

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ



ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ
ΔΙΚΤΥΩΝ ΜΕ
ΧΡΗΣΗ CISCO SOFTWARE

ΠΑΝΑΓΗ ΧΡΙΣΤΟΣ

21043

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΔΗΜΗΤΡΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ

ΑΘΗΝΑ 2016

ΠΕΡΙΕΧΟΜΕΝΑ

ΜΕΡΟΣ Α

1. Εισαγωγή

A. Κίνητρο και Σκοπός Εργασίας	4
B. Δομή.....	4

2. Προεπισκόπηση Δικτύων

A. LAN, WAN.....	5
B. Internet, Intranet, Extranet.....	6
Γ. Client and server, Peer to peer.....	7
Δ. Στοιχεία ενός Δικτύου.....	8
E. Πρωτόκολλα δικτύων.....	11
ΣΤ. Επίπεδα επικοινωνίας (Layers, TCP/IP & OSI Model).....	16

3. Φυσικό Επίπεδο (Physical layer)

A. Καλώδια από χαλκό.....	17
B. Οπτικές Ίνες.....	20
Γ. Ασύρματη επικοινωνία.....	22
Δ. Πλήμνη (Hub).....	27

4. Επίπεδο Συνδέσμου (Link Layer)

A. Τοπολογίες.....	28
B. Frame.....	30
Γ. Mac Address.....	34
Δ. Μεταγωγείς (Switches).....	35
E. Switch Configuration.....	36

5. Επίπεδο Δικτύου

A. Πρωτόκολλο IP.....	39
B. IPV4.....	40
Γ. IPV6.....	45
Δ. Δρομολόγηση, Routers.....	49
E. Router Configuration.....	51

6. Επίπεδο Μεταφοράς (Transport Layer)

A. Transport Layer.....	54
B. TCP, UDP, Port Numbers.....	57

7. Επίπεδο Εφαρμογών (Application Layer)

A. Application, Presentation Session Layers.....	72
B. Συνήθη Πρωτόκολλα Εφαρμογών.....	73

ΜΕΡΟΣ Β

A. Cisco Packet Tracer (CPT).....	84
B.Υλοποίηση εικονικού δικτύου.....	85

Επίλογος.....	92
---------------	----

Βιβλιογραφία.....	94
-------------------	----

1. Εισαγωγή

Α. Κίνητρο και Σκοπός Εργασίας

Ο σκοπός της παρούσας εργασίας είναι η ανάλυση της λειτουργίας των δικτύων και η υλοποίηση ενός δικτύου με την χρήση ενός προσομοιωτή. Επέλεξα να ασχοληθώ με αυτό το θέμα, γιατί το βρίσκω πολύ ενδιαφέρον και γιατί πλέον τα δίκτυα έχουν μπει για τα καλά στη ζωή μας. Βρίσκονται στην καθημερινότητα μας, όπως για παράδειγμα στο ίδιο μας το σπίτι, σε εστιατόρια και στο χώρο εργασίας μας. Επίσης ακόμη ένας λόγος ήταν να εμπλουτίσω τις γνώσεις μου σε αυτό τον τομέα, γιατί θα ήθελα να ασχοληθώ περισσότερο στο μέλλον. Πιστεύω ότι η έρευνα που έχω κάνει με βοήθησε αρκετά και ελπίζω να βοηθήσει το ίδιο και τους αναγνώστες.

Β. Δομή

Η εργασία χωρίζεται σε δυο μέρη. Στο πρώτο μέρος γίνεται μια βιβλιογραφική ανασκόπηση για τα δίκτυα και αναλύονται τα επτά επίπεδα από τα οποία αποτελείται το μοντέλο OSI.

Στο δεύτερο μέρος της εργασίας ασχολήθηκα με τη δημιουργία ενός εικονικού δικτύου μιας επιχείρησης χρησιμοποιώντας ένα προσομοιωτή δικτύων. Έγιναν όλες οι απαραίτητες ρυθμίσεις στις συσκευές ούτως ώστε να μπορούν να επικοινωνούν μεταξύ τους. Έτσι καταφέραμε να δημιουργήσουμε ένα δίκτυο το οποίο μπορεί να εξυπηρετήσει τις ανάγκες της επιχείρησης.

2. Προεπισκόπηση Δικτύων

A. LAN, WAN

Τοπικά Δίκτυα (LAN)

Τα τοπικά δίκτυα είναι η υποδομή που καλύπτει μια μικρή περιοχή. Ειδικά χαρακτηριστικά της LANs:

- Διασύνδεση συσκευών σε μια περιορισμένη περιοχή, όπως ένα σπίτι, ένα σχολείο, ένα κτίριο ή μία πανεπιστημιούπολη.
- Ένα LAN συνήθως χρησιμοποιείται από ένα μόνο οργανισμό ή άτομο. Ο διοικητικός έλεγχος που διέπει τις πολιτικές ασφαλείας και ελέγχου πρόσβασης επιβάλλονται σε επίπεδο δικτύου.
- Τα τοπικά δίκτυα παρέχουν υψηλού εύρους ζώνης ταχύτητας σε εσωτερικές τερματικές και ενδιάμεσες συσκευές.

Wide Area Networks(WAN)

WANs είναι μια υποδομή δικτύου που καλύπτει μια ευρεία περιοχή. Τα WANs συνήθως διαχειρίζονται από τους παρόχους υπηρεσιών (SP) ή παρόχους υπηρεσιών Διαδικτύου (ISP).

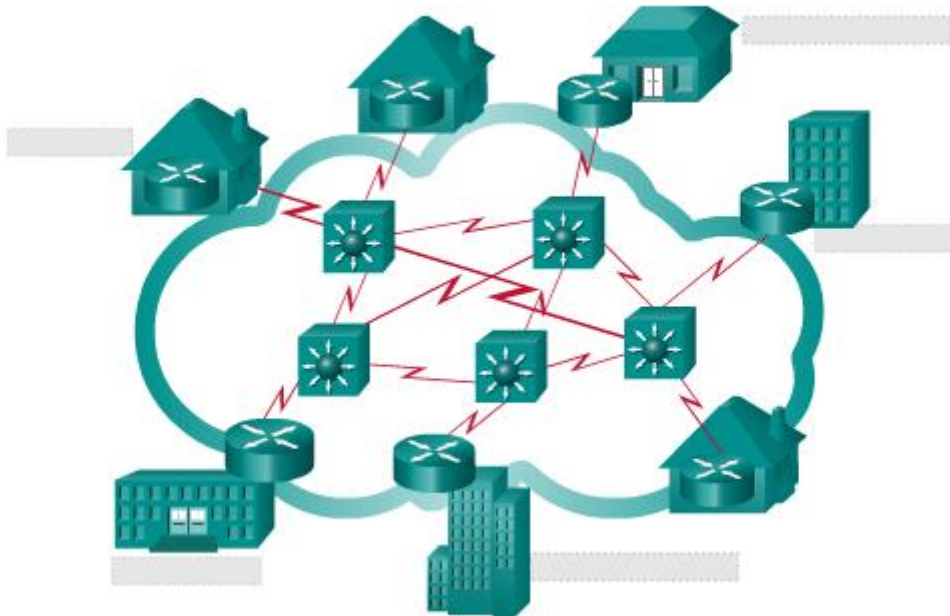
Ειδικά χαρακτηριστικά WANs:

- Διασύνδεση τοπικών δικτύων σε μεγάλες γεωγραφικές περιοχές, όπως μεταξύ των πόλεων, κρατών, επαρχίες, χώρες ή ηπείρους.
- Τα WANs συνήθως χορηγούνται από πολλούς φορείς παροχής υπηρεσιών.
- Τα WANs παρέχουν συνήθως πιο αργή σύνδεση μεταξύ LANs.

Άλλοι τύποι δικτύων:

- Metropolitan Area Network (MAN) - Μια υποδομή δικτύου που εκτείνεται σε ένα φυσικό χώρο μεγαλύτερο από ένα LAN, αλλά μικρότερο από ένα WAN (π.χ. μια πόλη).
- Ασύρματο LAN (WLAN) - Παρόμοια με ένα LAN αλλά διασυνδέει ασύρματα τους χρήστες και τα τελικά σημεία σε μια μικρή γεωγραφική περιοχή.
- Storage Area Network (SAN) - Μια δικτυακή υποδομή σχεδιασμένη για να υποστηρίζει τους διακομιστές αρχείων και να παρέχει την αποθήκευση δεδομένων, την ανάκτηση, και την αναπαραγωγή.

B. Internet, Intranet, Extranet



Το Διαδίκτυο είναι μια παγκόσμια συλλογή διασυνδεδεμένων δικτύων. Η εικόνα δείχνει το Διαδίκτυο ως μια συλλογή των διασυνδεδεμένων δικτύων LAN και WANs. Τα LANs είναι συνδεδεμένα μεταξύ τους μέσω σύνδεσης WAN. Τα WANs κατόπιν συνδέονται μεταξύ τους. Οι κόκκινες γραμμές σύνδεσης WAN αντιπροσωπεύουν όλους τους τρόπους που συνδέουν δίκτυα (χάλκινων καλωδίων, καλωδίων οπτικών ινών, και ασύρματης μετάδοσης).

Μέσω του Διαδικτύου μπορούν να δημιουργηθούν δύο κατηγορίες συνδέσεων. Τα:

- Intranet
- Extranet

Intranet είναι ένας όρος που χρησιμοποιείται συχνά όταν αναφερόμαστε σε μια ιδιωτική σύνδεση τοπικών δικτύων και WANs που ανήκει σε έναν οργανισμό, και έχει σχεδιαστεί ώστε να είναι προσβάσιμη μόνο από τα μέλη του οργανισμού, τους εργαζόμενους, ή άλλα άτομα με άδεια.

Η επέκταση προσβασιμότητας στο δίκτυο αλλά με μειωμένα δικαιώματα χρήσης μετατρέπει το δίκτυο σε extranet. Μερικά παραδείγματα είναι:

-Μια εταιρεία που παρέχει πρόσβαση σε εξωτερικούς προμηθευτές και πελάτες.

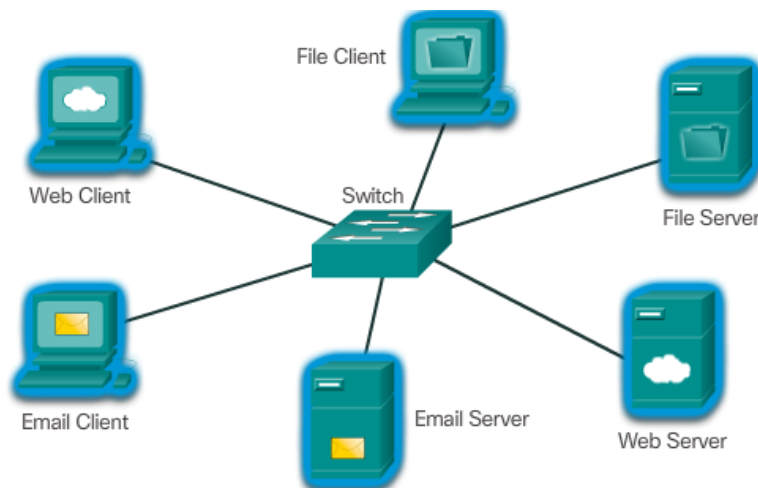
-Ένα νοσοκομείο που παρέχει ένα σύστημα όπου οι ασθενείς να μπορούν να κλείσουν ραντεβού για συγκεκριμένο γιατρό.

Γ. Client and server, Peer to peer

Clients and Servers

Όλοι οι υπολογιστές που είναι συνδεδεμένοι σε ένα δίκτυο και συμμετέχουν άμεσα στην επικοινωνία του δικτύου ταξινομούνται ως πελάτες (clients). Οι πελάτες ονομάζεται επίσης τερματικές συσκευές.

Διακομιστές (Servers) είναι οι υπολογιστές με λογισμικό που τους επιτρέπει να παρέχουν πληροφορίες, όπως το ηλεκτρονικό ταχυδρομείο ή Web σελίδες, στους πελάτες του δικτύου. Κάθε υπηρεσία απαιτεί ξεχωριστό λογισμικό. Για παράδειγμα, ένας διακομιστής απαιτεί λογισμικό Web Server με σκοπό την παροχή υπηρεσιών Web στο δίκτυο. Ένας υπολογιστής με λογισμικό Server μπορεί να παρέχει υπηρεσίες ταυτόχρονα σε ένα ή πολλούς πελάτες. Επιπλέον, σε έναν υπολογιστή μπορεί να τρέξει πολλούς τύπους λογισμικού Server. Σε ένα σπίτι ή μικρή επιχείρηση, μπορεί να είναι απαραίτητο για έναν υπολογιστή να ενεργεί ως file server, έναν Web Server, και ένα email server.



Οι Διακομιστές με το ανάλογο λογισμικό παρέχουν ασφάλεια στο δίκτυο και δίνουν δικαιώματα χρήσης στο κάθε πελάτη ξεχωριστά. Οι πελάτες με το μοναδικό όνομα και κωδικό πρόσβασης στο δίκτυο, ελέγχονται και παίρνουν δικαιώματα χρήσης του δικτύου από τον διακομιστή.

Για παράδειγμα θα μπορούσαμε να πούμε ότι κάποιοι χρήστες του δικτύου (πελάτες μπορούν να έχουν πρόσβαση στο διαδίκτυο και κάποιοι όχι, κάποιοι χρήστες μπορούν να στέλνουν email και κάποιοι όχι.

Peer-to-Peer

Μια απλή μορφή δικτύου είναι όταν όλες οι συσκευές που είναι συνδεδεμένες σε αυτό έχουν τα ίδια δικαιώματα. Δεν υπάρχει δηλαδή έλεγχος από κανένα σε κανένα. Αυτά τα είδη δικτύων ονομάζονται Peer to Peer. Η ουσιαστική διαφορά τους από τα δίκτυα Client and

Server είναι το λογισμικό που τρέχει στους υπολογιστές του δικτύου. Το λογισμικό πελάτη και διακομιστή τρέχει συνήθως σε διαφορετικούς υπολογιστές, αλλά ένας υπολογιστής μπορεί να πραγματοποιήσει και τους δύο ρόλους ταυτόχρονα. Σε μικρές επιχειρήσεις και σπίτια, πολλοί υπολογιστές λειτουργούν ως διακομιστές και πελάτες στο δίκτυο.

Τα πλεονεκτήματα του peer-to-peer δικτύου είναι:

- Εύκολο στην εγκατάσταση.
- Λιγότερη πολυπλοκότητα.
- Μπορούν να χρησιμοποιηθούν για απλές εργασίες, όπως στην μεταφορά αρχείων και την κοινή χρήση εκτυπωτών.



Τα μειονεκτήματα της peer-to-peer δίκτυα:

- Δεν είναι τόσο ασφαλές.
- Δεν είναι επεκτάσιμο.
- Όλες οι συσκευές μπορούν να ενεργούν ως πελάτες και εξυπηρετητές και αυτό μπορεί να επιβραδύνει την απόδοσή τους.

Δ. Στοιχεία ενός Δικτύου

Η διαδρομή που ακολουθεί ένα μήνυμα από την πηγή στον προορισμό μπορεί να είναι τόσο απλό όσο ένα καλώδιο που συνδέει έναν υπολογιστή σε έναν άλλο, ή τόσο σύνθετο όσο μια συλλογή δικτύων που εκτείνεται στον κόσμο. Η υποδομή του δικτύου παρέχει ένα σταθερό και αξιόπιστο κανάλι μέσω του οποίου γίνονται αυτές οι επικοινωνίες.

Η υποδομή του δικτύου περιλαμβάνει τρεις κατηγορίες στοιχείων δικτύου:

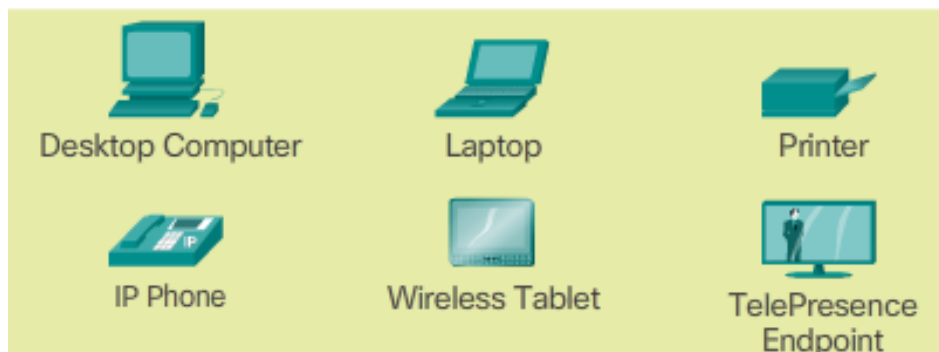
- Συσκευές
- Μέσα Μετάδοσης
- Υπηρεσίες

Οι συσκευές και τα μέσα μετάδοσης είναι τα φυσικά στοιχεία του δικτύου (Hardware) είναι συχνά τα ορατά στοιχεία του δικτύου, όπως laptop, PC, switch, router, ασύρματα σημεία πρόσβασης, ή η καλωδίωση που χρησιμοποιείται για τη σύνδεση των συσκευών.

Οι υπηρεσίες περιλαμβάνουν πολλές εφαρμογές, όπως το ηλεκτρονικό ταχυδρομείο, υπηρεσίες φιλοξενίας και υπηρεσίες web hosting, τις οποίες οι άνθρωποι χρησιμοποιούν καθημερινά. Οι διεργασίες παρέχουν τη λειτουργικότητα και μετάδοση μηνυμάτων μέσω του δικτύου. Οι διαδικασίες είναι λιγότερο προφανές για εμάς, αλλά είναι ζωτικής σημασίας για τη λειτουργία των δικτύων.

Συσκευές (Τελικές ή Τερματικές End Devices)

Τερματικές συσκευές ονομάζονται οι συσκευές δικτύου με τις οποίες οι άνθρωποι είναι πιο εξοικειωμένοι. Μερικά παραδείγματα των τελικών συσκευών φαίνεται στη παρακάτω εικόνα

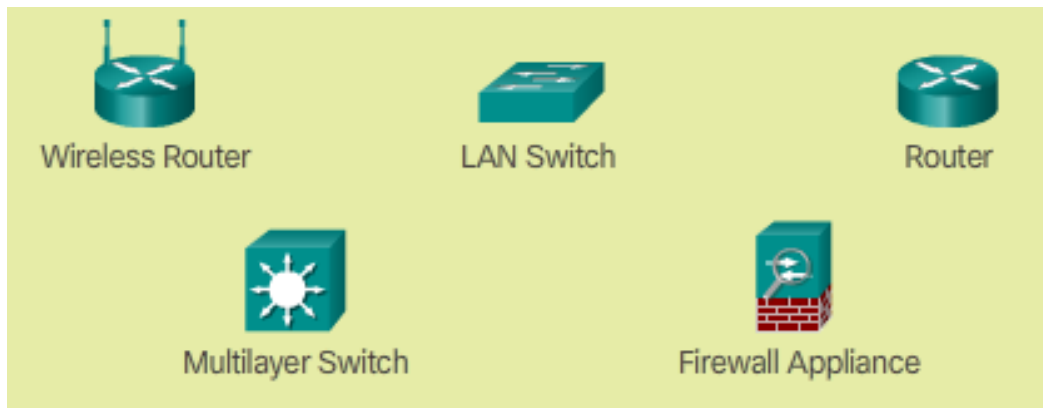


Μια συσκευή είναι είτε η πηγή ή ο προορισμός ενός μηνύματος που μεταδίδεται μέσω του δικτύου. Για να ξεχωρίσει μια συσκευή από άλλη, κάθε μια, προσδιορίζεται από μια διεύθυνση. Όταν μια τελική συσκευή ξεκινά επικοινωνία, χρησιμοποιεί τη διεύθυνση του τελικού προορισμού της συσκευής για να καθορίσει πού θα πρέπει να σταλεί το μήνυμα.

Ενδιάμεσες συσκευές (Intermediary Devices)

Οι ενδιάμεσες συσκευές συνδέουν τις τελικές συσκευές στο δίκτυο και μπορούν να συνδέσουν πολλά επιμέρους δίκτυα για να σχηματίσουν ένα internetwork. Αυτές οι ενδιάμεσες συσκευές παρέχουν συνδεσιμότητα και διασφαλίζουν τις ροές δεδομένων σε όλο το δίκτυο.

Οι ενδιάμεσες συσκευές χρησιμοποιούν τη διεύθυνση συσκευής τελικού προορισμού, σε συνδυασμό με πληροφορίες σχετικά με τις διασυνδέσεις του δικτύου, για να καθοριστεί η πορεία που πρέπει να ακολουθήσουν τα μηνύματα μέσω του δικτύου. Παραδείγματα από τις πιο κοινές ενδιάμεσες συσκευές φαίνονται στην πιο κάτω εικόνα.



Network Media

Η επικοινωνίας σε ένα δίκτυο πραγματοποιείται σε ένα μέσο. Το μέσο παρέχει το κανάλι μέσω του οποίου το μήνυμα ταξιδεύει από την πηγή στον προορισμό.

Τα σύγχρονα δίκτυα χρησιμοποιούν κυρίως τρεις τύπους μέσων για τη διασύνδεση συσκευών και παρέχουν το μονοπάτι πάνω στο οποίο μπορούν να μεταδοθούν δεδομένα.

1. μεταλλικά καλώδια (Cooper) - τα δεδομένα είναι κωδικοποιημένα σε ηλεκτρικούς παλμούς
2. καλώδιο οπτικών ινών (Fiber Optic)- τα δεδομένα κωδικοποιούνται ως παλμοί φωτός
3. ασύρματη μετάδοση (Wireless) - τα δεδομένα κωδικοποιούνται χρησιμοποιώντας μήκη κύματος από το ηλεκτρομαγνητικό φάσμα



Ε. Πρωτόκολλα δικτύων

Στις μέρες η χρήση των δικτύων γίνεται όλο και πιο απαραίτητη και πιο πολύπλοκη με τις νέες υπηρεσίες αναπτύσσονται καθημερινά. Οι άνθρωποι επικοινωνούν online από παντού.

Η τεχνολογία του δικτύου στο σύνολό της έχει υιοθετήσει ένα αναπτυξιακό πλαίσιο που επιτρέπει στους σχεδιαστές να κατανοήσουν τις τρέχουσες πλατφόρμες του δικτύου και τη διατήρησή τους. Ταυτόχρονα, το πλαίσιο αυτό χρησιμοποιείται για να διευκολύνει την ανάπτυξη νέων τεχνολογιών για την υποστήριξη των αναγκών και τη βελτίωση της τεχνολογίας αυτής.

Βασικές αρχές της επικοινωνίας (Communication Fundamentals)

Ένα δίκτυο μπορεί να είναι τόσο περίπλοκο όσο οι συσκευές που συνδέονται μέσω του Internet, ή τόσο απλό όσο δύο υπολογιστές που συνδέονται άμεσα μεταξύ τους με ένα μόνο καλώδιο και οτιδήποτε στο ενδιάμεσο. Τα δίκτυα μπορούν να ποικίλουν σε μέγεθος, σχήμα, και τη λειτουργία. Ωστόσο, αν απλά έχουν μια ενσύρματη ή ασύρματη φυσική σύνδεση μεταξύ των συσκευών δεν είναι αρκετή για να επιτρέψει την επικοινωνία. Για να συμβεί επικοινωνία, οι συσκευές πρέπει να ξέρουν «πώς» να επικοινωνούν.

Οι άνθρωποι επικοινωνούν, χρησιμοποιώντας πολλές μεθόδους. Ωστόσο, ανεξάρτητα από την μέθοδο που χρησιμοποιούν, όλες οι μέθοδοι επικοινωνίας έχουν τρία κοινά στοιχεία. Το πρώτο από αυτά τα στοιχεία είναι η πηγή του μηνύματος, ή ο αποστολέας. Πηγές μηνύματος είναι οι άνθρωποι, ή οι ηλεκτρονικές συσκευές που αποστέλλουν ένα μήνυμα σε άλλα άτομα ή συσκευές. Το δεύτερο στοιχείο της επικοινωνίας είναι ο προορισμός, ή ο δέκτης του μηνύματος. Ο προορισμός λαμβάνει το μήνυμα και το ερμηνεύει. Ένα τρίτο στοιχείο, που ονομάζεται δίαυλος, αποτελείται από το μέσο όπου μεταδίδεται το μήνυμα από την πηγή στον προορισμό.

Η επικοινωνία αρχίζει με ένα μήνυμα ή πληροφορίες που πρέπει να σταλούν από τη πηγή σε έναν προορισμό. Η αποστολή αυτού του μηνύματος, είτε γίνεται πρόσωπο με πρόσωπο επικοινωνία ή μέσω δικτύου, διέπεται από κανόνες που ονομάζονται πρωτόκολλα. Τα πρωτόκολλα αυτά είναι ανάλογα με το είδος της μεθόδου επικοινωνίας που χρησιμοποιείται.

Για παράδειγμα, σκεφτείτε δύο ανθρώπους που επικοινωνούν πρόσωπο με πρόσωπο. Πριν από την επικοινωνία, θα πρέπει να συμφωνήσουν για το πώς θα επικοινωνούν. Αν στην επικοινωνία χρησιμοποιείται η φωνή, θα πρέπει πρώτα να συμφωνήσουν σχετικά με τη γλώσσα. Στη συνέχεια, όταν έχουν ένα μήνυμα για να μοιραστούν, θα πρέπει να είναι σε θέση να διαμορφώσουν το μήνυμα αυτό με έναν τρόπο που να είναι κατανοητό. Για παράδειγμα, αν κάποιος χρησιμοποιεί την αγγλική γλώσσα, αλλά υπάρχει κακή σύνταξη της πρότασης, το μήνυμα μπορεί εύκολα να παρεξηγηθεί. Κάθε ένας από αυτούς τους όρους επικοινωνίας καθορίζεται στα πρωτόκολλα που εφαρμόζονται για την επίτευξη της επικοινωνίας.

Το ίδιο ισχύει και για την επικοινωνία με τον υπολογιστή.

Πολλοί διαφορετικοί κανόνες ή πρωτόκολλα διέπουν όλες τις μεθόδους επικοινωνίας που υπάρχουν σήμερα στον κόσμο.

Πριν από μια επικοινωνία με κάποιον άλλο, τα άτομα πρέπει να χρησιμοποιούν τους καθιερωμένους κανόνες ή συμφωνίες που διέπουν τη συνομιλία. Τα πρωτόκολλα είναι αναγκαία για την αποτελεσματική επικοινωνία. Αυτοί οι κανόνες ή τα πρωτόκολλα πρέπει να ακολουθούνται προκειμένου το μήνυμα να παραδοθεί με επιτυχία και να είναι κατανοητό. Στα πρωτόκολλα πρέπει να λαμβάνονται υπόψη οι ακόλουθες απαιτήσεις:

- Να προσδιορίζονται ο αποστολέας και ο παραλήπτης
- Να χρησιμοποιείται κοινή γλώσσα και γραμματική
- Ταχύτητα και χρονοδιάγραμμα της παράδοσης
- Απαιτήσεις επιβεβαίωσης ή αναγνώρισης

Τα πρωτόκολλα που χρησιμοποιούνται στο δίκτυο επικοινωνιών μοιράζονται πολλά από αυτά τα θεμελιώδη γνωρίσματα. Εκτός από τον εντοπισμό της πηγής και του προορισμού ηλεκτρονικών υπολογιστών και του δικτύου, τα πρωτόκολλα καθορίζουν και τις λεπτομέρειες για το πώς ένα μήνυμα μεταδίδεται σε ένα δίκτυο. Κοινά πρωτόκολλα υπολογιστών περιλαμβάνουν τις πιο πάνω απαιτήσεις.

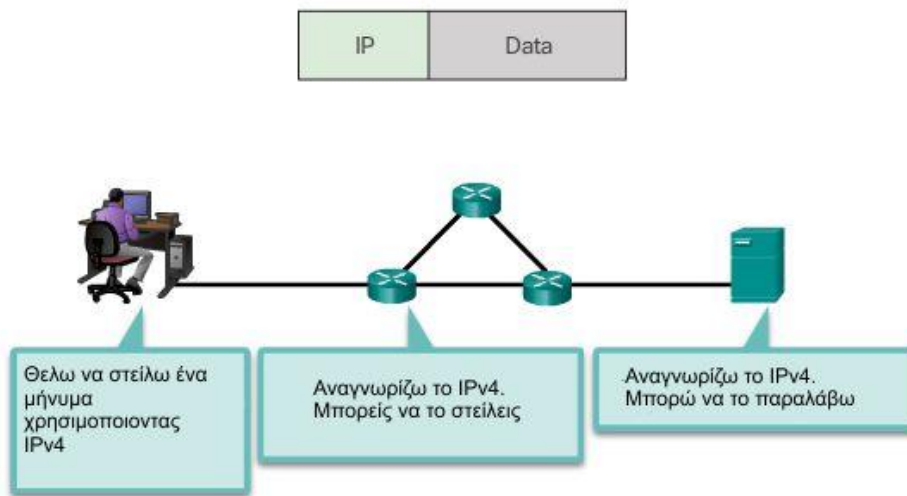
Στο ανθρώπινο επίπεδο, ορισμένοι κανόνες επικοινωνίας είναι τυπικοί και άλλοι είναι απλώς κατανοητοί με βάση την συνήθεια και πρακτική. Για επιτυχή επικοινωνία μεταξύ συσκευών, τα πρωτόκολλα του δικτύου πρέπει να περιγράφουν τις ακριβείς απαιτήσεις και τον τρόπο αλληλεπίδρασης. Τα πρωτόκολλα δικτύωσης καθορίζουν το σύνολο των κανόνων για την ανταλλαγή μηνυμάτων μεταξύ των συσκευών.

Μερικά κοινά πρωτόκολλα δικτύωσης είναι πρωτόκολλο μεταφοράς υπερκειμένου (HTTP), πρωτόκολλο ελέγχου μετάδοσης (TCP) και το πρωτόκολλο Internet (IP).

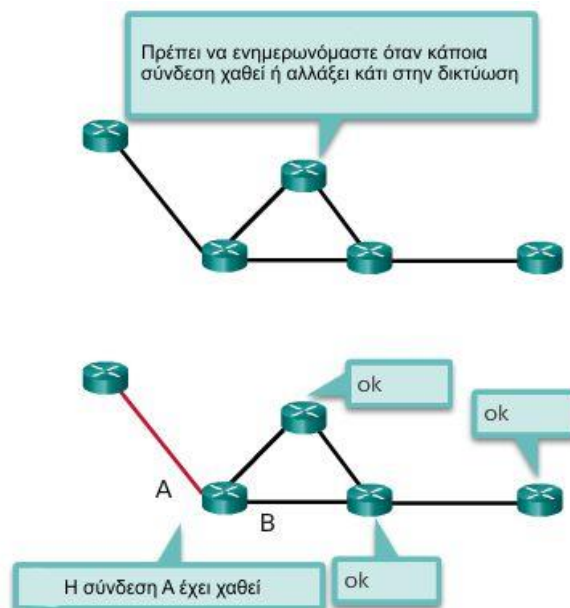
Τα στοιχεία δείχνουν πρωτόκολλα δικτύωσης που περιγράφουν τις ακόλουθες διαδικασίες:

Μερικές διαδικασίες επικοινωνίας φαίνονται πιο κάτω:

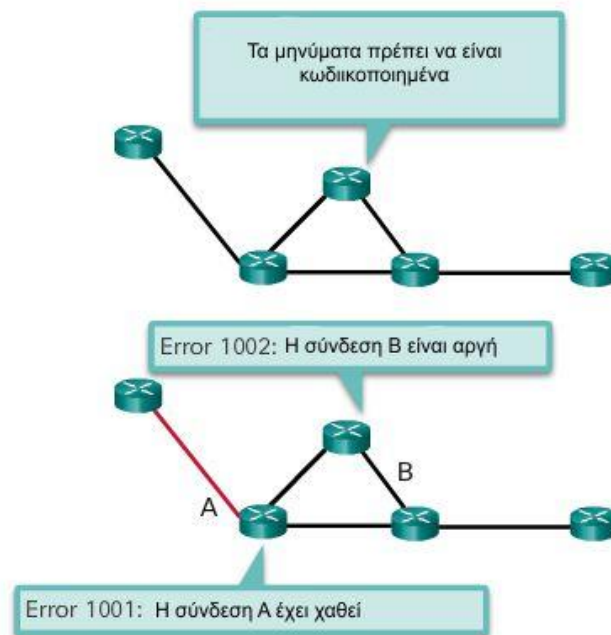
Η Δομή του μηνύματος:



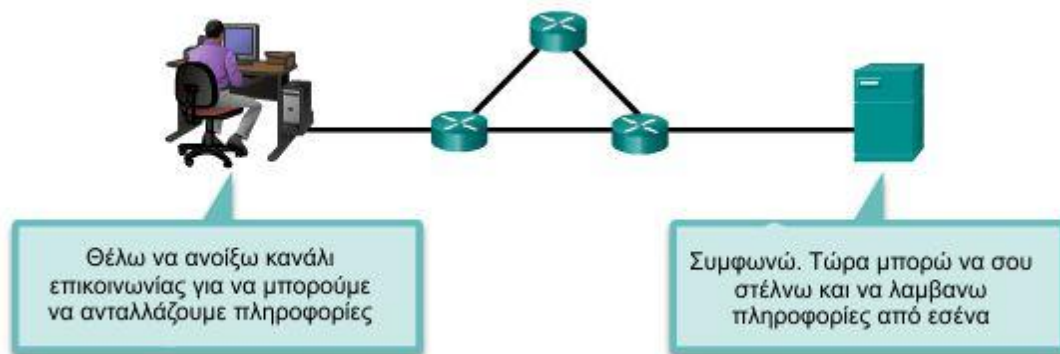
Η διαδικασία με την οποία λειτουργούν οι συσκευές δικτύωσης και μοιράζονται πληροφορίες για μονοπάτια με άλλα δίκτυα:



Ανταλλαγή μηνυμάτων σφάλματος μεταξύ των συσκευών δικτύου:



Η οργάνωση και ο τερματισμός των συνεδριών μεταφορά δεδομένων:



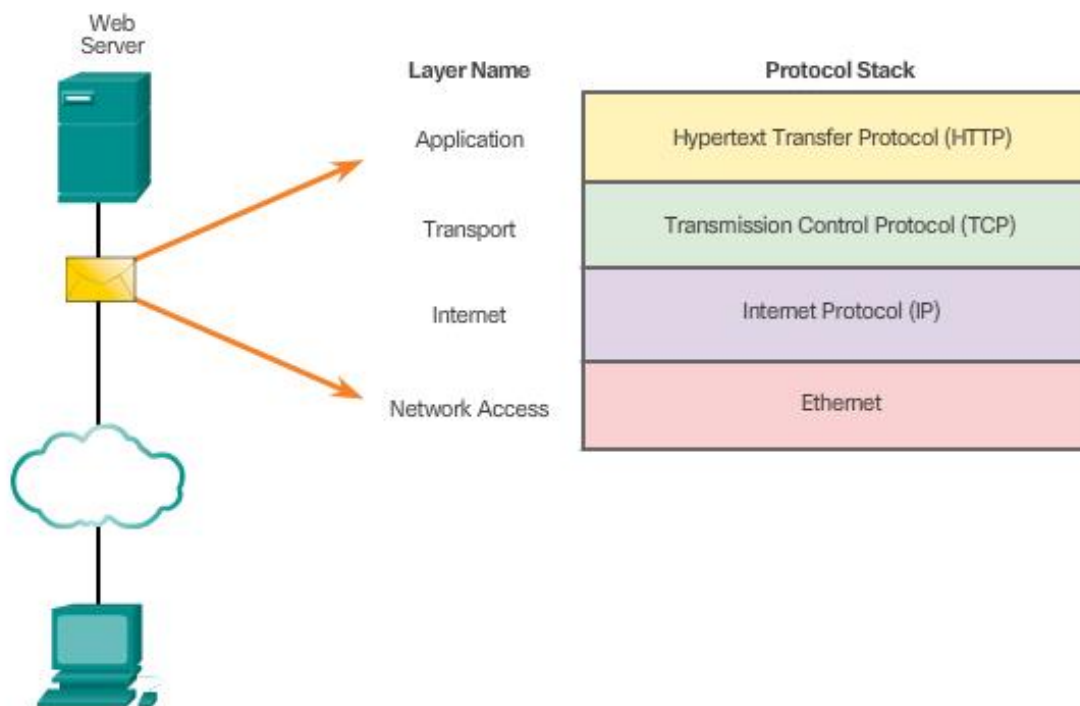
Ένα κλασικό παράδειγμα είναι η επικοινωνία μεταξύ ενός web server και client, η προσπάθεια κάποιου υπολογιστή να ανοίξει μία ιστοσελίδα δηλαδή. Εδώ έχουμε μία αλληλεπίδραση μεταξύ των πιο κάτω πρωτοκόλλων:

HTTP - είναι ένα πρωτόκολλο εφαρμογής που ρυθμίζει τον τρόπο που ένας web server αλληλεπιδρά με ένα client. Το HTTP καθορίζει το περιεχόμενο και τη μορφή των αιτήσεων και των απαντήσεων που ανταλλάσσονται μεταξύ του πελάτη και του διακομιστή. Το HTTP βασίζεται σε άλλα πρωτόκολλα να ρυθμίζουν τον τρόπο που τα μηνύματα μεταφέρονται μεταξύ του πελάτη και του διακομιστή.

