Δημιουργία εργαστηριακών ασκήσεων για το μάθημα Δίκτυα Υπολογιστών του τμήματος Ηλεκτρολόγων Μηχανικών

Πτυχιακή Εργασία

Μάρτης 2016
Εισηγητής: Βασιλάκης Κώστας
Σπουδαστής: Χαραλαμπάκος Ορέστης

ΤΕΙ Κρήτης
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

ΠΕΡΙΓΡΑΦΗ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Στόχος της πτυχιακής εργασίας είναι η δημιουργία μιας σειράς εργαστηριακών ασκήσεων για την επίδειξη των επιμέρους στρωμάτων και λειτουργιών ενός δικτύου TCP/IP. Κάθε άσκηση θα αναφέρεται σε ένα συγκεκριμένο δικτυακό στρώμα ή λειτουργία και θα περιλαμβάνει μια εισαγωγική θεωρητική περιγραφή, την πειραματική δικτυακή διάταξη που θα ελέγχεται κάθε φορά, τη διαδικασία και τα βήματα που θα πρέπει να εφαρμοστούν από τον ασκούμενο και τέλος ένα σύνολο ερωτήσεων (και των αντίστοιχων απαντήσεων) που θα καθοδηγούν τον ασκούμενο να παρατηρήσει και να ερμηνεύσει συμβάντα δικτυακής φύσεως χαρακτηριστικά των υπό μελέτη πρωτοκόλλων και λειτουργιών.

Οι ασκήσεις αυτές θα δημιουργηθούν με τέτοιο τρόπο ώστε να είναι έτοιμες να εισαχθούν σε Συστήματα Διαχείρισης Μάθησης που υποστηρίζουν πρότυπο SCORM (content packaging) και να ακολουθούν τη φιλοσοφία της flipped διδασκαλίας όπου μέρος του φόρτου εργασίας εκπονείται πριν τη διεξαγωγή του εργαστηρίου.

Μεθοδολογία εκπόνησης της πτυχιακής:

- Σχεδιασμός των ασκήσεων (μαθησιακά αποτελέσματα, περιεχόμενο, εργαλεία)
- Δημιουργία του εκπαιδευτικού ηλεκτρονικού περιεχομένου.
- Υλοποίηση των ασκήσεων σε SCORM format.
- Ανάρτηση σε Σύστημα Διαχείρισης Μάθησης.
- Συγγραφή της πτυχιακής εργασίας.

Contents

Κεφάλαιο 1ο

Εισαγωγή

Η εξέλιξη της ανθρώπινης κοινωνίας συνοδευόταν πάντα από την ολοένα και καλύτερη γνώση για τον κόσμο που μας περιβάλλει. Η εξέλιξη των επιστημών έδινε συνεχώς στην ανθρωπότητα ένα νέο ποιοτικό ανέβασμα καθώς και νέα αντικείμενα μελέτης και περαιτέρω έρευνας. Όλη αυτή η συσσωρευμένη γνώση χιλιάδων ετών και πολύ περισσότερο των τελευταίων χιλίων χρόνων στην ανθρώπινη ιστορία περνάει από γενιά σε γενιά, γίνεται κοινωνική γνώση. Η εκπαίδευση, και η μάθηση που στο σύγχρονο κόσμο αποτελεί συστατικό μέρος του, αποτελεί ένα κομμάτι αυτής της διαδικασίας.

Η εκπαίδευση δεν ήταν πάντα προσιτή στην πλειοψηφία των ανθρώπων. Στην γραμμή της ιστορίας βλέπουμε ότι η γνώση περιοριζόταν ανάλογα με τις οικονομικές ανάγκες της εποχής, και το ποιος την κατείχε είχε να κάνει και με την κοινωνική του θέση, τη θέση του στην παραγωγή. Τα τελευταία εκατό χρόνια με την εξέλιξη της τεχνολογίας και την ανάπτυξη των μέσων παραγωγής ήταν αναγκαία η πιο μαζική πρόσβαση στην εκπαίδευση, ενός όλο και πιο ειδικευμένου επιστημονικού και τεχνικού δυναμικού, ενώ ακολουθείται από τη σταδιακή αναβάθμιση του επιπέδου των σπουδών.

Το βασικό πρόβλημα με την εκπαίδευση στον καπιταλισμό είναι ότι η συσσωρευμένη γνώση υψηλού επιπέδου, ακόμα και αν για μια δεδομένη φάση - της γοργής καπιταλιστικής ανάπτυξης - «ανοίγει», για να συμπεριλάβει τα παιδιά ευρύτερων κοινωνικών στρωμάτων, σαν τάση έχει να κλείνει ολοένα τη στρόφιγγα με ταξικά φίλτρα και κριτήρια.

Ολοένα και περισσότερο η εκπαίδευση έχει την τάση να κλείνει αυτή τη στρόφιγγα σήμερα. Οδηγεί την πλειοψηφία των παιδιών και των νέων ανθρώπων μακριά από την κατάκτηση της γνώσης της επιστήμης που έχουν επιλέξει να σπουδάσουν. Οδηγεί ολοένα και περισσότερο στην μαζική κατάρτιση , την απόκτηση δεξιοτήτων, χρήσιμων αλλά παροδικών, για την παραγωγή. Αυτά τα ζητήματα δεν

μπορούν αντικειμενικά να λυθούν σε ένα εκμεταλλευτικό σύστημα, καθώς η βάση τους δεν είναι τεχνική, είναι κοινωνική- οικονομική πρώτα και κύρια.

Η απομακρυσμένη εκπαίδευση λοιπόν δεν μπορεί να αποτελέσει τη λύση λόγου χάρη για τις σπουδές ενός παιδιού από μία επαρχιακή πόλη σε ένα τμήμα κάποιου πανεπιστημίου ή ΤΕΙ σε άλλο μέρος μέσω του υπολογιστή. Μπορεί όμως να συμβάλλει αποφασιστικά πλάι σε ένα ολοκληρωμένο σύστημα εκπαίδευσης ώστε να πάει ένα βήμα παραπέρα την μελέτη του εκπαιδευόμενου, χωρίς να υποκαθιστά όμως τον ίδιο το διδάσκοντα, την πρακτική άσκηση του εργαστηρίου και άλλες βασικές πλευρές της εκπαίδευσης.

Απομακρυσμένη εκπαίδευση

Με τον όρο απομακρυσμένη εκπαίδευση θεωρούμε τη διαδικασία της εκπαίδευσης που λαμβάνει χώρα ανεξάρτητα από το χώρο που βρίσκεται ο εκπαιδευτής και ο εκπαιδευόμενος, γενικά χωρίς γεωγραφικούς περιορισμούς.

Απομακρυσμένη εκπαίδευση συναντάμε από τις αρχές του προηγούμενου αιώνα με μαθήματα που διεξάγονταν δια αλληλογραφίας. Με την εξέλιξη της τεχνολογίας και την αλματώδη ανάπτυξη των τηλεπικοινωνιών και των δικτύων υπολογιστών η απομακρυσμένη εκπαίδευση μπήκε σε νέα διάσταση. Με πολύ περισσότερες δυνατότητες μπορούσε πλέον να συμβάλει στο εκπαιδευτικό σύστημα. Συνολικά κάθε τύπος απομακρυσμένης εκπαίδευσης που χρησιμοποιεί τα δίκτυα υπολογιστών ως μέσο επικοινωνίας αναφέρεται στον γενικό όρο ηλεκτρονική μάθηση (e-learning).

Σήμερα Συναντάμε διάφορους τύπους e-learning , από την ταυτόχρονη διδασκαλία και εκπαίδευση ενός διδάσκοντα σε πολλούς μαθητές χωρίς γεωγραφικό περιορισμό αλλά την ίδια χρονική στιγμή, σαν να βρίσκονταν όλοι μαζί σε μία «εικονική αίθουσα» μέχρι την

ασύγχρονη ηλεκτρονική μάθηση που μπορεί είτε να προηγείται του μαθήματος, είτε να έρχεται συμπληρωματικά με αυτό, είτε να αποτελεί το ίδιο το μάθημα.

Θα μπορούσαμε να χωρίσουμε λοιπόν σε τρεις μορφές e-learning:

- Τηλεκπαίδευση σε εξατομικευμένο ρυθμό (self-paced training). Σε αυτή τη μορφή αναφερόμαστε όταν παρέχεται στον μαθητή ένα σύνολο μαθησιακού υλικού το οποίο βρίσκεται στην ευχέρεια και θέληση του πότε θα το χρησιμοποιήσει χωρίς τον περιορισμό ή την καθοδήγηση του διδάσκοντα.
- Ασύγχρονη τηλεκπαίδευση. Η μόνη διαφορά με την παραπάνω μορφή είναι ότι δύνεται η δυνατότητα αλληλεπίδρασης μαθητών τόσο μεταξύ τους , όσο και με τον διδάσκοντα με όρους ασύγχρονης όμως επικοινωνίας
- Η σύγχρονη τηλεκπαίδευση. Αναφερόμαστε στην ταυτόχρονη διδασκαλία όλων των μαθητών που μπορούν να βρίσκονται όμως σε διαφορετικό χώρο. Αυτή η διαδικασία μπορεί να γίνει εφικτή μέσω της τηλεδιάσκεψης ή παρόμοιων τεχνικών.

Η εξέλιξη της τεχνολογίας έχει φέρει και νέα εργαλεία στην διαδικασία της εκπαίδευσης τόσο στην ηλεκτρονική μάθηση, όσο και στην «τυπική». Η αξιοποίηση των παρουσιάσεων slides, το βίντεο, αλλά και διαδραστικές εργασίες βοηθούν το μαθητή στην καλύτερη κατανόηση και αφομοίωση του περιεχομένου του μαθήματος.

Ασύγχρονη τηλέκπαίδευση

Η ασύγχρονη τηλεκπαίδευση αναφέρεται όπως είπαμε και παραπάνω στην διαδικασία κατά την οποία δεν υπάρχει ούτε χρονικός περιορισμός (πέρα από deadlines κλπ), αλλά και ούτε γεωγραφικός κατά τη διάρκεια της εκπαίδευσης. Μπορεί να αποτελεί βοήθημα για την προεργασία του μαθήματος, βοήθημα για την καλύτερη μελέτη μετά από αυτό, αλλά και να αποτελεί το ίδιο το μάθημα.

Η ασύγχρονη τηλεκπαίδευση πατάει πάνω στα δίκτυα υπολογιστών ώστε να λύνει το βασικό πρόβλημα του γεωγραφικού περιορισμού αλλά και στην πρόσβαση, ανά πάσα ώρα, στο εκπαιδευτικό υλικό. Για την πρόσβαση στο εκπαιδευτικό υλικό έχουν δημιουργηθεί πλατφόρμες για την αποθήκευση, την πρόσβαση αλλά και την αλληλεπίδραση των μαθητών με το υλικό. Ένα τέτοιου είδους σύστημα ονομάζεται Learning management system (LMS).

Αντίστοιχα και για την μορφή που παρουσιάζεται το υλικό του μαθήματος έχουν δημιουργηθεί διάφορα πρότυπα ώστε να υπάρχει συμβατότητα με τις πλατφόρμες ασύγχρονης τηλεκπαίδευσης.

Ορισμένα πρότυπα περιγραφής του μαθησιακού υλικού είναι τα εξής:

- Το πρότυπο AICC (Aviation Industry CBT(Computer Based Training Committee)
- Το πρότυπο IMS Global Learning Consortium το οποίο βασίζεται στην XML.
- Το πρότυπο SCORM (Sharable Content Object Reference Model) το οποίο δημιουργήθηκε για να συνενώσει τα υπόλοιπα πρότυπα και βασίζεται επίσης στην XML.

ELearning authority tools

Πέρα από το περιεχόμενο των μαθημάτων ιδιαίτερο ρόλο στην διαδικασία της αφομοίωσης του, παίζει ο τρόπος που παρουσιάζεται καθώς και η δυνατότητα να είναι διαδραστικό, δηλαδή να μπορεί ο εκπαιδευόμενος να έχει αλληλεπίδραση με αυτό. Η παρουσίαση τους σε slides, ερωτήσεις και παιχνίδια που θα βοηθούν στην κατανόηση του μαθήματος είναι σημαντικό κομμάτι του ELearning.

Έχουν αναπτυχθεί αρκετά εργαλεία σύνταξης ηλεκτρονικού περιεχομένου μαθημάτων που δίνουν αρκετές δυνατότητες στην παρουσίαση των μαθημάτων , στην δημιουργία ελκυστικού προς τους μαθητές περιεχόμενο. Τα εργαλεία αυτά, συνήθως, απαιτούν ελάχιστες

γνώσεις προγραμματισμού, web design , πράγμα που τα καθιστά εύκολα στην χρήση από τους εκπαιδευτές ανεξάρτητα από το αντικείμενο της διδασκαλίας τους.

Μερικά από τα πιο γνωστά ELearning authority tools είναι τα παρακάτω.

1. **Adobe Presenter 11**. Το συγκεκριμένο εργαλείο αποτελεί ένα πολύ εύχρηστο πρόγραμμα ανάπτυξης eLearning περιεχομένου καθώς δίνει την δυνατότητα να μετατρέψουμε απευθείας τις παρουσιάσεις σε PowerPoint σε διαδικτυακό περιεχόμενο. Είναι ιδιαίτερα βολικό στη χρήση ακόμα και από αρχάριους χρήστες, όμως έχει περιορισμένες δυνατότητες.
2. **The Xerte Project**. Πρόκειται για ένα εργαλείο που έχει παραχθεί από το Πανεπιστήμιο του Nottingham και έχει στόχο να βοηθήσει τους εκπαιδευτές να δημιουργήσουν υψηλής ποιότητας εκπαιδευτικό υλικό. Με ευκολία μπορούμε να δημιουργήσουμε διαδραστικό υλικό, να προσθέσουμε πολυμεσικό περιεχόμενο ώστε να τραβάει το ενδιαφέρον των μαθητών.
3. **Quick Lessons**. Το εργαλείο Quick Lessons αποτελεί μία πολύ εύχρηστη online πλατφόρμα που δίνει αρκετές δυνατότητες στην συγγραφή eLearning υλικού. Δεν χρειάζεται να έχουμε προγραμματιστικές γνώσεις ή γνώσεις web design. Μπορούμε να εξάγουμε το υλικό μας σε μορφή HTML5, να μετατρέψουμε παρουσιάσεις σε PowerPoint σε μορφή Flash, καθώς και εξαγωγή σε πρότυπο SCORM και AICC.
4. **Composica**. Είναι μια άλλη συνεργατική πλατφόρμα που μας δίνει τη δυνατότητα να αναπτύξουμε εξαιρετικά διαδραστικά μαθήματα eLearning . Η έννοια της συλλογικής σύνταξης συνδέει τους συγγραφείς μέσω ενός blog για το project ,με ατομικές και ομαδικές συζητήσεις. Μπορούμε να κατηγοριοποιήσουμε την ομάδα μας σε τρία επίπεδα : στους προγραμματιστές (έχουν πρόσβαση σε όλα), στους

συνεργάτες (μπορούν να έχουν πρόσβαση σε ορισμένα χαρακτηριστικά), και σε αυτούς που έχουν δικαίωμα προβολής (που μπορούν να επεξεργαστούν το έργο σε κάποιο βαθμό, αλλά δεν μπορούν να προσθέσουν νέο περιεχόμενο). Μπορούμε να χρησιμοποιήσουμε το Composica ώστε να παραδοθούν τα μαθήματα σε οποιαδήποτε συσκευή , έτσι ώστε οι μαθητές να μπορούν να έχουν πρόσβαση μέσω tablet, επιτραπέζιους υπολογιστές και κινητά .

5. **Udutu**. Είναι ένα ελεύθερο εργαλείο ανάπτυξης το οποίο μας επιτρέπει να δημιουργήσουμε εκπαιδευτικό υλικό μέσω διαμορφωμένων θεμάτων και templates.
6. **Lesson Writer**. Το εργαλείο αυτό μας δίνει την δυνατότητα, πέρα από την απλή συγγραφή των μαθημάτων να διαμορφώσουμε ολόκληρο το πρόγραμμα σπουδών, ο τρόπος και το πως θα γίνονται τα μαθήματα με βάση το πλάνο του μαθήματος. Ακόμα δίνει τη δυνατότητα της συνεργασίας μεταξύ των εκπαιδευτικών ώστε να μπορεί να καλυφθεί μία ολόκληρη εκπαιδευτική μονάδα από το συγκεκριμένο εργαλείο.
7. **iSpring Suite**. Με αυτό το εργαλείο μπορούμε να δημιουργήσουμε τα μαθήματα που θα προσαρμόζονται στο μέγεθος της οθόνης του θεατή , έτσι ώστε οι μαθητές να έχουν πρόσβαση σε αυτά από οποιαδήποτε συσκευή . Η πλατφόρμα υποστηρίζει διαδραστικές ασκήσεις, μαγνητοσκόπησης της οθόνης , βίντεο και πολλά άλλα.
8. **Easygenerator**. Πρόκειται για μία online πλατφόρμα που μας δίνει τη δυνατότητα να δημιουργήσουμε ELearning περιεχόμενο χωρίς να χρειάζεται να εγκαταστήσουμε στον υπολογιστή μας το εν λόγω πρόγραμμα. Δίνει τη δυνατότητα να δημιουργήσουμε ασκήσεις και quizzes διαφόρων τύπων όπως πολλαπλής επιλογής, συμπλήρωσης κενών κλπ. Ακόμα με την ελεύθερη έκδοση τους μπορούμε να

χρησιμοποιήσουμε την ίδια την πλατφόρμα ώστε να διαθέσουμε το υλικό μας.

9. **authorPOINT.** Με το authorPOINT μπορούμε να μετατρέψουμε τα αρχεία PowerPoint σε μορφή SCORM. Αυτό είναι ένα από τα καλύτερα εργαλεία την ανάπτυξη παρουσιάσεων και πολυμέσων . Είναι συμβατό με την πλατφόρμα WiZiQ , η οποία μοιάζει με μια εικονική αίθουσα διδασκαλίας που υποστηρίζει συνομιλία , ανταλλαγή περιεχομένου , επικοινωνία μέσω ήχου και βίντεο , καθώς και λειτουργίες εγγραφής του μαθήματος .
10. **GoAnimate**. Με το συγκεκριμένο εργαλείο μπορούμε να φτιάξουμε βίντεο κινουμένων σχεδίων με τα οποία μπορούμε να κάνουμε ενδιαφέρον το μάθημα μας. Δεν είναι τόσο εύκολο στη χρήση και χρειάζεται γνώσεις προγραμμάτων δημιουργίας πολυμεσικού υλικού ώστε να το χρησιμοποιήσουμε.

Κεφάλαιο 2ο
Δημιουργία εργαστηριακού Οδηγού

Ένα μεγάλο μέρος της παρούσης πτυχιακής αφορά την συγγραφή του εργαστηριακού οδηγού καθώς και των ασκήσεων για το μάθημα «Δίκτυα Υπολογιστών» του τμήματος των Ηλεκτρολόγων Μηχανικών. Για να υποστηρίζει την flipped διδασκαλία ο οδηγός αυτός πρέπει να καλύπτει επαρκώς την ανάγκη θεωρητικής εκπαίδευσης των μαθητών προτού προχωρήσει στις ασκήσεις του εργαστηρίου.

Ο εργαστηριακός Οδηγός αποτελείται από δέκα κεφάλαια – μαθήματα. Το κάθε ένα από αυτά περιέχει τόσο το θεωρητικό μέρος όσο και τις ερωτήσεις καθώς και τις εργαστηριακές ασκήσεις. Στο τελευταίο κεφάλαιο δίδεται τελικό project που ενοποιεί τις γνώσεις που αποκτήθηκαν.

Κεφάλαιο 1ο

Εισαγωγή στα Δίκτυα Υπολογιστών

Εξερευνώντας τα Δίκτυα

Βρισκόμαστε σε μια κρίσιμη καμπή στη χρήση της τεχνολογίας για την επέκταση και ενδυνάμωση της ικανότητά μας να επικοινωνούμε. Η παγκοσμιοποίηση του Διαδικτύου έχει επιταχυνθεί ταχύτερα από κάθε φαντασία. Ο τρόπος με τον οποίο αξιοποιείται σήμερα, για κοινωνικές, εμπορικές και προσωπικές επικοινωνίες μεταβάλλεται ραγδαία ώστε να συμβαδίσει με την εξέλιξη αυτού του παγκόσμιου δικτύου. Στο επόμενο στάδιο της ανάπτυξής μας το Διαδίκτυο θα χρησιμοποιείται ως ένα σημείο εκκίνησης, δημιουργώντας νέα προϊόντα και υπηρεσίες που έχουν σχεδιαστεί ειδικά για να επωφεληθούν από τις δυνατότητες του δικτύου.

Σε αυτό το κεφάλαιο θα έρθουμε σε επαφή με βασικές έννοιες των δικτύων, προσπαθώντας να απαντήσουμε στην ερώτηση: Τι είναι τελικά το Internet ;

Εφαρμογές του Internet στην καθημερινότητα

Ανάμεσα σε όλα τα απαραίτητα για την ανθρώπινη ύπαρξη, η ανάγκη για να επικοινωνία κατατάσσεται ακριβώς κάτω από την ανάγκη μας για τη διατήρηση της ζωής . Η επικοινωνία είναι σχεδόν το ίδιο σημαντική για εμάς όσο εξάρτησή μας από τον αέρα , το νερό , τα τρόφιμα και στέγη .

Στο σημερινό κόσμο , μέσω της χρήσης των δικτύων , είμαστε συνδεδεμένοι όπως ποτέ πριν . Οι άνθρωποι με ιδέες μπορούν να επικοινωνούν άμεσα με τους άλλους για να κάνουν αυτές τις ιδέες πραγματικότητα . Νέα και εκδηλώσεις, ανακαλύψεις, γίνονται παγκοσμίως γνωστά μέσα σε λίγα δευτερόλεπτα . Μπορούμε να συνδεθούμε , να μιλήσουμε, να παίξουμε παιχνίδια με ανθρώπους από την άλλη άκρη του κόσμου!

Το Internet εξελίσσει την εκπαίδευση , φέρνοντας τη γνώση ουσιαστικά στο σπίτι μας. Το υλικό αυτού του μαθήματος είναι μια ζωντανή απόδειξη.

Το Internet εξελίσσει τον τρόπο με τον οποίο επικοινωνούμε φέρνοντας νέους τρόπους στη ζωή μας. Τα κοινωνικά δίκτυα, τα εργαλεία που μα βοηθούν να συνεργαζόμαστε με τους συναδέλφους μας χωρίς να παίζει ρόλο ο τόπος , ακόμα και ο χρόνος. Από τους πιο διαδεδομένους τρόπους για το διαμοιρασμό αρχείων που όλοι γνωρίζουμε από τα torrents είναι οι Peer-to-Peer (P2P) εφαρμογές.

Το Internet εξελίσσει την ψυχαγωγία μας. Ταινίες, μουσική, online games και πολλές άλλες εφαρμογές βρίσκονται μόλις ένα κλικ μακριά από τον υπολογιστή μας.

Δίκτυα για όλα τα γούστα. Τι είναι το Internet ;

Δίκτυα έρχονται σε όλα τα μεγέθη. Μπορούν να κυμαίνονται από απλά δίκτυα που αποτελούνται από δύο υπολογιστές σε δίκτυα που συνδέουν εκατομμύρια συσκευές.

Small Home Networks

Τα απλά δίκτυα που έχουμε στο σπίτι και μπορούμε να συνδέσουμε τον υπολογιστή μας, το smartphone, τον εκτυπωτή, ακόμα και την τηλεόραση μας και να διαμοιράζουμε τα αρχεία μας, έγγραφα, εικόνες, μουσική, βίντεο σε αυτό το δίκτυο.

Small Office/Home Office Networks

Τα οικιακά δίκτυα γραφείου και μικρά εταιρικά δίκτυα αφορούν επαγγελματίες που έχουν ένα μικρό γραφείο, ή δουλεύουν από το σπίτι και χρειάζονται απομακρυσμένη πρόσβαση στους πόρους του εταιρικού τους δικτύου. Επιπλέον, πολλοί αυτοαπασχολούμενοι χρησιμοποιούν το γραφείο στο σπίτι και μικρά εταιρικά δίκτυα για να διαφημίζουν και να πωλούν τα προϊόντα, να παραγγέλνουν αναλώσιμα και να επικοινωνούν με τους πελάτες.

Medium to Large Networks

Σε επιχειρήσεις και μεγάλους οργανισμούς, τα δίκτυα μπορούν να χρησιμοποιηθούν σε μια ακόμα ευρύτερη κλίμακα για να παρέχει ενοποίηση, την αποθήκευση και πρόσβαση σε πληροφορίες σχετικά με τους διακομιστές του δικτύου. Δίκτυα που επιτρέπουν επίσης την ταχεία επικοινωνία, όπως e-mail, instant messaging, και τη συνεργασία μεταξύ των εργαζομένων. Εκτός από τα εσωτερικά οφέλη, πολλοί οργανισμοί χρησιμοποιούν τα δίκτυά τους για την παροχή προϊόντων και υπηρεσιών στους πελάτες μέσω της σύνδεσής τους στο Διαδίκτυο.

World Wide Network

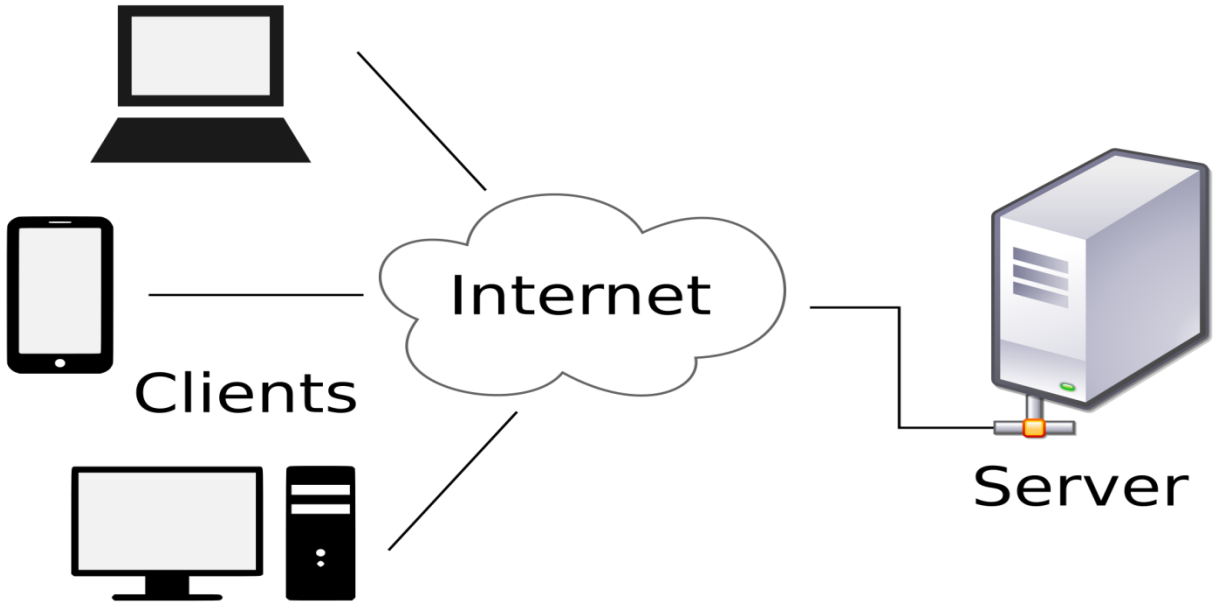
Το Διαδίκτυο είναι το μεγαλύτερο δίκτυο στην ύπαρξη. Στην πραγματικότητα, ο όρος Διαδικτύου σημαίνει ένα «δίκτυο των δικτύων». Το Διαδίκτυο είναι κυριολεκτικά μια συλλογή αλληλοσυνδεόμενων ιδιωτικά και δημόσια δίκτυα, όπως αυτά που περιγράφονται παραπάνω

Πελάτες και Διακομιστές (Clients and Servers)

Όλοι οι υπολογιστές που είναι συνδεδεμένοι σε ένα δίκτυο που συμμετέχουν άμεσα στην επικοινωνία του δικτύου χαρακτηρίζονται ως Hosts. Hosts ονομάζονται επίσης οι τερματικές συσκευές (End devices).

Οι Servers είναι υπολογιστές με λογισμικό που τους επιτρέπουν να παρέχουν πληροφορίες, όπως το ηλεκτρονικό ταχυδρομείο ή ιστοσελίδες, σε άλλες τερματικές συσκευές του δικτύου. Κάθε υπηρεσία απαιτεί ξεχωριστό λογισμικό διακομιστή. Για παράδειγμα, ένας διακομιστής απαιτεί το λογισμικό του web server για την παροχή διαδικτυακών υπηρεσιών στο δίκτυο. Ένας υπολογιστής με λογισμικό διακομιστή μπορεί να παρέχει υπηρεσίες ταυτόχρονα σε ένα ή πολλούς πελάτες. Επιπλέον, σε έναν υπολογιστή μπορεί να τρέχουν πολλοί τύποι του λογισμικού του διακομιστή. Σε ένα σπίτι ή μικρή επιχείρηση, μπορεί να είναι

απαραίτητο για έναν υπολογιστή να ενεργεί ως διακομιστής αρχείων, έναν web server, και ένα e-mail server.



Οι πελάτες είναι υπολογιστές με εγκατεστημένο λογισμικό που τους επιτρέπουν να ζητήσουν και να εμφανίσουν τις πληροφορίες που θα λάβουν από το διακομιστή. Ένα παράδειγμα του λογισμικού πελάτη είναι ένα πρόγραμμα περιήγησης στο Web, όπως το Chrome ή το Firefox. Σε έναν υπολογιστή μπορεί επίσης να τρέχουν πολλοί τύποι λογισμικού πελάτη. Για παράδειγμα, ένας χρήστης μπορεί να ελέγξει το e-mail και να δει μια ιστοσελίδα, ενώ χρησιμοποιεί instant messaging και να ακούει ραδιόφωνο στο Internet.

