθει η ηλικία του LSA (LS age field).

Εξαίρεση στον κανόνα τον προσαυξητικών ενημερώσεων είναι η αποστολή όλης της topology database του DR κάθε 30 λεπτά στην multicast IP 224.0.0.5, ώστε να είναι σίγουρο ότι όλοι οι δρομολογητές του area έχουν την πιο πρόσφατη έκδοση αυτής.

Παραδείγματα Παραμετροποίησης

Βασικές Εντολές

Για την ενεργοποίηση του OSPF πρωτοκόλλου σε ένα δρομολογητή Cisco, εφαρμόζουμε την παρακάτω ακολουθία εντολών σε Global Configuration Mode:

```
Router(config)# router ospf <process_ID>
Router(config-router)# network <IP_address> <wildcard_mask> area <area_#>
```

Ο αριθμός *process_ID* χρησιμοποιείται για να διαχωρίσει μεταξύ διαφορετικών διεργασιών του πρωτοκόλλου. Οι αριθμός αυτός δεν χρειάζεται να ταιριάζει με τους αντίστοιχους αριθμούς σε άλλους δρομολογητές και επιπλέον δεν έχει καμία σχέση με τον αριθμό του αυτόνομου συστήματος (Autonomous System).

Για να συσχετίσουμε κάποια διεπαφή με ένα area, χρησιμοποιούμε την εντολή **network**. Επειδή το OSPF είναι classless πρωτόκολλο, στη συγκεκριμένη εντολή η IP διεύθυνση συνοδεύεται από μάσκα

που καθορίζει ποιες ακριβώς διεπαφές συμμετέχουν στο area. Η μάσκα αυτή καλείται *wildcard mask* και ουσιαστικά είναι μια αντεστραμμένη *network mask*. Η wildcard mask, όπως και η network mask, έχει μήκος 32 bits αλλά αντίθετα από την network mask, όταν συγκρίνεται με την IP διεύθυνση της διεπαφής, το 0 bit σημαίνει ταίριασμα με την διεύθυνση της network εντολής. Το τελευταίο τμήμα της εντολής προσδιορίζει τον αριθμό του area.

Στο παρακάτω παράδειγμα, οι διεπαφές με διευθύνσεις 192.168.1.1, 192.168.2.1, 172.21.40.1 και 172.21.50.1 συμμετέχουν στο area 0, γνωστό και σαν backbone area. Η wildcard mask 0.0.0.0 υπονοεί ότι πρέπει να υπάρχει bit προς bit ταίριασμα μεταξύ των διευθύνσεων διεπαφής και εντολής ώστε να προστεθεί η διεπαφή στο area.

```
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.1 0.0.0.0 area 0
Router(config-router)# network 192.168.2.1 0.0.0.0 area 0
Router(config-router)# network 172.21.40.1 0.0.0.0 area 0
Router(config-router)# network 172.21.50.1 0.0.0.0 area 0
```

Στο επόμενο παράδειγμα, οι διεπαφές με IP διευθύνσεις στα διαστήματα 192.168.1.0/24 και 172.21.0.0/16 συμμετέχουν στο area 0.

```
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router(config-router)# network 172.21.0.0 0.0.255.255 area 0
```

Τέλος, εάν θέλουμε όλες οι διεπαφές του δρομολογητή να ανήκουν στο area 0 χρησιμοποιούμε την μάσκα 255.255.255.255:

```
Router(config)# router ospf 1
Router(config-router)# network 0.0.0.0 255.255.255.255 area 0
```

Ρυθμίζοντας το Router-ID

Όπως ήδη αναφέρθηκε, ο προτεινόμενος τρόπος για να καθορίσουμε το Router-ID ενός OSPF δρομολογητή είναι να χρησιμοποιήσουμε μια διεπαφή loopback. Η διεπαφή loopback είναι μια λογική, εικονική διεπαφή (όχι φυσική) και εξ' ορισμού δεν υπάρχουν στην παραμετροποίηση ενός Cisco δρομολογητή. Για να δημιουργήσουμε μια διεπαφή loopback εφαρμόζουμε την παρακάτω ακολουθία εντολών:

```
Router(config)# interface loopback <port_#>
Router(config-if)# ip address <IP_address> <subnet_mask>
```

Αλλάζοντας το Κόστος

Στους Cisco δρομολογητές, οι σειριακές διεπαφές έχουν προ-ρυθμισμένη ταχύτητα σύνδεσης στα 1,544 Kbps. Επειδή το κόστος είναι αντιστρόφως ανάλογο της ταχύτητας μιας διεπαφής, είναι επιθυμητό να ρυθμιστεί η σωστή τιμή της ταχύτητας ώστε να αντιστοιχηθεί το σωστό κόστος στην διεπαφή. Για να ρυθμίσουμε την ταχύτητα μιας διεπαφής εισάγουμε τις ακόλουθες εντολές:

```
Router(config) interface type <[slot_#/]port_#>
```

```
Router(config-if)# bandwidth <speed_in_Kbps>
```

Σε περίπτωση που είναι απαραίτητο να αλλάξουμε το κόστος μιας διεπαφής, εισάγουμε τις παρακάτω εντολές σε Global Configuration Mode:

```
Router(config)# interface <type> <[slot_#/]port_#>
Router(config-if)# ip ospf cost <cost_value>
```

10. IP Access Lists

Έχοντας παραμετροποιήσει τον Router μας, τα πακέτα πληροφοριών μπορούν να μετακινούνται ελεύθερα από το ένα interface στο άλλο. Προκειμένου να μπορέσουμε να ελέγξουμε την ροή των δεδομένων, θα πρέπει να εφαρμόσουμε ένα χαρακτηριστικό του CISCO IOS το οποίο ονομάζεται Access Control Lists (ACLs).

Αυτές οι λίστες εντολών, οι οποίες χρησιμοποιούνται για το φιλτράρισμα των πληροφοριών, μπορούν να εφαρμοστούν και σε άλλα πρωτόκολλα εκτός του IP, όπως το IPX, XNS, DECnet, AppleTalk και άλλα.

Οι Access Control Lists (ACLs), μπορούν επίσης να χρησιμοποιηθούν και για τους παρακάτω σκοπούς:

- Για να περιορίσουν την πρόσβασης μέσω Telnet (VTY) σε έναν δρομολογητή
- Για τον έλεγχο ροής των πληροφοριών δρομολόγησης
- Για να δώσει προτεραιότητα στα πακέτα πληροφοριών που αφορούν το WAN

10.1 Εισαγωγή στις ACL

Οι λίστες ACLs είναι ένα σύνολο εντολών, οι οποίες χρησιμοποιούνται για τον έλεγχο της ροής πληροφοριών διαμέσου των interfaces. Οι εντολές μιας λίστας ACL ελέγχουν το είδος της πληροφορίας η οποία εισέρχεται ή εξέρχεται από έναν δρομολογητή (Router) και ανάλογα καθορίζουν σε ποια πακέτα δεδομένων θα επιτραπεί η διέλευση και σε ποια θα απαγορευτεί. Οι λίστες ACLs δημιουργούνται στο Global Configuration Mode. Μόλις δημιουργηθεί η λίστα εντολών ACL, θα πρέπει να ενεργοποιηθεί, προκειμένου να αρχίσει τον έλεγχο ροής πληροφοριών . Η ενεργοποίηση γίνεται στη λειτουργία Interface Subconfiguration Mode.

Μόλις ενεργοποιηθεί μια λίστα ACL θα πρέπει να καθοριστεί σε ποια κατεύθυνση θα γίνεται ο έλεγχος ροής πληροφοριών:

- Εισερχόμενη (όταν τα δεδομένα εισέρχονται στο δρομολογιτή)
- Εξερχόμενη (όταν τα δεδομένα εξέρχονται από το δρομολογιτή)

Ένας περιορισμός που υπάρχει στις λίστες ACLs είναι ότι δεν μπορούν να φιλτράρουν την πληροφορία η οποία δημιουργείται από το δρομολογητής.

Υπάρχουν δύο ειδών λίστες ACLs:

- Numbered & Named
- Standard & Extended

Numbered ονομάζονται οι λίστες των οποίων οι εντολές ομαδοποιούνται με ένα μοναδικό αριθμό.
Named αντίστοιχα ονομάζονται οι λίστες των οποίων οι εντολές ομαδοποιούνται με ένα μοναδικό όνομα.
Κάθε ένα από αυτά τα δύο διαφορετικά είδη λιστών υποστηρίζει δύο τύπους φιλτραρίσματος: Standard & Extended.
Οι Standard λίστες μπορούν μόνο να ελέγξουν και να φιλτράρουν την διεύθυνση της συσκευής η οποία παράγει την πληροφορία. Αντίθετα οι Extended λίστες μπορούν να ελέγξουν και να φιλτράρουν τόσο την διεύθυνση (IP) της συσκευής η οποία παράγει την πληροφορία όσο και την διεύθυνση (IP) της συσκευής προορισμού, καθώς επίσης και το IP πρωτόκολλο των πακέτων δεδομένων (TCP, UDP, ICMP).

Ο παρακάτω πίνακας συγκρίνει τις Standard και Extended Access Lists.

Πληροφορίες Πακέτου	**Standard IP ACL**	**Extended IP ACL**
Source Address	Ναι	Ναι
Destination Address	Όχι	Ναι
IP protocol (i.e. TCP or UDP)	Όχι	Ναι
Protocol information (i.e. port number)	Όχι	Ναι

Οι Access Lists είναι ένα σύνολο εντολών οι οποίες ομαδοποιούνται και αναγνωρίζονται μέσω ενός μοναδικού αριθμού ή ονόματος. Τα πακέτα πληροφοριών τα οποία εισέρχονται στον Δρομολογητή (Router) επεξεργάζονται με ένα καθορισμένο τρόπο. Συγκεκριμένα, το πακέτο δεδομένων εξετάζεται από κάθε μία από τι εντολές ξεχωριστά μέχρι να βρεθεί μία αντιστοιχία. Η εντολή η οποία βρίσκεται στη κορυφή της λίστας εξετάζει πρώτη το πακέτο, αν δεν βρεθεί αντιστοιχία ανάμεσα στην πληροφορία την οποία εξετάζει η εντολή και στο περιεχόμενο του πακέτου τότε αυτό εξετάζεται από την δεύτερη εντολή της λίστας. Η διαδικασία αυτή συνεχίζεται μέχρι να βρεθεί αντιστοιχία ανάμεσα στο περιεχόμενο πληροφορίας του πακέτου δεδομένου και σε μία εντολή της Access List.

Αν βρεθεί αντιστοιχία τότε:

- Είτε επιτρέπεται η διέλευση του πακέτου (Permit)
- Είτε απαγορεύεται η διέλευση του πακέτου (Deny)

Αν δεν βρεθεί κάποια αντιστοιχία τότε το πακέτο απορρίπτεται από τον Router και δεν επιτρέπεται η διέλευση του και η διάδοση του μέσω αυτού.

Σύμφωνα λοιπόν με τα παραπάνω καταλαβαίνουμε ότι η σειρά, με την οποία είναι τοποθετημένες οι εντολές, είναι πολύ σημαντική για το αποτέλεσμα του ελέγχου των πακέτων δεδομένων. Τέλος αν βρεθεί μία αντιστοιχία, τότε δεν εξετάζονται οι υπόλοιπες εντολές της λίστας.

Implicit Deny

Όπως αναφέρθηκε παραπάνω, αν δεν υπάρξει καμία αντιστοιχία ανάμεσα στο πακέτο δεδομένων και στις εντολές τις Access Control List τότε το πακέτο απορρίπτεται. Το αποτέλεσμα της διαδικασίας αυτής ονομάζεται Implicit Deny.

Στο τέλος των εντολών κάθε Access Lists υπάρχει μια μη ορατή εντολή η οποία απορρίπτει τα πακέτα δεδομένων στα οποία δεν βρέθηκε κάποια αντιστοιχία με τις προηγούμενες εντολές. Κατά συνέπεια σε κάθε Access Control List θα πρέπει να υπάρχει τουλάχιστον μια εντολή Permit, ειδάλλως αν η Access Control List περιέχει μόνο εντολές Deny τότε όλη η κίνηση, η οποία διέρχεται από τον Δρομολογητή (Router), θα απορρίπτεται, δεδομένου της εντολής Implicit Deny στο τέλος της Access List.

10.2 Βασική διαμόρφωση ACL

Η δημιουργία μιας Access Control List δεν είναι μια απλή διαδικασία. Για την αποφυγή προβλημάτων και δυσλειτουργιών θα ήταν καλό να έχουμε υπόψιν μας τις ακόλουθες οδηγίες.

- Η σειρά με την οποία είναι τοποθετημένες οι εντολές σε μια λίστα είναι σημαντική. Τοποθετήστε τις περισσότερο περιοριστικές εντολές στην κορυφή της λίστας και τις λιγότερο περιοριστικές στο τέλος αυτής.
- Οι εντολές μιας Access Control List επεξεργάζονται από την πρώτη προς την τελευταία. Αν βρεθεί μία αντιστοιχία τότε δεν εξετάζονται οι υπόλοιπες εντολές.
- Αν δεν βρεθεί καμία αντιστοιχία, τότε το πακέτο δεδομένων απορρίπτεται.
- Κάθε Access Control List αναγνωρίζεται με ένα μοναδικό αριθμό ή ένα μοναδικό όνομα.
- Ο Δρομολογητής δεν μπορεί να φιλτράρει την κυκλοφορία που, ο ίδιος, δημιουργείσαι.
- Μπορούμε να έχουμε μόνο μία IP Access Control List η οποία να εφαρμόζεται σε ένα interface για κάθε κατεύθυνση (εισερχόμενη πληροφορία – inbound, εξερχόμενη πληροφορία - outbound). Δεν μπορούμε να έχουμε δύο ή περισσότερες inbound ή outbound Access Lists για κάθε interface.
- Αν εφαρμόσουμε μια κενή Access Control List σε ένα interface τότε όλα τα πακέτα δεδομένων θα εισέρχονται ή εξέρχονται ελεύθερα. Προκειμένου μια Access Control List να περιέχει την μη ορατή εντολή Implicit Deny θα πρέπει να αποτελείται από τουλάχιστον μία εντολή Deny ή Permit.

Για να δημιουργήσουμε μια ACL, θα πρέπει να γράψουμε την ακόλουθη εντολή:

Router(config)# ***access-list*** *ACL_#* ***permit***|***deny*** *conditions*

Ο σκοπός της παραμέτρου ACL_# είναι να ομαδοποιήσει όλες τις εντολές σε έναν ενιαίο κατάλογο. Δεν μπορούμε να επιλέξουμε οποιοδήποτε αριθμός για μία ACL. Κάθε πρωτόκολλο του επιπέδου-3 αντιστοιχεί σε ένα ορισμένο πεδίο αριθμών.
Στον πίνακα που ακολουθεί, φαίνονται τα πεδία των αριθμών τα οποίοι αντιστοιχούν στα διάφορα πρωτόκολλα.

ACL Type	ACL Number
IP Standard	1–99, 1300–1999
Standard Vines	1–99
IP Extended	100–199, 2000–2699
Extended Vines	100–199
Bridging type code (layer-2)	200–299
DECnet	300–399
Standard XNS	400–499

Extended XNS	500–599
AppleTalk	600–699
Bridging MAC address and vendor code	700–799
IPX Standard	800–899
IPX Extended	900–999
IPX SAP filters	1000–1099
Extended transparent bridging	1100–1199
IPX NLSP	1200–1299

Ένα μειονέκτημα των numbered ACLs έναντι των named ACLs είναι ότι μπορούμε να δημιουργήσουμε μόνο ένα περιορισμένο αριθμό numbered ACLs. Ο αριθμός αυτός είναι αντίστοιχος με την κλίμακα των αριθμών οι οποίοι αντιστοιχούν σε κάθε πρωτόκολλο. Αντίθετα ο μόνος περιορισμός των named ACLs είναι το μέγεθος της RAM και της NVRAM.

Η παράμετρος conditions περιγράφει ποιο είναι το περιεχόμενο ενός πακέτου δεδομένων το οποίο θα πρέπει να εξεταστεί, προκειμένου να βρεθεί αν υπάρχει αντιστοιχία με την εντολή της λίστας. Η παράμετρος αυτή μπορεί να προσδιορίζει διεύθυνση IP ή κάποιο πρωτόκολλο.

10.3 Ενεργοποίηση και επεξεργασία ACL

Προκειμένου να ενεργοποιήσουμε μια IP ACL, ώστε να μπορεί να ελέγχει τα πακέτα πληροφοριών τα οποία μετακινούνται μεταξύ των interfaces, θα πρέπει να εφαρμοστεί στο κατάλληλο interface ή interfaces:

Router(config)# ***interface*** *type [module_#/]port_#*
Router(config-if)# ***ip access-group*** *ACL_#* ***in|out***

Η εντολή ***ip access-group*** ενεργοποιεί μια Access Control List σε ένα interface.

Η παράμετρος *ACL_#* είναι ένας αριθμός και προσδιορίζει ποια ακριβώς ACL εφαρμόζεται στο συγκεκριμένο interface.
Η παράμετρος ***in|out*** προσδιορίζει την κατεύθυνση κατά την οποία θα εφαρμοστεί η ACL. Υπάρχουν δύο επιλογές:

- Εισερχόμενη πληροφορία (in)
- Εξερχόμενη πληροφορία (out)

Σε μια numbered Access Control List είναι αδύνατο να σβήσουμε μία μεμονωμένη εντολή. Αντίθετα μπορούμε να σβήσουμε ολόκληρη την Access List.

Για να σβήσουμε μια Access Control List χρησιμοποιούμε την εντολή:

Router(config)# no **access-list** ACL_#

Όπου ACL_# είναι το νούμερο της συγκεκριμένης λίστας.

Όταν εισάγουμε μια καινούργια εντολή σε μία ήδη υπάρχουσα λίστα τότε αυτή προστίθεται αυτόματα στο τέλος της λίστας. Η καινούργια εντολή είναι αδίνατο να παρεμβληθεί στη μέση ή στην αρχή της λίστας.

Τέλος είναι αδύνατον να τροποποιήσουμε μία εντολή η οποία είναι ήδη εισηγμένη σε μια ACL.

Wildcard Masks: Όπως έχουμε δει μέχρι τώρα κατά την δήλωση των δικτυακών διευθύνσεων (IP), χρησιμοποιούμε την subnet mask, προκειμένου να μπορέσουμε να διαφοροποιήσουμε τα bit τα οποία προσδιορίζουν την διεύθυνση του δικτύου από αυτά που προσδιορίζουν την διεύθυνση των hosts. Οι ACLs χρησιμοποιούν την wildcard mask προκειμένου να επιτύχουν το ίδιο στόχο. Παρόλα αυτά οι wildcard masks, δεν είναι ίδιες με τις subnet masks αλλά παρουσιάζουν κάποιες διαφορές ως προς την λειτουργία τους.

Η κύρια διαφορά τους είναι ότι στην wildcard mask η ύπαρξη ενός 0 σε μια θέση bit σημαίνει ότι η αντίστοιχη θέση στη διεύθυνση δικτύου της ACL θα πρέπει να είναι ίδια με την τιμή του bit στην αντίστοιχη θέση της δικτυακής διεύθυνση του υπό εξέταση πακέτου. Αντίστοιχα η ύπαρξη ενός 1 σε μια θέση bit σημαίνει ότι η αντίστοιχη θέση στη διεύθυνση δικτύου της ACL δεν θα πρέπει να είναι ίδια με την τιμή του bit στην αντίστοιχη θέση της δικτυακής διεύθυνση του υπό εξέταση πακέτου. Σύμφωνα με τα παραπάνω, μια wildcard mask καθορίζει ποια bits της IP διεύθυνσης του πακέτου πληροφορίας θα πρέπει να αντιστοιχούν με τα bits της IP διεύθυνσης της ACL.

Από τα παραπάνω μπορούμε να αντιληφθούμε ότι η wildcard mask είναι κατά κάποιο τρόπο η αντίστροφη μορφή της subnet mask. Για παράδειγμα αν σε μια Access Control List θέλουμε να ελέγξουμε την διεύθυνση ενός δικτύου το μόνο που έχουμε να κάνουμε είναι να αντιστρέψουμε τα bits της subnet mask (όπου υπάρχει 1 το μετατρέπουμε σε 0, και αντίστροφα όπου υπάρχει 0 το μετατρέπουμε σε 1) και με αυτό τον τρόπο να πάρουμε την αντίστοιχη wildcard mask. Στον παρακάτω πίνακα παρουσιάζονται οι διαφορές μεταξύ subnet mask και wildcard mask.

Bit Value	**Subnet Mask**	**Wildcard Mask**
0	Host Component	Must Match
1	Network Component	Ignore

Ας εξετάσουμε το παρακάτω παράδειγμα παράδειγμα.

Υποθέτουμε ότι έχουμε την ακόλουθη subnet mask 255.255.255.248 την οποία θέλουμε να μετατρέψουμε σε wildcard mask. Αν την παραπάνω subnet mask την μετατρέψουμε σε bits τότε θα προκύψει:

11111111.11111111.11111111.11111000

Προκειμένου να μετατρέψουμε την subnet mask σε wildcard mask το μόνο που έχουμε να κάνουμε είναι να αντιστρέψουμε τα bits οπότε προκύπτει:

00000000.00000000.00000000.00000111

Η wildcard mask σε δεκαδική μορφή είναι:

0.0.0.7

Ένας ευκολότερος τρόπος για την μετατροπή μιας subnet mask σε wildcard mask είναι να αφαιρούμε από το 255 την τιμή του κάθε byte της subnet mask. Έτσι για το παραπάνω παράδειγμα θα προέκυπτε:

Πρώτο byte: 255 – 255 = 0 (Η τιμή της wildcard mask)

Δεύτερο byte: 255 – 255 = 0 (Η τιμή της wildcard mask)
Τρίτο byte: 255 – 255 = 0 (Η τιμή της wildcard mask)
Τέταρτο byte: 255 – 248 = 7 (Η τιμή της wildcard mask)

Το αποτέλεσμα που προκύπτει είναι η ακόλουθη ψ:

0.0.0.7

Ειδικές Wildcard Masks: Υπάρχουν δύο ειδικοί τύποι wildcard mask:

- (host mask)
- (any)

Όταν εφαρμόζουμε την host mask την ACL τότε όλα τα bits της υπό εξέτασης IP διεύθυνσης του πακέτου δεδομένων θα πρέπει να ταιριάζει απόλυτα με την IP διεύθυνση της ACL προκειμένου ο Router να εκτελέσει την εντολή της ACL.

Η δεύτερη μορφή της wildcard mask έχει την ακριβώς αντίθετη λειτουργία από την host mask. Σε αυτή την περίπτωση η εντολή της ACL θα εκτελεστεί ανεξάρτητα από το ποια είναι η υπό εξεταζόμενη διεύθυνση του IP πακέτου.

10.4 Τύποι ACLs

Standard Numbered ACLs

Όπως έχουμε πει οι standard IP ACLs εξετάζουν μόνο την διεύθυνση αφετηρίας (source IP address) του IP πακέτου. Η δημιουργία μιας standard IP ACL γίνεται με την παρακάτω εντολή:

Router(config)# **access-list 1-99|1300-1999 permit|deny** source_IP_address [wildcard_mask] [**log**]

Όπως φαίνεται μια standard IP ACL παίρνει τιμές από 1-99 και 1300-1999, στη συνέχεια ακλουθεί η ενέργεια η οποία πρέπει να εκτελεστεί αν βρεθεί αντιστοιχία στη IP διεύθυνση της ACL και του υπό εξεταζόμενου πακέτου. Παρατηρούμε ότι η διεύθυνση που εξετάζεται είναι η source IP address. Η wildcard mask προσδιορίζει τα bits τα οποία θα πρέπει να ταιριάζουν μεταξύ της wildcard mask και του εξεταζόμενου πακέτου. Η τελευταία παράμετρος log μας δίνει την δυνατότητα της παρουσίασης των IP πακέτων που ταιριάζουν με τα κριτήρια της ACL στη console port.
Τα μηνύματα αυτά δεν θα εμφανίζονται σε μια Telnet σύνδεση με τον Router, εκτός και αν εκτελέσομε την παρακάτω εντολή:

Router# **terminal monitor**

Προκειμένου να ενεργοποιήσουμε μια standard IP ACL εκτελούμε τις ακόλουθες εντολές:

Router(config)# **interface** type [module_#]port_#
Router(config-if)# **ip access-group** ACL_# **in|out**

Παράδειγμα

Router(config)# **access-list 1 permit 192.168.1.1**
Router(config)# **access-list 1 deny 192.168.1.2**

Router(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**
Router(config)# **access-list 1 deny any**
Router(config)# **interface serial 0**
Router(config-if)# **ip access-group 1 in**

Στο παραπάνω παράδειγμα, η πρώτη εντολή της access control list θα επιτρέψει την διέλευση του IP πακέτου στο οποίο η source IP address έχει τιμή 192.168.1.1. Στην εντολή αυτή η wildcard mask παραλείπεται, οπότε η wildcard mask παίρνει την προεπιλεγμένη τιμή της 0.0.0.0. Δηλαδή η εντολή εκτελείται μόνο αν η IP διεύθυνση του πακέτου είναι ακριβώς ίδια με την IP διεύθυνση της εντολής.

Σε περίπτωση που δεν υπάρξει αντιστοιχία των διευθύνσεων το IP πακέτο θα εξεταστεί από την δεύτερη εντολή. Η εντολή αυτή θα απαγόρευση την διέλευση του IP πακέτου αν η source address έχει τιμή 192.168.1.2.

Αν και σε αυτή την περίπτωση δεν βρεθεί αντιστοιχία τότε εξετάζεται η Τρίτη εντολή. Η εντολή αυτή επιτρέπει την διέλευση των πακέτων τα οποία έχουν source IP address μεταξύ των τιμών 192.168.1.0 – 192.168.1.255.

Αν η source IP address του πακέτου δεδομένων δεν βρίσκεται μέσα σε αυτό το σύνολο των τιμών τότε εκτελείται η τελευταία εντολή η οποία σταματάει την διέλευση όλων των πακέτων ανεξάρτητα από την source IP address. Η εντολή αυτή δεν είναι απαραίτητη, εφόσον στο τέλος κάθε ACL υπάρχει μια μη ορατή εντολή implicit deny.

Οι τελευταίες δύο εντολές ενεργοποιούν την ACL στο interface serial 0 και φιλτράρουν την εισερχόμενη κίνηση.

Παρατηρώντας το παραπάνω παράδειγμα, μπορούμε να δούμε ότι η πρώτη εντολή ουσιαστικά ενσωματώνεται στην τρίτη, ενώ όπως είπαμε η τέταρτη εντολή δεν είναι απαραίτητη. Επομένως το παράδειγμα μας, μπορεί να γραφτεί ως εξής:

Router(config)# **access-list 1 deny 192.168.1.2**
Router(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**
Router(config)# **interface serial 0**
Router(config-if)# **ip access-group 1 in**

Προκειμένου να ελέγξουμε και να περιορίσουμε την πρόσβαση στον Router μας μέσω Telnet μπορούμε να δημιουργήσουμε μια standard access control list και να την εφαρμόσουμε – ενεργοποιήσουμε στη virtual terminal line (VTY) του Telnet. Οι εντολές που εκτελούμε είναι οι ακόλουθες:

Router(config)# **line vty 0 4**
Router(config-line)# **access-class** standard_ACL_# **in**|**out**

Παρατηρούμε ότι η εντολή που εκτελούμε για την ενεργοποίηση της ACL (**access-class**) είναι διαφορετική από την ενεργοποίηση μια ACL σε ένα interface. Χρησιμοποιώντας την παράμετρο **in** φιλτράρουμε την πρόσβαση μέσω Telnet στον Δρομολογητής μας. Αντίθετα η παράμετρος **out** περιορίζει του προορισμούς στους οποίους ο Δρομολογητής μας μπορεί να έχει πρόσβαση εκτελώντας την εντολή Telnet.