TCP - είναι το πρωτόκολλο μεταφοράς. Το TCP χωρίζει τα μηνύματα HTTP σε μικρότερα κομμάτια, που ονομάζονται τμήματα (segments). Τα τμήματα αυτά αποστέλλονται μεταξύ του web server και του client. Το TCP είναι επίσης υπεύθυνο για τον έλεγχο του μεγέθους και της ταχύτητας με την οποία ανταλλάσσονται τα μηνύματα μεταξύ του διακομιστή και του πελάτη.

IP - είναι υπεύθυνο για τη λήψη των τμημάτων από το TCP, ομαδοποιώντας τα σε πακέτα και την επικόλληση σε αυτών των κατάλληλων διευθύνσεων για τη σωστή παράδοση στον προορισμό τους.

Ethernet - είναι ένα πρωτόκολλο δικτύου πρόσβασης που είναι υπεύθυνο για παραλαβή και τη διαμόρφωση των δεδομένων για τη σωστή μεταφορά τους από το ανάλογο μέσο.



ΣΤ. Επίπεδα επικοινωνίας (Layers, TCP/IP & OSI Model)

Η διαδικασία αποστολής και παραλαβής πακέτων κατά τη διάρκεια μιας επικοινωνίας σε ένα δίκτυο, χωρίζεται σε διάφορα επίπεδα. Κατά κύριο λόγο έχουν κυριαρχήσει δύο πολυεπίπεδα μοντέλα. Το TCP/IP και το OSI.



OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	PPP, Frame Relay, Ethernet	Network Access
Physical		

Ένα μοντέλο δικτύωσης είναι μόνο μια αναπαράσταση της λειτουργίας του δικτύου. Το μοντέλο δεν είναι ένα πραγματικό δίκτυο.

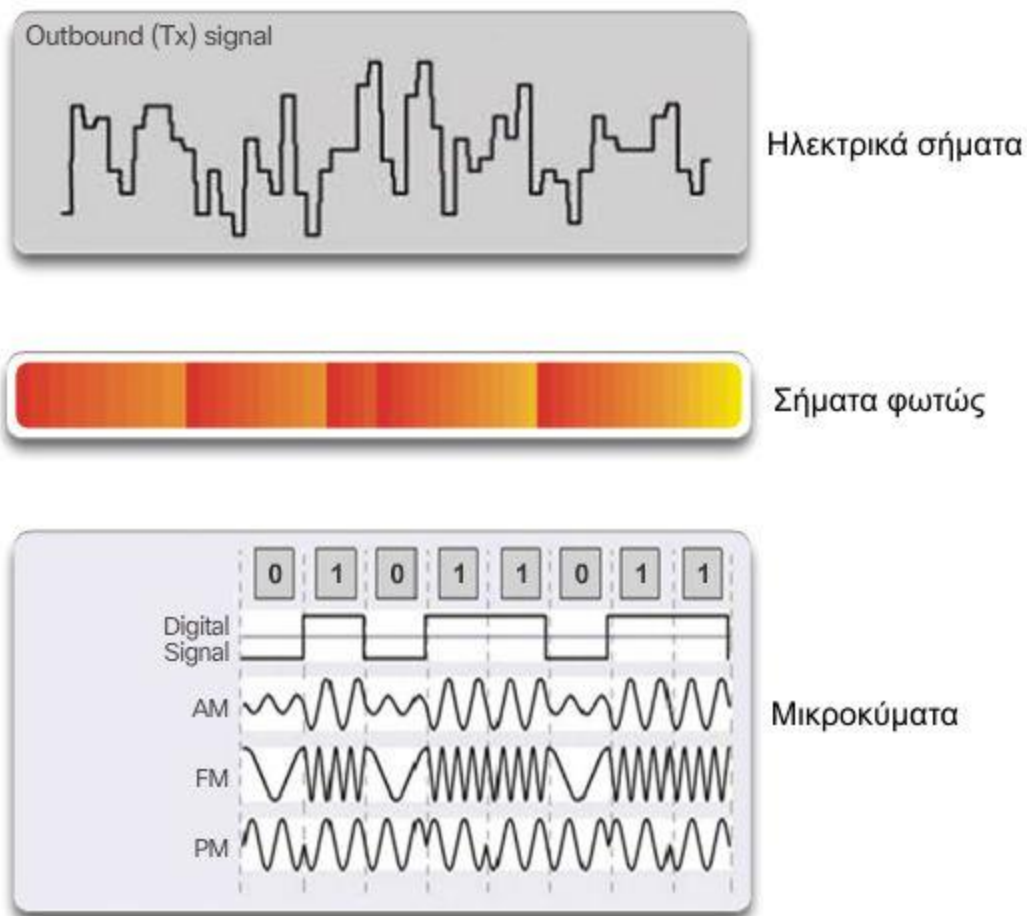
Όπως φαίνεται και στο σχήμα πιο πάνω τα δύο μοντέλα έχουν διαφορετικό αριθμό επιπέδων. Το OSI μοντέλο αποτελείται από 7 επίπεδα. Είναι το μοντέλο πάνω στο οποίο βασίστηκε η δημιουργία των πρωτοκόλλων.

Το TCP/IP μοντέλο σχεδιάστηκε μετά και είναι βασισμένο πάνω στα πρωτόκολλα. Γι' αυτό και τα 4 του επίπεδα περιγράφουν ουσιαστικά τα πρωτόκολλα επικοινωνίας.

3. Φυσικό Επίπεδο (Physical layer)

Το πρώτο (πιο χαμηλό) επίπεδο του μοντέλου OSI είναι το φυσικό. Είναι το επίπεδο που είναι υπεύθυνο για την μεταφορά των bits από μία συσκευή σε μία άλλη μέσα στο δίκτυο.

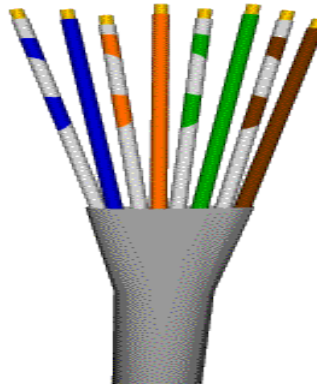
Το φυσικό επίπεδο κωδικοποιεί και σηματοδοτεί τα δεδομένα σε ηλεκτρικό ρεύμα ή φως ή ραδιοκύματα για να μπορέσουν να μεταδοθούν από τα ανάλογα μέσα (χαλκός, οπτικές ίνες ή ασύρματη επικοινωνία) .



A. Καλώδια από χαλκό

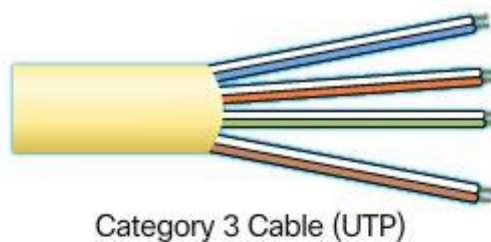
Συνεστραμμένα Ζεύγη Καλωδίων (Twisted Pair)

Το παλαιότερο και πιο συνηθισμένο μέσο μετάδοσης είναι το συνεστραμμένο ζεύγος καλωδίων. Αποτελείται από σύρματα με πυρήνα χαλκού, πάχους ενός περίπου χιλιοστού, τα οποία περιβάλλονται από μονωτικό υλικό.



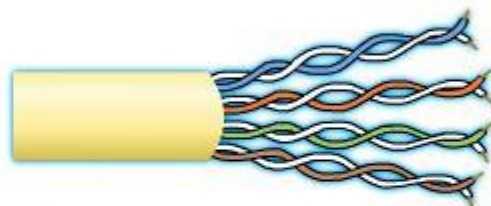
Τα συστραμμένα ζεύγη καλωδίων δημιουργούν κύκλωμα το οποίο μπορεί να μεταφέρει δεδομένα. Ένα καλώδιο αποτελείται από ένα ή περισσότερα τέτοια ζεύγη, τα οποία περιβάλλονται από μονωτικό υλικό, και υπάρχει σε δύο μορφές: το αθωράκιστο καλώδιο συνεστραμμένου ζεύγους (UTP: Unshielded Twisted Pair), συνηθισμένο στα τηλεφωνικά δίκτυα, και το θωρακισμένο καλώδιο συνεστραμμένου ζεύγους (STP: Shielded Twisted Pair), που παρέχει προστασία από θόρυβο ή παρεμβολές.

Αυτού του τύπου τα καλώδια χωρίζονται σε διάφορες κατηγορίες ανάλογα με τα χαρακτηριστικά τους.



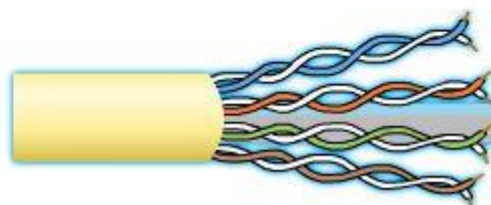
Category 3 Cable (UTP)

Χρήση από τηλεφωνικά δίκτυα.



Category 5 and 5e Cable (UTP)

Χρήση για μετάδοση δεδομένων.
ταχύτητα μετάδοσης:
100-1000 Mb/s



Category 6 Cable (UTP)

Χρήση για μετάδοση δεδομένων.
ταχύτητα μετάδοσης:
1000Mb/s-10Gb/s

Για τη σύνδεση συσκευών με αυτού του τύπου καλώδια χρησιμοποιούνται φίστες RJ45 είτε για τελική σύνδεση με συσκευή (Plugs) είτε για σύνδεση καλωδίων (Sockets).

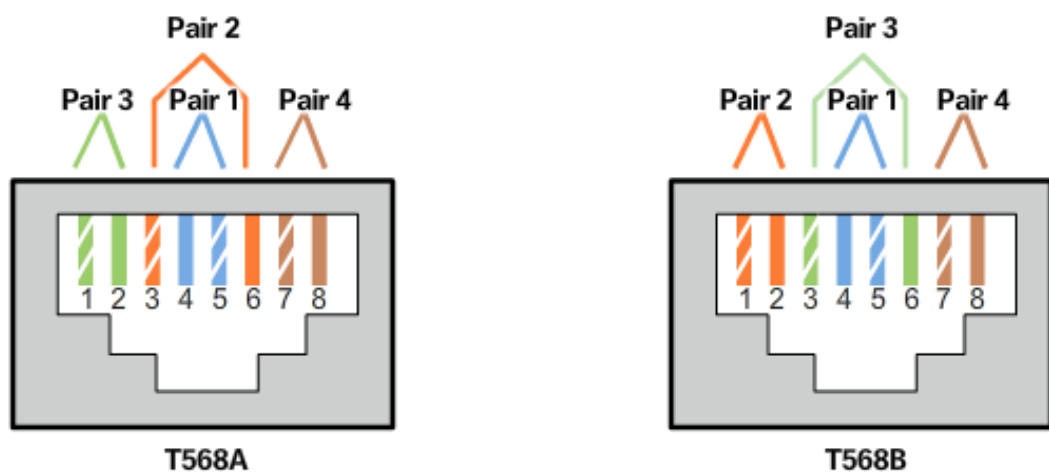
RJ-45 UTP Plugs



RJ-45 UTP Socket



Για τη συνδεσμολογία των RJ45 χρησιμοποιούνται δύο διεθνή στάνταρτ. Το T568A και το T568B.

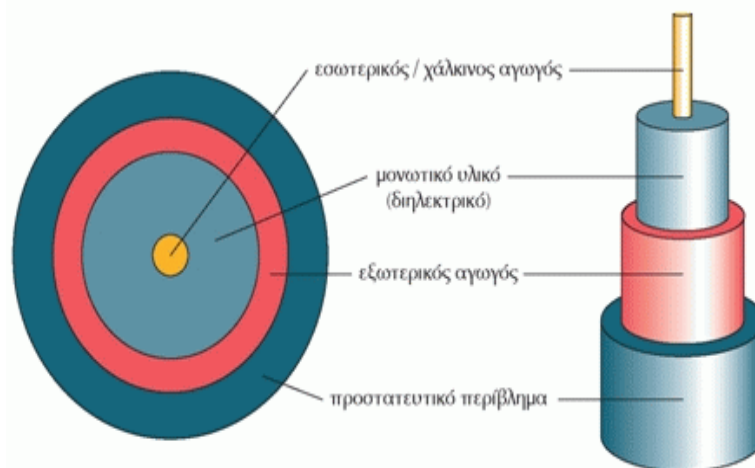


Με τη χρήση αυτών των δύο προτύπων δημιουργούνται 2 ειδών καλώδια.

- **Straight-through.** Χρησιμοποιείται για σύνδεση ανόμοιων συσκευών (τελικές συσκευές ή δρομολογητές με switch). Οι δυο πλευρές του καλωδίου πρέπει να είναι συνδεδεμένες με το ίδιο πρότυπο (T568A ή T568B).
- **Crossover.** Χρησιμοποιείται για σύνδεση όμοιων συσκευών. Οι δύο πλευρές του θα πρέπει να είναι διαφορετικές. Η μία T568A και η άλλη T568B.
-

Ομοαξονικά Καλώδια (Coaxial)

Το ομοαξονικό καλώδιο αποτελείται από δύο αγωγούς. Ο κεντρικός αγωγός περιβάλλεται από τον εξωτερικό. Γύρω από τον εξωτερικό αγωγό υπάρχει προστατευτικό και μονωτικό περίβλημα, ενώ ανάμεσα στον εσωτερικό αγωγό, που μεταφέρει το σήμα, και στον εξωτερικό υπάρχει διηλεκτρικό υλικό για την απομόνωσή τους. Λόγω της κατασκευής του ομοαξονικού καλωδίου, ο εσωτερικός αγωγός δέχεται πολύ μικρό ποσοστό θορύβου. Το ομοαξονικό καλώδιο προσφέρει υψηλό εύρος ζώνης (bandwidth, BW), με αποτέλεσμα να επιτυγχάνονται ταχύτητες μετάδοσης υψηλότερες από ότι στα χάλκινα καλώδια. Το γεγονός αυτό δικαιολογεί, την ευρεία χρησιμοποίησή του στην καλωδιακή τηλεόραση και στις υπεραστικές συνδέσεις του τηλεφωνικού δικτύου.



Β. Οπτικές Ίνες

Οι οπτικές ίνες, είναι πολύ λεπτά νήματα από πλαστικό ή γυαλί, όπου από μέσα τους, μεταδίδονται ψηφιακά δεδομένα, υπό μορφή φωτός.

Ένα καλώδιο οπτικών ινών, περιέχει μέσα του 10άδες ή και 100άδες πολύ λεπτές τέτοιες οπτικές ίνες, σε διάμετρο, μικρότερη και από μία τρίχα!

Οι ταχύτητες μετάδοσης των δεδομένων μέσω των οπτικών ινών, αφού τα δεδομένα ταξιδεύουν υπό μορφή φωτός, είναι πολύ μεγάλη, όσο η ταχύτητα του φωτός.

Στο ένα άκρο της οπτικής ίνας, υπάρχει ο πομπός και στο άλλο, ο δέκτης.

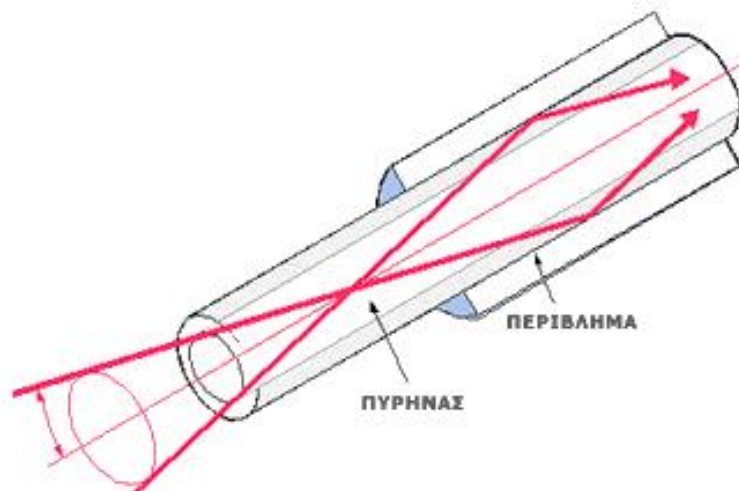
Ο πομπός, μετατρέπει τα ψηφιακά δεδομένα ενός υπολογιστή, σε ψηφιακά κύματα φωτός. Ο δέκτης, αποκωδικοποιεί τα ψηφιακά κύματα φωτός, σε ψηφιακά δεδομένα.

Τα ψηφιακά κύματα φωτός, ταξιδεύουν με την ταχύτητα του φωτός μέσα από την οπτική ίνα, με διαδοχικές ανακλάσεις στα τοιχώματα της οπτικής ίνας. Οι ανακλάσεις αυτές, γίνονται στα

τοιχώματα, σε γωνία μικρότερη των 42 μοιρών, με αποτέλεσμα να λειτουργούν τα τοιχώματα σαν καθρέφτες.

Το φαινόμενο αυτό ονομάζεται ολική ανάκλαση και είναι η αιτία που τα κύματα φωτός μένουνε μέσα στην οπτική ίνα, συνεχίζοντας το ταξίδι τους μέχρι το άλλο άκρο, χωρίς να βγαίνουν-χάνονται έξω από την ίνα.

Σε αυτό συνεισφέρει και η δομή της. Το εσωτερικό μέρος της οπτικής ίνας, ονομάζεται πυρήνας και μέσω αυτού, ταξιδεύουν τα κύματα φωτός. Ο πυρήνας, είναι περιτυλιγμένος από μία άλλη στρώση πλαστικού - γυαλιού που ονομάζεται περίβλημα.



Το περίβλημα από τις οπτικές ίνες, είναι έτσι κατασκευασμένο, ώστε να κρατάει τα κύματα φωτός, με ολικές ανακλάσεις, μέσα στον πυρήνα και να συνεχίζουν το ταξίδι τους μέσω αυτού (του πυρήνα).

Το περίβλημα το πετυχαίνει αυτό, λόγω της διαφορετικότητας του υλικού από το οποίο είναι κατασκευασμένο, σε σχέση με το υλικό του πυρήνα.

Τύποι οπτικών ινών

Υπάρχουν οι οπτικές ίνες απλού τύπου και οι πολλαπλού τύπου. Στις οπτικές ίνες απλού τύπου(single-mode), τα κύματα φωτός ταξιδεύουν σε ευθεία γραμμή και μπορούμε να στείλουμε δεδομένα σε μεγάλες αποστάσεις.

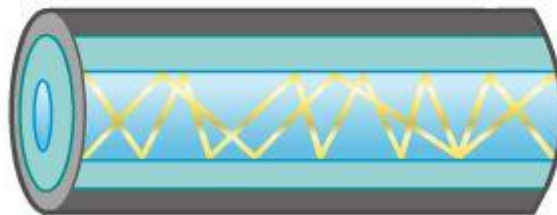
Οι οπτικές ίνες πολλαπλού τύπου(multi-mode), είναι πιο "χοντρές" από τις απλού τύπου, αλλά μπορούν να στείλουν παράλληλα, σε ξεχωριστό μονοπάτι, πολλά κύματα φωτός.

Το κάθε κύμα φωτός, εισέρχεται στην οπτική ίνα υπό ελαφρώς διαφορετική γωνία σε σχέση με τα άλλα, και ακολουθεί το δικό του μονοπάτι μέσα της, μέσω των διαδοχικών ανακλάσεων στο περίβλημα.

Απλού τύπου (Single Mode)



Πολλαπλού Τύπου (Multi Mode)



Αυτό συμβαίνει παράλληλα με πολλά κύματα φωτός (όλα σε διαφορετική γωνία σε σχέση με τα άλλα) κι έτσι μπορούμε να στείλουμε παράλληλα, τεράστιο όγκο δεδομένων.

Γ. Ασύρματη επικοινωνία

Ένα ασύρματο τοπικό δίκτυο (Wireless Local Area Network - WLAN ή Wireless Fidelity WiFi) χρησιμοποιεί ραδιοσυχνότητες (RF) προκειμένου να μεταδώσει και να λάβει δεδομένα μέσω του αέρα. Τα πλεονεκτήματα των ασύρματων τοπικών δικτύων είναι:

1.Κινητικότητα. Τα ασύρματα τοπικά δίκτυα παρέχουν στους χρήστες, εντός των χώρων κάλυψής τους, τη δυνατότητα πρόσβασης σε πληροφορίες σε πραγματικό χρόνο και από οποιοδήποτε μέρος του χώρου εργασίας τους. Αυτή η ευχέρεια στη κίνηση αυξάνει την παραγωγικότητα και τις ευκαιρίες για άμεση εξυπηρέτηση, ιδιότητες που δεν είναι εύκολα πραγματοποιήσιμες στα ενσύρματα δίκτυα.

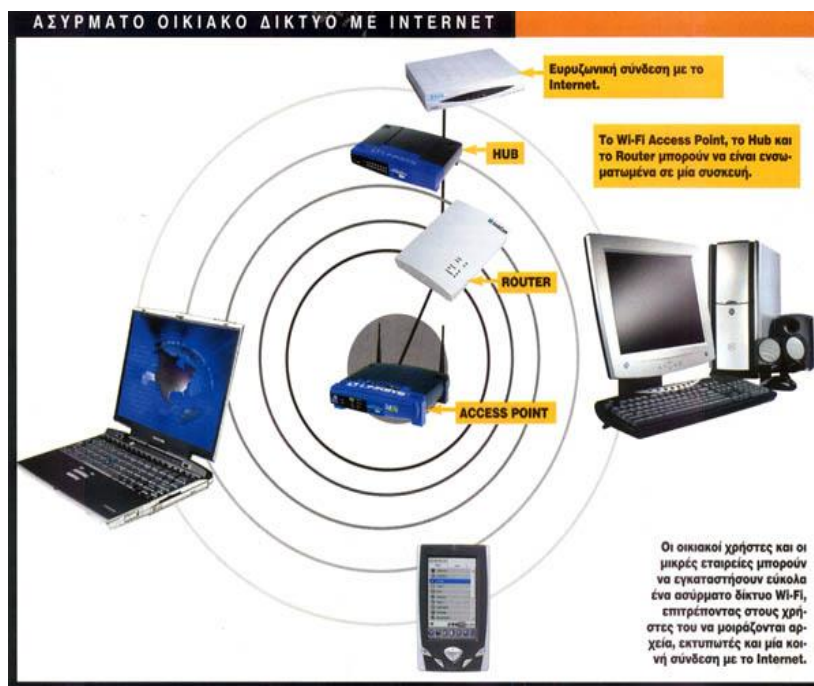
2.Ταχύτητα εγκατάστασης και απλότητα. Η εγκατάσταση ενός WLAN είναι γρήγορη και εύκολη και εξαλείφει την ανάγκη εγκατάστασης καλωδίων.

3.Ευελιξία εγκατάστασης. Η ασύρματη τεχνολογία επιτρέπει στο δίκτυο να επεκτείνεται εκεί που είναι δύσκολη η εγκατάσταση ενσύρματων υποδομών (π.χ. σε απομονωμένες περιοχές).

4.Μειωμένο κόστος συντήρησης. Ενώ η αρχική επένδυση που απαιτείται για την αγορά εξοπλισμού ενός ασύρματου τοπικού δικτύου είναι υψηλότερη από την αντίστοιχη μιας ενσύρματης σύνδεσης, το συνολικό κόστος λειτουργίας μπορεί να είναι σημαντικά χαμηλότερο. Τα μακροπρόθεσμα κέρδη είναι μεγαλύτερα, ειδικά σε δυναμικά περιβάλλοντα, όπου απαιτούνται πολύ συχνές μετακινήσεις και αλλαγές.

Τρόπος Λειτουργίας WLANs

Τα WLANs χρησιμοποιούν ηλεκτρομαγνητικά κύματα για να διαβιβάσουν τις πληροφορίες από ένα σημείο σε ένα άλλο, χωρίς απαίτηση για ενσύρματη σύνδεση. Αρχικά, οι πληροφορίες προς μετάδοση διαμορφώνουν κατάλληλα τη φέρουσα συχνότητα των ηλεκτρομαγνητικών κυμάτων του πομπού, κατόπιν τα κύματα μεταδίδονται μέσω του αέρα και τέλος, φτάνοντας στο δέκτη, αποδιαμορφώνονται και οι μεταδιδόμενες πληροφορίες ανακτώνται. Υπάρχει δυνατότητα ο πομπός να εκπέμπει ταυτόχρονα, στον ίδιο χώρο, περισσότερες της μίας φέρουσας συχνότητας, οι οποίες δεν παρεμβάλλονται μεταξύ τους, εφόσον βέβαια αυτές είναι όλες διαφορετικές. Στη συγκεκριμένη περίπτωση, για να ανακτήσει τις πληροφορίες ο δέκτης, συντονίζεται (ή επιλέγει) μια ραδιοσυχνότητα, απορρίπτοντας έτσι τα ραδιοσήματα στις υπόλοιπες συχνότητες. Σε μια τυπική διάταξη WLAN, μια συσκευή πομπού/δέκτη, αποκαλούμενη σημείο πρόσβασης, είναι συνδεδεμένη στο ενσύρματο δίκτυο σε συγκεκριμένη θέση, χρησιμοποιώντας συνήθως τυπικό καλώδιο Ethernet. Αυτό το σημείο πρόσβασης λαμβάνει, αποθηκεύει, και διαβιβάζει πληροφορίες μεταξύ του WLAN και του ενσύρματου δικτύου, ενώ μπορεί να υποστηρίξει μια μικρή ομάδα χρηστών και να λειτουργήσει εντός μιας ακτίνας από 30 έως μερικές 100άδες μέτρα. Οι τελικοί χρήστες έχουν πρόσβαση στο WLAN μέσω των ειδικών προσαρμογέων ασύρματου τοπικού δικτύου, οι οποίοι μπορούν να εφαρμοστούν ως κάρτες στους φορητούς υπολογιστές, κάρτες ISA ή PCI στους υπολογιστές γραφείου, ή ακόμα και να είναι πλήρως ενσωματωμένες συσκευές μέσα στους φορητούς υπολογιστές. Οι προσαρμογείς WLAN αποτελούν τη διεπαφή μεταξύ του λειτουργικού συστήματος των χρηστών του δικτύου και των ραδιοκυμάτων, μέσω μιας κεραίας. Η φύση της ασύρματης σύνδεσης είναι διαφανής (transparent) στο λειτουργικό σύστημα των τερματικών χρηστών.



Πλεονεκτήματα από τη χρήση ασύρματων τοπικών δικτύων

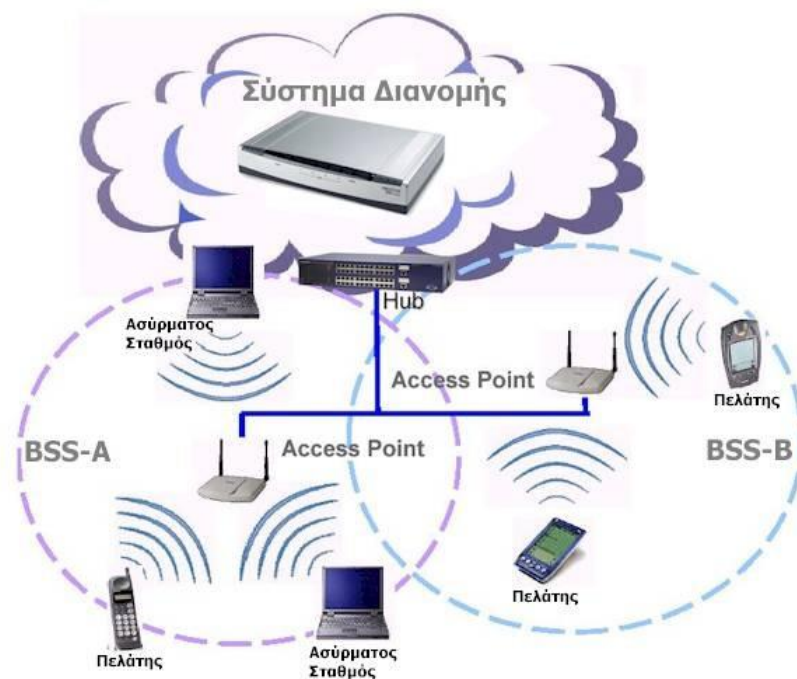
Τα ασύρματα δίκτυα έχουν φέρει αλλαγή στον τρόπο επικοινωνίας των υπολογιστών, αλλά και των χρηστών τους. Με την αύξηση του αριθμού των συσκευών που αλληλεπιδρούν με τους υπολογιστές τα ασύρματα δίκτυα μπορούν να προσφέρουν λύσεις, οι οποίες θα βελτιώσουν την επικοινωνία και θα αυξήσουν την αποδοτικότητα π.χ. σε ένα εργασιακό χώρο όπως μια εταιρεία, μια τράπεζα αλλά και μια σχολική μονάδα ή σε ένα νοσοκομείο. Με τη χρήση των ασύρματων δικτύων η επικοινωνία γίνεται πιο άμεση, το δίκτυο παρέχει κάλυψη χωρίς περιορισμούς και η επέκταση του γίνεται πολύ πιο εύκολα και με αμελητέο κόστος. Ο εξοπλισμός που χρησιμοποιείται είναι εντελώς ακίνδυνος για τον ανθρώπινο οργανισμό. Η ακτινοβολία είναι μη ιονίζουσα και τα επίπεδα ακτινοβολίας είναι πολύ πιο χαμηλά από τα επιτρεπτά για τον ανθρώπινο οργανισμό όρια. Αρκεί να αναφέρουμε ότι μια ασύρματη κάρτα δικτύου (802.11b) ακτινοβολεί ισχύ 50 - 100 mwatt, ενώ ένα κινητό τηλέφωνο φτάνει και τα 2000 mwatt. Επιπλέον, τα ασύρματα δίκτυα προσφέρουν διασύνδεση τοπικών δικτύων μεταξύ τους, όπως των καταστημάτων της επιχείρησης ή των εργαστηρίων ενός σχολικού εργαστηριακού κέντρου, επιτρέποντας τα ακόλουθα:

1. Επικοινωνία των υπολογιστών συνολικά και ανεξάρτητα από την τοποθεσία.
2. Φωνητική επικοινωνία μεταξύ των δικτύων χωρίς κόστος.
3. Μείωση των τηλεπικοινωνιακών εξόδων με το μοίρασμα μιας σύνδεσης με το Διαδίκτυο προς όλα τα υποδίκτυα.
4. Ακόμα και επισκόπηση χώρων χρησιμοποιώντας ασύρματες κάμερες.

Εξοπλισμός

Η πρόσβαση στο ασύρματο δίκτυο είναι δυνατή από ένα σύνολο συσκευών συμβατών με τα κατάλληλα πρωτόκολλα επικοινωνίας, όπως φορητοί υπολογιστές (laptops), έξυπνες συσκευές χειρός (handheld pdas, τηλέφωνα κλπ), ασύρματες κάμερες και οθόνες τηλεπροβολής κ.α. Η ευκολία με την οποία μπορεί κανείς να "στήσει" ένα ασύρματο τοπικό δίκτυο, ήταν ένας από τους βασικούς παράγοντες που συνέβαλαν στη ραγδαία εξάπλωση τους. Τα στοιχεία τα οποία χρειάζεται ένα WLAN για να λειτουργήσει, καθώς και για να συνδεθεί στο ευρύτερο δίκτυο, είναι:

1. Προσαρμογείς: που λειτουργούν ως συνδετικά στοιχεία μεταξύ του τελικού εξοπλισμού του χρήστη και του σημείου ασύρματης πρόσβασης του δικτύου.
2. Σημεία πρόσβασης: που είναι πομποδέκτες με μία ή δύο κεραίες. Συνδέονται με το ενσύρματο τοπικό δίκτυο (ή με την ευρυζωνική σύνδεση). Μέσω αυτών, επικοινωνεί ο προσαρμογέας του τελικού χρήστη με το υπόλοιπο δίκτυο.
3. Γέφυρες: Παρέχουν την από σημείο σε σημείο ασύρματη σύνδεση μεταξύ δύο WLANs, όπως μεταξύ δύο ορόφων.
4. Κόμβοι Διανομής: Συγκεντρώνουν και συνδέουν πολλαπλά σημεία ασύρματης πρόσβασης με το ενσύρματο ή ασύρματο δίκτυο κορμού.
5. Κόμβοι κορμού: Διασυνδέουν τους κόμβους διανομής. Καλύπτουν πολλούς χρήστες, λόγω του μεγάλου αριθμού των σημείων πρόσβασης που είναι συνδεδεμένα μέσω των κόμβων διανομής με αυτά. Σχεδόν πάντα επικοινωνούν μεταξύ τους, με περισσότερες από μία συνδέσεις, για να μειθούν περιπτώσεις απώλειας επαφής.



Με τον τρόπο αυτό, και χωρίς τη χρήση καλωδίων, επιτυγχάνεται η διασύνδεση όλων των υπολογιστικών συστημάτων του χώρου. Για την επέκταση του δικτύου απαιτείται απλά η εγκατάσταση ενός επιπλέον σημείου ασύρματης πρόσβασης.

Ένα δίκτυο WLAN υλοποιείται ως εξής: Πολυκατευθυντικές κεραίες τοποθετούνται σε σημεία πρόσβασης ή σε κόμβους διανομής / κορμού, ενώ κατευθυντικές στους τελικούς χρήστες. Οι κεραίες αυτές είναι εξωτερικές και συνήθως βρίσκονται στις κορυφές κτιρίων στο κέντρο της περιοχής χρήσης. Ένας απλός χρήστης που θέλει μόνο να συνδεθεί, αλλά να μη διευκολύνει την ευρύτερη δικτύωση, χρειάζεται μία κατευθυντική κεραία. Με αυτή, μπορεί να εξασφαλίσει πρόσβαση από ένα σημείο πρόσβασης, ώστε να έχει σύνδεση στο τοπικό δίκτυο και ενδεχομένως και στο διαδίκτυο (αν το σημείο πρόσβασης παρέχει τέτοια δυνατότητα). Ένας πιο ενεργός χρήστης μπορεί να χρησιμοποιεί δύο κατευθυντικές κεραίες, ώστε να φροντίζει για τη συνέχιση του δικτύου ή και μια πολυκατευθυντική για να λειτουργεί ο ίδιος σαν σημείο πρόσβασης άλλων χρηστών. Αν κάποιος κόμβος έχει πάνω από δύο κατευθυντικές κεραίες, μπορεί να διευκολύνει και την πολλαπλή δρομολόγηση. Με τον τρόπο αυτό μπορεί να δημιουργηθεί ένα δίκτυο που να καλύπτει μία πύλη. Τέλος, συνδέοντας ο χρήστης μία δική του γραμμή DSL με το WLAN, θα μπορούσε να γίνει "πύλη" για το Διαδίκτυο και να επιτρέπει την πρόσβαση γειτονικών χρηστών σε αυτό.