Ομότιμη Επικοινωνία (Peer to Peer)

Client-Server λογισμικό τρέχει συνήθως σε διαφορετικούς υπολογιστές, αλλά είναι επίσης δυνατό για έναν υπολογιστή να πραγματοποιήσει και τους δύο ρόλους ταυτόχρονα. Σε μικρές επιχειρήσεις και σπίτια , πολλοί υπολογιστές λειτουργούν ως

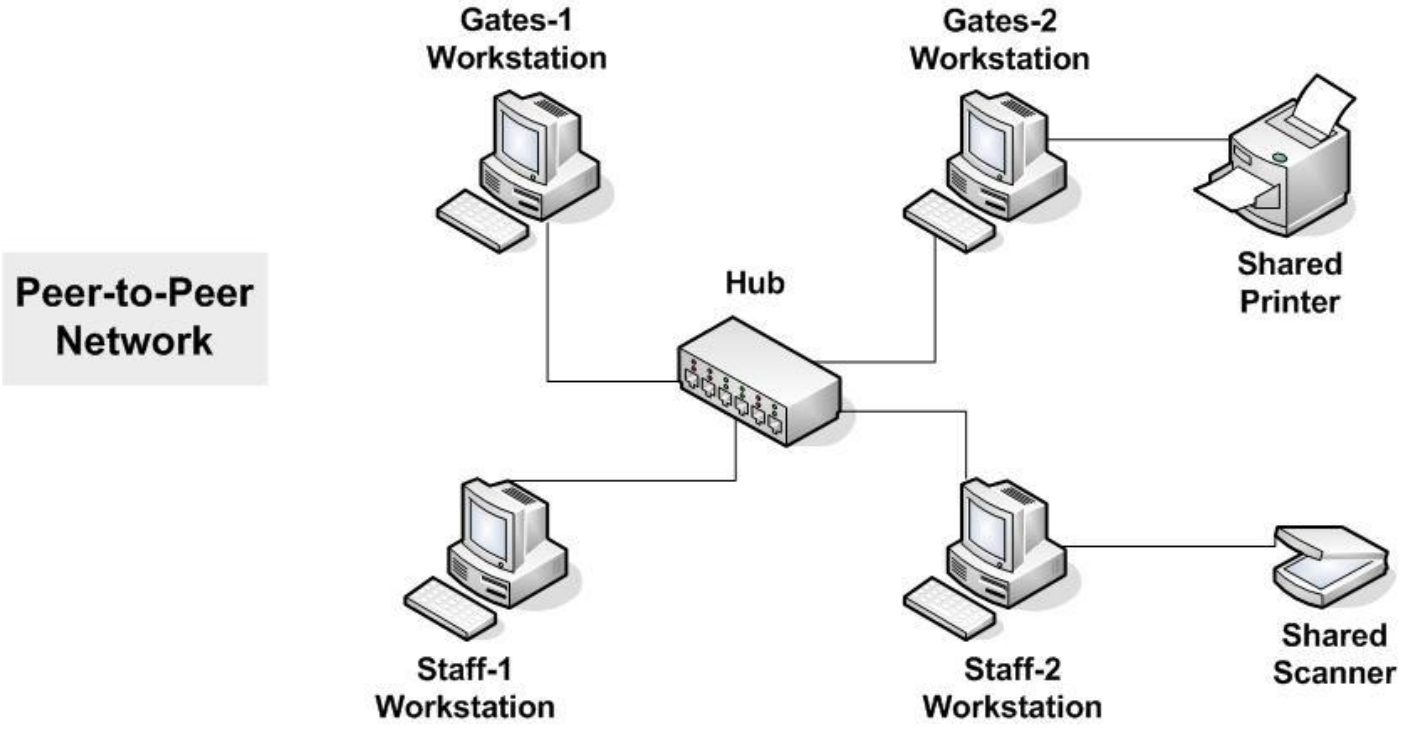
Servers και Clients στο δίκτυο . Αυτός ο τύπος του δικτύου ονομάζεται δίκτυο peer - to-peer.

Τα πλεονεκτήματα των peer-to - peer δίκτυα :

- Εύκολο στην εγκατάσταση
- Λιγότερη πολυπλοκότητα
- Χαμηλό κόστος
- Μπορεί να χρησιμοποιηθεί για απλές εργασίες, όπως η μεταφορά αρχείων και κοινή χρήση εκτυπωτών

Τα μειονεκτήματα των peer-to - peer δίκτυα :

- Δεν υπάρχει κεντρική διαχείριση
- Δεν είναι τόσο ασφαλές
- Όλες οι συσκευές μπορούν να ενεργούν ως Clients και Servers που μπορεί να επιβραδύνει την απόδοσή τους

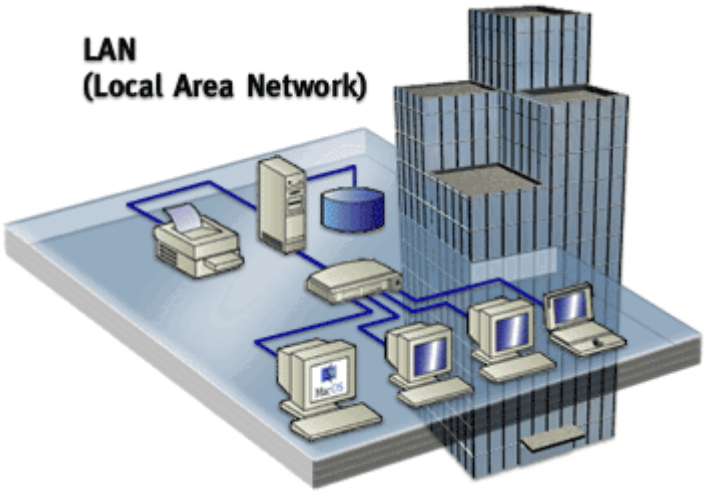


Κατηγοριοποίηση των Δικτύων

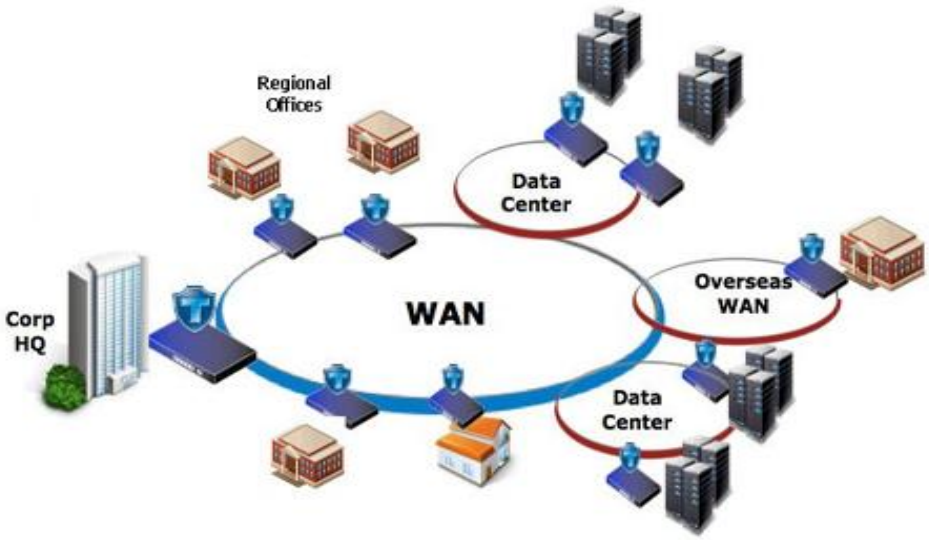
Οι δικτυακές υποδομές μπορεί να διαφέρουν σε μεγάλο βαθμό όσον αφορά:

- Μέγεθος της περιοχής που καλύπτεται
- Αριθμός χρηστών που είναι συνδεδεμένοι
- Αριθμός και τύποι των διαθέσιμων υπηρεσιών
- Τομέας ευθύνης

Τοπικό Δίκτυο (Local Area Network -LAN) : Μια δικτυακή υποδομή που παρέχει πρόσβαση στους χρήστες και συσκευές τελευταίας τεχνολογίας σε μια μικρή γεωγραφική περιοχή, η οποία είναι συνήθως μια επιχείρηση, το σπίτι ή μικρό δίκτυο επιχειρήσεων και διοικείται από ένα άτομο ή το τμήμα πληροφορικής.



Δικτύου ευρείας περιοχής (Wide Area Network -WAN) - Μια δικτυακή υποδομή που παρέχει πρόσβαση σε άλλα δίκτυα σε μια ευρεία γεωγραφική περιοχή, η οποία τυπικά ανήκει και διοικείται από έναν φορέα παροχής τηλεπικοινωνιακών υπηρεσιών.



Άλλοι τύποι δικτύων περιλαμβάνουν:

Δίκτυο Μητροπολιτικής Περιοχής (Metropolitan Area Network - MAN) - Η δικτυακή υποδομή που εκτείνεται σε ένα φυσικό χώρο μεγαλύτερο από ένα τοπικό δίκτυο, αλλά μικρότερη από ένα WAN (π.χ., μια πόλη).

Δίκτυο περιοχής αποθήκευσης (Storage Area Network - SAN) - Μια δικτυακή υποδομή που έχει σχεδιαστεί για να υποστηρίξει τους servers αρχείων και να παρέχει την αποθήκευση δεδομένων, την ανάκτηση, και την αναπαραγωγή τους.

Intranet – Extranet

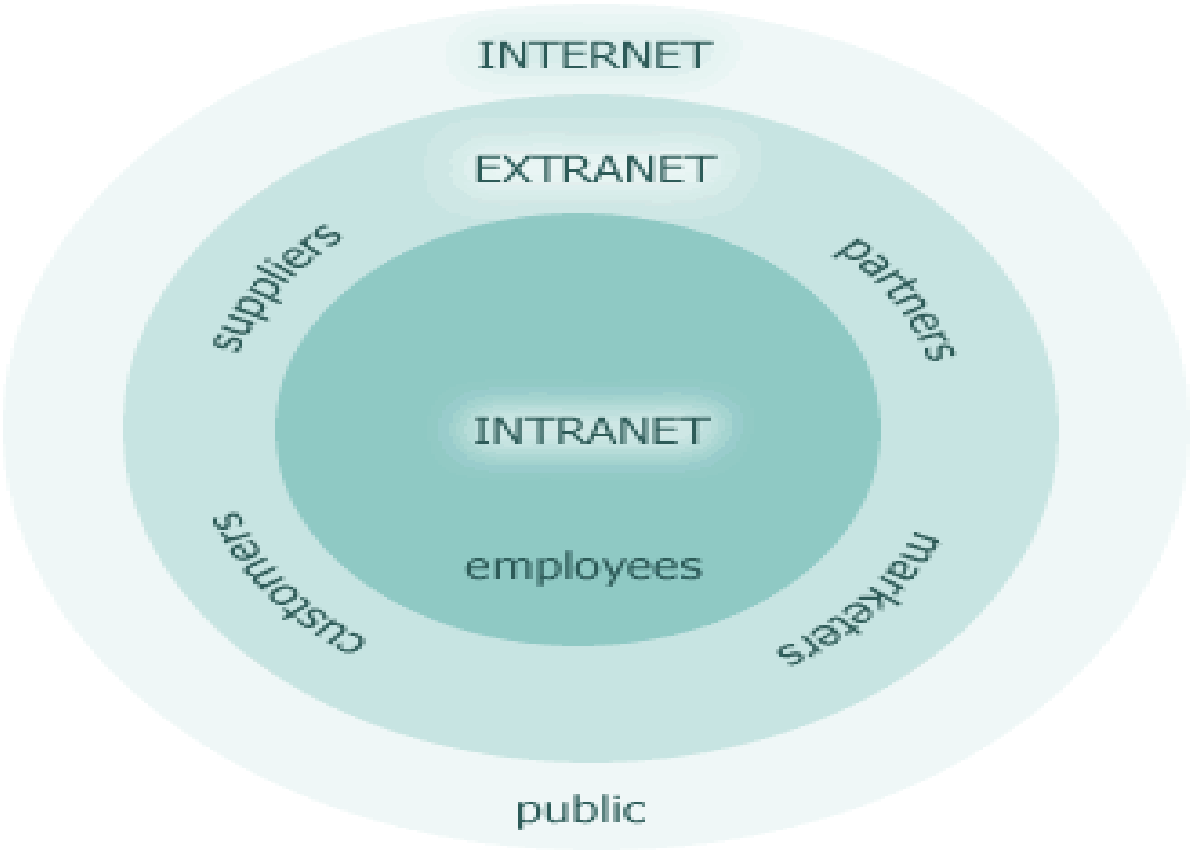
Υπάρχουν δύο άλλοι όροι που είναι παρόμοιοι με τον όρο Διαδίκτυο :

- Intranet
- Extranet

Intranet: Είναι ένας όρος που χρησιμοποιείται συχνά για να αναφερθεί σε μια ιδιωτική σύνδεση των τοπικών δικτύων και ευρυζωνικών δικτύων, που ανήκει σε έναν οργανισμό , και έχει σχεδιαστεί ώστε να είναι προσβάσιμο μόνο από τα μέλη του οργανισμού, τους εργαζόμενους , ή άλλους με άδεια .

Ένας οργανισμός μπορεί να χρησιμοποιήσει ένα extranet να παρέχει ασφαλή και ασφαλή πρόσβαση σε άτομα που εργάζονται για μια διαφορετική οργάνωση , αλλά απαιτούν πρόσβαση στα δεδομένα του οργανισμού .

Παραδείγματα extranets περιλαμβάνουν : Μια εταιρεία που παρέχει πρόσβαση σε εξωτερικούς προμηθευτές και εργολάβους . Ένα νοσοκομείο που παρέχει ένα σύστημα κράτησης για τους γιατρούς ώστε να μπορούν να κλείσουν ραντεβού για τους ασθενείς τους .



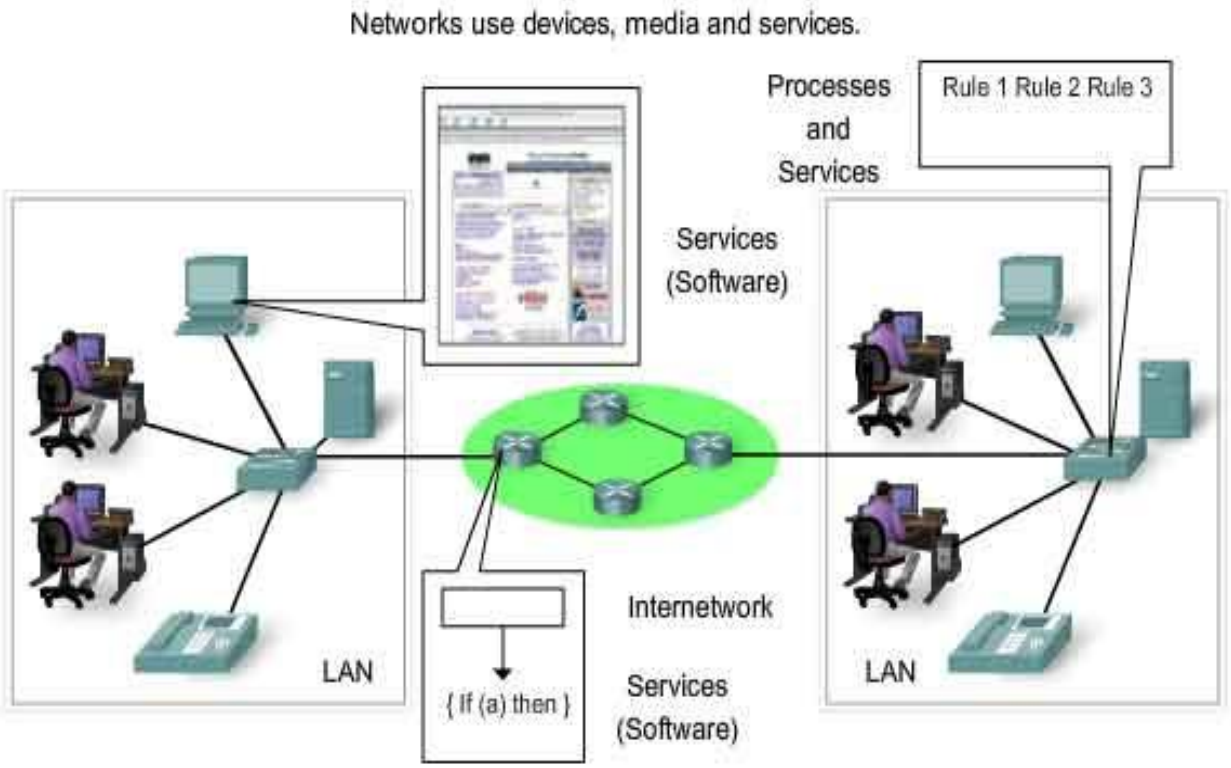
Υλικό δικτύου

Η διαδρομή που ακολουθεί ένα μήνυμα από την πηγή στον προορισμό μπορεί να είναι τόσο απλό όσο ένα μόνο καλώδιο που συνδέει έναν υπολογιστή σε έναν άλλο, ή τόσο σύνθετο όσο μια συλλογή των δικτύων που εκτείνεται κυριολεκτικά σε όλο τον κόσμο. Αυτή η υποδομή δικτύου παρέχει τη σταθερή και αξιόπιστη κανάλι μέσω του οποίου συμβαίνουν αυτές οι επικοινωνίες.

Η δικτυακή υποδομή περιλαμβάνει τρεις κατηγορίες στοιχείων του δικτύου:

- Συσκευές
- Μέσα Μετάδοσης
- Υπηρεσίες

Συσκευές και τα μέσα μετάδοσης είναι τα φυσικά στοιχεία του δικτύου. Π.χ. φορητός υπολογιστής, PC, switch, router, τα καλώδια που συνδέουν τις συσκευές.



Οι υπηρεσίες περιλαμβάνουν πολλές από τις κοινές εφαρμογές του δικτύου που χρησιμοποιούν καθημερινά οι άνθρωποι, όπως υπηρεσίες φιλοξενίας ηλεκτρονικού ταχυδρομείου και υπηρεσίες web hosting. Διαδικασίες παρέχουν τη λειτουργικότητα που κατευθύνει και μετακινεί τα μηνύματα μέσω του δικτύου. Οι διεργασίες είναι λιγότερο προφανείς σε μας, αλλά είναι κρίσιμες για τη λειτουργία των δικτύων

Συσκευές

Οι συσκευές δικτύου που οι άνθρωποι είναι πιο εξοικειωμένοι με ονομάζονται **τερματικές συσκευές** (end devices) . Μιλάμε φυσικά για τα PC, τα laptop, τα smartphone, smart-tv κλπ.

Μία τερματική συσκευή είναι είτε η πηγή ή ο προορισμός ενός μηνύματος που μεταδίδεται μέσω του δικτύου. Για να ξεχωρίζουμε μία τερματική συσκευή από μία άλλη κάθε τερματική συσκευή σε ένα δίκτυο προσδιορίζεται από μια διεύθυνση . Όταν μία τερματική συσκευή ξεκινά την επικοινωνία , χρησιμοποιεί τη διεύθυνση του τελικού προορισμού της συσκευής για να καθορίσει πού πρέπει να σταλεί το μήνυμα.

Οι ενδιάμεσες συσκευές (Intermediary devices) λέγονται οι συσκευές που συνδέονται πάνω τους οι τερματικές συσκευές και συνδέουν πολλά επιμέρους δίκτυα. Αυτές οι ενδιάμεσες συσκευές παρέχουν συνδεσιμότητα και εξασφαλίζουν τη σωστή ροή των δεδομένων σε όλο το δίκτυο . Μιλάμε για τα switch , τα routers κλπ.

Οι ενδιάμεσες συσκευές χρησιμοποιούν τη διεύθυνση συσκευής του τελικού προορισμού , σε συνδυασμό με πληροφορίες σχετικά με τις διασυνδέσεις του δικτύου , για να προσδιοριστεί η διαδρομή που πρέπει να ακολουθήσουν τα μηνύματα μέσω του δικτύου .

Μέσα μετάδοσης

Η επικοινωνία μέσω δικτύου γίνεται 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 να παρέχουν το μονοπάτι πάνω από την οποία τα δεδομένα μπορούν να μεταδοθούν .

- Μεταλλικά σύρματα μέσα καλώδια - δεδομένα κωδικοποιούνται σε ηλεκτρικούς παλμούς

- Γυαλί ή πλαστικό ινών (καλώδιο οπτικών ινών) - δεδομένα κωδικοποιούνται ως παλμούς φωτός
- Ασύρματη μετάδοση - δεδομένα κωδικοποιούνται χρησιμοποιώντας μήκη κύματος από το ηλεκτρομαγνητικό φάσμα

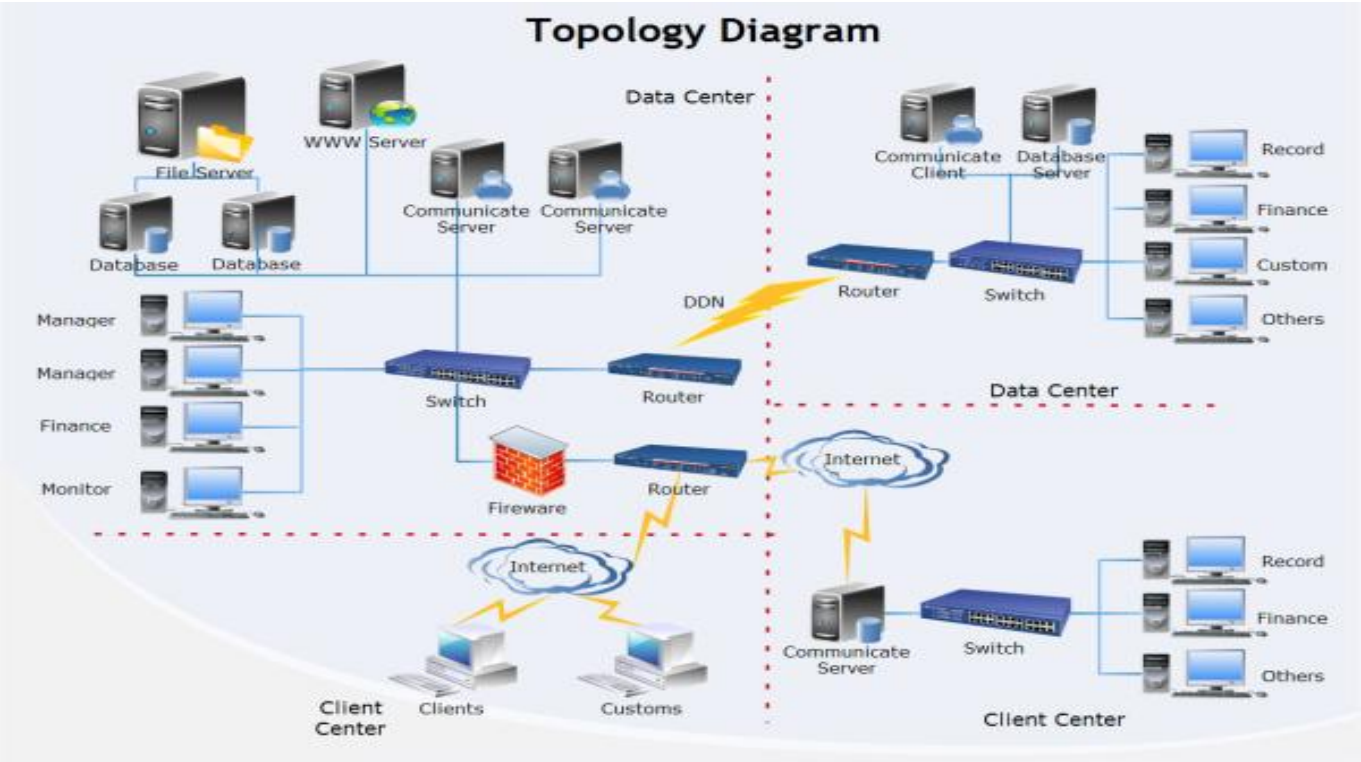
Διαφορετικοί τύποι των μέσων μεταφοράς του δικτύου έχουν διαφορετικά χαρακτηριστικά και οφέλη . Δεν είναι όλα τα μέσα του δικτύου ίδια , ούτε είναι όλα κατάλληλα για τον ίδιο σκοπό .

Τοπολογία Δικτύου

Ένα τοπολογικό διάγραμμα είναι απαραίτητο για όσους εργάζονται σε ένα δίκτυο . Παρέχει μια οπτική απεικόνιση του δικτύου και το πώς είναι συνδεδεμένο.

Υπάρχουν δύο τύποι διαγραμμάτων :

- Φυσικό διάγραμμα
- Λογικό διάγραμμα



Σύνδεση στο Internet

Το Διαδίκτυο είναι μία συλλογή των διασυνδεδεμένων δικτύων .

Το Διαδίκτυο δεν ανήκει σε κάποια επιχείρηση. Η εξασφάλιση της αποτελεσματικής επικοινωνίας σε όλη αυτή την ποικιλόμορφη υποδομή απαιτεί την εφαρμογή συνεπών και κοινώς αναγνωρισμένων τεχνολογιών και προτύπων, καθώς και τη συνεργασία πολλών φορέων διαχείρισης δικτύου. Υπάρχουν οργανισμοί που έχουν αναπτυχθεί για το σκοπό της βοηθώντας να διατηρηθεί δομή και τυποποίηση των πρωτοκόλλων Internet και των διαδικασιών.

Ο όρος internet (με πεζά γράμματα "i") χρησιμοποιείται για να περιγράψει πολλαπλά δίκτυα διασυνδέονται. Όταν γίνεται αναφορά στο παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών ή το World Wide Web, ο όρος Ίντερνετ (με κεφαλαίο «I») χρησιμοποιείται.

Internet Service Provider (ISP)

Υπάρχουν πολλοί διαφορετικοί τρόποι για να συνδεθούν οι χρήστες στο Internet . Οι οικιακοί χρήστες , οι τηλεργαζόμενοι (απομακρυσμένη εργασία) , και μικρά γραφεία συνήθως απαιτούν μια σύνδεση με μια υπηρεσία παροχής Internet (Internet Service Provider) για πρόσβαση στο Internet . Οι επιλογές σύνδεσης ποικίλλουν σε μεγάλο βαθμό μεταξύ των ISP και γεωγραφική θέση . Ωστόσο , δημοφιλείς επιλογές περιλαμβάνουν: ευρυζωνική καλωδιακή , ευρυζωνική ψηφιακή συνδρομητική γραμμή (DSL) , ασύρματα WANs , και υπηρεσίες κινητής τηλεφωνίας .

Οργανισμοί συνήθως απαιτούν πρόσβαση σε άλλα εταιρικά sites και το Διαδίκτυο . Οι γρήγορες συνδέσεις απαιτούνται για την υποστήριξη υπηρεσιών προς τις επιχειρήσεις , συμπεριλαμβανομένων των IP τηλεφώνων , video conferencing , και κέντρα αποθήκευσης δεδομένων .

Οι διασυνδέσεις business-class συνήθως παρέχονται από τους παρόχους υπηρεσιών (SP). Δημοφιλείς υπηρεσίες business-class περιλαμβάνουν: επιχειρηματικό DSL , μισθωμένες γραμμές , και Metro Ethernet.

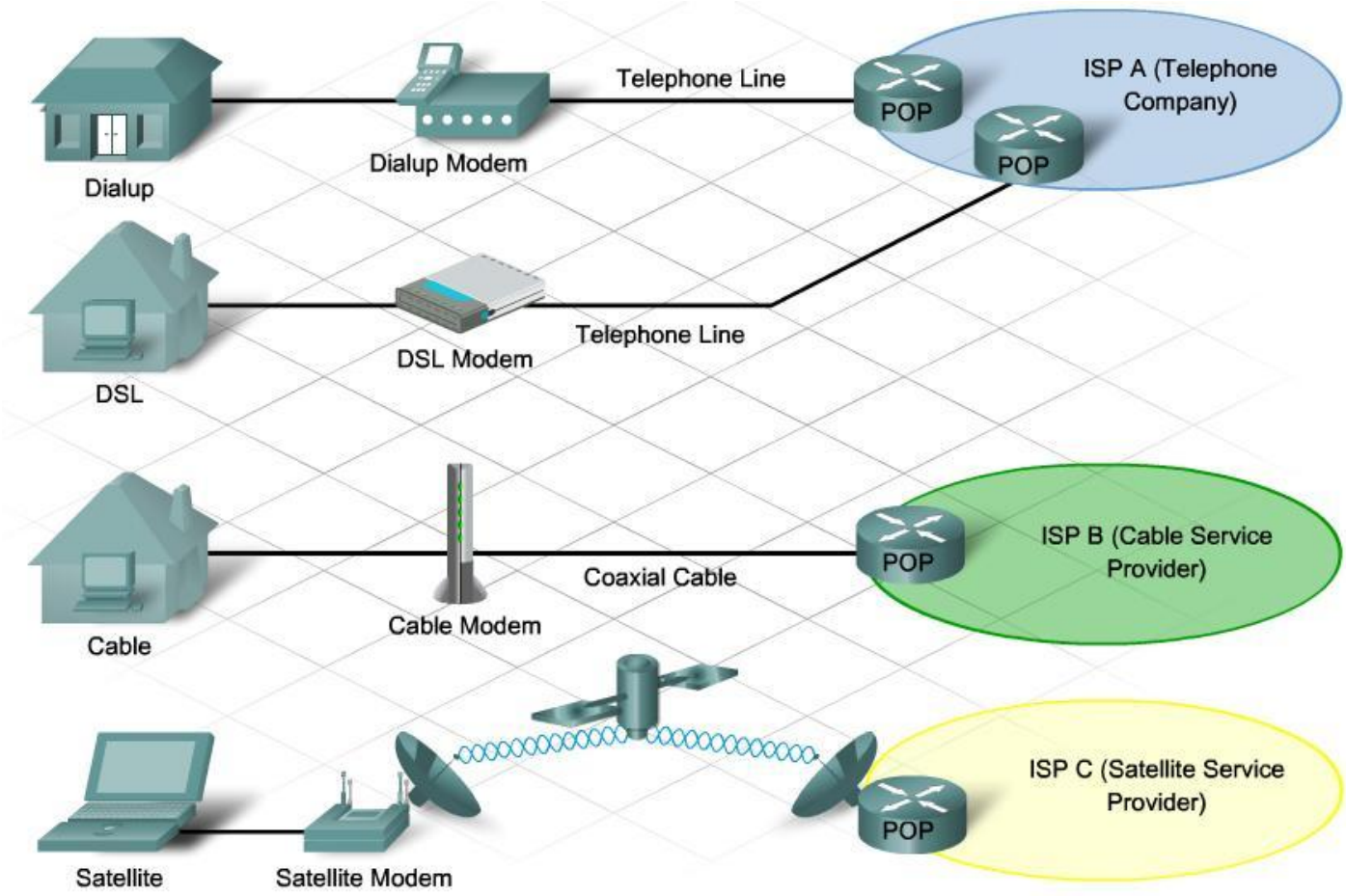
Συνδέσεις στο Internet

Τρόποι σύνδεσης για το γραφείο και το σπίτι:

- Καλωδιακή (δεν παρέχεται στην Ελλάδα) - Συνήθως προσφέρονται από τους παρόχους υπηρεσιών καλωδιακής τηλεόρασης, το σήμα δεδομένων στο Διαδίκτυο μεταφέρεται με το ίδιο καλώδιο που προσφέρει καλωδιακή τηλεόραση. Παρέχει ένα υψηλό εύρος ζώνης.
- DSL - ψηφιακές συνδρομητικές γραμμές παρέχουν υψηλό εύρος ζώνης σύνδεσης με το Διαδίκτυο. Το DSL τρέχει μέσω μιας τηλεφωνικής γραμμής. Σε γενικές γραμμές, σε μικρούς χρήστες γραφείου και σπιτιού χρησιμοποιείται η Ασύμμετρη DSL (ADSL) σύνδεση, πράγμα που σημαίνει ότι η ταχύτητα λήψης είναι μεγαλύτερη από την ταχύτητα upload.
- Cellular - Κινητή Πρόσβαση στο Internet. Χρησιμοποιεί ένα δίκτυο κινητής τηλεφωνίας για να συνδεθεί. Ανάλογα με το σήμα και τις υποστηριζόμενες τεχνολογίες του πύργου που συνδέεται (3G,4G) , θα έχει ανάλογη ποιότητα στη σύνδεση.
- Δορυφορική - Η διαθεσιμότητα της πρόσβασης στο Διαδίκτυο μέσω δορυφόρου είναι ένα πραγματικό πλεονέκτημα σε μέρη που διαφορετικά δεν θα είχαν σύνδεση στο Internet Δορυφορικά πιάτα απαιτούν μια σαφή οπτική επαφή με τον δορυφόρο.
- Dial-up Τηλέφωνο - μια φθηνή επιλογή που χρησιμοποιεί οποιαδήποτε τηλεφωνική γραμμή και ένα modem. Το χαμηλό εύρος ζώνης που παρέχεται από dial-up σύνδεση μόντεμ δεν είναι συνήθως αρκετή για μετάδοση μεγάλου όγκου δεδομένων.