Extended Numbered ACLs

Οι Extended ACLs μας δίνουν την δυνατότητα να εφαρμόσουμε περισσότερα κριτήρια στο φιλτράρισμα ενός IP πακέτου απ' ότι οι Standard ACLs. Έτσι μέσω μίας Extended ACL μπορούμε να ελέγξουμε τις ακόλουθες πληροφορίες:

- Source και destination IP addresses
- IP protocol—IP, TCP, UDP, ICMP
- Λεπτομερείς πληροφορίες για το πρωτόκολλο, όπως port numbers για TCP και UDP, η τύπου μηνυμάτων για πακέτα ICMP

Η δημιουργία μίας Extended Numbered ACL γίνεται με την ακόλουθη εντολή:

Router(config)# **access-list 100-199|2000-2699 permit|deny**
IP_protocol
source_address source_wildcard_mask
[protocol_information]
destination_address destination_wildcard_mask
[protocol_information] [**log**]

Οι Extended IP Numbered ACLs μπορούν να χρησιμοποιήσουν για τον ορισμό τους ένα αριθμό ο οποίος να βρίσκεται μέσα στην ακόλουθη κλίμακα 100–199 και 2000–2699. Μετά την ενέργεια η οποία θα πρέπει να εκτελεστεί (**permit** ή **deny**) ακολουθεί το πρωτόκολλο IP το οποίο εξετάζεται από την εντολή. Τα πρωτόκολλα τα οποία εξετάζονται είναι τα ακόλουθα: **ip**, **icmp**, **tcp**, **gre**, **udp**, **igrp**, **eigrp**, **igmp**, **ipinip**, **nos**, και **ospf**. Χρησιμοποιώντας την παράμετρο **ip** μπορούμε ελέγξουμε κάθε IP πρωτόκολλο (TCP, UDP, ICMP). Στη συνέχεια παρατηρούμε ότι δηλώνεται και εξετάζεται τόσο η source IP address όσο και η destination IP addresses καθώς επίσης και οι αντίστοιχες wildcard masks. Με τις Extended IP Numbered ACLs μπορούμε να ελέγξουμε περισσότερες πληροφορίες σε ορισμένα IP πρωτόκολλα. Έτσι στη περίπτωση των πρωτοκόλλων TCP και UDP μπορούμε να φιλτράρουμε το source και destination port number, ενώ στην περίπτωση των πακέτων ICMP μπορούμε να ελέγξουμε τον τύπο μηνύματος.

Για την δημιουργία μιας extended ACL που να ελέγχει πακέτα TCP η UDP χρησιμοποιούμε την ακόλουθη σύνταξη:

Router(config)# **access-list 100-199|2000-2699 permit|deny**
tcp|udp
source_address source_wildcard_mask
[operator source_port_#]
destination_address destination_wildcard_mask
[operator destination_port_#]
[**established**] [**log**]

Operators. Στις extended ACLs, οι οποίες εξετάζουν πακέτα TCP και UDP, όπως είδαμε μπορούμε να φιλτράρουμε το source και destination port number. Προκειμένου να προσδιορίσουμε το είδος του ελέγχου που θα γίνει επάνω σε αυτές της πληροφορίες χρησιμοποιούμε τους operators.
Στην επόμενο πίνακα παρουσιάζεται μια λίστα με τους operators.

Operator	Εξήγηση

lt	Μικρότερο από
gt	Μεγαλύτερο από
neq	Όχι ίσο με
eq	Ίσο με
range	κλίμακα από port numbers

Ports Numbers and Names. Για συνδέσεις TCP και UDP μπορούμε να χρησιμοποιούμε είτε το port number είτε το port name. Για παράδειγμα, προκειμένου να φιλτράρουμε την κίνηση telnet, μπορούμε είτε να χρησιμοποιήσουμε την λέξη κλειδί telnet είτε το νούμερο της πόρτας 23.
Οι ακόλουθοι πίνακες παρουσιάζουν τα πιο συνηθισμένα ονόματα και νούμερα πορτών για TCP και UDP αντίστοιχα.

Port Name	**Command Parameter**	**Port Number**
FTP Data	ftp-data	20
FTP Control	ftp	21
Telnet	telnet	23
SMTP	smtp	25
WWW	www	80

Port Name	**Command Parameter**	**Port Number**
DNS Query	dns	53
TFTP	tftp	69
SNMP	snmp	161
IP RIP	rip	520

Φιλτράρισμα πακέτων ICMP. Η σύνταξη της Extended Numbered ACL η οποία φίλτραρε τα ICMP πακέτα είναι η ακόλουθη:

Router(config)# **access-list 100-199|2000-2699 permit|deny icmp**
source_address source_wildcard_mask
destination_address destination_wildcard_mask
[icmp_message] [**log**]

Σε αντίθεση με το TCP και UDP, τα ICMP πακέτα δεν χρησιμοποιούν νούμερα πορτών αλλά τύπους μηνυμάτων. Στον επόμενο πίνακα παρουσιάζονται οι συνηθισμένοι τύποι μηνυμάτων για το ICMP.

Τύπος Μηνύματος	**Περιγραφή Μηνύματος**
administratively-prohibited	Μήνυμα το οποίο μας λέει ότι κάποιος φίλτραρε ένα πακέτο
echo	Χρησιμοποιείται από την εντολή ping για να ελέγξει ένα προορισμό
echo-reply	Η απάντηση σε ένα μήνυμα echo το οποίο δημιουργήθηκε από την εντολή ping
host-unreachable	Έχουμε πρόσβαση στο subnet αλλά όχι στον host.
net-unreachable	Ο host Και το subnet δεν είναι προσβάσημα
traceroute	Φιλτράρισμα των πληροφοριών οι οποίες προέρχονται

	από την εντολή traceroute

Η ενεργοποίηση μιας extended numbered IP ACL γίνεται με την ακόλουθη εντολή:

Router(config)# **interface** type [module_#] port_#
Router(config-if)# **ip access-group** ACL_# **in**|**out**

Παράδειγμα

Router(config)# **access-list 100 permit tcp any 172.16.0.0 0.0.255.255**
established log
Router(config)# **access-list 100 permit udp any host 172.16.1.1 eq dns**
Router(config)# **access-list 100 permit tcp 172.17.0.0 0.0.255.255**
host 172.16.1.2 eq telnet
Router(config)# **access-list 100 permit icmp any 172.16.0.0 0.0.255.255**
echo-reply
Router(config)# **access-list 100 deny ip any any**
Router(config)# **interface ethernet 0**
Router(config-if)# **ip access-group 100 in**

Η παραπάνω Extended Numbered ACL εφαρμόζεται στο interface **ethernet 0** και φιλτράρει όλη την εισερχόμενη κίνηση.

Η πρώτη εντολή επιτρέπει την διέλευση ενός TCP πακέτου πληροφορίας το οποίο έχει παραχθεί από οποιοδήποτε διεύθυνση αφετηρίας και η διεύθυνση προορισμού είναι 172.16.0.0/16, ενώ παράλληλα τα bits RST/ACK στο TCP header είναι ίσα με 1(**established**). Εφόσον δεν έχουμε προσδιορίσει κάποιο port number όλη η TCP πληροφορία θα φιλτράρεται από αυτή την εντολή.

Η δεύτερη εντολή επιτρέπει την διέλευση ενός DNS query από οποιαδήποτε IP source address προς το host 172.16.1.1.

Η τρίτη εντολή επιτρέπει οποιαδήποτε telnet σύνδεση η οποία προέρχεται από το δίκτυο 172.17.0.0/16 προς το host 172.16.1.2.

Η τέταρτη εντολή επιτρέπει οποιοδήποτε ICMP πακέτο με τύπο μηνύματος echo-reply (δηλαδή απάντηση σε μια εντολή ping) να κατευθυνθεί στις συσκευές του δικτύου 172.16.0.0./16.

Η πέμπτη εντολή κόβει τα πακέτα πληροφοριών τα οποία δεν ταιριάζουν στα κριτήρια των προηγούμενων εντολών.

Named ACLs

Το πιο σημαντικό μειονέκτημα των numbered ACLs είναι ότι μπορούμε να δημιουργήσουμε ένα περιορισμένο αριθμό ACLs. Ο αριθμός αυτός των ACLs εξαρτάται από τις ακόλουθες κλίμακες: Standard ACL 1-99 και 1300-1999, Extended ACL 100-199 και 2000-2699.
Προκειμένου να προσπεράσουμε αυτό τον περιορισμό η CISCO δημιούργησε της Named ACLs. Σύμφωνα με αυτό τον τύπο των Access Control Lists μπορούμε να χρησιμοποιήσουμε ένα όνομα για

να αναφερθούμε σε ένα σύνολο εντολών access control.

Για να δημιουργήσουμε μια named IP ACL, χρησιμοποιούμε την ακόλουθη εντολή:

Router(config)# **ip access-list standard|extended** ACL_name

Η πρώτη παράμετρος που θα πρέπει να προσδιορίσουμε είναι ο τύπος της ACL: standard ή extended. Στη συνέχεια θα πρέπει να δώσουμε ένα όνομα το οποίο θα χρησιμοποιηθεί σαν αναφορά για την λίστα μας. Το όνομα αυτό θα πρέπει να είναι μοναδικό σε σχέση με όλες τις υπόλοιπες named ACLs. Μετά την εκτέλεση αυτής της εντολής μετακινούμαστε στο κατάλληλο Subconfiguration mode, όπως φαίνεται και παρακάτω:

Router(config-std-acl)#
-ή-
Router(config-ext-acl)#

Στη συνέχεια εκτελούμε τις κατάλληλες εντολές:

Standard Named ACL:
Router(config)# **ip access-list standard** ACL_name
Router(config-std-acl)# **permit**|**deny** source_IP_address [wildcard_mask]

Extended Named ACL:
Router(config)# **ip access-list extended** ACL_name
Router(config-ext-acl)# **permit**|**deny** IP_protocol source_IP_address wildcard_mask [protocol_information] destination_IP_address wildcard_mask
[protocol_information] [**log**]

Μόλις δημιουργήσουμε μια named ACL, θα πρέπει να την ενεργοποιήσουμε σε ένα interface του Δρομολογητή σύμφωνα με την παρακάτω σύνταξη:

Router(config)# **interface** type [module_#] port_#
Router(config-if)# **ip access-group** ACL_name **in**|**out**

Παράδειγμα
Σε αυτό το παράδειγμα θα μετατρέψουμε την extended IP numbered ACL από την προηγούμενη ενότητα σε extended IP named ACL:

Router(config)# **ip access-list extended do_not_enter**
Router(config-ext-acl)# **permit tcp any 172.16.0.0 0.0.255.255**
established
Router(config-ext-acl)# **permit udp any host 172.16.1.1 eq dns**
Router(config-ext-acl)# **permit tcp 172.17.0.0 0.0.255.255**
host 176.16.1.2 eq telnet
Router(config-ext-acl)# **permit icmp any 176.16.0.0 0.0.255.255**
echo-reply
Router(config-ext-acl)# **deny ip any any**

Router(config)# **interface ethernet 0**
Router(config-if)# **ip access-group do_not_enter in**
Και οι δύο εκδόσεις της ACL προκαλούν τα ίδια αποτελέσματα.

Αφού δημιουργήσουμε και ενεργοποιήσουμε μια ACL, μπορούμε να την ελέγξουμε χρησιμοποιώντας διάφορες εντολές **show.**
Μια συνηθισμένη εντολή την οποία χρησιμοποιούμε στη λειτουργία *Privilege EXEC* είναι η εντολή ***show*** *running-config*. Η εντολή αυτή εμφανίζει την ACL που δημιουργήσαμε καθώς επίσης και σε ποιο interface ή interfaces έχει ενεργοποιηθεί. Ωστόσο, υπάρχουν πολλές άλλες εντολές τις οποίες μπορούμε να χρησιμοποιήσουμε.

Για να δούμε ποιες ACLs είναι ενεργοποιημένες στα interfaces του Δρομολογητή μας χρησιμοποιούμε την εντολή: ***show*** *ip interfaces* **.**

Για να δούμε τις εντολές που αποτελούν μια ACL, χρησιμοποιούμε τις παρακάτω εντολές:

Router# **show access-lists** [ACL_#_or_name]
Router# **show ip access-list** [ACL_#_or_name]

Μπορούμε να μηδενίσουμε τους μετρητές αυτούς με την παρακάτω εντολή:

Router# **clear access-list counters** [ACL_#_or_name]

Σχετικά με την τοποθέτηση των ACLs θα πρέπει να ακολουθούμε τους παρακάτω κανόνες:

- Οι Standard ACLs θα πρέπει να τοποθετούνται κοντά στις συσκευές προορισμού

- Οι Extended ACLs θα πρέπει να τοποθετούνται κοντά στις συσκευές δημιουργίας των μηνυμάτων που θέλουμε να φιλτράρουμε

Standard ACLs . Οι Standard ACLs ελέγχουν μόνο την IP διεύθυνση της συσκευής δημιουργίας του μηνύματος. Αν λοιπόν τοποθετήσουμε αυτές τις ACLs κοντά στη συσκευή δημιουργίας των δεδομένων τότε θα παρεμποδίσουμε την συνολική εκπομπή δεδομένων προς όλες τις υπόλοιπες συσκευές του δικτύου. Για το λόγο αυτό οι Standard ACLs θα πρέπει να τοποθετούνται κοντά στον προορισμό τον οποίο θέλουμε να εμποδίσουμε από το να λάβει δεδομένα από μια συγκεκριμένη συσκευή.

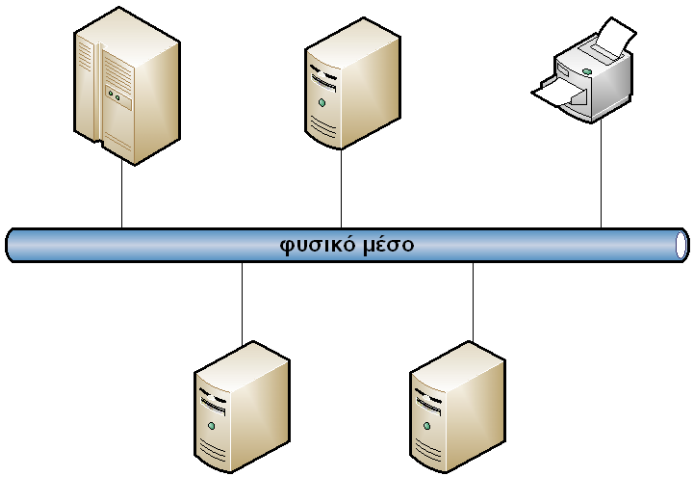
Extended ACLs. Οι Extended ACLs ελέγχουν τόσο την διεύθυνση δημιουργίας των δεδομένων όσο και την διεύθυνση προορισμού. Εκμεταλλευόμενοι αυτή την ιδιότητα τοποθετούμε τις Extended ACLs κοντά στη συσκευή δημιουργίας του μηνύματος. Με τον τρόπο αυτό παρεμποδίζουμε την κίνηση μη επιθυμητών IP πακέτων στο δίκτυο μας, ενώ παράλληλα επιτρέπουμε την αποστολή δεδομένων σε επιθυμητούς προορισμούς.

11. Μεταγωγείς (switches)

11.1 Εισαγωγή στους μεταγωγείς

Οι ρίζες της τεχνολογίας Ethernet βρίσκονται στην δεκαετία του 1960, στο πειραματικό τότε σύστημα

Aloha του Πανεπιστημίου της Χαβάης. Σήμερα, έχουν περάσει περισσότερα από 25 χρόνια από την εποχή που το Ethernet τυποποιήθηκε και έγινε παγκόσμιο στάνταρντ. Από τα 3 Mbps της αρχικής του έκδοσης, έχει πλέον φθάσει σε ταχύτητες 10 Gbps περνώντας από τα «ορόσημα» των 10, 100 Mbps και 1 Gbps. Το Ethernet είναι σήμερα η δημοφιλέστερη τεχνολογία υλοποίησης τοπικών δικτύων (LAN), τάση που δεν φαίνεται να αλλάζει.
Η αρχική σχεδίαση του Ethernet έγινε με βάση τη λογική ότι πολλές συσκευές θα ήταν συνδεδεμένες πάνω στο ίδιο φυσικό μέσον –τυπικά, ένα καλώδιο – μέσα από το οποίο θα επικοινωνούν και ανταλλάσσουν δεδομένα (εικ. 11.1).



Εικόνα 11.1 - Διαμοιραζόμενος Τομέας Ethernet

Όπως γνωρίζουμε, οι δικτυακές συσκευές έρχονται σε επαφή με το καλώδιο μέσω ειδικής κάρτας δικτύου που διαθέτουν (NIC). Κάθε κάρτα NIC φέρει ένα μοναδικό αναγνωριστικό που το Ethernet, σε επίπεδο 2 (OSI Layer 2, Data Link), χρησιμοποιεί για να αναγνωρίζει την κάθε συσκευή που είναι συνεδεδεμένη στο δίκτυο. Η διεύθυνση MAC (Media Access Control address) είναι είναι γραμμένη στα κυκλώματα της NIC με φυσικό τρόπο και έχει μήκος 48 bits.

Προκειμένου να αποφασίζεται ποια συσκευή μπορεί κάθε χρονική στιγμή να χρησιμοποιεί το φυσικό μέσον, το Ethernet χρησιμοποιεί τον αλγόριθμο Ανίχνευσης Φέροντος Σήματος και Εντοπισμού Συγκρούσεων CSMA/CD (Carrier Sense Multiple Access Collision Detect). Υπενθυμίζουμε τα κύρια χαρακτηριστικά του πρωτοκόλλου CSMA/CD:

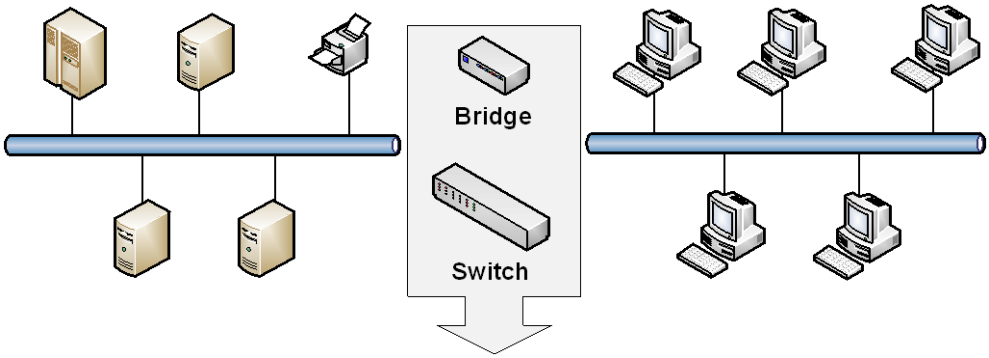
- Όταν μία NIC έχει να μεταδώσει κάποιο frame, «ακούει» στο μέσον για να δει αν τη στιγμή εκείνη κάποιος άλλος ήδη μεταδίδει.
- Σε περίπτωση που το καλώδιο είναι κατειλημμένο, η NIC περιμένει μέχρι να ελευθερωθεί και μετά μεταδίδει, διαφορετικά αν το βρει ελεύθερο μεταδίδει αμέσως.
- Στην περίπτωση που δύο ή περισσότερες NIC, βρίσκοντας το μέσον ελεύθερο, μεταδίδουν ταυτόχρονα τα frames τους, έχουμε Σύγκρουση (Collision) και τα δεδομένα καταστρέφονται.
- Όταν οι συσκευές εντοπίσουν σύγκρουση, περιμένουν κάποιο χρονικό διάστημα που είναι τυχαίο, πιθανότατα διαφορετικό για την καθεμία, και επιχειρούν να ξαναμεταδώσουν.
- Σε περίπτωση νέας σύγκρουσης η διαδικασία επαναλαμβάνεται, με τον χρόνο αναμονής να είναι διαρκώς αυξανόμενος.

Παρόλη την αδιαμφισβήτητη επιτυχία του το πρωτόκολλο αυτό, φυσικά, έχει και μειονεκτήματα. Το κυριότερο πρόβλημα είναι ο υπερπληθυσμός και βέβαια πηγάζει από την ανταγωνιστική φύση του Ethernet. Όσο οι συσκευές αυξάνονται σε ένα δίκτυο, τόσο μεγαλώνει η κίνηση στον δίαυλο και επομένως αυξάνεται η πιθανότητα συγκρούσεων (εικ. 11.1). Αυτό οδηγεί σε

ένα φαύλο κύκλο. Κάθε σύγκρουση έχει σαν αποτέλεσμα την επανεκπομπή των δεδομένων που χάθηκαν και άρα αύξηση της κίνησης στο δίκτυο που με τη σειρά της φέρνει αύξηση της πιθανότητας νέων συγκρούσεων. Τελική κατάληξη είναι η πολύ χαμηλή ταχύτητα κίνησης στο δίκτυο.

Οι συσκευές που συμμετέχουν σε ένα δίκτυο με τα χαρακτηριστικά που μόλις περιγράψαμε λέμε ότι ανήκουν όλες στην ίδια **Επικράτεια ή Τομέα Σύγκρουσης** (Collision Domain).

Το πρόβλημα των αυξημένων συγκρούσεων αντιμετωπίζεται χρησιμοποιώντας ειδικές συσκευές που κυρίως είναι οι **Γέφυρες (Bridges)** και οι **Μεταγωγείς (Switches)** (εικ. 11.2). Τα ειδικά αυτά «κουτιά» διαιρούν τους μεγάλους τομείς σύγκρουσης δημιουργώντας περισσότερους, με λιγότερους υπολογιστές ανά τομέα και επομένως μικρότερο ποσοστό συγκρούσεων. Μια πρώτη προσέγγιση ορίζει ότι οι συγκρούσεις δεν πρέπει να ξεπερνούν το 1% της συνολικής κίνησης σε ένα collision domain.

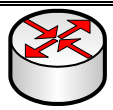
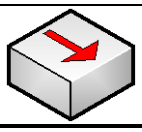


Εικόνα 11.2 – Δύο collision domains

Είναι αλήθεια ότι υπάρχει αρκετή σύγχυση στο θέμα της ορολογίας σε σχέση με τις λειτουργικότητες κάθε συσκευής, που συχνά είναι κοινές ή και αλληλοκαλυπτόμενες. Σε πολύ γενικές γραμμές ωστόσο, μπορούμε να κάνουμε τις παρακάτω παρατηρήσεις για τη σχέση bridge, switch, αλλά και router:

- Οι bridges δουλεύουν μέσω λογισμικού ενώ οι switches μέσω υλικού, πράγμα που συνήθως τους κάνει να είναι ταχύτεροι.
- Μια bridge έχει 2 θύρες ενώ ένας switch περισσότερες. Ωστόσο, αυτό δεν είναι περιοριστικό για τις bridges, δεν υπάρχει δηλαδή κάποιος κανόνας που να απαγορεύει σε μία γέφυρα να έχει περισσότερες από 2 θύρες.
- Οι (συνήθως δύο) θύρες μιας bridge συνδέουν μεταξύ τους ολόκληρα δίκτυα, ενώ οι θύρες ενός switch δημιουργούν μια ένα-προς-ένα σύνδεση μεταξύ δύο κόμβων (υπολογιστών κλπ). Ωστόσο, σήμερα οι switches μπορούν να συνδέονται μεταξύ τους, και ο καθένας να «έχει επάνω του» ένα ολόκληρο LAN.
- Χωρισμό των collision domains κάνει και ο Δρομολογητής (Router). Όμως, ο router δουλεύει σε επίπεδο 3 (Layer 3) του OSI. Οι bridges και switches δουλεύουν σε Layer 2, παρόλο που υπάρχουν και Layer 3 switches. Ακόμα, ένας router εκτός από collision domain δημιουργεί και broadcast domain «κόβοντας» τα broadcasts ανάμεσα στα τμήματα που χωρίζει/συνδέει.

Layer	OSI	Συσκευή	TCP/IP
7	Application		Application
6	Presentation		

5	Session		
4	Transport		Transport
3	Network	**Router** 	**Internet**
		L3 Switch	
2	Data Link	**Bridge** 	**Data Link**
		Switch 	
		NIC	
		Intelligent Hub	
1	Physical	Repeater	Physical
		Hub 	

Πίνακας 11.1 – Επίπεδα & συσκευές

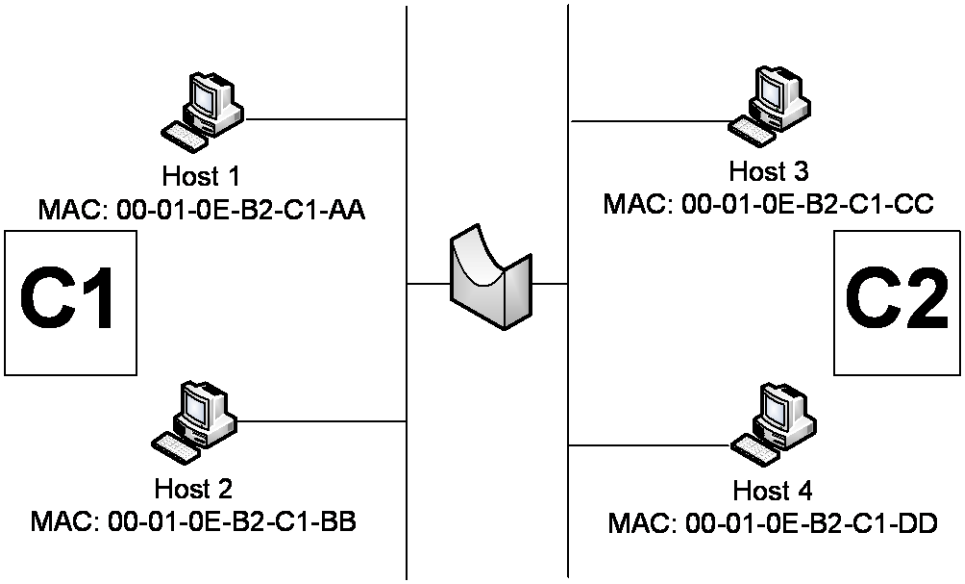
Με τα παραπάνω που αναφέραμε γίνεται κατανοητό ότι bridges, switches και routers (πίνακας 11.1) έχουν κοινά ή αλληλοεπικαλυπτόμενα χαρακτηριστικά. Έχουν όμως και αρκετές διαφορές. Όλα αυτά, και κυρίως οι διαφορές, θα φανούν καλύτερα μόλις δούμε τον τρόπο που ένα bridge/switch λειτουργεί: τις ρυθμίσεις τους, τους αλγόριθμους που χρησιμοποιούν, το πως «βλέπουν» τον κόσμο και τους γείτονές τους κλπ. Στην επόμενη παράγραφο θα δούμε τις βασικές αρχές λειτουργίας του bridging και switching.

11.2 Bridging & Switching

Μια bridge, στην κλασσική περίπτωση, χωρίζει ένα LAN σε 2 collision domains. Ας εξετάσουμε την τοπολογία σύνδεσης της εικόνας 11.3. Οι Host1 και Host2 ανήκουν σε ένα collision domain C1, ενώ οι Host3 και Host4 σε δεύτερο C2. Προκειμένου να γίνει κατανοητή η λειτουργία περιγράφουμε κάποιες περιπτώσεις:

1. **Επικοινωνία στην επικράτεια C1.** Ο Host1 θέλει να μεταδώσει frame για τον Host2. Η NIC του Host1 μόλις βρεί ελεύθερο το φυσικό μέσο εκπέμπει και έστω ότι δεν δημιουργείται σύγκρουση. Το σήμα κινείται σε όλη την επικράτεια του C1, φθάνοντας και στον Host2, ενώ η bridge δεν επιτρέπει να προχωρήσει στην επικράτεια C2.
2. **Επικοινωνία στην επικράτεια C2.** Την ίδια ακριβώς χρονική στιγμή οι Host3 και Host4 μπορούν να επικοινωνούν στα πλαίσια της επικράτειας C2, χωρίς αυτό να προκαλεί συγκρούσεις από την κίνηση δεδομένων στην C1 .
3. **Επικοινωνία μεταξύ C1 & C2.** Εάν ο Host1 θέλει να επικοινωνήσει με τον Host4, τότε η bridge θα αφήσει το frame να περάσει από την επικράτεια C1 στην C2. Στην περίπτωση αυτή, αν ταυτόχρονα θέλει να επικονωνήσει και ο Host3 με τον Host4, τότε είναι πιθανό να

προκληθεί σύγκρουση.