Ακτίνα κάλυψης και επιδόσεις ασύρματων τοπικών δικτύων
Η ταχύτητα ενός WLAN εξαρτάται από πολλούς παράγοντες, από την αποδοτικότητα του ενσύρματου δικτύου που συνδέει τα σημεία πρόσβασης, μέχρι τη δομή του κτιρίου που έχει εγκατασταθεί και τον τύπο του WLAN που χρησιμοποιείται. Κατά γενικό κανόνα για όλα τα WLANs, η ταχύτητα μειώνεται με την αύξηση της απόστασης μεταξύ του σημείου πρόσβασης του ασύρματου δικτύου και των χρηστών. Τα πρότυπα 802.11 υποστηρίζουν διάφορους ρυθμούς μετάδοσης, προκειμένου να προσαρμόζονται στην απώλεια ισχύος των σημάτων και να διατηρούν υψηλή την ποιότητα συναρμολόγησης των πακέτων δεδομένων. Ο χρήστης του

WLAN εκτελεί συνεχώς διαδικασίες που ανιχνεύουν και θέτουν αυτόματα την καλύτερη δυνατή ταχύτητα. Οι συχνότητες στις οποίες εκπέμπουν τα πρότυπα 802.11b και 802.11g, τους επιτρέπουν να διεισδύουν σε στερεά υλικά και να έχουν έτσι μια ακτίνα κάλυψης της τάξης των 100 μ. Το πρότυπο 802.11a παρουσιάζει μια πιο απότομη πτώση στην ταχύτητα καθώς η απόσταση αυξάνεται από το σημείο πρόσβασης, και επιδεικνύει έτσι μια ακτίνα κάλυψης της τάξης των 50 μ στα περισσότερα εσωτερικά περιβάλλοντα.



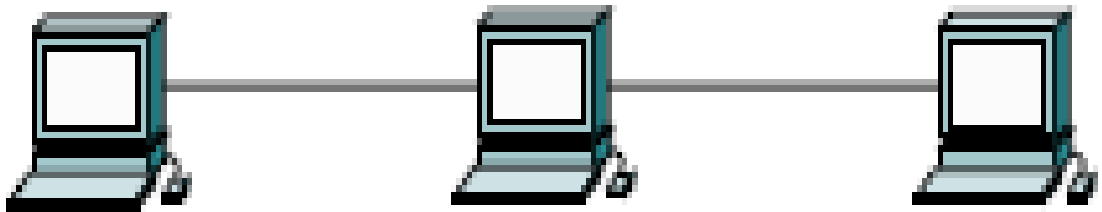
Δ. Πλήμνη (Hub)

Ένα hub είναι μία απλή συσκευή που ανήκει στο φυσικό επίπεδο. Χρησιμοποιείται για την διακλάδωση και την σύνδεση των διαφόρων υπολογιστών στο δίκτυο. Κάθε πακέτο δεδομένων που προέρχεται από μια θύρα αποστέλλεται σε όλες τις άλλες θύρες. Πλέον κάθε υπολογιστής αναλαμβάνει να αποφασίσει αν θα δεχθεί το πακέτο (αν είναι αυτός ο παραλήπτης του πακέτου) ή αν θα το απορρίψει. Το μεγαλύτερο πρόβλημα με τα hubs είναι η απλότητα τους. Επειδή κάθε πακέτο στέλνεται σε κάθε υπολογιστή του δικτύου, υπάρχει μια μεγάλη σπατάλη μετάδοσης. Αυτό σημαίνει ότι το δίκτυο μπορεί εύκολα να υποστεί συμφόρηση. Το hub δημιουργεί ένα collision domain και ένα broadcast domain. Hubs, χρησιμοποιούνται συνήθως για μικρά δίκτυα, όπου η ποσότητα των δεδομένων που πηγαίνει σε όλο το δίκτυο δεν είναι ποτέ πολύ υψηλή.

4. Επίπεδο Συνδέσμου (Link Layer)

A. Τοπολογίες

Τοπολογία δικτύου είναι η γεωμετρική και φυσική διάταξη των καλωδίων και των συσκευών που συνδέονται με το δίκτυο. Αυτή η διάταξη μπορεί να είναι ένας δίαυλος, ένας δακτύλιος ή ένας αστέρας. Αν το δίκτυο είναι πολύ μεγάλο, ενδέχεται να υπάρχουν και τα τρία είδη σε διάφορα σημεία του δικτύου. Οι τοπολογίες είναι είτε φυσικές είτε λογικές. Τα κυριότερα είδη τοπολογιών είναι η γραμμική, η τύπου διαύλου, δακτυλίου, αστέρα, η κατακεντρωμένη, η πλήρως κατακεντρωμένη και η τύπου δένδρου.

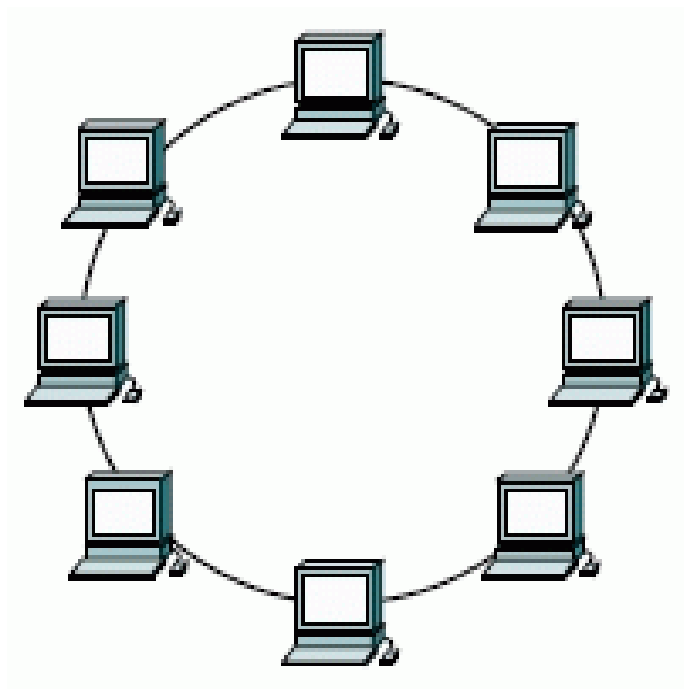


Τοπολογία διαύλου

Δίαυλος(Bus) Στην τοπολογία αυτή ολόκληρο το δίκτυο στηρίζεται σε ένα καλώδιο, το οποίο συνήθως καλείται ραχοκοκαλιά (Backbone). Όλοι οι κόμβοι συνδέονται με το κεντρικό καλώδιο. Τα καλώδια είναι συνήθως ομοαξονικά, ενώ η ραχοκοκαλιά είναι τερματισμένη στα δύο άκρα της. Αυτό γίνεται προκειμένου το σήμα να απορροφάται στα δύο άκρα και να μην ανακλάται δημιουργώντας επιπλέον θόρυβο. Τα πλεονεκτήματα του είναι ότι είναι εύκολο στην εγκατάσταση και σχετικά φθηνό. Τα μειονεκτήματα είναι ότι αν σε ένα σημείο του διαύλου διακοπεί η επικοινωνία, τότε καταρρέει όλο το δίκτυο, ενώ δύσκολα εντοπίζεται η βλάβη. Αυτή η τοπολογία συνδυάζεται συνήθως με τα πρωτόκολλα 10Base5 και 10Base2. Τα δίκτυα διαύλου είναι σχετικά ανέξοδα και εύκολο να εγκατασταθούν για τα μικρά δίκτυα.

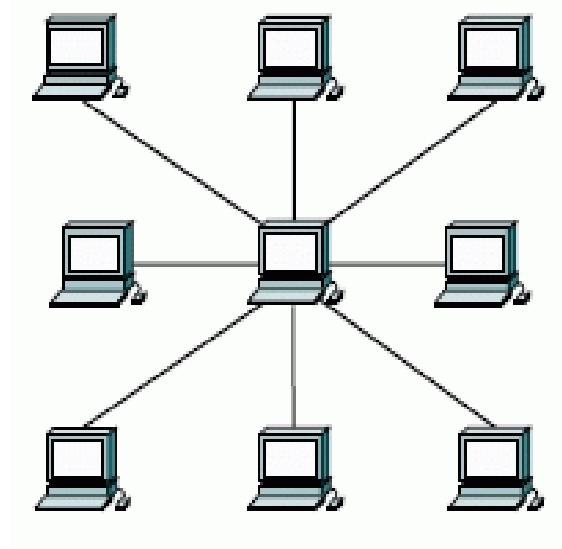
Τοπολογία δακτυλίου

Δακτύλιος(Ring) Σε αυτή τη τοπολογία, όλοι οι κόμβοι συνδέονται έτσι, ώστε να σχηματίζουν ένα κύκλο. Τα δεδομένα ακολουθούν πάντα την ίδια φορά και κάθε κόμβος αναπαράγει το σήμα. Αν λοιπόν κάποια συσκευή σταματήσει να λειτουργεί, τότε καταρρέει ολόκληρο το δίκτυο. Την τοπολογία αυτήν την συναντάμε σε πρωτόκολλα Token Ring και FDDI και χρησιμοποιείται σε δίκτυα με πολλούς κόμβους όπου απαιτείται υψηλή ταχύτητα. Άλλο ένα μειονέκτημα είναι το υψηλό κόστος αφού για την δημιουργία ενός δακτυλίου με πρωτόκολλο FDDI χρειάζεται η αγορά οπτικών ινών και ανάλογες κάρτες δικτύου(NIC).



Τοπολογία αστέρα (Star)

Στην τοπολογία αστέρα όλες οι συσκευές συνδέονται με μια κεντρική συσκευή (hub ή switch). Το Hub και το switch είναι συσκευές με εισόδους RJ-45 όπου συνδέονται οι κόμβοι, ενώ συνήθως έχουν και λαμπάκια τα οποία δείχνουν την κατάσταση λειτουργίας τους.



Τα δίκτυα αστεριών είναι σχετικά εύκολο να εγκατασταθούν και να διαχειριστούν, αλλά οι δυσχέρειες μπορούν να εμφανιστούν επειδή όλα τα στοιχεία πρέπει να περάσουν μέσω του hub ή του switch. Το πλεονέκτημα αυτής της τοπολογίας είναι ότι, αν κάποιος κόμβος τεθεί εκτός λειτουργίας, δεν καταρρέει το δίκτυο.

Εξίσου εύκολη είναι και η επέκταση του δικτύου με την προσθήκη παραπάνω κόμβων, αφού το δίκτυο δεν χρειάζεται να σταματήσει να λειτουργεί. Το μειονέκτημα εδώ είναι το αυξημένο κόστος λόγω των περισσότερων καλωδίων και των συσκευών hub ή switch.

B. Frame

Η βασική μονάδα πληροφορίας που μεταφέρεται μέσα στα δίκτυα ονομάζεται πλαίσιο (Frame).

Τα δίκτυα των υπολογιστών δεν μεταφέρουν δεδομένα με τη μορφή μιας τυχαίας ακολουθίας από συνεχόμενα bit. Το δικτυακό σύστημα διαιρεί τα δεδομένα σε μικρές ενότητες που ονομάζονται πακέτα (packets), τις οποίες στέλνει μεμονωμένα. Επειδή τα δίκτυα υπολογιστών χρησιμοποιούν αυτή τη τεχνολογία, ονομάζονται συνήθως και ως δίκτυα μεταγωγής πακέτων (packet switching networks).

Ένα πακέτο αποτελείται από δύο μέρη δεδομένων: τις πληροφορίες ελέγχου και τα δεδομένα του χρήστη. Οι πληροφορίες ελέγχου, εμπεριέχουν τα δεδομένα που χρειάζεται το δίκτυο έτσι ώστε να μεταφέρει τα δεδομένα του χρήστη. Μερικές από τις πληροφορίες αυτές είναι: διευθύνσεις αποστολέα και παραλήπτη, εντοπισμός σφαλμάτων και ένας αύξων αριθμός για το κάθε πακέτο. Αυτό το μέρος του πακέτου αποκαλείται κεφαλίδα (header).

Πλαίσια υλικού

Αν και ο όρος πακέτο αναφέρεται στη γενική έννοια μιας ενότητας δεδομένων, δεν υπάρχει καθολική ομοφωνία για τη συγκεκριμένη μορφή ενός πακέτου. Το υλικό (χαλκός, οπτικές ίνες, αέρας) πάνω στο οποίο βασίζονται τα δίκτυα υπαγορεύει τη μορφή του πακέτου και τις μεθόδους μετάδοσης μέσα στο δίκτυο. Για τον λόγο αυτό, χρησιμοποιείται συχνά ο όρος πλαίσιο (frame), για την περιγραφή της μορφής ενός πακέτου για μια δεδομένη τεχνολογία υλικού. Επομένως, ο όρος αυτός χρησιμοποιείται για τα πακέτα των πρωτοκόλλων που βρίσκονται στο Φυσικό Επίπεδο (π.χ. Ethernet frame).

Παραδείγματα Πακέτων

Παρακάτω περιγράφονται οι δυο τύποι πακέτων που χρησιμοποιούνται πιο συχνά κατά τη μεταγωγή δεδομένων, στα δίκτυα υπολογιστών.

Πλαίσιο Ethernet (Ethernet frame)

Η πιο διαδεδομένη και πιο συχνά χρησιμοποιούμενη τεχνολογία τοπικών δικτύων, είναι το Ethernet. Όταν ένα πακέτο (IP datagram, UDP datagram κλπ) χρειάζεται να ταξιδέψει μέσα σε ένα δίκτυο Ethernet, πρέπει πρώτα να ενθυλακωθεί μέσα σε ένα πλαίσιο Ethernet. Η μορφή αυτού του πλαισίου είναι η εξής:



Destination Address: έχει μέγεθος 6 byte, και αντιστοιχεί στην φυσική διεύθυνση (διεύθυνση MAC) του παραλήπτη.

Source Address: έχει μέγεθος 6 byte, και αντιστοιχεί στην φυσική διεύθυνση του αποστολέα.

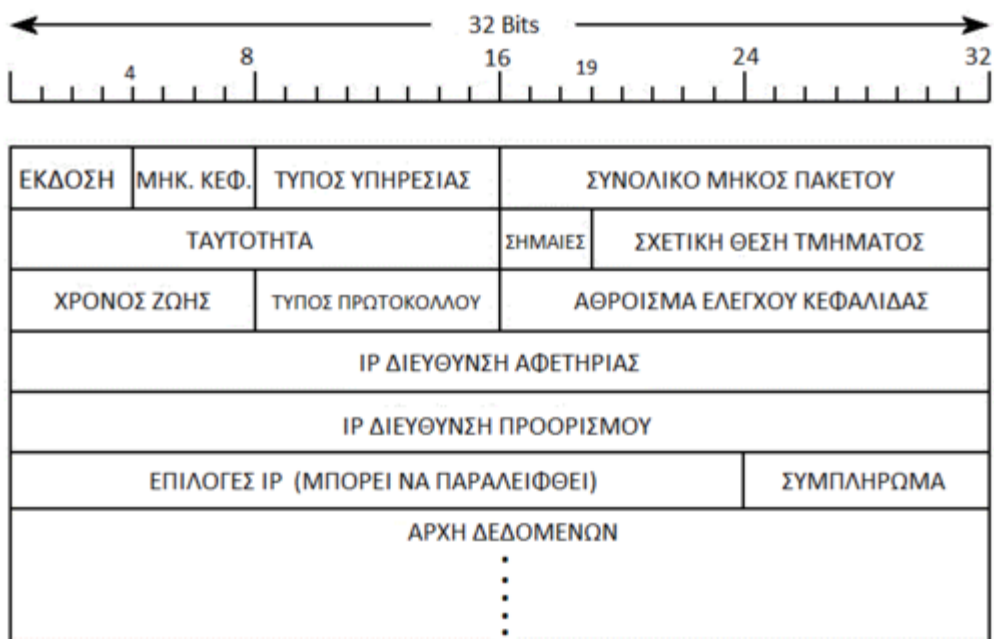
Type: έχει μέγεθος 2 byte, προσδιορίζει τον τύπο του πλαισίου.

ΔΕΔΟΜΕΝΑ: μπορεί να έχει μέγεθος από 46-1500 bytes. Τα δεδομένα αυτά, δεν αντιστοιχούν εξ' ολοκλήρου στα καθαρά δεδομένα.

CRC (έλεγχος σφαλμάτων): έχει μέγεθος 4 byte και αντιστοιχεί στον έλεγχο της ομαλής μετάδοσης των δεδομένων της κεφαλίδας (και όχι όλου του πακέτου). Το πεδίο αυτό, έπεται των δεδομένων.

Κεφαλίδα αυτοδύναμου πακέτου IP

Η κεφαλίδα του πακέτου IP στην έκδοση 4 (IPv4), έχει τη μορφή που φαίνεται στην εικόνα, και αποτελείται από τα εξής πεδία:



Έκδοση (Version): το πεδίο αυτό έχει μέγεθος 4 bits, και περιγράφει την έκδοση του πρωτοκόλλου IP (4 ή 6).

Μήκος Κεφαλίδας (IP Header Length – IHL): το πεδίο αυτό έχει μέγεθος 4 bits, και περιγράφει το μήκος της κεφαλίδας σε 32bits λέξεις. Οι λέξεις αυτές είναι συνήθως 5, οπότε και η τιμή του πεδίου αυτού είναι επίσης 5.

Τύπος(ή Ποιότητα) Υπηρεσίας (Type of Service or Quality of Service – T.o.S. or Q.o.S.): το πεδίο αυτό έχει μέγεθος 8 bits (1 byte), και περιγράφει τον τρόπο δρομολόγησης του πακέτου.

Συνολικό Μήκος πακέτου (Total Length): περιέχει έναν ακέραιο αριθμό των 16 bit, ο οποίος καθορισμένος το συνολικό αριθμό οκτάδων που περιέχει το αυτοδύναμο πακέτο (κεφαλίδα + δεδομένα).

Ταυτότητα (Identification): έχει μέγεθος 16 bit (2 byte) και αποτελεί τον αναγνωριστικό αριθμό του πακέτου. Έτσι όταν ένα πακέτο κατακερματιστεί, τα διάφορα κομμάτια του θα έχουν τον ίδιο αριθμό ταυτότητας, για να υποδηλώνουν ότι αποτελούν μέρη, του ίδιου πακέτου.

Σημαίες (Flags): έχει μέγεθος 3 bit. Κάθε bit, αποτελεί και μια ξεχωριστή σημαία και ανάλογα με το αν είναι 0 ή 1, εκτελούνται διαδικασίες κατακερματισμού του πακέτου.

Χρόνος Ζωής (Time To Live – TTL): έχει μέγεθος 8 bit (1 byte). Περιέχει έναν αριθμό (1-255), ο οποίος προσδιορίζει το χρόνο ζωής του datagram. Μετρίεται σε αριθμό αλμάτων μεταξύ των δρομολογητών. Σε κάθε διέλευση από κάποιο δρομολογητή ο αριθμός μειώνεται κατά 1. Όταν μηδενιστεί, το πακέτο απορρίπτεται.

Τύπος Πρωτοκόλλου (Protocol): έχει μέγεθος 8 bit (1 byte). Δείχνει πιο πρωτόκολλο χρησιμοποιείται, στο Επίπεδο Μεταφοράς.

Άθροισμα Ελέγχου Κεφαλίδας (Header Checksum): έχει μέγεθος 16 bit (2 byte). Χρησιμοποιείται για τον έλεγχο της ορθής μετάδοσης της επικεφαλίδας, και όχι ολόκληρου του πακέτου.

IP Διεύθυνση Αφετηρίας (Source IP Address): έχει μέγεθος 32 bit, και περιέχει την IP διεύθυνση του αρχικού αποστολέα του πακέτου.

IP Διεύθυνση Προορισμού (Destination IP Address): έχει μέγεθος 32 bit, και περιέχει την IP διεύθυνση του τελικού παραλήπτη του πακέτου.

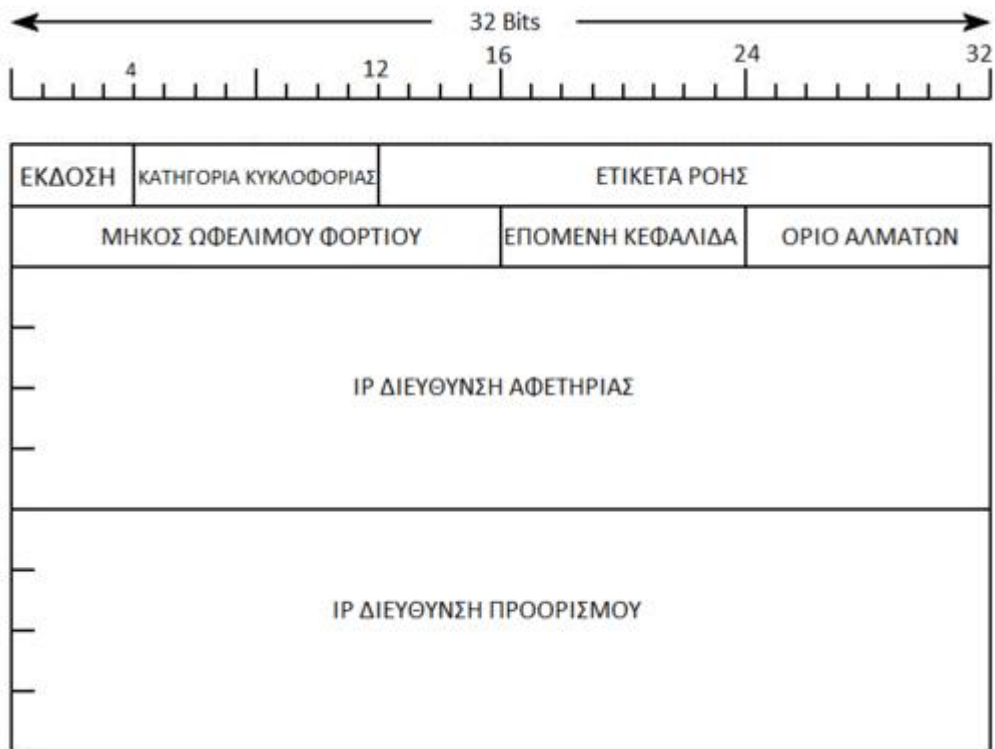
Επιλογές IP (IP Options): Συνήθως δεν χρησιμοποιείται. Η χρήση του αφορά σε διαγνωστικούς και διαχειριστικούς ελέγχους. Αν δεν χρησιμοποιείται ολόκληρο συμπληρώνεται με μηδενικά. Σε αντίθετη περίπτωση, το πεδίο IHL θα είναι >5, ώστε να δείχνει το μέγεθός του.

IPv6

Λόγω της σταδιακής έλλειψης διευθύνσεων IP, δημιουργήθηκε η ανάγκη για την αναθεώρηση του Πρωτοκόλλου IP. Αναπόφευκτη συνέπεια, ήταν να αλλάξει και η μορφή της κεφαλίδας του πακέτου IP.

Η κεφαλίδα του πακέτου IP στην έκδοση 6 (IPv6), διαφέρει σχεδόν εξ' ολοκλήρου, από την έκδοση 4. Παρ' ότι η κεφαλίδα του IPv6 είναι διπλάσια σε μέγεθος από μια κεφαλίδα του

IPv4, περιέχει λιγότερες πληροφορίες. Ορισμένα πεδία έχουν συγχωνευτεί ενώ άλλα έχουν πλήρως παραλειφθεί, δίνοντας τη θέση τους σε νέα. Τα πεδία της κεφαλίδας ενός πακέτου IPv6 είναι τα εξής:



Έκδοση (Version): έχει μέγεθος 4 bit, και προσδιορίζει την έκδοση του πρωτοκόλλου, δηλαδή έχει τη τιμή 6.

Κατηγορία Κυκλοφορίας (Traffic Class): έχει μέγεθος 8 bit, και καθορίζει την κατηγορία κυκλοφορίας, η οποία χρησιμοποιείται για την επιλογή ενός δρομολογίου. Το πεδίο αυτό αντικαθιστά τα πεδία Μήκος Κεφαλίδας (IP Header Length – IHL) και Τύπος Υπηρεσίας (Type of Service or Quality of Service – T.o.S. or Q.o.S.) του πρωτοκόλλου IPv4.

Ετικέτα Ροής (Flow Label): έχει μέγεθος 20 bit, και χρησιμοποιείται για τον προσδιορισμό μιας συγκεκριμένης διαδρομής μέσω του δικτύου.

Μήκος Ωφέλιμου Φορτίου (Payload Length): έχει μέγεθος 16 bit, και προσδιορίζει μόνο το μέγεθος των δεδομένων που μεταφέρει το πακέτο, εξαιρείται δηλαδή η κεφαλίδα. Το πεδίο αυτό αντικαθιστά το πεδίο Συνολικό Μήκος πακέτου (Total Length).

Επόμενη Κεφαλίδα (Next Header): έχει μέγεθος 8 bit, και χρησιμοποιείται για να καθορίσει τον τύπο των πληροφοριών που ακολουθούν μετά τη τρέχουσα κεφαλίδα.

Όριο Αλμάτων (Hop Limit): έχει μέγεθος 8 bit, και αντιστοιχεί στο πεδίο Χρόνος Ζωής (TTL) του IPv4.

IP Διεύθυνση Αφετηρίας (Source IP Address): έχει μέγεθος 128 bit (4 φορές μεγαλύτερο), , και περιέχει την IP διεύθυνση του αποστολέα του πακέτου.

IP Διεύθυνση Προορισμού (Destination IP Address): έχει μέγεθος 128 bit (4 φορές μεγαλύτερο), και περιέχει την IP διεύθυνση του τελικού παραλήπτη του πακέτου.

Γ. Mac Address

Μία διεύθυνση Media Access Control (MAC), που καλείται επίσης και φυσική διεύθυνση, είναι μία μοναδική διεύθυνση (ταυτότητα) που αποδίδεται στις συσκευές (network interfaces controller, NIC) που διασυνδέουν ένα υπολογιστή ή μια άλλη συσκευή στο δίκτυο. Οι διευθύνσεις MAC συνήθως αποδίδονται από τον κατασκευαστή και αποθηκεύονται στο hardware της διασύνδεσης (στη ROM).

Ένας κόμβος δικτύου μπορεί να έχει πολλές NICs και κάθε NIC πρέπει να έχει μία μοναδική MAC. Οι διευθύνσεις MAC σχηματίζονται σύμφωνα με τους κανόνες μιας από τρεις περιοχές διευθύνσεων. Τις περιοχές αυτές τις διαχειρίζεται το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronics Engineers (IEEE) και είναι οι:

- MAC-48
- EUI-48
- EUI-64.

Το EUI είναι συντόμευση του Extended Unique Identifier (Εκτεταμένη Μοναδική Ταυτότητα).

Μια διεύθυνση MAC είναι δυαδικός αριθμός, επειδή όλα τα δεδομένα σε ένα υπολογιστικό σύστημα παριστάνονται, αποθηκεύονται και διαχειρίζονται σε δυαδική μορφή.

Έτσι οι διευθύνσεις MAC-48, EUI-48 αποτελούνται από 48 bit, ενώ η διεύθυνση EUI-64 από 64 bit.

Οι διευθύνσεις MAC χρησιμοποιούνται για την φυσική διευθυνσιοδότηση σε ένα τοπικό δίκτυο, όπου η δρομολόγηση με βάση την διεύθυνση IP θα "ανάγκαζε" τους υπολογιστές να κάνουν επεξεργασία μέχρι και το επίπεδο δικτύου (στο οποίο χρησιμοποιούνται κυρίως οι διευθύνσεις IP) κάτι που σημαίνει παραπάνω επεξεργασία που εν τέλει είναι περιττή.

Συμβολισμοί

Όπως αναφέραμε παραπάνω οι διευθύνσεις MAC αποτελούνται από 48 ή 64 bit. Επειδή όμως με αυτή την μορφή είναι δύσκολος ο χειρισμός τους, αναπαριστώνται σε δεκαεξαδική μορφή. Δηλαδή κάθε 4 bit της διεύθυνσης, αντικαθίστανται από έναν δεξαεξαδικό αριθμό.

Η συνηθισμένη μορφή αναπαράστασης μιας MAC-48 διεύθυνσης σε φιλική μορφή προς τον άνθρωπο, είναι έξι διψήφιοι δεκαεξαδικοί αριθμοί χωρισμένοι με παύλες (-), με την σειρά που αποστέλλονται (π.χ 01-ea-4f-67-89-ab). Ο τρόπος αυτός χρησιμοποιείται στα Windows.

Αυτή η μορφή χρησιμοποιείται και για το EUI-64 (π.χ 1a-cd-3f-ac-42-34-ed-ab).

Σε άλλες συμβάσεις σαν διαχωριστικά χρησιμοποιούνται η άνω και κάτω τελεία (:) (π.χ 01:23:45:67:89:ab). Ο διαχωρισμός με άνω κάτω τελείες χρησιμοποιείται στο unix/linux.

Άλλη μορφή αναπαράστασης είναι σε τετράδες δεκαεξαδικών ψηφίων χωρισμένες με τελείες, πάλι με τη σειρά εκπομπής (π.χ 1236.adc4.23da).

Μία γενικά διαχειριζόμενη διεύθυνση είναι μοναδική στον κόσμο και αποδίδεται στη συσκευή από τον κατασκευαστή της.

Αποτελείται από δύο μέρη: Το πρώτο μέρος το απαρτίζουν οι πρώτες τρεις οκτάδες (με τη σειρά εκπομπής) και προσδιορίζει τον οργανισμό ο οποίος εξέδωσε την ταυτότητα. Οι τρεις αυτές οκτάδες είναι γνωστές με το όνομα Μοναδική Ταυτότητα του Οργανισμού (Organizationally Unique Identifier-OUI) . Η ταυτότητα αυτή χορηγείται κατά αποκλειστικότητα στον κατασκευαστή από το IEEE και είναι μοναδική. Οι ακόλουθες τρεις οκτάδες στο MAC-48 και EUI-48 ή πέντε οκτάδες στο EUI-64, αποδίδονται στη διασύνδεση από τους κατασκευαστές με όποιον τρόπο θέλουν, αρκεί να είναι μοναδικές.

Unicast: Αυτός ο τύπος εκπομπής πακέτων χρησιμοποιείται όταν ένας κόμβος στέλνει πακέτα σε κάποιο άλλο κόμβο του δικτύου. Το switch εφ' όσον δεν γνωρίζει σε ποια θύρα του είναι συνδεδεμένη η συσκευή προορισμού του πλαισίου, θα προωθήσει το πλαίσιο σε όλες τις θύρες, εκτός από τη θύρα προέλευσης. Εάν γνωρίζει τη θύρα στην οποία είναι συνδεδεμένη η MAC προορισμού, τότε προωθεί το πακέτο μόνο σε αυτήν.

Γενικά όταν οι NIC παίρνουν πακέτα με διαφορετική MAC προορισμού από τη δική τους τα αγνοούν.

Multicast: Αυτός ο τύπος εκπομπής πακέτων χρησιμοποιείται για την αποστολή σε πολλούς κόμβους μέσα στο δίκτυο ταυτόχρονα.

Broadcast: Αυτός ο τύπος εκπομπής χρησιμοποιείται για την αποστολή πακέτων σε όλους τους κόμβους του δικτύου. Μία ειδική διεύθυνση MAC είναι η διεύθυνση με όλα τα δυαδικά ψηφία 1, δηλ. ή ff-ff-ff-ff-ff-ff, η οποία είναι η διεύθυνση εκπομπής. Ένα Frame δηλαδή με διεύθυνση προορισμού την ff-ff-ff-ff-ff-ff απευθύνεται σε όλους τους κόμβους ενός τοπικού δικτύου (broadcast). Επομένως στην περίπτωση αυτή ο μεταγωγέας (switch) προωθεί το μήνυμα σε όλες τις θύρες του.

Δ. Μεταγωγείς (Switches)

Ο μεταγωγέας (switch) είναι μια ηλεκτρονική συσκευή που χρησιμοποιείται σε δίκτυα υπολογιστών. Οι μεταγωγείς χρησιμοποιούν λογισμικό και καταγράφουν τις φυσικές διευθύνσεις όλων των συσκευών που είναι ενωμένοι σε αυτούς. Με αυτό το πλεονέκτημα μπορούν να προωθούν το κάθε μήνυμα μόνο προς τον παραλήπτη (σε αντίθεση με τα hub) μειώνοντας την ανώφελο φόρτωση του δικτύου με άσκοπες μεταφορές πακέτων. Προσφέρουν ταχύτητες της τάξης των Gigabits. Μπορούν να πάρουν τη θέση των Hubs χωρίς να γίνει καμιά απολύτως επανασχεδίαση στο δίκτυο.

Το switch δημιουργεί πίνακες προώθησης.

Σε περίπτωση που δύο υπολογιστές θέλουν να επικοινωνήσουν και βρίσκονται σε διαφορετικές θύρες του switch, το switch εξετάζει τον πίνακα προώθησης για να βρει

τη διεύθυνση MAC προορισμού και σε ποια θύρα να το προωθήσει. Έτσι αφού βρεθεί η καταχώρηση θα σταλθεί το πακέτο στην κατάλληλη θύρα. Με αυτόν τον τρόπο το switch μειώνει την κίνηση - συγκρούσεις και αυξάνει την επίδοση του δικτύου.

Τα switches έχουν την δυνατότητα να εργάζονται σε δυο καταστάσεις λειτουργίας:

Store and forward: Εξετάζεται όλο το πλαίσιο και σε περίπτωση που υπάρχει λάθος στο πεδίο ακολουθίας ελέγχου πλαισίου (Frame Check sequence , FCS) το πλαίσιο απορρίπτεται.

Cut-through : Εξετάζεται από το πλαίσιο μόνο η διεύθυνση προορισμού (destination MAC) και προβαίνει στην προώθηση του πλαισίου.

Η λειτουργία Cut-through είναι γρηγορότερη από την Store and forward.

E. Switch Configuration

Για τη ρύθμιση των συσκευών Cisco (Switch ή Router) χρειάζεται να γίνει σύνδεση μεταξύ ενός υπολογιστή και της συσκευής μέσω της σειριακής θύρας του υπολογιστή και του console port της συσκευής χρησιμοποιώντας καλώδιο console.



Για πιο απλές και απομακρυσμένες ρυθμίσεις υπάρχει και η δυνατότητα σύνδεσης μέσω δικτύου αλλά και μέσω ενός modem. Αυτοί οι τρόποι σύνδεσης όμως δίνουν περιορισμένη δυνατότητα ρυθμίσεων.

Οι συσκευές Cisco δουλεύουν με δικό τους λειτουργικό σύστημα, το CISCO IOS. Είναι ένα CLI (Command Line Interface) λειτουργικό σύστημα.

Τα διάφορα επίπεδα χρήσης του δίνουν περισσότερη ασφάλεια στην όλη διαδικασία ρύθμισης τους.

Ξεκινώντας την σύνδεση, η συσκευή βρίσκεται στο επίπεδο απλής χρήσης (User Exec Mode). Εδώ η δυνατότητες είναι περιορισμένες. Σε αυτό το επίπεδο η γραμμή εντολών (command prompt) είναι της εξής μορφής:

Switch>

(όπου η λέξη Switch είναι το όνομα της συσκευής)

Με τη χρήση της εντολής **enable** ο χρήστης μεταφέρεται στο επίπεδο **privilege mode**. Εδώ οι δυνατότητες αυξάνονται και η γραμμή εντολών αλλάζει σε:

Switch#

Η εντολή **disable** μεταφέρει τον χρήστη στο προηγούμενο επίπεδο (User Exec Mode).

Πιο κάτω φαίνονται κάποιες εντολές για τη περιήγηση στο λειτουργικό και για βασικές ρυθμίσεις.

Switch #reload (Επανεκκίνηση της συσκευής)

Switch >enable (Μεταφορά σε privilege mode user mode)

Switch # (Privilege mode)

Switch #disable (Επιστροφή σε user mode από privilege mode)

Switch > (User Mode)

Switch #configure terminal (Μεταφορά σε global configuration mode)

Switch (config)# (Global Configuration Mode)

Switch #copy running-config startup-config (Αντιγράφει τις τρέχουσες ρυθμίσεις (RAM) στο αρχείο ρυθμίσεων (NVRAM) για μόνιμη αποθήκευση).