- Σύνδεση με οπτικές ίνες

Η επιλογή της σύνδεσης διαφέρει ανάλογα με τη γεωγραφική τοποθεσία και τη διαθεσιμότητα παροχής υπηρεσιών.



Αρχιτεκτονική Δικτύου

Τα σύγχρονα δίκτυα πρέπει να υποστηρίξουν ένα ευρύ φάσμα εφαρμογών και υπηρεσιών , καθώς λειτουργούν σε πολλούς διαφορετικούς τύπους καλωδίων και συσκευών , που αποτελούν την υλική υποδομή . Η αρχιτεκτονική του δικτύου αναφέρεται στις τεχνολογίες που υποστηρίζουν την υποδομή, τις προγραμματισμένες υπηρεσίες και τους κανόνες , ή πρωτόκολλα , που μεταφέρουν δεδομένα μέσω του δικτύου .

Καθώς τα δίκτυα εξελίσσονται , ανακαλύπτουμε ότι υπάρχουν τέσσερα βασικά χαρακτηριστικά που οι υποκείμενες

αρχιτεκτονικές πρέπει να αντιμετωπίσουν , προκειμένου να ανταποκριθεί στις προσδοκίες των χρηστών :

- ανοχή σε σφάλματα
- επεκτασιμότητα
- Quality of Service (QoS)
- Ασφάλεια

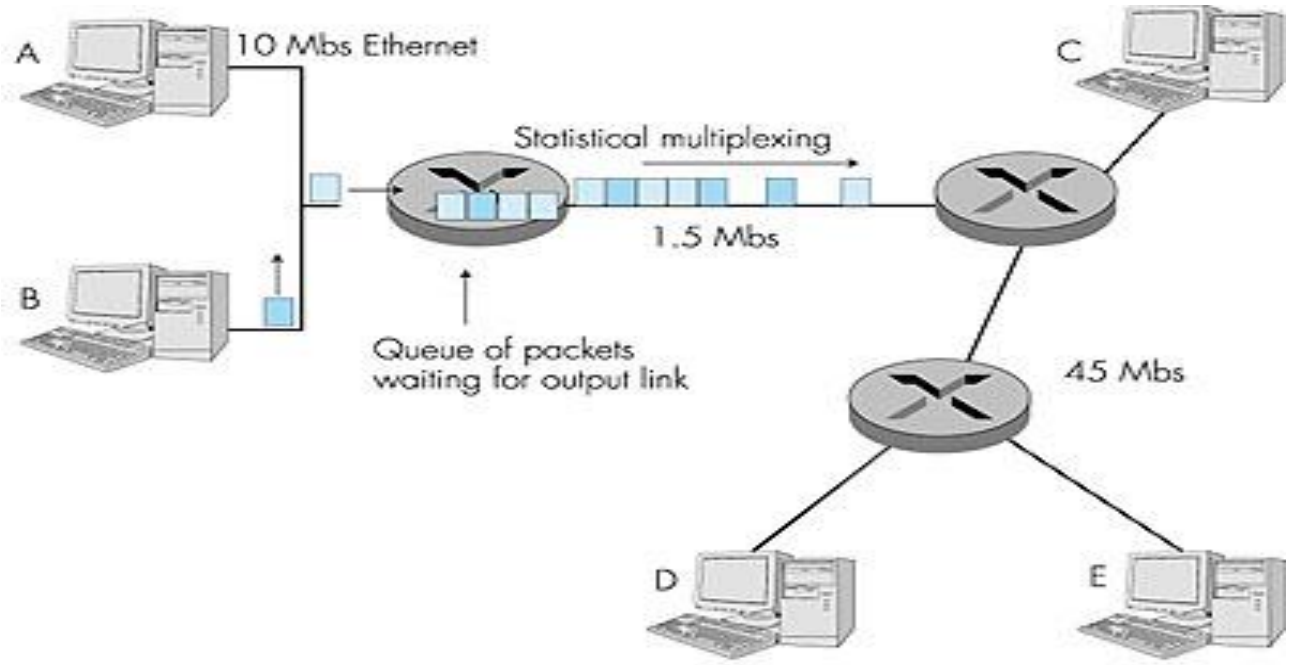
Ανοχή Σφαλμάτων (Fault Tolerance)

Η προσδοκία είναι ότι το Διαδίκτυο είναι πάντα διαθέσιμο για τα εκατομμύρια των χρηστών που βασίζονται σε αυτό. Αυτό απαιτεί μια αρχιτεκτονική δικτύου ώστε να είναι ανεκτικό σε σφάλματα. Ένα δίκτυο ανεκτικό σε σφάλματα, περιορίζει την επίδραση μιας αποτυχίας, έτσι ώστε ο μικρότερος αριθμός των συσκευών να επηρεάζονται. Είναι κτισμένο με τέτοιο τρόπο που να επιτρέπει την ταχεία ανάκαμψη, όταν συμβαίνει μια τέτοια αποτυχία. Τα δίκτυα αυτά εξαρτώνται από την πολλαπλότητα των διαδρομών μεταξύ της πηγής και του προορισμού του μηνύματος. Εάν μία διαδρομή αποτύχει, τα μηνύματα μπορούν να σταλούν άμεσα σε μια διαφορετική σύνδεση.

Μεταγωγή Πακέτων

Ένας τρόπος για την παροχή αξιόπιστων δικτύων, είναι με την εφαρμογή ενός δικτύου μεταγωγής πακέτων. Η μεταγωγή πακέτων χωρίζει την κυκλοφορία σε πακέτα που δρομολογούνται πάνω από ένα κοινόχρηστο δίκτυο. Ένα απλό μήνυμα, όπως ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή μία ροή βίντεο, χωρίζεται σε πολλαπλά μπλοκ μηνυμάτων, που ονομάζονται πακέτα. Κάθε πακέτο έχει τις απαραίτητες πληροφορίες για την διεύθυνση της πηγής και του προορισμού του μηνύματος. Οι δρομολογητές εντός του δικτύου δρομολογούν τα πακέτα με βάση την κατάσταση του δικτύου εκείνη τη στιγμή. Αυτό σημαίνει ότι όλα τα πακέτα σε ένα

μήνυμα μπορεί να φτάσουν από πολύ διαφορετικές πορείες προς τον προορισμό.



Επεκτασιμότητα (Scalability)

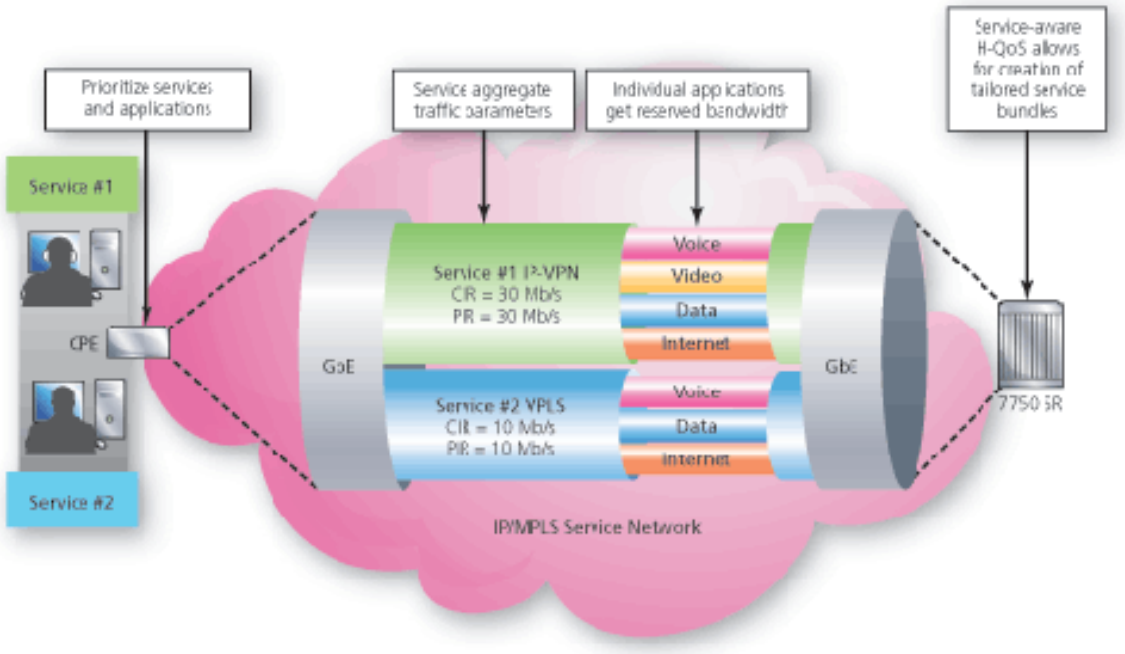
Ένα εξελικτικό δίκτυο μπορεί να επεκταθεί γρήγορα για να υποστηρίξει τους νέους χρήστες και εφαρμογές , χωρίς να επηρεάζεται η εκτέλεση της υπηρεσίας που παρέχεται στους υπάρχοντες χρήστες. Επιπλέον, τα δίκτυα είναι επεκτάσιμα επειδή οι σχεδιαστές ακολουθούν τα αποδεκτά πρότυπα και πρωτόκολλα

. Αυτό επιτρέπει στους προμηθευτές λογισμικού και υλικού να επικεντρωθούν στη βελτίωση των προϊόντων και των υπηρεσιών , χωρίς να ανησυχούν για το σχεδιασμό ενός νέου συνόλου κανόνων για τη λειτουργία του δικτύου .

Quality of Service

Quality of Service (QoS). Η ποιότητα των υπηρεσιών είναι επίσης μία διαρκώς αυξανόμενη απαίτηση των δικτύων σήμερα. Οι νέες εφαρμογές που είναι διαθέσιμες στους χρήστες μέσω του Διαδικτύου, όπως η μετάδοση φωνής και το ζωντανό βίντεο, έχουν δημιουργήσει υψηλότερες προσδοκίες για την ποιότητα των παρεχόμενων υπηρεσιών. Έχετε δοκιμάσει ποτέ να παρακολουθήσετε ένα βίντεο με συνεχή διαλείμματα και παύσεις; Το QoS είναι ο κύριος μηχανισμός για τη διαχείριση της συμφόρησης και την εξασφάλιση αξιόπιστης παράδοσης του περιεχομένου σε όλους τους χρήστες.

Συμφόρηση παρατηρείται όταν η ζήτηση για εύρος ζώνης ξεπερνά τη διαθέσιμη ποσότητα. Το εύρος ζώνης του δικτύου μετράται με τον αριθμό των bits που μπορεί να μεταδοθεί σε ένα ενιαίο δευτερόλεπτα, ή bits ανά δευτερόλεπτο (bps). Όταν ταυτόχρονες επικοινωνίες επιχειρούνται σε όλο το δίκτυο, η ζήτηση για το εύρος



ζώνης του δικτύου μπορεί να υπερβαίνει τη διαθεσιμότητά του, δημιουργώντας συμφόρηση του δικτύου.

Ασφάλεια

Η υποδομή του δικτύου, οι υπηρεσίες και τα δεδομένα που περιέχονται σε συσκευές συνδεδεμένες με το δίκτυο είναι ζωτικής σημασίας πληροφορίες τόσο για την προσωπική όσο και για την επιχειρηματική ζωή. Υπάρχουν δύο τομείς για την ασφάλεια του δικτύου που πρέπει να αντιμετωπιστούν: Η ασφάλεια της υποδομής του δικτύου και η ασφάλεια των πληροφοριών.

Η ασφάλεια μιας υποδομής δικτύου περιλαμβάνει τη φυσική εξασφάλιση των συσκευών που παρέχουν συνδεσιμότητα με το δίκτυο, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση στο λογισμικό διαχείρισης που βρίσκεται πάνω τους.

Η ασφάλεια των πληροφοριών αναφέρεται στην προστασία των πληροφοριών που περιέχονται εντός των πακέτων που μεταδίδονται μέσω του δικτύου και των πληροφοριών που είναι αποθηκευμένες στις συνδεδεμένες συσκευές. Προκειμένου να επιτευχθούν οι στόχοι της ασφάλειας των δικτύων, υπάρχουν τρεις πρωτογενείς απαιτήσεις.

- Εμπιστευτικότητα - Η εμπιστευτικότητα των δεδομένων σημαίνει ότι μόνο οι εγκεκριμένοι χρήστες μπορούν να έχουν πρόσβαση και να διαβάσουν τα δεδομένα.

- Ακεραιότητα - Η ακεραιότητα των δεδομένων εξασφαλίζει ότι η πληροφορία δεν έχει αλλοιωθεί κατά τη διαβίβαση, από την αφετηρία μέχρι τον προορισμό.

- Διαθεσιμότητα - Διαθεσιμότητα δεδομένων σημαίνει ότι έχει εξασφαλιστεί η έγκαιρη και αξιόπιστη πρόσβαση σε υπηρεσίες δεδομένων στους εξουσιοδοτημένους χρήστες.

.

Η ασφάλεια των δικτύων αποτελεί αναπόσπαστο μέρος της δικτύωσης υπολογιστών, ανεξάρτητα από το αν το δίκτυο περιορίζεται σε ένα σπίτι με μία μόνο σύνδεση στο Internet ή τόσο μεγάλο όσο μια εταιρία με χιλιάδες χρήστες. Η ασφάλεια του δικτύου που υλοποιείται πρέπει να λαμβάνει υπόψη το περιβάλλον, καθώς και τα εργαλεία και τις απαιτήσεις του δικτύου. Πρέπει να είναι σε θέση να εξασφαλίσει τα δεδομένα, επιτρέποντας παράλληλα την ποιότητα των υπηρεσιών που αναμένεται από το δίκτυο.

Η ασφάλεια ενός δικτύου περιλαμβάνει πρωτόκολλα, τεχνολογίες, συσκευές, εργαλεία και τεχνικές για την ασφάλεια των δεδομένων και να μετριάσουν τις απειλές. Η απειλή μπορεί να είναι εξωτερική ή εσωτερική. Πολλές απειλές εξωτερικής ασφάλειας του δικτύου έχουν σήμερα εξαπλωθεί μέσω του Διαδικτύου.

Οι πιο κοινές εξωτερικές απειλές σε δίκτυα περιλαμβάνουν:

- Virus, worms and Trojan Horses - κακόβουλο λογισμικό αυθαίρετου κώδικα που εκτελείται σε μια συσκευή χρήστη.

- Spyware και adware - λογισμικού που έχουν εγκατασταθεί σε μια συσκευή χρήστη που συλλέγει κρυφά πληροφορίες σχετικά με τον χρήστη.

- Zero-day attacks, ονομάζεται επίσης επιθέσεις ώρα μηδέν - μια επίθεση που λαμβάνει χώρα κατά την πρώτη ημέρα που μια ευπάθεια γίνεται γνωστή.

- Επιθέσεις χάκερ - μια επίθεση από ένα καταρτισμένο πρόσωπο σε συσκευές χρηστών ή στους πόρους του δικτύου.

- Οι επιθέσεις Denial of Service - επιθέσεις που έχουν σχεδιαστεί για να επιβραδύνουν ή και να συντρίψουν εφαρμογές και διαδικασίες σε μία συσκευή του δικτύου.

- Παραποίηση δεδομένων και κλοπή τους - μια επίθεση για να κλέψει ή να αλλοιώσει τις ιδιωτικές πληροφορίες από το δίκτυο ενός οργανισμού.

- Η κλοπή ταυτότητας - μια επίθεση για να κλαπούν τα διαπιστευτήρια σύνδεσης του χρήστη, ώστε να έχει πρόσβαση σε προσωπικά δεδομένα μη εξουσιοδοτημένος χρήστης.

Είναι εξίσου σημαντικό να εξεταστούν εσωτερικές απειλές. Έχουν υπάρξει πολλές μελέτες που δείχνουν ότι οι πιο συχνές παραβιάσεις δεδομένων έχουν συμβεί λόγω των εσωτερικών χρηστών του δικτύου. Αυτό μπορεί να οφείλεται σε κακή χρήση των συσκευών του δικτύου από τους εργαζομένους, ακόμα και κακοπροαίρετους υπαλλήλους.

Κεφάλαιο 2ο

Επίπεδα Δικτύου – Μοντέλα αναφοράς

Βασικοί κανόνες επικοινωνίας

Ένα δίκτυο μπορεί να είναι τόσο περίπλοκο με πολλές συσκευές που συνδέονται μέσω του Internet, είτε τόσο απλό όσο δύο υπολογιστές που συνδέονται άμεσα το ένα στο άλλο με ένα μόνο καλώδιο. Τα δίκτυα μπορούν να διαφέρουν σε μέγεθος, στο σχήμα και τη λειτουργία. Ωστόσο, απλά μια ενσύρματη ή ασύρματη φυσική σύνδεση μεταξύ των τερματικών συσκευών, δεν είναι αρκετή για να επικοινωνήσουν. Για να επικοινωνήσουν, οι συσκευές πρέπει να ξέρουν το «πώς»!

Οι άνθρωποι επικοινωνούν, χρησιμοποιώντας πολλές διαφορετικές μεθόδους. Ωστόσο, ανεξάρτητα από την επιλεγείσα μέθοδο, όλες οι μέθοδοι επικοινωνίας έχουν τρία κοινά στοιχεία.

1. Η πηγή του μηνύματος. Πηγή ενός μηνύματος είναι οι άνθρωποι, ή ηλεκτρονικές συσκευές, που χρειάζονται για να σταλεί ένα μήνυμα σε άλλα άτομα ή συσκευές.
2. Ο προορισμός του μηνύματος. Ο προορισμός λαμβάνει το μήνυμα και τοα ερμηνεύει.
3. Ο δίαυλος. Το μέσο που παρέχει την οδό κατά την οποία το μήνυμα ταξιδεύει από την πηγή στον προορισμό.

Η επικοινωνία διέπεται από ένα σύνολο κανόνων που ονομάζονται πρωτόκολλα. Τα πρωτόκολλα αυτά είναι ειδικά για το είδος της μεθόδου επικοινωνίας που χρησιμοποιείται.

Για παράδειγμα, όταν μιλάνε δύο άνθρωποι, χρειάζεται ένα σύνολο κανόνων, όπως να μιλάνε την ίδια γλώσσα!

Πρωτόκολλα δικτύου

Τα πρώτα δίκτυα υπολογιστών σχεδιάστηκαν κατά κύριο λόγω ως προς το υλικό , και μόνο δευτερευόντως εξέταζαν το λογισμικό. Αυτή η λογική με την πολυπλοκότητα των δικτύων σήμερα δεν αποδίδει πια. Στις μέρες μας , το λογισμικό δικτύων είναι δομημένο σε υψηλό βαθμό.

Για να μειωθεί η σχεδιαστική πολυπλοκότητα, τα περισσότερα δίκτυα οργανώνονται σαν μια στοίβα επιπέδων (network layers), με τα επίπεδα να χτίζονται το ένα πάνω στο άλλο. Ο στόχος του κάθε επιπέδου είναι να προσφέρει υπηρεσίες στα ανώτερα επίπεδα , κρύβοντας από τα επίπεδα αυτά τις λεπτομέρειες της υλοποίησης των παρεχόμενων υπηρεσιών.

Το πρωτόκολλο είναι μία συμφωνία ανάμεσα στα επικοινωνούντα μέρη για το πώς πρέπει να διεξαχθεί η επικοινωνία. Τα πρωτόκολλα δικτύου, λοιπόν ορίζουν το σύνολο των κανόνων για την ανταλλαγή μηνυμάτων μεταξύ των τερματικών συσκευών. Μερικά γνωστά πρωτόκολλα δικτύου είναι το πρωτόκολλο μεταφοράς υπερκειμένου (HTTP), το πρωτόκολλο ελέγχου μετάδοσης (TCP) και το πρωτόκολλο Internet (IP).

Αλληλεπίδραση πρωτοκόλλων

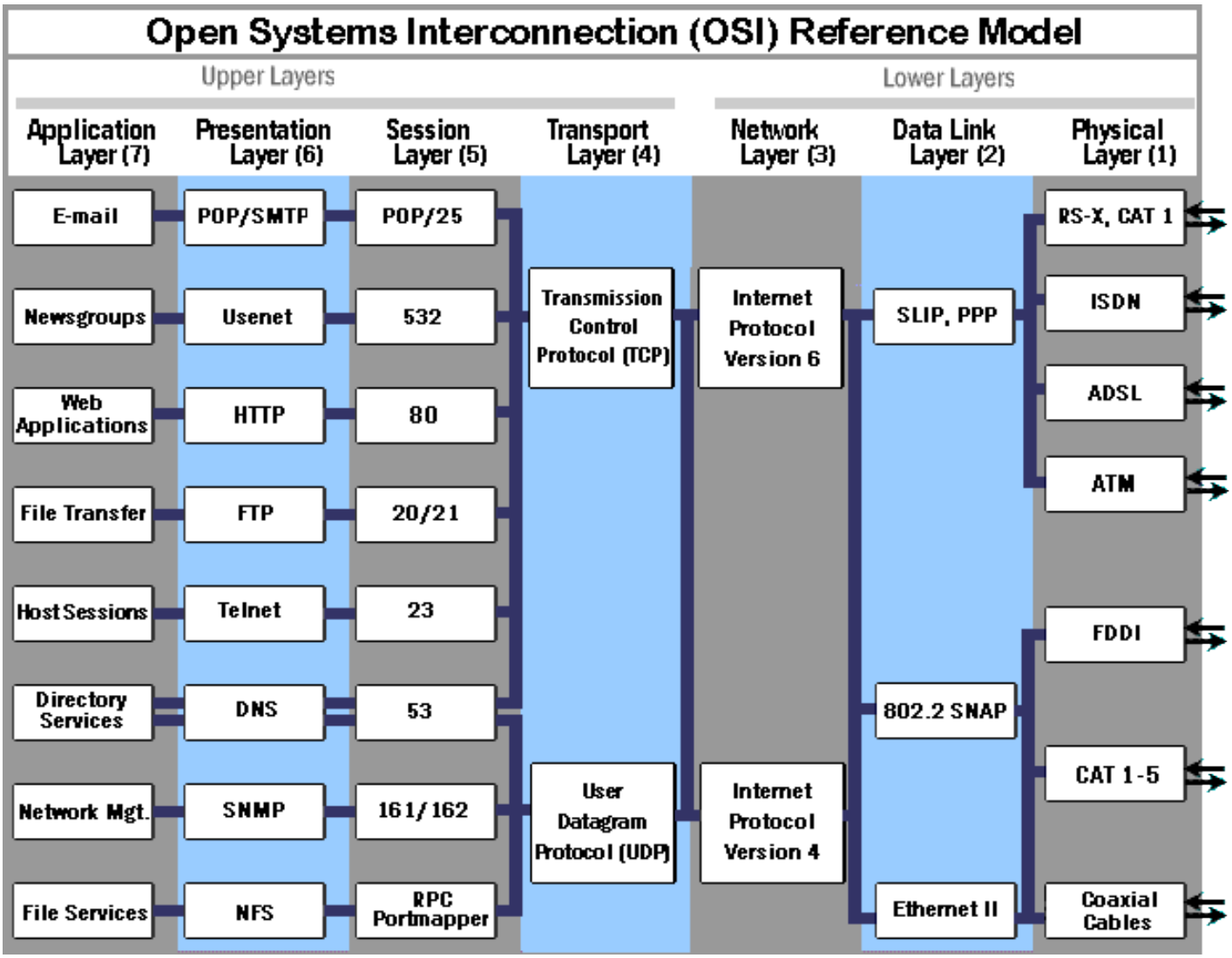
Η επικοινωνία μεταξύ ενός web server και ενός web client είναι ένα παράδειγμα της αλληλεπίδρασης μεταξύ των διαφόρων πρωτοκόλλων όπως:

- HTTP - είναι ένα πρωτόκολλο εφαρμογής που διέπει τον τρόπο όπου ένας web server και ένας web client αλληλεπιδρούν. Το πρωτόκολλο HTTP καθορίζει το περιεχόμενο και τη μορφοποίηση των αιτήσεων και των απαντήσεων που ανταλλάσσονται μεταξύ του client και του server. Τόσο ο client αλλά και ο server «τρέχουν» το πρωτόκολλο HTTP ως μέρος της εφαρμογής της επικοινωνίας τους. Το HTTP βασίζεται σε άλλα πρωτόκολλα που διέπουν τον τρόπο με τον οποίο τα μηνύματα που μεταφέρονται μεταξύ του client-server.

- TCP - είναι το πρωτόκολλο μεταφοράς. Το TCP χωρίζει τα μηνύματα, HTTP στην προκειμένη περίπτωση, σε μικρότερα κομμάτια, που ονομάζονται τμήματα (segments). Αυτά τα πακέτα στέλνονται μεταξύ των διεργασιών του web server και του client. Το TCP είναι επίσης υπεύθυνο για τον έλεγχο του μεγέθους και της ταχύτητα με την οποία ανταλλάσσονται τα μηνύματα.

- IP - Είναι υπεύθυνο για τη λήψη των διαμορφωμένων τμημάτων από το πρωτόκολλο TCP, την ενσωμάτωσή τους σε πακέτα (packets), ανάθεση σε αυτά τις κατάλληλες διευθύνσεις, και την παράδοσή τους στον προορισμό τους.

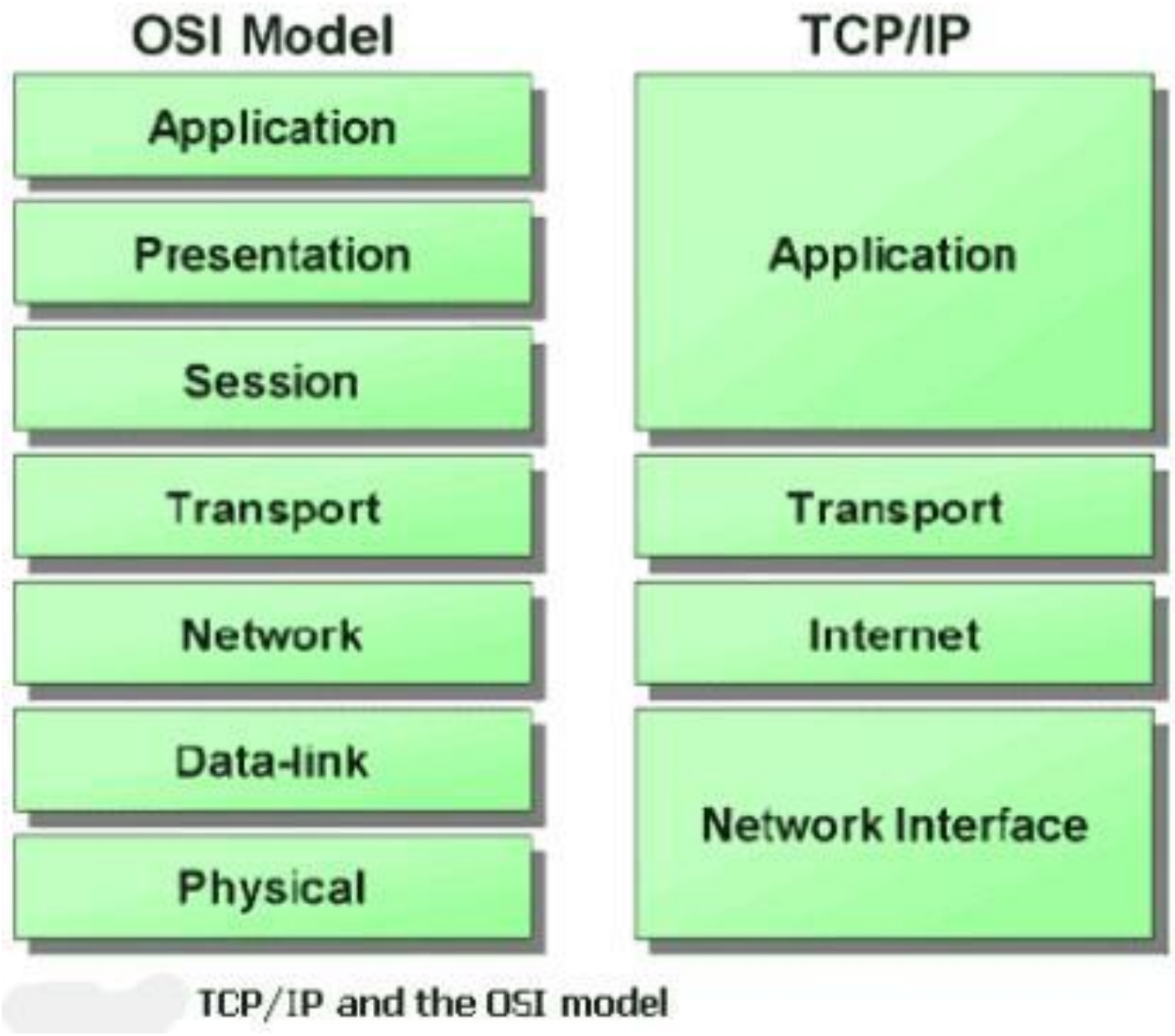
- Ethernet - Είναι ένα πρωτόκολλο δικτύου πρόσβασης που περιγράφει δύο κύριες λειτουργίες: την επικοινωνία κατά τη διάρκεια μιας σύνδεσης δεδομένων και τη φυσική διαβίβαση των στοιχείων σχετικά με τα μέσα μεταφοράς του δικτύου. Τα πρωτόκολλα πρόσβασης δικτύου είναι υπεύθυνα για τη λήψη των IP πακέτων και τη μορφοποίηση τους ώστε να μεταφέρονται από τα μέσα μετάδοσης.