Εικόνα 11.3 – Transparent Bridging

Πως όμως μία bridge κάνει αυτή τη δουλειά; Πως δηλαδή μπορεί να γνωρίζει πότε θα αφήσει δεδομένα που εισέρχονται από τη μία θύρα της, να περάσουν από την άλλη; Η έννοια του transparent bridging καθορίζεται από την προδιαγραφή 802.1D της IEEE και αποτελείται από πέντε διαδικασίες, που ενεργοποιούνται ανάλογα με την περίπτωση:
Learning. Η bridge κρατάει την τοπολογία του δικτύου σε πίνακα που ονομάζεται bridge table, MAC table, port address table ή Content Addressable Memory (CAM) table. Όταν ξεκινάει τη λειτουργία της ο πίνακας είναι κενός. Καθώς στις θύρες της φθάνουν δεδομένα, καταγράφει στον bridge table την MAC address του αποστολέα, καθώς και την θύρα από όπου τα έλαβε (πίνακας 11.2).

Hosts	Port 1	Port 2
Host1 / 00-01-0E-B2-C1-AA	✓	
Host2 / 00-01-0E-B2-C1-BB	✓	
Host3 / 00-01-0E-B2-C1-CC		✓
Host4 / 00-01-0E-B2-C1-DD		✓

Πίνακας 11.2 – Παράδειγμα MAC table

Flooding. Όταν μια bridge δεν γνωρίζει κάποια MAC address παραλήπτη αφήνει τα συγκεκριμμένα δεδομένα να περάσουν από τους τους θύρες τους, εκτός από αυτή απ' όπου τα έλαβε. Με τον τρόπο αυτό αποφεύγεται ο κίνδυνος να χάνονται δεδομένα, περίπτωση πιθανή αν π.χ. συνδεθεί τους τους Host στο δίκτυο αλλά ιδιαίτερα στη φάση Learning, όπου ο πίνακας CAM είναι άδειος. Επιπλέον, η bridge πάντα πλημυρίζει τους τους θύρες (πλην τους που το παρέλαβε) με δεδομένα broadcast (MAC address παραλήπτη
FF-FF-FF-FF-FF-FF) και multicast (π.χ. MAC address παραλήπτη που αρχίζει με 01-00-5E, και τους) .
Οι διαδικασίες Filtering και Forwarding εκτελούνται όταν πλέον η bridge έχει «μάθει» τους διευθύνσεις.
Filtering. Αν η bridge λάβει δεδομένα τους κάποια MAC address που, εξετάζοντας τον πίνακα CAM, δει ότι βρίσκεται στην ίδια επικράτεια με τον αποστολέα (ίδια θύρα) τότε δεν προωθεί σε άλλη θύρα τα

δεδομένα (περιπτώσεις 1 & 2).

Forwarding. Αν η bridge λάβει δεδομένα τους κάποια MAC address που, εξετάζοντας τον πίνακα CAM, δει ότι βρίσκεται σε άλλη επικράτεια από αυτή του αποστολέα (διαφορετικές θύρες) τότε προωθεί στην άλλη θύρα τα δεδομένα (περίπτωση 3).

Aging. Η bridge, εκτός από διευθύνσεις και θύρες, καταχωρεί στον bridge table την χρονική στιγμή που «έμαθε» τη συγκεκριμμένη εγγραφή. Κάθε φορά που προωθεί ή φιλτράρει δεδομένα από αυτή την συσκευή, ο χρόνος ανανεώνεται. Σε περίπτωση που η bridge δεν λάβει δεδομένα από κάποια συσκευή για κάποιο χρονικό διάστημα (εξ ορισμού 5 min), τότε βγάζει τη σχετική εγγραφή από τον bridge table.

Ένα switch, στην ουσία, λειτουργεί σαν το κλασσικό bridge αλλά με πολλαπλές θύρες. Διαχειρίζεται MAC addresses τους και η bridge, επομένως είναι συσκευή επιπέδου 2 (data link layer). Τους σε έναν switch οι επιλογές μεταγωγής των δεδομένων γίνονται μέσω ειδικά σχεδιασμένων υπολογιστικών κυκλωμάτων hardware (application-specific integrated circuits – ASICs).

Μία bridge τους και τους switch κάνουν τρεις βασικές λειτουργίες, από τους οποίες έχουμε ήδη δει τους δυο πρώτες, δηλαδή:

1. Μαθαίνουν πληροφορίες για την τοπολογία του δικτύου, «σε τους θύρα βρίσκεται, τους συσκευή» και τους αποθηκεύουν στον CAM table.
2. Με βάση τους πληροφορίες του CAM table κάνουν έξυπνες επιλογές μεταγωγής των δεδομένων του δικτύου.

Η Τρίτη λειτουργία έχει να κάνει με προβλήματα που παρουσιάζονται όταν σε ένα δίκτυο συνδέουμε περισσότερες από μία bridges. Τους σοβαρός λόγος για να το κάνουμε αυτό είναι η αύξηση τους αξιοπιστίας του δικτύου τους. Αν έχουμε μόνο μια bridge, σε περίπτωση αστοχίας τους η συνδεσιμότητα θα χαθεί. Βάζουμε επομένως και τους ώστε να εξασφαλίσουμε εναλλακτικές διαδρομές. Αυτό δημιουργεί τα λεγόμενα layer-2 loops:

3. Αφαιρούν τους **Βρόγχους 2ου Επιπέδου** (layer-2 loops) που τυχόν υπάρχουν στο δίκτυο. Αυτό το επιτυγχάνουν εκτελώντας τον αλγόριθμο **Spanning Tree Protocol** (STP).

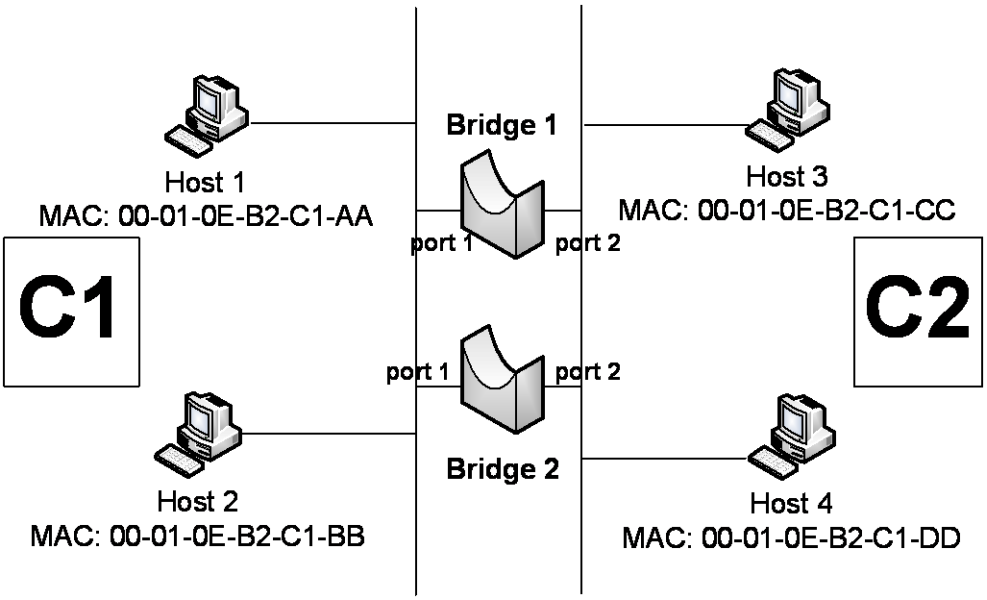
Στην επόμενη παράγραφο θα δούμε το Spanning tree protocol και την εφαρμογή του σε switches και bridges.

11.3 Το Spanning Tree protocol (STP) σε δίκτυα μεταγωγέων.

Η δημιουργία βρόγχων με πλεονάζουσες bridges ή switches αυξάνει την αξιοπιστία του δικτύου μας δημιουργεί όμως, όπως είπαμε, προβλήματα. Για παράδειγμα, στην εικόνα 11.4 έχουμε συνδέσει τα δύο τμήματα (segments) του δικτύου μας με δύο bridges. Στην περίπτωση που, για παράδειγμα, η bridge1 πάψει να λειτουργεί, το δίκτυό μας δεν θα πέσει διότι η κυκλοφορία θα γίνεται μέσω της bridge 2. Τι πρόβλημα μπορεί να δημουργεί ένας τέτοιος σχεδιασμός; Ας δούμε ένα παράδειγμα.

Όπως έχουμε ήδη πει, μια bridge πλημυρίζει (floods), μεταξύ άλλων, τα broadcasts. Έστω ότι ο Host1 από την επικράτεια C1 εκπέμπει ένα broadcast, που λαμβάνεται τόσο από την bridge1 όσο και από την bridge 2. Επειδή πρόκειται για broadcast, και οι δύο bridges το στέλνουν σε όλες τις υπόλοιπες θύρες τους. Αυτό έχει σαν αποτέλεσμα το broadcast να εμφανιστεί δύο φορές στην επικράτεια C2. Κάθε bridge βλέπει το broadcast της άλλης εντός του C2 και το προωθεί στις άλλες θύρες της, επόμένως περνά σε δύο αντίτυπα στον τομέα C1.

Η παραπάνω διαδικασία επαναλαμβάνεται επ' άπειρον καταναλώνοντας εύρος ζώνης (bandwidth) αλλά και υπολογιστικούς πόρους σε όλες τις συσκευές και των δύο τομέων C1 και C2 εφόσον πρέπει να επεξεργαστούν το broadcast ξανά και ξανά.



Εικόνα 11.4 – Bridging (layer-2) loop

Τα προβλήματα αυτά αντιμετωπίζονται με το Spanning Tree Protocol (STP). Πρόκειται για έναν αλγόριθμο που οι switches (bridges) εκτελούν προκειμένου να εξαφανίσουν τα layer-2 loops. Το STP εκτελείται και μπλοκάρει τις πλεονάζουσες θύρες, π.χ. την θύρα 2 της bridge 2. Η απενεργοποίηση γίνεται με λογικό τρόπο, ενώ η φυσική σύνδεση εξακολουθεί να υπάρχει διαθέσιμη για ενεργοποίηση. Όταν τώρα το broadcast φθάσει στην port1 των bridge1 και bridge2, θα περάσει στην επικράτεια C2 μόνο μέσα από την port2 της bridge1, καθόσον η αντίστοιχη της bridge2 είναι ανενεργή (blocked).

Σε κάθε θύρα (port) αντιστοιχίζεται ένα αριθμητικό κόστος (**port cost**) σύμφωνα με τον πίνακα 11.3. Ακόμα σε κάθε θύρα ορίζεται ένας αριθμός προτεραιότητας (εξ ορισμού το 32).

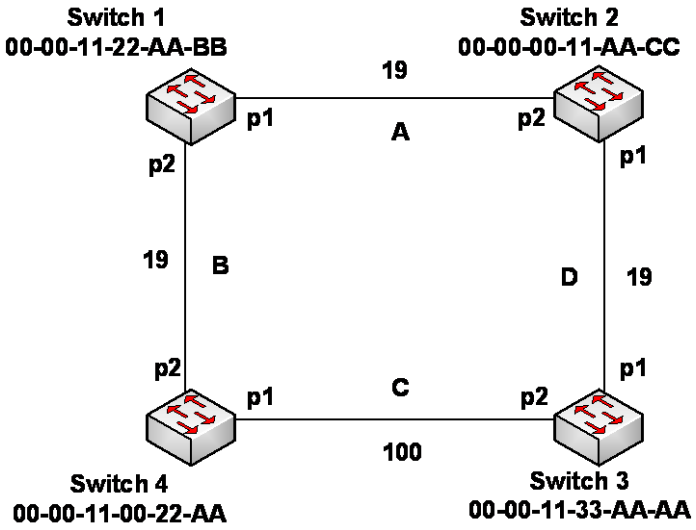
Είδος σύνδεσης	Κόστος
10 Gb	2
1 Gb	4
100 Mb	19
10 Mb	100

Πίνακας 11.3 – port cost

Το πρωτόκολλο STP χρειάζεται επικοινωνία ανάμεσα στους Switches που συμμετέχουν. Αυτή επιτυγχάνεται με την αποστολή ειδικών μηνυμάτων με όνομα Bridge Protocol Data Units (**BPDUs**). Τα BPDUs στέλνονται σαν multicast κάθε 2 δευτερόλεπτα (**Hello timer**) και περιέχουν πληροφορίες που βοηθούν τους Switches να ανακαλύψουν την τοπολογία του δικτύου και την ύπαρξη layer-2 loops. Ειδικότερα:

1. Εκλέγουν έναν από όλους ως Root Bridge (Root Switch). Η εκλογή γίνεται με βάση το μικρότερο **Switch ID**. Το switch ID δημιουργείται από δύο κομμάτια, την προτεραιότητα του switch (**priority**, εξ ορισμού 32.768, δηλ. 2 bytes μήκος) και την **MAC address** του switch (6 bytes μήκος).
2. Με βάση το κόστος θύρας, κάθε switch υπολογίζει το κόστος κάθε διαδρομής του προς την root switch.

3. Μετά την εκλογή του root switch, κάθε άλλος switch στο δίκτυο ορίζει μιά θύρα του ως **root port** (**RP**) για να επικοινωνεί με την root switch. Η εκλογή γίνεται με τα παρακάτω κριτήρια κατά σειρά προτεραιότητας:
    3.1. το συσσωρευμένο κόστος κάθε διαδρομής προς τον switch. Η πόρτα με το μικρότερο αθροιστικό κόστος γίνεται root port,
    3.2. σε περίπτωση ισοπαλίας εκλέγεται η θύρα που επικοινωνεί με τον γείτονα switch που έχει το μικρότερο ID,
    3.3. στη συνέχεια η θύρα με τη μικρότερη προτεραιότητα,
    3.4. και τέλος αυτή με τη μικρότερη αρίθμηση (π.χ. e0/0).
4. Τελευταίο βήμα η εκλογή για κάθε Τμήμα του δικτύου της **designated port (DP)**, μιάς θύρας σε έναν μόνο switch του τμήματος, μέσω της οποίας θα επικοινωνεί το τμήμα αυτό με τον root switch. Ο Switch λέγεται και designated switch για το συγκεκριμμένο τμήμα του δικτύου. Για κάθε τμήμα δικτύου (segment) η εκλογή γίνεται με την παρακάτω, κατά σειρά προτεραιότητας, διαδικασία:
    4.1. Ο switch (port) με το μικρότερο αθροιστικό κόστος,
    4.2. Αν υπάρχει ισοπαλία στα κόστη ανάμεσα σε διαφορετικούς switches επιλέγεται το μικρότερο switch ID,
    4.3. Αν έχουμε ίδια κόστη στον ίδιο switch (συνδέεται με δύο συνδέσεις στο τμήμα του LAN), επιλέγεται η θύρα με τη μικρότερη προτεραιότητα.
    4.4. Τέλος, επιλέγεται η θύρα με τη μικρότερη αρίθμηση.



Εικόνα 11.5 – Ένα δίκτυο με πλεονασμούς συνδέσεων

Θα δούμε ένα απλό παράδειγμα για να κατανοήσουμε την όλη διαδικασία. Στην εικόνα 11.5 βλέπουμε την τοπολογία ενός δικτύου LAN, με τέσσερεις switches. Κάτω από το όνομα καθενός υπάρχει η MAC address του, ενώ πάνω σε κάθε τμήμα (segment) του δικτύου βλέπουμε το σχετικό κόστος (πιν. 11.3). Οι switches, μέσα από την αποστολή μηνυμάτων BPDUs προχωράνε στην εκτέλεση του αλγορίθμου STP.

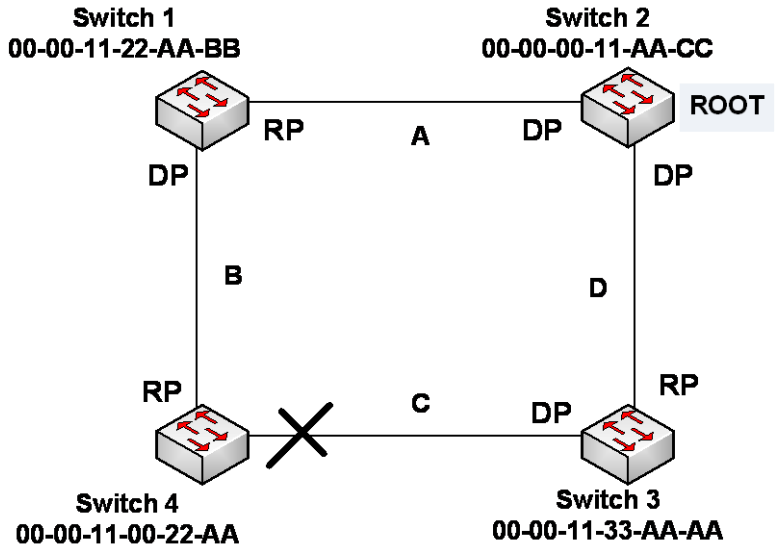
1. **Εκλογή root switch**. Υποθέτουμε ότι η προτεραιότητα κάθε switch είναι η εξ ορισμού (32768), επομένως root switch θα εκλεγεί ο switch2 που έχει τη μικρότερη MAC address.
2. **Εκλογές root port**.
    - Ο switch1 έχει δύο διαδρομές προς τον root switch, μέσω της θύρας p1 με κόστος 19 και μέσω της θύρας p2 με κόστος 19+100+19=138. Η θύρα p1 γίνεται RP για τον switch1.

- Ο switch4 έχει δύο διαδρομές προς τον root switch, μέσω της p1 με κόστος 100+19=119 και μέσω της p2 με κόστος 19+19=38. Η θύρα p2 γίνεται RP για τον switch3.
- Ο switch3 επικοινωνεί με τον root switch μέσω της θύρας p1 με κόστος 19 και μέσω της p2 με κόστος 19+19+100=138. Η θύρα p1 γίνεται RP για τον switch4.

3. **Εκλογές designated port**.
   - Στο τμήμα A συνδέονται 2 switches, οι switch1 και switch2. Ο switch2 είναι ο root switch, επομένως έχει απόσταση 0 από τον root switch (τον εαυτό του), ενώ ο switch1 απέχει 19. Η θύρα p2 του switch2 γίνεται DP για το τμήμα A.
   - Όμοια, η θύρα p1 του switch2 γίνεται DP για το τμήμα D.
   - Στο τμήμα B ο switch1 απέχει 19 και ο switch4 119 από τον root switch. Η θύρα p2 του switch1 γίνεται DP για το τμήμα B.
   - Στο τμήμα C τέλος, συνδέονται οι switch4 με απόσταση 38 και και ο switch3 με απόσταση 19. Η θύρα p2 του switch3 γίνεται DP.

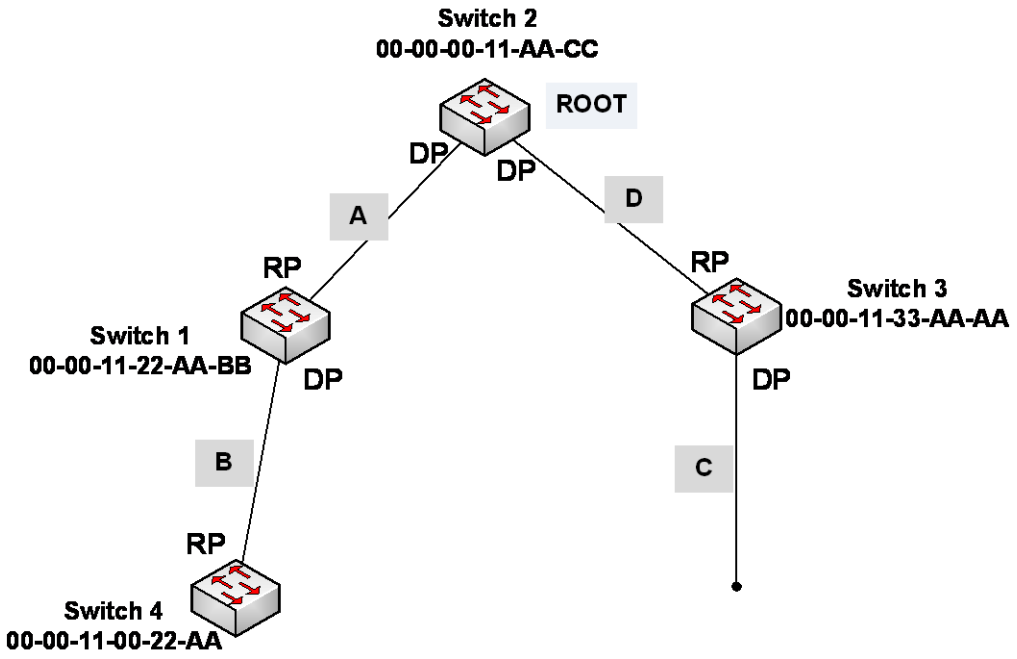
Μετά την επιτυχή εκτέλεση του STP, το δίκτυο πλέον έχει **συγκλίνει** (converged topology), όπως φαίνεται στην εικόνα 11.6. Παρατηρούμε ότι:

- όλες οι ενεργές θύρες στον root switch είναι DP,
- ο root switch δεν έχει RP,
- κάθε switch έχει **μία θύρα** με την οποία επικοινωνεί με τον root switch και κάθε τμήμα έχει **μία θύρα** σε **έναν συνδεδεμένο switch** μέσω της οποίας επικοινωνεί με τον root switch.



Εικόνα 11.6 – Η τοπολογία STP μετά τη σύγκλιση

Η θύρα p1 του switch4 θα περάσει σε κατάσταση blocked, κόβοντας έτσι τα layer-2 loops. Το πρωτόκολλο λέγεται spanning tree διότι δημιουργεί ένα (ανεστραμμένο) δέντρο με κορυφή τον root, σε τρόπο ώστε για κάθε switch να υπάρχει μόνο ένας δρόμος (εικόνα 11.7).



Εικόνα 11.7 – Το Spanning Tree

Πως όμως αποφασίζεται ποιά θύρα θα τεθεί σε κατάσταση blocked; Το θέμα θα ξεκαθαρίσει μόλις δούμε τις καταστάσεις όπου μπορεί να βρίσκεται μιά θύρα. Κάθε θύρα μπορεί να βρίσκεται σε μία από πέντε διαφορετικές καταστάσεις:

Blocking. Μιά θύρα θα μπει σε blocking state:

- Κατά τη διάρκεια εκλογής root switch,
- Όταν ένας switch λάβει BPDU που αναφέρει ότι υπάρχει καλύτερη RP από αυτήν που χρησιμοποιεί,
- Όταν δεν είναι RP ή DP.

Είναι η τρίτη περίπτωση που στο παράδειγμά μας (εικ. 11.6 & 11.7) θα κρατήσει την θύρα του switch4 σε blocking state.

Η θύρα που μπαίνει σε blocking state παραμένει για 20 sec (maximum age timer), δέχεται και επεξεργάζεται BPDUs ενώ απορρίπτει τα δεδομένα χρήστη. Σε αυτή τη φάση ο switch κάνει όποιους υπολογισμούς χρειάζεται για να αποφασίσει την ανάθεση ρόλων τους θύρες του (RP,DP, blocked).

Listening. Μόλις περάσουν τα 20 sec, όσες θύρες έχουν εκλεγεί RP και DP περνάνε στη φάση Listening, ενώ οι τους παραμένουν blocked. Στη φάση Listening οι θύρες εξακολουθούν μόνο να δέχονται BPDUs και να απορρίπτουν την άλλη κίνηση. Η φάση διαρκεί 15 sec (forward delay timer).

Learning. Στη φάση αυτή, οι θύρες δέχονται BPDUs αλλά πλέον επεξεργάζονται και τα frames με κανονικά δεδομένα, σχηματίζοντας τον πίνακα CAM. Η διάρκεια τους φάσης τους είναι 15 sec (forward delay timer).

Forwarding. Στη φάση αυτή περνάνε οι θύρες από την φάση learning. Τώρα, δέχονται BPDUs, ενημερώνουν τον CAM table αλλά πλέον προωθούν τα δεδομένα των χρηστών.

Disabled. Ευρισκόμενη στην κατάσταση αυτή, η θύρα δεν συμμετέχει στην διαδικασία STP. Στη φάση αυτή μπαίνει π.χ. με ενέργεια του διαχειριστή, επειδή αποσυνδέθηκε το καλώδιο κλπ.

Παρατηρούμε ότι με βάση τους εξ ορισμού τιμές των χρονομετρητών για να συγκλίνει μια STP τοπολογία χρειάζεται 20+15+15 = 50 sec, χρόνος καθόλου αμελητέος. Υπάρχουν διάφορες

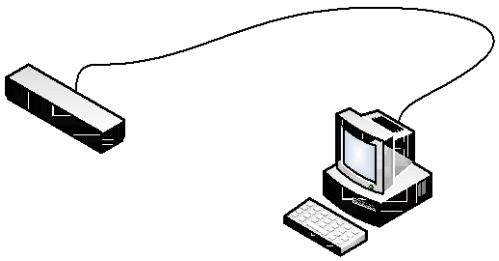
δυνατότητες για να ελαττώσει κανείς αυτό το χρόνο, βελτιώνοντας έτσι την όλη απόδοση του δικτύου, χρειάζεται τους ιδιαίτερη προσοχή διότι υπάρχει περίπτωση να φέρουν τα αντίθετα αποτελέσματα. Για παράδειγμα, μπορεί κάποιος να μειώσει τους χρονομετρητές (max age, fwd delay). Ακόμα, μπορεί να χρησιμοποιήσει την δυνατότητα *PortFast* για τους θύρες, που πολλοί switches διαθέτουν, με βάση την οποία η θύρα θα βρίσκεται πάντα σε κατάσταση forwarding. Η ιδιότητα αυτή ταιριάζει ειδικά για τους θύρες που έχουν επάνω τους συνδεδεμένους χρήστες, PCs, Servers, Routers κλπ, οπότε δεν υπάρχει περίπτωση να δημιουργήσουν layer-2 loops. Τέλος αναφέρουμε το Rapid Spanning Tree Protocol (RSTP) από την IEEE (στάνταρντ 802.1w) με πολλούς νεωτερισμούς και χαρακτηριστικά που στοχεύουν, μεταξύ άλλων, να μειώσουν το χρόνο σύγκλισης.

11. 4 Βασική ρύθμιση μεταγωγέα

Υπάρχουν πολλοί, προφανείς λόγοι για τους οποίους θέλουμε να ρυθμίζουμε τις παραμέτρους ενός switch. Ανάμεσά τους η ασφάλεια (κωδικοί πρόσβασης κλπ), η προσαρμογή στο περιβάλλον και διαχείριση (IP address κλπ) και η βελτίωση της απόδοσής του (ταχύτερη σύγκλιση του STP, λιγότερα λάθη κλπ).