Switch (config)#hostname MySwitch (Αλλάζει το όνομα της συσκευής σε MySwitch)

Switch (config)#enable password <password>

Switch (config)#enable secret <password> (καθορισμός κωδικού πρόσβασης στο privilege mode – με κρυπτογράφηση)

Switch(config)# line console 0 (Είσοδο στο επίπεδο για ρύθμιση της σειριακής σύνδεσης με console καλώδιο, όπως καθορισμού κωδικού πρόσβασης)

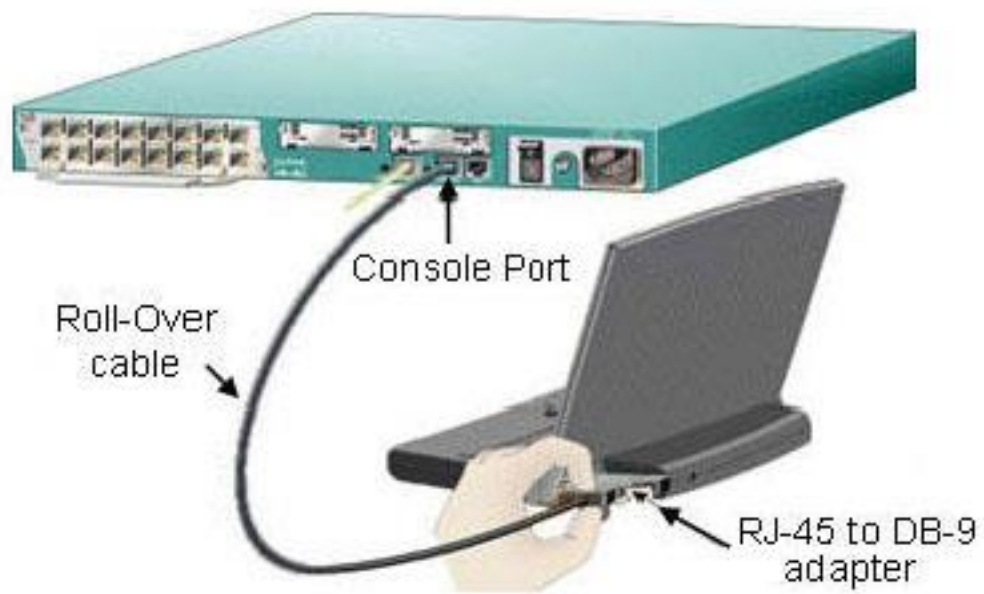
Switch(config-line)#

Switch(config-line)# exit (Επιστροφή στο επίπεδο global configuration)

Switch(config)#

Switch(config-line)# interface FastEthernet 0/1 (Είσοδος στο επίπεδο ρύθμισης των θυρών σύνδεσης των συσκευών (Ethernet Ports). Ο αριθμός 0/1 δηλώνει τη πρώτη θύρα. Ακολουθούν οι αντίστοιχοι αριθμοί για τις υπόλοιπες)

Switch(config-if)#



5. Επίπεδο Δικτύου

A. Πρωτόκολλο IP

Το Πρωτόκολλο Διαδικτύου IP (Internet Protocol), αποτελεί το κύριο πρωτόκολλο επικοινωνίας για τη μετάδοση δεδομενογραμμάτων (datagrams), δηλαδή πακέτων δεδομένων, στο διαδίκτυο. Το Πρωτόκολλο IP είναι υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων ανάμεσα στα διάφορα δίκτυα.

Το Πρωτόκολλο IP, ανήκει στο Επίπεδο Δικτύου, στο Μοντέλο TCP/IP. Καθορίζει τη μορφή των πακέτων που στέλνονται μέσω ενός διαδικτύου, καθώς και τους μηχανισμούς που χρησιμοποιούνται για την προώθηση των πακέτων από έναν υπολογιστή προς έναν τελικό προορισμό μέσω ενός ή περισσότερων δρομολογητών (Routers). Γι' αυτούς τους σκοπούς, το IP, χρησιμοποιεί συγκεκριμένες μεθόδους διευθυνσιοδότησης και δομές για την συμπίεση των πακέτων δεδομένων.

Το Πρωτόκολλο IP εισήχθη από τους Vint Cerf και Bob Kahn το 1974. Συνδέεται στενά με το Πρωτόκολλο Ελέγχου Μετάδοσης (TCP), με αποτέλεσμα όλα τα πρωτόκολλά του Διαδικτύου να αναφέρονται απλά ως TCP/IP.

Η πρώτη έκδοση του Πρωτοκόλλου IP, ήταν η έκδοση 4 (IPv4) η οποία επικρατεί μέχρι και σήμερα σε όλο το Διαδίκτυο. Ωστόσο, λόγω του ότι δεν επαρκούν πλέον οι διευθύνσεις, τα τελευταία χρόνια, έχει αναπτυχθεί η νέα έκδοση του πρωτοκόλλου, η έκδοση 6 (IPv6), η οποία είναι εν ενεργεία και χρησιμοποιείται εξαπλωνόμενη σε όλο τον κόσμο.

Υπηρεσίες του Πρωτοκόλλου IP

Το Πρωτόκολλο IP, είναι υπεύθυνο για τη διευθυνσιοδότηση των κόμβων και την δρομολόγηση των πακέτων από έναν υπολογιστή προς έναν τελικό προορισμό, κατά μήκος ενός ή περισσότερων δικτύων. Για το σκοπό αυτό, το πρωτόκολλο IP, καθορίζει ένα σύστημα διευθυνσιοδότησης, το οποίο έχει δύο λειτουργίες. Έτσι κάθε πακέτο IP, αποτελείται από μια κεφαλίδα και στη συνέχεια ακολουθούν τα δεδομένα. Στη κεφαλίδα αυτή εμπεριέχονται πληροφορίες: πρώτον, για τα δεδομένα που εμπεριέχονται στο πακέτο και δεύτερον, οι διευθύνσεις αποστολέα και προορισμού. Η διαδικασία προσθήκης της κεφαλίδας σε ένα πακέτο δεδομένων ονομάζεται **ενθυλάκωση**.

Εκτός από τον ορισμό της μορφής των αυτοδύναμων πακέτων, το Πρωτόκολλο IP ορίζει τη σημασιολογία της επικοινωνίας, και χρησιμοποιεί τον όρο βέλτιστη προσπάθεια, για να περιγράψει την υπηρεσία που παρέχει. Ουσιαστικά το πρότυπο αυτό ορίζει, ότι παρ' όλο που το πρωτόκολλο IP κάνει τη βέλτιστη δυνατή προσπάθεια για να αποδώσει ένα πακέτο στο προορισμό του, το υποκείμενο υλικό από το οποίο είναι φτιαγμένα τα εκάστοτε δίκτυα που διασχίζει, μπορεί να συμπεριφερθεί λανθασμένα. Έτσι, το πρωτόκολλο, δεν εγγυάται ότι θα μπορέσει να αντιμετωπίσει τα παρακάτω προβλήματα:

Αλλοίωση δεδομένων

Απώλεια αυτοδύναμου πακέτου

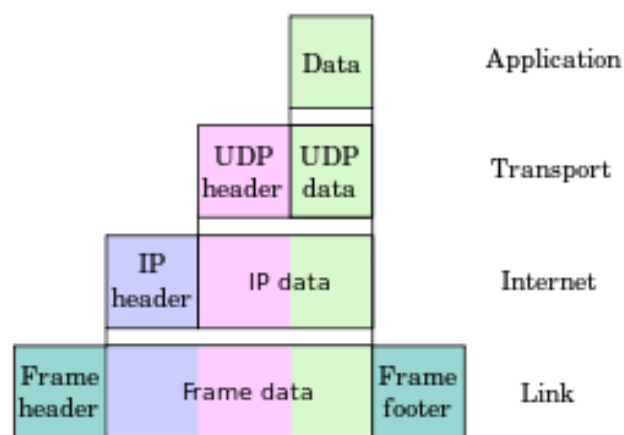
Επανάληψη αυτοδύναμου πακέτου

Επίδοση με καθυστέρηση ή εκτός σειράς.

Για την αντιμετώπιση του κάθε ενός από αυτά τα σφάλματα, χρειάζονται πρόσθετα, υψηλότερα επίπεδα λογισμικού πρωτοκόλλων.

Η μόνη διαβεβαίωση που μπορεί να δώσει το πρωτόκολλο IP στην έκδοση 4 (IPv4), είναι το αν τα μπιτ της κεφαλίδας έχουν υποστεί αλλοίωση ή όχι κατά τη διάρκεια της μεταφοράς. Αυτή η πληροφορία εμπεριέχεται σε ένα πεδίο της κεφαλίδας του IP πακέτου, που ονομάζεται Άθροισμα Ελέγχου Κεφαλίδας (Header Checksum). Κάνοντας χρήση του checksum, μπορεί να διαπιστωθεί εάν η κεφαλίδα έχει μεταφερθεί σωστά ή όχι, και αναλόγως το πακέτο απορρίπτεται ή όχι.

Στην έκδοση 6 (IPv6) ωστόσο, έχει εγκαταλειφθεί η χρήση του αθροίσματος ελέγχου κεφαλίδας, προς όφελος της ταχείας προώθησης μέσω ορισμένων στοιχείων δρομολόγησης στο δίκτυο.



Ενθυλάκωση των δεδομένων(πράσινο χρώμα) μιας εφαρμογής.

B. Διευθύνσεις IPV4

Για τη σωστή επικοινωνία μέσα σε ένα δίκτυο ή μεταξύ πολλών δικτύων είναι αναγκαία η ταυτοποίηση όλων των συσκευών που είναι συνδεδεμένα σε αυτά.

Η φυσική διεύθυνση (MAC Address) είναι χρήσιμη μέχρι το επίπεδο συνδέσμου (Link Layer). Με απλά λόγια θα μπορούσαμε να πούμε ότι η φυσική διεύθυνση χρησιμοποιείται για μετάδοση δεδομένων εσωτερικά σε ένα δίκτυο. Εκεί που την ευθύνη μετάδοσης έχουν οι μεταγωγείς.

Εκτός από την φυσική διεύθυνση, που είναι μοναδική στον κόσμο, οι συσκευές που είναι ενωμένες με δίκτυα έχουν και λογική διεύθυνση, το IP Address.

Αυτή η διεύθυνση, στην έκδοση 4 IPV4, αποτελείται από 32 δυαδικούς αριθμούς, χωρισμένους σε τέσσερις οκτάδες με τελεία. Παράδειγμα η διεύθυνση 10101100.10101000.00011100.00101011 είναι μία έγκυρη λογική διεύθυνση που μπορεί να έχει ένας υπολογιστής που είναι συνδεδεμένος σε ένα δίκτυο. Η πιο πάνω διεύθυνση μπορεί να γραφτεί και στο δεκαδικό σύστημα για να είναι πιο εύκολα κατανοητή σε εμάς. Στην

δεκαδική μορφή θα γραφόταν 172.168.28.43. Αυτό προκύπτει αν μετατρέψουμε τον κάθε οκταψήφιο δυαδικό αριθμό σε δεκαδικό. Στο πιο πάνω παράδειγμα ο δυαδικός 10101100 αντιστοιχεί με τον δεκαδικό 172, ο 10101000 με τον 168, ο 00011100 με το 28 και ο 00101011 με το 43.

Οι λογικές διευθύνσεις IP έχουν διπλή έννοια. Ένα κομμάτι τους φανερώνει τον αριθμό του δικτύου που βρίσκεται η συσκευή και ένα άλλο κομμάτι δηλώνει την μοναδική ταυτότητα που έχει η συσκευή στο δίκτυο.

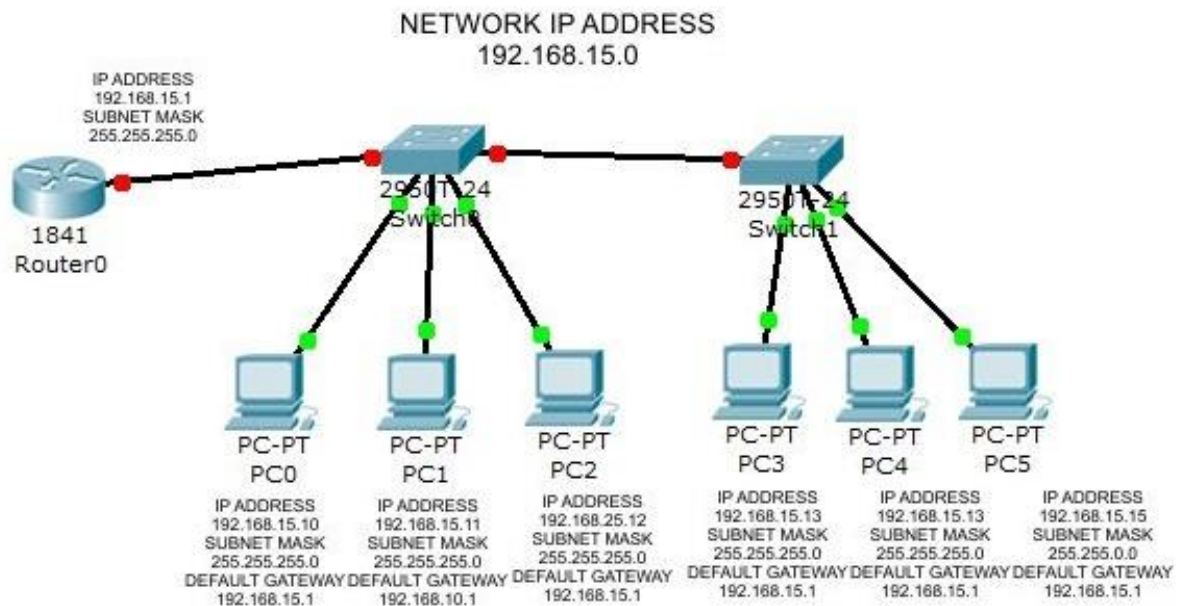
Πόσοι και ποιοι αριθμοί δηλώνουν τα πιο πάνω, καθορίζεται από ένα άλλο αριθμό, την μάσκα του δικτύου (Subnet Mask). Αυτός ο αριθμός αποτελείται από 32 δυαδικά ψηφία χωρισμένα σε οκτάδες, όπως η διεύθυνση IP. Έχει ένα αριθμό με διαδοχικά 1 (αρχίζοντας από αριστερά) ακολουθούμενα με διαδοχικά 0. Ο αριθμός των 1 καθορίζει τον αριθμό των ψηφίων της διεύθυνσης IP που αντιστοιχεί στο δίκτυο και ο αριθμός των 0 καθορίζει τον αριθμό των ψηφίων που αντιστοιχούν στην μοναδική ταυτότητα της συσκευής στο δίκτυο.

Για παράδειγμα η διεύθυνση 10101100.10101000.00011100.00101011 (172.168.28.43) που έχει Subnet Mask 11111111.11111111.00000000.00000000 (255.255.0.0) μας λέει ότι η συσκευή ανήκει στο δίκτυο 172.168.0.0 και έχει σαν ταυτότητα στο δίκτυο αυτό τον αριθμό 28.43.

Για να μπορέσει να λειτουργήσει σωστά ένα δίκτυο θα πρέπει όλες οι συσκευές να έχουν το ίδιο Subnet Mask και ο καθορισμένος από αυτόν αριθμός δικτύου να είναι ο ίδιος και η αριθμός που αντιστοιχεί στην ταυτότητα του να είναι μοναδικός για κάθε συσκευή.

Μια Τρίτη και σημαντική παράμετρος για να μπορεί μία συσκευή να επικοινωνεί με άλλα δίκτυα είναι να καθοριστεί σωστά ο αριθμός Προεπιλεγμένης Πύλης (Default Gateway). Αυτός ο αριθμός δεν είναι άλλος από τη φυσική διεύθυνση του Δρομολογητή (Router). Αν δεν καθοριστεί σωστά

το Default Gateway τότε η συσκευή δεν θα μπορεί να επικοινωνεί με άλλη συσκευή που βρίσκεται σε άλλο δίκτυο. Θα περιοριστεί στην επικοινωνία με συσκευές που ανήκουν στο ίδιο με αυτή δίκτυο.



Πιο πάνω βλέπουμε ένα δίκτυο με αριθμό 192.168.15.0. Εδώ έχουμε μερικές λάθος ρυθμίσεις.

Ο δρομολογητής έχει ρυθμιστεί να έχει IP 168.168.15.1 και Subnet Mask (SM) 255.255.255.0

Το PC0 είναι ρυθμισμένο σωστά με IP 192.168.15.11 SM 255.255.255.0 και Default Gateway (DG) 192.168.15.1 άρα θα μπορεί να επικοινωνεί σωστά και μέσα και έξω από το δίκτυο.

Το PC1 έχει πρόβλημα με το DG. Έχει ρυθμιστεί λάθος άρα δεν θα μπορεί να επικοινωνεί εκτός του δικτύου. Εντός του δικτύου δεν θα έχει πρόβλημα.

Το PC2 έχει λάθος IP. Με βάση το SM τα πρώτα 24 ψηφία (οι 3 πρώτοι δεκαδικοί αριθμοί) των διευθύνσεων ανήκουν στο δίκτυο. Γι' αυτό όλες οι συσκευές για να ανήκουν σε αυτό το δίκτυο θα πρέπει να έχουν IP που να αρχίζει με 192.168.15. Το τελευταίο ψηφίο μπορεί να είναι οτιδήποτε (από το 1 μέχρι το 254. Θα μιλήσω πιο κάτω γιατί) και σίγουρα να είναι μοναδικό στο δίκτυο.

Τα PC3 και PC4 έχουν πρόβλημα γιατί έχουν το ίδιο IP. Αυτό προκαλεί σύγκρουση (IP Conflict), δεν αφήνει τις συσκευές να επικοινωνούν στην πιο απλή περίπτωση και μπορεί να διαταράξουν όλο το δίκτυο στην χειρότερη.

Τέλος το PC5 έχει καθορισμένα λάθος το SM. Άρα ούτε και αυτό θα μπορεί να επικοινωνεί με άλλες συσκευές.

Τις Διευθύνσεις IP με το SM μπορούμε να τις συναντήσουμε και με μια άλλη συνδυασμένη μορφή, με τη χρήση προθέματος (prefix). Παράδειγμα το IP 192.168.15.11 με SM 255.255.255.0 μπορούμε να το γράψουμε και σαν 192.168.15.11/24. Το πρόθεμα /24 δηλώνει ότι τα πρώτα 24 δυαδικά ψηφία της διεύθυνσης ανήκουν στο δίκτυο. Τα υπόλοιπα 8 ανήκουν στην ταυτότητα της συσκευής.

Η χρήση των διευθύνσεων δεν είναι ανεξέλεγκτη. Η κατηγοριοποίηση των διευθύνσεων σε κλάσεις, σε ιδιωτικές και δημόσιες και η δέσμευση κάποιων διευθύνσεων διασφαλίζει την ομαλή χρήση τους και επικοινωνία σε όλο τον κόσμο.

Κλάσεις IP

Οι διευθύνσεις IP είναι χωρισμένες σε 5 κλάσεις. Οι βασικές κλάσεις είναι οι πρώτες τρεις. Οι άλλες δύο είναι δεσμευμένες για ειδική χρήση και ειδικές περιπτώσεις και δεν θα μας απασχολήσουν.

Κλάση A:

Σε αυτή τη κλάση ανήκουν όλες οι διευθύνσεις μεταξύ 0.0.0.0 και 127.0.0.0. Αυτή η κλάση διευθύνσεων έχει προκαθορισμένο Subnet Mask 255.0.0.0. Αυτό σημαίνει ότι μόνο τα πρώτα 8 δυαδικά ψηφία της διεύθυνσης ανήκουν στο δίκτυο. Όλα τα άλλα 24 μπορούν να χρησιμοποιηθούν για διευθύνσεις συσκευών στο δίκτυο. Αυτή η κλάση χρησιμοποιείται για μεγάλα δίκτυα που έχουν πολλούς χρήστες συνδεδεμένους σε αυτά. Με 24 δυαδικά ψηφία μπορούμε να σχηματίσουμε $2^{24} = 16,777,216$ συνδυασμούς. Από αυτούς δεν μπορούν να χρησιμοποιηθούν ο πρώτος (αριθμός δικτύου) και ο τελευταίος (broadcast διεύθυνση) άρα σε ένα δίκτυο που χρησιμοποιεί κλάση A διευθύνσεις μπορούν να συνδεθούν 16,777,214 συσκευές. Παράδειγμα:

Το δίκτυο με αριθμό 10.0.0.0 (00001010.00000000.00000000.00000000) έχει εύρος διαθέσιμων διευθύνσεων από το 10.0.0.1 (00001010.00000000.00000000.00000001) μέχρι το 10.255.255.254 (00001010.11111111.11111111.11111110). Η πρώτη διεύθυνση με 0 στα τελευταία 24 ψηφία και η τελευταία με 1 σε όλα τα τελευταία 24 ψηφία (10.255.255.255 00001010.11111111.11111111.11111111) δεν μπορούν να χρησιμοποιηθούν.

Κλάση B:

Σε αυτή τη κλάση ανήκουν όλες οι διευθύνσεις μεταξύ 128.0.0.0 μέχρι την 191.255.0.0. Αυτή η κλάση διευθύνσεων έχει προκαθορισμένο Subnet Mask 255.255.0.0. Αυτό σημαίνει ότι τα πρώτα 16 δυαδικά ψηφία της διεύθυνσης ανήκουν στο δίκτυο. Όλα τα άλλα 16 μπορούν να χρησιμοποιηθούν για διευθύνσεις συσκευών στο δίκτυο. Με 16 δυαδικά ψηφία μπορούμε να σχηματίσουμε $2^{16} = 65,536$ συνδυασμούς. Από αυτούς δεν μπορούν να χρησιμοποιηθούν ο πρώτος (αριθμός δικτύου) και ο τελευταίος (broadcast διεύθυνση) άρα σε ένα δίκτυο που χρησιμοποιεί κλάση B διευθύνσεις μπορούν να συνδεθούν 65,534 συσκευές. Παράδειγμα:

Το δίκτυο με αριθμό 172.49.0.0 (10101100.00110001.00000000.00000000) έχει εύρος διαθέσιμων διευθύνσεων από το 172.49.0.1 (10101100.00110001.00000000.00000001) μέχρι το 172.49.255.254 (10101100.00110001.11111111.11111110). Η πρώτη διεύθυνση με 0 στα τελευταία 16 ψηφία και η τελευταία με 1 σε όλα τα τελευταία 16 ψηφία (172.49.255.255 10101100.00110001.11111111.11111111) δεν μπορούν να χρησιμοποιηθούν.

Κλάση C:

Σε αυτή τη κλάση ανήκουν όλες οι διευθύνσεις μεταξύ 192.0.0.0 μέχρι την 223.255.255.0. Αυτή η κλάση διευθύνσεων έχει προκαθορισμένο Subnet Mask 255.255.255.0. Αυτό σημαίνει ότι τα πρώτα 24 δυαδικά ψηφία της διεύθυνσης ανήκουν στο δίκτυο. Μόνο τα άλλα 8 μπορούν να χρησιμοποιηθούν για διευθύνσεις συσκευών στο δίκτυο. Με 8 δυαδικά ψηφία μπορούμε να σχηματίσουμε $2^8 = 256$ συνδυασμούς. Από αυτούς δεν μπορούν να χρησιμοποιηθούν ο πρώτος (αριθμός δικτύου) και ο τελευταίος (broadcast διεύθυνση) άρα σε ένα δίκτυο που χρησιμοποιεί κλάση C διευθύνσεις μπορούν να συνδεθούν 254 συσκευές. Παράδειγμα:

Το δίκτυο με αριθμό 192.168.10.0 (11000000.10101000.00001010.00000000) έχει εύρος διαθέσιμων διευθύνσεων από το 192.168.10.1 (11000000.10101000.00001010.00000001) μέχρι το 192.168.10.254 (11000000.10101000.00001010.11111110). Η πρώτη διεύθυνση με 0 στα τελευταία 8 ψηφία και η τελευταία με 1 σε όλα τα τελευταία 8 ψηφία (192.168.10.255 11000000.10101000.00001010.11111111) δεν μπορούν να χρησιμοποιηθούν.

Κλάση D:

Σε αυτή τη κλάση ανήκουν όλες οι διευθύνσεις μεταξύ 224.0.0.0 μέχρι την 239.0.0.0. Αυτές οι διευθύνσεις χρησιμοποιούνται για multicast.

Κλάση E:

Σε αυτή τη κλάση ανήκουν όλες οι διευθύνσεις μεταξύ 240.0.0.0 μέχρι την 255.0.0.0. Αυτές οι διευθύνσεις είναι δεσμευμένες για γενική χρήση. Συνήθως έχουν πειραματική χρήση.

Ειδικές κατηγορίες IP διευθύνσεων

Loopback διευθύνσεις (127.0.0.0 - 127.255.255.254): Χρησιμοποιούνται για αυτοέλεγχο. Αν δεν μπορώ να επικοινωνήσω με τον εαυτό μου, πως θα μπορέσω να επικοινωνήσω με άλλους; Αποστολή μηνυμάτων στον εαυτό μου για να διαφανεί ότι όλα τα πρωτόκολλα λειτουργούν σωστά.

Link-Local διευθύνσεις (169.254.0.1 - 169.254.255.254): Αυτές τις διευθύνσεις τις παίρνει από μόνη της μία συσκευή όταν υπάρχει πρόβλημα επικοινωνίας με τον δρομολογητή (ή τον υπεύθυνο server που χειρίζεται τις διευθύνσεις σε ένα δίκτυο).

Test-Net διευθύνσεις (192.0.2.0 – 192.0.2.254): Είναι διευθύνσεις που χρησιμοποιούνται για εκπαιδευτικούς σκοπούς ή για επίδειξη δικτύων.

Ιδιωτικές και δημόσιες IP διευθύνσεις

Η όλο και αυξανόμενη χρήση του διαδικτύου, δεν δίνει την δυνατότητα σε κάθε χρήστη του να έχει μία μοναδική διεύθυνση κατά την χρήση του.

Για αυτό κυρίως τον λόγο οι διευθύνσεις είναι χωρισμένες σε ιδιωτικές και δημόσιες.

Μία συσκευή που είναι συνδεδεμένη σε ένα δίκτυο έχει μία μοναδική διεύθυνση εσωτερικά του δικτύου. Αυτές τις διευθύνσεις τις διαχειρίζεται ο δρομολογητής (router). Όταν η συσκευή θα επικοινωνήσει εκτός δικτύου, τότε χρησιμοποιεί μία κοινή με το υπόλοιπο δίκτυο,

διεύθυνση, τη δημόσια. Την αλλαγή αυτή την κάνει η διαδικασία Network Address Translator (NAT) που είναι εγκατεστημένη στους δρομολογητές. Τις δημόσιες διευθύνσεις τις χειρίζεται ο οργανισμός που μας συνδέει με το διαδίκτυο (ISP).

Οι ιδιωτικές διευθύνσεις που μπορούμε να χρησιμοποιούμε σε ένα δίκτυο είναι περιορισμένες.

Αν χρησιμοποιούμε διευθύνσεις κλάσης A τότε απαραίτητα μόνο μία επιλογή έχουμε, την διεύθυνση δικτύου 10.0.0.0.

Αν χρησιμοποιούμε διευθύνσεις κλάσης B, μπορούμε να έχουμε μεταξύ 172.16.0.0 και 172.31.255.255, δεκαέξι δηλαδή διαφορετικές επιλογές (αφού μόνο το δεύτερο μέρος της διεύθυνσης μπορεί να αλλάξει από 16 μέχρι το 31).

Αν χρησιμοποιούμε διευθύνσεις κλάσης C, μπορούμε να έχουμε μεταξύ 192.168.0.0 και 192.168.255.255, διακόσιες πενήντα έξι διαφορετικές επιλογές (μόνο το τρίτο μέρος της διεύθυνσης μπορεί να αλλάξει από 0 σε 255).

Αυτές οι διευθύνσεις χρησιμοποιούνται μόνο εσωτερικά των δικτύων και δεν αναγνωρίζονται εκτός αυτών. Εννοείται ότι οι ίδιες διευθύνσεις μπορούν να χρησιμοποιηθούν από πολλά δίκτυα οι ίδιες χωρίς να δημιουργείται κανένα πρόβλημα.

Όταν ένα πακέτο πληροφοριών έχει διεύθυνση προορισμού μία ιδιωτική διεύθυνση, δεν αποστέλλεται από τον δρομολογητή εκτός του δικτύου αφού αναγνωρίζεται ως ιδιωτική.

Όλες οι υπόλοιπες διευθύνσεις (εκτός των ιδιωτικών και των ειδικών κατηγοριών) χρησιμοποιούνται σε όλο τον κόσμο υπό την ρύθμιση του παγκόσμιου οργανισμού IANA (Internet Assigned Numbers Authority). Γίνεται διαμοιρασμός σε 5 μεγάλες γεωγραφικά διαμερίσματα του κόσμου, τα οποία με τη σειρά τους τα διαχωρίζουν σε μικρότερες περιοχές και στο τέλος φτάνουν στους οργανισμούς ή εταιρίες που λειτουργούν ως παροχείς διαδικτύου για να τις μοιράζουν στους πελάτες τους.

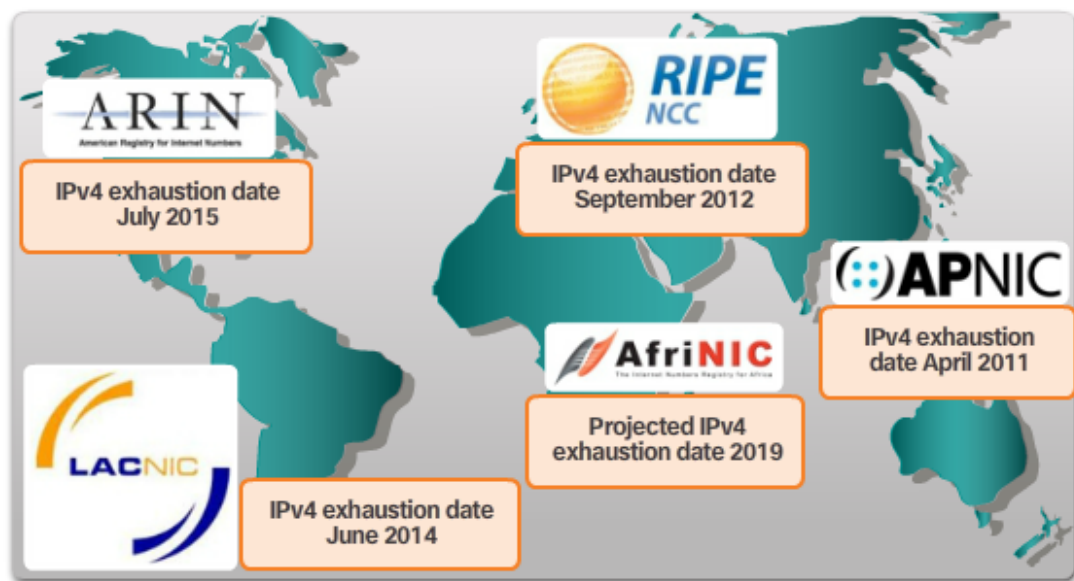
Με τη ραγδαία αύξηση όμως των τελευταίων ετών στην χρήση του διαδικτύου, ο αριθμός των διευθύνσεων δεν είναι αρκετός. Για αυτό τον λόγο τα τελευταία χρόνια έχει δημιουργηθεί νέα έκδοση διευθύνσεων η IPv6 ή οποία μπορεί να καλύψει τις σημερινές και άμεσα μελλοντικές ανάγκες.

Γ. Διευθύνσεις IPV6

Το IPv6 έχει σχεδιαστεί για να είναι ο διάδοχος του IPv4. Το IPv6 έχει ένα μεγαλύτερο χώρο διευθύνσεων 128 δυαδικών ψηφίων, το οποίο προβλέπει 340 undecillion διευθύνσεις. (Αυτός είναι ο αριθμός 340, ακολουθούμενο από 36 μηδενικά). Όταν η IETF άρχισε την ανάπτυξη του διαδόχου του IPv4, προσπάθησε να εξαλείψει τους περιορισμούς της έκδοσης IPv4 και περιλαμβάνει πρόσθετες βελτιώσεις.

Ανάγκη για IPv6

Η εξάντληση των διευθύνσεων IPv4 ήταν το κίνητρο για τη μετάβαση σε νέα έκδοση, την IPv6. Από την στιγμή που η Αφρική, η Ασία και άλλες περιοχές του κόσμου άρχισαν να συνδέονται με το Διαδίκτυο, δεν υπάρχουν αρκετές διευθύνσεις IPv4 για να υποστηρίξουν αυτή την ανάπτυξη. Όπως φαίνεται στο σχήμα, τέσσερις από τις πέντε γεωγραφικές περιφέρειες έχουν ξεμείνει από διευθύνσεις IPv4.



Το IPv4 έχει ένα θεωρητικό μέγιστο αριθμό 4,3 δισεκατομμύρια διευθύνσεις. Οι ιδιωτικές διευθύνσεις σε συνδυασμό με μετάφρασης διευθύνσεων δικτύου (NAT) έχουν συμβάλει στην επιβράδυνση την εξάντληση των διευθύνσεων IPv4. Ωστόσο το NAT δημιουργεί προβλήματα σε πολλές εφαρμογές και έχει τους περιορισμούς που εμποδίζουν σοβαρά την peer-to-peer επικοινωνία.

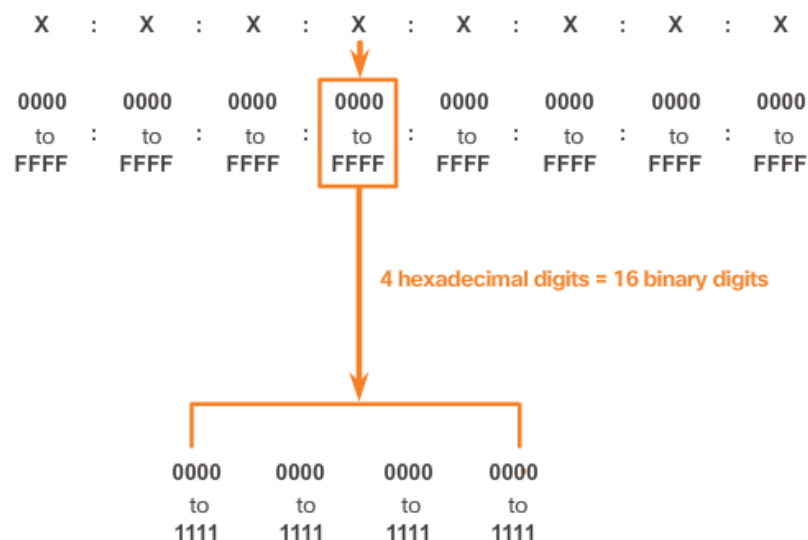
Το Διαδίκτυο του σήμερα είναι πολύ διαφορετική από ό, τι το Διαδίκτυο των τελευταίων δεκαετιών. Το Διαδίκτυο σήμερα είναι περισσότερο από ό, τι το ηλεκτρονικό ταχυδρομείο, ιστοσελίδες, και τη μεταφορά αρχείων μεταξύ υπολογιστών. Δεν θα είναι πλέον οι υπολογιστές οι μόνες συσκευές πρόσβασης στο Διαδίκτυο αλλά έχουμε και τις ταμπλέτες και τα smartphones. Το Internet εξαπλώνεται σε όλες τις συσκευές του αύριο, από αυτοκίνητα και βιοϊατρικές συσκευές, τις οικιακές συσκευές και τα φυσικά οικοσυστήματα.

Μορφή διευθύνσεων IPv6

Οι διευθύνσεις IPv6 αποτελούνται από 128 δυαδικά ψηφία (σε σύγκριση με τα 32 του IPv4).

Γράφονται με το δεξαεδαδικό σύστημα αρίθμησης στην μορφή x:x:x:x:x:x όπου κάθε x αντιστοιχεί σε ένα τετραψήφιο δεκαεξαδικό αριθμό (0000 – FFFF). Παράδειγμα είναι η διεύθυνση 2001:0DB8:0000:0000:ABCD:0000:0000:1234.