Μοντέλα Αναφοράς

Μοντέλο αναφοράς ονομάζουμε το μοντέλο που παρέχει συνοχή ανάμεσα σε όλους τους τύπους των πρωτοκόλλων και των υπηρεσιών του δικτύου περιγράφοντας το τι πρέπει να γίνει σε ένα συγκεκριμένο στρώμα, αλλά δεν προδιαγράφουν πώς πρέπει να επιτευχθεί. Το μοντέλο OSI είναι ένα ευρέως γνωστό μοντέλο αναφοράς, που μπορεί να χρησιμοποιείται πλέον σπάνια αλλά είναι αρκετά γενικό, πράγμα που το καθιστά ακόμα έγκυρο, και μπορεί επίσης να μας βοηθήσει να κατανοήσουμε τα επίπεδα του δικτύου. Το μοντέλο TCP/IP έχει τις αντίθετες ιδιότητες: το ίδιο το

μοντέλο δεν είναι ιδιαίτερα χρήσιμο αλλά τα πρωτόκολλα του χρησιμοποιούνται ευρύτατα.



TCP/IP and the OSI model

Το μοντέλο OSI

Το μοντέλο OSI παρέχει μια εκτενή λίστα των λειτουργιών και υπηρεσιών που μπορεί να υλοποιηθεί σε κάθε στρώμα . Περιγράφει επίσης την αλληλεπίδραση του κάθε στρώματος με τα στρώματα ακριβώς πάνω και κάτω . OSI σημαίνει Διασύνδεση

Ανοιχτών Συστημάτων – δηλαδή συστημάτων που είναι ανοιχτά στην επικοινωνία με άλλα συστήματα.

Όπως φαίνεται και στην εικόνα, το μοντέλο OSI χωρίζεται σε 7 επίπεδα:

7. Application Layer: Το *επίπεδο εφαρμογών* παρέχει στον χρήστη έναν τρόπο να προσπελάσει μέσω μιας εφαρμογής τις πληροφορίες ενός δικτύου. Αυτό το επίπεδο είναι η κύρια διασύνδεση του χρήστη με την εφαρμογή και, συνεπώς, με το δίκτυο. Στο επίπεδο αυτό γίνεται η διαχείριση των κατανεμημένων εφαρμογών, η αποστολή του ηλεκτρονικού ταχυδρομείου κλπ. Παραδείγματα πρωτοκόλλων επιπέδου εφαρμογών αποτελούν τα Telnet, FTP, SMTP και http.

6. Presenation Layer: Το επίπεδο παρουσίασης μετασχηματίζει τα δεδομένα σε τυπική μορφή που την αναμένει το επίπεδο εφαρμογών. Στο επίπεδο αυτό τα δεδομένα υφίστανται κρυπτογράφηση, συμπίεση, κωδικοποίηση MIME και όποια άλλη διαμόρφωση απαιτεί η μορφή δεδομένων ή ο σχεδιαστής του πρωτοκόλλου. Παραδείγματα αποτελούν η μετατροπή αρχείων από κώδικα EBCDIC σε κώδικα ASCII και η μετατροπή της δομής των δεδομένων σε μορφή XML ή αντίστροφα (π.χ. από XML σε έγγραφο τύπου DOC).

5. Session Layer: Το επίπεδο συνόδου ελέγχει τις συνόδους (δηλαδή τις ανταλλαγές δεδομένων) μεταξύ δύο υπολογιστών, του Α και του Β. Ξεκινά, διαχειρίζεται και τερματίζει τη σύνδεση μεταξύ μιας τοπικής και μιας απομακρυσμένης εφαρμογής. Αντιμετωπίζει λειτουργίες FDX (full duplex, οι Α και Β μιλούν ταυτόχρονα από δύο κανάλια) ή HDX (half-duplex, μιλάει ο Α και μετά απαντάει ο Β από το ένα διαθέσιμο κανάλι), ενώ υποστηρίζει διαδικασίες αποθήκευσης κατάστασης (checkpoint), αναβολής (adjournment), τερματισμού (termination) και επανεκκίνησης (restart). Αυτό το επίπεδο είναι υπεύθυνο για το ομαλό κλείσιμο της συνόδου (που είναι ιδιότητα του TCP) και επίσης για την αποθήκευση και ανάκτηση

κατάστασης, λειτουργίες οι οποίες δεν χρησιμοποιούνται στην στοίβα πρωτοκόλλων του Διαδικτύου

4. Transport Layer: Το επίπεδο μεταφοράς διεκπεραιώνει τη μεταφορά των δεδομένων από χρήστη σε χρήστη, απαλλάσσοντας έτσι τα ανώτερα επίπεδα από κάθε φροντίδα να προσφέρουν αξιόπιστη μεταφορά δεδομένων από το ένα άκρο της επικοινωνίας στο άλλο. Το επίπεδο μεταφοράς ελέγχει την αξιοπιστία ενός χρησιμοποιούμενου καναλιού με έλεγχο ροής (flow control), κατάτμηση και αποτμηματοποίηση (segmentation / desegmentation), καθώς και έλεγχο σφαλμάτων (error control). Ορισμένα πρωτόκολλα καταγράφουν καταστάσεις και συνδέσεις, οπότε κρατούν λογαριασμό των πακέτων και επανεκπέμπουν αυτά που δεν παρελήφθησαν σωστά. Τα διάφορα πρωτόκολλα μορφοποιούν διαφορετικά τα εκπεμπόμενα πακέτα πληροφοριών, αλλά τα προς αποστολή δεδομένα παραλαμβάνονται αρχικά από τα ανώτερα επίπεδα.

Το συνηθέστερο παράδειγμα πρωτοκόλλου μεταφοράς είναι το TCP (Transmission Control Protocol, πρωτόκολλο ελέγχου μετάδοσης). Άλλα πρωτόκολλα μεταφοράς είναι τα UDP (User Datagram Protocol, πρωτόκολλο για ασυνδεσμική αποστολή δεδομένων, SCTP (αγγλ. Stream Control Transmission Protocol, πρωτόκολλο ελέγχου της ροής μετάδοσης), κλπ.

3. Network Layer: Το επίπεδο δικτύου παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά στοιχειοσειρών δεδομένων μεταβλητού μήκους από μια προέλευση σε έναν προορισμό, μέσα από ένα ή περισσότερα ενδιάμεσα δίκτυα, ενώ διατηρεί την ποιότητα εξυπηρέτησης που απαιτεί το επίπεδο μεταφοράς. Το επίπεδο δικτύου εκτελεί λειτουργίες δρομολόγησης, με πιθανές κατατμήσεις / αποτμηματοποιήσεις, και αναφέρει σφάλματα σχετικά με την παράδοση των πακέτων. Οι δρομολογητές (routers) λειτουργούν στο επίπεδο αυτό· διακινώντας δεδομένα σε διασυνδεδεμένα δίκτυα έκαναν το Διαδίκτυο πραγματικότητα. Υπάρχουν και δικτυακοί διακόπτες που σχετίζονται με τις διευθύνσεις (IP). Το πλέον αναγνωρίσιμο

παράδειγμα πρωτοκόλλου δικτύου είναι το Πρωτόκολλο Διαδικτύου (Internet Protocol, IP).

2. Data Link Layer: Το επίπεδο ζεύξης δεδομένων παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά δεδομένων από μια συσκευή ενός τοπικού δικτύου σε άλλη, αλλά και για την ανίχνευση και διόρθωση σφαλμάτων που συμβαίνουν στο φυσικό επίπεδο. Οι μη ιεραρχημένες διευθύνσεις των συσκευών εδώ είναι οι φυσικές (π.χ. MAC διευθύνσεις), δηλαδή είναι προκαθορισμένες και αποθηκευμένες στις κάρτες δικτύου των επικοινωνούντων κόμβων από το εργοστάσιο.

Το πιο γνωστό πρότυπο αυτού του επιπέδου είναι το Ethernet, για τοπικά δίκτυα. Άλλα παραδείγματα πρωτοκόλλων ζεύξης δεδομένων αποτελούν τα:

- HDLC και ADCCP, για συνδέσεις από-σημείο-σε-σημείο (point-to-point).
- 802.11, για ασύρματα τοπικά δίκτυα.

Στα τοπικά δίκτυα της οικογένειας πρωτοκόλλων IEEE 802, και σε κάποια άλλα όπως το FDDI, αυτό το επίπεδο μπορεί να διαιρεθεί σε δύο μικρότερα:

1. Επίπεδο ελέγχου πρόσβασης στο κοινό μέσο, το υποεπίπεδο MAC (Media Access Control, Έλεγχος Πρόσβασης Μέσου)
2. Επίπεδο ελέγχου λογικών συνδέσεων, το υποεπίπεδο LLC (αγγλ. Logical Link Control, Έλεγχος Λογικών Ζεύξεων), όπου επικρατεί καθολικά το πρωτόκολλο IEEE 802.2 ανεξάρτητα από το υποκείμενο πρωτόκολλο MAC ή φυσικού επιπέδου.

Στο επίπεδο αυτό λειτουργούν τα Switch

1. Physical Layer: Το φυσικό επίπεδο ορίζει όλες τις ηλεκτρικές και φυσικές προδιαγραφές της επικοινωνίας. Σ' αυτές περιλαμβάνονται οι σχηματισμοί των ακίδων, οι επιτρεπτές τάσεις, οι προδιαγραφές των καλωδίων κλπ. Συσκευές φυσικού επιπέδου είναι οι διανεμητές, οι επαναλήπτες (repeaters), οι

κάρτες δικτύου, οι προσαρμοστές διαύλου (bus adapters). Οι κυριότερες λειτουργίες και υπηρεσίες του φυσικού επιπέδου είναι:

- Έναρξη και τερματισμός της ηλεκτρικής σύνδεσης μιας επικοινωνιακής συσκευής.
- Συμμετοχή σε διαδικασίες όπου οι επικοινωνιακές συσκευές εξυπηρετούν αποτελεσματικά πολλούς χρήστες (πολυπλεξία). Επιλύονται προβλήματα προτεραιότητας πρόσβασης και ελέγχου ροής δεδομένων.
- Διαμόρφωση και αποδιαμόρφωση των ψηφιακών δεδομένων κατά τη μετάδοση από συσκευή σε συσκευή. Για παράδειγμα, τα ψηφιακά ηλεκτρικά σήματα μπορεί να ταξιδέψουν ως αναλογικά σε χάλκινο καλώδιο, μετά σε οπτική ίνα, μετά να μεταδοθούν από ραδιοζεύξη ή δορυφορικά, να φθάσουν πάλι αναλογικά σε χάλκινο καλώδιο και να γίνουν ψηφιακά στον παραλήπτη.

Επίσης τα επίπεδα 1 και 2 αφορούν οι προδιαγραφές των πρωτοκόλλων Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface, Διασύνδεση Κατανεμημένων Δεδομένων με Οπτικές Ίνες) και IEEE 802.11.

Τμηματοποίηση μηνυμάτων (Message segmentation)

Θεωρητικά, ένα και μόνο μήνυμα, όπως ένα μουσικό βίντεο ή ένα μήνυμα ηλεκτρονικού ταχυδρομείου, θα μπορούσε να σταλεί μέσω ενός δικτύου από μια πηγή σε έναν προορισμό, σαν μία αδιάκοπη ροή από bits. Εάν τα μηνύματα πραγματικά μεταδίδονταν με αυτόν τον τρόπο, αυτό θα σήμαινε ότι καμία άλλη συσκευή δεν θα ήταν σε θέση να στείλει ή να λάβει μηνύματα από το ίδιο δίκτυο, ενώ η εν λόγω μεταβίβαση δεδομένων θα ήταν σε εξέλιξη. Αυτές οι μεγάλες ροές δεδομένων θα οδηγήσουν σε σημαντικές καθυστερήσεις. Περαιτέρω, εάν μια σύνδεση στο διασυνδεδεμένο δίκτυο υποδομής απέτυχε κατά τη διάρκεια της μετάδοσης, το πλήρες μήνυμα θα χανόταν και θα έπρεπε να αναμεταδοθεί από την αρχή.

Μια καλύτερη προσέγγιση είναι να χωρίσουμε τα δεδομένα σε μικρότερα, πιο εύχρηστα κομμάτια ώστε να σταλούν. Αυτή η διαίρεση της ροής δεδομένων σε μικρότερα κομμάτια ονομάζεται τμηματοποίηση ή κατάτμηση (Segmentation). Η κατάτμηση των μηνυμάτων έχει δύο βασικά πλεονεκτήματα:

- Με την αποστολή μικρότερων μεμονωμένων κομματιών από την πηγή στον προορισμό, πολλά διαφορετικά μηνυμάτων από διάφορες εφαρμογές μπορούν να σταλούν ταυτόχρονα από το δίκτυο. Αυτό ονομάζεται πολυπλεξία.
- Η κατάτμηση μπορεί να αυξήσει την αποτελεσματικότητα των επικοινωνιών του δικτύου. Εάν μέρος του μηνύματος αποτύχει να φτάσει στον προορισμό, λόγω βλάβης στο δίκτυο ή συμφόρηση, μόνο τα κομμάτια που λείπουν θα αναμεταδοθούν

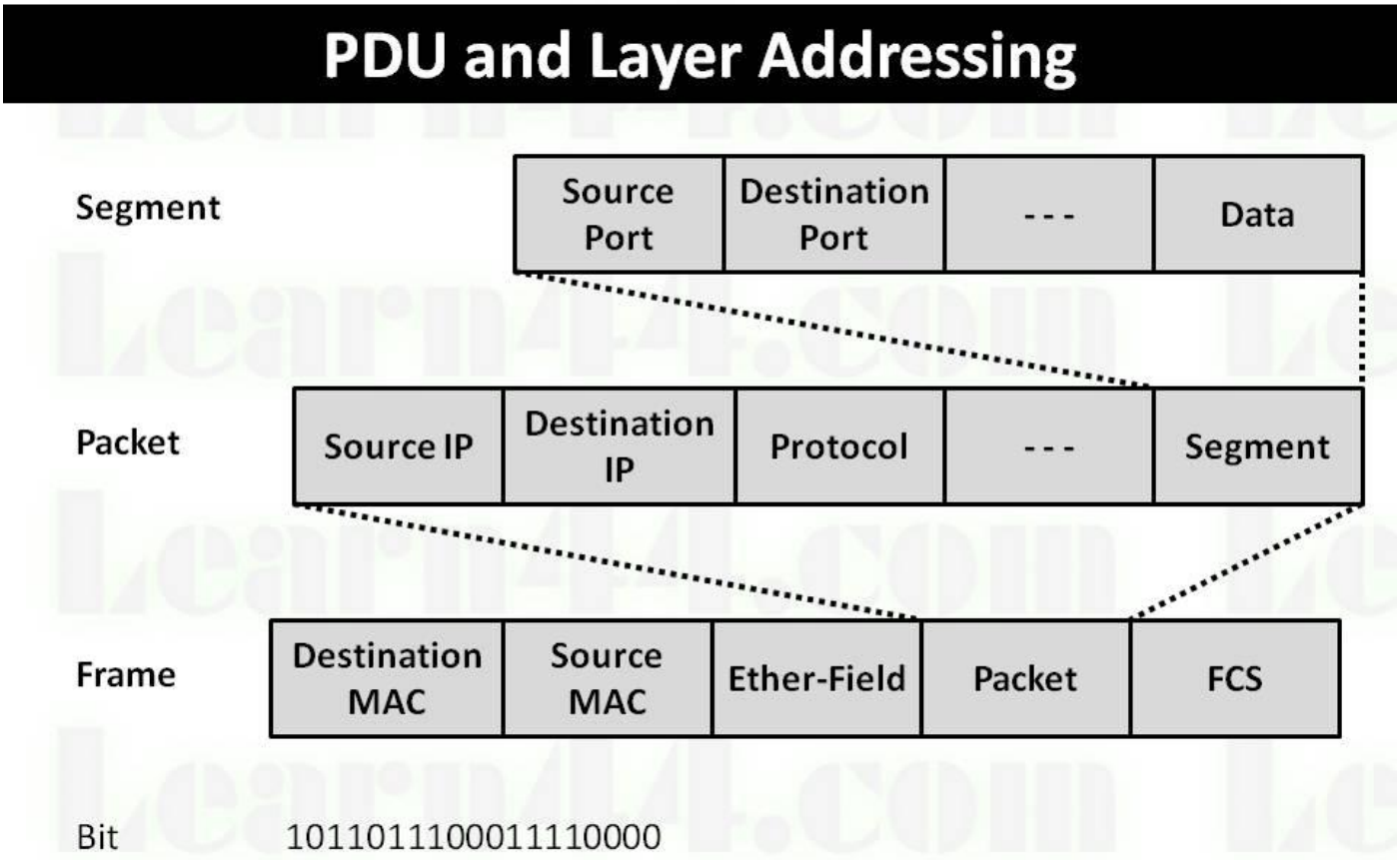
Η πρόκληση για τη χρήση της τμηματοποίησης και πολυπλεξίας για τη μετάδοση μηνυμάτων σε ένα δίκτυο είναι το επίπεδο πολυπλοκότητας που προστίθεται στη διαδικασία. Φανταστείτε εάν είχατε να στείλετε ένα e-mail 100 σελίδων, αλλά κάθε φάκελος χωράει μόνο μία σελίδα. Η διαδικασία της εξέτασης, της διευθυνσιοδότησης, της αποστολής, της λήψης και το άνοιγμα των 100 φακέλων θα ήταν χρονοβόρα τόσο για τον αποστολέα και τον παραλήπτη.

Στο δίκτυο επικοινωνιών, κάθε τμήμα του μηνύματος πρέπει να περάσει από μια παρόμοια διαδικασία για να διασφαλιστεί ότι θα φτάσει στο σωστό προορισμό και να συγκεντρωθεί το περιεχόμενο του αρχικού μηνύματος

Protocol Data Units (PDU)- Ενθυλάκωση

Καθώς τα δεδομένα περνούν από τη στοίβα πρωτοκόλλων ώστε να μεταφερθούν από τα μέσα μεταφοράς στο δίκτυο, διάφορες πληροφορίες πρωτοκόλλου προστίθενται σε κάθε επίπεδο. Αυτή η διαδικασία είναι γνωστή ως ενθυλάκωση .

Το κομμάτι των δεδομένων που λαμβάνει σε κάθε στρώμα αυτές τις πληροφορίες ονομάζεται Protocol Data Unit (PDU) . Κατά τη διάρκεια της ενθυλάκωσης , κάθε επόμενο στρώμα συμπυκνώνει το PDU που λαμβάνει από το ανώτερο επίπεδο σύμφωνα με το πρωτόκολλο που χρησιμοποιείται. Σε κάθε στάδιο της διαδικασίας , ένα PDU έχει διαφορετικό όνομα για να αντικατοπτρίζονται οι νέες λειτουργίες του .



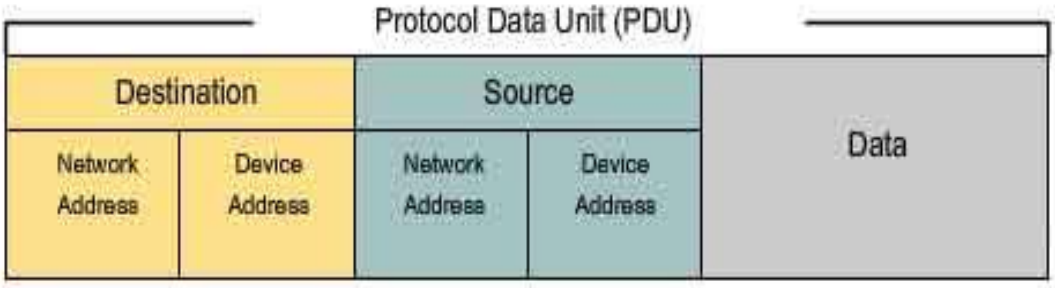
Την παραπάνω εικόνα μπορούμε να την αντιστοιχήσουμε στα επίπεδα του δικτύου.

Διευθύνσεις Δικτύου

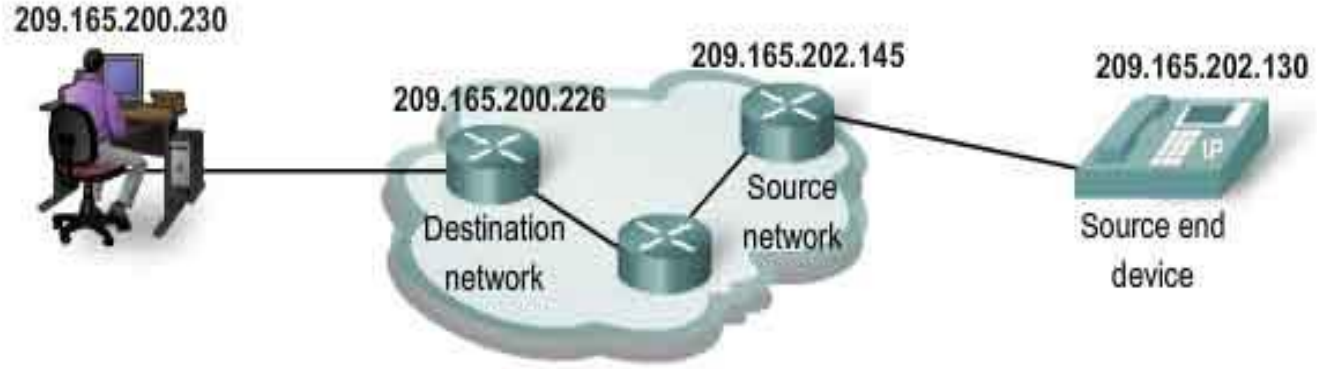
Το στρώμα του δικτύου και ζεύξης δεδομένων είναι υπεύθυνα για την παράδοση των δεδομένων από τη συσκευή της πηγής στη συσκευή του προορισμού. Τα πρωτόκολλα και στα δύο επίπεδα περιέχουν τη διεύθυνση πηγής και προορισμού, αλλά οι διευθύνσεις που δίνει το κάθε επίπεδο έχει διαφορετικό σκοπό.

Η διεύθυνση πηγής και προορισμού (IP) που δίνει το στρώμα δικτύου είναι υπεύθυνες για την παράδοση του πακέτου IP από την αρχική πηγή μέχρι τον τελικό προορισμό, είτε στο ίδιο δίκτυο είτε σε ένα απομακρυσμένο δίκτυο.

Η διεύθυνση πηγής και προορισμού που δίνει το επίπεδο ζεύξης δεδομένων είναι υπεύθυνες για την παράδοση του datalink frame από τη μία κάρτα δικτύου (NIC) σε μία άλλη NIC στο ίδιο δίκτυο.



The Protocol Data Unit header also contains the network address.



Ο ρόλος των Διευθύνσεων στο Επίπεδο Δικτύου

Οι διευθύνσεις επίπεδο δικτύου, ή διευθύνσεις IP, αναφέρουν την αρχική πηγή και τον τελικό προορισμό. Μια διεύθυνση IP περιέχει δύο μέρη:

Τμήμα του δικτύου (network portion) - Το πιο αριστερό μέρος της διεύθυνσης που δείχνει το δίκτυο που η διεύθυνση IP είναι μέλος. Όλες οι συσκευές στο ίδιο δίκτυο θα έχουν το ίδιο τμήμα του δικτύου της διεύθυνσης.

Τμήμα χρήστη (Host portion)- Το υπόλοιπο τμήμα της διεύθυνσης που προσδιορίζει μια συγκεκριμένη συσκευή στο δίκτυο. Το τμήμα χρήστη είναι μοναδικό για κάθε συσκευή στο δίκτυο.

Σημείωση: Η μάσκα υποδικτύου (subnet mask) χρησιμοποιείται για να προσδιορίσει το τμήμα δικτύου της διεύθυνσης από το τμήμα υποδοχής. Με τη μάσκα υποδικτύου θα ασχοληθούμε σε επόμενα μαθήματα.

Ο ρόλος των Διευθύνσεων στο Επίπεδο Data Link

Όταν ο αποστολέας και ο παραλήπτης του πακέτου IP βρίσκονται στο ίδιο δίκτυο, τα δεδομένα αποστέλλονται απευθείας στη συσκευή λήψης. Σε ένα δίκτυο Ethernet, οι διευθύνσεις ζεύξης δεδομένων είναι γνωστές ως Ethernet (Media Access Control) διευθύνσεις. Διευθύνσεις MAC είναι φυσικώς ενσωματωμένες στο Ethernet NIC.

Διεύθυνση MAC πηγής - Αυτή είναι η διεύθυνση ζεύξης δεδομένων, ή η διεύθυνση Ethernet MAC, της συσκευής που στέλνει το data link frame με τα έγκλειστα IP πακέτα.

Διεύθυνση MAC προορισμού - Όταν η συσκευή λήψης είναι στο ίδιο δίκτυο με τη συσκευή αποστολής, αυτή είναι η διεύθυνση της NIC της συσκευής λήψης.

Οι διευθύνσεις MAC αναπαρίστανται σε δεκαεξαδική μορφή

Κεφάλαιο 3ο

Wireshark

Το Wireshark είναι ένα πρόγραμμα open source το οποίο χρησιμοποιείται στην ανάλυση , παρακολούθηση , αλλά και εντοπισμό προβλημάτων που πιθανά να προκύψουν στο δίκτυο μας.

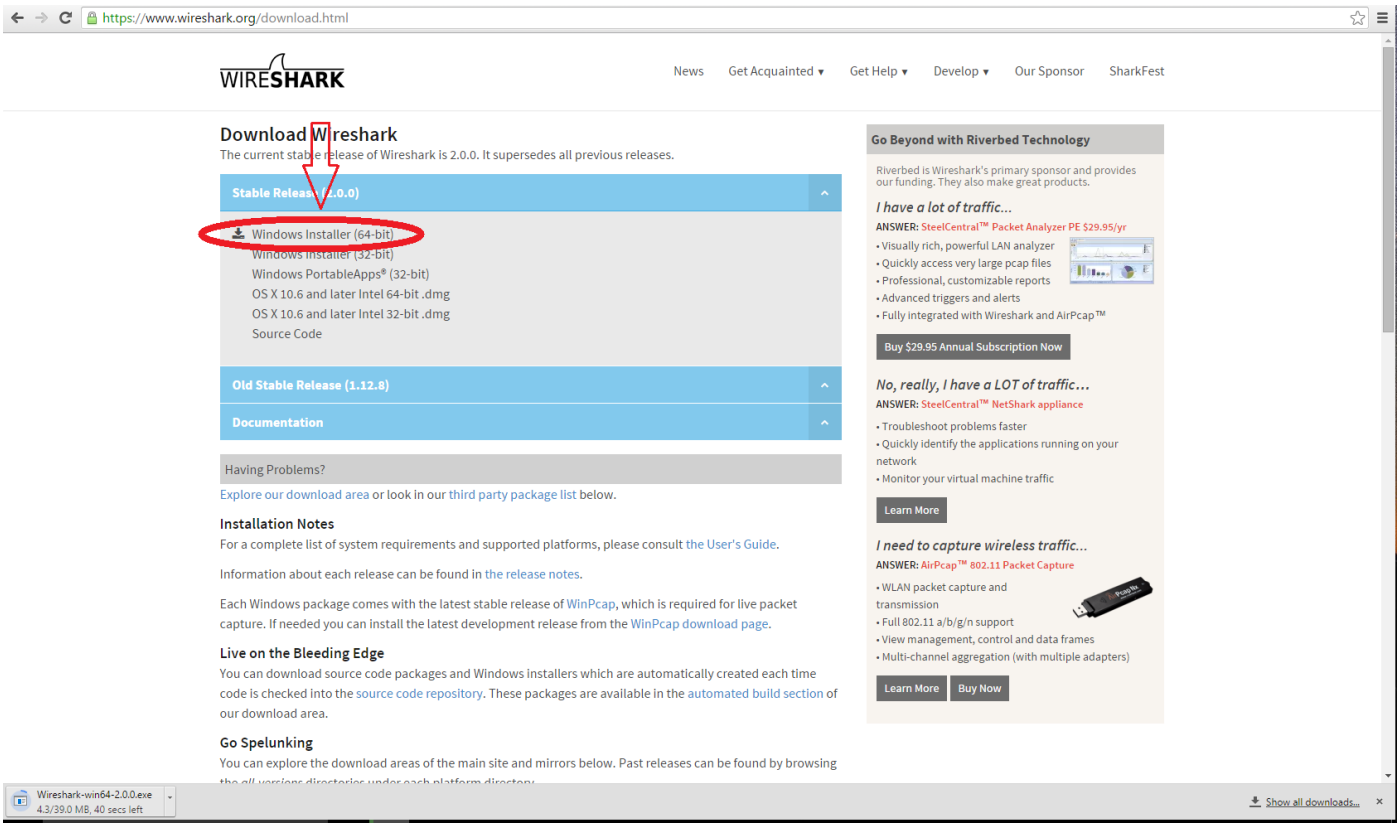
Είναι αρκετά εύχρηστο ακόμα και για μη εξοικειωμένους χρήστες χάρη στο γραφικό του περιβάλλον. Στην ουσία επιτρέπει στο χρήστη να παρακολουθήσει όλη την κίνηση που γίνεται στο δίκτυο του, να «πιάσει» και να «δει» τα πακέτα που στέλνονται και λαμβάνονται.