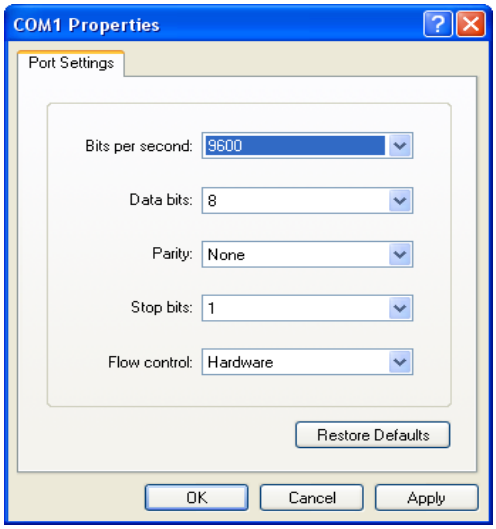
Ένας switch μπορεί να ρυθμιστεί με διάφορους τρόπους: Κονσόλα (console), Telnet (VTY), SNMP, TFTP, HTTP.

Η κονσόλα είναι ο μόνος τρόπος με τον οποίο μπορούμε να συνδεθούμε και να ρυθμίσουμε τον switch στην πρώτη του εκκίνηση. Η σύνδεση γίνεται με ειδικό καλώδιο (rollover) ανάμεσα σε ειδική θύρα (console port) του switch (εικ. 11.8) και σε σειριακή θύρα υπολογιστή.



Εικόνα 11.8 – Σύνδεση στην console port

Η επικοινωνία με τον switch, συνήθως γίνεται μέσω του hyperterminal, εφόσον βρισκόμαστε σε περιβάλλον windows. Στην εικόνα 11.9 βλέπουμε ένα σετ τυπικών ρυθμίσεων για την περίπτωση μας.



Εικόνα 11.9 – Τυπικές ρυθμίσεις Hyperterminal

Σημειώνεται ότι console port δεν έχουν όλοι οι switches. Όταν ο switch αποκτήσει IP διεύθυνση (ή αν έχει κάποια από κατασκευής), τότε μπορούμε να χρησιμοποιήσουμε τους υπόλοιπους τρόπους. Η σύνδεση σε αυτές τις περιπτώσεις γίνεται μέσω δικτύου.
Telnet: η διάδραση με τον switch μέσω γραμμής εντολών όπως και στην κονσόλα.
SNMP: ρύθμιση μέσα από ειδικό λογισμικό διαχείρισης δικτυακών συσκευών.
TFTP: κατέβασμα των ρυθμίσεων στον switch από file server.
HTTP: μέσα από περιηγητή ιστοσελίδων (π.χ. Internet Explorer), όπου ο switch παίζει το ρόλο Web Server.

Στην παράγραφο αυτή θα δούμε τις εντολές ρύθμισης ενός cisco switch, που σε πολλά σημεία μοιάζουν με αυτές ενός router. Στόχος μας ωστόσο δεν είναι να μάθουμε τη λειτουργία των προϊόντων της συγκεκριμένης εταιρείας. Άλλωστε υπάρχουν αρκετές διαφορές ανάμεσα στις ρυθμίσεις των διαφόρων μοντέλων της cisco. Καλό είναι επομένως να επικεντρωθεί κάποιος στις έννοιες και γενικές μεθοδολογίες παρά στην αυστηρή μορφή και σύνταξη των εντολών, προκειμένου να σχηματίσει σφαιρική άποψη.

Όπως ήδη γνωρίζουμε όλες οι συσκευές cisco, άρα και ένας cisco switch, τρέχουν το δικό τους λειτουργικό σύστημα, που είναι γνωστό με το όνομα IOS (Internetwork Operating System). Μετά την εκκίνηση και το φόρτωμα του λειτουργικού, ο χρήστης έρχεται σε επαφή με το περιβάλον γραμμής εντολών. Όμοια με τους routers, υπάρχουν τρείς καταστάσεις της γραμμής εντολών User EXEC mode, Privilege EXEC mode και (Global) Configuration mode (απ' όπου περνάμε σε subconfiguration mode).

Αλλαγή ονόματος. Γίνεται σε κατάσταση configuration με την εντολή *hostname*.

```
Switch>
Switch>enable
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname EKDDA

EKDDA(config)#
```

Καθορισμός κωδικού για είσοδο σε Privilege EXEC. Γίνεται σε configuration mode με την εντολή

- *enable password <κωδικός>* που κρατά τον κωδικό σε μορφή κειμένου. Για να τον

κρυπτογραφήσουμε χρησιμοποιούμε στη ίδια κατάσταση την εντολή *service password-encryption* . Πολύ καλύτερη είναι η εντολή

- *enable secret <κωδικός>* που κρυπτογραφεί πολύ ισχυρότερα τον κωδικό απ' ότι στην προηγούμενη περίπτωση.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable secret mysecret

Switch(config)#
```

Καθορισμός κωδικού για είσοδο σε user EXEC <u>από κονσόλα</u>. Μπαίνουμε σε line subconfiguration mode και δίνουμε τις εντολές *password <κωδικός>* και *login*.

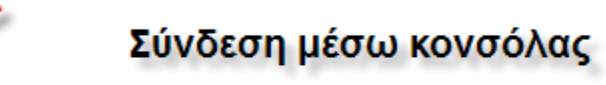
```
Switch>enable
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line console 0
Switch(config-line)#password mystiko
Switch(config-line)#login

Switch(config-line)#
```

Καθορισμός κωδικού για είσοδο σε user EXEC <u>από telnet</u>. Μπαίνουμε στο αντίστοιχο line subconfiguration mode και δίνουμε τις εντολές password <κωδικός> και login.

```
Switch(config)#line vty 0 15
Switch(config-line)#password kodikos
Switch(config-line)#login

Switch(config-line)#
```

Η τελευταία εντολή ρυθμίζει το ίδιο κωδικό σε όλες τις telnet συνδέσεις που υποστηρίζει ο switch (συνολικά 16). Όταν επιχειρήσουμε telnet στον switch (αφού αποκτήσει IP), θα μας ζητηθεί αυτός ο κωδικός για να εισέλθουμε σε user EXEC mode. Στην περίπτωση σύνδεσης μέσω κονσόλας, θα μας ζητηθεί ο αντίστοιχος κωδικός αρχικά με την σύνδεση για να μπούμε σε user EXEC. Και στις δύο περιπτώσεις θα πρέπει να δώσουμε τον κωδικό enable για να περάσουμε σε privilege EXEC. Παρακάτω βλέπουμε την είσοδο μέσω κονσόλας. Με βέλη τα σημεία όπου ζητούνται τα σχετικά κωδικά.

```
Press RETURN to get started.


Password:
Enter password:
Switch>en
Enter password:
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#
```



Ανάθεση IP διεύθυνσης. Ένας switch μπορεί να δημιουργήσει πολλαπλά Virtual LANs (VLANs). Σε κάθε ένα από αυτά μπορεί να έχει διαφορετικό IP address. Θα δούμε τα VLANs στην επόμενη παράγραφο. Το VLAN διαχείρισης (management VLAN) είναι, συνήθως, το VLAN1. Ακολουθούν οι εντολές ανάθεσης μιάς IP στο management VLAN.

```
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan1
Switch(config-if)#ip address 192.168.0.20 255.255.255.0
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.0.1

Switch(config)#
```

Η εντολή *ip default-gateway <router address>* χρησιμεύει όταν θέλουμε να έχουμε πρόσβαση στον switch από άλλα δίκτυα. Η διεύθυνση router address είναι ο router που εξυπηρετεί το δίκτυο του switch.

Πρόσβαση σε interface. Γίνεται με τρόπο παρόμοιο με την πρόσβαση σε VLAN. Η πρόσβαση στο subconfiguration ενός interface γίνεται με την εντολή *interface <τύπος> <θέση>/<πόρτα>*, π.χ. *interface fastethernet 0/1* ή *int fa 0/1*.

Στους switches οι θύρες είναι εξ ορισμού ενεργές. Για να απενεργοποιήσουμε μία θύρα η εντολή είναι *no shutdown*. Για να την επαναενεργοποιήσουμε η εντολή γίνεται *shutdown*.

```
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fastethernet0/1
Switch(config-if)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

Switch(config-if)#
```

Αποθήκευση ρυθμίσεων. Και εδώ τα πράγματα είναι παρόμοια με τους routers. Οι ρυθμίσεις που κάνουμε βρίσκονται στη RAM και αναγνωρίζονται με το όνομα running-config. Για να αποθηκεύσουμε τις ρυθμίσεις ώστε να ισχύσουν σε επόμενη επανεκκίνηση του switch πρέπει να τις γράψουμε στην NVRAM με την εντολή *copy running-config startup-config* (ή *copy run start*) του privilege EXEC mode.

```
EKDDA#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]


EKDDA#
```

Εμφάνιση πληροφοριών.

α) Η εντολή *show interfaces* εμφανίζει πληροφορίες για όλες τις διασυνδέσεις (interfaces) του switch. Η εντολή μπορεί να αναφέρεται και σε ένα μόνο interface, π.χ. *show interface fa0/1*. Στην επόμενη σελίδα βλέπουμε την έξοδο της εντολής για ένα μόνο interface.

```
EKDDA#show interface fa0/1
FastEthernet0/1 is administratively down, line protocol is down
  Hardware is Fast Ethernet, address is 000C.2187.9744 (bia 000C.2187.9744)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Auto-duplex, Auto-speed
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 02:29:44, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); 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
     269 packets input, 71059 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     7290 packets output, 429075 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Η πρώτη γραμμή της εξόδου

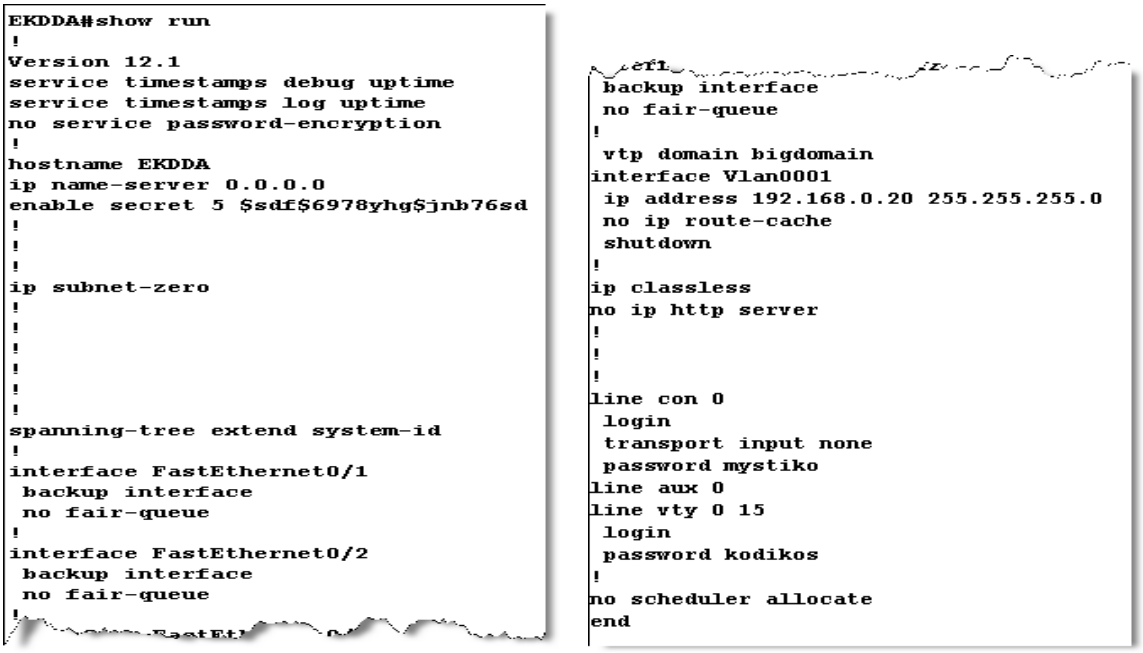
FastEthernet0/1 is administratively down, line protocol is down

αναφέρεται στην κατάσταση που βρίσκεται η συγκεκριμένη θύρα. Το πρώτο μέρος αναφέρεται στο επίπεδο 1 του OSI (physical), ενώ το δεύτερο στο επίπεδο data link. Στον πίνακα 11.4 βλέπουμε τις διαφορετικές περιπτώσεις για την κατάσταση τις θύρας στα δύο αυτά επίπεδα του OSI.

Status	Physical Layer	Data Link Layer
Up	Υπάρχει ηλεκτρικό σήμα στη θύρα	Το layer 2 λειτουργεί κανονικά.
Down	Δεν υπάρχει ηλεκτρικό σήμα στη θύρα. Πιθανά η συσκευή στην άλλη πλευρά να είναι κλειστή ή να χρησιμοποιούμε λάθος καλώδιο.	Πιθανόν δεν δουλεύουν σωστά τα keepalives, πρόβλημα χρονισμού κλπ.
Administratively down	Έχει γίνει χρήση τις εντολής shutdown	

```
EKDDA#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
EKDDA(config)#int fa0/1
EKDDA(config-if)#no shut
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
EKDDA(config-if)#exit
EKDDA(config)#exit
EKDDA#show interface fa0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 000C.2187.9744 (bia 000C.2187.9744)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Au[illegible]plex, Auto-speed
```

β) *show running-config* (ή *show run*). Μπορούμε να δούμε τις τρέχουσες ρυθμίσεις (βρίσκονται στη RAM). Μέρος τις εξόδου τις εντολής βλέπουμε παρακάτω.



```
EKDDA#show run
!
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname EKDDA
ip name-server 0.0.0.0
enable secret 5 $sdf$6978yhg$jnb76sd
!
!
!
ip subnet-zero
!
!
!
!
!
!
spanning-tree extend system-id
!
interface FastEthernet0/1
 backup interface
 no fair-queue
!
interface FastEthernet0/2
 backup interface
 no fair-queue
!
 backup interface
 no fair-queue
!
 vtp domain bigdomain
interface Vlan0001
 ip address 192.168.0.20 255.255.255.0
 no ip route-cache
 shutdown
!
ip classless
no ip http server
!
!
!
line con 0
 login
 transport input none
 password mystiko
line aux 0
line vty 0 15
 login
 password kodikos
!
no scheduler allocate
end
```

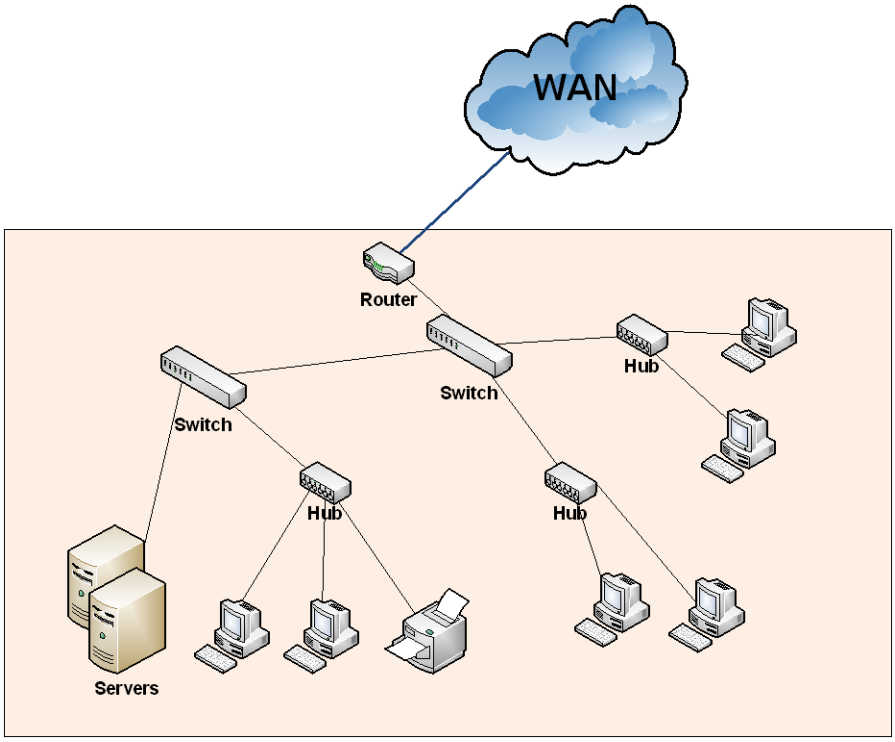
γ) Η εντολή *show startup-config* (ή *show start*) δείχνει τις αποθηκευμένες στην NVRAM ρυθμίσεις.
Δ) Η εντολή *show version* εμφανίζει πληροφορίες για το υλικό του switch και το λειτουργικό του σύστημα IOS.

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE
SOFTWARE(fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
Image text-base: 0x80010000, data-base: 0x80562000

ROM: Bootstrap program is is C2950 boot loader

Switch uptime is 24 seconds
System returned to ROM by power-on
System image file is "flash:/c2950-i6q4l2-mz.121-22.EA4.bin"

Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of memory.
Processor board ID FHK0610Z0WC
Last reset from system-reset
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 0003.E423.776B
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: FOC061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950-24
System serial number: FHK0610Z0WC
Configuration register is 0xF
```

11.5 VLANs και ρύθμιση τους σε μεταγωγείς

Η προσθήκη ενός switch κατακερματίζει το LAN δημιουργώντας περισσότερα collision domains και επομένως λιγότερες συγκρούσεις. Ο switch όμως δεν κόβει τα broadcasts όπως ένας router.

Στην κλασσική του μορφή ένα εταιρικό (τοπικό) δίκτυο έχει τη μορφή που βλέπουμε στην εικόνα 11.10. Ο σχεδιασμός αυτός, παρόλα τα πλεονεκτήματα, έχει το πρόβλημα όλη η επικράτεια του LAN, πίσω από τον router, να αποτελεί ένα broadcast domain.



Εικόνα 11.10 – Ολοκληρο το LAN, ένα broadcast domain

Τα broadcasts (και τα multicasts) είναι μιά φυσιολογική λειτουργία ενός LAN. Μερικά routing πρωτόκολλα όπως τα RIP, OSPF τα χρησιμοποιούν για να διαφημίζουν οι routers τις υπηρεσίες τους. Το πρωτόκολλο ARP (Address Resolution Protocol) χρησιμοποιείται από τους hosts για να εντοπίσουν IP διευθύνσεις στο δίκτυο. Για το σκοπό αυτό στέλνουν ειδικά ερωτήματα σε μορφή broadcast.

Τα σημερινά LANs γίνονται όλο και μεγαλύτερα, αυξάνοντας και το πλήθος των broadcasts. Υπάρχουν περιπτώσεις όπου ένα broadcast μήνυμα κινούμενο κατά μήκος ενός δικτύου προκαλεί περισσότερες αποκρίσεις από τις συσκευές του δικτύου, που και αυτές με τη σειρά τους ακόμα περισσότερες, κάτι σαν το φαινόμενο ντόμινο. Αυτή η κατάσταση ονομάζεται **Broadcast Storm** και μπορεί να διαλύσει πλήρως ένα δίκτυο, μη επιτρέποντας την κίνηση των κανονικών δεδομένων.

Αιτίες για broadcast storm μπορεί να είναι οι πλεονάζουσες τοπολογίες των switches (π.χ. ένας τεχνικός συνδέει με δεύτερη θύρα δύο switches), κάποια προβληματική συσκευή στο LAN, ακόμα και κακόβουλη επίθεση από εξωτερικούς παράγοντες (π.χ. κάποιος στέλνει διαρκώς broadcast σε ένα δίκτυο υποχρεώνοντας τις συσκευές να απαντήσουν), κλπ.

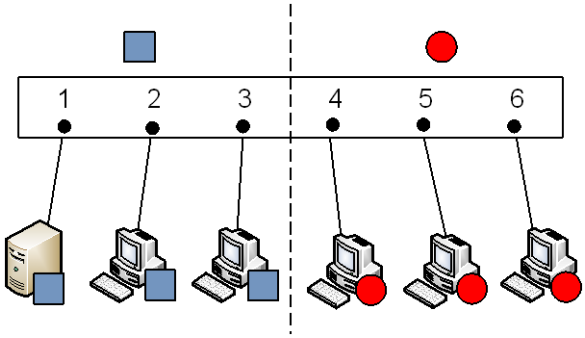
Η χρήση router λύνει το πρόβλημα αυτό, ωστόσο ένας router είναι περισσότερο αργός από ένα switch, ενώ είναι και ακριβότερος και έχει λιγότερες θύρες. Επιπλέον, υπάρχουν περιπτώσεις που ο router δεν κόβει κάποια broadcasts.

Μιά αποτελεσματική λύση στο πρόβλημα των broadcast storms, στηριγμένη σε switches, είναι τα **VLANs.**

VLAN είναι ένα λογικό σύνολο από δικτυακές συσκευές που βρίσκονται μέσα στο ίδιο broadcast domain.

Διακρίνουμε δύο κατηγορίες VLANs:

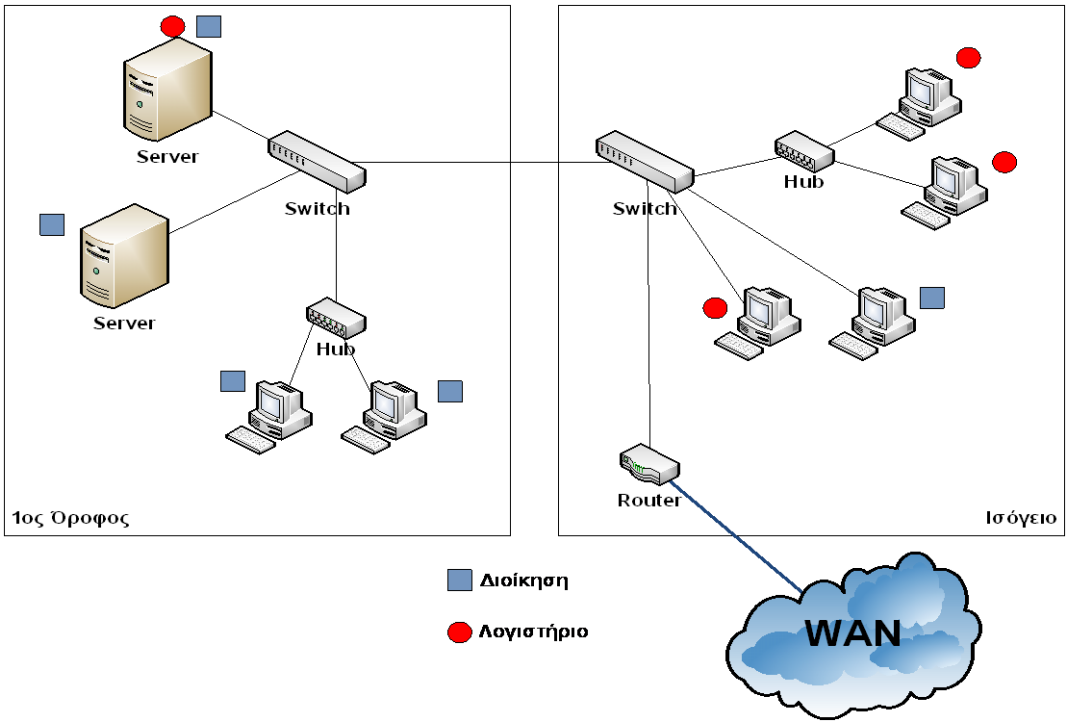
- **Στατικά (Static ή και port-based) VLANs.** Ο διαχειριστής μέσα από το περιβάλλον διαχείρισης του switch αντιστοιχίζει θύρα σε VLAN (εικ. 11.11).
- **Δυναμικά (Dynamic) VLANs.** Η αντιστοίχιση γίνεται με από επικοινωνία με έναν από τους switches που παίζει το ρόλο του VLAN membership policy server (VMPS), και ο οποίος έχει πίνακες αντιστοίχισης, π.χ. MAC address με VLAN, ή IP address με VLAN.



Εικόνα 9.11 – Στατικό VLAN

Στα πλεονεκτήματα των VLANs περιλαμβάνονται (εικ. 11.12):

- η αυξημένη δυνατότητα ευέλικτου κατακερματισμού του δικτύου και λογικής ομαδοποίησης των συσκευών άσχετα από περιορισμούς χώρου (όροφος, δωμάτιο κλπ),
- ευκολότερη διαχείριση (προσθαφαίρεση συσκευών κλπ),
- μείωση της κυκλοφορίας στο δίκτυο (broadcast storms κλπ),
- αυξημένη ασφάλεια και οικονομία σε πόρους.

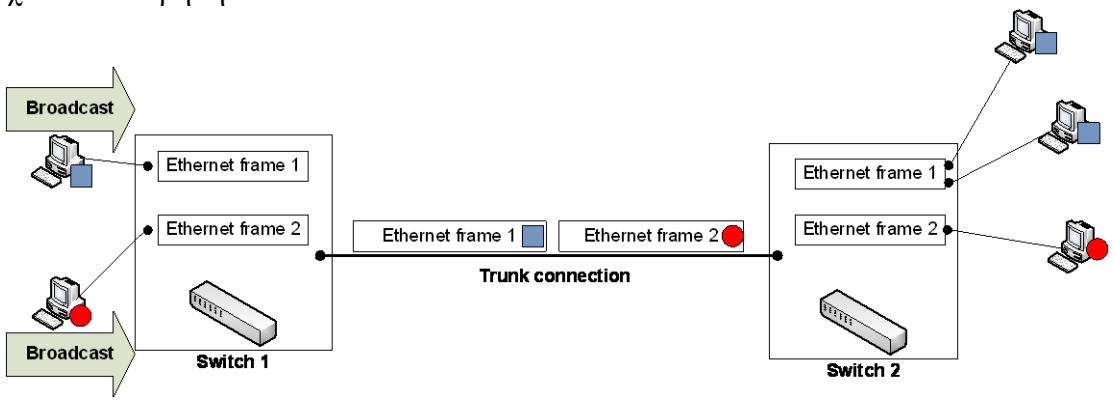


Εικόνα 11.12 – Δύο VLANs

Τα VLANs είναι υποδίκτυα και επομένως για να μεταφέρουμε δεδομένα από το ένα στο άλλο χρειάζεται η μεσολάβηση router. Οι switches μπορούν να υποστηρίζουν πολλαπλά VLANs μέσα από την ίδια θύρα. Για το σκοπό αυτό υποστηρίζουν δύο κατηγορίες συνδέσεων, τις **access links** και τα **trunks**.

Access Link: η σύνδεση μεταξύ του switch και μιάς συσκευής που διαθέτει κλασσικού τύπου NIC, για παράδειγμα η σύνδεση μεταξύ switch και host, switch και hub κλπ. Στην περίπτωση του hub, όσες συσκευές είναι συνδεδεμένες επάνω του θα ανήκουν στο ίδιο VLAN και επομένως στο ίδιο broadcast domain.

Trunk connection: επιτρέπει σε δεδομένα που προορίζονται για διαφορετικά VLANs να περνάνε από το ίδιο φυσικό μέσον (σύνδεση). Για να γίνει το trunking δυνατό, αλλάζει δομή του κλασικού ethernet frame πριν αυτό περάσει στο trunk, το αλλαγμένο (άρα μη έγκυρο) frame περνά την σύνδεση trunk και μετατρέπεται σε κανονικό frame στο τέλος του trunk, όπου παραδίδεται στο σωστό VLAN (εικ. 11.13). Η μετατροπή γίνεται με ειδικά hardware κυκλώματα-επεξεργαστές και επομένως δεν υπάρχει καθυστέρηση.



Εικόνα 11.13 –Σύνδεση trunk

Παραδείγματα εφαρμογής trunk connection μπορεί να είναι στη σύνδεση μεταξύ δύο switches, router με switch, switch με server. Επειδή γίνεται όλη η διαδικασία μετατροπής του frame που περιγράψαμε, πρέπει η συσκευές που συνδέονται στα άκρα του trunk connection να υποστηρίζουν τα κατάλληλα πρωτόκολλα. Ειδικά στην περίπτωση του server πρέπει αυτός να είναι εφοδιασμένος με ειδική κάρτα NIC διότι η κλασικές κάρτες δεν θα αναγνωρίσουν τα frames και θα τα απορρίψουν.

Τα κύρια πρωτόκολα trunking για το Ethernet είναι το ISL που είναι ιδιοκτησία της Cisco και το 802.1Q από την IEEE. Το τελευταίο είναι και το επικρατέστερο διότι επιτρέπει trunk συνδέσεις ανάμεσα σε συσκευές διαφορετικών κατασκευαστών, δεδομένου ότι το υποστηρίζουν και οι συσκευές της Cisco.

Το πρωτόκολλο ISL (InterSwitch Link) ενθυλακώνει (encapsulation) το τυπικό Ethernet frame ανάμεσα σε ένα header των 26 bytes και ενός trailer μήκους 4 bytes.

Το πρωτόκολλο 802.1Q εισάγει 4 bytes μέσα στο αρχικό frame και επαναυπολογίζει το checksum, αντικαθιστώντας το αρχικό.

Στα επόμενα θα δούμε τα βασικά βήματα δημιουργίας, ρύθμισης και ελέγχου VLANs.

Δημιουργία VLANs. Από Privilege EXEC περνάμε στη βάση δεδομένων των vlan με την εντολή *vlan database* (*****). Η δημιουργία ενός VLAN γίνεται με την εντολή *vlan <αριθμός vlan> name <όνομα vlan>*. Ολοκληρώνουμε με *exit*.