Ο κάθε δεκαεξαδικός αριθμός αναπαρίσταται με 4 δυαδικούς. Έτσι οι 32 δεκαεξαδικοί μπορούν να γραφτούν με 128 δυαδικούς αριθμούς.



Απλοποιημένη μορφή παρουσίασης διευθύνσεων IPv6

Οι διευθύνσεις IPv6 μπορούν να γραφτούν πιο απλά αφαιρώντας τα μηδενικά όπως φαίνεται στο πιο κάτω παράδειγμα:

Preferred	2001:0DB8:0000:1111:0000:0000:0000:0200
No leading 0s	2001: DB8: 0:1111: 0: 0: 0: 200
Compressed	2001:DB8:0:1111::200

Μπορούν να αφαιρεθούν τα μηδενικά που βρίσκονται αριστερά σε κάθε τετραψήφιο δεκαεξαδικό αριθμό (No leading 0s) ή ακόμα να αφαιρεθούν τελείως διαδοχικά μηδενικά χρησιμοποιώντας το διπλό : (::) (Compressed).

Τύποι διευθύνσεων IPv6

Όπως και οι διευθύνσεις IPv4, έτσι και αυτές του IPv6 χωρίζονται σε κάποιους τύπους:

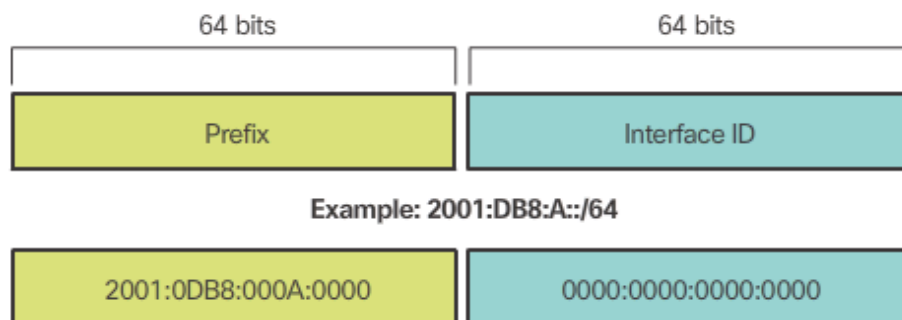
Unicast - Μια μοναδική διεύθυνση που αποκτά μία συσκευή σε ένα δίκτυο.

Multicast - Μια multicast IPv6 διεύθυνση χρησιμοποιείται για να στείλει ένα ενιαίο πακέτο IPv6 σε πολλαπλούς προορισμούς.

Anycast - Μια διεύθυνση anycast IPv6 είναι κάθε unicast διεύθυνση IPv6 που μπορεί να ανατεθεί σε πολλαπλές συσκευές. Ένα πακέτο που αποστέλλεται σε μια διεύθυνση anycast δρομολογείται στην πλησιέστερη συσκευή έχει αυτή τη διεύθυνση. Η χρήση των Anycast διευθύνσεων έχουν πολύ εξειδικευμένη χρήση.

Πρόθεμα IPv6 (Prefix)

Η έκδοση IPv6 διευθύνσεων, δεν χρησιμοποιεί τη μάσκα υποδικτύου (subnet mask). Εδώ συναντάμε μόνο τη μορφή διευθύνσεων με τη χρήση του προθέματος (prefix). Το πρόθεμα είναι αυτό που καθορίζει ποιοι αριθμοί της διεύθυνσης ανήκουν στο δίκτυο και ποιοι στη συσκευή. Η πιο συνηθισμένη μορφή διευθύνσεων είναι αυτή με το πρόθεμα /64. Τα μισά πρώτα ψηφία ανήκουν στο δίκτυο και τα άλλα μισά στη συσκευή (όπως φαίνεται στο σχήμα)



Διευθύνσεις IPv6 Unicast

Μια διεύθυνση unicast IPv6 προσδιορίζει μοναδικά μια διασύνδεση σε μια IPv6-enabled συσκευή. Ένα πακέτο που αποστέλλεται σε μια unicast διεύθυνση λαμβάνεται από τη διεπαφή που έχει εκχωρηθεί αυτή τη διεύθυνση. Παρόμοια με το IPv4, η διεύθυνση IPv6 πηγή πρέπει να είναι μια unicast διεύθυνση. Η διεύθυνση IPv6 προορισμό μπορεί να είναι είτε μια unicast ή multicast διεύθυνση.

Οι πιο κοινοί τύποι IPv6 unicast διευθύνσεις είναι παγκόσμια unicast διευθύνσεις (GUA) και unicast διευθύνσεις τοπικού συνδέσμου.

Global unicast

Μια Global unicast διεύθυνση είναι παρόμοια με μια δημόσια (public) διεύθυνση IPv4. Αυτά είναι μοναδικές στον κόσμο. Οι Global unicast διευθύνσεις μπορεί να ρυθμιστούν στατικά ή εκχωρηθούν δυναμικά. Το εύρος των Global unicast διευθύνσεων είναι 2000::/3 (τα πρώτα τρία δυαδικά ψηφία δηλαδή θα πρέπει να είναι 001).

Link Local

Οι Link Local διευθύνσεις χρησιμοποιούνται για την επικοινωνία με άλλες συσκευές στο ίδιο δίκτυο. Το εύρος των διευθύνσεων αυτών είναι FE80::/10.

Unique local

Οι unicast local διευθύνσεις είναι παρόμοιες με τις ιδιωτικές διευθύνσεις για IPv4. Οι unicast local διευθύνσεις έχουν στο εύρος των FC00 :: / 7 μέχρι FDFF :: / 7.

Δ. Δρομολογητές – Routers

Η πιο σημαντική συσκευή του επιπέδου δικτύου είναι οι δρομολογητές (routers).

Οι δρομολογητές είναι μια ηλεκτρονικές συσκευές η οποίες αναλαμβάνουν την αποστολή και λήψη πακέτων δεδομένων μεταξύ ενός ή περισσοτέρων διακομιστών, άλλων δρομολογητών και πελατών, κατά μήκος πολλαπλών δικτύων. Είναι οι συσκευές δηλαδή που ενώνουν τοπικά δίκτυα μεταξύ τους. Ουσιαστικά ο δρομολογητής οριοθετεί ένα τοπικό δίκτυο (LAN).

Η δρομολόγηση, δηλαδή η διαδικασία μεταφοράς δεδομένων από ένα σημείο σε ένα άλλο αποτελεί κεντρική λειτουργία του επιπέδου δικτύου, γίνεται με βάση διάφορα κριτήρια και τελικώς επιλέγεται μία ανάμεσα σε διάφορες πιθανές διαδρομές.

Κάθε δρομολογητής χρησιμοποιεί ένα ή περισσότερα πρωτόκολλα δρομολόγησης. Με βάση αυτά τα πρωτόκολλα ο δρομολογητής καθορίζει ποιος ή ποιοι διακομιστές ή δρομολογητές είναι οι καταλληλότεροι κάθε χρονική στιγμή και δρομολογεί τα πακέτα δεδομένων προς αυτούς. Ορισμένα πολύ γνωστά πρωτόκολλα δρομολόγησης είναι τα:

- RIP
- OSPF
- BGP
- IS-IS

Στοιχεία δρομολογητών

Παρόλο που μεταξύ τους διαφέρουν, όλοι οι δρομολογητές έχουν κάποια κοινά χαρακτηριστικά

Οι δρομολογητές είναι μικροί υπολογιστές. Λειτουργούν, με το δικό τους ο καθένας, λειτουργικό σύστημα. Διαθέτουν CPU (Κεντρική Μονάδα Επεξεργασίας) που είναι υπεύθυνη για την εκτέλεση εντολών του λειτουργικού συστήματος, λειτουργιών αρχικοποίησης, δρομολόγησης πακέτων και ελέγχου δικτυακής διασύνδεσης. Έχουν μνήμη για μόνιμη αποθήκευση του λειτουργικού συστήματος και των ρυθμίσεων αλλά και RAM για φόρτωση των δεδομένων όταν είναι σε λειτουργία.

Πρώθηση (Forwarding)

Για τις διαδικασίες πρώθησης αμιγώς του Internet Protocol (IP), ο δρομολογητής έχει κατασκευαστεί ώστε να ελαχιστοποιεί την κατάσταση της πληροφορίας που σχετίζεται με το

κάθε πακέτο. Ο κύριος σκοπός ενός δρομολογητή είναι να συνδέει πολλαπλά δίκτυα και να προωθεί τα πακέτα που προορίζονται είτε στα δίκτυά του, είτε σε άλλα δίκτυα.

Ένας δρομολογητής θεωρείται συσκευή επιπέδου 3 (Layer 3) του πρωτοκόλλου OSI, επειδή η πρωταρχική απόφαση προώθησης βασίζεται στις πληροφορίες του IP πακέτου Layer 3. Αυτή η διαδικασία είναι γνωστή ως δρομολόγηση (routing).

Όταν ένας δρομολογητής δέχεται ένα πακέτο, ψάχνει στον πίνακα (routing table) του, ώστε να κάνει το καλύτερο ταίριασμα μεταξύ της διεύθυνσης προορισμού του IP πακέτου με μια από τις διευθύνσεις δικτύου που περιέχει ο πίνακας (routing table) του. Αφού γίνει το ταίριασμα, το πακέτο “ενθυλακώνεται” και παραδίδεται στο επίπεδο 2 (Layer 2) του OSI, προκειμένου να προωθηθεί.

Ένας δρομολογητής δεν ελέγχει την ορθότητα των δεδομένων που περιέχονται στο πακέτο, αλλά μόνο τις διευθύνσεις του επιπέδου 3, έτσι ώστε να αποφασίσει για την προώθηση του πακέτου. Εκτός από τις διευθύνσεις του επιπέδου 3, ο δρομολογητής μπορεί να ελέγξει και για κάποιες άλλες πληροφορίες της επικεφαλίδας του πακέτου, όπως π.χ. το quality of service (QoS).

Αφού προωθηθεί το πακέτο, ο δρομολογητής δεν διατηρεί καμία ιστορική πληροφορία για το πακέτο, παρά μόνο την πράξη της προώθησής του, η οποία συλλέγεται ως στατιστική πληροφορία.

Ένας πίνακας (routing table) διατηρεί πληροφορίες που μπορεί να προέρχονται από διάφορες πηγές όπως:

- η προεπιλεγμένη, η στατική δρομολόγηση (default or static route), η οποία μπορεί να ρυθμιστεί χειροκίνητα. Όταν στον δρομολογητή φτάσει ένα πακέτο με προορισμό άγνωστο προς αυτόν (δεν διαθέτει πληροφορίες για αυτό το δίκτυο στο πίνακα δρομολόγησης, τότε προωθεί το πακέτο στον δρομολογητή που έχει προεπιλεγεί (default route) για περαιτέρω προώθηση μέχρι να φτάσει στον τελικό του προορισμό. Από την άλλη υπάρχει δυνατότητα στατικής δρομολόγησης (static route) για συγκεκριμένους προορισμούς. Προκαθορίζεται η δρομολόγηση για κάποιους προορισμούς και έτσι αποφεύγεται η χρήση αλγορίθμων για επιλογή δρομολόγιου. Λιγότερος χρόνος και λιγότερο κόστος υπολογιστικής ισχύς του δρομολογητή.

- το δυναμικό πρωτόκολλο δρομολόγησης (dynamic routing protocol), όπου ο δρομολογητής μαθαίνει πληροφορίες για τα κοντινά σε αυτόν δίκτυα ούτως ώστε να μπορεί να αποφασίζει που θα προωθήσει ένα πακέτο ανάλογα με τον προορισμό του. Με βάση κάποιους αλγόριθμους δρομολόγησης επιλέγεται κάθε φορά η καλύτερη οδός δρομολόγησης για κάθε πακέτο. Αυτό επιφέρει μεγαλύτερη καθυστέρηση και επιβάρυνση στην ισχύ του δρομολογητή.

Η προεπιλεγμένη δρομολόγηση (default or static route) είναι αυτή που χρησιμοποιείται όταν η δρομολόγηση όλων των προορισμών δεν διαφοροποιείται στον πίνακα (routing table). Αυτή χρησιμοποιείται στα μικρά δίκτυα όπως είναι π.χ. τα οικιακά ή τα δίκτυα μικρών επιχειρήσεων, όπου η προεπιλεγμένη δρομολόγηση απλά στέλνει όλη την κίνηση στον πάροχο - Internet Service Provider (ISP).

Η προεπιλεγμένη (η στατική) δρομολόγηση μπορεί να ρυθμιστεί χειροκίνητα ως static route, η μπορεί να αποκτηθεί από το δυναμικό πρωτόκολλο δρομολόγησης (dynamic routing protocol), η από το DHCP. Ο δρομολογητής μπορεί να χρησιμοποιηθεί τόσο ως DHCP client, όσο και ως DHCP server.

Ένας δρομολογητής μπορεί να τρέξει περισσότερα από ένα πρωτόκολλα δρομολόγησης ταυτόχρονα, ειδικά όταν λειτουργεί ως αυτόνομο σύστημα δρομολόγησης που βρίσκεται στα όρια μεταξύ των τμημάτων ενός δικτύου, το οποίο καλείται να τρέχει διαφορετικά πρωτόκολλα δρομολόγησης. Σε αυτήν την περίπτωση, η επανακατανομή (redistribution) μπορεί να χρησιμοποιηθεί για το διαμοιρασμό της πληροφορίας μεταξύ των διαφορετικών πρωτοκόλλων που τρέχουν στον ίδιο δρομολογητή.

Ε. Ρυθμίσεις Router CISCO

Όπως και για τη ρύθμιση των switch της CISCO έτσι και για τη ρύθμιση των routers χρειάζεται σύνδεση μεταξύ ενός υπολογιστή και της συσκευής μέσω της σειριακής θύρας του υπολογιστή και του console port της συσκευής χρησιμοποιώντας καλώδιο console.

Για πιο απλές και απομακρυσμένες ρυθμίσεις υπάρχει και η δυνατότητα σύνδεσης μέσω δικτύου αλλά και μέσω ενός modem. Αυτοί οι τρόποι σύνδεσης όμως δίνουν περιορισμένη δυνατότητα ρυθμίσεων.

Οι συσκευές Cisco δουλεύουν με δικό τους λειτουργικό σύστημα, το CISCO IOS. Είναι ένα CLI (Command Line Interface) λειτουργικό σύστημα.

Μερικές βασικές εντολές και ρυθμίσεις που μπορούμε να κάνουμε στα router της CISCO είναι:

Router#**reload** Επανεκκίνηση της συσκευής

Router>**enable** Μεταφορά στο privilege mode από user mode
Router# Privilege mode

Router#**disable** Επιστροφή στο user mode από το privilege mode
Router> User Mode

Router#**configure terminal** Μεταφορά στο global configuration mode.
Router(config)# Global Configuration Mode

Router#**copy running-config startup-config** Αντιγραφή των αλλαγών στις ρυθμίσεις από τη RAM στο startup configuration file (NVRAM) για μόνιμη αποθήκευση και χρήση των νέων ρυθμίσεων όταν ξαναξεκινήσει.

Router(config)#**hostname MyRouter** Αλλαγή ονόματος της συσκευής

Router(config)#**enable password <password>** καθορισμός κωδικού πρόσβασης για το privilege mode – χωρίς κρυπτογράφηση

Router(config)#**enable secret <password>** καθορισμός κωδικού πρόσβασης για το privilege mode – με κρυπτογράφηση

Καθορισμός κωδικού για το Console

```
Router(config)#line console 0
Router(config-line)#password <password>
Router(config-line)#login
```

Καθορισμός κωδικού για το Virtual Terminal (εικονικό interface για σύνδεση μέσω δικτύου)

```
Router(config)#line vty 0 4
Router(config-line)#password <password>
Router(config-line)#login
```

Καθορισμός κωδικού για το Auxiliary Port (για σύνδεση μέσω modem)

```
Router(config)#line aux 0
Router(config-line)#password <password>
Router(config-line)#login
```

```
Router(config)#service password-encryption    εφαρμογή κρυπτογράφησης σε
όλους τους κωδικούς
```

Ρυθμίσεις Interface

```
Router(config)#interface <Interface_Type> <Int_Port_No>
Router(config-if)#description <Description identifying the purpose of the
interface>
Router(config-if)#ip address <IP_Address> <Subnet_Mask>
Router(config-if)#no shutdown
Router(config-if)#clock rate <speed>          Μόνο για σειριακές συνδέσεις DCE.
Router(config-if)#exit
```

Παράδειγματα:

```
Router(config)#interface FastEthernet 0/0
Router(config-if)#Description connection to Admin LAN
Router(config-if)#ip Address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

```
Router(config)#interface Serial 0/0/0
Router(config-if)#Description Connection to router 2
Router(config-if)#ip Address 192.168.2.1 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

Default Routes

```
Router(config)#ip route 0.0.0.0 0.0.0.0 <Interface-Name>
Router(config)#ip route 0.0.0.0 0.0.0.0 <Next Hop IP>
```

DHCP Configuration

```
Router(config)#ip dhcp excluded-address <low_ip> <high_ip>
Router(config)#ip dhcp pool <POOL_NAME>
Router(dhcp-config)#network <net_id> <mask | #_net_bits>
Router(dhcp-config)#default-router <dg_ip>
Router(dhcp-config)#dns-server <dns1_ip>...<dns8_ip>
Router(dhcp-config)#domain-name <domain_name>
Router(dhcp-config)#lease { <#_days> <#_hrs> <#_mins> | infinite}
```

Παράδειγμα:

```
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10
Router(config)#ip dhcp pool ADMIN_LAN
Router(dhcp-config)#network 172.16.0.0 255.255.0.0
```

```
Router(dhcp-config)#default-router 172.16.1.1  
Router(dhcp-config)#dns-server 172.16.1.5 10.10.0.5  
Router(dhcp-config)#domain-name cisco.com  
Router(dhcp-config)#lease 0 8
```

6. Επίπεδο Μεταφοράς (Transport Layer)

A. Transport Layer

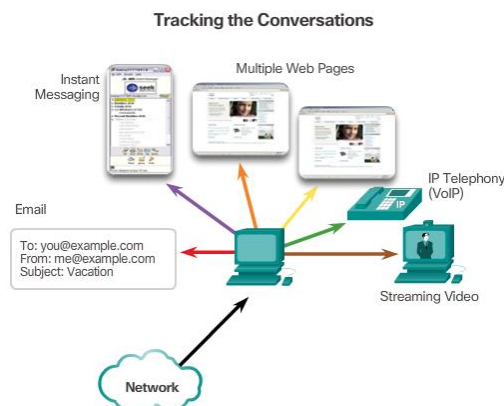
Τα δεδομένων δικτύων και το Διαδίκτυο παρέχουν αξιόπιστη επικοινωνία μεταξύ των ανθρώπων. Σε μία συσκευή οι άνθρωποι μπορούν να χρησιμοποιούν πολλαπλές εφαρμογές και υπηρεσίες όπως το ηλεκτρονικό ταχυδρομείο, το διαδίκτυο και την άμεση ανταλλαγή μηνυμάτων. Τα δεδομένα από κάθε μια από αυτές τις εφαρμογές είναι συσκευασμένα και μεταφέρονται και παραδίδονται στη συσκευή προορισμού με την κατάλληλη εφαρμογή.

Οι μέθοδοι που περιγράφονται στο επίπεδο μεταφοράς (Transport layer) του OSI δέχονται δεδομένα από το επίπεδο εφαρμογής και τα προωθούν στο επίπεδο δικτύου. Ένας υπολογιστής (αποστολέας) επικοινωνεί με έναν υπολογιστή (παραλήπτη) για να καθορίσουν τους κανόνες επικοινωνίας όπως, πώς να χωριστούν τα δεδομένα σε τμήματα, να βεβαιωθούν ότι κανένα από τα τμήματα δεν έχει χαθεί και να γίνει έλεγχος ότι όλα τα δεδομένα έφτασαν κανονικά.

Το επίπεδο μεταφοράς είναι υπεύθυνο για τη δημιουργία μιας προσωρινής επικοινωνίας μεταξύ δύο εφαρμογών και για την παροχή δεδομένων μεταξύ τους. Τα πρωτόκολλα αυτού του επιπέδου παρέχουν υπηρεσίες επικοινωνίας host-to-host για τις εφαρμογές όπως η σύνδεση με στήριξη της ροής δεδομένων, την αξιοπιστία, έλεγχο ροής, και πολυπλεξίας.

Εντοπισμός Μεμονωμένων Συζητήσεων (Tracking Individual Conversations)

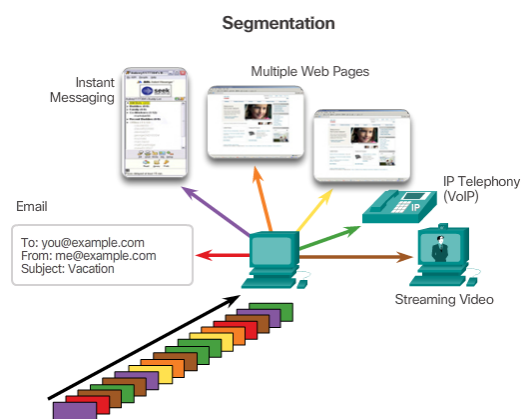
Στο επίπεδο μεταφοράς κάθε σύνολο δεδομένων που ρέει ανάμεσα σε μια εφαρμογή πηγής και μια εφαρμογή προορισμού είναι γνωστή ως μια συνομιλία. Μια συσκευή μπορεί να έχει πολλαπλές εφαρμογές που επικοινωνούν μέσω του δικτύου ταυτόχρονα. Κάθε μία από αυτές τις εφαρμογές επικοινωνεί με μία ή περισσότερες εφαρμογές σε έναν ή περισσότερους απομακρυσμένους υπολογιστές. Είναι ευθύνη του επιπέδου μεταφοράς να διατηρεί και να παρακολουθεί αυτές τις πολλαπλές συζητήσεις.



Διαχωρισμός και συναρμολόγηση δεδομένων (Segmenting Data and Reassembling Segments)

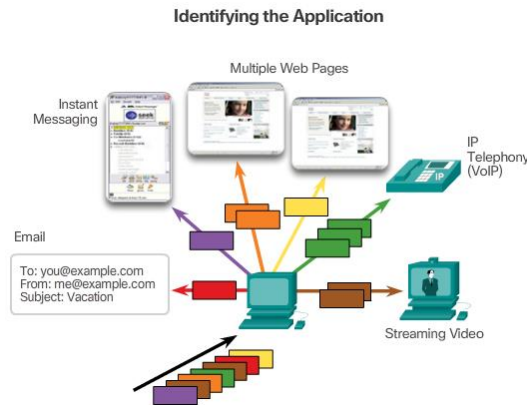
Τα δεδομένα πρέπει να είναι προετοιμασμένα να αποστέλλονται μέσω των μέσων σε αναγνωρίσιμα κομμάτια. Τα περισσότερα δίκτυα έχουν ένα περιορισμό στην ποσότητα των δεδομένων που μπορούν να συμπεριληφθούν σε ένα ενιαίο πακέτο. Τα πρωτόκολλα επιπέδου μεταφοράς έχουν υπηρεσίες οι οποίες ανήκουν στο τμήμα των δεδομένων της εφαρμογής και βρίσκονται σε ένα μπλοκ κατάλληλου μεγέθους. Η υπηρεσία αυτή περιλαμβάνει την ενθυλάκωση που απαιτείται, σε κάθε κομμάτι των δεδομένων. Μια κεφαλίδα προστίθεται σε κάθε μπλοκ δεδομένων και χρησιμοποιείται για την επανασυναρμολόγηση των δεδομένων. Αυτή η κεφαλίδα χρησιμοποιείται επίσης και για την παρακολούθηση της ροής των δεδομένων.

Στον τόπο προορισμού, το επίπεδο μεταφοράς θα πρέπει να είναι σε θέση να ανακατασκευάσει τα κομμάτια των δεδομένων σε μια πλήρη ροή δεδομένων που είναι χρήσιμα για το επίπεδο εφαρμογής. Τα πρωτόκολλα στο επίπεδο μεταφοράς περιγράφουν πώς χρησιμοποιούνται οι πληροφορίες της κεφαλίδας για να συγκεντρώνονται εκ νέου τα κομμάτια δεδομένων επανενωμένα, όπως πρέπει να περάσουν στο επίπεδο εφαρμογής.



Προσδιορίζοντας τις εφαρμογές (Identifying the Applications)

Το επίπεδο μεταφοράς πρέπει να προσδιορίζει από πού έγινε αίτημα, έτσι ώστε προωθήσει τα σωστά δεδομένα στις κατάλληλες εφαρμογές. Για να επιτευχθεί αυτό, το επίπεδο μεταφοράς αναθέτει σε κάθε αίτηση ένα αναγνωριστικό που ονομάζεται αριθμός θύρας. Κάθε εφαρμογή που κάνει χρήση του δικτύου, προσδιορίζεται από ένα μοναδικό αριθμό θύρας (port number).



Πολυπλοκότητα Επικοινωνίας (Conversation Multiplexing)

Η αποστολή ορισμένων τύπων δεδομένων (π.χ. μια ζωντανή μετάδοση βίντεο) σε ένα δίκτυο, σαν είδος επικοινωνίας μεγάλου όγκου δεδομένων, μπορεί να καταναλώσει όλο το διαθέσιμο εύρος ζώνης του δικτύου. Αυτό θα δημιουργήσει πρόβλημα σε άλλου είδους επικοινωνίες. Θα κάνει επίσης δύσκολο τον εντοπισμό των σφαλμάτων και την αναμετάδοση των κατεστραμμένων δεδομένων.

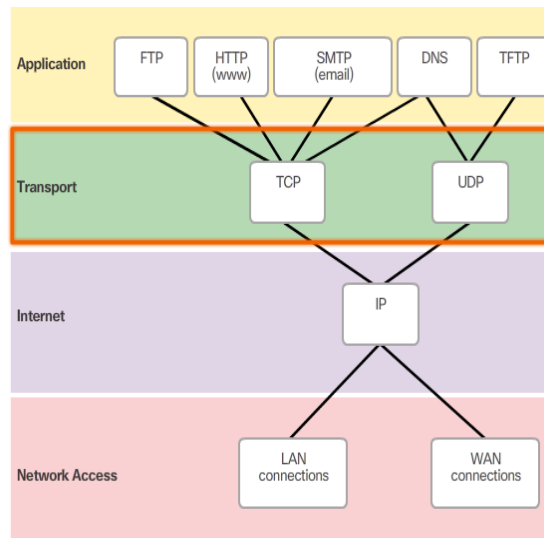
Ο διαχωρισμός των δεδομένων σε μικρότερα κομμάτια επιτρέπει πολλά είδη επικοινωνίας να συνυπάρχουν, από πολλούς διαφορετικούς χρήστες και να γίνεται μια διαπλοκή (πολυπλεγμένη) στο ίδιο δίκτυο.

Για τον εντοπισμό του κάθε τμήματος δεδομένων, το επίπεδο μεταφοράς προσθέτει μια επικεφαλίδα που περιέχει δυαδικά δεδομένα τα οποία οργανώνονται σε διάφορους τομείς. Είναι οι τιμές σε αυτούς τους τομείς που επιτρέπουν στα διάφορα πρωτόκολλα επιπέδου μεταφοράς να εκτελούν διάφορες λειτουργίες στη διαχείριση της επικοινωνίας των δεδομένων.

Αξιοπιστία επιπέδου μεταφοράς (Transport Layer Reliability)

Το επίπεδο μεταφοράς είναι επίσης υπεύθυνο για τη διαχείριση των απαιτήσεων για την αξιοπιστία μιας συνομιλίας. Διαφορετικές εφαρμογές έχουν διαφορετικές απαιτήσεις αξιοπιστίας.

Το IP ασχολείται μόνο με τη δομή, την αντιμετώπιση, και τη δρομολόγηση των πακέτων. Το IP δεν διευκρινίζει πώς συμβαίνει η παράδοση ή μεταφορά των πακέτων. Τα πρωτόκολλα μεταφοράς καθορίζουν τον τρόπο που μεταφέρονται τα μηνύματα μεταξύ των συσκευών. Το TCP/IP παρέχει δύο πρωτόκολλα επιπέδου μεταφοράς: Το πρωτόκολλο ελέγχου μετάδοσης (TCP) και το User Datagram Protocol (UDP), όπως φαίνεται στην πιο κάτω εικόνα. Το IP χρησιμοποιεί αυτά τα πρωτόκολλα μεταφοράς για να ενεργοποιήσει τις συσκευές ώστε να επικοινωνούν και να μεταφέρουν δεδομένα.



Το TCP θεωρείται ένα αξιόπιστο, με πλήρεις δυνατότητες πρωτόκολλο επιπέδου μεταφοράς, το οποίο εξασφαλίζει ότι όλα τα δεδομένα φτάνουν στον προορισμό τους. Σε αντίθεση, το UDP είναι ένα πολύ απλό πρωτόκολλο επιπέδου μεταφοράς που δεν προβλέπει καμία αξιοπιστία.

B. TCP

Με το TCP, υπάρχουν τρεις βασικές λειτουργίες αξιοπιστίας:

- Αρίθμηση και ταυτοποίηση των δεδομένων που μεταδίδονται σε ένα συγκεκριμένο υπολογιστή από μια συγκεκριμένη εφαρμογή.
- Επιβεβαίωση παραλαβής των δεδομένων.
- Γίνεται αναμετάδοση οποιοδήποτε μη επιβεβαιωμένων δεδομένων μετά από ένα ορισμένο χρονικό διάστημα.

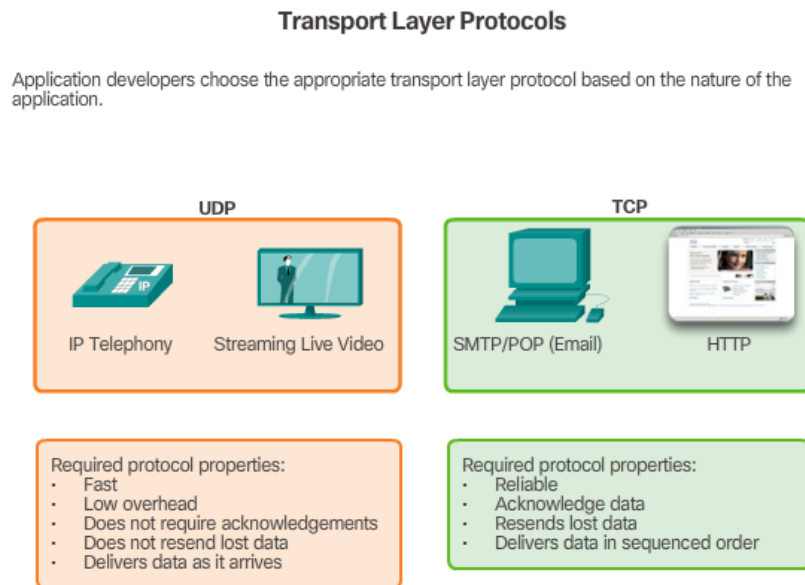
UDP

Ενώ οι λειτουργίες αξιοπιστίας του TCP παρέχουν πιο ισχυρή και σίγουρη επικοινωνία μεταξύ των εφαρμογών, μπορούν επίσης να επιφέρουν πρόσθετη επιβάρυνση και πιθανές καθυστερήσεις στη μετάδοση. Σε αυτή την περίπτωση υπάρχει μία αναλογία μεταξύ της αξίας της αξιοπιστίας και της επιβάρυνσης του δικτύου. Αυξάνοντας την αξιοπιστία αυξάνεται και η επιβάρυνση του δικτύου και η μείωση της ταχύτητας μετάδοσης του που θα μπορούσε να μειώσει τη χρησιμότητα για ορισμένες εφαρμογές και να γίνει επιβλαβής. Σε τέτοιες περιπτώσεις, το UDP είναι ένα πιο ιδανικό πρωτόκολλο μεταφοράς.

Το UDP παρέχει τις βασικές λειτουργίες για την μεταφορά δεδομένων μεταξύ των κατάλληλων εφαρμογών, με πολύ μικρή επιβάρυνση και έλεγχο των δεδομένων. Το UDP είναι γνωστό ως πρωτόκολλο καλύτερης προσπάθειας παράδοσης (best-effort delivery protocol). Στο πλαίσιο της δικτύωσης, το best-effort delivery protocol αναφέρεται ως αναξιόπιστο, γιατί δεν υπάρχει καμία απόδειξη ότι τα δεδομένα έχουν φτάσει στον προορισμό τους. Με το UDP, δεν υπάρχουν διαδικασίες επιπέδου μεταφοράς που να ενημερώνουν τον αποστολέα για επιτυχή παράδοση.

Το UDP είναι παρόμοιο με την αποστολή μιας απλής επιστολής στο ταχυδρομείο. Ο αποστολέας της επιστολής δεν γνωρίζει την διαθεσιμότητα του παραλήπτη για το αν μπορεί να λάβει την επιστολή και ούτε το ταχυδρομείο είναι υπεύθυνο για την παρακολούθηση της επιστολής ή την ενημέρωση του αποστολέα, για το αν η επιστολή δεν έχει φθάσει στον τελικό προορισμό της.

Επιλογή του σωστού πρωτοκόλλου για την κάθε εφαρμογή



Για ορισμένες εφαρμογές, τα κομμάτια δεδομένων πρέπει να φτάνουν σε μια πολύ συγκεκριμένη ποσότητα για να μπορούν να επεξεργαστούν επιτυχώς. Για κάποιες άλλες εφαρμογές, πρέπει να λαμβάνονται πλήρως όλα τα δεδομένα πριν θεωρηθεί χρήσιμα. Και στις δύο αυτές περιπτώσεις, το TCP χρησιμοποιείται ως πρωτόκολλο μεταφοράς. Οι προγραμματιστές εφαρμογών πρέπει να επιλέξουν τον τύπο του πρωτοκόλλου μεταφοράς που είναι πιο κατάλληλος, βάση των απαιτήσεων των εφαρμογών.

Για παράδειγμα, για εφαρμογές όπως οι βάσεις δεδομένων, τα προγράμματα περιήγησης στο Web και εφαρμογές ηλεκτρονικού ταχυδρομείου, απαιτείται όλα τα δεδομένα που αποστέλλονται να φτάνουν στον προορισμό τους στην αρχική τους κατάσταση. Για τυχόν δεδομένα που λείπουν θα μπορούσε να προκληθεί μια προβληματική επικοινωνία που είτε είναι ελλιπείς είτε δυσανάγνωστη. Αυτές οι εφαρμογές έχουν σχεδιαστεί να χρησιμοποιούν το πρωτόκολλο TCP.

Σε κάποιες άλλες περιπτώσεις, η επικοινωνία δεν επηρεάζεται σημαντικά με κάποια απώλεια δεδομένων κατά τη μετάδοση μέσω του δικτύου, αλλά σημαντική είναι η ταχύτητα μετάδοσης. Το UDP είναι η καλύτερη επιλογή για αυτές τις εφαρμογές, επειδή υπάρχει λιγότερη επιβάρυνση του δικτύου. Το UDP είναι προτιμότερο για εφαρμογές όπως η ροή ζωντανών ήχων, ζωντανών βίντεο, και Voice over IP (VoIP).

Για παράδειγμα, αν ένα ή δύο κομμάτια μια ζωντανής ροής βίντεο δεν καταλήξουν στο προορισμό τους, δημιουργείται μια στιγμιαία διακοπή στη ροή. Αυτό μπορεί να φαίνεται σαν παραμόρφωση στην εικόνα ή στον ήχο, αλλά δεν μπορεί να είναι εμφανής στον χρήστη.

Χαρακτηριστικά του TCP

Για να κατανοήσουμε τις διαφορές μεταξύ TCP και UDP, είναι σημαντικό να κατανοήσουμε πώς υλοποιεί κάθε πρωτόκολλο τα ειδικά χαρακτηριστικά αξιοπιστίας και πώς παρακολουθεί επικοινωνία. Εκτός από την υποστήριξη των βασικών λειτουργιών της κατάκτησης δεδομένων και επανασυναρμολόγησης, το TCP, παρέχει επίσης και άλλες υπηρεσίες.