Εγκατάσταση του Wireshark

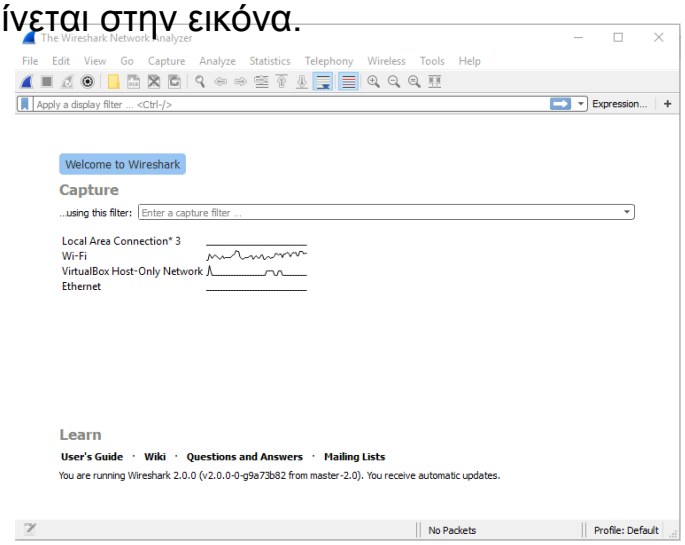
Όπως είπαμε και παραπάνω το Wireshark είναι open source πράγμα που σημαίνει ότι μπορούμε να το κατεβάσουμε ελεύθερα από την επίσημη σελίδα του.

Πηγαίνουμε λοιπόν: https://www.wireshark.org/download.html

Εκεί θα βρούμε σύνδεσμο από τον οποίο μπορούμε να κατεβάσουμε το λογισμικό μας ανάλογα με το λειτουργικό του υπολογιστή μας. Στην εικόνα παρακάτω βλέπουμε τη σελίδα από την οποία θα κατεβάσουμε το Wireshark.

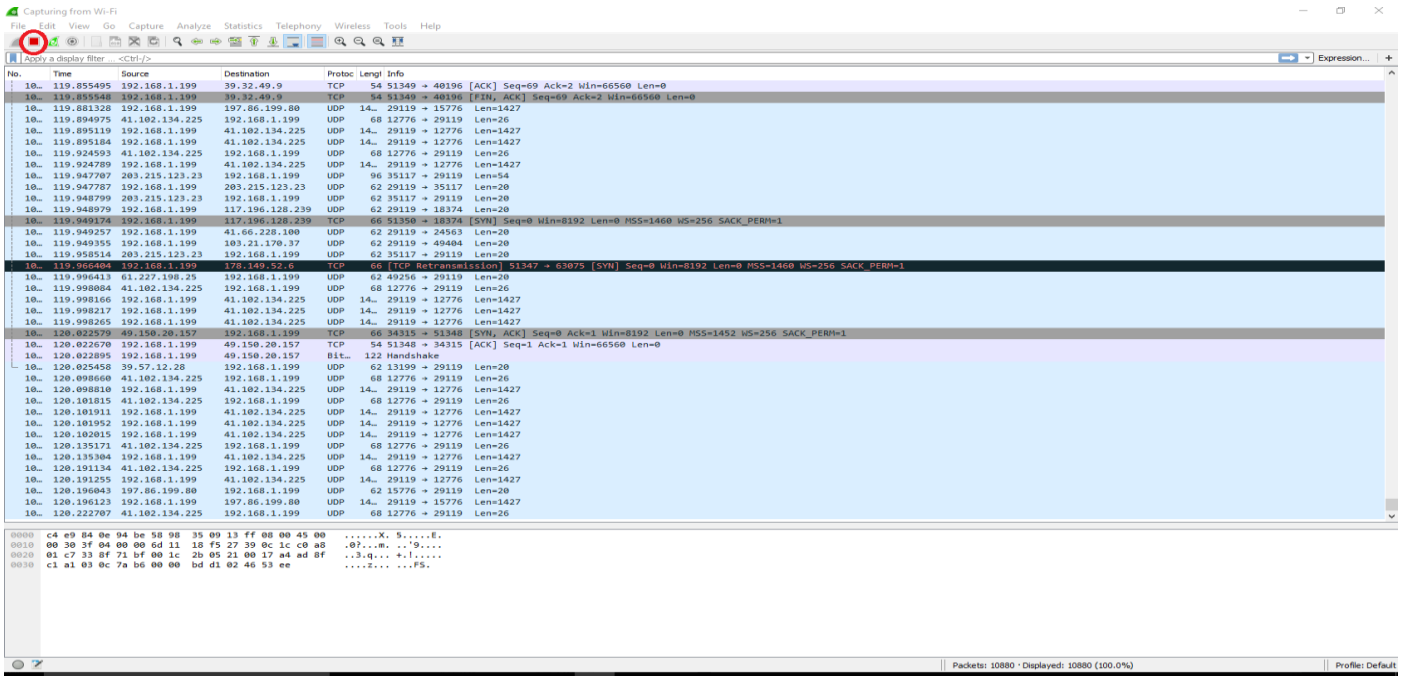


Μόλις κατέβει ξεκινάμε την εγκατάσταση. Με το που ολοκληρωθεί ανοίγουμε το πρόγραμμα που πρέπει να εμφανίζεται περίπου όπως φαίνεται στην εικόνα.



Χρήση του Wireshark

Επιλέγουμε τη σύνδεση που θέλουμε να παρακολουθήσουμε κάνοντας διπλό κλικ πάνω της . Στο παράδειγμα μας παρακολουθούμε τη wife σύνδεση.



Πατώντας το κουμπί που βρίσκεται στον κόκκινο κύκλο μπορούμε να καταγράψουμε ένα στιγμιότυπο της κίνησης του δικτύου μας, ενώ με το ακριβώς δίπλα κουμπί να συνεχίσουμε στην προηγούμενη κατάσταση. Κάτω από τη γραμμή εργαλείων έχουμε τη δυνατότητα να πιάνουμε πακέτα βάση φίλτρων πχ HTTP.

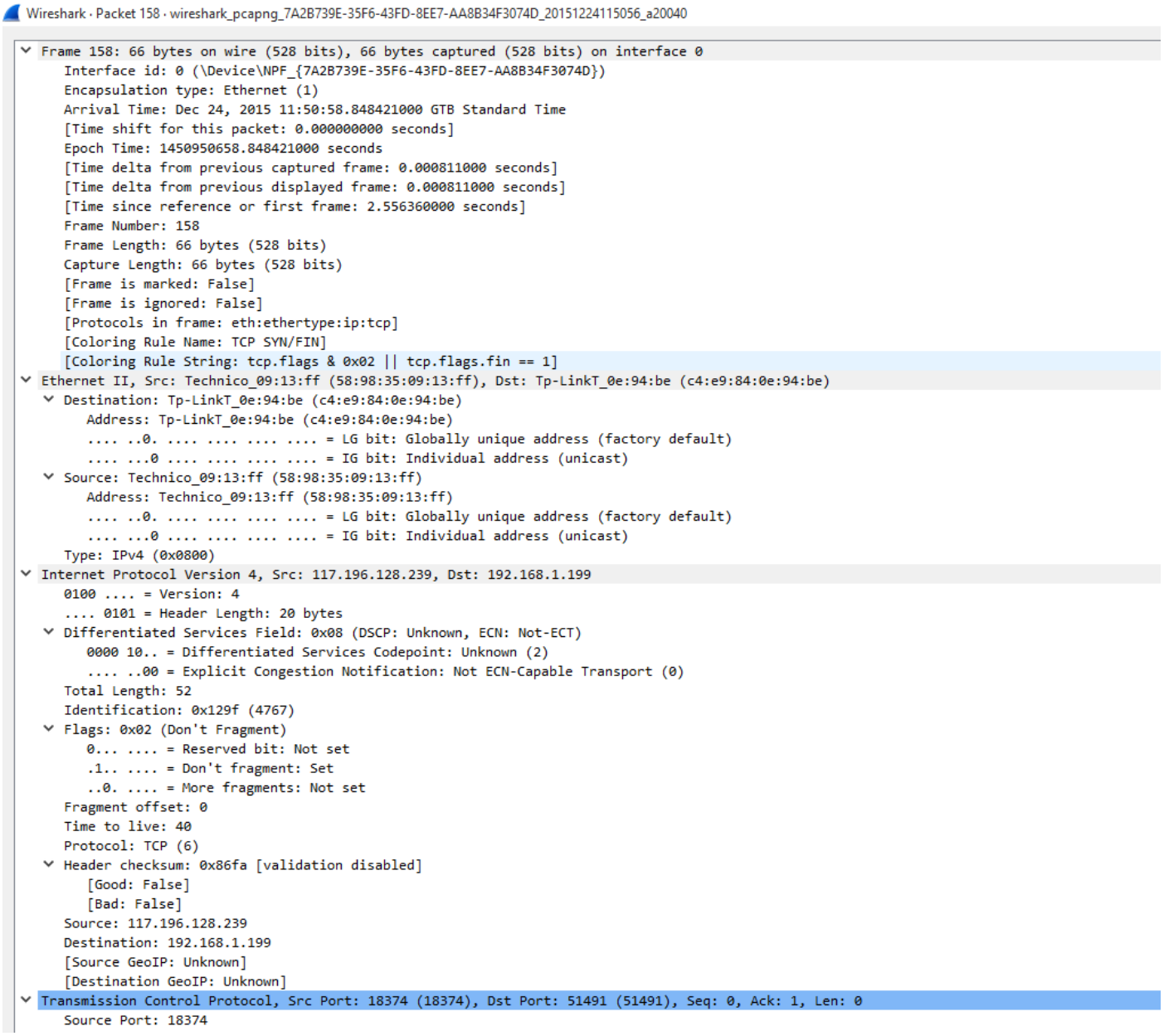
Πάμε να διαβάσουμε ένα στιγμιότυπο της κίνησης του δικτύου μας!

No.	Time	Source	Destination	Protocol	Length	Info
133	1.449827	61.227.198.25	192.168.1.199	UDP	239	49256 → 29119 Len=197
134	1.449956	192.168.1.199	61.227.198.25	UDP	1469	29119 → 49256 Len=1427
135	1.450019	192.168.1.199	61.227.198.25	UDP	62	29119 → 49256 Len=20
136	1.592723	50.49.113.104	192.168.1.199	UDP	62	25525 → 29119 Len=20
137	1.592898	192.168.1.199	50.49.113.104	UDP	62	29119 → 25525 Len=20
138	1.592977	192.168.1.199	61.227.198.25	UDP	62	29119 → 49256 Len=20
139	1.593039	192.168.1.199	50.49.113.104	UDP	62	29119 → 25525 Len=20
140	1.744664	192.168.1.199	197.86.199.80	UDP	1469	29119 → 15776 Len=1427
141	1.967466	61.227.198.25	192.168.1.199	UDP	62	49256 → 29119 Len=20
142	1.967600	192.168.1.199	61.227.198.25	UDP	1469	29119 → 49256 Len=1427
143	2.009755	61.227.198.25	192.168.1.199	UDP	62	49256 → 29119 Len=20
144	2.009859	192.168.1.199	61.227.198.25	UDP	1469	29119 → 49256 Len=1427
145	2.056642	197.86.199.80	192.168.1.199	UDP	62	15776 → 29119 Len=20
146	2.056766	192.168.1.199	197.86.199.80	UDP	1469	29119 → 15776 Len=1427
147	2.135254	192.168.1.199	121.218.199.126	UDP	145	29119 → 35999 Len=103
148	2.149722	192.168.1.199	77.68.41.118	TCP	62	51484 → 51900 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
149	2.159798	192.168.1.199	117.196.128.239	UDP	62	29119 → 18374 Len=20
150	2.160015	192.168.1.199	117.196.128.239	TCP	66	51491 → 18374 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
151	2.260924	192.168.1.199	41.102.134.225	UDP	1469	29119 → 12776 Len=1427
152	2.261120	192.168.1.199	77.68.41.118	UDP	62	29119 → 51900 Len=20
153	2.531899	117.196.128.239	192.168.1.199	UDP	62	18374 → 29119 Len=20
154	2.532028	192.168.1.199	117.196.128.239	UDP	130	29119 → 18374 Len=88
155	2.534444	121.218.199.126	192.168.1.199	UDP	329	35999 → 29119 Len=287
156	2.555257	61.227.198.25	192.168.1.199	UDP	62	49256 → 29119 Len=20
157	2.555549	192.168.1.199	61.227.198.25	UDP	1469	29119 → 49256 Len=1427
158	2.556360	117.196.128.239	192.168.1.199	TCP	66	18374 → 51491 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1400 WS=256 SACK_PERM=1
159	2.556539	192.168.1.199	117.196.128.239	TCP	54	51491 → 18374 [ACK] Seq=1 Ack=1 Win=65792 Len=0
160	2.557018	192.168.1.199	117.196.128.239	BitTorrent	122	Handshake
161	2.569146	41.102.134.225	192.168.1.199	UDP	62	12776 → 29119 Len=20
162	2.592588	61.227.198.25	192.168.1.199	UDP	62	49256 → 29119 Len=20
163	2.668175	192.168.1.199	41.102.134.225	UDP	1469	29119 → 12776 Len=1427
164	2.769340	192.168.1.199	2.84.252.120	UDP	1480	29119 → 18086 Len=1438
165	2.813559	115.242.168.197	192.168.1.199	TCP	54	[TCP Window Update] 59890 → 50991 [ACK] Seq=1 Ack=1 Win=195 Len=0
166	2.838652	2.84.252.120	192.168.1.199	UDP	62	18086 → 29119 Len=20
167	2.838802	192.168.1.199	2.84.252.120	UDP	163	29119 → 18086 Len=121
168	2.838878	192.168.1.199	2.84.252.120	UDP	163	29119 → 18086 Len=121
169	2.888744	192.168.1.199	203.215.123.23	UDP	1469	29119 → 35117 Len=1427
170	2.898774	2.84.252.120	192.168.1.199	UDP	96	18086 → 29119 Len=54
171	2.898902	192.168.1.199	2.84.252.120	UDP	62	29119 → 18086 Len=20

```
0000  c4 e9 84 0e 94 be 58 98  35 09 13 ff 08 00 45 08   ......X. 5.....E.
0010  00 34 12 9f 40 00 28 06  86 fa 75 c4 80 ef c0 a8   .4..@.(. ..u.....
0020  01 c7 47 c6 c9 23 d3 89  40 8c 19 76 da 2a 80 12   ..G..#.. @..v.*..
0030  20 00 7d 78 00 00 02 04  05 78 01 03 03 08 01 01    .}x.... .x......
0040  04 02                                              ..
```

Στην 2η στήλη βλέπουμε την ώρα που «πιάστηκε» το πακέτο από τη στιγμή που ξεκινήσαμε την παρακολούθηση. Στην 3η στήλη βλέπουμε την IP διεύθυνση της πηγής ενώ στην 4η τη IP του προορισμού. Όπως φαίνεται και στην εικόνα η IP 192.168.1.199 τη συναντάμε πολλές φορές σαν διεύθυνση πηγής αλλά και προορισμού. Αυτό συμβαίνει γιατί πρόκειται για τη δική μας διεύθυνση που εμφανίζεται σε κάθε γραμμή είτε όταν στέλνουμε ένα πακέτο , είτε όταν λαμβάνουμε. Στην 5η στήλη βλέπουμε το πρωτόκολλο που χρησιμοποιείται για την αποστολή (TCP ή UDP εδώ). Στην 6η στήλη βλέπουμε το μήκος του πακέτου ενώ στην τελευταία διάφορες σημαντικές πληροφορίες για το πακέτο.

Με διπλό κλικ πάνω στο πακέτο που μας ενδιαφέρει μπορούμε να δούμε αναλυτικά όλες τις πληροφορίες για το πακέτο μας.



Όπως βλέπετε στην εικόνα παραπάνω μιλάμε για ένα πλήθος πληροφοριών από το πότε ακριβώς λήφθηκε ή στάλθηκε το πακέτο στον υπολογιστή μας, το Ethernet protocol. Μπορούμε να δούμε τη MAC address της πηγής αλλά και τη MAC address της δικής μας κάρτας δικτύου καθώς και τον τύπο τους.

Ακόμα μπορούμε να δούμε ποια έκδοση IP χρησιμοποιεί τόσο η πηγή όσο και ο προορισμός. Πχ βλέπουμε ότι η πηγή χρησιμοποιεί IPv4 με διεύθυνση 117.192.128.239.

Στο κομμάτι του TCP μπορούμε να δούμε την πόρτα της πηγής αλλά και την πόρτα που κατευθύνθηκε το πακέτο. Με scroll

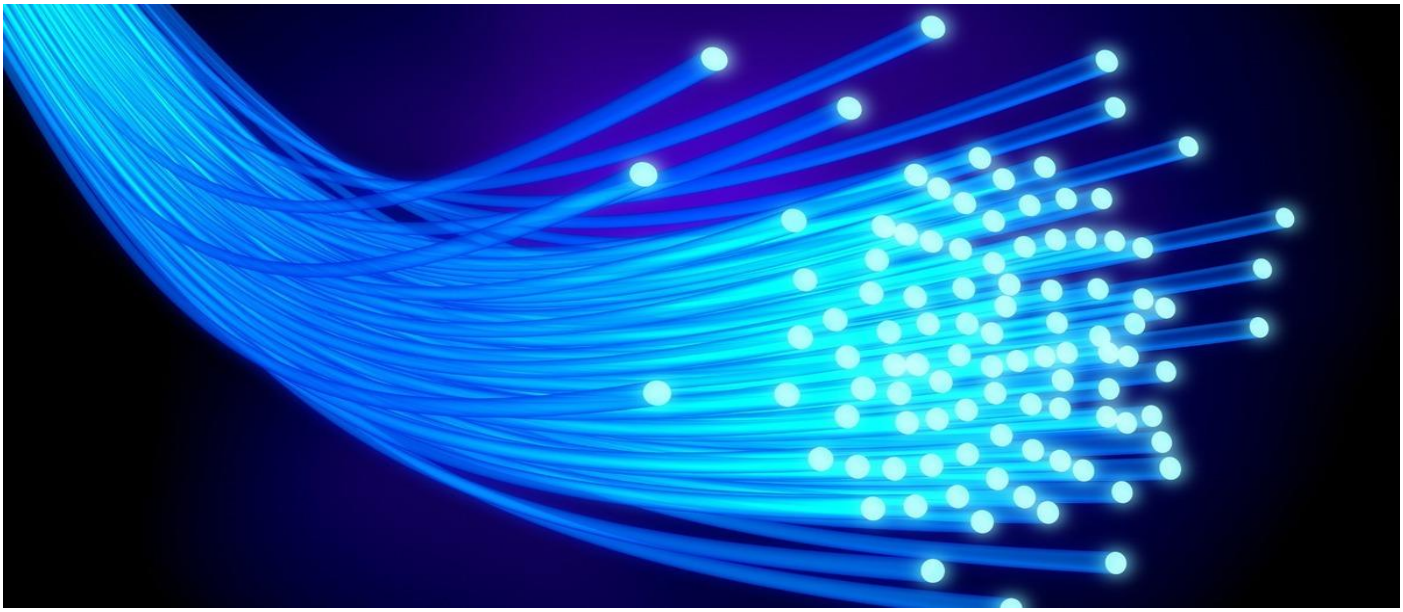
down μπορούμε να δούμε και άλλες πληροφορίες για το πακέτο μας.

Φυσικά η χρήση και λειτουργία του Wireshark δεν περιορίζεται εδώ. Δεν θα προχωρήσουμε όμως καθώς θα ξεφύγουμε από το σκοπό του μαθήματος.

Ασκήσεις σε Wireshark : 1. Πληροφορίες συνοπτικές από screenshot 2. Αναλυτικές πληροφορίες πακέτων από scrrenshot.3. Πιάνοντας ένα HTTP packet.

Κεφάλαιο 4ο

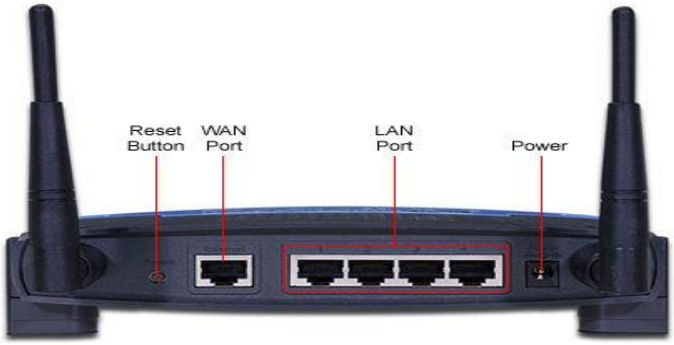
Φυσικό επίπεδο



Φυσική σύνδεση

Για να συνδέσουμε τερματικές συσκευές μεταξύ τους , είτε πρόκειται για ένα τοπικό δίκτυο, είτε για να συνδεθούμε σε ένα server στην άλλη άκρη του κόσμου, χρειάζεται πρώτα να εγκατασταθεί μία φυσική σύνδεση. Μία φυσική σύνδεση μπορεί να είναι ενσύρματη χρησιμοποιώντας καλώδια αλλά μπορεί να είναι και ασύρματη χρησιμοποιώντας ραδιοκύματα.

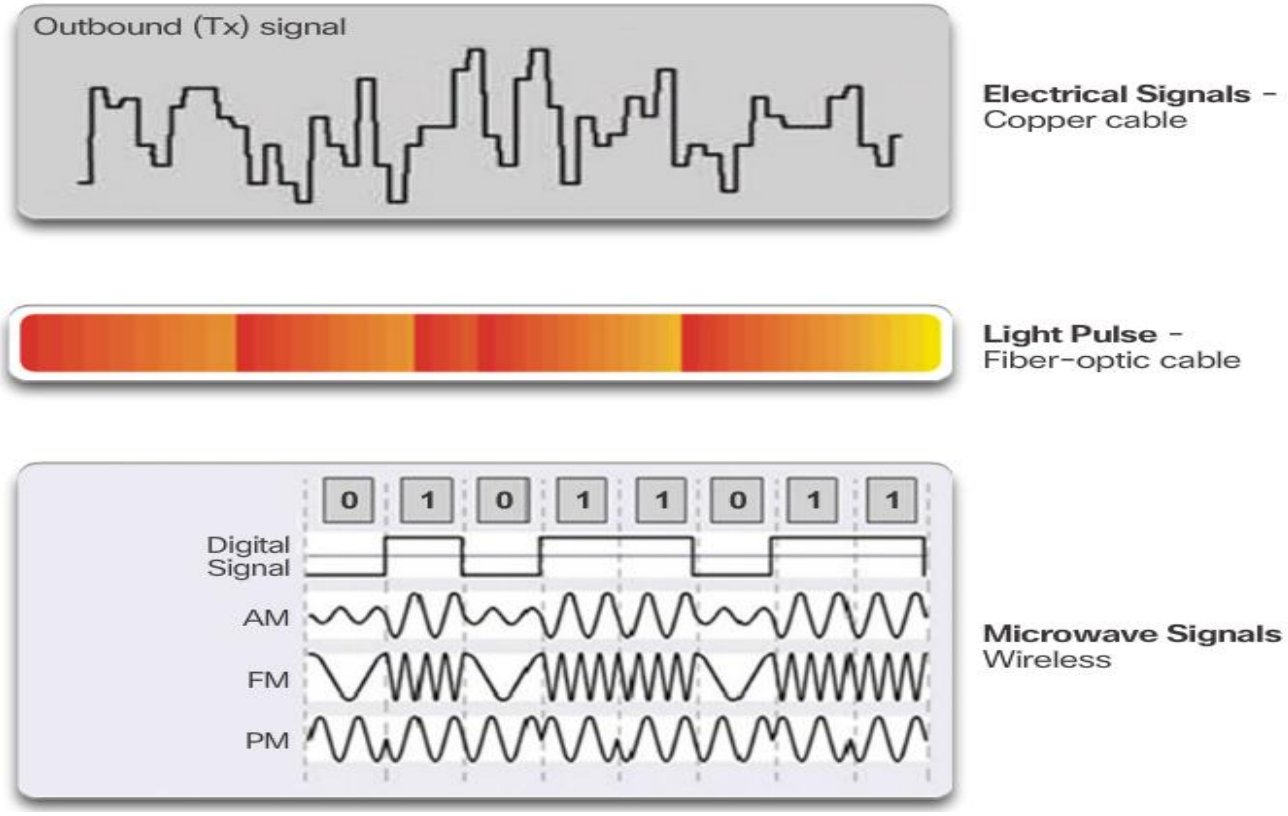
Στο σπίτι μας συνδυάζουμε την ενσύρματη με την ασύρματη σύνδεση καθώς το router μας λειτουργεί ταυτόχρονα και σαν switch αλλά και σαν wireless access point!



Μέσα μετάδοσης

Υπάρχουν 3 βασικοί τύποι μέσων μετάδοσης δικτύου:

1. Χάλκινο καλώδιο
2. Καλώδιο οπτικών ινών
3. Wireless (Μικροκύματα)



Ιδιότητες μέσων μετάδοσης

Bandwidth: Είναι η ικανότητα του μέσου να μεταφέρει πληροφορίες. Μετριέται σε bits per second (b/s)

Throughput: είναι η μονάδα μέτρησης από τα μεταφερόμενα Bits διαμέσου του καλωδίου σε μία συγκεκριμένη περίοδο του χρόνου. Παίρνουμε υπόψη την «κίνηση» στο μέσο (traffic), τον τύπο της κίνησης , την καθυστέρηση από τις ενδιάμεσες συσκευές μεταξύ της πηγής και του προορισμού. (bps)

Καλώδιο UTP

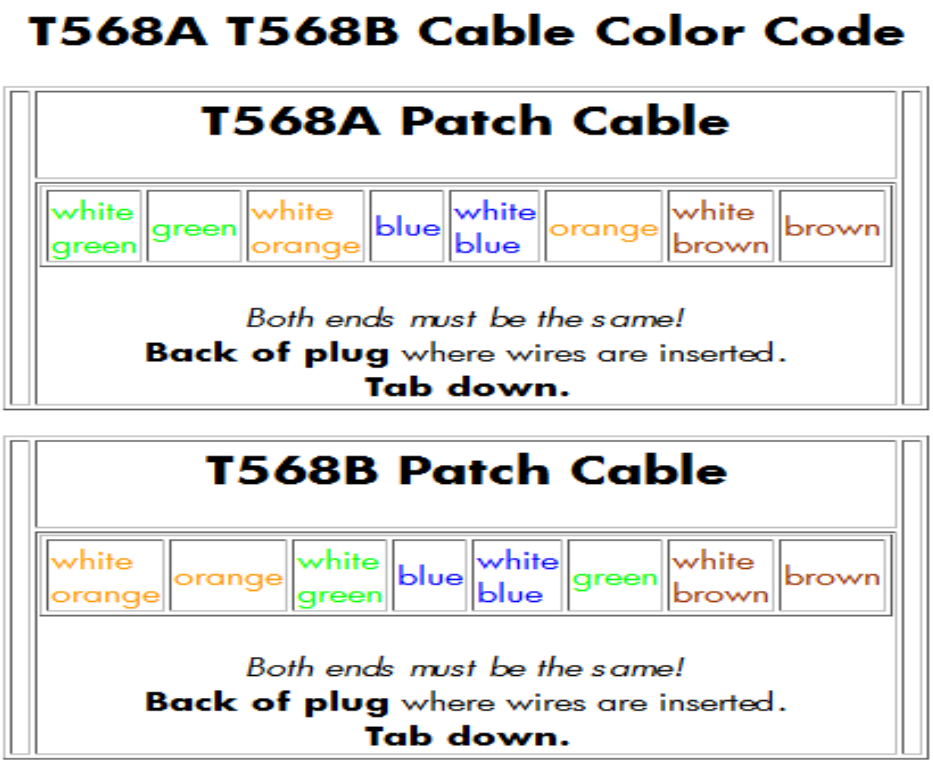
Το καλώδιο UTP (Unshielded Twisted-Pair Cable) είναι το πιο γνωστό και κοινό καλώδιο δικτύου. Περιέχει 4 ζεύγη χρωματισμένων συνεστραμμένων καλωδίων το οποίο προστατεύει από τις παρεμβολές το καλώδιο. Υπάρχουν διαφορετικοί τύποι UTP καλωδίων που υποστηρίζουν και αντίστοιχα bandwidth.

Βάσει της συνδεσμολογίας των συνεστραμμένων ζευγαριών καλωδίων που υπάρχουν μέσα στο UTP μπορούμε να φτιάξουμε και το αντίστοιχο καλώδιο για τη δουλειά που θέλουμε. Έχουμε 2 βασικές συνδεσμολογίες : την T568A και την T568B.

Όταν και οι δύο άκρες του καλωδίου είναι συνδεδεμένες με τον ίδιο τρόπο έχουμε straight-through καλώδιο ενώ όταν είναι ανάποδα έχουμε Crossover καλώδιο.

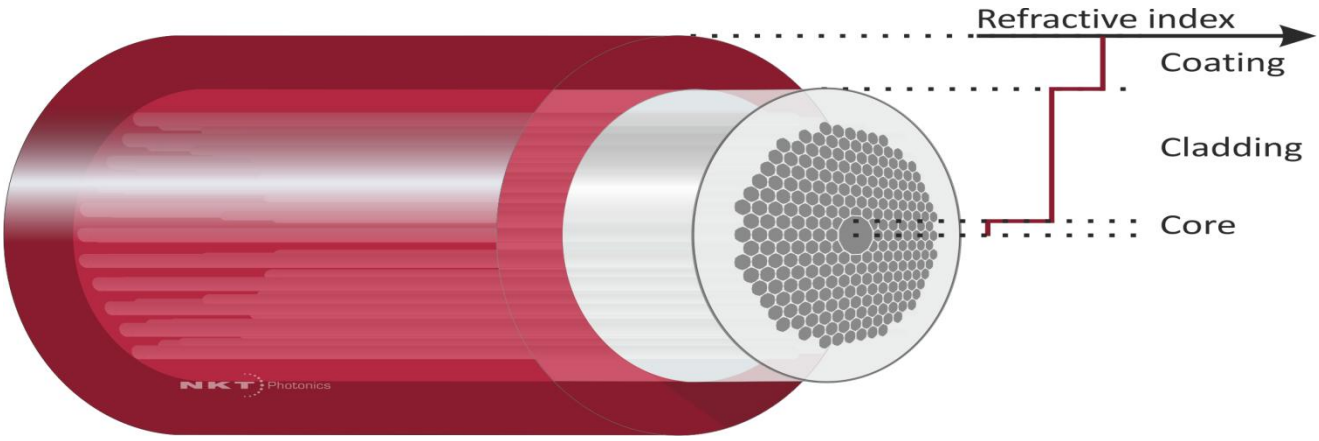
Straight-through: Το πιο κοινό καλώδιο, αυτό που συνδέει ένα χρήστη στο switch, το switch με το router.