```
Switch>en
Switch#vlan database
Switch(vlan)#vlan 10 name Dioikisi
VLAN 10 added:
    Name:Dioikisi
Switch(vlan)#vlan 20 name Logistirio
VLAN 20 added:
    Name:Logistirio
Switch(vlan)#exit
APPLY completed.
Exiting....

Switch#
```

(*) Στις νεότερες εκδόσεις της cisco η δημιουργία γίνεται περνώντας μέσα από το configuration mode σε subconfiguration.

```
Switch>en
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name kitsos
Switch(config-vlan)#exit
Switch(config)#
```

Εμφάνιση περιεχομένων της βάσης δεδομένων vlan. Με την εντολή *show vlan*.

```
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
10   Dioikisi                          active

20   Logistirio                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

Όπως βλέπουμε, το VLAN1 είναι το εξ ορισμού, στο οποίο ανήκουν αρχικά όλες οι θύρες.

Ανάθεση θυρών σε VLANs. Από global configuration mode περνάμε σε subconfiguration για κάθε θύρα. Η εντολή *switchport mode access* καθορίζει το είδος σύνδεσης για το συγκεκριμμένο interface σε access. Η εντολή *switchport access vlan <αριθμός vlan>* αντιστοιχεί το συγκεκριμμένο interface στο vlan με τον αριθμό που δηλώνουμε. Ολοκληρώνουμε με *end*.

```
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#end
Switch#
```

Η ίδια εργασία γίνεται διαδοχικά για όλες τις θύρες που θέλουμε να τις αναθέσουμε σε VLAN.
Καθορισμός της σύνδεσης trunk. Περνάμε στο subconfiguration mode της θύρας που επιθυμούμε και με την εντολή *switchport mode trunk* την ορίζουμε ως trunk connection. Για να επιλέξουμε πρωτόκολλο, χρησιμοποιούμε την εντολή *switchport trunk encapsulation <dot1q ή isl>*.

```
Switch(config)#int fa0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#end
```

Οι trunk συνδέσεις πρέπει να είναι ίδιου τύπου και από τις δύο πλευρές τους.
Συνοπτικές πληροφορίες των VLANs. Τις βλέπουμε με την εντολή
show vlan brief.

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12
10   Dioikisi                         active    Fa0/1

20   Logistirio                       active    Fa0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Πληροφορίες για θύρα σε σχέση με VLAN. Τις βλέπουμε με την εντολή
show interface <είδος, αριθμός> switchport.

```
Switch#show int fa0/3 switchport
Name: Fa0/3
Switchport:     Enabled
Administrative mode: trunk
Operational mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false

Voice vlan: none (Inactive)
Appliance trust: none
```

Όπως έχουμε πει, κάθε VLAN είναι και ένα διαφορετικό υποδίκτυο. Η πρακτική είναι να υπάρχει σχέση 1-1 μεταξύ των VLANs και των IPs. Έτσι, κάθε VLAN έχει ένα αντίστοιχο Layer 3 υποδίκτυο, πράγμα που επιτρέπει στους router να κινούν δεδομένα ανάμεσα στα VLAN.

Το εξ ορισμού Management VLAN είναι το VLAN 1 που δεν μπορεί να διαγραφεί. Αρχικά όλες οι ethernet θύρες ανήκουν στο VLAN1. Μπορούμε να τις αναθέσουμε σε άλλα, όμως πρέπει να υπάρχει τουλάχιστον μία θύρα στο VLAN1, προκειμένου να μπορούμε να διαχειριστούμε τον switch.

Όταν διαγράφουμε ένα VLAN οι θύρες του γίνονται ανενεργές, παραμένουν όμως συσχετισμένες με το VLAN, μέχρι να τις αναθέσουμε σε άλλο.

11.6 Το πρωτόκολλο VTP

Όπως είδαμε στην προηγούμενη παράγραφο, για να προσθέσουμε και ρυθμίσουμε ένα VLAN πρέπει να το κάνουμε «χειρωνακτικά» μέσα από σύνδεση με κάθε switch που θα μετέχει σ' αυτό. Τι γίνεται όμως αν έχουμε π.χ. 10 ή 20 switches;

Το **VLAN Trunk Protocol** (**VTP**) δημιουργήθηκε από την Cisco για να αυτοματοποιήσει την διαδικασία. Με το πρωτόκολλο αυτό, οι ρυθμίσεις VLAN (δημιουργία, διαγραφή, μετονομασία) μπορούν να γίνονται από έναν switch και να μεταδίδονται σε όλους τους υπόλοιπους, οι οποίοι ρυθμίζονται χωρίς άλλη επέμβαση. Το VTP χρειάζεται συνδέσεις trunk για να μεταφέρει τα layer-2 μηνύματά του.

Τα μηνύματα του VTP, και επομένως η τηλε-ρύθμιση των switches γίνονται στο **domain** που ορίζουμε εμείς. Ένας switch μπορεί να ανήκει μόνο σε ένα domain. Ακόμα, ένας switch μπορεί να ανήκει σε μία από τις τρείς παρακάτω κατηγορίες, οι οποίες και ρυθμίζουν τον τρόπο που θα συμπεριφέρεται μέσα στο domain:

1. **Server.** Ο Server μπορεί να προσθέτει, αλλάζει, διαγράφει VLANs από το configuration του. Ο Server δέχεται αλλαγές και μέσω VTP μηνυμάτων. Σε κάθε περίπτωση, όταν υποστεί κάποια αλλαγή την διαφημίζει σε όλες τις (trunk) θύρες του.
2. **Client.** Ο Client δεν μπορεί να κάνει αλλαγές στη διαμόρφωσή του. Οι αλλαγές που δέχεται είναι μόνον αυτές που λαμβάνει από κάποιον Server με VTP. Όποτε λάβει κάποιο VTP μήνυμα αλλαγής, αφού την ενσωματώσει στην διαμόρφωσή του, προωθεί το μήνυμα στις άλλες trunk θύρες του.
3. **Transparent.** Ο Transparent μπορεί επίσης να προσθέτει, αλλάζει, διαγράφει VLANs από το configuration του. Οι αλλαγές όμως δεν διαφημίζονται, δεν δημιουργεί δηλαδή VTP μηνύματα. Ακόμα, αγνοεί τα VTP μηνύματα που λαμβάνει, απλά τα προωθεί σε όλες τις

θύρες χωρίς να τα λάβει υπόψιν στο σχηματισμό της διαμόρφωσής του.

Αν δεν το ορίσει ο διαχειριστής διαφορετικά, ένας switch εντάσσεται αυτόματα στην κατηγορία Server. Συνήθως, ορίζεται ένας switch ως server και οι υπόλοιποι ως client. Αυτή η διαμόρφωση είτε διατηρείται διαρκώς και ο διαχειριστής χρησιμοποιεί τον server για να ρυθμίζει όλους τους switch του domain, ή αφού γίνει η ρύθμιση, μετατρέπονται όλοι σε Transparent για να αποφεύγονται λάθη.

Υπάρχουν και περιπτώσεις, όπως στο **VTP pruning**, όπου απαιτείται όλοι οι switch να είναι server. Μία trunk σύνδεση εξ ορισμού ανήκει σε όλα τα VLANs, επομένως προωθεί όλα τα broadcasts είτε στην άλλη άκρη υπάρχει μέλος (host) του VLAN είτε όχι. Το VTP pruning είναι μία λειτουργία με την οποία αφαιρούνται (ή και προστίθενται) VLANs σε ένα trunk.

Η λειτουργία του VTP γίνεται μέσω μηνυμάτων που δημιουργούν ή/και προωθούν οι switches ανάλογα με την κατάσταση (mode) στην οποία βρίσκονται. Τα μηνύματα, μεταξύ άλλων, περιέχουν έναν αριθμό τον **configuration revision number**. Κάθε φορά που ο switch στέλνει ένα μήνυμα μεταβολής αυξάνει κατά 1 τον αριθμό αυτό. Όσο μεγαλύτερος είναι επομένως, τόσο πιό πρόσφατο είναι το configuration που περιέχει το μήνυμα. Ακολουθούν οι εντολές ρύθμισης του VTP.

Δημιουργία ή αλλαγή VTP Domain. Από Privilege EXEC περνάμε στη βάση δεδομένων των vlan με την εντολή *vlan database*. Δημιουργούμε το domain με την εντολή *vtp domain <όνομα domain>* .

```
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#vtp domain ekdda
Changing VTP domain name from NULL to ekdda
Switch(vlan)#
Switch(vlan)#vtp domain MyDomain
Changing VTP domain name from ekdda to MyDomain
```

Καθορισμός της κατάστασης (mode) ενός switch. Εξ ορισμού ένας switch μπαίνει σε server mode. Σε περίπωση που θέλουμε να το αλλάξουμε χρησιμοποιούμε την εντολή *vtp <mode>* όπου το mode μπορεί να είναι client, server ή transparent.

```
Switch(vlan)#vtp server
Setting device to VTP SERVER mode.
```

Εμφάνιση πληροφοριών για το VTP. Με την εντολή *show vtp status.*

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 64
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : MyDomain
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xD5 0xE7 0x54 0xFC 0x64 0x4A 0x09 0x2D
Configuration last modified by 0.0.0.0 at 3-1-93 00:42:30
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

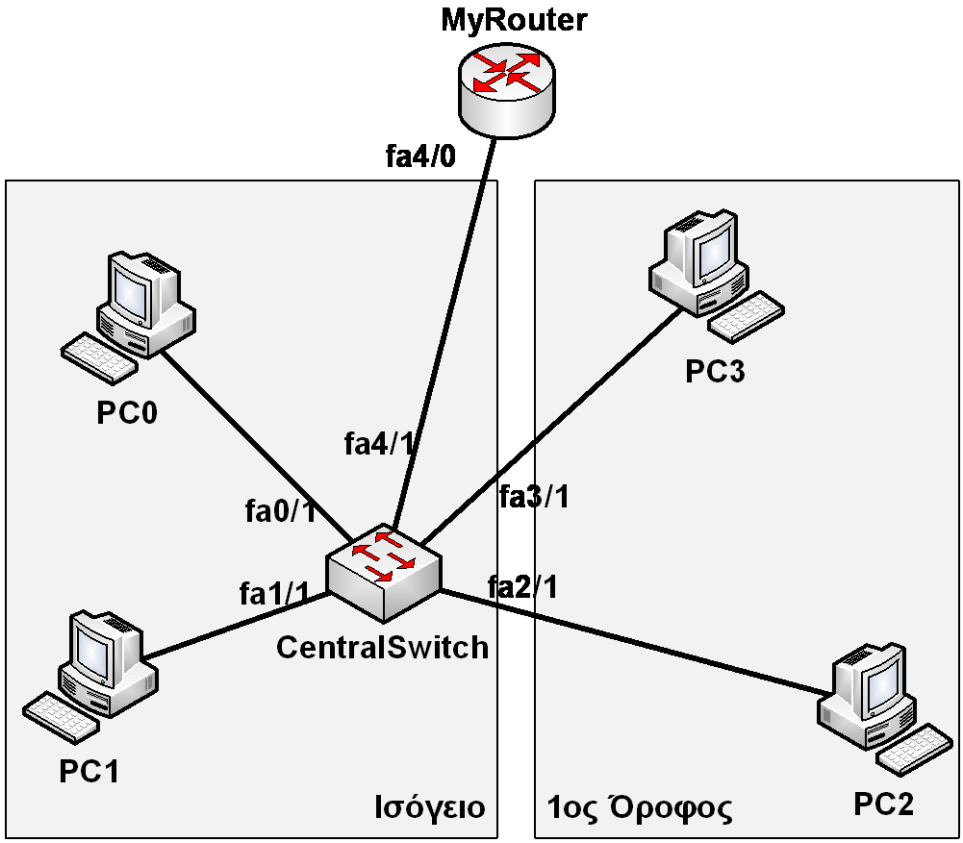
Ένταξη switch σε υπάρχον domain. Υπάρχει περίπτωση αν ο νέος switch που συνδέουμε έχει μεγαλύτερο configuration revision number να περάσει τη δική, λανθασμένη διαμόρφωση σε όλο το

δίκτυο (π.χ. από το άλλο δίκτυο που τον μεταφέραμε). Ωστόσο, ο αριθμός αυτός μηδενίζεται όταν επανεκκινήσουμε τον switch.

11.7 Παράδειγμα ρύθμισης μεταγωγέα σε δίκτυο

Στα επόμενα ακολουθεί ένα παράδειγμα ρύθμισης μικρού δικτύου (εικ. 11.14) που ανήκει σε οργανισμό με δύο τμήματα: λογιστήριο και αποθήκη. Για κάθε τμήμα θα υπάρχει ένα VLAN.

Το δίκτυο έχει έναν κεντρικό switch που θα υποστηρίζει τα VLANs και έναν router που είναι επιφορτισμένος με την επικοινωνία (σε layer 3) των VLANs. Συνολικά θα έχουμε τρία Virtual LANS.



Εικόνα 11.14 – Ρυθμίζοντας ένα απλό δίκτυο

Στο σχήμα 11.14 φαίνεται η τοπολογία του δικτύου. Προτού ξεκινήσουμε την ρύθμιση των συσκευών, σχεδιάζουμε τα βασικά χαρακτηριστικά του. Συνολικά θα έχουμε τρία VLANs. Οι ρυθμίσεις και οι παράμετροι φαίνονται στους πίνακες 11.4 έως και 11.7. Κάθε πίνακας τον ακολουθείται από τις εντολές ρύθμισης της αντίστοιχης συσκευής.

Βασική διαμόρφωση του switch

Όνομα	Enable		VTY & Console password	VLAN 1		
	Secret	Password		IP address	subnet mask	default gateway

CentralSwitch	greece	athens	europe	192.168.1.2	255.255.255.0	192.168.1.1

Πίνακας 11.4 – Switch

```
Switch>en
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CentralSwitch
CentralSwitch(config)#enable password athens
CentralSwitch(config)#enable secret greece
CentralSwitch(config)#line con 0
CentralSwitch(config-line)#password europe
CentralSwitch(config-line)#login
CentralSwitch(config-line)#line vty 0 15
CentralSwitch(config-line)#password europe
CentralSwitch(config-line)#login
CentralSwitch(config-line)#exit
CentralSwitch(config)#service password-encryption
CentralSwitch(config)#int vlan 1
CentralSwitch(config-if)#ip address 192.168.1.2 255.255.255.0
CentralSwitch(config-if)#no shut

%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
CentralSwitch(config-if)#exit
CentralSwitch(config)#ip default-gateway 192.168.1.1
CentralSwitch(config)#end
%SYS-5-CONFIG_I: Configured from console by console
CentralSwitch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
CentralSwitch#
```

Διαμόρφωση των VLANs του switch

VLAN		**Υποδίκτυο**	**Θύρες***	**Host**
3	Apothiki	192.168.3.0	fa1/1, fa3/1	PC1, PC3
2	Logistirio	192.168.2.0	fa0/1, fa2/1	PC0, PC2
1	Management	192.168.1.0	Υπόλοιπες	
* fa4/1: trunk port Θα ρυθμιστεί ως trunk port ώστε να υποστηρίζει και τα τρία VLANs				

Πίνακας 11.5 - VLANs

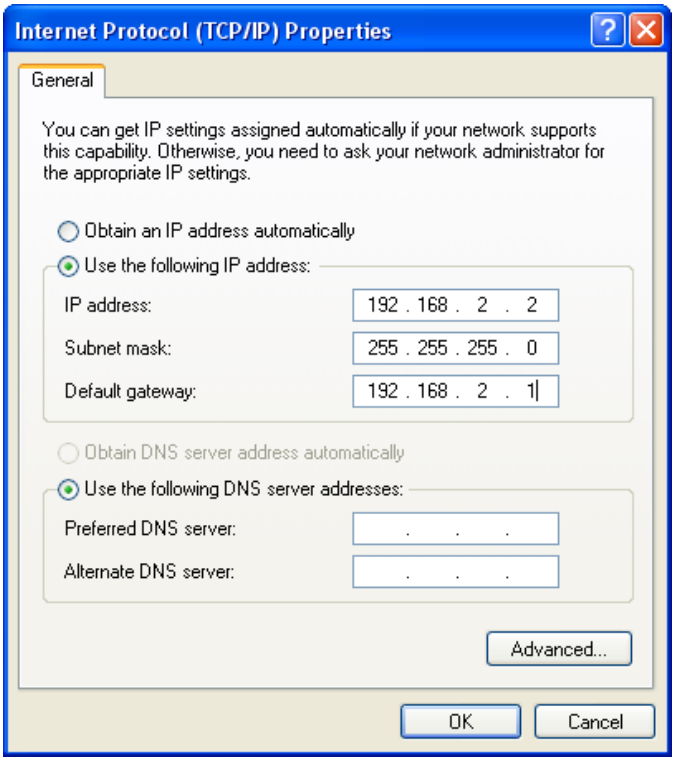
```
CentralSwitch#vlan database

CentralSwitch(vlan)#vlan 2 name Logistirio
VLAN 2 modified:
    Name: Logistirio
CentralSwitch(vlan)#vlan 3 name Apothiki
VLAN 3 modified:
    Name: Apothiki
CentralSwitch(vlan)#exit
APPLY completed.
Exiting....
CentralSwitch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
CentralSwitch(config)#int fa1/1
CentralSwitch(config-if)#switchport mode access
CentralSwitch(config-if)#switchport access vlan 3
CentralSwitch(config-if)#int fa3/1
CentralSwitch(config-if)#switchport mode access
CentralSwitch(config-if)#switchport access vlan 3
CentralSwitch(config-if)#int fa0/1
CentralSwitch(config-if)#switchport mode access
CentralSwitch(config-if)#switchport access vlan 2

CentralSwitch(config-if)#int fa2/1
CentralSwitch(config-if)#switchport mode access
CentralSwitch(config-if)#switchport access vlan 2

CentralSwitch(config-if)#int fa4/1
CentralSwitch(config-if)#switchport mode trunk
CentralSwitch(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
CentralSwitch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
CentralSwitch#
```

Ρυθμίσεις των Hosts

PC #	VLAN	port	IP address	subnet mask	gateway
0	2	fa0/1	192.168.2.2	255.255.255.0	192.168.2.1
1	3	fa1/1	192.168.3.2	255.255.255.0	192.168.3.1
2	2	fa2/1	192.168.2.3	255.255.255.0	192.168.2.1
3	3	fa3/1	192.168.3.3	255.255.255.0	192.168.3.1

Πίνακας 11.6 - Hosts

Οι hosts συνδέονται φυσικά στις αντίστοιχες θύρες. Η συμμετοχή τους στο Vlan αποφασίζεται από την θύρα που συνδέεται. Εφόσον τρέχουν Windows οι άλλες ρυθμίσεις γίνονται μέσα από τον Πίνακα Ελέγχου, όπως βλέπουμε στην εικόνα 11.15



Εικόνα 11.15 – Διευθυνσιοδότηση IP σε PC

Ρυθμίσεις του Router

Όνομα	**Enable**		**VTY & Console password**	**port fa4/0**		
				subinterfaces		
				fa4/0.1 dot1q vlan 1	**fa4/0.2** dot1q vlan 2	**fa4/0.3** dot1q vlan 3
	Secret	**Password**				
MyRouter	greece	athens	europe	**IP address** 192.168.1.1	**IP address** 192.168.2.1	**IP address** 192.168.3.1
				subnet mask 255.255.255.0		