Άνοιγμα επικοινωνίας (Establishing a Session)

Το TCP είναι ένα πρωτόκολλο προσανατολισμένης σύνδεσης (connection-oriented protocol). Ένα πρωτόκολλο προσανατολισμένης σύνδεσης είναι αυτό που διαπραγματεύεται και δημιουργεί μια μόνιμη σύνδεση μεταξύ της πηγής και της συσκευής προορισμού πριν από την προώθηση οποιωνδήποτε δεδομένων. Μέσω του ανοίγματος της επικοινωνίας, οι συσκευές αποφασίζουν για τη ποσότητα της κίνησης που μπορεί να διαβιβαστεί σε μια δεδομένη στιγμή, καθώς και τα στοιχεία επικοινωνίας.

Αξιόπιστη Παράδοση (Reliable Delivery)

Στα δίκτυα, η αξιοπιστία σημαίνει εξασφάλιση ότι κάθε τμήμα που στέλνει η πηγή φτάνει στον προορισμό του. Για πολλούς λόγους, ένα τμήμα μπορεί να καταστραφεί ή να χαθεί εντελώς, καθώς μεταδίδεται μέσω του δικτύου.

Σωστή σειρά παράδοσης (Same-Order Delivery)

Επειδή τα δίκτυα μπορούν να παρέχουν πολλαπλές διαδρομές που μπορεί να έχουν διαφορετικούς ρυθμούς μετάδοσης, τα δεδομένα μπορούν να φτάσουν με λάθος σειρά. Με την αρίθμηση και την ταυτοποίηση των τμημάτων, το TCP μπορεί να διασφαλίσει ότι αυτά τα τμήματα ανακατασκευάζονται με την σωστή σειρά.

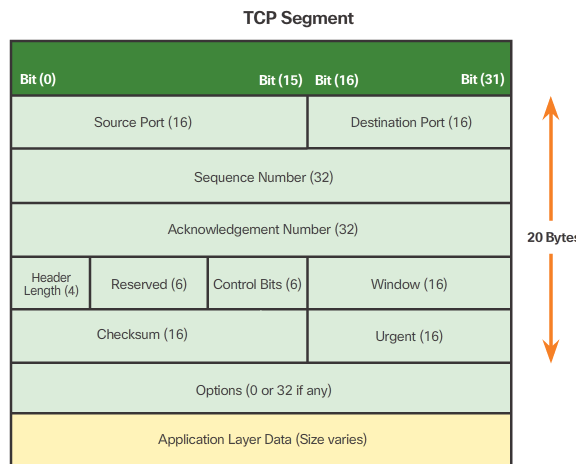
Flow Control

Μερικές συσκευές που συνδέονται σε δίκτυα έχουν περιορισμένους πόρους, όπως η μνήμη και η επεξεργαστική ισχύ. Όταν το TCP γνωρίζει ότι οι πόροι αυτοί υπερφορτώνονται, μπορεί να ζητήσει από την εφαρμογή αποστολής να μειώσει το ρυθμό ροής δεδομένων. Αυτό γίνεται από το TCP μέσω μιας ρύθμισης της ποσότητας των δεδομένων που εκπέμπει η πηγή. Ο έλεγχος ροής μπορεί να αποτρέψει την ανάγκη για αναμετάδοση των δεδομένων όταν δέκτης αδυνατεί να ανταποκριθεί.

Επικεφαλίδα TCP

Το TCP είναι ένα stateful πρωτόκολλο. Ένα stateful πρωτόκολλο είναι ένα πρωτόκολλο που παρακολουθεί την κατάσταση της επικοινωνίας. Για να παρακολουθείτε, τα αρχεία TCP καταγράφουν τις πληροφορίες οι οποίες έχουν σταλεί και αναγνωριστεί.

Όπως φαίνεται στο σχήμα, κάθε τμήμα TCP έχει 20 bytes για πληροφορίες της επικεφαλίδας:

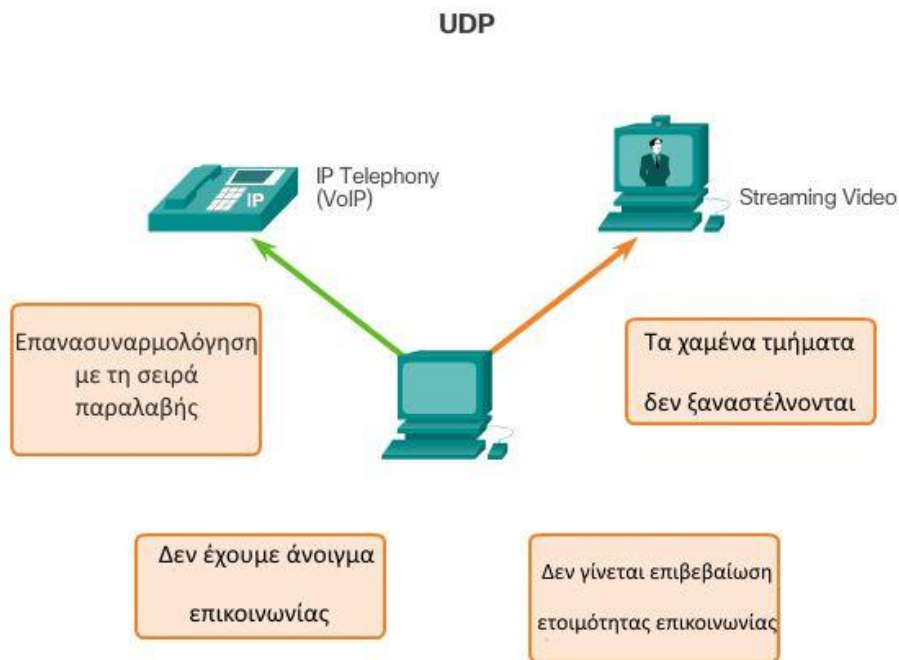


- Source Port (16 bits) και Destination Port (16 bit) - χρησιμοποιείται για να προσδιορίσει την εφαρμογή.
 - Sequence number (32 bits) - Χρησιμοποιείται για σκοπούς επανασυναρμολόγηση των δεδομένων.
 - Acknowledgment number (32 bits) - Υποδεικνύει τα δεδομένα που έχει λάβει.
 - Header length (4 bits) – Γνωστό ως "data offset". Δείχνει το μήκος της επικεφαλίδας του πακέτου TCP.
 - Reserved (6 κομμάτια) - Το πεδίο αυτό προορίζεται για μελλοντική χρήση.
- Control bits (6 κομμάτια) - Περιλαμβάνει κωδικούς bit ή σημαίες, η οποία αναφέρουν το σκοπό και τη λειτουργία του τμήματος TCP.
- Window size (16 bits) - Δείχνει τον αριθμό των bytes που μπορεί να γίνει αποδεκτός κάθε φορά.
 - Checksum (16 bits) - Χρησιμοποιείται για τον έλεγχο σφαλμάτων της επικεφαλίδας και των δεδομένων.
 - Urgent (16 bits) - Υποδεικνύει εάν τα δεδομένα έχουν πρωτεραιότητα.

UDP Features

Το User Datagram Protocol (UDP) θεωρείται ένα πρωτόκολλο καλύτερης προσπάθειας μεταφοράς (best-effort transport protocol). Το UDP είναι ένα ελαφρύ πρωτόκολλο μεταφοράς που προσφέρει τον ίδιο χωρισμό δεδομένων σε τμήματα και την επανασυναρμολόγηση, όπως το TCP, αλλά χωρίς την αξιοπιστία του TCP και τον έλεγχο ροής.

Τα χαρακτηριστικά του UDP που περιγράφονται στο σχήμα.



Επικεφαλίδα UDP

Το UDP είναι ένα stateless πρωτόκολλο, χωρίς δηλαδή ο πελάτης ή ο διακομιστής να είναι υποχρεωμένοι να παρακολουθούν την κατάσταση της επικοινωνίας. Αν όταν χρησιμοποιείτε το UDP ως πρωτόκολλο μεταφοράς απαιτείται αξιοπιστία, θα πρέπει να χειρίζεται από την εφαρμογή.

Ένας από τους πιο σημαντικούς παράγοντες για την μετάδοση ζωντανών βίντεο και φωνής μέσω του δικτύου είναι ότι τα δεδομένα πρέπει να μεταδίδονται γρήγορα. Οι ζωντανές εφαρμογές βίντεο και φωνής μπορεί να ανεχθούν κάποια απώλεια δεδομένων με ελάχιστη ή καμία σημαντική επίδραση και είναι απολύτως κατάλληλα για το UDP.

Τα κομμάτια της επικοινωνίας σε UDP ονομάζονται datagrams. Αυτά τα πακέτα δεδομένων αποστέλλονται ως best-effort από το πρωτόκολλο επιπέδου μεταφοράς. Η επικεφαλίδα του UDP έχει χαμηλή επιβάρυνση των 8 bytes.

Multiple Separate Conversations

Το επίπεδο μεταφοράς πρέπει να είναι σε θέση να διαχωρίζει και να διαχειρίζεται πολλαπλές επικοινωνίες με διαφορετικές ανάγκες μεταφορών. Οι χρήστες αναμένουν να είναι σε θέση να λαμβάνουν ταυτόχρονα και να στέλνουν email και μηνύματα, να βλέπουν ιστοσελίδες και να διεξάγουν VoIP κλήση. Κάθε μία από αυτές τις εφαρμογές διενεργά αποστολή και λήψη δεδομένων μέσω του δικτύου παρά τις διαφορετικές απαιτήσεις αξιοπιστίας. Επιπλέον, τα δεδομένα από την τηλεφωνική κλήση δεν κατευθύνεται προς το πρόγραμμα περιήγησης στο Web και το κείμενο από ένα άμεσο μήνυμα δεν εμφανίζεται σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου.

Το TCP και το UDP διαχειρίζονται αυτές τις πολλαπλές ταυτόχρονες συνομιλίες με τη χρήση των πεδίων κεφαλίδας που μπορούν να προσδιορίσουν με μοναδικό τρόπο αυτές τις εφαρμογές. Αυτά τα μοναδικά αναγνωριστικά είναι οι αριθμοί θύρας (port numbers).

Port Numbers

Ο αριθμός θύρας προέλευσης (source port number) συνδέεται με την εφαρμογή του αποστολέα στον τοπικό υπολογιστή. Ο αριθμός θύρας προορισμού (destination port number) σχετίζεται με την εφαρμογή του δέκτη.

Source Port

Οι αριθμοί θύρας προέλευσης (source port number) δημιουργούνται δυναμικά από τη συσκευή αποστολής για να προσδιοριστεί μια συνομιλία μεταξύ των δύο συσκευών. Αυτή η διαδικασία επιτρέπει σε πολλαπλές συνομιλίες να πραγματοποιούνται ταυτόχρονα. Είναι συνηθισμένο για μια συσκευή για να στείλει πολλαπλά αιτήματα υπηρεσίας HTTP σε έναν web server ταυτόχρονα. Κάθε ξεχωριστή συνομιλία HTTP καθορίζεται με βάση τις θύρες πηγής (source ports).

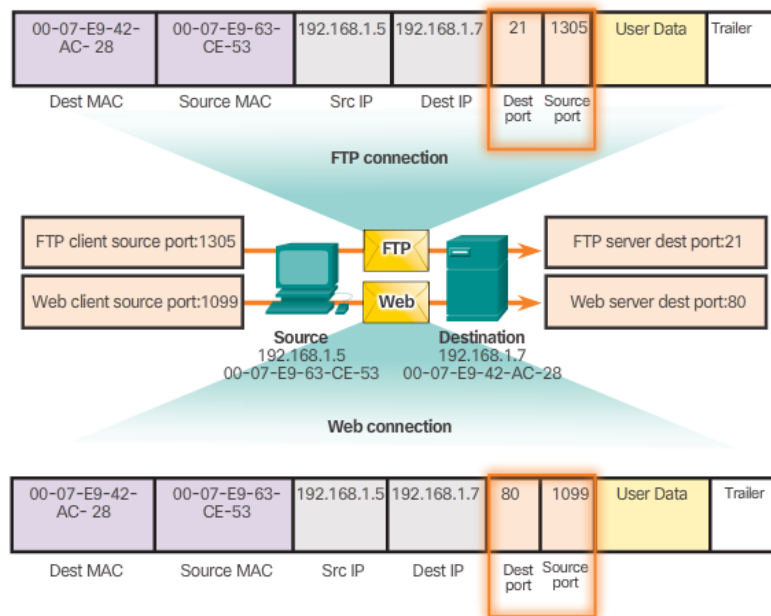
Destination Port

Ο αποστολέας χρησιμοποιεί ένα αριθμό θύρας προορισμού (destination port number) στο τμήμα για να δείξει στο διακομιστή προορισμού (destination server) ποια υπηρεσία ζητείται. Για παράδειγμα, όταν ένας πελάτης καθορίζει τη θύρα 80 στη θύρα προορισμού (destination port), ο διακομιστής που λαμβάνει το μήνυμα γνωρίζει ότι έχει ζητηθεί η υπηρεσία web. Ένας διακομιστής μπορεί να προσφέρει περισσότερες από μία υπηρεσίες ταυτόχρονα, όπως οι υπηρεσίες web στη θύρα 80 την ίδια στιγμή που προσφέρει το πρωτόκολλο μεταφοράς αρχείων (FTP) δημιουργεί μια σύνδεση στη θύρα 21.

Socket Pairs

Οι θύρες προέλευσης και προορισμού (source and destination ports) τοποθετούνται εντός του τμήματος. Τα τμήματα στη συνέχεια διαμορφώνονται σε ένα πακέτο IP. Το πακέτο IP περιέχει τη διεύθυνση IP της πηγής και του προορισμού. Ο συνδυασμός της διεύθυνσης IP πηγής και του αριθμού θύρας (port number) προέλευσης ή του αριθμού διεύθυνσης IP προορισμού και της θύρας προορισμού είναι γνωστή ως socket. Το socket χρησιμοποιείται για την αναγνώριση του διακομιστή και την υπηρεσία που ζητείται από τον πελάτη. Μια υποδοχή πελάτη μπορεί να μοιάζει με 192.168.1.5:1099, με το 1099 να αντιπροσωπεύει τον αριθμό της θύρας προέλευσης. Το socket σε έναν web server μπορεί να είναι: 192.168.1.7:80. Αυτές οι δύο διευθύνσεις συνδυάζονται και σχηματίζουν ένα ζεύγος υποδοχής (socket pair) όπως τα 192.168.1.5:1099, 192.168.1.7:80

Ο αριθμός θύρας προέλευσης (source port number) λειτουργεί ως διεύθυνση επιστροφής για την εφαρμογή αίτησης. Το επίπεδο μεταφοράς παρακολουθεί αυτή τη διεύθυνση και την εφαρμογή που υπέβαλε την αίτηση, έτσι ώστε όταν μια απάντηση επιστρέφεται, να μπορεί να διαβιβάζεται στην ορθή εφαρμογή.



Κατηγορίες Port Number

Το Internet Assigned Numbers Authority (IANA) είναι το αρμόδιο σώμα για τη χορήγηση διαφόρων προτύπων, συμπεριλαμβανομένου και των αριθμών θυρών (port numbers). Υπάρχουν διαφορετικοί τύποι αριθμούς θυρών, όπως στην πιο κάτω εικόνα:

Port Number Range	Port Group
0 to 1023	Well-known Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

- Well-known Ports (Αριθμοί 0-1023) - Οι αριθμοί αυτοί προορίζονται για υπηρεσίες και εφαρμογές. Χρησιμοποιούνται συνήθως για εφαρμογές όπως προγράμματα περιήγησης στο Web, πελάτες ηλεκτρονικού ταχυδρομείου και πελάτες απομακρυσμένης πρόσβασης. Με τον καθορισμό αυτών των γνωστών θυρών για διακομιστές εφαρμογές και εφαρμογές πελάτη, μπορεί να προγραμματιστεί για να ζητηθεί μια σύνδεση με τη συγκεκριμένη θύρα και των συνδεόμενων υπηρεσιών του.

Well-Known Port Numbers

Port Number	Protocol	Application	Acronym
20	TCP	File Transfer Protocol (data)	FTP
21	TCP	File Transfer Protocol (control)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	–
25	TCP	Simple Mail Transfer Protocol	SMTP
53	UDP, TCP	Domain Name Service	DNS
67	UDP	Dynamic Host Configuration Protocol (server)	DHCP
68	UDP	Dynamic Host Configuration Protocol (client)	DHCP
69	UDP	Trivial File Transfer Protocol	TFTP
80	TCP	Hypertext Transfer Protocol	HTTP
110	TCP	Post Office Protocol version 3	POP3
143	TCP	Internet Message Access Protocol	IMAP
161	UDP	Simple Network Management Protocol	SNMP
443	TCP	Hypertext Transfer Protocol Secure	HTTPS

- **Registered Ports** (Αριθμοί 1.024 έως 49.151) - Αυτοί οι αριθμοί θύρας έχουν ανατεθεί από την IANA σε ένα φορέα για χρήση με συγκεκριμένες διαδικασίες ή εφαρμογές. Αυτές οι διαδικασίες είναι κυρίως ιδιωτικές εφαρμογές που ο κάποιος χρήστης έχει επιλέξει για να εγκαταστήσει και ζητά και χρησιμοποιεί κάποια από αυτές παρά αυτές των κοινών εφαρμογών που μπορεί να πάρει από την κατηγορία Well-known Port. Για παράδειγμα, στη Cisco έχει καταχωρηθεί η θύρα 1985 για τη διαδικασία της Hot Standby Routing Protocol (HSRP).

- **Dynamic or Private Ports** (Αριθμοί 49.152 - 65535) - Αυτά συνήθως αναθέτονται δυναμικά από το λειτουργικό σύστημα του πελάτη όταν ξεκινά μια σύνδεση σε μια υπηρεσία. Η δυναμική θύρα στη συνέχεια χρησιμοποιείται για να προσδιορίσει την εφαρμογή-πελάτη κατά τη διάρκεια της επικοινωνίας.

Η εντολή netstat

Για κάποιους λόγους οι συνδέσεις TCP μπορεί να αποτελέσουν σημαντική απειλή για την ασφάλεια. Μπορούν να δείχνουν ότι κάτι ή κάποιος είναι συνδεδεμένο με τον τοπικό κεντρικό υπολογιστή. Μερικές φορές είναι απαραίτητο να γνωρίζουμε ποιες ενεργές συνδέσεις TCP είναι ανοικτές και λειτουργούν σε μία συσκευή που είναι ενωμένη σε ένα δίκτυο. Το Netstat είναι ένα σημαντικό βοηθητικό πρόγραμμα δικτύου που μπορεί να χρησιμοποιηθεί για την επαλήθευση αυτών των συνδέσεων. Όπως φαίνεται στην εικόνα, εκτελώντας την εντολή netstat καταγράφει τα πρωτόκολλα που χρησιμοποιούνται, τα local address και τα port numbers, τα foreign address και την κατάσταση σύνδεσης.

```
C:\> netstat

Active Connections

Proto Local Address Foreign Address State
TCP kenpc:3126 192.168.0.2:netbios-ssn ESTABLISHED
TCP kenpc:3158 207.138.126.152:http ESTABLISHED
TCP kenpc:3159 207.138.126.169:http ESTABLISHED
TCP kenpc:3160 207.138.126.169:http ESTABLISHED
TCP kenpc:3161 sc.msn.com:http ESTABLISHED
TCP kenpc:3166 www.cisco.com:http ESTABLISHED

C:\>
```

Από προεπιλογή, η εντολή netstat θα προσπαθήσει να αναλύσει τις διευθύνσεις IP σε ονόματα τομέα (domain names) και αριθμούς θύρας (port numbers) σε γνωστές εφαρμογές (well-known applications). Η επιλογή -n μπορεί να χρησιμοποιηθεί για να εμφανίσει τις διευθύνσεις IP και τους αριθμούς θύρας στην αριθμητική τους μορφή.

Διεργασίες TCP διακομιστή

Κάθε διαδικασία εφαρμογής που τρέχει στον διακομιστή έχει ρυθμιστεί να χρησιμοποιεί έναν αριθμό θύρας, είτε από προεπιλογή ή από το λειτουργικό του συστήματος. Ένας ιδιωτικός διακομιστής δεν μπορεί να έχει δύο υπηρεσίες που να της έχουν ανατεθεί ο ίδιος αριθμός θύρας εντός των ίδιων των υπηρεσιών του επιπέδου μεταφοράς. Για παράδειγμα, ένας κεντρικός υπολογιστής που εκτελεί μια εφαρμογή web server και μια εφαρμογή μεταφοράς αρχείων δεν μπορεί να ρυθμιστεί ώστε να χρησιμοποιεί την ίδια θύρα. Μια ενεργή εφαρμογή διακομιστή που ανατίθεται σε συγκεκριμένη θύρα θεωρείται ότι είναι ανοικτή, πράγμα που σημαίνει ότι το επίπεδο μεταφοράς δέχεται και τις διαδικασίες τμήματος που απευθύνονται σε αυτήν τη θύρα. Κάθε εισερχόμενη αίτηση πελάτη που απευθύνεται στην σωστή υποδοχή είναι αποδεκτή, και τα δεδομένα διοχετεύονται στο διακομιστή. Μπορεί να υπάρχουν πολλές θύρες που ανοίγουν ταυτόχρονα σε ένα διακομιστή, μια για κάθε ενεργή εφαρμογή διακομιστή.

Άνοιγμα σύνδεσης TCP

Σε μερικούς πολιτισμούς, όταν συναντώνται δύο άτομα, συχνά χαιρετούν ο ένας τον άλλον με χειραψία. Η πράξη της χειραψία γίνεται κατανοητή από τα δύο μέρη ως σήμα για ένα φιλικό χαιρετισμό και σαν έναρξη μιας συνομιλίας. Οι συνδέσεις με το δίκτυο είναι παρόμοιες. Σε συνδέσεις TCP, ο πελάτης δημιουργεί τη σύνδεση με το διακομιστή.

Μια σύνδεση TCP γίνεται σε τρία βήματα:

Βήμα 1 - Ο πελάτης ζητά επικοινωνία client-to-server με το διακομιστή.

Βήμα 2 - Ο διακομιστής αναγνωρίζει τη αίτηση επικοινωνίας client-to-server και ζητά επικοινωνίας server-to-client.

Βήμα 3 - Η πελάτης αναγνωρίζει τη αίτηση επικοινωνίας server-to-client. Η επικοινωνία είναι έτοιμη να ξεκινήσει.

Τερματισμός σύνδεσης TCP

Για να κλείσετε μια σύνδεση, πρέπει να οριστεί στην κεφαλίδα του τμήματος ο Finish (FIN) control flag. Στο τέλος κάθε μονόδρομης σύνδεσης TCP χρησιμοποιείται μια αμφίδρομη επικοινωνία, που αποτελείται από ένα τμήμα FIN και ένα τμήμα επιβεβαίωσης (ACK). Ως εκ τούτου, για να τερματιστεί μία συνομιλία που υποστηρίζεται από το πρωτόκολλο TCP, απαιτούνται τέσσερις ανταλλαγές.

Η διαδικασία τερματισμού μπορεί να ξεκινήσει από οποιαδήποτε από τις δύο συσκευές που έχουν μια ανοικτή συνομιλία:

Βήμα 1 - Όταν ο πελάτης δεν έχει περισσότερα στοιχεία για αποστολή, στέλνει ένα τμήμα ενεργοποιώντας το FIN flag set.

Βήμα 2 - Ο διακομιστής στέλνει ένα αποδεικτικό παραλαβής (ACK) της FIN για να τερματίσει την σύνοδο από τον πελάτη στον διακομιστή.

Βήμα 3 - Ο διακομιστής στέλνει ένα FIN για τον πελάτη να τερματίσει τη σύνοδο server-to-client.

Βήμα 4 - Ο πελάτης απαντά με ACK σαν απόδειξη παραλαβής του FIN από το διακομιστή.

Όταν όλα τα τμήματα έχουν αναγνωρισθεί, η σύνδεση κλείνει.

TCP Three-way Handshake

Συσκευές που παρακολουθούν κάθε τμήμα δεδομένων μέσα από μια σύνδεση και ανταλλάσσουν πληροφορίες σχετικά με το τι δεδομένα λαμβάνονται χρησιμοποιώντας τις πληροφορίες στην κεφαλίδα TCP. Το TCP είναι ένα πλήρως αμφίδρομο πρωτόκολλο, όπου κάθε σύνδεση αντιπροσωπεύει δύο κατευθύνσεις μονόδρομης επικοινωνίας. Για να δημιουργηθεί η σύνδεση, οι συσκευές εκτελούν μια συνεννόηση τριών βημάτων (three-way handshake). Τα bits ελέγχου στην κεφαλίδα TCP δείχνουν την πρόοδο και την κατάσταση της σύνδεσης.

Η συνεννόηση τριών βημάτων (three-way handshake):

- Επιβεβαιώνεται ότι η συσκευή προορισμού βρίσκεται στο δίκτυο.
- Επιβεβαιώνει ότι η συσκευή προορισμού έχει ενεργό υπηρεσία που αποδέχεται τα αιτήματα σχετικά με τον αριθμό θύρας προορισμού τα οποία θα χρησιμοποιήσει ο πελάτης.
- Ενημερώνει τη συσκευή προορισμού ότι ο πελάτης σκοπεύει να ανοίξει επικοινωνία στον συγκεκριμένο αριθμό θύρας.

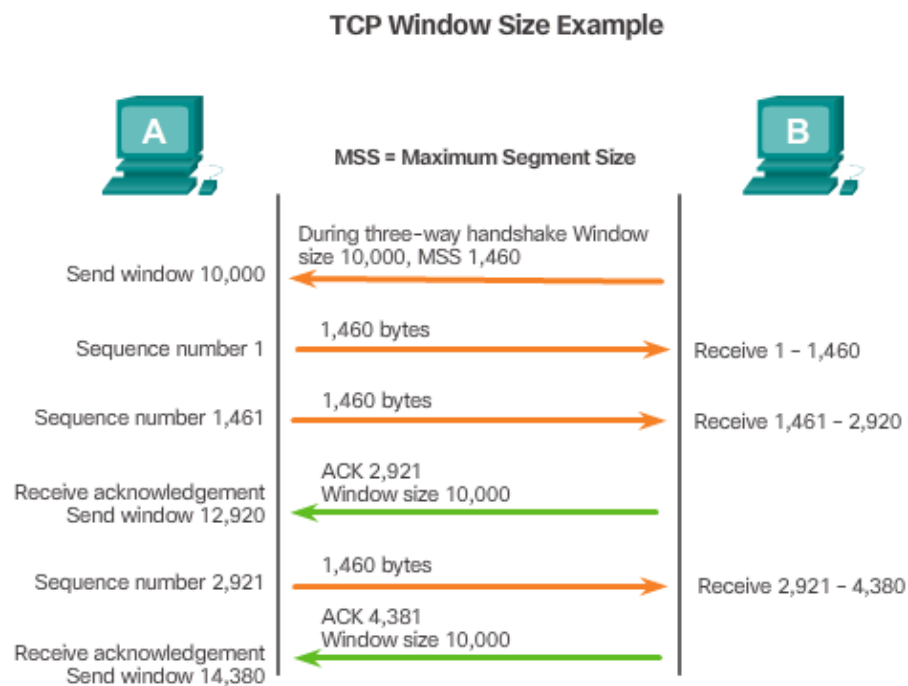
Μετά την ολοκλήρωση της επικοινωνίας αυτής, η επικοινωνία κλείνει και η σύνδεση τερματίζεται. Οι μηχανισμοί σύνδεσης και επικοινωνίας ενεργοποιούν τη λειτουργία αξιοπιστίας του TCP.

Αξιοπιστία – Διατεταγμένη αποστολή δεδομένων TCP

Τα τμήματα του TCP μπορεί να φτάνουν στον προορισμό με διαφορετική σειρά από ότι έχουν σταλεί. Για να γίνει κατανοητό το αρχικό μήνυμα από τον παραλήπτη, τα δεδομένα σε αυτά τα τμήματα πρέπει να ανακατασκευαστούν στην αρχική μορφή. Για την επίτευξη αυτού οι έχουν αποδοθεί αριθμοί σειράς στην επικεφαλίδα του κάθε πακέτου. Ο αύξων αριθμός αντιπροσωπεύεται με το πρώτο byte δεδομένων του πακέτου TCP.

Μέγεθος παραθύρου και απόδειξη παραλαβής (TCP Flow Control - Window Size and Acknowledgments)

Το TCP παρέχει επίσης μηχανισμούς για τον έλεγχο της ροής, την ποσότητα των δεδομένων που μπορεί να λάβει ο προορισμός και τη διαδικασία αξιοπιστίας. Ο έλεγχος της ροής βοηθά στη διατήρηση της αξιοπιστίας της μετάδοσης TCP ρυθμίζοντας το ρυθμό ροής δεδομένων μεταξύ της πηγής και του προορισμού για μια συγκεκριμένη σύνδεση. Για να επιτευχθεί αυτό, η επικεφαλίδα TCP περιλαμβάνει ένα πεδίο 16-bit που ονομάζεται μέγεθος του παραθύρου (window size).



The **window size** determines the number of bytes that can be sent before expecting an acknowledgment.
The **acknowledgment** number is the number of the next expected byte.

Το σχήμα δείχνει ένα παράδειγμα για το μέγεθος και το αποδεικτικό παραλαβής (acknowledgments) του παραθύρου. Το μέγεθος του παραθύρου είναι ο αριθμός των bytes που η συσκευή προορισμού μιας σύνδεσης TCP μπορεί να δεχθεί και να επεξεργαστεί κάθε φορά. Σε αυτό το παράδειγμα, το αρχικό μέγεθος του παραθύρου PC B για τη σύνδεση TCP είναι 10.000 bytes. Ξεκινώντας με το πρώτο byte, ο αριθμός byte 1, το τελευταίο byte PC A μπορεί να στείλει, χωρίς να λάβει μια αναγνώριση είναι 10.000 byte. Αυτό είναι γνωστό ως παράθυρο αποστολής PC A. Το μέγεθος του παραθύρου περιλαμβάνεται σε κάθε τμήμα TCP,

ώστε ο προορισμός να μπορεί να τροποποιεί το μέγεθος του παραθύρου ανά πάσα στιγμή ανάλογα με τη διαθεσιμότητα του ρυθμιστή.

Το αρχικό μέγεθος του παραθύρου συμφωνείται όταν η σύνδεση TCP ενεργοποιηθεί με το three-way handshake. Η συσκευή πηγής πρέπει να περιορίσει τον αριθμό των bytes που αποστέλλονται στη συσκευή προορισμού με βάση το μέγεθος του παραθύρου του προορισμού. Αφού πρώτα η συσκευή προέλευσης λάβει μια επιβεβαίωση ότι τα bytes έχουν ληφθεί, τότε μπορεί να συνεχίσει την αποστολή περισσότερων δεδομένων. Ο προορισμός δεν θα περιμένει να παραλάβει το σύνολο των byte για το μέγεθος του παραθύρου του πριν να απαντήσει με μια αναγνώριση. Καθώς τα bytes λαμβάνονται και επεξεργάζονται, ο προορισμός θα στείλει αναγνωρίσεις για να ενημερώσει την πηγή ότι μπορεί να συνεχίσει να στέλνει επιπλέον bytes.

Το PC B δεν θα περιμένει μέχρι όλα τα 10,000 bytes να ληφθούν για να στείλει απόδειξη παραλαβής. Αυτό σημαίνει πως το PC A μπορεί να προσαρμόσει το παράθυρο αποστολής του καθώς λαμβάνει αναγνωρίσεις από το PC B. Όπως φαίνεται στο σχήμα, όταν ο PC A λαμβάνει απόδειξη παραλαβής με τον αριθμό επιβεβαίωσης 2921, το παράθυρο αποστολής PC A θα αυξήσει ακόμα 10.000 bytes (το μέγεθος των PC B θα είναι το τρέχον μέγεθος του παραθύρου) σε 12.920. Το PC A μπορεί πλέον να συνεχίσει να στέλνει μέχρι ακόμα 10.000 bytes στον υπολογιστή PC B εφ' όσον δεν αποστέλλει στο νέο παράθυρο αποστολής πέραν των 12.920.

Η διαδικασία του προορισμού στέλνει αναγνωρίσεις καθώς επεξεργάζεται τα bytes που ελήφθησαν. Η συνεχής προσαρμογή του παραθύρου αποστολής της πηγής είναι γνωστή ως συρόμενα παράθυρα. Αν η διαθεσιμότητα του χώρου buffer του προορισμού μειώνεται, μπορεί να περιορίσει το μέγεθος του παραθύρου του για να ενημερώσει την πηγή ώστε να μειωθεί ο αριθμός των bytes που πρέπει να στείλει χωρίς να λάβει επιβεβαίωση.

Αποφυγή συμφόρησης (TCP Flow Control - Congestion Avoidance)

Όταν γίνεται συμφόρηση σε ένα δίκτυο, αυτό οδηγεί σε πακέτα να απορρίπτονται από το υπερφορτωμένο δρομολογητή. Όταν τα πακέτα που περιέχουν τμήματα TCP δεν φθάνουν στον προορισμό τους, μένουν μη αναγνωρίσιμα. Ο ρυθμός με τον οποίο στέλνονται τα τμήματα TCP που χάνονται, δίνει στον αποστολέα μια εικόνα για το επίπεδο συμφόρησης του δικτύου.

Όποτε υπάρχει συμφόρηση, θα γίνεται αναμετάδοση των χαμένων τμημάτων TCP από την πηγή. Εάν η αναμετάδοση δεν ελέγχεται σωστά, η πρόσθετη αναμετάδοση των τμημάτων TCP μπορεί να κάνει τη συμφόρηση ακόμα χειρότερη. Δεν είναι μόνο τα νέα πακέτα με τα τμήματα TCP που εισάγονται στο δίκτυο, αλλά θα προστεθούν επίσης στην κυκλοφοριακή συμφόρηση τα αποτελέσματα της αναμετάδοσης των τμημάτων TCP που χάθηκαν. Για την αποφυγή και τον έλεγχο της συμφόρησης, το TCP χρησιμοποιεί διάφορους μηχανισμούς χειρισμού της κυκλοφοριακής συμφόρησης, όπως χρονόμετρα και αλγόριθμους.

Εάν η πηγή καθορίσει ότι τα τμήματα TCP δεν αναγνωρίστηκαν ή δεν αναγνωρίστηκαν εγκαίρως, τότε μπορεί να μειώσει τον αριθμό των bytes που στέλνονται πριν από τη λήψη της

βεβαίωσης. Είναι η πηγή που μειώνει των αριθμό των μη αναγνωρισμένων bytes που στέλνει και όχι το μέγεθος του παραθύρου ανάλογα με τον προορισμό.

Χαμηλή επιβάρυνση σε σχέση με Αξιοπιστία - UDP

Το UDP είναι ένα απλό πρωτόκολλο που παρέχει τις βασικές λειτουργίες του επιπέδου μεταφοράς. Έχει πολύ χαμηλότερο κόστος συμφόρησης από το TCP, διότι δεν χρησιμοποιεί προσανατολισμένη σύνδεση (connection-oriented) και δεν προσφέρει την εξελιγμένη αναμετάδοση, αλληλουχία, και μηχανισμούς ελέγχου ροής που παρέχουν αξιοπιστία.

Αυτό δεν σημαίνει ότι οι εφαρμογές που χρησιμοποιούν το UDP είναι πάντα αναξιόπιστες, ούτε σημαίνει ότι το UDP είναι ένα κατώτερο πρωτόκολλο. Απλά σημαίνει ότι αυτές οι λειτουργίες δεν παρέχονται από το πρωτόκολλο επιπέδου μεταφοράς και πρέπει να εφαρμοστούν αλλού αν απαιτείται.

Η χαμηλή επιβάρυνση του UDP το καθιστά πολύ επιθυμητό για τα πρωτόκολλα που χρησιμοποιούν απλή επικοινωνία. Για παράδειγμα, χρησιμοποιώντας το πρωτόκολλο TCP για DHCP θα εισάγει περιττή κίνηση στο δίκτυο. Εάν υπάρχει ένα πρόβλημα με ένα αίτημα ή μια απάντηση, η συσκευή απλά στέλνει την αίτηση ξανά αν δεν έχει ληφθεί καμία απάντηση.