CrossOver: Είναι καλώδιο που χρησιμοποιείται ώστε να συνδέει παρόμοιες συσκευές όπως ένα switch με ένα άλλο switch, ένα υπολογιστή με ένα άλλο κλπ. Χρησιμοποιείται επίσης για να συνδέσουμε απευθείας πάνω στο router ένα PC (Προσοχή στο σπίτι μας έχουμε layer 3 switch και όχι router και για αυτό χρησιμοποιούμε Straight-through!!).



Οπτική ίνα

Οι οπτικές ίνες μεταδίδουν πληροφορίες σε πολύ μεγάλες αποστάσεις ενώ έχουν πολύ μεγάλο bandwidth. Στην εικόνα από κάτω βλέπουμε το σχεδιασμό της.



Έχουμε 2 τύπους οπτικών ινών:

1. Single-mode fiber (SMF): Περιέχει ένα πολύ μικρό πυρήνα και χρησιμοποιεί τεχνολογία laser ώστε να στείλει μία

ακτίνα. Χρησιμοποιείται σε μεγάλες αποστάσεις πολλών χιλιομέτρων.

2. Multimode fiber (MMF): Περιέχει μεγαλύτερο πυρήνα και χρησιμοποιεί τεχνολογία led ώστε να στείλει παλμούς φωτός. Υποστηρίζει bandwidth έως 10Gb/s σε αποστάσεις μέχρι μισό χιλιόμετρο.

Short name	Long form	Coupling type	Ferrule diameter	Standard	Typical Applications
SC	Subscriber Connector or square connector or Standard Connector	Snap (push-pull)	2.5 mm	IEC 61754-4	Datacom and telcom; GBIC; extremely common
FC	Fix Connector or Ferrule Connector	Screw	2.5 mm	IEC 61754-13	Datacom, telecom, measurement equipment, single-mode lasers;
LC	Lucent Connector or Little Connector	Snap	1.25 mm	IEC 61754-20	High-density connections
ST	Straight Tip	Bayonet	2.5 mm	IEC 61754-2	Multimode, rarely single-mode; APC not possible

Short name	Long form	Coupling type	Ferrule diameter	Standard	Typical Applications
MU	Miniature unit	Snap	1.25 mm	IEC 61754-6	Common in Japan
FDDI	Fiber Distribution Data Interface	Positive Latching Mechanism	2.5mm	ANSI	Duplex multimode connector utilized as High-speed Backbone in FDDI networks
MTRJ	Mechanical Transfer Registered Jack	Snap (Duplex)	2.45×4.4 mm	IEC 61754-18	Duplex multimode connections
SMA	Sub Miniature A	Screw	Typ. 3.14 mm		Industrial lasers, military; telecom multimode

Έλεγχος καλωδίων

Το πιο συνηθισμένο πρόβλημα συνδεσιμότητας σε ένα δίκτυο βρίσκεται στο καλώδιο. Μπορεί να έχει κοπεί σε κάποιο σημείο , είτε οι άκρες του να έχουν αποκολληθεί από κάποιο απότομο τράβηγμα. Η πρώτη δουλειά μας λοιπόν σε μία βλάβη στο δίκτυο αφού έχουμε διαπιστώσει ανικανότητα σύνδεσης είναι να ελέγξουμε τα καλώδια μας.

Για αυτό το λόγο έχουμε το tester. Είναι ένα μηχάνημα το οποίο συνδέουμε ένα μέρος του στη μία άκρη ενός καλωδίου και το κύριο μέρος του στο άλλο. Ανάλογα με το πόσο καλό είναι, το

κύριο μέρος μπορεί να έχει οθόνη που να μας δείχνει αν όλα είναι συνδεδεμένα σωστά, αν έχει κοπεί κάπου το καλώδιο και σε τι απόσταση κλπ.

Κεφάλαιο 5ο

Διευθύνσεις Δικτύου

Διευθύνσεις IPv4

Η διευθυνσιοδότηση είναι μία βασική λειτουργία του επιπέδου δικτύου (network layer). Δίνει τη δυνατότητα να μπορεί να επικοινωνεί ο ένας χρήστης με τον άλλον στο δίκτυο ανεξάρτητα με το πόσοι χρήστες βρίσκονται συνδεδεμένοι σε αυτό. Κάθε χρήστης στο δίκτυο έχει μία διεύθυνση IP η οποία είναι μοναδική.

Κάθε IPv4 αποτελείται από 32 bit χωρισμένα σε 8 τομείς. Κάθε τομέας αποτελείται από 8 bit και χωρίζονται μεταξύ τους από μία τελεία. Για παράδειγμα μία διεύθυνση δικτύου σε δυαδική μορφή είναι η εξής:

11000000.10101000.00001010.00000001

Το να δουλεύουμε και να επεξεργαζόμαστε τις IP σε δυαδικό σύστημα είναι δύσκολο. Γι αυτό και μετατρέπουμε τις IP σε δεκαδικό σύστημα ώστε να μπορούμε να τις επεξεργαζόμαστε πιο εύκολα. Έτσι η παραπάνω διεύθυνση μεταφράζεται σε δεκαδικό:

192.168.10.1

Χρειαζόμαστε όμως να μπορούμε να μετατρέπουμε από δεκαδικό σε δυαδικό οπότε θα δώσουμε λίγο βάρος στο πως θα κάνουμε αυτή τη διαδικασία εύκολη!

Μετατροπή δυαδικού σε δεκαδικό

Για να κάνουμε εύκολη τη μετατροπή από δεκαδικό σε δυαδικό χρειάζεται να έχουμε στο μυαλό μας τις δυνάμεις του 2.

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Αντιστοιχίζοντας τον παραπάνω πίνακα σε 8 bit που έχει ο κάθε τομέας μπορούμε να δούμε ότι:

Ο 1ος τομέας του παραδείγματος IP που δώσαμε παραπάνω αντιστοιχεί:

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	0	0	0	0	0	0

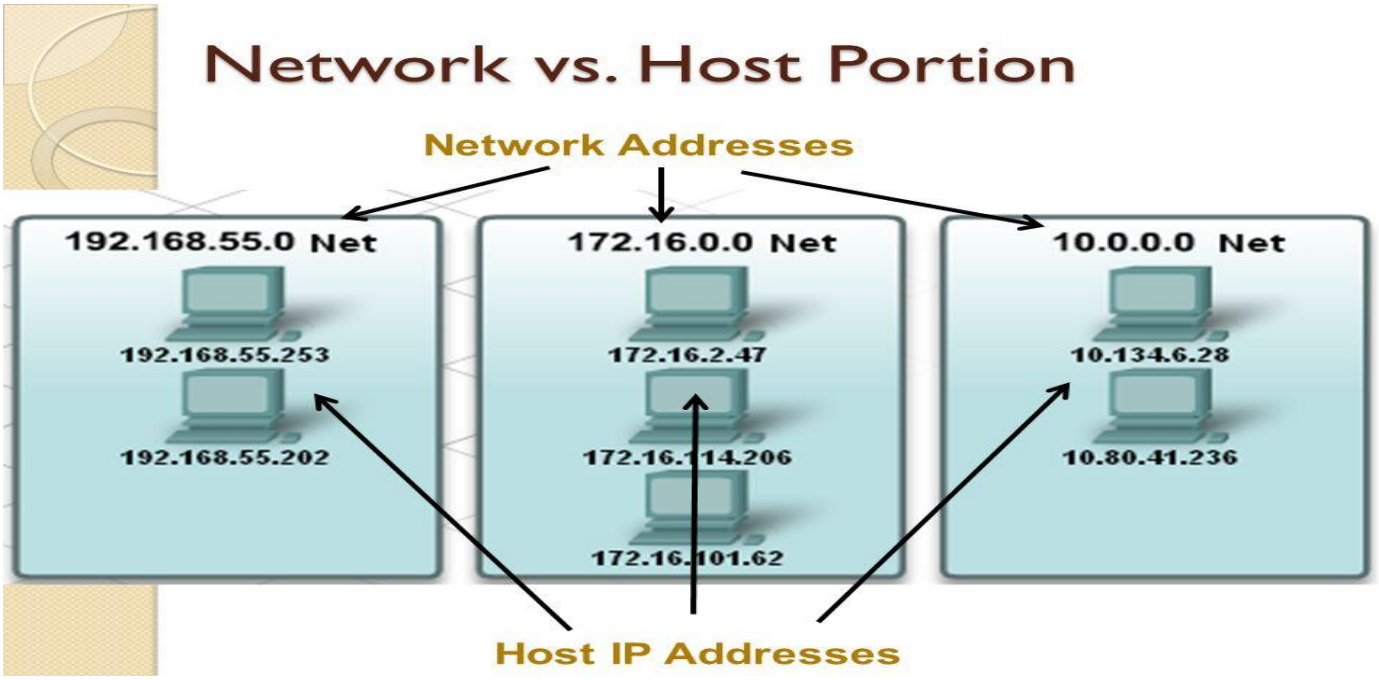
128 + 64 + 0 + 0 + 0 + 0 + 0 + 0 =192

Όπως βλέπουμε αν «γεμίσουμε με άσσους» και τα 8 bit θα έχουμε αποτέλεσμα ίσο με 255. Άρα οι διευθύνσεις φτάνουν έως :

255.255.255.255

Τμήμα δικτύου και τμήμα χρηστών

Οι IP διευθύνσεις δεν μοιράζονται τυχαία στους χρήστες σε όλο το δίκτυο , σε όλο το internet. Οι χρήστες που βρίσκονται στο ίδιο δίκτυο μοιράζονται ένα τμήμα της IP (είναι κοινό), και ένα τμήμα διαφέρει ώστε να τους καθορίζει μονοσήμαντα.



Για να ξεχωρίσουμε ποιο τμήμα της διεύθυνσης ανήκει στο δίκτυο και ποιο στους χρήστες χρειαζόμαστε τη μάσκα δικτύου (subnet mask). Ένα παράδειγμα μάσκας δικτύου :

255.255.255.0

Τι σημαίνει όμως αυτό; Ας το δούμε σε ένα παράδειγμα! Έστω ότι έχουμε IP σε ένα υπολογιστή 192.168.10.65 με μάσκα δικτύου 255.255.255.0. Αυτό σημαίνει ότι:

192 .	168 .	10 .	65
11000000 .	10101000 .	00001010 .	01000001
255 .	255 .	255 .	0
11111111 .	11111111	11111111 .	00000000

Κάνοντας την πράξη and μεταξύ της IP και της μάσκας δικτύου παίρνουμε αποτέλεσμα το τμήμα δικτύου.

Άρα το τμήμα δικτύου είναι:

{11000000 . 10101000 . 00001010 } . 00000000

{192 . 168 . 10 }. 0

Μπορούμε να αναπαραστήσουμε τη μάσκα δικτύου επίσης με βάση του πόσους άσσους έχει στη δυαδική της μορφή. Στο παράδειγμα μας είναι **/ 24**

192.168.10.65 /24

Διεύθυνση δικτύου , χρηστών, και broadcast

Όπως είδαμε παραπάνω οι χρήστες που βρίσκονται στο ίδιο δίκτυο μοιράζονται ένα κοινό μέρος της IP διεύθυνσης το οποίο ξεχωρίζει από τη μάσκα δικτύου. Καταλαβαίνουμε ότι με βάση τα bit που μένουν με μηδενικά στο τέλος της IP ενός δικτύου καθορίζουν το πόσες διευθύνσεις έχει αυτό το δίκτυο. Στο προηγούμενο παράδειγμα με /24 μάσκα, έχουμε 255 διευθύνσεις. Από 192.168.10.0 έως 192.168.10.255. Πόσους χρήστες όμως χωράει; Χωράει 255 που είναι οι διευθύνσεις – 2 διευθύνσεις που χρησιμοποιεί το ίδιο το δίκτυο. Αυτές είναι:

1. Διεύθυνση δικτύου: Είναι η πρώτη διεύθυνση που καθορίζει το δίκτυο (την αρχή του), στην προκειμένη περίπτωση 192.168.10.0 Αυτή η διεύθυνση δεν δίνεται σε κανένα χρήστη.
2. Broadcast διεύθυνση: είναι η τελευταία διεύθυνση του δικτύου και χρησιμοποιείται για να επικοινωνεί με όλους τους χρήστες του δικτύου. Στο δικό μας παράδειγμα είναι η

192.168.10.255. Επίσης δεν μπορεί να ανατεθεί σε κανένα χρήστη.

Όλες οι ενδιάμεσες διευθύνσεις , δηλαδή οι υπόλοιπες 253 μπορούν να ανατεθούν στους χρήστες του δικτύου.

Δημόσιες και ιδιωτικές IPv4 διευθύνσεις

Το σύνολο των IPv4 διευθύνσεων είναι από 0.0.0.0 έως 255.255.255.255 εκ των οποίων κάποιες είναι δεσμευμένες από ερευνητικούς οργανισμούς, μεγάλες εταιρίες, το στρατό, μυστικές υπηρεσίες κ.α. Αυτό μας δίνει ένα σύνολο 2^32 διευθύνσεων, κάτι λιγότερο από 4,3 δισεκατομμύρια!

Μπορεί να φαίνονται πάρα πολλές αλλά η πραγματικότητα το διαψεύδει. Με τόσες συσκευές που πλέον συνδέονται στο internet, από υπολογιστές, tablet, smartphones, μέχρι και οικιακές συσκευές καταλαβαίνουμε ότι ο αριθμός αυτός δεν επαρκεί. Αυτό είχε λυθεί ως ένα βαθμό προσωρινά με το διαχωρισμό των IPv4 διευθύνσεων σε ψεύτικες και πραγματικές, ιδιωτικές-δημόσιες. Ακόμα και με αυτό το διαχωρισμό όμως οι IPv4 διευθύνσεις έχουν εξαντληθεί από το Φλεβάρη του 2011! Στη συνέχεια του κεφαλαίου θα δούμε πως έχει λυθεί αυτό το πρόβλημα. Προς το παρόν θα ασχοληθούμε με τις πραγματικές και ψεύτικες διευθύνσεις.

Τι είναι όμως μια ψεύτικη διεύθυνση και τι μια πραγματική; Είπαμε πριν ότι κάθε συσκευή που βρίσκεται μέσα σε ένα δίκτυο έχει μία διεύθυνση που την καθορίζει μονοσήμαντα. Αυτό μας δίνει τη δυνατότητα σε 2 συσκευές που βρίσκονται σε διαφορετικά δίκτυα να έχουν την ίδια IP(ψεύτική-ιδιωτική) όσο επικοινωνούν με άλλες συσκευές στο ίδιο με αυτές δίκτυο, αλλά θα χρειαστούν ξεχωριστή (πραγματική -δημόσια) όταν «βγουν» στο internet.

Με αυτό το σκεπτικό ένα κομμάτι των IPv4 διευθύνσεων έχουν ξεχωριστεί και θεωρούνται ψεύτικες, δεν αναγνωρίζονται στο internet. Τα μπλοκ των ψεύτικων διευθύνσεων είναι:

- 24-bit Block (/8 prefix,) 10.0.0.0 - 10.255.255.255

- 20-bit Block (/12 prefix) 172.16.0.0 - 172.31.255.255
- 16-bit Block (/16 prefix) 192.168.0.0 - 192.168.255.255

Όλες οι υπόλοιπες διευθύνσεις είναι πραγματικές και χρησιμοποιούνται από τις συσκευές μόλις «βγαίνουν» στο internet. Πραγματικές διευθύνσεις μας δίνουν οι ISP.

Κλάσεις των IPv4 διευθύνσεων

Υπάρχει ακόμα ένας διαχωρισμός των IPv4 διευθύνσεων που πλέον έχει ξεπεραστεί και χρησιμοποιείται σε ελάχιστες περιπτώσεις.

- Κλάση A (0.0.0.0/8 να 127.0.0.0/8) - Σχεδιασμένη για να υποστηρίξει εξαιρετικά μεγάλα δίκτυα με περισσότερες από 16 εκατομμύρια διευθύνσεις υποδοχής.
- Κλάση B (128.0.0.0 / 16 - 191.255.0.0 / 16) - Σχεδιασμένο για να υποστηρίξει ανάγκες μέτριου έως μεγάλου μεγέθους δίκτυα με μέχρι περίπου 65.000 διευθύνσεις υποδοχής.
- Κλάση C (192.0.0.0 / 24 - 223.255.255.0 / 24) - Σχεδιασμένο για να υποστηρίξει μικρά δίκτυα με μέγιστο αριθμό 254 διευθύνσεων.
- Υπάρχει επίσης ένα μπλοκ πολλαπλής D κλάσης που αποτελείται από 224.0.0.0 239.0.0.0 και ένα κλάσης E μπλοκ που αποτελείται από 240.0.0.0 - 255.0.0.0. και χρησιμοποιείται για πειραματικούς λόγους.

IPv6 Διευθύνσεις

Το πρόβλημα της εξάντλησης των IPv4 διευθύνσεων δεν λύθηκε όπως είπαμε με τις πραγματικές και ψεύτικες διευθύνσεις, απλά καθυστέρησε λίγο την εμφάνιση του προβλήματος.

Η λύση στην εξάντληση των IPv4 διευθύνσεων είναι οι διευθύνσεις IPv6! Η σημαντική διαφορά τους είναι ότι, αντί για 32 bit αριθμητικές διευθύνσεις που χρησιμοποιεί η IPv4 η IPv6

χρησιμοποιεί 128bit αριθμητικές διευθύνσεις. Αυτό μας δίνει 2^128 διευθύνσεις IPv6 δηλαδή:

340.000.000.000.000.000.000.000.000.000.000.000.000 διευθύνσεις!!!

Αυτή τη στιγμή χρησιμοποιούνται και οι δύο τύποι IP διευθύνσεων στο internet.

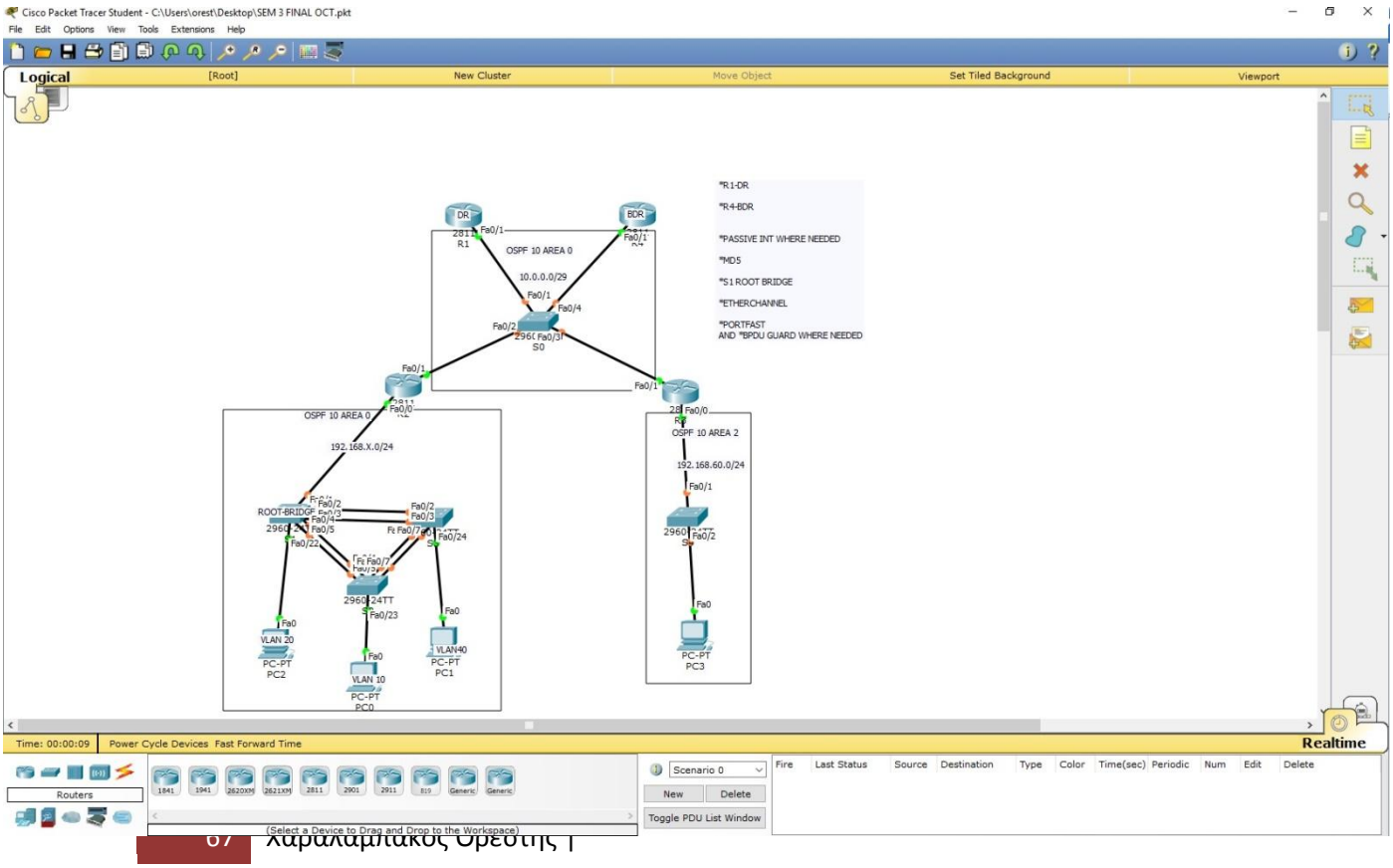
Ένα παράδειγμα IPv6 διεύθυνσης είναι:

2001:0DB8:0000:1111:0000:0000:0000:0200

Ο κάθε τομέας εδώ που χωρίζεται με : αποτελείται από 16 bit και το κάθε νούμερο αντιπροσωπεύει 4 bit. Όπως βλέπουμε οι IPv6 διευθύνσεις γράφονται στο δεκαεξαδικό σύστημα.

Packet Tracer

Το packet tracer είναι ένα πολύ χρήσιμο εργαλείο για την εκμάθηση και την προσομοίωση δικτύων! Θα είναι το πρόγραμμα με το οποίο θα δουλέψουμε κατά κύριο λόγο από εδώ και πέρα!



Ένα στιγμιότυπο του packet tracer

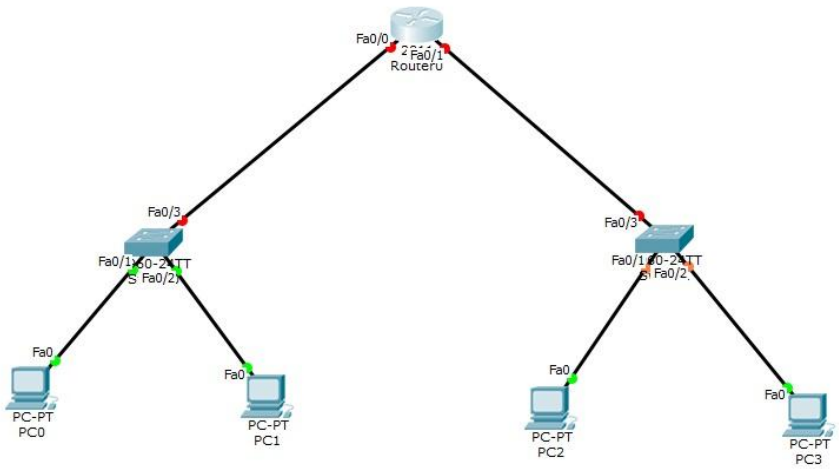
Στο κάτω αριστερό μέρος του packet tracer μπορούμε να βρούμε κάθε τύπο συσκευής δικτύου, από υπολογιστές και smartTV έως routers και switches , webservers κ.α, και κάθε τύπου καλώδια δικτύου!

Ο κεντρικός χώρος είναι η μακέτα μας και με drag and drop φτιάχνουμε το δίκτυο που θέλουμε! Χρειάζεται προσοχή στο τι τύπου καλώδιο χρησιμοποιούμε κάθε φορά (βλ κεφ 4) καθώς και να συνδέονται στη σωστή θύρα!

Με μονό κλικ μπαίνουμε στο interface της συσκευής και από εκεί ανάλογα με το τι θέλουμε να κάνουμε επιλέγουμε αντίστοιχα από το μενού που μας δίνει.

Στήνουμε το πρώτο μας δίκτυο!

Στη μακέτα μας βάζουμε 4 υπολογιστές, 2 switch 2960 και 1 router 2811. Συνδέουμε τους 4 υπολογιστές με τα switch και τα switch με το router χρησιμοποιώντας τα αντίστοιχα (σωστά) καλώδια, όπως φαίνεται στην εικόνα.



Basic configuration στο switch

Πηγαίνουμε στην καρτέλα CLI που μας δίνει το command line του switch. Έχουμε τρία επίπεδα που δίνουμε εντολές. Στην πραγματικότητα για να συνδεθούμε στο switch συνδεόμαστε πάνω σε αυτό με ένα καλώδιο κονσόλας στην αντίστοιχη θύρα. Στο 1ο μπορούμε να εκτελέσουμε λίγες απλές εντολές που μας δείχνουν πληροφορίες για το switch και το ονομάζουμε user mode. Στο 2ο επίπεδο μπορούμε να εκτελέσουμε όλες τις εντολές που μας δίνουν πληροφορίες για το switch, κάποιες βασικές εντολές και ονομάζεται privileged mode. Στο 3ο επίπεδο εκτελούμε τις εντολές για το configuration του switch και ονομάζεται global configuration mode. Στο βασικό «σετάρισμα» του switch χρησιμοποιούμε ένα μπλοκ απλών εντολών που διασφαλίζουν την ασφάλεια του switch από εξωτερικούς , μη εξουσιοδοτημένους χρήστες.

Switch>**enable** *με την εντολή αυτή μπαίνουμε στο privileged mode*
Switch#**configure terminal** *με την εντολή αυτή μπαίνουμε στο global configuration mode*
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#**enable secret *pass*** *ενεργοποιούμε κωδικό για την είσοδο στο privileged mode (pass)*
Switch(config)#**line console 0** *μπαίνουμε για configuration στην θύρα της κονσόλας (line console)*
Switch(config-line)#**password pass** *βάζουμε κωδικό (pass) στην σύνδεση στο switch μέσω κονσολοκαλωδιου.*
Switch(config-line)#**login** *ενεργοποιούμε τη διαδικασία αυθεντικοποίησης με κωδικό για τη σύνδεση*
Switch(config-line)#**exit** *βγαίνουμε από τη θύρα της κονσόλας*
Switch(config)#**service password-encryption** *κρυπτογραφούμε τους κωδικούς μας*
Switch(config)#**hostname SW1** *δίνουμε όνομα στο switch*
SW1(config)#**banner motd *Authorised Access Only*** *φτιάχνουμε banner που ειδοποιεί για απαγόρευση εισόδου*
SW1(config)#**exit** *βγαίνουμε από το global configuration mode*
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1#**copy running-config startup-config** *αποθηκεύουμε τις αλλαγές μας*
Destination filename [startup-config]?
Building configuration...
[OK]
SW1#

Η κάθε εντολή εκχωρείται με το πάτημα του enter.
Οι εντολές είναι μαρκαρισμένες με το bold.

,

Basic configuration στο router

Ακριβώς το ίδιο «σετάρισμα» κάνουμε και στο router. Στο router όμως χρειάζεται να χρησιμοποιήσουμε μερικές εντολές ακόμα να ενεργοποιήσουμε τα interface που συνδέουν το router με τα switch.

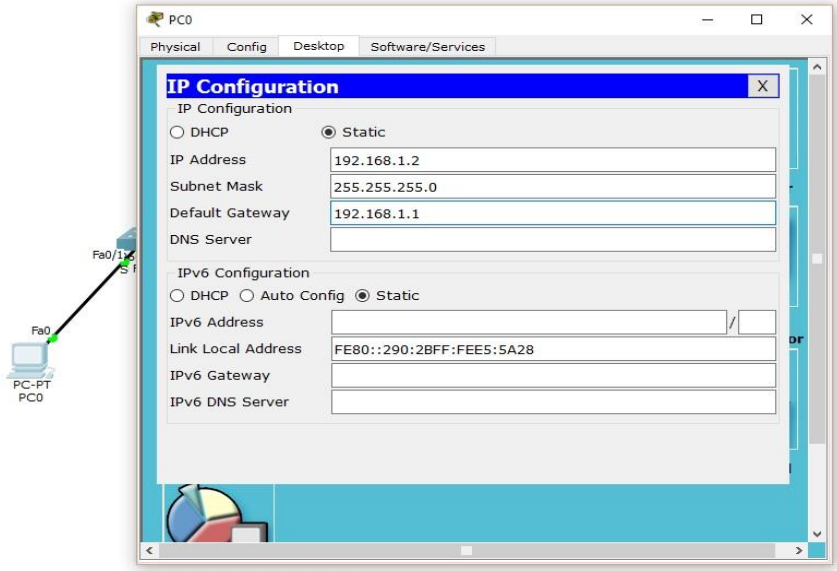
Continue with configuration dialog? [yes/no]: **n** *δίνουμε no*

Press RETURN to get started!