Πίνακας 11.7 – Router

```
Router>en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa4/0
Router(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet4/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet4/0, changed state t
o up
Router(config-if)#int fa4/0.1

%LINK-5-CHANGED: Interface FastEthernet4/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet4/0.1, changed state
 to upRouter(config-subif)#
Router(config-subif)#encapsulation dotlq 1
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#int fa4/0.2

%LINK-5-CHANGED: Interface FastEthernet4/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet4/0.2, changed state
 to upRouter(config-subif)#
Router(config-subif)#encapsulation dotlq 2
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#int fa4/0.3

%LINK-5-CHANGED: Interface FastEthernet4/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet4/0.3, changed state
 to upRouter(config-subif)#
Router(config-subif)#encapsulation dotlq 3
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#end
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

Οι βασικές ρυθμίσεις του Router (όνομα, κωδικοί) παραλείπονται.

12.Μετάφραση Διεύθυνσης

12.1 Μετάφραση Διεύθυνσης Δικτύου (NAT). Γενικά.

Η μετάφραση διεύθυνσης δικτύου αναπτύχθηκε, αρχικά, για την επίλυση δύο προβλημάτων: τον χειρισμό της έλλειψης IP διευθύνσεων και την απόκρυψη της διευθυνσιοδότησης (addressing scheme). Ωστόσο, η μετάφραση διεύθυνσης δικτύου παρέχει λύσεις για ποικίλα προβλήματα και έχει πολλά πλεονεκτήματα.

Έλλειψη Κοινών IP Διευθύνσεων. Η μακροπρόθεσμη λύση σε αυτό το πρόβλημα οδήγησε στον εμπλουτισμό της στοίβας πρωτοκόλλων TCP/IP συμπεριλαμβανομένης μιας νέας διάταξης της διευθυνσιοδώτησης (IPv6). Η παρούσα διάταξη (IPv4) χρησιμοποιεί 32 bits ενώ η IPv6 χρησιμοποιεί 128 bits.

Ιδιωτικές Διευθύνσεις Δικτύου. Η βραχυπρόθεσμη λύση στην έλλειψη κοινών IP διευθύνσεων βασίζεται σε ιδιωτικές IP διευθύνσεις και την μετάφραση τους σε κοινές IP διευθύνσεις με χρήση Network Address Translation (NAT). Η παραπάνω λύση υπερτερεί της μακροπρόθεσμης ανάμεσα στις εταιρίες επικοινωνιών και τους ISP.

Το πρότυπο RFC 1918 ορίζει τις παρακάτω περιοχές ιδιωτικών IP διευθύνσεων:

Κλάση	Περιοχή Ιδιωτικών Διευθύνσεων
A	10.0.0.0-10.255.255.255
B	172.16.0.0-172.31.255.255.255
C	192.168.0.0-192.168.255.255

Πίνακας 1. RFC 1918 Ιδιωτικές IP Διευθύνσεις.

Οι διευθύνσεις του Πίνακα 1 είναι για εσωτερική χρήση και μόνο. Τα πακέτα με ιδιωτική διεύθυνση δεν θα δρομολογηθούν από τον ISP. Το γεγονός αυτό δημιουργεί ένα πρόβλημα συνδεσιμότητας των συσκευών με ιδιωτικές IP διευθύνσεις όταν αυτές θέλουν να επικοινωνήσουν με δημόσια δίκτυα όπως το Internet.

Το πρότυπο RFC 1631 καθορίζει την διεργασία γνωστή ως Network Address Translation (NAT) η οποία μας επιτρέπει την αλλαγή μιας ιδιωτικής IP διεύθυνσης ενός πακέτου σε μια κοινή IP διεύθυνση πρωτού το πακέτο σταλεί στο δημόσιο δίκτυο. Το RFC 1631 δεν προσδιορίζει αν η IP διεύθυνση που θα μεταφραστεί πρέπει να είναι ιδιωτική, απαραίτητα, μπορεί να είναι οποιαδήποτε διεύθυνση.

Κάποιοι κοινοί λόγοι για την χρήση του NAT είναι οι παρακάτω:

- ο ISP δεν μας έχει εκχωρήσει αρκετές κοινές IP διευθύνσεις.
- ο ISP δεν υποστηρίζει τις κοινές IP διευθύνσεις που χρησιμοποιεί το δίκτυο μας.
- μετά από την συγχώνευση δύο εταιριών που χρησιμοποιούν το ίδιο εύρος IP διευθύνσεων, π.χ. 10.0.0.0, πράγμα το οποίο δημιουργεί προβλήματα δρομολόγησης και επεκτασιμότητας.
- θέλουμε να αναθέσουμε την ίδια IP διεύθυνση σε πολλαπλούς υπολογιστές έτσι ώστε οι χρήστες του Διαδικτύου να βλέπουν την παρεχόμενη υπηρεσία ως έναν υπολογιστή.

Είδη Μετάφρασης Διευθύνσεων Δικτύου (NAT).

Υπάρχει μια πλειάδα από διαφορετικά είδη Μετάφρασης Διευθύνσεων Δικτύου όπως: Network Address Translation (NAT), Port Address Translation (PAT), στατική μετάφραση και δυναμική μετάφραση.

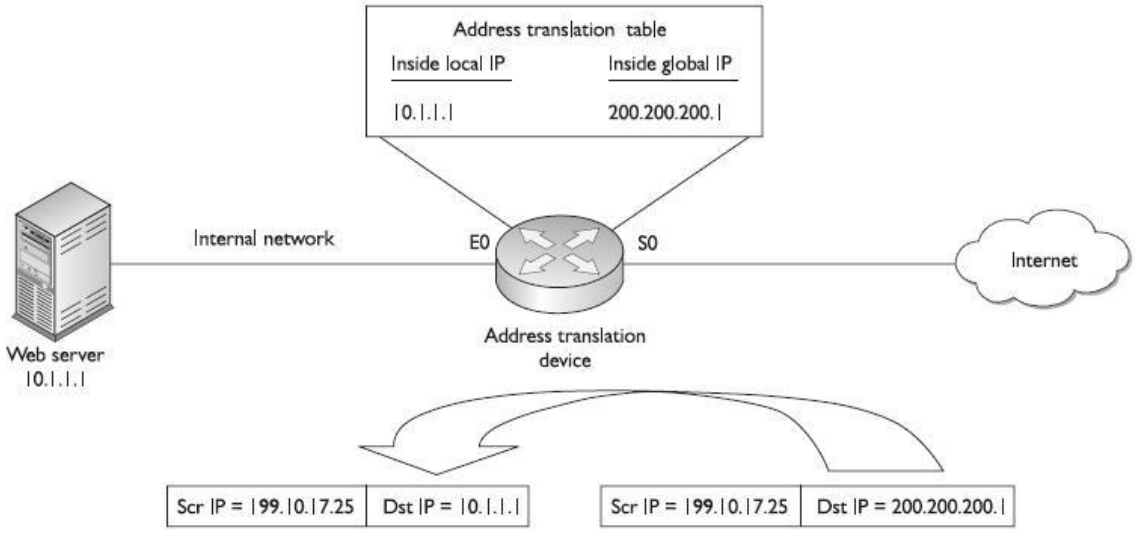
Όρος	Ορισμός
Εσωτερικό(Inside)	Δίκτυα εγκατεστημένα εντός του δικτύου μας
Εξωτερικό (Outside)	Δίκτυα εγκατεστημένα εκτός του δικτύου μας
Τοπικό (Local)	IP διεύθυνση που έχει καταχωρηθεί φυσικά σε μια συσκευή
Γενικό (Global)	IP διεύθυνση που έχει καταχωρηθεί φυσικά ή λογικά σε μια συσκευή
Εσωτερική τοπική IP διεύθυνση (Inside local)	Μια εσωτερική συσκευή με καταχωρημένη ιδιωτική IP διεύθυνση
Εσωτερική γενική IP διεύθυνση (Inside global)	Μια εσωτερική συσκευή με καταχωρημένη κοινή IP διεύθυνση
Εξωτερική τοπική IP διεύθυνση (Outside local)	Μια εξωτερική συσκευή με καταχωρημένη κοινή IP διεύθυνση
Εξωτερική γενική IP διεύθυνση (Outside global)	Μια εξωτερική συσκευή με καταχωρημένη ιδιωτική IP διεύθυνση

Πίνακας 2. Κοινή ορολογία Μετάφρασης διεύθυνσης δικτύου.

Μετάφραση Διεύθυνσης Δικτύου.

Το NAT μεταφράζει μια διεύθυνση σε μια άλλη. Αυτή η διεύθυνση μπορεί να είναι της πηγής ή του προορισμού. Υπάρχουν δύο τύποι υλοποίησης: στατικός και δυναμικός.

Με το στατικό NAT , συνήθως, γίνεται η μετάφραση της IP διεύθυνσης προορισμού στα εισερχόμενα πακέτα. Αλλά μπορεί να γίνει η μετάφραση της IP διεύθυνσης πηγής επίσης. Η **Εικόνα 1** απεικονίζει ένα απλό παράδειγμα όπου εξωτερικοί χρήστες έχουν πρόσβαση σε εσωτερικό web server.



Εικόνα 1. Στατικό NAT. Παράδειγμα.

Στην περίπτωση του στατικού NAT οι εγγραφές στον πίνακα μετάφρασης (address translation table) γίνονται χειροκίνητα. Όταν οι συσκευές μετάφρασης ή οι στατικές εγγραφές μετάφρασης είναι πολλές (π.χ. 1000) η διαχείριση γίνεται πολύ δύσκολη. Συνήθως, οι στατικές μεταφράσεις γίνονται για εσωτερικούς πόρους τους οποίους θέλουμε να είναι προσβάσιμοι από εξωτερικούς χρήστες. Όταν θέλουμε οι εσωτερικοί χρήστες να έχουν πρόσβαση σε εξωτερικούς πόρους χρησιμοποιούμε, συνήθως, το δυναμικό NAT. Σε αυτή την περίπτωση ορίζουμε δύο ομάδες διευθύνσεων, μια για τις εσωτερικές διευθύνσεις που επιτρέπεται να μεταφραστούν, και μια για τις διευθύνσεις στις οποίες θα μεταφραστούν. Όταν ένας εσωτερικός χρήστης στέλνει ένα πακέτο μέσω μιας συσκευής μετάφρασης, π.χ. ενός δρομολογητή, γίνεται σύγκριση της πηγαίας IP διεύθυνσης με το pool εσωτερικών διευθύνσεων (internal local pool). Εάν βρεθεί η διεύθυνση, τότε ο δρομολογητής καθορίζει ποιο inside global pool θα χρησιμοποιηθεί για την μετάφραση. Μετά, επιλέγεται δυναμικά μια global διεύθυνση η οποία δεν έχει ανατεθεί αλλού και προστίθεται αυτή η εγγραφή στο address translation table, και το πακέτο με αλλαγμένη την διεύθυνση αποστέλλεται στον έξω κόσμο. Εάν δεν βρεθεί η διεύθυνση στο local address pool, το πακέτο αποστέλλεται χωρίς καμία αλλαγή.
Στα εισερχόμενα πακέτα ο δρομολογητής ελέγχει το address translation table. Εάν βρεθεί εγγραφή με την διεύθυνση προορισμού γίνεται η μετατροπή της inside global διεύθυνσης σε inside local και το πακέτο προωθείται στο εσωτερικό δίκτυο.

12.2 Μετάφραση Θύρας Διεύθυνσης Δικτύου (PAT).

Το πρόβλημα τόσο με το στατικό όσο και το δυναμικό NAT είναι ότι παρέχει, μόνο, μετάφραση διευθύνσεων μια προς μια. Εάν οι εσωτερικές συσκευές, που χρειάζονται πρόσβαση στα εξωτερικά δίκτυα, είναι πολλές (π.χ. 5000) και μας έχουν εκχωρηθεί λιγότερες (π.χ. 1000) κοινές διευθύνσεις, τότε θα έχουν ταυτόχρονη πρόσβαση μόνο οι 1000 συσκευές. Για να ξεπεραστεί αυτό το πρόβλημα μπορούμε να χρησιμοποιήσουμε μια διεργασία που ονομάζεται υπερφόρτωση διεύθυνσης (address overloading). Αυτή η διεργασία είναι επίσης γνωστή ως Port Address Translation (PAT) ή Network

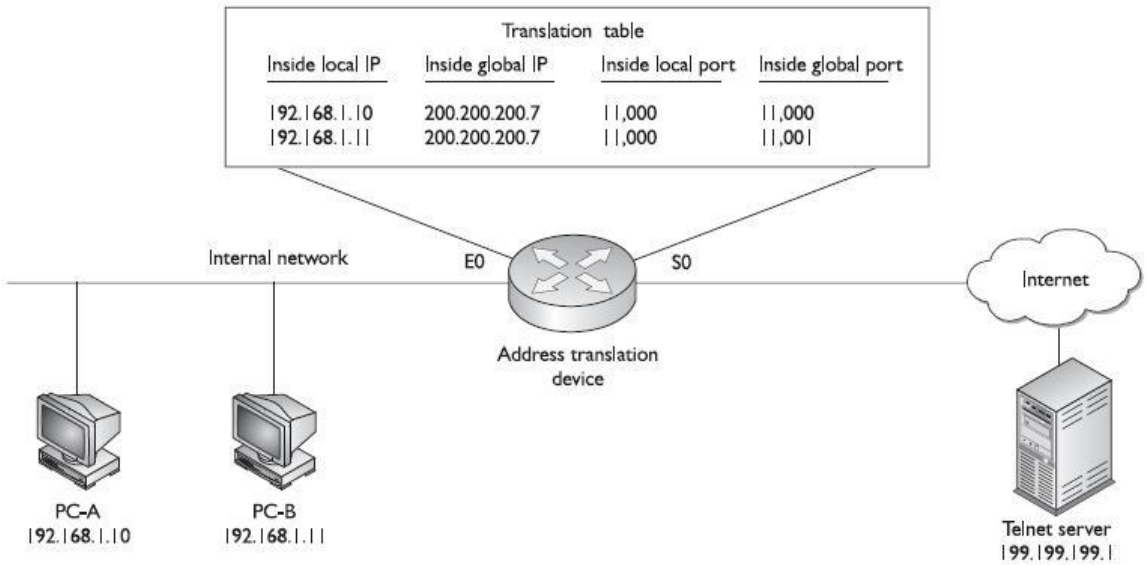
Address Port Translation (NAPT).

Στην περίπτωση του PAT όλοι οι υπολογιστές χρησιμοποιούν την ίδια inside global διεύθυνση και ο διαχωρισμός γίνεται βάσει του αριθμού της πηγαίας θήρας. Εάν δύο υπολογιστές χρησιμοποιούν την ίδια θήρα η συσκευή μετάφρασης αλλάζει τον αριθμό σε μια από αυτές (π.χ. αυξάνοντας τον αριθμό κατά μια μονάδα) για να εξασφαλιστεί η μοναδικότητα. Στο πίνακα μετάφρασης (translation table) θα υπάρχουν τα παρακάτω στοιχεία:

- Inside local IP address (original source private IP)
- Inside local port number (original source port number)
- Inside global IP address (translated public source IP)
- Inside global port number (new source port number)
- Outside global IP address (destination public address)
- Outside global port number (destination port number)

Ένα πλεονέκτημα του NAT σε σχέση με τον PAT είναι ότι το NAT δουλεύει για όλους τους τύπους IP συνδέσεων, ενώ το PAT, που βασίζεται στους αριθμούς θυρών για να κάνει τον διαχωρισμό, δουλεύει μόνο για τα TCP και UDP πρωτόκολλα. Η Cisco και μερικοί άλλοι κατασκευαστές υποστηρίζουν και το πρωτόκολλο ICMP με PAT χρησιμοποιώντας μια ιδιόκτητη μέθοδο μετάφρασης.

Παράδειγμα Χρήσης PAT.



Εικόνα 2. Παράδειγμα PAT

Αφού ο αριθμός της θύρας αποτελείται από 16 bit μπορούμε θεωρητικά να χρησιμοποιήσουμε την ίδια inside global διεύθυνση για 65536 υπολογιστές. Στην πραγματικότητα αυτός ο αριθμός είναι περίπου 4000.

Στην περίπτωση που θέλουμε οι εξωτερικοί χρήστες να έχουν πρόσβαση σε έναν εσωτερικό web server το δυναμικό PAT που είδαμε παραπάνω δεν μας κάνει. Η λύση σε αυτή την περίπτωση είναι το στατικό PAT (είναι γνωστό και ως Port Address Redirection – PAR).
Ας πάρουμε ένα παράδειγμα. Ο πάροχος (ISP) μας έχει εκχωρήσει μια κοινή IP διεύθυνση (π.χ.

199.199.199.1) και θέλουμε να δώσουμε πρόσβαση στους εξωτερικούς χρήστες για τον (εσωτερικό) web server. Με το στατικό PAT διαμορφώνουμε τον δρομολογητή μας έτσι ώστε να ελέγχει τον συνδυασμό IP διεύθυνση προορισμού και θύρας προορισμού (π.χ. 80). Εισάγουμε μια στατική PAT εγγραφή που όταν βρεθεί ένα εισερχόμενο πακέτο με αυτό τον συνδυασμό να μεταφράζει την διεύθυνση προορισμού σε inside local IP διεύθυνση, και ενδεχομένως να μεταφράζει και την θύρα σε θύρα που χρησιμοποιεί ο υπολογιστής που βρίσκεται στο εσωτερικό μας δίκτυο (ο web server μας).

Πλεονεκτήματα Μετάφρασης Διευθύνσεων Δικτύου.

- Μας δίνει έναν πρακτικά ανεξάντλητο αριθμό διευθύνσεων.
- Μας επιτρέπει την απόκρυψη του εσωτερικού δικτύου
- Στην περίπτωση αλλαγής παρόχου (ISP) δεν χρειάζετε να αλλάξουμε διευθυνσιοδώτηση.
- Καλύτερο έλεγχο της κυκλοφορίας των εισερχομένων και εξερχομένων πακέτων.

Μειονεκτήματα Μετάφρασης Διευθύνσεων Δικτύου.

- Η κάθε σύνδεση έχει μια επιπλέον καθυστέρηση.
- Ο εντοπισμός των βλαβών είναι πιο δύσκολος.
- Η μετάφραση διεύθυνσης δικτύου δεν υποστηρίζει όλες τις εφαρμογές (εφαρμογές πολυμέσων, NetBIOS).

12.3 Διαμόρφωση NAT & PAT

Η διαμόρφωση των διαφορετικών ειδών μετάφρασης, NAT και PAT, είναι παρόμοια.

Διαμόρφωση NAT.

Υπάρχουν δυο βασικά βήματα που πρέπει να εκτελέσουμε:

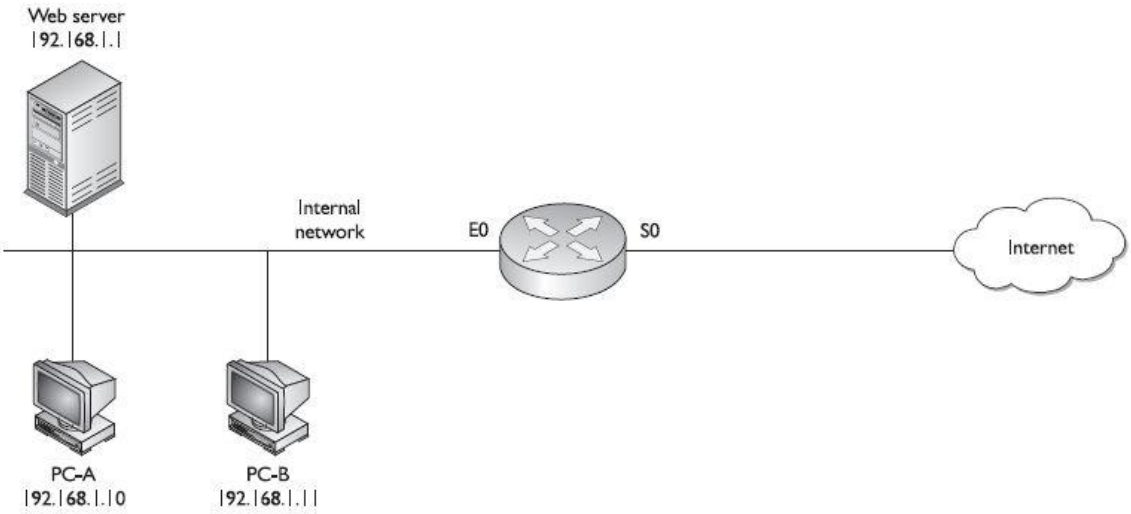
- Καθορισμός του είδους της μετάφρασης (εντολές Global Configuration).
- Καθορισμός των τοπικών συσκεύων (εντολές Interface Subconfiguration).

Στατικό NAT.

Router(config)# **ip nat inside source static**
inside_local_source_IP_address
inside_global_source_IP_address
Router(config)# **ip nat outside source static**
outside_global_destination_IP_address
inside_local_destination_IP_address

Οι παράμετροι **inside** και **outside** καθορίζουν την κατεύθυνση της μετάφρασης (π.χ. το inside καθορίζει ότι το inside source local IP διεύθυνση θα μεταφραστεί στην inside global IP διεύθυνση).
Μετά πρέπει να οριστούν ποιές διεπαφές (interfaces) του δρομολογητή μας θεωρούνται ‘μέσα’ και ‘έξω’:

Router(config)# **interface** *type [slot_#|]port_#*
Router(config-if)# **ip nat *inside*|*outside***



Εικόνα 3. Παράδειγμα NAT.

Router(config)# **ip nat inside source static 192.168.1.1 200.200.200.1**
Router(config)# **interface ethernet 0**
Router(config-if)# **ip nat inside**
Router(config-if)# **exit**
Router(config)# **interface serial 0**
Router(config-if)# **ip nat outside**

Δυναμικό NAT.

Στην περίπτωση του δυναμικού NAT, πρέπει να καθορίσουμε 3 πράγματα:
ποιες είναι οι εσωτερικές διευθύνσεις, ποιες είναι οι εξωτερικές διευθύνσεις, ποιες είναι οι εμπλεκόμενες διεπαφές.

Router(config)# **ip nat inside source**
list standard_IP_ACL_#
pool NAT_pool_name
Router(config)# **ip nat pool** NAT_pool_name
beginning_inside_global_IP_address
ending_inside_global_IP_address
netmask subnet_mask_of_addresses

Στην περίπτωση της Εικόνας 3 η διαμόρφωση είναι ως εξής:

Router(config)# **ip nat inside source list 1 pool nat-pool**
Router(config)# **access-list 1 permit 192.168.1.10 0.0.0.0**
Router(config)# **access-list 1 permit 192.168.1.11 0.0.0.0**
Router(config)# **ip nat pool nat-pool 200.200.200.2 200.200.200.3 netmask 255.255.255.0**
Router(config)# **interface ethernet 0**
Router(config-if)# **ip nat inside**
Router(config-if)# **exit**
Router(config)# **interface serial 0**
Router(config-if)# **ip nat outside**

Διαμόρφωση PAT.

Η διαμόρφωση του μοιάζει με το δυναμικό NAT. Χρησιμοποιούμε την ίδια εντολή, προσθέτοντας την λέξη κλειδί **overload**:

Router(config)# **ip nat inside source**
list standard_IP_ACL_#
pool NAT_pool_name **overload**

Μετά καθορίζουμε το global pool:

Router(config)# **ip nat pool** NAT_pool_name
beginning_inside_global_IP_address
ending_inside_global_IP_address
netmask subnet_mask_of_addresses

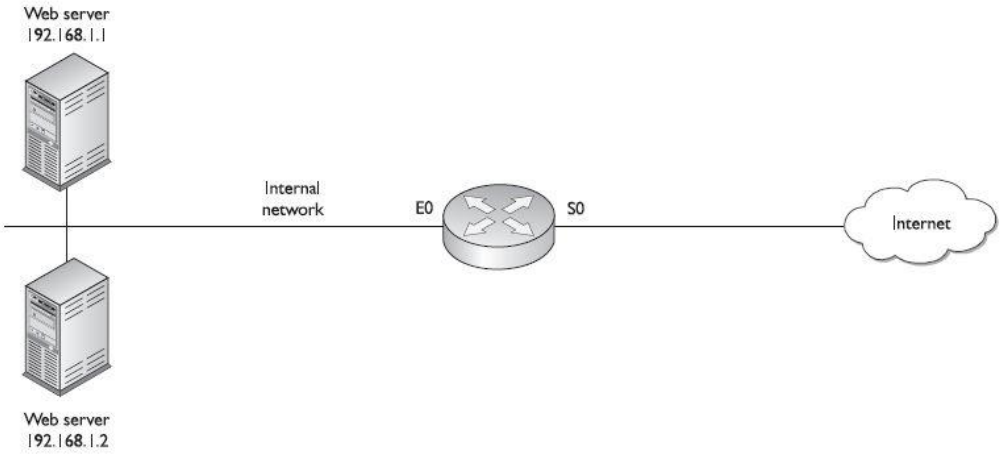
Η διαμόρφωση για την Εικόνα 3 είναι:

Router(config)# **ip nat inside source list 1 pool nat-pool overload**
Router(config)# **access-list 1 permit 192.168.1.10 0.0.0.0**
Router(config)# **access-list 1 permit 192.168.1.11 0.0.0.0**
Router(config)# **ip nat pool nat-pool 200.200.200.2 200.200.200.2 netmask 255.255.255.0**
Router(config)# **interface ethernet 0**
Router(config-if)# **ip nat inside**
Router(config-if)# **exit**
Router(config)# **interface serial 0**
Router(config-if)# **ip nat outside**

Διαμόρφωση Διανομής Φορτίου.

Χρησιμοποιούμε την εντολή:

Router(config)# **ip nat pool** pool_name
beginning_inside_local_IP_address
ending_inside_local_IP_address
prefix-length subnet_mask_bits
type rotary



Εικόνα 4. Διανομή φορτίου.

```
Router(config)# ip nat pool inside-hosts 192.168.1.1 192.168.1.2 prefix-length 24 type rotary
Router(config)# ip nat inside destination list 1 pool inside-hosts
Router(config)# access-list 1 permit 200.200.200.1
Router(config)# interface ethernet 0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface serial 0
Router(config-if)# ip nat outside
```

Χρήσιμες εντολές για την **Επαλήθευση Μετάφρασης Διεύθυνσης Δικτύου.**

```
Router# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 200.200.200.1 192.168.1.1 --- ---
--- 200.200.200.2 192.168.1.2 --- ---
```

Στην περίπτωση του PAT:

```
Router# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 200.200.200.1:1080 192.168.1.1:1080 201.1.1.1:23 201.1.1.1:23
tcp 200.200.200.1:1081 192.168.1.2:1080 201.1.1.1:23 201.1.1.1:23
```

Άλλες χρήσιμες εντολές:

```
Router# show ip nat statistics
Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet0
Hits: 98 Misses: 4
Expired translations: 1
Dynamic mappings:
-- Inside Source
access-list 1 pool nat-pool refcount 2
pool nat-pool: netmask 255.255.255.255
start 200.200.200.10 end 200.200.200.254
type generic, total addresses 12, allocated 1 (9%), misses 0
```

Για να καθαρίσουμε τις υφιστάμενες μεταφράσεις (δυναμικό NAT):

```
Router# clear ip nat translation *
Router# clear ip nat translation inside
            global_IP_address local_IP_address
Router# clear ip nat translation outside
            global_IP_address local_IP_address
Router# clear ip nat translation protocol inside
            global_IP_address global_port
            local_IP_address local_port
```

Για έρευνα των λαθών (debugging):

Router# **debug ip nat**
05:32:23: NAT: s=192.168.1.10->200.200.200.2, d=201.1.1.1 [70]
05:32:23: NAT*: s=201.1.1.1, d=200.200.200.2->192.168.1.10 [70]

13. Dynamic Host Configuration Protocol (DHCP).

Το DHCP επιτρέπει στις συσκευές να αποκτήσουν, δυναμικά, την πληροφορία διευθυνσιοδώτησης τους. Το DHCP, που καθορίζεται από το RFC 2131, είναι βασισμένο στο BOOTP. Είναι σχηματισμένο επάνω σε ένα μοντέλο client/server και έχει δύο αρθρώματα:

- Server. Που επιδίδει την πληροφορία διαμόρφωσης του host.
- Client. Που αιτήται και αποκτά την πληροφορία διαμόρφωσης του host.

Το DHCP παρέχει τα εξής πλεονεκτήματα:

- Ελαττώνει την πληροφορία διαμόρφωσης των συσκευών.
- Ελαττώνει την πιθανότητα σφαλμάτων διαμόρφωσης.
- Παρέχει καλύτερο και κεντρικό έλεγχο της IP διευθυνσιοδότησης.

DHCP Συσκευές και Λειτουργία.

Το DHCP περιέχει δύο είδη συσκευών: servers και clients. Οι δρομολογητές με IOS υποστηρίζουν και τις δύο λειτουργίες. Οι servers είναι υπεύθυνοι για την ανάθεση της πληροφορίας διευθυνσιοδώτησης στους clients, και οι clients αιτούνται αυτή την πληροφορία από τους servers.

Ο DHCP server μπορεί να χρησιμοποιήσει τρεις μηχανισμούς, οι οποίοι περιγράφονται στον Πίνακα 1, για την ανάθεση πληροφορίας διευθυνσιοδώτησης. Οι περισώτερες υλοποιήσεις χρησιμοποιούν την δυναμική ανάθεση.

Για να αποκτήσει πληροφορία διευθυνδιοδώτησης ο DHCP client ακολουθεί τα παρακάτω 4 βήματα:

1. ο client εκπέμπει DHCPDISCOVER για να εντοπίσει τους DHCP servers στο δικό του τμήμα δικτύου (broadcast).
2. όλοι οι servers που ανήκουν σε αυτό το τμήμα δικτύου μπορουν να απαντήσουν με ένα DHCPOFFER (unicast), με την προσφορά πληροφορίας IP διευθυνσιοδώτησης στον client. Εάν ένας client δεχτεί πολλαπλές προσφορές, επιλέγει μία (συνήθως την πρώτη).
3. αφού επιλέξει την προσφορά, ο client, απαντάει στον server με ένα DHCPREQUEST και αιτήται να κάνει χρήση της πληροφορίας διευθυνσιοδώτησης που έχει στείλει ο συγκεκριμένος server. Εάν υπάρχει μόνον ένας server και πληροφορία που έχει λάβει βρίσκεται σε διένεξη με την δική του διαμόρφωση, ο client απαντάει με DHCPDECLINE.
4. ο server απαντάει με ένα DHCPACK (acknowledgment). Ο server μπορεί να απαντήσει και με DHCPNACK το οποίο λέει στον client ότι η προσφορά του δεν είναι έγκυρη. Αυτό μπορεί να συμβεί όταν ο client αργήσει να στείλει το DHCPREQUEST.

Είδος κατανομής	**Επεξήγηση**
Αυτόματη	Ο server αναθέτει μια μόνιμη IP διεύθυνση στον client.
Δυναμική	Ο server αναθέτει μια IP διεύθυνση στον client για μια χρονική περίοδο.
Χειροκίνητη	Η IP διεύθυνση έιναι χειροκίνητα διαμορφωμένη στον client, και το DHCP

	χρησιμοποιήται για την μεταβίβαση επιπλέον πληροφορίας διευθυνσιοδώτησης και για επαλήθευση.

Πίνακας 1. DHCP. Είδη Κατανομής.

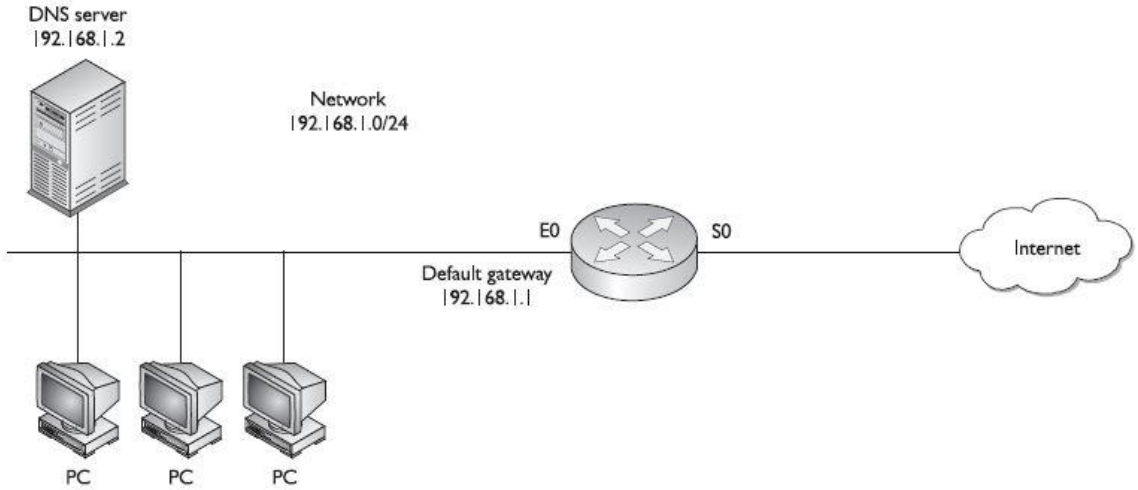
Όταν ένας client σταματάει τη λειτουργία του (shut down) μπορεί να στείλει μήνυμα DHCPRELEASE, λέγοντας στον server ότι δεν χρειάζεται πλεον την IP διεύθυνση.
Οι πλειονότητα των DHCP εγκαταστάσεων συνεπάγονται μια χρονική περίοδο ενοικίασης διεύθυνσης (lease time). Όταν παρέλθει αυτός ο χρόνος ο client πρέπει να ανανεώσει την ενοικίαση της IP διεύθυνσης του.

Το μήνυμα DHCPOFFER περιέχει την εξής πληροφορία: IP διεύθυνση του client, μάσκα υποδικτύου, IP διεύθυνση της πύλης (default gateway), όνομα τομέα DNS, διεύθυνση(εις) WINS server(s), διεύθυνση(εις) TFTP server(s) και άλλα.

DHCP Server. Διαμόρφωση.

Οι Cisco IOS δρομολογητές μπορούν να γίνουν DHCP servers. Σημειώσατε, ωστόσο, ότι δεν είναι πλρήρεις DHCP εξυπηρετητές και χρησιμοποιούνται συνήθως σε μικρά δικτυακά περιβάλοντα, όπως υποκαταστήματα και οικίες. Για την διαμόρφωση ενός DHCP server χρησιμοποιούμε τις εξής εντολές:

Η εντολή **service dhcp** ενεργοποιεί ή απενεργοποιεί την υπηρεσία στον δρομολογητή μας. Αυτή η υπηρεσία είναι ενεργοποιημένει εξ οριζμού. Η εντολή **ip dhcp pool** δημιουργεί μια ομάδα διευθύνσεων με μοναδικό όνομα. Αυτή η εντολή δίνεται σε *DHCP Subconfiguration mode.*
Η εντολή **network** καθορίζει το εύρος των διευθύνσεων, οι οποίες θα ανατεθούν στους clients.
Η εντολή **domain-name** καθορίζει το όνομα του τομέα για τον client. Οι εντολές **netbios-name-server** καθορίζει τους εξυπηρετητές WINS (μέχρι 8 εξυπηρετητές). Και η εντολή **netbios-name-type** καθορίζει το είδος του client που μπορεί να είναι: **b (**broadcast**), p (**WINS**), m (**broadcast και μετά WINS**)**. Η εντολή **default-router** μας επιτρέπει να καθορίσουμε την δικτυακή πύλη (μέχρι 8 default gateways). Η εντολή **lease** καθορίζει την διάρκεια της ανάθεσης IP διεύθυνσης.
Πρωτού αναθέσει μια IP διεύθυνση στον client ο server κάνει ping την συγκεκριμένη διεύθυνση για να ελέγξει την διαθεσιμότητα της πριν στείλει το μήνυμα DHCPOFFER. Γι'αυτό το λόγο υπάρχει η εντολή **ip dhcp ping timeout**. Εξ ορισμού το timeout είναι 500 ms.
Υπάχει και η εντολή **ip dhcp excluded-address** για τον αποκλεισμό ορισμένων διευθύνσεων από το pool, που θα αντεθούν, ενδεχομένως, στατικά.



Εικόνα 1. Παράδειγμα DHCP.