Επανασυναρμολόγηση Datagram UDP

Όπως και τα τμήματα με το TCP, όταν τα datagrams του UDP στέλνονται σε έναν προορισμό, συχνά λαμβάνουν διαφορετικές διαδρομές και φτάνουν με λάθος σειρά. Το UDP δεν παρακολουθεί τους αριθμούς ακολουθίας με τον τρόπο που το κάνει το TCP. Το UDP δεν έχει τρόπο να αλλάξει τη σειρά των datagrams.

Το UDP συγκεντρώνει τα δεδομένα με τη σειρά που παραλήφθηκαν επανασυναρμολογεί. Αν η ακολουθία των δεδομένων είναι σημαντική για την εφαρμογή, η εφαρμογή πρέπει να προσδιορίσει τη σωστή ακολουθία και να καθορίσει πώς θα πρέπει να επεξεργαστούν τα δεδομένα.

Διαδικασία διακομιστή UDP

Όπως οι εφαρμογές που χρησιμοποιούν TCP σύνδεση, έτσι και οι εφαρμογές διακομιστή UDP χρησιμοποιούν γνωστούς και εγγεγραμμένους αριθμούς θύρας. Όταν αυτές οι εφαρμογές ή διαδικασίες τρέχουν σε ένα διακομιστή, δέχονται τα δεδομένα που ταιριάζουν με τον αριθμό θύρας που ανατέθηκε. Όταν το UDP λαμβάνει ένα datagram που προορίζονται για μία από αυτές τις θύρες, διαβιβάζει τα δεδομένα εφαρμογής για την κατάλληλη εφαρμογή με βάση τον αριθμό θύρας του.

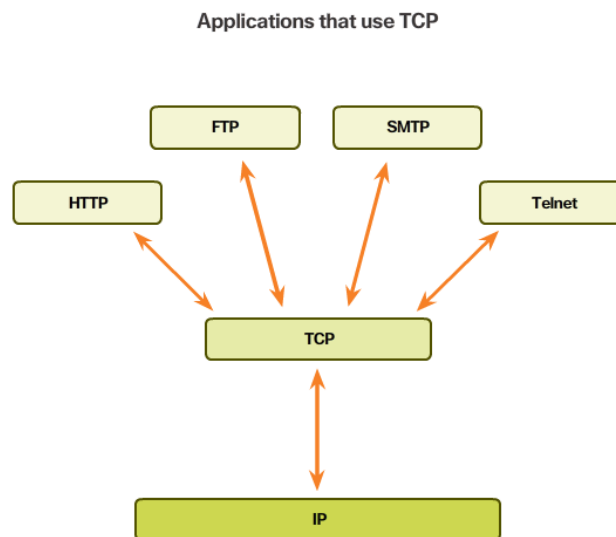
Διαδικασία πελάτη UDP

Όπως και με το πρωτόκολλο TCP, η επικοινωνία client-server ξεκινά από μια εφαρμογή πελάτη που ζητά δεδομένα από μια υπηρεσία ενός διακομιστή. Η διαδικασία πελάτη UDP επιλέγει δυναμικά έναν αριθμό θύρας από την περιοχή της θύρας αριθμών και το χρησιμοποιεί ως πηγή για τη σύνδεση. Η θύρα προορισμού είναι συνήθως ο γνωστός ή εγγεγραμμένος αριθμός θύρας που ανατεθεί με τη διαδικασία του server.

Μετά που ένας πελάτης έχει επιλέξει τις θύρες πηγής και προορισμού, το ίδιο ζευγάρι των θυρών χρησιμοποιείται στην κεφαλίδα όλων των datagrams που χρησιμοποιούνται στη συναλλαγή. Για τα δεδομένα που επιστρέφονται στον πελάτη από το διακομιστή, οι αριθμοί θυρών πηγής και προορισμού στην κεφαλίδα datagram αντιστρέφονται.

Εφαρμογές που χρησιμοποιούν TCP

Το TCP είναι ένα μεγάλο παράδειγμα για το πώς τα διαφορετικά επίπεδα πρωτοκόλλων TCP/IP έχουν συγκεκριμένους ρόλους. Το TCP χειρίζεται όλα τα καθήκοντα που σχετίζονται με τη διαίρεση της ροής δεδομένων σε τμήματα, παρέχοντας αξιοπιστία, έλεγχο ροής των δεδομένων, καθώς και την αναδιάταξη των τμημάτων. Το TCP απελευθερώνει την εφαρμογή από την υποχρέωση να διαχειριστεί οποιαδήποτε από αυτά τα καθήκοντα. Εφαρμογές, όπως αυτές που φαίνονται στο σχήμα, μπορούν απλά να στείλουν τη ροή δεδομένων στο επίπεδο μεταφοράς και να χρησιμοποιήσουν τις υπηρεσίες του TCP.



Εφαρμογές που χρησιμοποιούν UDP

Υπάρχουν τρεις τύποι των εφαρμογών που είναι οι πλέον κατάλληλες για χρήση UDP:

- Ζωντανό βίντεο και εφαρμογές πολυμέσων (Live video and multimedia applications). Μπορούν να ανεχθούν κάποια απώλεια δεδομένων, αλλά απαιτούν ελάχιστη ή καθόλου καθυστέρηση. (π.χ. VoIP, live streaming βίντεο)
- Απλό αίτημα και εφαρμογές απάντησης (Simple request and reply applications). Εφαρμογές με απλές συναλλαγές, όπου ένας κεντρικός υπολογιστής στέλνει ένα αίτημα και μπορεί ή δεν μπορεί να λάβει απάντηση. (π.χ. DNS και DHCP)
- Εφαρμογές που χειρίζονται οι ίδιοι την αξιοπιστία (Applications that handle reliability themselves). Μονής κατεύθυνσης επικοινωνία όπου ο έλεγχος ροής, εντοπισμός σφαλμάτων, αναγνώρισης και ανάκτησης λάθους δεν απαιτούνται ή μπορεί να αντιμετωπιστούν από την εφαρμογή. (π.χ. SNMP και TFTP)

Παρά το γεγονός ότι το DNS και το SNMP χρησιμοποιούν το UDP από προεπιλογή, και οι δύο μπορούν επίσης να χρησιμοποιήσουν το πρωτόκολλο TCP. Ο DNS θα χρησιμοποιήσει το πρωτόκολλο TCP, αν η αίτηση DNS ή η απάντηση DNS είναι περισσότερο από 512 bytes, όπως όταν μια απάντηση DNS περιέχει ένα μεγάλο αριθμό ανάλυσης ονομάτων. Ομοίως, κάτω από ορισμένες καταστάσεις ο διαχειριστής του δικτύου μπορεί να θελήσει να ρυθμίσει το SNMP για να χρησιμοποιήσει το πρωτόκολλο TCP.

7. Επίπεδο Εφαρμογών (Application Layer)

A. Application, Presentation Session Layers

Εφαρμογές, όπως Web browsers, online gaming, ηλεκτρονικό ταχυδρομείο, μας δίνουν τη δυνατότητα να στέλνουμε και να λαμβάνουμε δεδομένα με σχετική ευκολία. Συνήθως χρησιμοποιούμε αυτές τις εφαρμογές χωρίς να γνωρίζουμε πώς λειτουργούν. Ωστόσο, για τους ειδικούς του δικτύου, είναι σημαντικό να γνωρίζουν πώς μορφοποιείται μια εφαρμογή και πρέπει να μπορούν να διαβιβάζουν και να ερμηνεύουν τα μηνύματα που αποστέλλονται και λαμβάνονται μέσω του δικτύου. Η τρόπος επικοινωνίας μέσω του δικτύου γίνεται πιο εύκολος με τη χρήση του πολυεπίπεδου πλαισίου του μοντέλου OSI.

Παρακάτω θα εξετάσουμε το ρόλο των στρωμάτων εφαρμογής και πώς οι εφαρμογές, οι υπηρεσίες και τα πρωτόκολλα μέσα στο επίπεδο εφαρμογής κάνουν ισχυρή την επικοινωνία μέσω δικτύων δεδομένων δυνατόν.

The Application Layer

Το επίπεδο εφαρμογής είναι πλησιέστερο, από τα άλλα επίπεδα που ανήκουν στην ίδια κατηγορία, προς τον χρήστη. Είναι το επίπεδο που παρέχει τη διεπαφή μεταξύ των εφαρμογών που χρησιμοποιούνται για την επικοινωνία και το δίκτυο κατά το οποίο μεταδίδονται τα μηνύματα.

Τα πρωτόκολλα επιπέδου εφαρμογής χρησιμοποιούνται για την ανταλλαγή δεδομένων μεταξύ των προγραμμάτων που είναι εγκατεστημένα στους υπολογιστές προέλευσης και προορισμού.

Οι λειτουργίες του ενιαίου επιπέδου εφαρμογής TCP / IP ορίζονται από τρία επίπεδα του μοντέλου OSI (αίτηση, την παρουσίαση και συνεδρία).

Υπάρχουν πολλά πρωτόκολλα επιπέδου εφαρμογής, αλλά αναπτύσσονται συνεχώς και νέα πρωτόκολλα. Μερικά από τα πιο γνωστά πρωτόκολλα επιπέδου εφαρμογής είναι: Hypertext Transfer Protocol (HTTP), πρωτόκολλο μεταφοράς αρχείων (FTP), Trivial πρωτόκολλο μεταφοράς αρχείων (TFTP), πρωτόκολλο πρόσβασης μηνυμάτων Internet (IMAP), και Domain Name System (DNS).

Δύο άλλα επίπεδα που ανήκουν στα επίπεδα εφαρμογών είναι το Presentation (παρουσίασης) και το Session Layer (συνόδου).

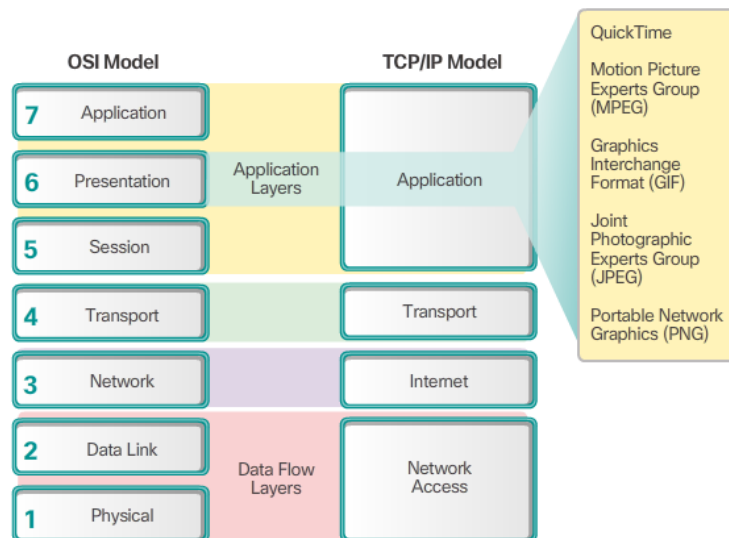
Επίπεδο παρουσίασης (Presentation Layer)

Το επίπεδο παρουσίασης έχει τρεις κύριες λειτουργίες:

- Τη μορφοποίηση ή την παρουσίαση των δεδομένων της συσκευής πηγής σε μια συμβατή μορφή, για να μπορεί να γίνει η παραλαβή από τη συσκευή προορισμού.
- Τη συμπίεση δεδομένων με έναν τρόπο έτσι ώστε να μπορεί να αποσυμπίεστεί η συσκευή προορισμού.

- Την κρυπτογράφηση δεδομένων για τη μετάδοση και την αποκρυπτογράφηση των δεδομένων κατά την παραλαβή.

Όπως φαίνεται στο σχήμα, το επίπεδο παρουσίασης θέτει πρότυπα για συγκεκριμένες μορφές αρχείων. Μερικά γνωστά πρότυπα για το βίντεο είναι το QuickTime και το Motion Picture Experts Group (MPEG). Μερικές γνωστές μορφές γραφικών εικόνων που χρησιμοποιούνται σε δίκτυα είναι το Portable Network Graphics (PNG), το Graphics Interchange Format (GIF) και το Joint Photographic Experts Group (JPEG).

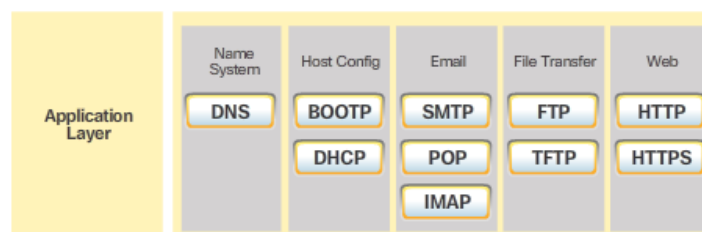


Επίπεδο συνόδου (Session Layer)

Στο επίπεδο συνόδου δημιουργείται και διατηρείται επαφή μεταξύ των εφαρμογών πηγής και προορισμού. Το επίπεδο συνόδου χειρίζεται την ανταλλαγή πληροφοριών για την έναρξη διαλόγων, τους κρατάει ενεργούς και επαναφέρει την επικοινωνία όταν διακοπεί ή είναι σε αδράνεια για μεγάλο χρονικό διάστημα.

B. TCP/IP Application Layer Protocols

Τα πρωτόκολλα εφαρμογής TCP / IP καθορίζουν τη μορφή και τον έλεγχο πληροφοριών που είναι απαραίτητες για πολλές λειτουργίες επικοινωνίας του Internet.



Τα πρωτόκολλα επιπέδου εφαρμογής χρησιμοποιούνται κατά τη διάρκεια επικοινωνίας από τις συσκευές τόσο για αποστολή όσο και για παραλαβή δεδομένων. Για να είναι επιτυχής η

επικοινωνία, τα πρωτόκολλα επιπέδου εφαρμογής πρέπει να είναι συμβατά και στον αποστολέα και στον παραλήπτη.

Μοντέλο Πελάτη-Διακομιστή (Client-Server Model)

Στο μοντέλο client-server, η συσκευή που ζητά την πληροφορία ονομάζεται πελάτης (client) και η συσκευή που ανταποκρίνεται στο αίτημα ονομάζεται διακομιστής (server). Οι επικοινωνία πελάτη και διακομιστή ανήκει στο επίπεδο εφαρμογής. Ο πελάτης ξεκινά την επικοινωνία ζητώντας δεδομένα από το διακομιστή, ο οποίος απαντά στέλνοντας τα στον πελάτη. Τα πρωτόκολλα επιπέδου εφαρμογής περιγράφουν τη μορφή των αιτήσεων και των απαντήσεων μεταξύ του πελάτη και του εξυπηρετητή. Εκτός από την πραγματική μεταφορά δεδομένων, η επικοινωνία αυτή μπορεί επίσης να απαιτεί έλεγχο της ταυτότητας του χρήστη και τον εντοπισμό ενός αρχείου δεδομένων.

Ένα παράδειγμα ενός δικτύου client-server χρησιμοποιείται στην υπηρεσία ηλεκτρονικού ταχυδρομείου ενός ISP για να στέλνονται, να λαμβάνονται και να αποθηκεύονται ηλεκτρονικά μηνύματα. Ο πελάτης ηλεκτρονικού ταχυδρομείου σε έναν υπολογιστή στο σπίτι ζητά από τον email server του ISP του να πάρει τα μη αναγνωσμένα μηνύματα. Ο διακομιστής ανταποκρίνεται στέλνοντας τα στον πελάτη.

Δίκτυο ομότιμων κόμβων (Peer-to-Peer P2P)

Στο μοντέλο δικτύωσης peer-to-peer (P2P), τα δεδομένα είναι προσβάσιμα από μια συσκευή χωρίς τη χρήση ενός κεντρικού υπολογιστή.

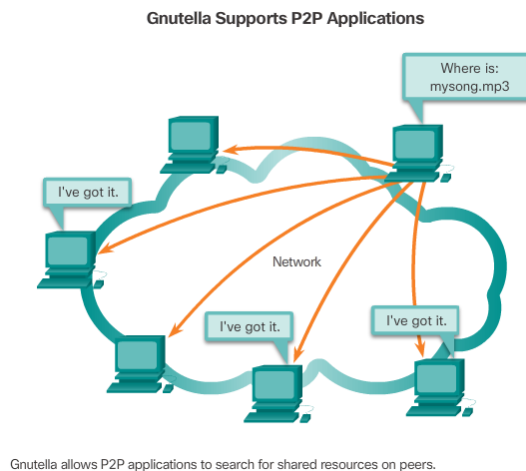
Σε ένα δίκτυο P2P δύο ή περισσότεροι υπολογιστές μπορούν να συνδέονται μέσω ενός δικτύου και να μοιράζονται πόρους (όπως οι εκτυπωτές και αρχεία) χωρίς να χρειάζεται ένας ειδικός server. Κάθε συνδεδεμένη τερματική συσκευή (peer) μπορεί να λειτουργήσει τόσο ως ένας διακομιστής όσο και ένας πελάτης. Ένας υπολογιστής μπορεί να αναλάβει το ρόλο του διακομιστή για μια συναλλαγή, ενώ ταυτόχρονα λειτουργεί ως πελάτης για μια άλλη.

Ένα απλό παράδειγμα των P2P δικτύων είναι ένα δίκτυο που εκτός από την κοινή χρήση αρχείων, επιτρέπει στους χρήστες να ενεργοποιήσουν παιχνίδια δικτύων ή να μοιραστούν μια σύνδεση στο Internet.

Peer-to-Peer Εφαρμογές

Μια εφαρμογή P2P επιτρέπει σε μια συσκευή να δρα εντός της ίδιας της επικοινωνίας τόσο ως πελάτης όσο και ένας εξυπηρετητής. Σε αυτό το μοντέλο κάθε πελάτης μπορεί να είναι και διακομιστής και κάθε διακομιστής να είναι και πελάτης. Οι P2P εφαρμογές απαιτούν από κάθε συσκευή να υποστηρίζει και να χρησιμοποιεί κοινές υπηρεσίες.

Με τις εφαρμογές P2P, κάθε υπολογιστής που εκτελεί την εφαρμογή στο δίκτυο μπορεί να λειτουργήσει ως ένας πελάτης ή ένας διακομιστής για άλλους υπολογιστές στο δίκτυο.



Ορισμένες εφαρμογές P2P βασίζονται στο πρωτόκολλο Gnutella. Όπως φαίνεται στο σχήμα, το Gnutella επιτρέπει στους χρήστες να συνδεθούν με τις υπηρεσίες Gnutella μέσω του Διαδικτύου και να εντοπίσουν και να αποκτήσουν πρόσβαση σε πηγές από κοινού με άλλους χρήστες Gnutella. Πολλές εφαρμογές Gnutella είναι διαθέσιμες, συμπεριλαμβανομένων των gtk-gnutella, WireShare, Shareaza, και Bearshare.

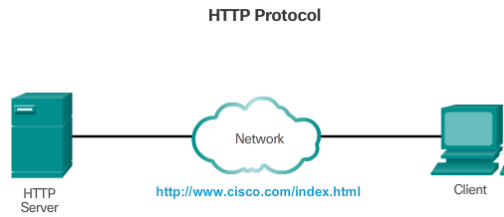
Πολλές εφαρμογές P2P επιτρέπουν στους χρήστες να μοιράζονται ταυτόχρονα με άλλους χρήστες κομμάτια από πολλά αρχεία. Οι πελάτες χρησιμοποιούν ένα μικρό αρχείο που ονομάζεται αρχείο torrent για να εντοπίσουν άλλους χρήστες που έχουν τα κομμάτια που χρειάζονται ώστε να μπορούν να συνδεθούν απευθείας σε αυτούς. Οι πελάτες ζητούν κομμάτια από πολλούς χρήστες ταυτόχρονα, γνωστά ως σμήνος. Αυτή η τεχνολογία ονομάζεται BitTorrent. Υπάρχουν πολλοί πελάτες BitTorrent όπως BitTorrent, uTorrent, Frostwire και qBittorrent.

Μεταξύ των χρηστών μπορεί να μοιραστεί οποιοσδήποτε τύπος αρχείου. Πολλά από αυτά τα αρχεία έχουν πνευματικά δικαιώματα, πράγμα που σημαίνει ότι μόνο ο δημιουργός έχει το δικαίωμα να τα χρησιμοποιήσει για διανομή. Είναι ενάντια στο νόμο να κατεβάζετε ή να διανέμετε αρχεία με πνευματικά δικαιώματα χωρίς την άδεια του κατόχου των πνευματικών δικαιωμάτων. Η παραβίαση πνευματικών δικαιωμάτων μπορεί να οδηγήσει σε ποινικές διώξεις και αστικές αγωγές.

Hypertext Transfer Protocol (HTTP) και Hypertext Markup Language (HTML)

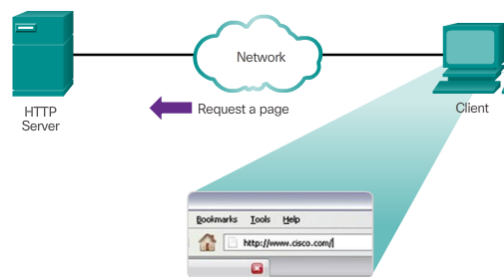
Όταν μια διεύθυνση ιστοσελίδας είναι δακτυλογραφημένοι σε ένα πρόγραμμα περιήγησης, το πρόγραμμα περιήγησης δημιουργεί μια σύνδεση με την υπηρεσία web η οποία εκτελείται στο διακομιστή χρησιμοποιώντας το πρωτόκολλο HTTP. URL και Uniform Resource Identifier (URI) είναι τα ονόματα που οι περισσότεροι άνθρωποι συνδέουν με τις διευθύνσεις ιστοσελίδων.

Για να κατανοήσουμε καλύτερα το πώς το web browser και web server αλληλεπιδρούν, μπορούμε να εξετάσουμε το πώς μια ιστοσελίδα ανοίγει σε ένα πρόγραμμα περιήγησης. Για αυτό το παράδειγμα, χρησιμοποιήστε τη διεύθυνση URL <http://www.cisco.com/index.html>.

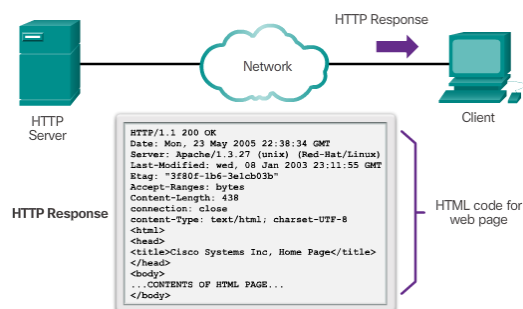


Όπως φαίνεται στο σχήμα, το πρόγραμμα περιήγησης ερμηνεύει τα τρία μέρη του URL:

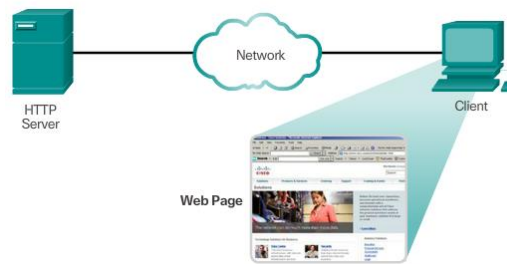
1. http (το πρωτόκολλο)
2. www.cisco.com (το όνομα του διακομιστή)
3. index.html (το συγκεκριμένο όνομα αρχείου που ζητήθηκε)



Το πρόγραμμα περιήγησης ελέγχει στη συνέχεια με ένα διακομιστή ονομάτων για να μετατρέψετε το `www.cisco.com` σε μια αριθμητική διεύθυνση (IP), το οποίο χρησιμοποιεί για να συνδεθεί με το διακομιστή. Χρησιμοποιώντας απαιτήσεις HTTP, ο browser στέλνει ένα αίτημα GET στον server και ζητά για το αρχείο `index.html`.



Ο διακομιστής στέλνει τον κώδικα HTML για αυτήν την ιστοσελίδα στο πρόγραμμα περιήγησης.



Τέλος το πρόγραμμα περιήγησης αποκρυπτογραφεί τον κώδικα HTML και παρουσιάζει τη σελίδα στο παράθυρο του προγράμματος περιήγησης.

HTTP και HTTPS

Το HTTP είναι ένα πρωτόκολλο αιτήματος/απάντησης. Όταν ένας πελάτης, συνήθως ένα web browser, στέλνει μια αίτηση σε έναν web server, το HTTP καθορίζει τους τύπους των μηνυμάτων που χρησιμοποιούνται για την εν λόγω επικοινωνία. Οι τρεις τύποι μηνυμάτων είναι GET, POST, PUT.

- GET - Η αίτηση του πελάτη για τα δεδομένα. Ένας πελάτης (web browser) στέλνει το μήνυμα GET στο διακομιστή web για να ζητήσει σελίδες HTML.
- POST - Προσθήκες αρχείων δεδομένων στο web server όπως δεδομένα φόρμας.
- PUT - Προσθήκες πόρων ή περιεχομένων για να τον web server.

Αν και το HTTP είναι εξαιρετικά ευέλικτο, δεν είναι ασφαλές πρωτόκολλο. Τα μηνύματα αιτήματος στέλνουν πληροφορίες στον server σε μορφή απλού κειμένου και μπορεί να υποκλαπούν. Οι απαντήσεις του server, που συνήθως είναι σελίδες HTML, είναι επίσης χωρίς κρυπτογράφηση.

Για την ασφαλή επικοινωνία μέσω του Internet, χρησιμοποιείται το Secure (HTTPS) πρωτόκολλο HTTP. Το HTTPS χρησιμοποιεί έλεγχο ταυτότητας και κρυπτογράφηση για την ασφάλεια των δεδομένων καθώς μεταδίδονται μεταξύ του πελάτη και του διακομιστή. Το HTTPS χρησιμοποιεί την ίδια διαδικασία απάντησης, αίτημα-εξυπηρετητή-πελάτη, όπως το HTTP, αλλά η ροή δεδομένων είναι κρυπτογραφημένη με Secure Socket Layer (SSL) πριν μεταφερθούν σε όλο το δίκτυο.

Email Protocols

Μία από τις κύριες υπηρεσίες που προσφέρονται από έναν ISP είναι το ηλεκτρονικό ταχυδρομείο. Για να εκτελεστεί σε έναν υπολογιστή ή άλλη συσκευή απαιτεί αρκετές εφαρμογές και υπηρεσίες. Τα μηνύματα ηλεκτρονικού ταχυδρομείου αποθηκεύονται σε βάσεις δεδομένων σε διακομιστές ηλεκτρονικού ταχυδρομείου.

Οι πελάτες του ηλεκτρονικού ταχυδρομείου επικοινωνούν με διακομιστές ηλεκτρονικού ταχυδρομείου για την αποστολή και λήψη email. Οι διακομιστές ηλεκτρονικού ταχυδρομείου επικοινωνούν με άλλους διακομιστές ηλεκτρονικού ταχυδρομείου για να μεταφέρουν μηνύματα από τον ένα τομέα στον άλλο. Ένας email client δεν επικοινωνεί απευθείας με άλλο

πελάτη ηλεκτρονικού ταχυδρομείου κατά την αποστολή email. Αντίθετα οι δύο πελάτες βασίζονται στο διακομιστή αλληλογραφίας για τη μεταφορά μηνυμάτων.

Το Email υποστηρίζει τρία ξεχωριστά πρωτόκολλα λειτουργίας: Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), και IMAP.

SMTP

Οι μορφές μηνυμάτων SMTP απαιτούν μια επικεφαλίδα και το σώμα του μηνύματος. Ενώ το σώμα του μηνύματος μπορεί να περιέχει οποιοδήποτε ποσό του κειμένου, η κεφαλίδα του μηνύματος πρέπει να έχει μια σωστά διαμορφωμένη διεύθυνση email του παραλήπτη και του αποστολέα.

Όταν ένας πελάτης στέλνει email, η διαδικασία πελάτη SMTP συνδέεται με μια διαδικασία SMTP διακομιστή στο γνωστό port 25. Μετά τη σύνδεση, ο πελάτης επιχειρεί να στείλει το μήνυμα του ηλεκτρονικού ταχυδρομείου στο διακομιστή κατά μήκος της σύνδεσης. Όταν ο διακομιστής λαμβάνει το μήνυμα, είτε το τοποθετεί σε έναν τοπικό λογαριασμό, εάν ο αποδέκτης είναι τοπικός ή προωθεί το μήνυμα σε έναν άλλο διακομιστή αλληλογραφίας για παράδοση.

Ο διακομιστής ηλεκτρονικού ταχυδρομείου προορισμού μπορεί να μην είναι σε απευθείας σύνδεση ή μπορεί να είναι απασχολημένος όταν αποστέλλονται μηνύματα ηλεκτρονικού ταχυδρομείου. Ως εκ τούτου, τα μηνύματα SMTP θα σταλούν σε μεταγενέστερο χρόνο. Σε τακτά χρονικά διαστήματα, ο διακομιστής ελέγχει την ουρά για μηνύματα και προσπαθεί να τα στέλνει ξανά. Εάν το μήνυμα εξακολουθεί να μην παραδίδεται μετά από ένα προκαθορισμένο χρονικό διάστημα λήξης, θα επιστρέφεται στον αποστολέα ως μη παραδοτέο.

POP

Η λειτουργία POP χρησιμοποιείται από μια εφαρμογή για να ανακτήσει ένα ηλεκτρονικό μήνυμα από ένα διακομιστή αλληλογραφίας. Με τη λειτουργία POP, γίνεται λήψη της αλληλογραφίας από το διακομιστή στον πελάτη και στη συνέχεια διαγράφεται από τον διακομιστή. Αυτή είναι η προεπιλεγμένη λειτουργία του POP.

Ο διακομιστής ξεκινά την υπηρεσία POP από παθητική ακρόαση στη θύρα TCP 110 για αιτήσεις σύνδεσης πελάτη. Όταν ένας πελάτης θέλει να κάνει χρήση της υπηρεσίας, στέλνει ένα αίτημα για να δημιουργήσει μια σύνδεση TCP με το διακομιστή. Όταν πραγματοποιηθεί η σύνδεση, ο διακομιστής POP στέλνει ένα χαιρετισμό. Ο πελάτης και ο διακομιστής POP στη συνέχεια ανταλλάσσουν εντολές και απαντήσεις έως ότου η σύνδεση κλείσει ή ματαιωθεί.

Με τη λειτουργία POP λαμβάνονται τα μηνύματα ηλεκτρονικού ταχυδρομείου στον πελάτη και απομακρύνονται από το διακομιστή, έτσι δεν υπάρχει καμία κεντρική τοποθεσία όπου φυλάσσονται τα μηνύματα ηλεκτρονικού ταχυδρομείου. Επειδή POP δεν αποθηκεύει

μηνύματα, είναι ανεπιθύμητο για μια μικρή επιχείρηση που χρειάζεται μια κεντρική λύση δημιουργίας αντιγράφων ασφαλείας.

IMAP

Το IMAP είναι ένα άλλο πρωτόκολλο που περιγράφει μια μέθοδο για την ανάκτηση μηνυμάτων ηλεκτρονικού ταχυδρομείου. Σε αντίθεση με το POP, όταν ο χρήστης συνδέεται με έναν IMAP με δυνατότητα διακομιστή γίνεται λήψη των αντιγράφων των μηνυμάτων στην εφαρμογή του πελάτη. Τα πρωτότυπα μηνύματα διατηρούνται στο διακομιστή μέχρι να διαγραφούν χειροκίνητα. Οι χρήστες βλέπουν αντίγραφα των μηνυμάτων στο λογισμικό πελάτη ηλεκτρονικού ταχυδρομείου τους.

Οι χρήστες μπορούν να δημιουργήσουν μια ιεραρχία στα αρχεία που βρίσκονται στο διακομιστή για να οργανώσουν και να αποθηκεύουν την αλληλογραφία. Αυτή η δομή των αρχείων αντιγράφεται και στο ηλεκτρονικό ταχυδρομείο του πελάτη. Όταν ένας χρήστης αποφασίσει να διαγράψει ένα μήνυμα ο διακομιστής συγχρονίζει αυτή τη λειτουργία και διαγράφει το μήνυμα από το διακομιστή.

Domain Name Service (DNS)

Στα δίκτυα δεδομένων, οι συσκευές ταυτοποιούνται με αριθμητικές διευθύνσεις IP για την αποστολή και λήψη δεδομένων μέσω δικτύων. Τα ονόματα (URL) δημιουργήθηκαν για να μετατρέπουν την αριθμητική διεύθυνση σε μια απλή, αναγνωρίσιμο όνομα.

Στο Διαδίκτυο είναι πολύ πιο εύκολο για τους χρήστες να θυμούνται domain names όπως <http://www.cisco.com> σε αντίθεση με την πραγματική αριθμητική διεύθυνση, 198.133.219.25, για αυτόν το διακομιστή. Αν η Cisco αποφασίζει να αλλάξει την αριθμητική διεύθυνση του www.cisco.com, δεν είναι φανερό στον χρήστη, επειδή το domain name παραμένει το ίδιο. Η νέα διεύθυνση απλά συνδέεται με το υπάρχον domain name και η συνδεσιμότητα διατηρείται.

Ιεραρχία DNS

Το πρωτόκολλο DNS χρησιμοποιεί ένα ιεραρχικό σύστημα για να δημιουργήσει μια βάση δεδομένων για να παρέχει ανάλυση των ονομάτων. Η ιεραρχία μοιάζει με ένα ανάποδο δένδρο με τη ρίζα στην κορυφή και τα κλαδιά κάτω. Το DNS χρησιμοποιεί τα domain names για να σχηματίσουν την ιεραρχία.

Η δομή της ονομάτων διασπάται σε μικρές, εύχρηστες ζώνες. Κάθε διακομιστής DNS διατηρεί ένα συγκεκριμένο αρχείο βάσης δεδομένων και είναι υπεύθυνος μόνο για τη διαχείριση των αντιστοιχίσεων των IP ονομάτων για αυτό το μικρό μέρος του συνόλου της δομής DNS. Όταν ένας διακομιστής DNS λάβει μια αίτηση για μετάφραση ονόματος που δεν είναι εντός της ζώνης του, ο διακομιστής DNS προωθεί την αίτηση σε άλλο διακομιστή DNS εντός της κατάλληλης ζώνης για τη μετάφραση.

Τα διάφορα domains αντιπροσωπεύουν είτε τον τύπο του οργανισμού ή τη χώρα προέλευσης. Παραδείγματα των ανώτερων domains είναι:

.com - χρησιμοποιείται για μια επιχείρηση

.org - χρησιμοποιείται για ένα μη-κερδοσκοπικό οργανισμό

.au - Αυστραλία

.CO – Κολομβία

Η εντολή nslookup

Κατά τη ρύθμιση μιας συσκευής του δικτύου, μπορούν να χρησιμοποιηθούν μία ή περισσότερες διευθύνσεις διακομιστή DNS για την ανάλυση ονόματος. Συνήθως η υπηρεσία παροχής Internet (ISP) παρέχει τις διευθύνσεις που θα χρησιμοποιηθούν για τους διακομιστές DNS.

Τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών έχουν επίσης ένα βοηθητικό πρόγραμμα που ονομάζεται nslookup που επιτρέπει στο χρήστη να διερευνήσει χειροκίνητα τους διακομιστές ονομάτων για να επιλύσει ένα host name. Αυτό το βοηθητικό πρόγραμμα μπορεί επίσης να χρησιμοποιηθεί για να αντιμετωπίσει ζητήματα ανάλυσης ονομάτων και να επαληθεύσει την τρέχουσα κατάσταση των εξυπηρετητών ονομάτων.