Router>
Router>**enable**
Router#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#**enable secret pass**
Router(config)#**line console 0**
Router(config-line)#**password pass**
Router(config-line)#**login**
Router(config-line)#**service password-encryption**
Router(config)#**hostname R1**
R1(config)#**banner motd *Authorised Access Only***
R1(config)#**interface fastethernet0/0** *μπαίνουμε στο interface fastethernet0/0*
R1(config-if)#**ip address 192.168.1.1 255.255.255.0** *δίνουμε ip και subnetmask*
R1(config-if)#**no shutdown** *Ενεργοποιούμε το interface*
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#**exit** *βγαίνουμε από το interface*
R1(config)#**interface fastethernet0/1** *μπαίνουμε στο interface fastethernet0/1*
R1(config-if)#**ip address 10.0.0.1 255.255.255.0** *δίνουμε ip και subnetmask*
R1(config-if)#**no shutdown** *Ενεργοποιούμε το interface*
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R1(config-if)#**exit** *βγαίνουμε από το interface*
R1(config)#**exit** *βγαίνουμε από το global configuration mode*
%SYS-5-CONFIG_I: Configured from console by console
R1#**copy running-config startup-config** *αποθηκεύουμε τις αλλαγές μας*

Destination filename [startup-config]?
Building configuration...
[OK]
R1#

Στη συνέχεια στους υπολογιστές δίνουμε IP ,subnetmask και default gateway που είναι η ip που δώσαμε στο αντίστοιχο interface (fa0/0 ή fa0/1). Προσοχή δίνουμε IP που είναι μέσα στο εύρος των διευθύνσεων μας βάσει της subnetmask εξαιρούμενης αυτής του interface που χρησιμοποιείται ως default gateway και σωστή subnetmask.



Αφού ολοκληρώσουμε αυτή τη διαδικασία ελέγχουμε τη συνδεσιμότητα κάνοντας ping μέσω του command prompt.

Packet Tracer PC Command Line 1.0
PC>**ping 10.0.0.3** *κάνουμε ping στη διεύθυνση 10.0.0.3*

Pinging 10.0.0.3 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.3: bytes=32 time=0ms TTL=127 *Παίρνουμε απάντηση άρα επικοινωνούν!*
Reply from 10.0.0.3: bytes=32 time=0ms TTL=127
Reply from 10.0.0.3: bytes=32 time=0ms TTL=127

Ping statistics for 10.0.0.3:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>

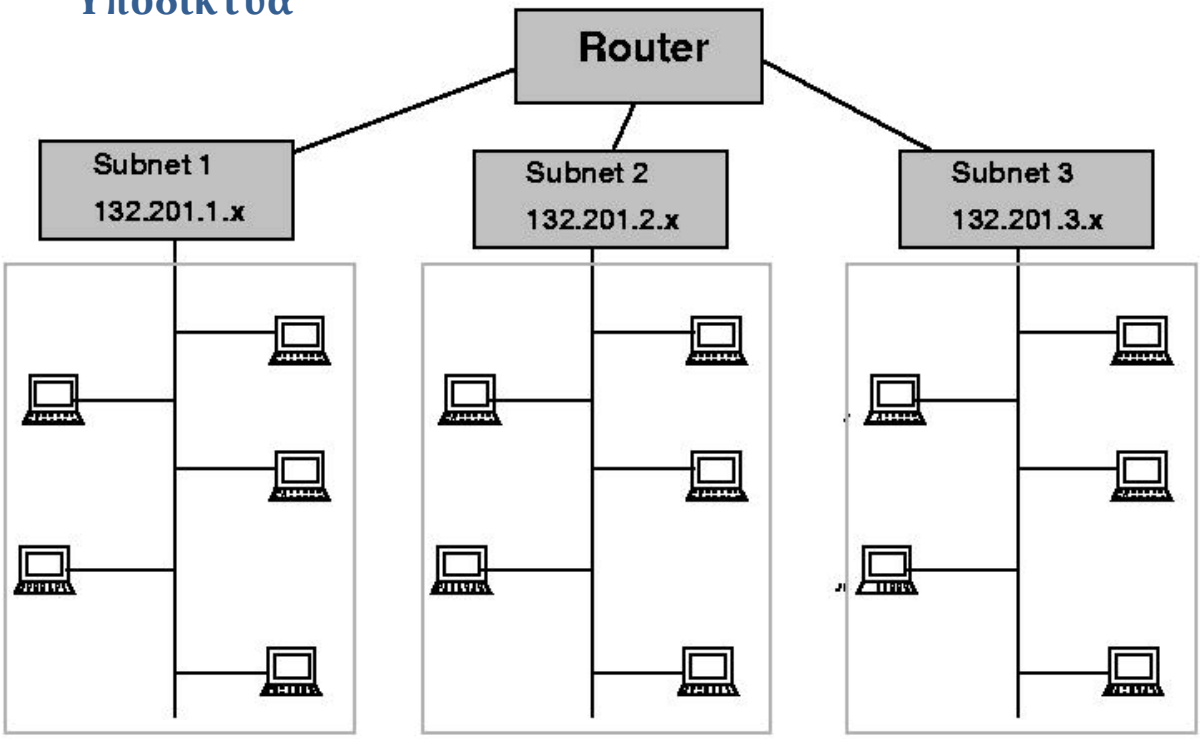
Ασκήσεις:

1. βρίσκουμε το εύρος διευθύνσεων με βάσει τη subnet mask (/8,/16,/24)
2. ξεχωρίζουμε πραγματικές και ψεύτικες διευθύνσεις
3. Υλοποιούμε στο packet tracer το παραπάνω δίκτυο και ελέγχουμε την επικοινωνία!

Κεφάλαιο 7ο

Subnetting

Υποδίκτυα



Ο σχεδιασμός ενός δικτύου έχουμε δει και στο πρώτο κεφάλαιο χρειάζεται να παίρνει υπόψη του πολλούς παράγοντες, ένας εκ των οποίων είναι και ο αριθμός των χρηστών που θα «σηκώσει». Το να γνωρίζουμε τις απαιτήσεις σε χρήστες στο δίκτυο που σχεδιάζουμε είναι κομβικό καθώς μας δίνει μία πρώτη εικόνα του φόρτου εργασίας του δικτύου αλλά και μας βάζει τις βάσεις ώστε να το ασφαλίσουμε από μη εξουσιοδοτημένους χρήστες.

Με βάση το προηγούμενο κεφάλαιο θα μπορούσαμε ανάλογα το μέγεθος του δικτύου που θέλουμε να σχεδιάσουμε να

διαλέξουμε ένα μπλοκ ψεύτικων διευθύνσεων από την ανάλογη κλάση (A,B,C). Αυτό όμως δεν επαρκεί ούτε για την ασφάλεια του δικτύου αλλά και ούτε είναι βοηθητικό στο να έχουμε τις απαραίτητες δυνατές διευθύνσεις ώστε να δώσουμε στους χρήστες. Το πιθανότερο είναι να αν διαλέξουμε πχ την κλάση A για ένα μεγάλο δίκτυο να μας δώσει χιλιάδες παραπάνω διευθύνσεις από όσες χρειαζόμαστε. Με αυτό τον τρόπο δεν μπορούμε να λύσουμε το σχεδιασμό ενός δικτύου μίας εταιρίας που θέλει να το χωρίσει σε υποδίκτυα ανάλογα με τα τμήματα της.

Η λύση σε αυτό το πρόβλημα είναι το «σπάσιμο» ενός δικτύου σε μικρότερα ανάλογα τους χρήστες με τη subnet mask. Τη subnet mask την είδαμε στο προηγούμενο κεφάλαιο και τη χρησιμοποιήσαμε για να καθορίσουμε το τμήμα δικτύου από το τμήμα των χρηστών σε μία IP. Ας δούμε ένα παράδειγμα χωρισμού δικτύου με βάση τους χρήστες.

Παράδειγμα

Έστω ότι μία εταιρία χρειάζεται να σχεδιάσει το δίκτυο της ώστε να καλύπτει τις ανάγκες δύο τμημάτων της που έχουν 120 το πρώτο και 200 χρήστες το δεύτερο. Με βάση το πλήθος των χρηστών θα ξεκινήσουμε το δίκτυο από το 192.168.1.0 (κλάση C).

Ξεκινάμε πάντα από το μεγαλύτερο σε πλήθος χρηστών δίκτυο. Οπότε θέλουμε να χωρίσουμε στο πρώτο υποδίκτυο για 200 χρήστες. Εδώ θα χρειαστεί να θυμηθούμε πάλι το πινακάκι με τις δυνάμεις του 2!

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Για να καλύψουμε 200 χρήστες θα χρειαστούμε τουλάχιστον 200 διευθύνσεις σε χρήστες που σημαίνει ότι θέλουμε να πάρουμε τόσα bit από τη subnet mask όσα θα μας δώσουν τουλάχιστον αυτό το πλήθος.

2^8 =256 άρα μας καλύπτουν 9 Bit από τη subnet mask.

(*Subnet mask 32 bit) 32-8= 24 δηλαδή 24 άσσους και 8 μηδενικά! Η subnetmask του δικτύου θα είναι /24!

11111111.11111111.11111111.00000000
255 . 255 . 255 . 0

Κάνουμε την πράξη and της subnet mask με την IP που έχουμε και παίρνουμε αποτέλεσμα τη διεύθυνση του 1ου υποδικτύου (βλ κεφ 5).

Για να βρούμε το τέλος του υποδικτύου μας κάνουμε (2^8/256)-1 = 0 (το 256 είναι το 2^8 , δηλαδή τα 8 τελευταία bit και με την πράξη αυτή βλέπουμε πόσα «256» παραπάνω χρειαζόμαστε για να καλύψουμε τους χρήστες). Οπότε οι χρήστες μας καλύπτονται όλοι έως την 192.168.1.0+255 άρα 192.168.1.255 (προσοχή προσθέτουμε 255 γιατί μετράμε και το 0)

Οπότε έχουμε :
Διεύθυνση LAN1: 192.168.1.0
Πρώτη δυνατή διεύθυνση χρήστη: 192.168.1.1
Τελευταία δυνατή διεύθυνση χρήστη: 192.168.1.254
Broadcast διεύθυνση υποδικτύου: 192.168.1.255

<u>Για το LAN2 με 120 χρήστες</u>

Ακολουθούμε την ίδια διαδικασία. Μας καλύπτει το 2^7=128 άρα θα έχουμε subnet mask /25!

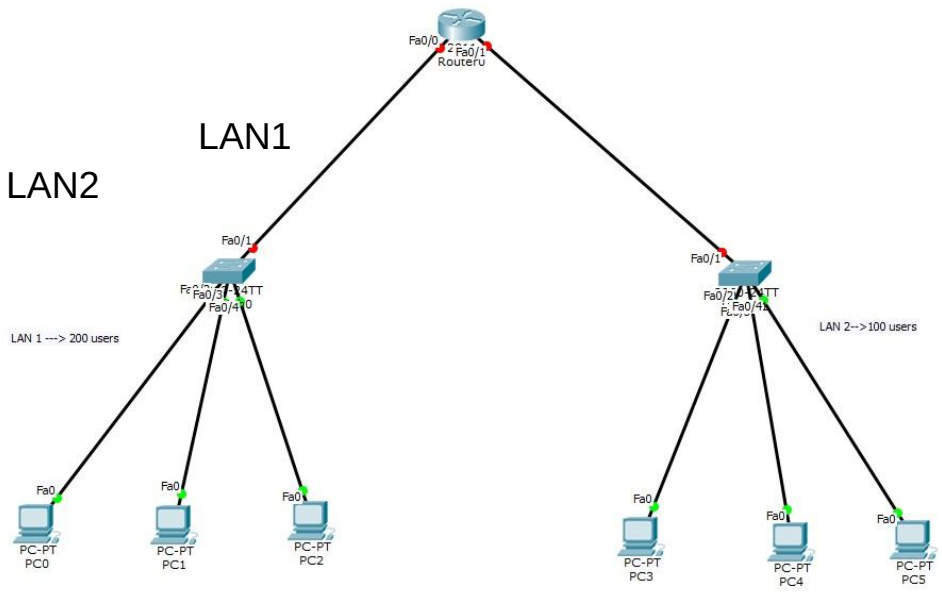
11111111.11111111.11111111.10000000
255 . 255 . 255 . 128

Συνεχίζουμε από την επόμενη διεύθυνση από την broadcast του LAN1 άρα από την 192.168.2.0 και κάνουμε την and πράξη. Από τη στιγμή που οι χρήστες μας είναι λιγότεροι από 256 δεν χρειάζεται να κάνουμε την πράξη. Πάμε κατευθείαν και λέμε 192.168.2.0+127 άρα 192.168.2.127

Οπότε έχουμε :
Διεύθυνση LAN2: 192.168.2.0
Πρώτη δυνατή διεύθυνση χρήστη: 192.168.2.1
Τελευταία δυνατή διεύθυνση χρήστη: 192.168.1.126
Broadcast διεύθυνση υποδικτύου: 192.168.1.127

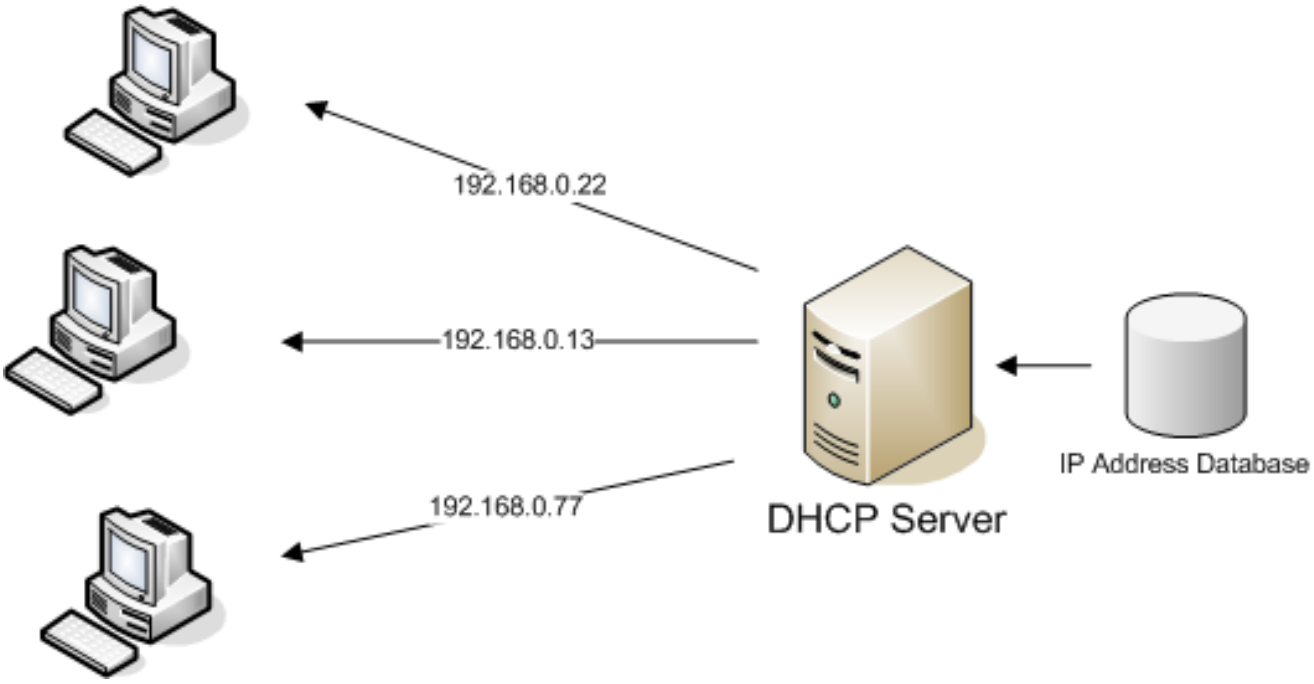
(* πάντα η διεύθυνση του υποδικτύου είναι ζυγός όπως και η τελευταία διεύθυνση χρήστη ενώ η πρώτη διεύθυνση χρήστη και η broadcast μονές!!!)

Άσκηση: Να σχεδιάσουμε το δίκτυο για μία εταιρία με 3000 χρήστες για το πρώτο τμήμα , 200 στο δεύτερο. Α) Από ποια κλάση θα διαλέξουμε ψεύτικες διευθύνσεις και γιατί; Β) Να βρεθούν οι διευθύνσεις των υποδικτύων LAN1 και LAN2 καθώς και οι πρώτες και τελευταίες δυνατές διευθύνσεις χρηστών αντίστοιχα. Να υλοποιηθεί το δίκτυο στο packet tracer



Κεφάλαιο 7ο

Dynamic Host Configuration Protocol



Τι είναι ένας DHCP server

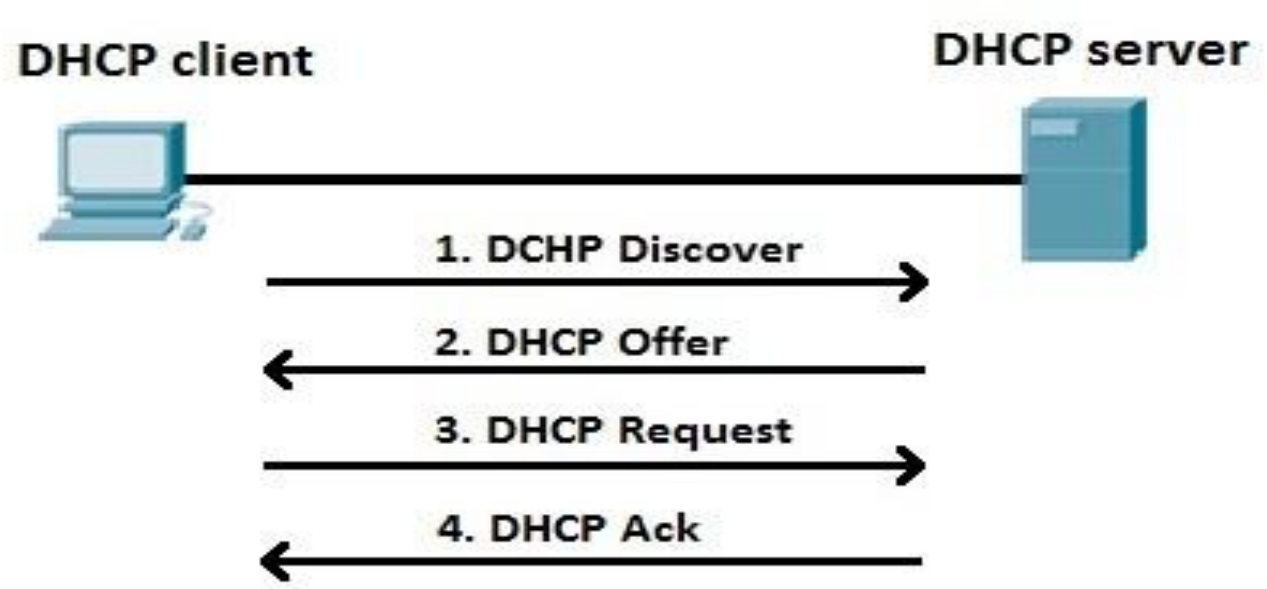
Κάθε συσκευή που συνδέεται στο δίκτυο χρειάζεται να καθορίζεται μονοσήμαντα από μία IP διεύθυνση μέσα σε αυτό. Για ένα δίκτυο με λίγες συσκευές μπορούμε να δώσουμε στατικά τις IP όπως έχουμε κάνει μέχρι τώρα. Τι γίνεται όμως αν έχουμε ένα δίκτυο με 200 συσκευές ή χρήστες που αλλάζουν συνεχώς (πχ σε ένα free wifi μιας καφετέριας); Καταλαβαίνουμε ότι χρειάζεται με κάποιο τρόπο να φτιάξουμε ένα server ο οποίος θα μοιράζει αυτόματα στους χρήστες IP μέσα από ένα προκαθορισμένο με βάση το δίκτυο μας μπλοκ διευθύνσεων.

Τη δουλειά αυτή κάνει ένας DHCP server. Όπως υποδηλώνουν και τα αρχικά ο DHCP server τρέχει ένα πρωτόκολλο που είναι υπεύθυνο ώστε να κάνει δυναμικά το «σεταρισμα» των διευθύνσεων, της subnet mask, και της default gateway σε όλες τις συσκευές που συνδέονται στο δίκτυο που έχει στην ευθύνη του. Σε μικρότερα δίκτυα το ρόλο του DHCP server μπορεί να παίξει το router. Χρειάζεται όμως από εμάς να του καθορίσουμε με ακρίβεια ποιο είναι το μπλοκ αυτό των διευθύνσεων που μπορεί να χρησιμοποιήσει.

Πως λειτουργεί;

Όταν μία συσκευή επικοινωνεί με έναν DHCP, ο server εκχωρεί μια διεύθυνση IPv4 σε αυτό τον πελάτη. Η συσκευή συνδέεται στο δίκτυο με αυτή την διεύθυνση IP, μέχρι να λήξει η μίσθωση.

Όταν μία συσκευή θέλει να συνδεθεί σε ένα δίκτυο αρχίζει μια διαδικασία τεσσάρων βημάτων για να αποκτήσει μια IP. Η συσκευή ξεκινά τη διαδικασία με ένα μήνυμα DHCPDISCOVER ώστε να ανακαλύψει διαθέσιμους DHCP servers.



DHCP Discover (DHCPDISCOVER)

Το μήνυμα DHCPDISCOVER βρίσκει DHCP servers του δικτύου. Επειδή ο χρήστης δεν έχει έγκυρη IP στην αρχή, χρησιμοποιεί τις MAC address διευθύνσεις για να επικοινωνήσει με το DHCP server.

Προσφορά DHCP (DHCPOFFER)

Όταν DHCP server λαμβάνει ένα μήνυμα DHCPDISCOVER, διατηρεί μια διαθέσιμη διεύθυνση IPv4 ώστε να διαθέσει στον χρήστη. Ο DHCP server δημιουργεί επίσης μια καταχώριση που αποτελείται από τη διεύθυνση MAC του αιτούντος χρήστη και της IP διεύθυνσης του χρήστη. Ο DHCP server στέλνει ένα μήνυμα DHCPOFFER στον χρήστη. Το μήνυμα DHCPOFFER αποστέλλεται, χρησιμοποιώντας τη διεύθυνση MAC Layer 2 του DHCP server ως διεύθυνση πηγής και τη διεύθυνση MAC Layer 2 του χρήστη ως προορισμό.

Αίτηση DHCP (DHCPREQUEST)

Όταν ο χρήστη λαμβάνει το DHCPOFFER από τον DHCP server, στέλνει πίσω ένα μήνυμα DHCPREQUEST.

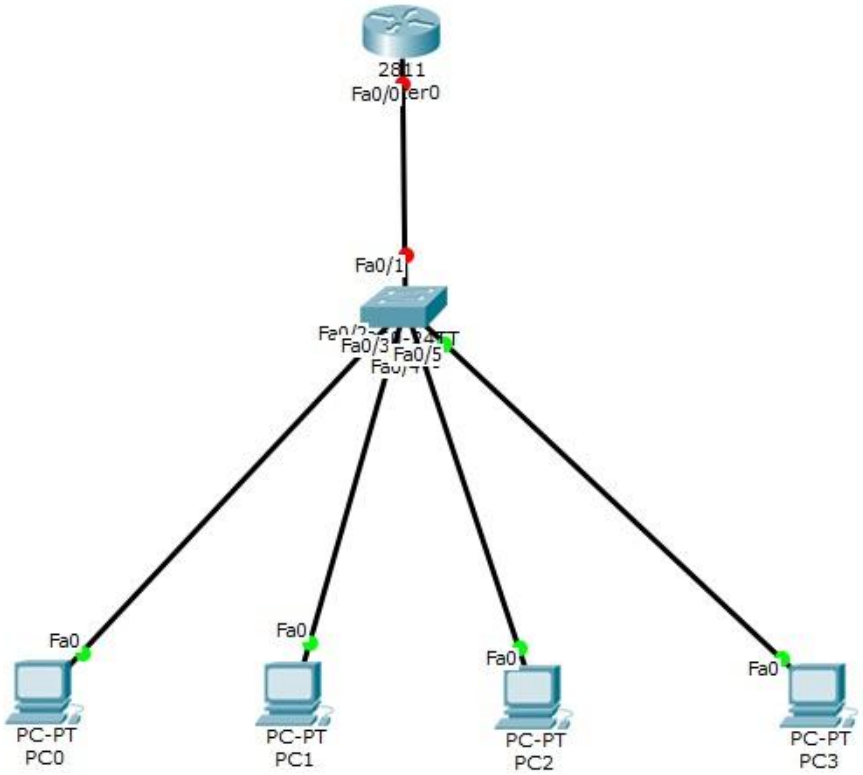
DHCP Acknowledgment(DHCPACK)

Κατά τη λήψη ενός DHCPREQUEST μήνυμα, ο DHCP server ελέγχει αν χρησιμοποιείται αυτή η IP, και απαντά με ένα μήνυμα DHCPACK . Το μήνυμα DHCPACK είναι ένα αντίγραφο του DHCPOFFER, Όταν ο χρήστης λαμβάνει το μήνυμα DHCPACK,

ελέγχει με τη σειρά του αν χρησιμοποιείται η διεύθυνση και αν δεν ισχύει αρχίζει να την χρησιμοποιεί σαν δικιά του.

Στήνοντας ένα DHCP σε ένα δίκτυο (Packet tracer)

Στη μακέτα του packet tracer βάζουμε 4 υπολογιστές, 1 switch 2960 και 1 router 2811. Συνδέουμε τους 4 υπολογιστές με το switch και το switch με το router χρησιμοποιώντας τα αντίστοιχα (σωστά) καλώδια, όπως φαίνεται στην εικόνα.



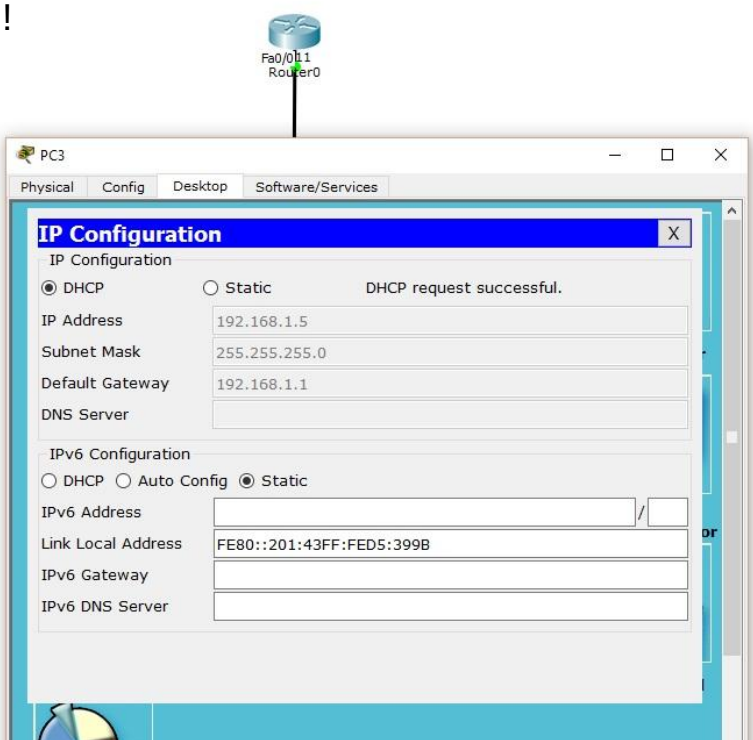
Ξεκινάμε υλοποιώντας το basic configuration switch-router. Θα χρησιμοποιήσουμε την 192.168.1.0 /24 διεύθυνση δικτύου.

Πως στήνουμε στο router μας το dhcp.

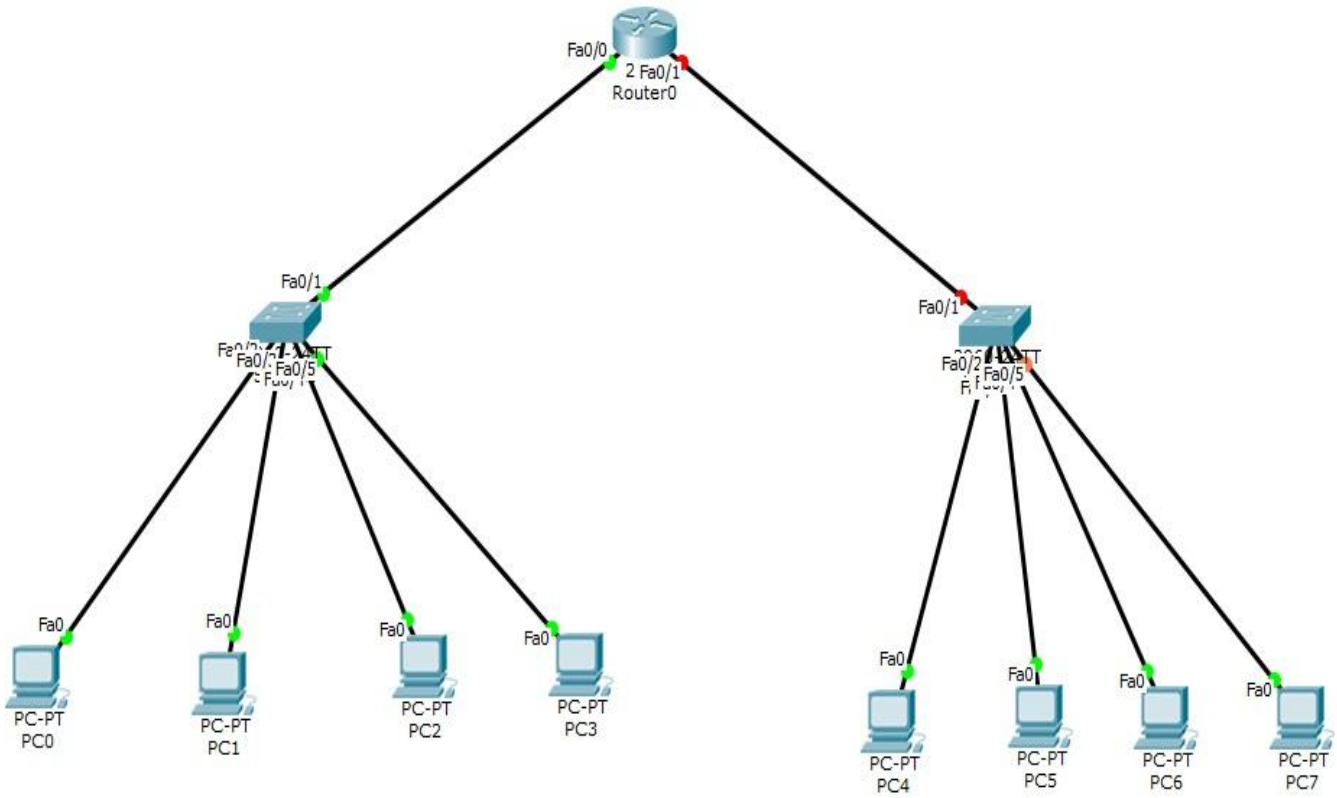
Στο global configuration mode του router

Router(config)#**interface fa0/0** μπαίνουμε στο interface που έχει συνδεθεί το switch
Router(config-if)#**ip address 192.168.1.1 255.255.255.0** δίνουμε ip(default-gateway) και subnet mask
Router(config-if)#**no shut**
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#
Router(config-if)#**exit** βγαίνουμε από το interface
Router(config)#**ip dhcp excluded-address 192.168.1.1** δηλώνουμε ποιες διευθύνσεις δεν μπορεί να δώσει
Router(config)#**ip dhcp pool LAN1-Pool** Δηλώνουμε το όνομα της «πισίνας» από την οποία θα παίρνει IP
Router(dhcp-config)#**network 192.168.1.0 255.255.255.0** δηλώνουμε το δίκτυο και τη subnet mask
Router(dhcp-config)#**default-router 192.168.1.1** δηλώνουμε την default διαδρομή
Router(dhcp-config)#**end** βγαίνουμε από το dhcp-config και από το global configuration mode
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#**copy running-config startup-config** αποθηκεύουμε τις αλλαγές
Destination filename [startup-config]?
Building configuration...
[OK]
Router#

Πηγαίνουμε στους υπολογιστές, στο IP configuration και επιλέγουμε DHCP. Οι υπολογιστές παίρνουν αυτόματα διευθύνσεις IP!