```
Router(config)# [no] service dhcp
Router(config)# ip dhcp pool pool_name
Router(config-dhcp)# network network_number [subnet_mask |
/prefix_length]
Router(config-dhcp)# domain-name domain_name
Router(config-dhcp)# dns-server IP_address [IP_address_2...IP_address_8]
Router(config-dhcp)# netbios-name-server IP_address
[IP_address_2...IP_address_8]
Router(config-dhcp)# netbios-node-type node_type
Router(config-dhcp)# default-router IP_address
[IP_address_2...IP_address_8]
Router(config-dhcp)# lease days [hours][minutes] | infinite
Router(config-dhcp)# exit
Router(config)# ip dhcp ping timeout milliseconds
Router(config)# ip dhcp excluded-address beginning_IP_address
[ending_IP_address]
```

DHCP Client. Διαμόρφωση. Μπορούμε να διαμορφώσουμε μια διεπαφή του IOS δρομολογητή μας να αποκτήση την IP διεύθυνση του με DHCP. Είναι η περίπτωση όπου ο δρομολογητής μας είναι κατευθείαν συνδεδεμένος με τον πάροχο (ISP) μέσω dialup, PPPoE, PPPoA.

```
Router(config)# interface type [slot_#/]port_#
Router(config-if)# ip address dhcp
```

DHCP Επαλήθευση. Οι εντολές επαλήθευσης είναι οι εξής:

```
Router# show ip dhcp binding [client_address]
Router# clear ip dhcp binding client_address |
Router# debug ip dhcp server events|packet|linkage *
```

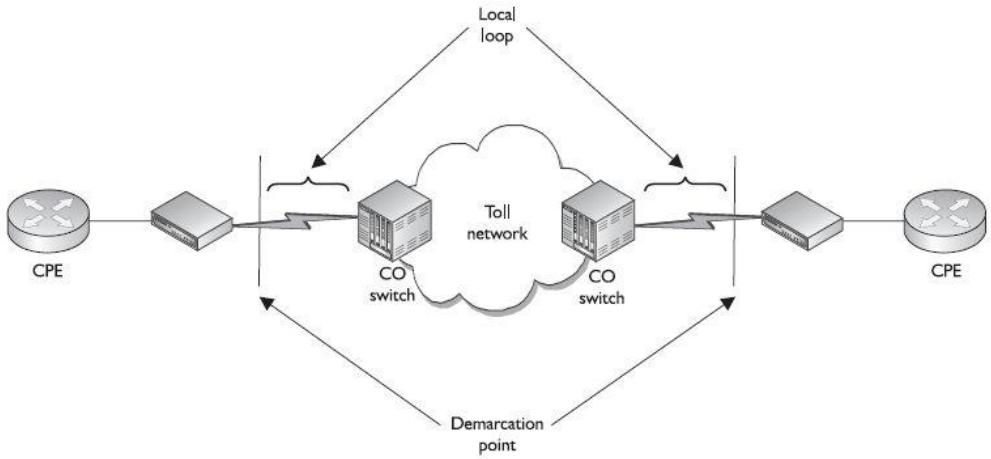
14. Τεχνολογίες WAN (Wide Area Networks).

Συνήθως, οι συνδέσεις LAN υπάρχουν εντός μιας εταιρίας, ενώ, οι συνδέσεις WAN μας επιτρέπουνε να συνδεθούμε σε απομακρυσμένες τοποθεσίες. Συνήθως, δεν είμαστε οι κάτοχοι της υποδομής για συνδέσεις WAN και αυτές οι συνδέσεις είναι πιο αργές.

Ένα παράγωγο του WAN είναι το MAN (Metropolitan Area Network). Τα MAN είναι υψηλής ταχύτητας συνδέσεις, μέσα σε μία μικρή γεωγραφικά έκταση, μεταξύ διαφορετικών εταιριών ή μεταξύ διαφορετικών διευθύνσεων μιας εταιρίας. Τα MAN έχουν γίνει πολύ δημοφιλή σε μεγάλες πόλεις και παρέχουν ακόμα και συνδέσεις πάνω από LAN μέσα, όπως το Ethernet.

Ένας από τους βασικούς παράγοντες όταν επιλέγουμε πάροχο WAN ή MAN είναι το κόστος. Επιπλέον, οι επιλογές των λύσεων μπορεί να είναι πολλές στο πρόβλημα της σύνδεσης WAN. Για να κάνουμε την σωστή επιλογή πρέπει να εκτιμήσουμε προσεκτικά τής απαιτήσεις της σύνδεσης, την πληροφορία που διακινείτε και το κόστος.

Οι συνδέσεις WAN αποτελούνται από πολλά είδη εξοπλισμού και αρθρωμάτων. Στην Εικόνα 1 απεικονίζονται μερικά από αυτά.



Εικόνα 1. Αρθρώματα WAN.

Ο Πίνακας 1 αριθμεί μία λίστα από όρους και ορισμούς.

Όρος	Ορισμός
CPE (Customer Premises Equipment)	Ο δικτυακός εξοπλισμός μας, συμπεριλαμβάνει το DCE (modem, NT1, CSU/DSU) και το DTE (δρομολογητής, διακομιστής πρόσβασης).
Demarcation point	Το σημείο παραχώρησης της υπευθυνότητας από τον φορέα σε εμάς. Η οριοθέτηση είναι λογική όχι απαραίτητα φυσική.
Local loop	Η σύνδεση από τον μεταγωγικό εξοπλισμό του φορέα στο demarcation point.
CO (Central Office)	Ο μεταγωγέας του φορέα εντός του δικτύου του.
Toll network	Το δίκτυο του φορέα με την υποδομή μεταφοράς δεδομένων.

Πίνακας 1. Όροι και Ορισμοί.

14.1 Είδη Συνδέσεων.

Οι επιλογές για συνδέσεις WAN περιλαμβάνουν: αναλογικά modem, ISDN, ATM, μισθωμένες γραμμές (ή κυκλώματα), DSL, Frame Relay, SMDS, ασύρματες συνδέσεις (κυψελοτές, μικροκυματικές-laser, ράδιο-συχνότητες, δορυφορικές), X.25. Υπάρχουν 4 βασικές κατηγορίες:

- Μισθωμένες γραμμές.
- Μεταγωγικά κυκλώματα (π.χ. ISDN).
- Μεταγωγή πακέτων (π.χ. Frame Relay, X.25).
- Μεταγωγή κυψελών (π.χ. ATM, SMDS).

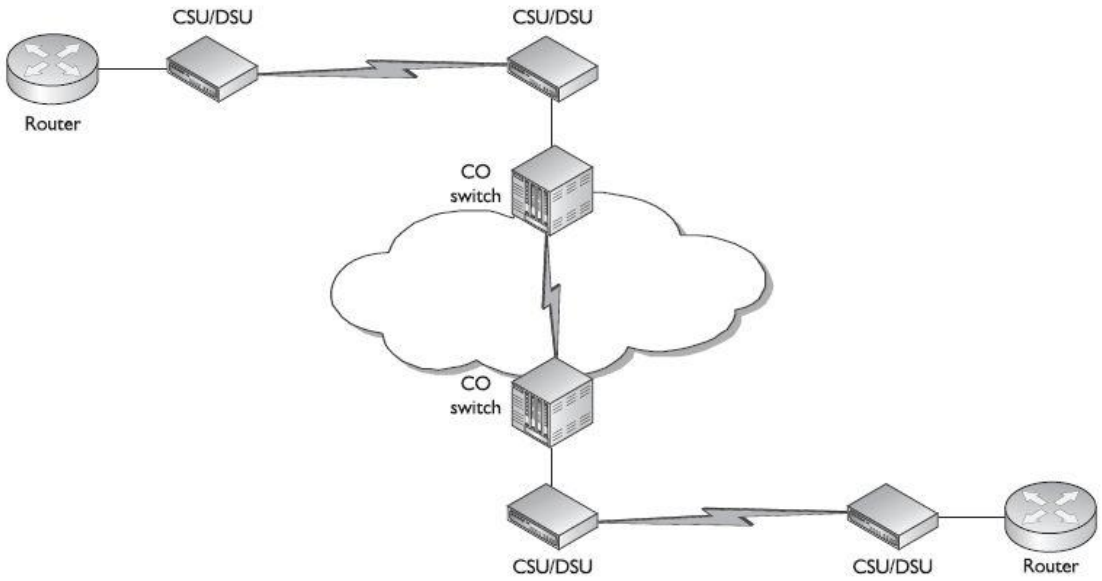
Μισθωμένες Γραμμές.

Η μισθωμένη γραμμή είναι βασικά μια σύνδεση μεταξύ δύο τοποθεσιών. Υπάρχουν δύο απαραίτητες συνθήκες:

- Μικρή απόσταση μεταξύ των δύο τοποθεσιών.
- Σταθερή κυκλοφορία μεταξύ των δύο τοποθεσιών και ανάγκη εγγυημένου bandwidth.

Αν και οι μισθωμένες γραμμές παρέχουν εγγυημένο bandwidth και ελάχιστη καθυστέρηση, υπάρχουν και άλλες διαθέσιμες λύσεις (π.χ. ATM) με τα ίδια χαρακτηριστικά. Το βασικό μειονέκτημα των μισθωμένων γραμμών είναι το κόστος.
Οι μισθωμένες γραμμές χρησιμοποιούν σύγχρονες συνδέσεις με ταχύτητες από 2400 bps έως 45 Mbps (DS3).
Για μια μισθωμένη γραμμή χρειαζόμαστε τον εξής εξοπλισμό:

- DTE δρομολογητής με σύγχρονες σειριακές διεπαφές που παρέχουν το data link framing και τερματίζουν τη σύνδεση.
- DCE συσκευή CSU/DSU που τερματίζει την σύνδεση του φορέα πάνω από την μισθωμένη γραμμή και παρέχει χρονισμό και συγχρονισμό.



Εικόνα 2. Εξοπλισμός μισθωμένης γραμμής.

Τα πρωτόκολλα που χρησιμοποιούνται περιλαμβάνουν: PPP, SLIP, HDLC.

Μεταγωγικά Κυκλώματα.

Οι συνδέσεις μεταγωγικών κυκλωμάτων συμπεριλαμβάνουν τα εξής είδη:

- Ασύγχρονες σειριακές συνδέσεις. Είναι συνδέσεις αναλογικού modem μέσω POTS. Είναι οι φθηνότερες.
- Σύγχρονες σειριακές συνδέσεις. Είναι ψηφιακές συνδέσεις ISDN BRI ή PRI που παρέχουν εγγυημένο bandwidth. Είναι ακριβότερες και, συνήθως, κοστολογούνται με χρονοχρέωση.

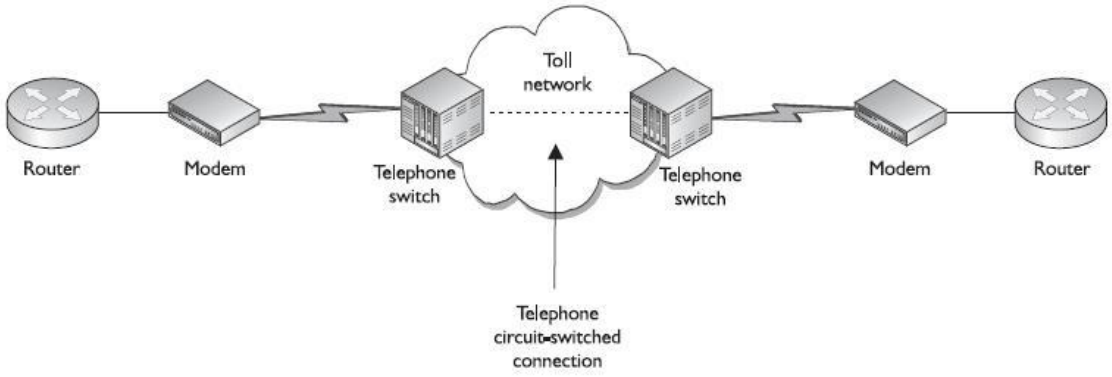
Ο εξοπλισμός που χρειάζεται για τις αναλογικές συνδέσεις είναι ο παρακάτω:

- DTE. Ένας δρομολογητής με ασύγχρονη σειριακή διεπαφή.
- DCE. Ένα modem.

Ο εξοπλισμός που χρειάζεται για τις ψηφιακές συνδέσεις είναι ο παρακάτω:

- DTE. Ένας δρομολογητής με ISDN διεπαφή.
- DCE. Μια NT1 συσκευή για BRI ή μια συσκευή CSU/DSU για PRI.

Οι ψηφιακές συνδέσεις, πολλές φορές, χρησιμοποιούνται εναλλακτικά (backup) των αναλογικών.
Τα πρωτόκολλα που χρησιμοποιούνται είναι, συνήθως, τα εξής: PPP, HDLC και SLIP (σπανίως).



Εικόνα 3. Σύνδεση Αναλογικού μεταγωγικού κυκλώματος.

Μεταγωγή Πακέτων.

Με τις μισθωμένες γραμμές υπάρχει ένα φυσικό κύκλωμα, πάντα το ίδιο, που υλοποιεί τη σύνδεση. Χρειάζεται ξεχωριστό φυσικό κύκλωμα για κάθε ζεύξη. Με τα μεταγωγικά κυκλώματα σχηματίζεται ένα κύκλωμα κάθε φορά που γίνεται η τηλεφωνική κλήση. Υπάρχει μεγάλη πιθανότητα να σχηματιστεί το ίδιο κύκλωμα για κάθε τηλεφωνική κλήση.

Στην περίπτωση της μεταγωγής πακέτων, οι συνδέσεις χρησιμοποιούν λογικά κυκλώματα τα οποία ονομάζονται ιδεατά κυκλώματα (VC - virtual circuits). Τα πλεονεκτήματα αυτής της αντιμετώπισης είναι τα εξής: το λογικό κύκλωμα δεν δεσμεύεται με κανένα φυσικό κύκλωμα και πάνω από ένα φυσικό κύκλωμα μπορούν να σχηματιστούν πολλαπλά λογικά κυκλώματα.

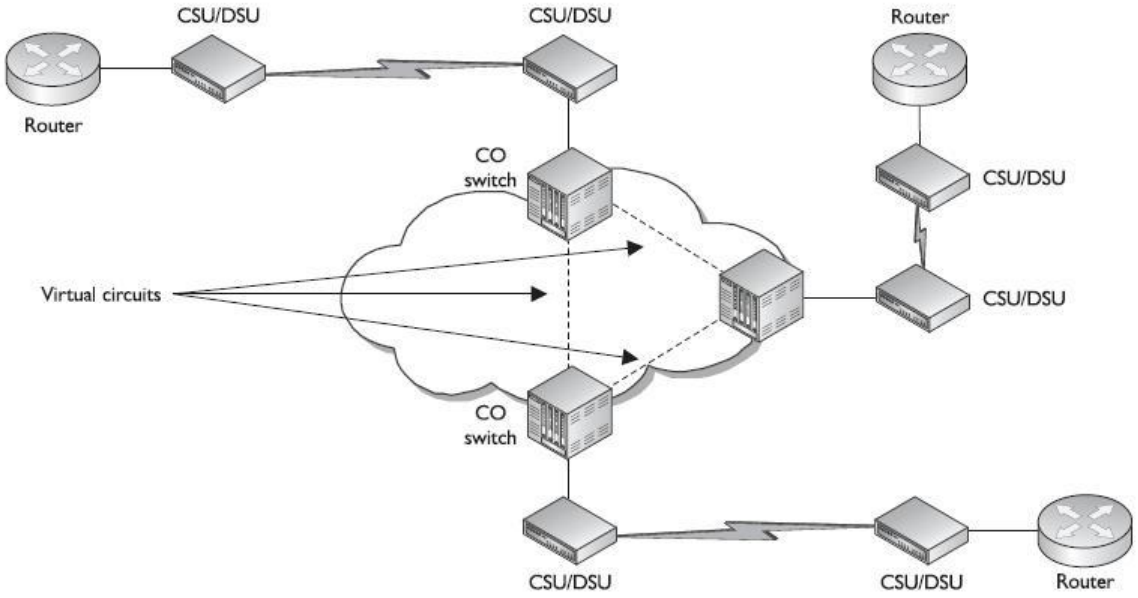
Η μεταγωγή πακέτων χρησιμοποιεί τις εξής τεχνολογίες: ATM, Frame Relay, SMDS και X.25. Από πλευράς κόστους οι λύσεις μεταγωγής πακέτων βρίσκονται κάπου ανάμεσα στις μισθωμένες γραμμές και στα μεταγωγικά κυκλώματα.

Το X.25, η παλαιότερη από της 4 τεχνολογίες, τρέχει πάνω από, τόσο, σύγχρονα, όσο και, ασύγχρονα κυκλώματα. Έχει σχεδιαστεί να τρέχει πάνω από αναξιόπιστες συνδέσεις, και παρέχει εντοπισμό λαθών όσο και διόρθωση λαθών τόσο στο data link επίπεδο (LAPB) όσο και στο network επίπεδο (X.25). Στην περίπτωση που έχουμε αναξιόπιστες ασύγχρονες αναλογικές συνδέσεις το X.25 είναι το πιο ενδεδειγμένο.

Στην περίπτωση που έχουμε σύγχρονες ψηφιακές συνδέσεις οι τεχνολογίες ATM ή Frame Relay είναι πιο αποδοτικές. Το Frame Relay δεν κάνει, όπως το X.25, διόρθωση λαθών ή έλεγχο ροής, ωστόσο κάνει εντοπισμό λαθών και κόβει τα λανθασμένα frames. Είναι ευθύνη πρωτοκόλλου υψηλότερου επιπέδου (π.χ. TCP) η επανα-αποστολή της πληροφορίας που έχει χαθεί. Το Frame Relay υποστηρίζει ταχύτητες από κλασματικές E1/T1 συνδέσεις (56-64 Kbps) έως DS3 (45 Mbps).
Για Frame Relay χρειαζόμαστε τον εξής εξοπλισμό:

- DTE. Δρομολογητής με σύγχρονη σειριακή διεπαφή.
- DCE. Συσκευή CSU/DSU για τη σύνδεση με τον φορέα.

Οι τεχνολογίες ATM, SMDS είναι ειδικές περιπτώσεις μεταγωγής πακέτων πάνω από ψηφιακά κυκλώματα οι οποίες χρησιμοποιούν πακέτα αμετάβλητου μήκους (53 bytes) τα οποία ονομάζονται κυψέλες (cells). Για αυτό το λόγο οι τεχνολογίες αυτές ονομάζονται υπηρεσίες μεταγωγής κυψελών. Τα πλεονεκτήματα τους σε σύγκριση με το Frame Relay είναι ότι παρέχουν εγγυημένο throughput και ελάχιστη καθυστέρηση για μια πλειάδα υπηρεσιών όπως: φωνή, βίντεο και δεδομένα. Το ATM, για παράδειγμα, παρέχει εγγυημένο bandwidth, περιορισμένο delay, περιορισμένο αριθμό λαθών, Quality Of Service (QOS) κα. Οι ταχύτητες του ATM μπορούν να φτάσουν σε πολύ υψηλά επίπεδα 10Gbps (OC-192 SONET). Το κόστος είναι μεγαλύτερο από το Frame Relay.



Εικόνα 4. Σύνδεση Frame Relay.

Διεπαφές WAN στους δρομολογητές Cisco.

Η Cisco υποστηρίζει μια μεγάλη ποικιλία από σειριακά καλώδια για σύγχρονες συνδέσεις, συμπεριλαμβανομένων των παρακάτω: EIA/TIA-232, EIA/TIA-449, EIA/TIA-530, V.35 και X.21. Αυτά είναι τα πρότυπα εκείνου του άκρου του καλωδίου που συνδέεται στο DCE. Ωστόσο το άκρο που συνδέεται στον δρομολογητή ακολουθεί ένα ιδιόκτητο πρότυπο που έχει δύο ειδών βύσματα:

- DB-60. Έχει 60 ακίδες.
- DB-26. Έχει 26 ακίδες και μοιάζει με το USB.

Μέθοδοι Encapsulation.

Πρωτόκολλο	**Επεξήγηση**
High-level Data Link Control (HDLC)	Βασισμένο σε πρότυπα ISO για χρήση με σύγχρονες ή ασύγχρονες συνδέσεις.
Synchronous Data Link Control (SDLC)	Για χρήση σε IBM SNA περιβάλλοντα. Αντικαταστάθηκε από το HDLC.
Link Access Procedure Balanced (LAPB)	Γι α χρήση X.25 με εκτεταμένο εντοπισμό και διόρθωση λαθών.
Link Access Procedure D channel (LAPD)	Για χρήση ISDN call setup, teardown τηλεφωνικών συνδέσεων.
Link Access Procedure Frame mode bearer services (LAPF)	Για χρήση Frame Relay μεταξύ DTE, DCE. Όμοιο με το LAPD.
Point-to-Point Protocol (PPP)	Βασισμένο σε πρότυπα RFC. Παρέχει πιστοποίηση χρηστών, διαχείριση πολλαπλών πρωτοκόλλων, συμπίεση και διόρθωση λαθών.

Πίνακας 2. Κοινές μέθοδοι encapsulation.

15. Point-to-Point Protocol (PPP).

Το πρωτόκολλο PPP είναι βασισμένο στο πρότυπο που ορίζεται από τα ακόλουθα RFC: 1332, 1661 και 2153. Το PPP υποστηρίζει ασύγχρονες, σύγχρονες σειριακές διεπαφές, διεπαφές High-Speed Serial Interfaces (HSSI) και διεπαφές ISDN (BRI, PRI).

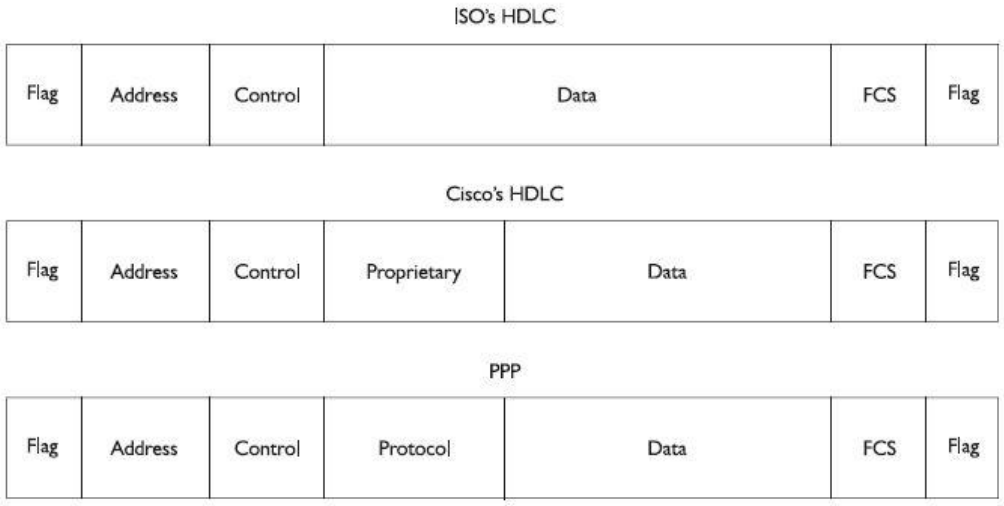
Το PPP έχει τα εξής χαρακτηρηστικά:

- Είδος frame
- Πολυπλεξία πρωτοκόλλων (data link και network layer)
- Δυναμική διαμόρφωση των ζεύξεων
- Συμπίεση επικεφαλλίδων των πακέτων
- Ελέγχος ποιότητας των ζεύξεων
- Εντοπισμός και διόρθωση λαθών
- Δέσιμο πολλαπλών φυσικών συνδέσεων PPP σε μια λογική σύνδεση

Το PPP έχει 3 βασικά αρθρώματα:

- Διάταξη του frame
- LCP (Link Control Protocol)
- NCP (Network Control Protocol)

Το είδος του frame καθορίζει πως τα πακέτα του network layer περικλείονται σε ένα PPP frame (encapsulation) και τη διάταξη του frame. Συνήθως, το PPP χρησιμοποιείται για σειριακές WAN συνδέσεις λόγο του ότι είναι βασισμένο σε ανοιχτό πρότυπο. Το PPP υποστηρίζει ασύγχρονες, σύγχρονες σειριακές διεπαφές, διεπαφές High-Speed Serial Interfaces (HSSI) και διεπαφές ISDN (BRI, PRI). Η διάταξη του frame απεικονίζεται στην Εικόνα 1 συγριτικά με το HDLC και έδω μπορούμε να δούμε ότι η βασική διαφορά μεταξύ τους είναι το πεδίο που ορίζει το network layer πρωτόκολλο.



Εικόνα 1. Διατάξεις frame (ISO HDLC, Cisco HDLC, PPP)

Το LCP ορίζεται από τα ακόλουθα RFCs 1548 και 1570. Η κύρια υπευθυνότητα του είναι να αποκαταστήσει, να διαμορφώσει, να πιστοποιήσει και να ελέγξει τη PPP σύνδεση. Μερικά από τα πράγματα που το LCP θα διαπραγματευτεί στο στήσιμο μιας σύνδεσης είναι τα εξής:

- Μέθοδο πιστοποίησης (PAP ή CHAP), εάν υπάρχει

- Αλγόριθμο συμπίεσης (Stacker ή Predictor), εάν υπάρχει
- Τηλεφωνικό αριθμό αντίστροφης κλήσης, εάν έχει οριστεί
- Multilink: άλλη φυσική σύνδεση προς χρήση, εάν έχει ρυθμιστεί

Υπάρχουν 3 βήματα τα οποία ακολουθούνται από τα LCP και NCP για την αποκατάσταση μιας PPP σύνδεσης:

1. Αποκατάσταση ζεύξης (LCP)
2. Πιστοποίηση (LCP)
3. Διαπραγμάτευση πρωτοκόλλου (NCP)

Στην πρώτη φάση της αποκατάστασης της ζεύξης το LCP θα διαπραγματευτεί τις παραμέτρους PPP που θα χρησιμοποιηθούν από τη σύνδεση όπως τη μέθοδο πιστοποίησης και τον αλγόριθμο συμπίεσης. Εάν έχει οριστεί πιστοποίηση γίνεται διαπραγμάτευση του είδους της πιστοποίησης (PAP ή CHAP). Στο δεύτερο βήμα εκτελείται η πιστοποίηση. Σε περίπτωση επιτυχούς πιστοποίησης, το NCP, στο τρίτο βήμα θα διαπραγματευτεί τα πρωτόκολλα υψηλοτέρου επιπέδου τα οποία περιλαμβάνουν IP, IPX (network layer πρωτόκολλα), όπως επίσης και Ethernet, CDP (data link layer πρωτόκολλα) τα οποία θα μεταδοθούν δια μέσου της PPP σύνδεσης.
Άπαξ και η σύνδεση έχει αποκατασταθεί, το LCP θα χρησιμοποιήσει τον εντοπισμό λαθών για τη συνεχή παρακολούθηση των δεδομένων που έχουν χαθεί και θα κάνει έλεγχο για βρόγχους στο data link layer επίπεδο.

Η διαμόρφωση γίνεται απλά με τις παρακάτω εντολές. Σημειώσατε ότι έδώ δεν θα σηζητηθούν όλες οι PPP παράμετροι.