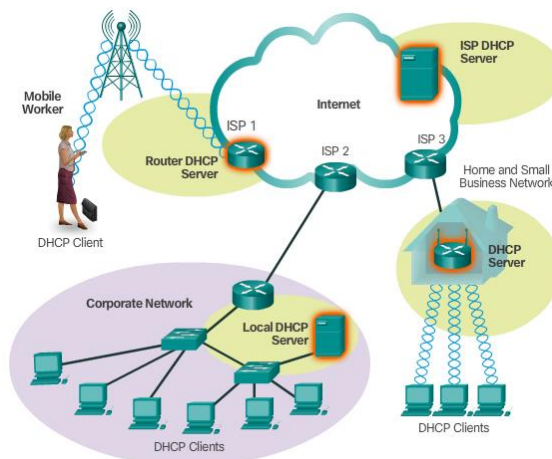
Dynamic Host Configuration Protocol (DHCP)

(Πρωτόκολλο δυναμικής διαμόρφωσης κεντρικού υπολογιστή)

Το Dynamic Host Configuration Protocol (DHCP) για την υπηρεσία IPv4, μοιράζει αυτόματα διευθύνσεις IPv4, τις μάσκες υποδικτύου (Subnet Mask), τη προεπιλεγμένη πύλη (Default Gateway) και άλλες παραμέτρους για να γίνει σωστά η δικτύωση. Αυτό αναφέρεται ως δυναμική ανάθεση. Η εναλλακτική λύση πέραν της δυναμικής ανάθεσης είναι στατική. Όταν χρησιμοποιείται στατική διευθυνσιοδότηση, ο διαχειριστής του δικτύου εισάγει χειροκίνητα πληροφορίες για τη διεύθυνση IP στις συσκευές του δικτύου.

Όταν ένας υπολογιστής συνδέεται στο δίκτυο, ζητά μια διεύθυνση από τον DHCP server. Ο DHCP server επιλέγει μια διεύθυνση από ένα διαμορφωμένο εύρος διευθύνσεων που ονομάζεται pool και το εκχωρεί στη συσκευή.

Σε μεγαλύτερα δίκτυα, ή όπου αλλάζουν συχνά οι χρήστες, προτιμάται το DHCP για εκχώρηση διευθύνσεων. Νέες συνδέσεις γίνονται πιο εύκολα και πιο αποτελεσματικά αν εκχωρούνται αυτόματα με χρήση DHCP αντί να χρησιμοποιείται η στατική εκχώρηση. Τα DHCP διανέμει διευθύνσεις οι οποίες διατηρούνται για ορισμένο χρονικό διάστημα. Όταν η σύνδεση σταματήσει, η διεύθυνση επιστρέφεται στο pool για επαναχρησιμοποίηση.



Όπως φαίνεται στην εικόνα, διάφοροι τύποι συσκευών μπορεί να είναι DHCP servers. Ο διακομιστής DHCP στα περισσότερα μεσαίου προς μεγάλου μεγέθους δίκτυα είναι συνήθως ένας τοπικός διακομιστής. Στα οικιακά δίκτυα, ο DHCP server βρίσκεται συνήθως στο τοπικό δρομολογητή που συνδέει το δίκτυο του σπιτιού με τον ISP.

Πολλά δίκτυα χρησιμοποιούν τόσο DHCP και στατικές διευθυνσιοδοτήσεις. Το DHCP χρησιμοποιείται για τις συσκευές γενικού σκοπού, όπως τερματικές συσκευές. Η στατική διευθυνσιοδότηση χρησιμοποιείται για συσκευές δικτύου, όπως πύλες, μεταγωγείς, εξυπηρετητές και εκτυπωτές.

Το DHCPv6 (DHCP για IPv6) παρέχει παρόμοιες υπηρεσίες για τους χρήστες με διευθύνσεις IPv6. Μια σημαντική διαφορά είναι ότι DHCPv6 δεν παρέχει προεπιλεγμένη διεύθυνση πύλης. Αυτό μπορεί να επιτευχθεί μόνο δυναμικά από το μήνυμα Router Advertisement του δρομολογητή.

File Transfer Protocol (Πρωτόκολλο μεταφοράς αρχείων)

Το FTP είναι ένα άλλο ευρέως χρησιμοποιούμενο πρωτόκολλο επιπέδου εφαρμογής. Το πρωτόκολλο αυτό αναπτύχθηκε για να καταστεί δυνατή η μεταφορά δεδομένων μεταξύ ενός πελάτη και ενός εξυπηρετητή. Ένας πελάτης FTP χρειάζεται μια εφαρμογή που τρέχει σε έναν υπολογιστή που χρησιμοποιεί για να στείλει ή να λάβει δεδομένα από ένα διακομιστή FTP.

Μία συσκευή για να μεταφέρει με επιτυχία τα δεδομένα στο διακομιστή FTP απαιτεί δύο συνδέσεις μεταξύ του πελάτη και του διακομιστή, μία για τις εντολές και τις απαντήσεις και άλλη για την πραγματική μεταφορά αρχείων:

Ο πελάτης δημιουργεί την πρώτη σύνδεση με το διακομιστή για τον έλεγχο της κυκλοφορίας χρησιμοποιώντας τη θύρα TCP 21, που αποτελείται από τις εντολές του πελάτη και τις απαντήσεις του server.

Ο πελάτης καθορίζει τη δεύτερη σύνδεση με το διακομιστή για την πραγματική μεταφορά δεδομένων χρησιμοποιώντας τη θύρα TCP 20. Αυτή η σύνδεση δημιουργείται κάθε φορά που υπάρχουν δεδομένα που πρέπει να μεταφερθούν.

Η μεταφορά των δεδομένων μπορεί να συμβεί με οποιαδήποτε κατεύθυνση. Ο πελάτης μπορεί να κατεβάσει (pull) τα δεδομένα από το διακομιστή, ή ο πελάτης μπορεί να ανεβάσει (push) τα δεδομένα στο διακομιστή.

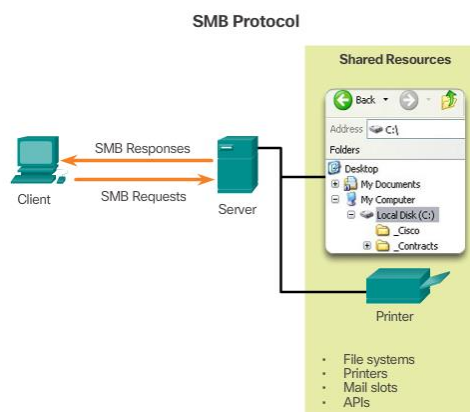
Server Message Block (Μπλοκ μηνυμάτων διακομιστή)

Το μπλοκ μηνυμάτων διακομιστή (SMB) είναι ένα πρωτόκολλο διαμοιρασμού αρχείων πελάτη/διακομιστή το οποίο περιγράφει τη δομή των κοινόχρηστων πόρων του δικτύου όπως, καταλόγους, αρχεία, εκτυπωτές, και σειριακές θύρες. Είναι ένα πρωτόκολλο αίτησης-απάντησης. Όλα τα μηνύματα SMB μοιράζονται μια κοινή μορφή. Αυτή η μορφή χρησιμοποιεί μια σταθερού μεγέθους κεφαλίδα, που ακολουθείται από μια παράμετρο μεταβλητού μεγέθους και συστατικά στοιχεία.

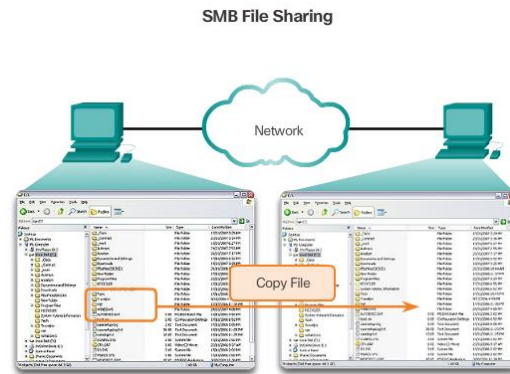
Τα μηνύματα SMB μπορούν:

- Να ξεκινήσουν συνδέσεις, να κάνουν έλεγχο ταυτότητας και να τερματίσουν συνδέσεις.
- Να κάνουν έλεγχο αρχείων και να έχουν πρόσβαση στον εκτυπωτή.
- Να επιτρέψουν μια εφαρμογή να στείλει ή να λάβει μηνύματα προς ή από άλλη συσκευή.

Η κοινή χρήση αρχείων SMB και των υπηρεσιών εκτύπωσης έχουν γίνει ο στυλοβάτης της Microsoft δικτύωσης. Με την εισαγωγή της σειράς λογισμικού των Windows 2000, η Microsoft άλλαξε την υποκείμενη δομή για τη χρήση των SMB. Σε προηγούμενες εκδόσεις των προϊόντων της Microsoft, οι υπηρεσίες SMB χρησιμοποιούν ένα πρωτόκολλο TCP/IP για να εφαρμόσουν την ανάλυση ονόματος. Αρχίζοντας με τα Windows 2000, όλα τα επόμενα προϊόντα της Microsoft χρησιμοποιούν την ονομασία DNS, η οποία επιτρέπει πρωτόκολλα TCP/IP να υποστηρίξουν άμεσα την κοινή χρήση των πόρων SMB, όπως φαίνεται στο Σχήμα.



Η διαδικασία ανταλλαγής αρχείων SMB μεταξύ των Windows PCs φαίνεται στο πιο κάτω σχήμα.



Σε αντίθεση με την κοινή χρήση αρχείων που υποστηρίζονται από το FTP, οι πελάτες δημιουργούσαν μια μακροπρόθεσμη σύνδεση με τους διακομιστές.

Τα λειτουργικά συστήματα Linux και Unix παρέχουν επίσης μια μέθοδο κατανομής των πόρων όπως τα δίκτυα της Microsoft, χρησιμοποιώντας μια έκδοση του SMB που ονομάζεται SAMBA. Τα λειτουργικά συστήματα Apple Macintosh υποστηρίζουν επίσης τη κατανομή των πόρων χρησιμοποιώντας το πρωτόκολλο SMB.

ΜΕΡΟΣ Β

A. Cisco Packet Tracer (CPT)

Το Cisco Packet Tracer(CPT) είναι ένας προσομοιωτής δικτύων της Cisco που μας επιτρέπει να ρυθμίζουμε και να συνδέουμε διάφορες συσκευές για να δημιουργήσουμε ένα εικονικό δίκτυο. Το Cisco Packet Tracer είναι διαθέσιμο για λειτουργικά Windows και Linux, αλλά και για κινητά τηλέφωνα. Για να κατεβάσεις τον προσομοιωτή της Cisco χρειάζεται να κάνεις εγγραφή στο Cisco Networking Academy.

Για να χρησιμοποιήσεις το CPT δεν χρειάζονται εξειδικευμένες γνώσεις προγραμματισμού δικτυακών συσκευών. Αρκούν οι βασικές γνώσεις δικτύων.

Το CPT διαθέτει μια σειρά από προσομοιωμένα πρωτόκολλα στρώματος εφαρμογής, όπως HTTP και DNS, καθώς και βασικά πρωτόκολλα δρομολόγησης με RIP, OSPF και EIGRP.

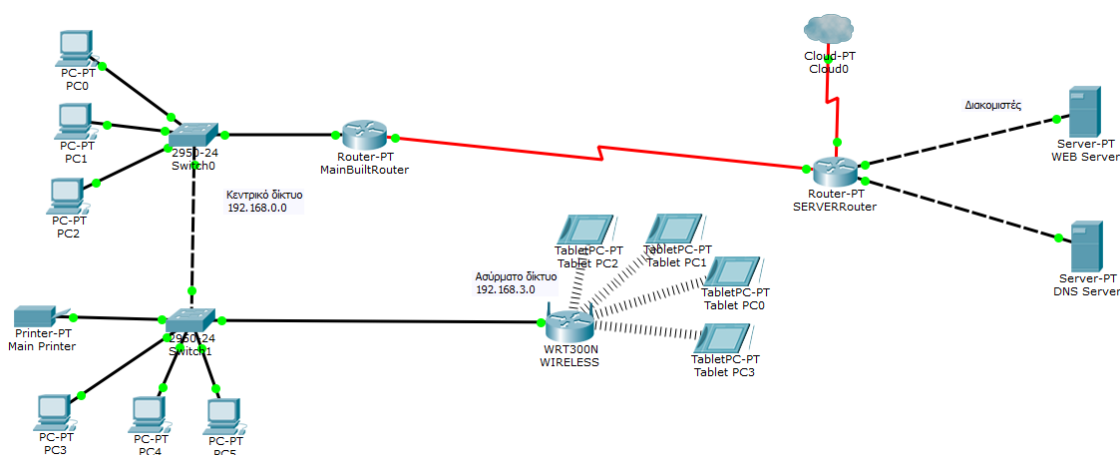
Το γραφικό περιβάλλον του CPT είναι πολύ πρακτικό και πολύ εύκολο στη χρήση. Παρέχει ρεαλισμό στην προσομοίωση, καθώς προσομοιώνει πραγματικές συσκευές σε πραγματικές συνθήκες. Εκτός από το γραφικό περιβάλλον, υπάρχει επίσης και το CLI με το οποίο μπορούμε να προγραμματίσουμε τις δικτυακές συσκευές.

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

Το Packet Tracer 6.2 εισήγαγε την υποστήριξη τηλεφωνίας 3G / 4G, καθώς και ένα νέο Cisco 819 ISR router με ενσωματωμένο ασύρματο σημείο πρόσβασης. Σε αυτήν την έκδοση προστέθηκαν επίσης και οι βελτιώσεις OSPF και EIGRP.

Το Packet Tracer 7.0 έχει κυκλοφορήσει στις 17 Ιουνίου 2016. Αυτή είναι μια νέα σημαντική έκδοση που περιλαμβάνει 3 νέους δρομολογητές Cisco (819IOX, 829, 1240 routers), ένα νέο IE2000 διακόπτη industrial και τεράστια βελτιωμένα πρωτόκολλα. Ακόμη έχουν προστεθεί οι δυνατότητες Python και javascript scripting.

B. Με βάση τα πιο πάνω θα δημιουργήσω και θα παρουσιάσω εικονικά ένα δίκτυο μίας επιχείρησης με τα βασικά συστατικά του και τις βασικές ρυθμίσεις για να μπορεί να λειτουργεί όσο το δυνατόν καλύτερα.



Στην πιο πάνω εικόνα φαίνεται μια απλοποιημένη μορφή του δικτύου. Φυσικά το δίκτυο μπορεί να επεκταθεί και να εξυπηρετήσει περισσότερους χρήστες.

Ο κεντρικός Router έχει ρυθμιστεί ώστε να μοιράζει διευθύνσεις στο κεντρικό δίκτυο. Οι διευθύνσεις των χρηστών εδώ δεν μας ενδιαφέρει να είναι γνωστές και για ευκολία και αποφυγή λαθών αφήνουμε τον DHCP server του Router ελέγχει αυτή τη πτυχή.

```

MainBuiltRouter
Physical Config CLI
IOS Command Line Interface
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
3 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool lan1
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.0.254
Router(dhcp-config)#dns-server 192.168.2.200
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.99
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Copy Paste

```

Στην πιο πάνω εικόνα φαίνονται οι εντολές που δώσαμε στον router για να ρυθμιστεί ώστε να ενεργοποιηθεί ο dhcp και να μοιράζει διευθύνσεις με βάση τους δικούς μας περιορισμούς.

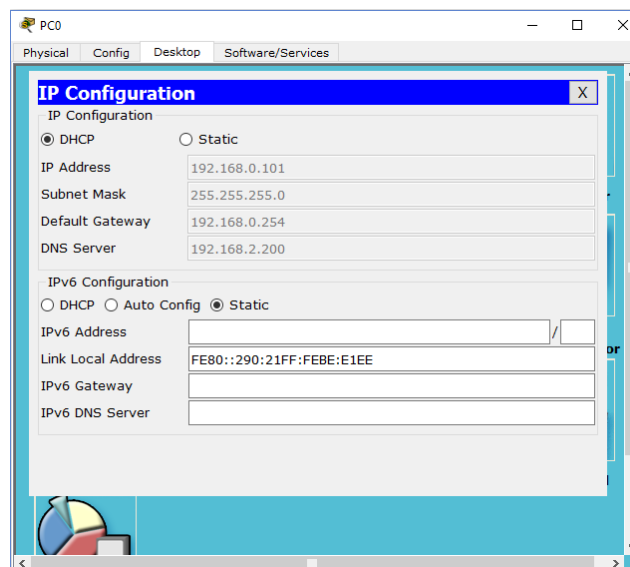
Η εντολή **ip dhcp pool lan1** μας δίνει την δυνατότητα να ρυθμίσουμε το dhcp το οποίο ονομάσαμε lan1. Φαίνεται αμέσως και η αλλαγή του προθέματος σε **Router(dhcp-config)#**.

Η εντολή **network 192.168.0.0 255.255.255.0** καθορίζει το δίκτυο με το subnet mask.

Για να ρυθμίζει αυτόματα το default gateway και τον dns server χρησιμοποιούμε τις εντολές **default 192.168.0.254** και **dns-server 192.168.2.200** αντιστοίχα.

Κάποιες από τις διευθύνσεις θα πρέπει να εξαιρεθούν από το dhcp ούτως ώστε να δοθούν στατικά σε συγκεκριμένες συσκευές, όπως εκτυπωτές για παράδειγμα. Για να το πετύχουμε αυτό δίνουμε την εντολή **ip dhcp exc 192.168.0.1 192.168.0.99** όπου αποκλείουμε τις διευθύνσεις από την 192.168.0.1 μέχρι 192.168.0.99 από τον αυτόματο διαμοιρασμό τους στο δίκτυο.

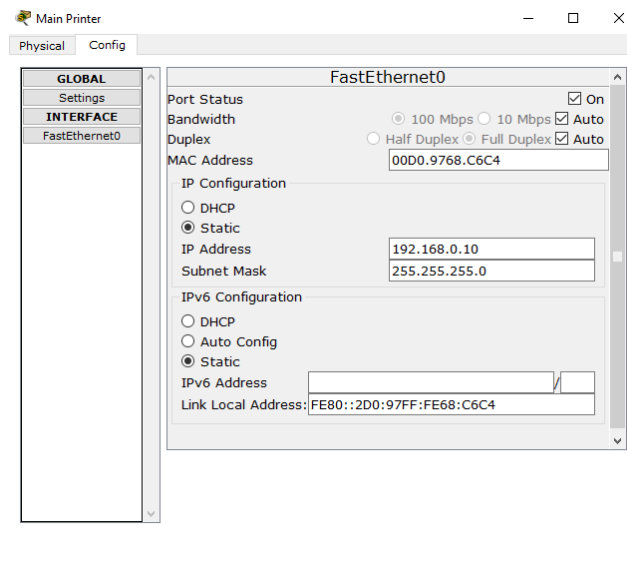
Με βάση τις πιο πάνω ρυθμίσεις στο router, όλες οι συσκευές μπορούν να ρυθμιστούν αυτόματα. Στο πιο κάτω σχήμα βλέπουμε τις ρυθμίσεις που πήρε το PC0 μόλις ενεργοποιήσαμε την αυτόματη ενημέρωση από τον dhcp.



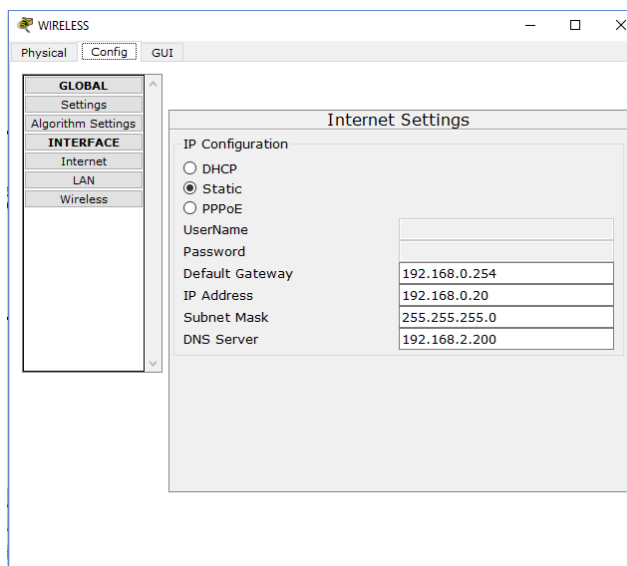
Το ίδιο θα ισχύει για όλες τις συσκευές οι οποίες θα συνδεθούν στο δίκτυο αυτό και θα ρυθμίζονται αυτόματα από τον dhcp του router. Θα καθορίζεται σε όλους μια διαφορετική IP διεύθυνση και τα υπόλοιπα (subnet mask, default gateway και dns server) θα είναι κοινά.

Από αυτή τη διαδικασία εξαιρούνται οι συσκευές που για κάποιο λόγο θα θέλαμε να έχουν μία σταθερή διεύθυνση και να μην αλλάζει ανάλογα με την διαθεσιμότητα διευθύνσεων από τον dhcp. Παράδειγμα είναι οι εκτυπωτές του δικτύου οι οποίοι θα θέλαμε να έχουν μία σταθερή διεύθυνση ούτως ώστε να ρυθμιστούν μία φορά οι υπολογιστές για να τυπώνουν σε

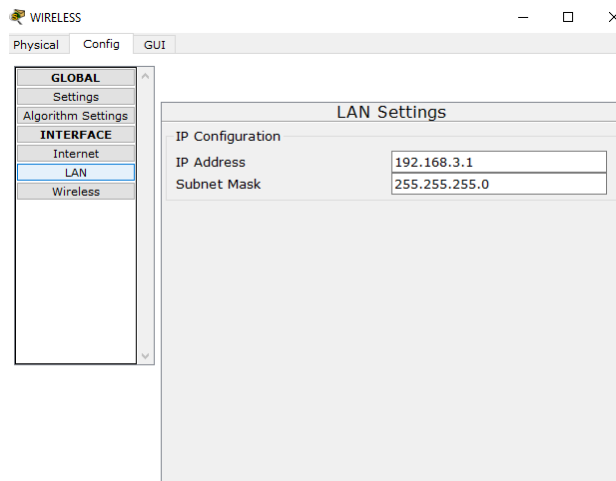
αυτούς και να μην χρειάζεται κάθε φορά να ψάχνουν τις διευθύνσεις του που μπορεί να αλλάζουν. Πιο κάτω φαίνεται η ρύθμιση του Main Printer.



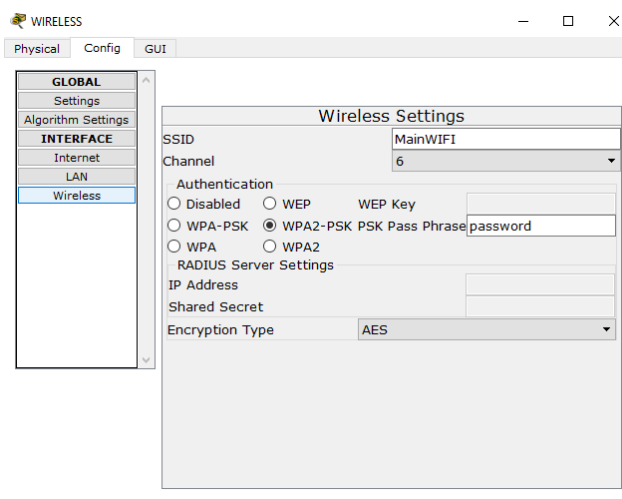
Ο ασύρματος router έχει ρυθμιστεί στατικά και αυτός όπως φαίνεται στο πιο κάτω σχήμα.



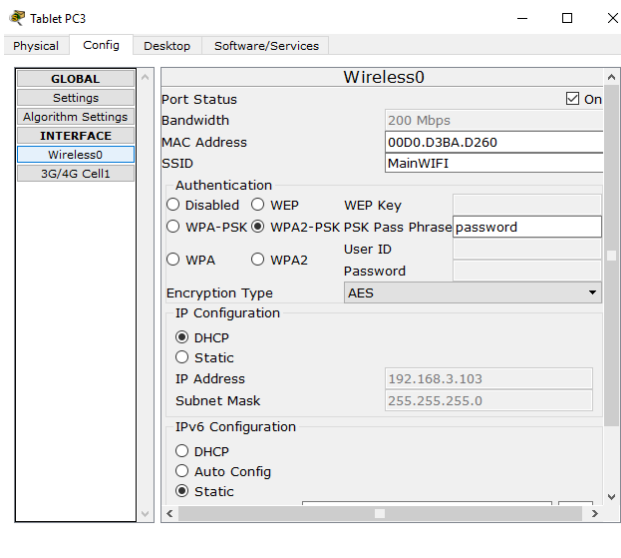
Με τη χρήση του ασύρματος router δημιουργήσαμε ένα καινούριο δίκτυο με αριθμό 192.168.3.0 για περισσότερη ασφάλεια.



Φυσικά το ότι είναι διαφορετικό δίκτυο από το κεντρικό δεν σημαίνει ότι το αφήνουμε ανεξέλεγκτο. Ο κωδικός πρόσβασης είναι προφανής (password). Το SSID (MainWIFI) είναι το όνομα του ασύρματου δικτύου που βλέπουν οι χρήστες.



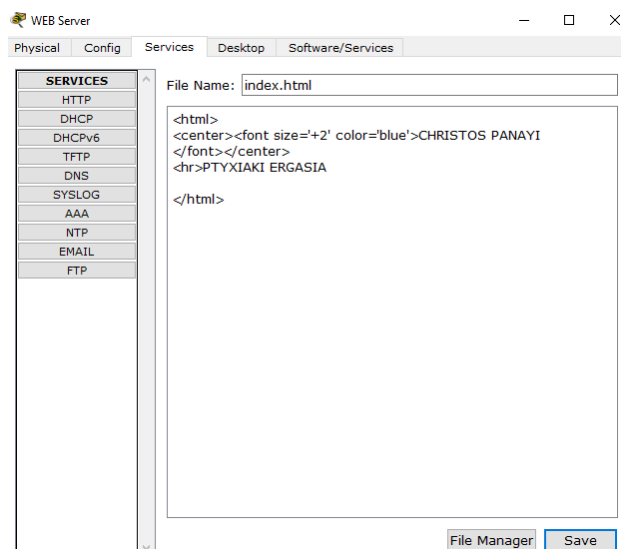
Η κάθε συσκευή που θέλει να συνδεθεί στο ασύρματο δίκτυο θα πρέπει να ρυθμιστεί με το σωστό SSID και κωδικό πρόσβασης όπως φαίνεται η ρύθμιση του Tablet στην πιο κάτω εικόνα.



Διακομιστές

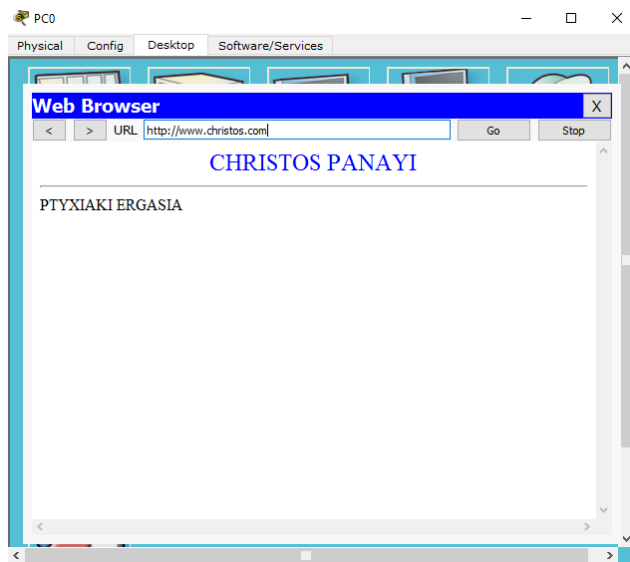
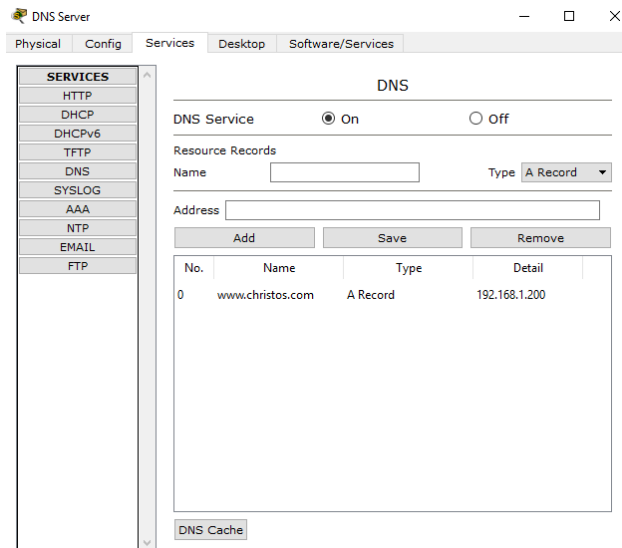
Το δίκτυο με τους διακομιστές είναι ξεχωριστό από το υπόλοιπο δίκτυο. Για παράδειγμα έχω τοποθετήσει δύο διακομιστές, ένα WEB και ένα DNS.

Ο WEB έχει σταθερή διεύθυνση 192.168.1.200 μπορεί να φιλοξενήσει ιστοσελίδες.



Ο DNS έχει σταθερή διεύθυνση 192.168.2.200. Ο ρόλος του στο δίκτυο είναι να μεταφράζει ονόματα ιστοσελίδων σε IP διευθύνσεις και να δίνει τη δυνατότητα στους χρήστες να επισκέπτονται τις ιστοσελίδες χωρίς να γνωρίζουν την IP διεύθυνση της.

Στις δύο πιο κάτω εικόνες φαίνεται η ρύθμιση του DNS να συνδέει το www.christos.com με την διεύθυνση του WEB server 192.168.1.200 και η χρήση της ιστοσελίδας από το PC0.



Για τη σωστή επικοινωνία μεταξύ των δικτύων οι router έχουν ρυθμιστεί να χρησιμοποιούν τον αλγόριθμο RIP για αυτοενημέρωση για όλα τα δίκτυα και αλλαγές που προκύπτουν σε αυτά. Παράδειγμα φαίνεται στο πιο κάτω σχήμα με τη ρύθμιση του MainRouter για αυτό.

MainBuitRouter

PhysicalConfigCLI

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

INTERFACE

FastEthernet0/0

FastEthernet1/0

Serial2/0

Serial3/0

FastEthernet4/0

FastEthernet5/0

Serial6/0

RIP Routing

Network

Add

Network Address

88.0.0.0

192.168.0.0

Remove

Equivalent IOS Commands

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#

Επίλογος

Η σύνδεση συσκευών μεταξύ τους είναι πλέον πολύ σημαντική στον τομέα της πληροφορικής. Η μεταφορά δεδομένων από μία συσκευή σε άλλη είναι μια διαδικασία η οποία σε μερικές περιπτώσεις είναι πολύπλοκη, επικίνδυνη και σημαντική.

Για να γίνει η διαδικασία πιο εύκολη και πιο ασφαλές χωρίζεται σε διαφορετικά επίπεδα στα οποία διαμοιράζεται η ευθύνη και οι ρόλοι.

Συνοψίζοντας το Μέρος Α της εργασίας αυτής θα αναλύσω το πιο κάτω σχήμα που δείχνει τα επτά επίπεδα στα οποία χωρίζεται η όλη διαδικασία με βάση το OSI μοντέλο.



Επίπεδο εφαρμογής - Επίπεδο παρουσίασης - Επίπεδο συνόδου

Αυτά τα τρία επίπεδα μπορούν να ομαδοποιηθούν. Είναι τα επίπεδα όπου έχει άμεση επαφή ο χρήστης. Με την βοήθεια των διαφόρων προγραμμάτων και των αντίστοιχων πρωτοκόλλων που χρησιμοποιεί το καθένα ο χρήστης μπορεί να κάνει χρήση των διαφόρων υπηρεσιών που μπορεί να του παρέχει το δίκτυο.

Επίπεδο Μεταφοράς

Σε αυτό το επίπεδο προετοιμάζεται η επικοινωνία των δύο συσκευών. Γίνονται οι ανάλογες ρυθμίσεις και συνεννοήσεις για την ομαλότερη δυνατή επικοινωνία. Τα πρωτόκολλα TCP και UDP είναι υπεύθυνα για αυτό. Παράλληλα με βάση τα προγράμματα και τα πρωτόκολλα που χρησιμοποιούνται καθορίζονται και τα ανάλογα port numbers τα οποία θα διασφαλίσουν τη σωστή και ασφαλή επικοινωνία. Στα δεδομένα προστίθενται τα port numbers και πλέον τα δεδομένα αποκτούν μορφή με το όνομα segment.

Επίπεδο Δικτύου

Στο επίπεδο δικτύου εμπλέκονται οι router και οι IP διευθύνσεις. Είναι το επίπεδο όπου στα segments τοποθετούνται και οι IP διευθύνσεις (αποστολής και προορισμού) και η μορφή τους παίρνει το όνομα packets. Η δομή των διευθύνσεων είναι σημαντική για τη σωστή επικοινωνία. Αυτό το επίπεδο εμπλέκεται στη διαδικασία στις περιπτώσεις που πρέπει να μεταφέρουμε δεδομένα μεταξύ διαφορετικών δικτύων.

Επίπεδο Σύνδεσης

Χαρακτηριστική συσκευή του επιπέδου σύνδεσης είναι το switch. Σε αυτό το επίπεδο έχουμε την ενσωμάτωση των δεδομένων της φυσικής διεύθυνσης (MAC Address) του αποστολέα και του παραλήπτη. Τα packets αλλάζουν μορφή και πλέον ονομάζονται frames. Το επίπεδο σύνδεσης αναλαμβάνει την επικοινωνία στο εσωτερικό ενός δικτύου.

Φυσικό Επίπεδο

Το πιο χαμηλό επίπεδο στη διαδικασία της επικοινωνίας είναι το φυσικό. Εδώ έχουμε τη μετατροπή των frames σε μορφή που να μπορούν να μεταδοθούν από τα διαθέσιμα μέσα. Είτε σε ηλεκτρικά σήματα για τη μετάδοση μέσω χάλκινων καλωδίων είτε σε φως για χρήση οπτικών ινών είτε σε ηλεκτρομαγνητικά σήματα για μετάδοση μέσω αέρα.

Στο Μέρος Β της εργασίας ασχολήθηκα με τη εικονική δημιουργία ενός δικτύου μιας επιχείρησης χρησιμοποιώντας ένα προσομοιωτή δικτύων. Με σωστή ρύθμιση όλων των συσκευών δημιούργησα ένα δίκτυο μπορεί να εξυπηρετήσει τις ανάγκες της επιχείρησης. Διάφορα σενάρια μπορούν να αλλάξουν τα δεδομένα αλλά με τη βοήθεια του προσομοιωτή έχω τη δυνατότητα να τα αντιμετωπίσω.

Συμπεράσματα

Η τεχνολογία των δικτύων είναι ο τομέας της επιστήμης της πληροφορικής ο οποίος έχει λάβει τα τελευταία χρόνια την μεγαλύτερη εξέλιξη. Οι μελέτες δείχνουν ότι η επόμενη δεκαετία θα επιφέρει αρκετές αλλαγές στον τομέα αυτό λόγω των προβλέψεων της μεγάλης αύξησης που θα έχει ο αριθμός των χρηστών του ίντερνετ παγκόσμια. Άρα είναι ένας τομέας ο οποίος έχει ακόμα πολλά περιθώρια βελτίωσης.

Η γνώση της υφιστάμενης τεχνολογίας είναι κάτι σημαντικό και για εμένα και για όλους όσους θα ήθελαν να ασχοληθούν με την επιστήμη της πληροφορικής. Αυτό ήταν ένα κίνητρο για την εκπόνηση αυτής της εργασίας. Σε μεγάλο βαθμό αυτός ο στόχος επιτεύχθηκε. Μετά από την σχετική έρευνα πάνω στη τεχνολογία των δικτύων κατάφερα να ενημερωθώ κατάλληλα και να είμαι έτοιμος να ακολουθήσω και να συμβάλω αν είναι δυνατόν στην εξέλιξη του τομέα αυτού.

Ελπίζω και πιστεύω πως η εργασία αυτή θα βοηθήσει τον κάθε αναγνώστη να εμπλουτίσει τις γνώσεις του γύρω από τον τόσο σημαντικό τομέα των δικτύων.

Βιβλιογραφία

<http://coolweb.gr/ti-einai-optikes-ines-pos-leitourgoun/>

<http://users.sch.gr/pepoudi/site/pages/page12.html>

<https://el.wikipedia.org/>

<http://www.ifeed.gr/>

www.netacad.com

<http://www.packettracernetwork.com/>

<http://docplayer.gr/2835662-Symvoli-toy-cisco-packet-tracer-sti-didaskalia-toy-mathimatos-diktya-ypologiston-ii-ton-epaggelmatikon-lykeion.html>