```
Router(config)# interface type [slot_#]port_#
Router(config-if)# encapsulation ppp
```

Επαλήθευση, Εύρεση Λαθών (Troubleshooting).

```
Router# show interfaces serial 0
Serial0 is up, line protocol is up
Hardware is MCI Serial
Internet address is 192.168.1.2 255.255.255.0
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255,load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
lcp state = OPEN
ncp ccp state = NOT NEGOTIATED ncp ipcp state = OPEN
ncp osicp state = NOT NEGOTIATED ncp ipxcp state = NOT NEGOTIATED
ncp xnscp state = NOT NEGOTIATED ncp vinescp state = NOT NEGOTIATED
ncp deccp state = NOT NEGOTIATED ncp bridgecp state = NOT NEGOTIATED
ncp atalkcp state = NOT NEGOTIATED ncp lex state = NOT NEGOTIATED
ncp cdp state = OPEN
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters never
<--output omitted-->
```

Στην πέμπτη γραμμή βλέπουμε ότι το encapsulation είναι PPP. Παρακάτω την κατάσταση του LCP (lcp state = OPEN) αυτό σημαίνει ότι το LCP διαπραγματεύτικε επιτυχώς τις παραμέτρους και αποκατέστησε το data link layer. Οι καταστάσεις των NCP πρωτοκόλλων ακολουθούν. Σε αυτό το παράδειγμα τρέχουν δύο πρωτόκολλα δια μέσου της PPP σύνδεσης: IP (ncp icp state = OPEN) και CDP (ncp cdp state = OPEN).
Στην περίπτωση που έχουμε πρόβλημα με το data link layer μπορούμε να χρησιμοποιήσουμε την παρακάτω εντολή:

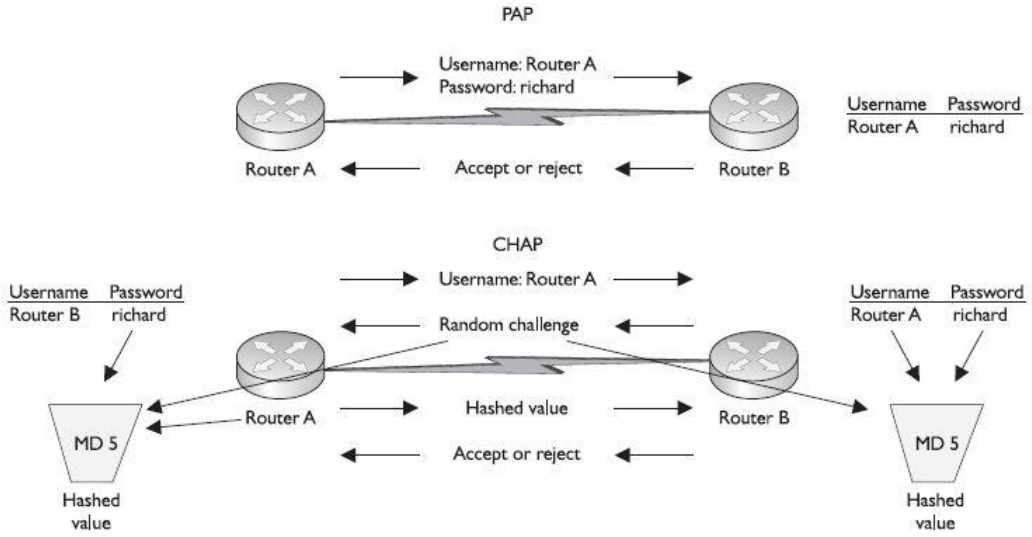
```
Router# debug ppp negotiation
PPP protocol negotiation debugging is on
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface serial 0
Router(config-if)# no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 4FEFE5
PPP Serial0: received config for type = 0x5 (MAGICNUMBER) value =
0x561036 acked
PPP Serial0: state = ACKSENT fsm_rconfack(0xC021): rcvd id 0x2
ppp: config ACK received, type = 5 (CI_MAGICNUMBER), value = 4FEFE5
ipcp: sending CONFREQ, type = 3 (CI_ADDRESS), Address = 192.168.2.1
ppp Serial0: Negotiate IP address: her address 192.168.2.2 (ACK)
ppp: ipcp_reqci: returning CONFACK.
ppp: cdp_reqci: returning CONFACK
PPP Serial0: state = ACKSENT fsm_rconfack(0x8021): rcvd id 0x2
ipcp: config ACK received, type = 3 (CI_ADDRESS), Address = 192.168.2.1
PPP Serial0: state = ACKSENT fsm_rconfack(0x8207): rcvd id 0x2
ppp: cdp_reqci: received CONFACK
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state
to up
```

Στο παράδειγμα τρέξαμε πρώτα debug και μετά ενεργοποιήσαμε την σειριακή διεπαφή. Μπορούμε να δούμε πώς οι δύο δρομολογητές κάνουν την διαπραγμάτευση. Πρώτα ελέγχουν τις IP διευθύνσεις 192.168.2.1, 192.168.2.2 να μήν είναι ίδιες και μετά διαπραγματεύονται τα πρωτόκολλα (ipcp_reqci και cdp_reqci). Στο παράδειγμα μας τα πρωτόκολλα IP και CDP έχουν διαπραγματευτεί επιτυχώς και το data link layer ενεργοποιείται.

15.1 Πιστοποίηση PPP.

Το PPP, αντιθέτως από το HDLC, υποστηρίζει την πιστοποίηση της συσκευής. Υπάρχουν δύο μέθοδοι προς επιλογή: PPP Authentication Protocol (PAP) και Challenge Handshake Authentication Protocol (CHAP). Και οι δύο μέθοδοι πιστοποίησης ορίζονται από το πρότυπο RFC 1334. Το RFC 1994 αντικαθιστά το CHAP που υπάρχει στο RFC 1334. Η διαδικασία της πιστοποίησης εκτελείται πρωτού τις διαπραγματεύσεις των network και data link layer πρωτοκόλλων από το NCP για λογαριασμό της PPP σύνδεσης. Εάν η πιστοποίηση αποτύχει τότε η ζεύξη δεν θα αποκατασταθεί. Η διαδικασία της πιστοποίησης είναι προαιρετική και προσθέτει μια πολύ μικρή καθυστέρηση.



Εικόνα 2. Πιστοποίηση PPP

PAP.

Το PAP είναι πιο απλό αλλά λιγότερο ασφαλές. Εκτελείται μια διαδικασία two-way handshake. Κατά την διάρκεια αυτής της διαδικασίας το όνομα χρήστη (username) ή hostname και ο κωδικώς (password) αποστέλλονται χωρίς να κρυπτογραφηθούν από την αφετηρία στον προορισμό. Εκεί συγκρίνονται με μια τοπική λίστα από usernames και passwords και αν βρεθεί ένα ίδιο ζεύγος τότε αποστέλλεται ένα μήνυμα accept. Διαφορετικά αποστέλλεται ένα μήνυμα reject.
Για την διαμόρφωση του PAP πρώτα πρέπει να καθοριστούν οι δύο πλευρές: client και server side. Στην πλευρά του client εκτελούμε τα εξής:

```
Router(config)# interface type [slot_#]port_#
Router(config-if)# encapsulation ppp
Router(config-if)# ppp pap sent-username your_hostname
password password
```

Στην πλευρά του server εκτελούμε τα εξής:

```
Router(config)# hostname your_router's_hostname
Router(config)# username remote_hostname
password matching_password
Router(config)# interface type [slot_#/]port_#
Router(config-if)# encapsulation ppp
Router(config-if)# ppp authentication pap
```

CHAP.

Το CHAP χρησιμοποιεί μια one-way hash συνάρτηση βασισμένει στο Message Digest 5 (MD5) αλγόριθμο για την κρυπτογράφηση του κωδικού χρήστη. Η συνάρτηση λέγεται one-way hash επιδή δεν μπορεί να αποκρυπτογραφηθεί (δεν υπάρχει αντίστροφη συνάρτηση αποκρυπτογράφησης).
Επίσης, το CHAP χρησιμοποιεί μια διαδικασία three-way handshake για την πιστοποίηση.
Το challenge περιέχει τις παρακάτω πληροφορίες:

- Packet identifier: 01 challenge, 02 reply, 03, allow PPP connection, 04 deny.
- ID: ένας αριθμός τοπικής σημασίας για τον διαχωρισμό μεταξύ διαφορετικών διαδικασιών πιστοποίησης.
- Random number: ένας τυχαίος αριθμός που θα χρησιμοποιηθεί από την συνάρτηση MD5.
- Router Name: το όνομα που στέλνει ochallenging δρομολογητή (server) και που θα χρησιμοποιήσει μετά για την επαλήθευση (matching) της πιστοποίησης.

Οι εντολές για τη διμόρφωση μιας διπλής κατεύθυνσης CHAP πιστοποίησης είναι οι παρακάτω:

```
Router(config)# hostname your_router's_hostname
Router(config)# username remote_hostname
password matching_password
Router(config)# interface type [slot_#/]port_#
Router(config-if)# encapsulation ppp
Router(config-if)# ppp authentication chap
```

15.2 Επαλήθευση, Εύρεση Λαθών Πιστοποίησης (Troubleshooting Authentication).

Οι βασικές εντολές είναι show interface και debug.

```
Router# show interfaces serial 0
Serial0 is up, line protocol is down
Hardware is MCI Serial
Internet address is 192.168.1.2 255.255.255.0
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 254/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
lcp state = ACKRCVD
ncp ccp state = NOT NEGOTIATED ncp ipcp state = CLOSED
ncp osicp state = NOT NEGOTIATED ncp ipxcp state = NOT NEGOTIATED
ncp xnscp state = NOT NEGOTIATED ncp vinescp state = NOT NEGOTIATED
ncp deccp state = NOT NEGOTIATED ncp bridgecp state = NOT NEGOTIATED
ncp atalkcp state = NOT NEGOTIATED ncp lex state = NOT NEGOTIATED
ncp cdp state = CLOSED
Last input 0:00:01, output 0:00:01, output hang never
<--output omitted-->
```

Στο παράδειγμα το lcp state = CLOSED, όπως επίσης και η κατάσταση των IP και CDP. Υπήρξε, λοιπόν , ένα πρόβλημα στην αποκατάσταση της σύνδεσης. Το πρόβλημα ήταν ότι οι κωδικόι των δύο δρομολογητών δεν ήταν ίδιοι. Αλλά αυτό δεν είναι εμφανές με αυτή την εντολή. Για να προσδιοριστεί το σφάλμα πρέπει να εκτελέσουμε την debug εντολή:

```
RouterA# debug ppp authentication
%LINK-3-UPDOWN: Interface Serial0, changed state to up
Se0 PPP: Treating connection as a dedicated line
Se0 PPP: Phase is AUTHENTICATING, by both
Se0 CHAP: O CHALLENGE id 2 len 28 from "RouterA"
Se0 CHAP: I CHALLENGE id 3 len 28 from "RouterB"
Se0 CHAP: O RESPONSE id 3 len 28 from "RouterA"
Se0 CHAP: I RESPONSE id 2 len 28 from "RouterB"
Se0 CHAP: O SUCCESS id 2 len 4
Se0 CHAP: I SUCCESS id 3 len 4
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state
to up
```

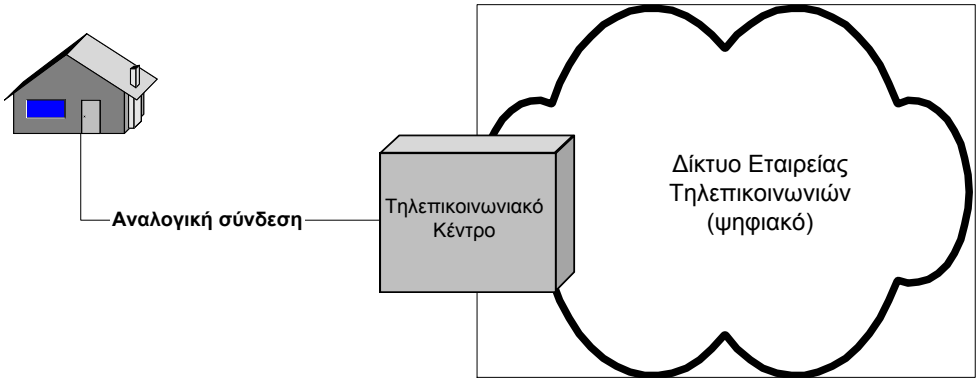
Στο παραπάνω παράδειγμα οι δύο δρομολογητές χρησιμοποιούν CHAP. Το I και το O που ακολουθούν το Se0 δείχνουν την κατεύθυνση (input, output). Παρακάτω είναι ένα παράδειγμα με PAP:

```
RouterA# debug ppp authentication
%LINK-3-UPDOWN: Interface Serial0, changed state to up
Se0 PPP: Treating connection as a dedicated line
Se0 PPP: Phase is AUTHENTICATING, by both
Se0 PAP: O AUTH-REQ id 2 len 18 from "RouterA"
Se0 PAP: I AUTH-REQ id 3 len 18 from "RouterB"
Se0 PAP: Authenticating peer RouterB
Se0 PAP: O AUTH-ACK id 2 len 5
Se0 PAP: I AUTH-ACK id 3 len 5
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state
to up
```

16. Δίκτυα ISDN

Με τον όρο ISDN προσδιορίζουμε ένα σύνολο από τεχνολογίες δικτύου που παρέχουν σύνδεση μεταξύ δύο άκρων και μπορούν να ολοκληρώσουν σε ένα ενιαίο πακέτο ένα σύνολο υπηρεσιών που περιλαμβάνουν τόσο υπηρεσίες φωνής όσο και δεδομένων.
Το ISDN επιτρέπει την ταυτόχρονη λειτουργία πολλαπλών ψηφιακών καναλιών μέσω της ίδιας τηλεφωνικής καλωδίωσης που χρησιμοποιούν και οι κλασικές, αναλογικές γραμμές. Η βασική διαφορά εδώ είναι ότι στο ISDN το σήμα μεταδίδεται ψηφιακά και όχι αναλογικά. Η υστέρηση σε γραμμές ISDN είναι πολύ μικρότερη αυτής των αναλογικών γραμμών.

PSTN και ISDN



Στο κλασικό δίκτυο PSTN, ο αδύναμος κρίκος συνήθως είναι ο τοπικός βρόχος, η σύνδεση δηλαδή μεταξύ συνδρομητή και τηλεπικοινωνιακού κέντρου. Αυτή η σύνδεση είναι αναλογική, κάτι το οποίο συνεπάγεται περιορισμούς ως προς το εύρος ζώνης που μπορεί να επιτευχθεί. Η τεχνολογία δεν επιτρέπει αναλογικό εύρος ζώνης πάνω από περίπου 3000Hz.
Με το ISDN, ο τοπικός βρόχος μπορεί να χρησιμοποιηθεί για τη μετάδοση ψηφιακών δεδομένων, κάτι που βελτιώνει την ταχύτητα αλλά και την αξιοπιστία.
Ο στόχος πίσω από την ανάπτυξη του ISDN ήταν η δημιουργία ενός πλήρως ψηφιακού δικτύου, από άκρη σε άκρη. Αυτό προϋποθέτει ότι η ψηφιοποίηση, αντί να γίνεται στο τηλεφωνικό κέντρο, όπως στο PSTN, θα πρέπει να γίνεται στο σημείο σύνδεσης του χρήστη, έτσι ώστε η μετάδοση μέχρι το κέντρο να γίνεται ψηφιακά.

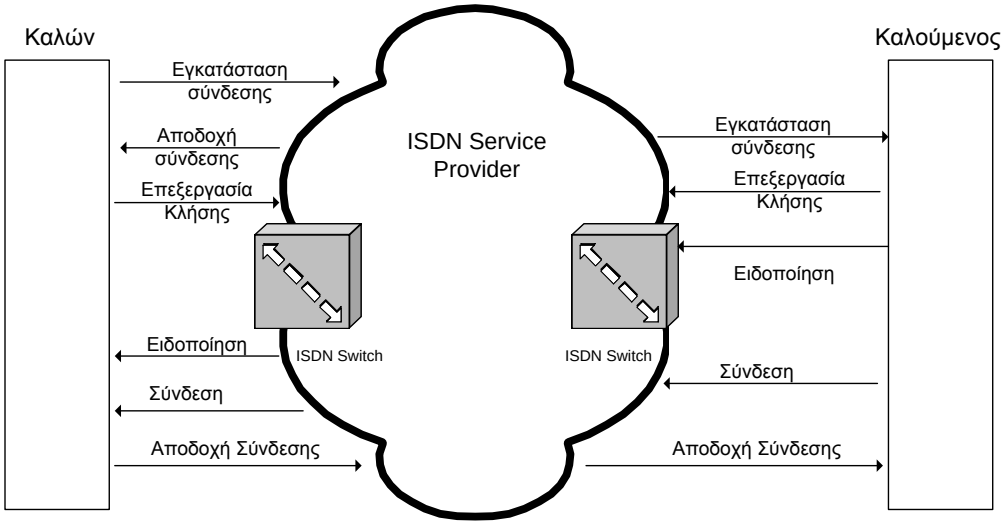
16.1 Πλεονεκτήματα και εγκατάσταση του ISDN

- Μπορεί να μεταφέρει πολλαπλά είδη σήματος (φωνή, εικόνα, δεδομένα)
- Προσφέρει πολύ ταχύτερο χρόνο σύνδεσης σε σχέση συνδέσεις αναλογικού modem
- Προσφέρει ταχύτερο ρυθμό μεταφοράς από τις απλές τηλεφωνικές συνδέσεις
- Είναι κατάλληλο για συνδέσεις PPP

Το ISDN χρησιμοποιεί σηματοδοσία εκτός ζώνης πάνω από το κανάλι D προκειμένου να εγκατασταθεί μια σύνδεση.
Το ISDN χρησιμοποιεί δύο τύπους καναλιών, ο καθένας με διαφορετικό ρυθμό μετάδοσης. Το φέρον κανάλι (κανάλι B) είναι ένας καθαρός δίαυλος 64Kbps. Ονομάζεται καθαρό γιατί μπορεί να χρησιμοποιηθεί για τη μετάδοση οποιουδήποτε τύπου δεδομένων σε full duplex mode.
Σε αντίθεση π.χ. με μια σύνδεση TCP/IP όπου η πληροφορία ελέγχου και τα δεδομένα μεταδίδονται πάνω από το ίδιο κανάλι, στο ISDN όλη η πληροφορία ελέγχου περνά πάνω από το D-channel, το οποίο διαχωρίζεται εντελώς από το κανάλι από όπου περνούν τα δεδομένα. Η μέθοδος αυτή ονομάζεται out-of-band signaling.
Ο δεύτερος τύπος καναλιού ονομάζεται κανάλι Δ (D-channel). Το D channel ανάλογα με την περίπτωση (BRI ή PRI) μπορεί να είναι 16 ή 64 Kbps και χρησιμοποιείται προκειμένου να μεταφέρει πληροφορία ελέγχου για τα B-κανάλια.
Υπάρχουν δυο μορφές ISDN, η BRI (Basic Rate Interface) και η PRI (Primary Rate Interface). Οι BRI

συνδέσεις χρησιμοποιούν 2 B-channels των 64Kbps και ένα D-channel των 16 Kbps. (γι'αυτό και ονομάζεται επίσης 2B+D).
Οι PRI συνδέσεις διαφέρουν ανάλογα με την περιοχή. Στην Ιαπωνία και την Β. Αμερική, οι PRI συνδέσεις προσφέρουν 23 B κανάλια των 64 Kbps και ένα D κανάλι επίσης των 64 Kbps. Στην Ευρώπη, οι PRI συνδέσεις δίνουν 30 B και ένα D κανάλι.
Οι συνδέσεις ISDN είναι Circuit-switched συνδέσεις.

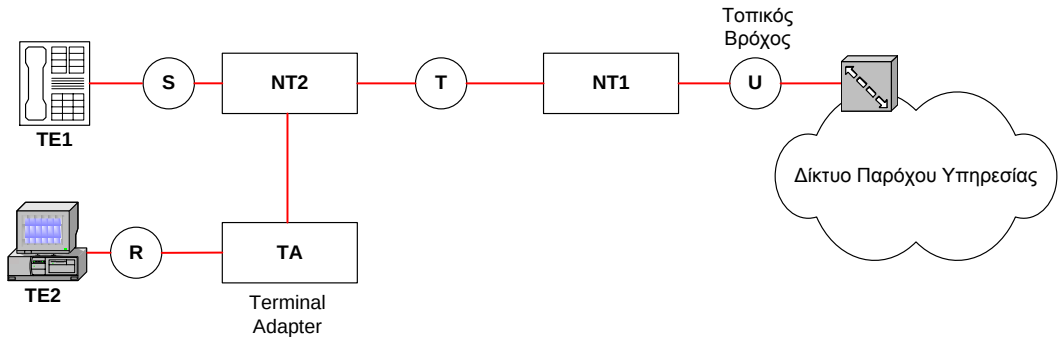
Διαδικασία εγκατάστασης τηλεφωνικής σύνδεσης ISDN σε BRI γραμμή



Προκειμένου να εγκατασταθεί μια σύνδεση ISDN, χρησιμοποιείται το D-channel. Η διαδικασία έχει ως εξής:

1. Ο αριθμός καλούντος αποστέλλεται στο τοπικό ISDN Switch
2. Το τοπικό Switch χρησιμοποιεί το πρωτόκολλο SS7 και εγκαθιστά μια σύνδεση με το απομακρυσμένο ISDN Switch.
3. Το απομακρυσμένο ISDN Switch χρησιμοποιεί το D-Channel για να επικοινωνήσει με το λήπτη.
4. Η τερματική συσκευή του λήπτη (NT1) στέλνει ένα μήνυμα call-connect στο απομακρυσμένο switch.
5. Το απομακρυσμένο switch στέλνει στο τοπικό switch το μήνυμα call-connect.
6. Το τοπικό switch συνδέει ένα Β-κανάλι από άκρη σε άκρη, αφήνοντας το άλλο κανάλι ελεύθερο για μια νέα σύνδεση. Εάν χρειάζεται, και τα δυο Β-κανάλια μπορούν να αξιοποιηθούν για την ίδια σύνδεση (αυξάνοντας το bandwidth).

Η επικοινωνία αυτή είναι εφικτή με τη χρήση των πρωτοκόλλων Q.921/Q.931.



Σημεία αναφοράς σε μια σύνδεση ISDN
TE1: Υποδηλώνει τερματικό εξοπλισμό ISDN (π.χ ISDN τηλέφωνο, ISDN router)
TE2: Υποδηλώνει τερματική συσκευή μη-ISDN, η οποία απαιτεί TA προκειμένου να συνδεθεί στο ISDN δίκτυο
NT2: Συσκευή που συγκεντρώνει τα σήματα όλων των ISDN TE1 συσκευών και όλων των TA's και τα προωθεί στην NT1
NT1: Συσκευή που συνδέεται απευθείας στο δίκτυο του provider. Μετατρέπει τα σήματα των συσκευών που βρίσκονται συνδεδεμένα στο NT2 σε μορφή κατάλληλη για μετάδοση πάνω από τη δισύρματη ψηφιακή ISDN γραμμή που παρέχει ο Provider.

Το γνωστό μας netmod, που παρέχεται από τον ΟΤΕ στους ISDN καταναλωτές του συνδυάζει τις λειτουργίες του TA, του NT2 και του NT1.
Στο παραπάνω διάγραμμα μπορούμε να διακρίνουμε τέσσερις διαφορετικούς τύπους συνδέσεων:

- R: αναφέρεται στη σύνδεση μεταξύ TA και μη-ISDN συσκευών (TE2), όπως για παράδειγμα μια RS 232 σύνδεση.
- S: Αναφέρεται σε συνδέσεις μεταξύ ISDN συσκευών και NT2.
- T: Με ίδια ηλεκτρικά χαρακτηριστικά όπως η S, αναφέρεται στη σύνδεση μεταξύ NT2 και NT1
- U: Σύνδεση από το NT1 έως το τοπικό switch του internet provider.

Συχνά οι S και T αναφέρονται μαζί, ως S/T συνδέσεις.

16.2 Ρύθμιση ενός ISDN router

Α) BRI σύνδεση

Interface bri module/port

Π.χ.

Interface bri0/0

Κατόπιν ρυθμίζουμε τον τύπο του switch εισάγοντας την εντολή isdn από global ή interface configuration mode.

Router(config)#**isdn switch-type** *switch-type*

Η παράμετρος switch type αναφέρεται στον τύπο switch που χρησιμοποιεί ο service provider. Αυτή η παράμετρος έχει σημασία, καθώς υπάρχουν πολλές διαφορετικές υλοποιήσεις των πρωτοκόλλων ISDN καθεμία με τα δικά της χαρακτηριστικά.

Συγκεντρωτικό παράδειγμα:

```
Router(config)#interface bri0/0
Router(config-if)#isdn switch-type basic-net3
Router(config-if)#no shutdown
```

Β) PRI ISDN

Οι συνδέσεις PRI στην Ευρώπη παραδίδονται σαν μια γραμμή E1. Πριν εκτελεστούν οι εντολές ρύθμισης ενός ISDN PRI router interface θα πρέπει:

1. Να καθοριστεί ο τύπος του switch που χρησιμοποιεί ο internet provider
2. Να καθοριστεί ο controller, ο τύπος framing και η κωδικοποίηση γραμμής
3. Να οριστεί ένα PRI Group Timeslot για τη γραμμή E1 και να οριστεί η ταχύτητα.

Καθώς χρησιμοποιούμε γραμμές E1, στην περίπτωση του PRI δεν υπάρχει η αντίστοιχη «interface pri» εντολή, όπως στο BRI ISDN. Αντίθετα, το φυσικό interface του router όπου συνδέεται η E1 γραμμή, ονομάζεται E1 controller και πρέπει να καθοριστεί ανεξάρτητα προκειμένου να μπορέσουμε να

επικοινωνήσουμε με τον provider. Τα κανάλια D και B ρυθμίζονται ανεξάρτητα από τον controller με τη χρήση της εντολής interface serial.
Αρχικά, ορίζουμε τον τύπο switch π.χ.

```
Router(config)#isdn switch-type primary-net5
```

Η ρύθμιση του controller γίνεται σε τέσσερα στάδια:
Α) ρύθμιση του controller και του slot/port όπου βρίσκεται η PRI card.

```
Router(config)#controller e1 0/0
```

Β) Ρύθμιση του framing, line coding και του χρονισμού.

```
Router(config-controller)#framing  crc4
Router(config-controller)#linecode hdb3
```

Router(config-controller)#**pri-group** [**timeslots***range*]

Π.χ.

```
Router(config-controller)#pri-group [1-31]
```

Κατόπιν ορίζουμε ένα από τα interfaces για λειτουργία D-channel. Αυτό το interface θα είναι ένα serial interface στο router για E1 σύνδεση:

```
Router(config)#interface serial{slot/port: | unit:}{23 | 15}
```

Π.χ. interface serial 0/0:15 (ορίζει το κανάλι 16 σαν D channel)

Η επαλήθευση της λειτουργίας μιας ISDN σύνδεσης γίνεται με τις εντολές

```
Show isdn status (πληροφορίες για την κατάσταση όλων των bri
interfaces)
Show interface bri0/0 (πληροφορίες για το int bri0/0)
Show isdn active (πληροφορίες για τρέχουσα ISDN κλήση)
```