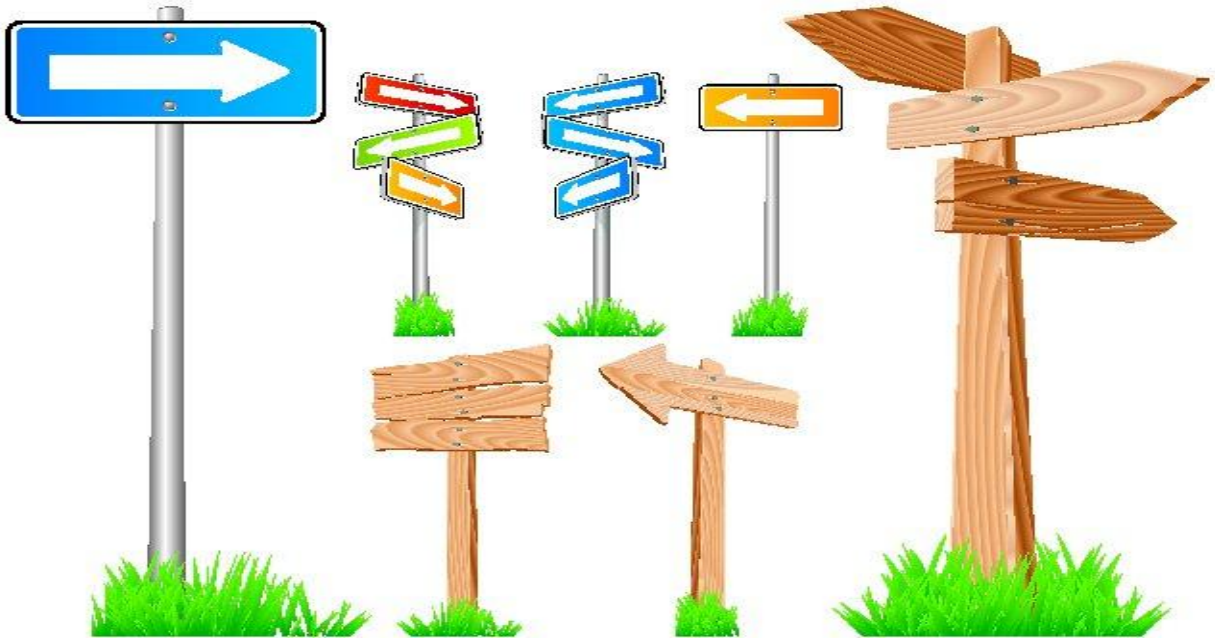


Άσκηση: Να υλοποιήσουμε ένα δίκτυο όπως φαίνεται στην εικόνα παρακάτω. Το LAN1 έχει διεύθυνση δικτύου 192.168.1.0 και το LAN2 έχει 192.168.2.0. Να υλοποιηθεί dhcp στο router ώστε να παίρνουν διευθύνσεις και στα δύο υποδίκτυα. (Προσοχή στην default διαδρομή που θα αντιστοιχήσουμε σε κάθε pool!)



Κεφάλαιο 8ο

Δρομολόγηση πακέτων και πρωτόκολλα



Στατική δρομολόγηση

Η δρομολόγηση βρίσκεται στον πυρήνα του κάθε δικτύου δεδομένων. Για να φτάσει ένα πακέτο από την συσκευή της πηγής ως την συσκευή του προορισμού περνάει μέσα από διάφορα δίκτυα και routers. Τα routers είναι οι υπεύθυνες συσκευές για την δρομολόγηση των πακέτων δεδομένων. Για να γνωρίζει το router που θα πρέπει να στείλει το πακέτο (προς ποια κατεύθυνση) χρειάζεται να ξέρει τα συνδεδεμένα πάνω του δίκτυα. Αυτό καλύπτεται από το **routing table** , ένα πίνακα που διατηρεί το κάθε router.

Για τα πακέτα που δεν γνωρίζει το router προς τα που πρέπει να τα στείλει φτιάχνουμε μία default στατική διαδρομή (**default static route**). Μέσα από αυτή στέλνεται σε ένα άλλο

router που πιθανά να γνωρίζει τον προορισμό. Συνήθως οι ISP οργανώνουν το δίκτυο σε δομή πυραμίδας ώστε όταν τα κατώτερα στρώματα δεν γνωρίζουν τον προορισμό του πακέτου, να στέλνεται μέσω της στατικής διαδρομής στο ανώτερο στρώμα μέχρι να βρεθεί το router που γνωρίζει τον προορισμό.

Εντολή για την default static route: **ip route 0.0.0.0 0.0.0.0 *{exit-interface}***

```
Router>enable
Router#configure terminal
Router(config)#ip route 0.0.0.0 0.0.0.0 se0/0/0
```

Μπορούμε να δώσουμε επίσης στατική διαδρομή για ένα συγκεκριμένο δίκτυο δίνοντας την διεύθυνση του δικτύου, την subnetmask καθώς και το exit interface.

Εντολή για την static route: **ip route 192.168.1.0 255.255.255.0 *{exit-interface}***

```
Router>enable
Router#configure terminal
Router(config)#ip route 192.168.1.0 255.255.255.0 se0/0/0
```

Δυναμική δρομολόγηση

Σε μεγάλα δίκτυα καταλαβαίνουμε ότι η στατική δρομολόγηση δεν βοηθά, μπορεί να οδηγήσει σε λάθη. Για το λόγο αυτό υπάρχουν πρωτόκολλα που αυτοματοποιούν τη διαδικασία ανταλλαγής routing πληροφοριών μεταξύ των κόμβων. Τα πρωτόκολλα δρομολόγησης ανάλογα με τον αλγόριθμο που χρησιμοποιούν διαλέγουν και το καλύτερο μονοπάτι για την δρομολόγηση. Υπάρχουν διάφορα πρωτόκολλα δρομολόγησης με τα πλεονεκτήματα και τα μειονεκτήματα τους όπως το rip, ospf, eigrp, bgp κλπ. Εμείς θα δούμε πως στήνουμε το OSPF πρωτόκολλο.

OSPF

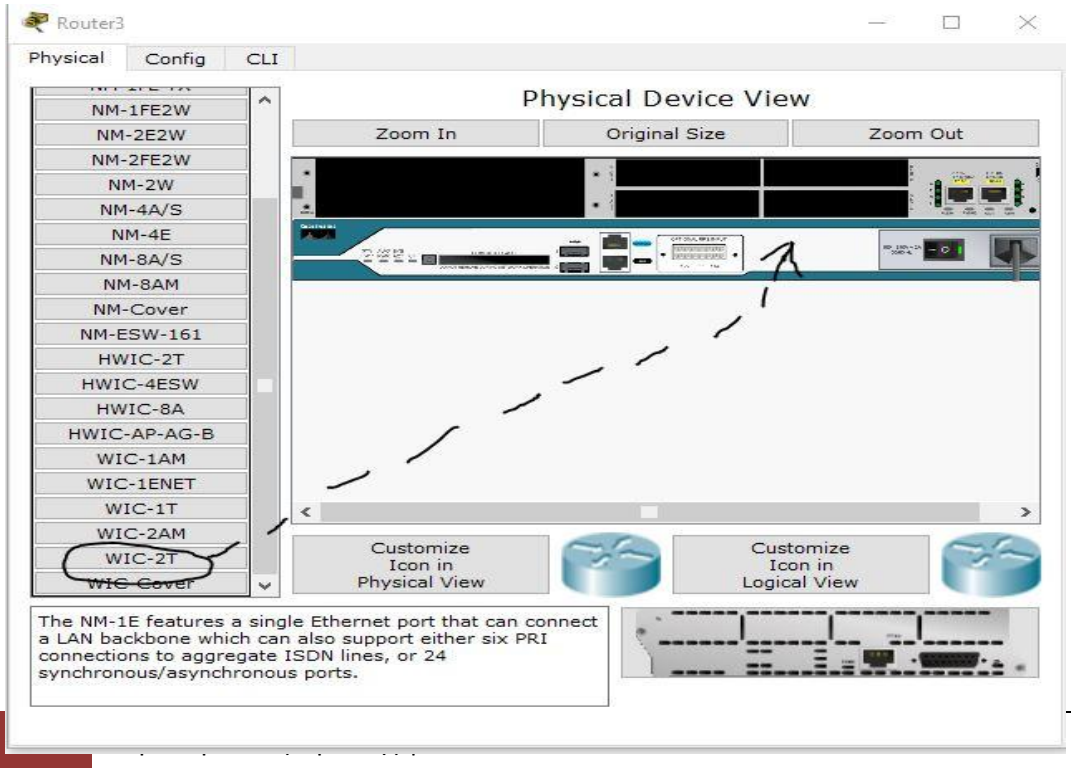
Τα χαρακτηριστικά του OSPF:

- Δεν παίρνει υπόψη του τις κλάσεις των IP διευθύνσεων πράγμα που επιτρέπει τον υπολογισμό των δικτύων με βάση τη subnetmask.
- Χρησιμοποιεί τον αλγόριθμο SPF για την επιλογή του καλύτερου μονοπατιού
- Υποστηρίζει κρυπτογράφηση MD5 πράγμα που το κάνει πολύ ασφαλές.

Σε ένα δίκτυο που χρησιμοποιεί OSPF πρωτόκολλο χρειάζεται να ορίσουμε ένα router ως τον designated αυτόν που ορίζει δηλαδή το δίκτυο (από εδώ και πέρα θα αναφερόμαστε σε αυτό το router ως DR). Αυτό μπορούμε να το πετύχουμε με πολλούς τρόπους ένας εκ των οποίων είναι να δώσουμε χαμηλότερο router-id σε αυτόν που θέλουμε. Θα το δούμε παρακάτω στο configuration OSPF.

Configuration OSPF – σύνδεση router με router

Για να συνδέσουμε 2 και παραπάνω router μεταξύ τους χρειαζόμαστε να βάλουμε ένα module στο router που να υποστηρίζει το σειριακό καλώδιο. Ακριβώς όπως και στην πραγματικότητα χρειάζεται να κλείσουμε το router πριν βάλουμε το κατάλληλο module. Στις εικόνες που ακολουθούν φαίνεται πως θα το κάνουμε.



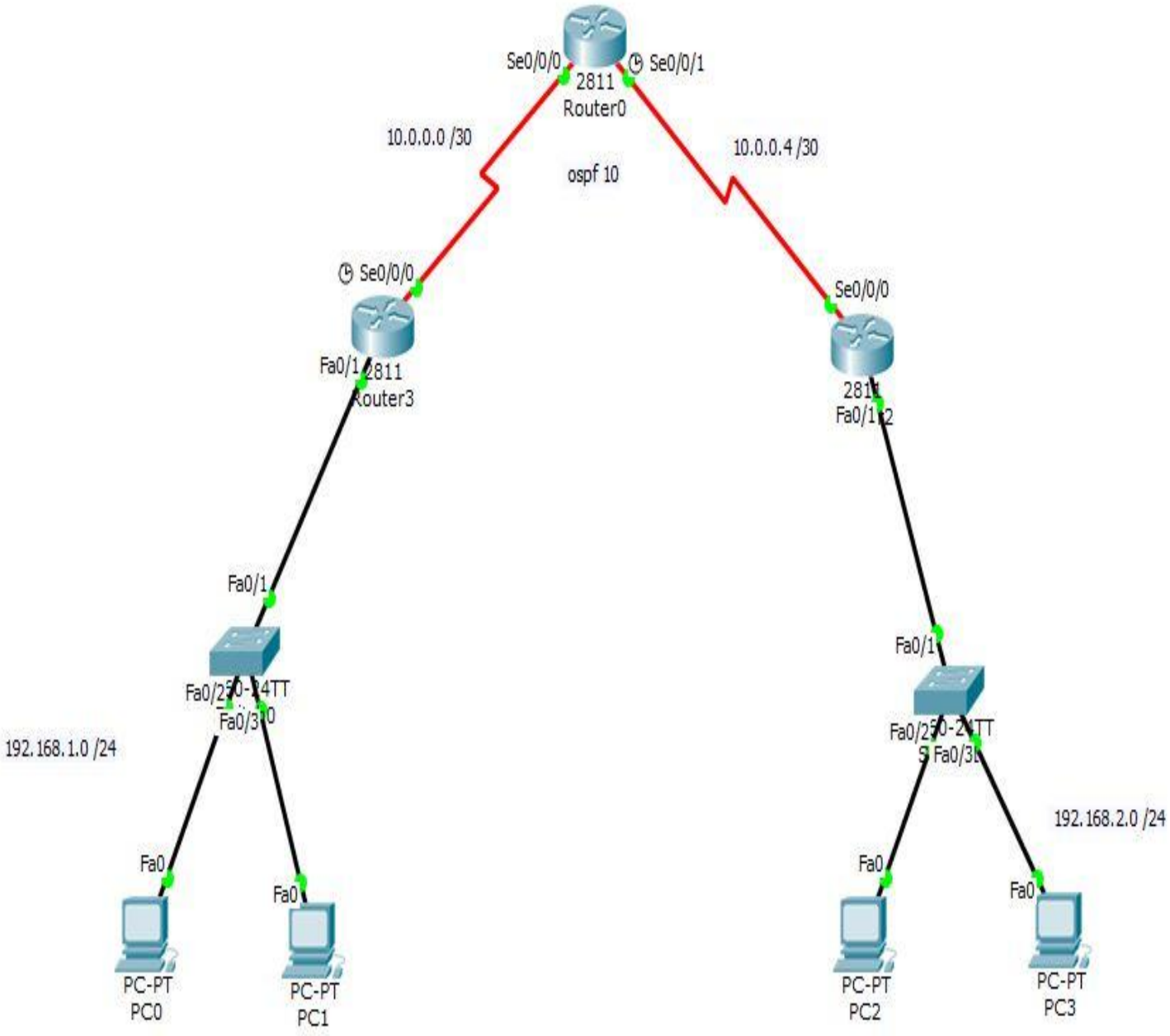
Configure OSPF

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#router ospf 10
Router(config-router)#router-id 1.1.1.1
Router(config-router)#network 10.0.0.0 0.0.0.3 area 0
Router(config-router)#network 10.0.0.4 0.0.0.3 area 0
Router(config-router)#end
```

Με την εντολή **network *{network-address} {wildcard}{area}*** γνωρίζουμε στο router μας τα απευθείας συνδεδεμένα πάνω του δίκτυα. Η wildcard όπως και η subnet καθορίζει το δίκτυο μας. Η σχέση τους είναι η εξής: αν έχουμε subnet mask 255.255.255.252 τότε η wildcard είναι 0.0.0.3.

Την ίδια διαδικασία χρειάζεται να ακολουθήσουμε σε όλα τα router που έχουμε συνδεδεμένα γνωστοποιώντας τους τα απευθείας πάνω τους συνδεδεμένα δίκτυα!

Άσκηση: Να στηθεί το δίκτυο της εικόνας. Ανάμεσα στα router να χρησιμοποιηθούν τα δίκτυα 10.0.0.0 /30 και το 10.0.0.4 /30 ενώ για τα άλλα το 192.168.1.0 /24 και το 192.168.2.0 /24. Θεωρήστε ότι όλα τα δίκτυα ανήκουν στην περιοχή 0 του ospf 10. Να υλοποιηθεί ospf 10 σε όλα τα router! Να ελεγχθεί η επικοινωνία μεταξύ των δύο δικτύων κάνοντας ping από τον ένα υπολογιστή στον άλλο, να δούμε τη διαδρομή του πακέτου με την εντολή tracert!



Κεφάλαιο 9ο

Network Address Translation (NAT)

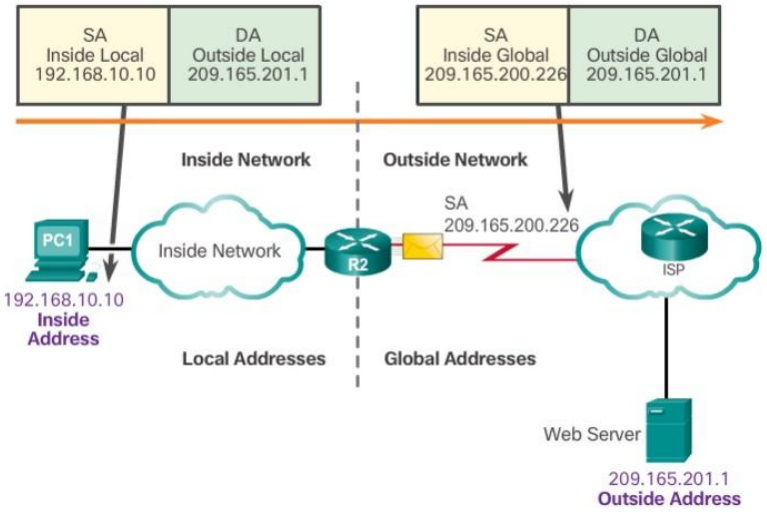
Εισαγωγή στο NAT

Στο κεφάλαιο 5, ήρθαμε αντιμέτωποι με το πρόβλημα έλλειψης IP διευθύνσεων, και το απαντήσαμε έστω προσωρινά με τις ψεύτικες διευθύνσεις που υπάρχουν μονοσήμαντα μέσα στο δικό μας μόνο δίκτυο. Τι γίνεται όμως όταν θέλουμε να βγούμε στο internet; Πως παίρνουμε πραγματική διεύθυνση για να επικοινωνήσουμε με μία συσκευή εκτός του δικού μας δικτύου;

Τη δουλειά αυτή κάνει το NAT. Το NAT αναθέτει δημόσια IP στη συσκευή μας μόνο για την περίπτωση που θέλουμε να επικοινωνήσουμε έξω από το δίκτυο μας. Ταυτόχρονα μας προστατεύει καθώς κρύβει την εσωτερική-ψεύτικη διεύθυνση μας από τα έξω δίκτυα. Συνήθως έχουμε αναθέσει στο NAT μία πισίνα από δημόσιες IP ώστε να μοιράζει με βάση τις ανάγκες στο δίκτυο. Τις δημόσιες διευθύνσεις μας δίνει ο ISP.

Το NAT περιλαμβάνει 4 τύπους διευθύνσεων

1. Εξωτερική δημόσια (Outside global)
2. Εσωτερική δημόσια (Inside global)
3. Εξωτερική τοπική (Outside local)
4. Εσωτερική τοπική (Inside local)



Τύποι του NAT

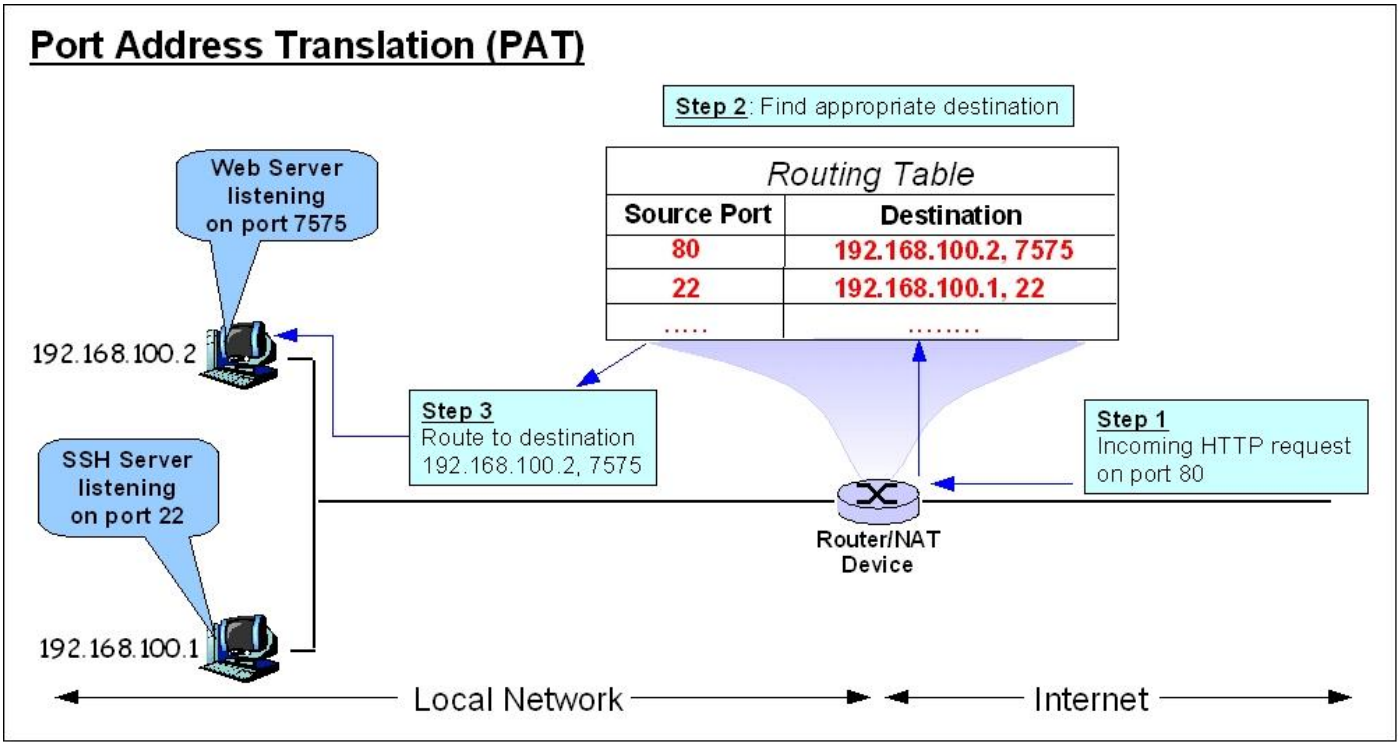
Υπάρχουν τρεις τύποι για το NAT:

1. Το στατικό NAT που αντιστοιχεί μία ιδιωτική με μία δημόσια διεύθυνση με σχέση 1 προς 1
2. Το δυναμικό NAT που λειτουργεί με σχέση πολλές προς πολλές
3. Και το Port Address Translation (PAT) που λειτουργεί με τη σχέση πολλές ιδιωτικές προς μία δημόσια. Με αυτό τον τρόπο λειτουργεί NAT στο σπίτι μας.

Port Address Translation (PAT)

Με τη χρήση του PAT πολλές ιδιωτικές διευθύνσεις μεταφράζονται σε μία δημόσια ώστε να βγει στο Internet. Η διαδικασία που ακολουθείται έχει να κάνει με το ποια θύρα της συσκευής μας χρησιμοποιείται για την επικοινωνία. Πχ αν θέλουμε να ξεκινήσουμε μία http σύνδεση ο υπολογιστής μας θα χρησιμοποιήσει την θύρα 80. Το NAT που βρίσκεται στο router μας παίρνει το πακέτο με θύρα πηγής την 80 και μία ιδιωτική διεύθυνση και το στέλνει με την δημόσια διεύθυνση συσχετισμένο στον πίνακα του με την θύρα πηγής. Έτσι όταν λάβει απάντηση θα ξέρει που να προωθήσει το πακέτο.

Μία αντίστοιχη λειτουργία εκτελείται στον ίδιο τον υπολογιστή μας ώστε να ξεχωρίζει το κάθε πακέτο αν πρόκειται για http, ftp κλπ . Αν και ένας δεύτερος χρήστης θέλει την ακριβώς επόμενη στιγμή να ξεκινήσει μία http σύνδεση θα έχει και αυτός θύρα πηγής την 80. Το NAT/PAT θα συσχετίσει όμως την ιδιωτική του διεύθυνση με την αμέσως επόμενη θύρα, την 81, ώστε να τον ξεχωρίσει από τον πρώτο χρήστη



Στήνοντας το NAT στο δίκτυο μας (Packet Tracer)

Το NAT στήνεται πάντα στην άκρη του δικτύου μας, εκεί που η περαιτέρω επικοινωνία ξεπερνάει τα όρια του δικτύου μας και χρειάζεται δημόσιες IP.

Static NAT configuration on router

Router(config)#**ip nat inside source static** 192.168.1.3 209.165.201.5
Router(config)#interface fa0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#**ip nat inside**
Router(config-if)#no shutdown

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

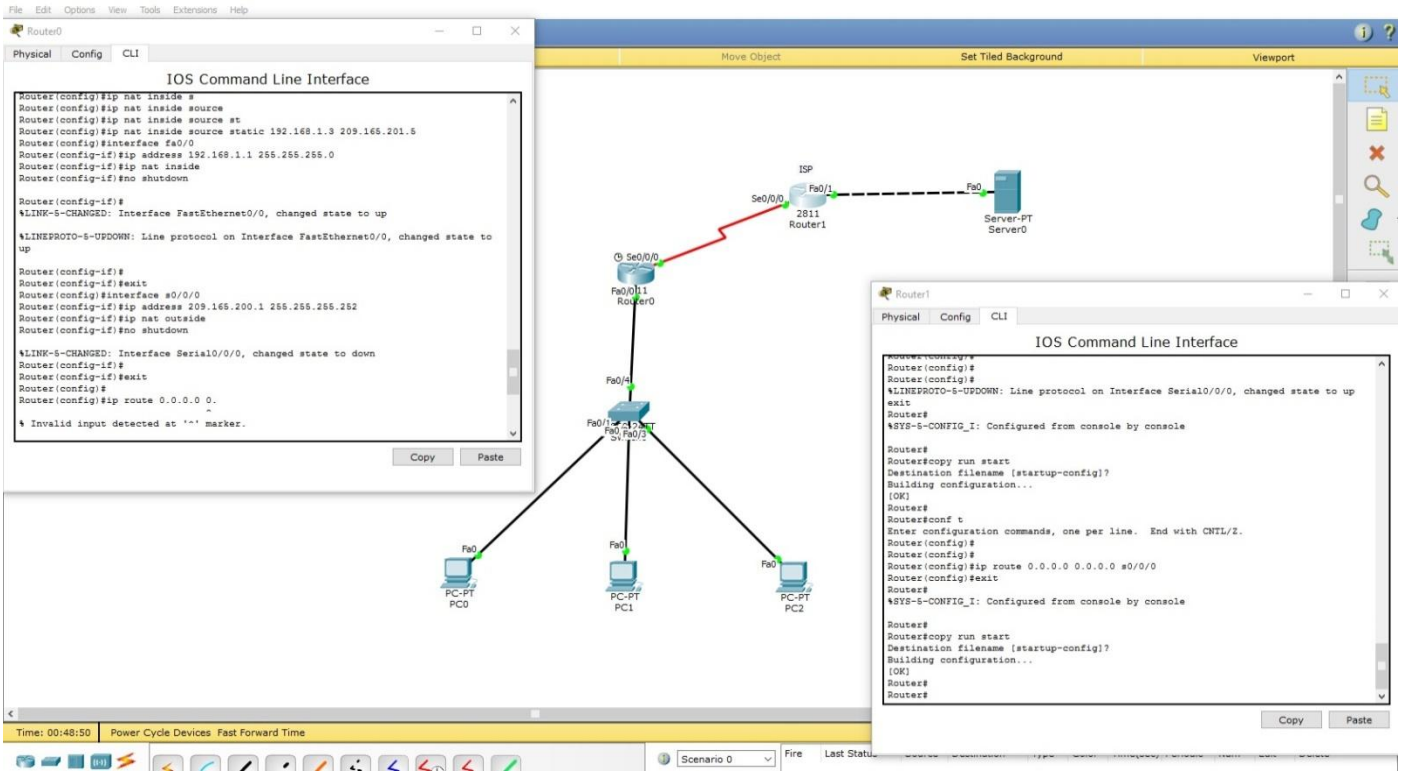
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#interface s0/0/0
Router(config-if)#ip address 209.165.200.1 255.255.255.252
Router(config-if)#**ip nat outside**

Router(config-if)#no shutdown

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

Οι εντολές *ip nat inside* και *ip nat outside* δίνονται αντίστοιχα στο εσωτερικό και εξωτερικό interface του router του δικτύου μας. Σημείωση: Χρειάζεται να δώσουμε default route τόσο στο router μας όσο και στον ISP (***ip route 0.0.0.0 0.0.0.0 se0/0/0***)



dynamic NAT configuration on router

Router(config)#**ip nat pool** NAT-POOL 209.165.200.226 209.165.200.240 netmask 255.255.255.224
Router(config)#**access-list 1 permit** 192.168.1.0 0.0.0.255
Router(config)#**ip nat inside source list 1 pool** NAT-POOL
Router(config)#interface fa0/0
Router(config-if)#**ip nat inside**
Router(config-if)#exit
Router(config)#interface se0/0/0
Router(config-if)#**ip nat outside**
Router(config-if)#exit
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console

Router#copy run start
Destination filename [startup-config]?
Building configuration...

Με την εντολή *ip nat pool* NAT-POOL(το όνομα της πισίνας) δίνουμε το ευρος και την μάσκα των διευθύνσεων που μπορεί να μεταφράσει τις ιδιωτικές. Με την εντολή *access-list 1permit* δημιουργούμε μία access-list με την οποία επιτρέπουμε σε ένα συγκεκριμένο εύρος ιδιωτικών διευθύνσεων να «περνάνε» και με την αμέσως επόμενη εντολή, *ip nat inside source list 1 pool NAT-POOL* αντιστοιχούμε την access-list με την πισίνα του NAT. Η διαδικασία στα interface είναι ίδια όπως και στο static NAT.

Port Address Translation configuration on router

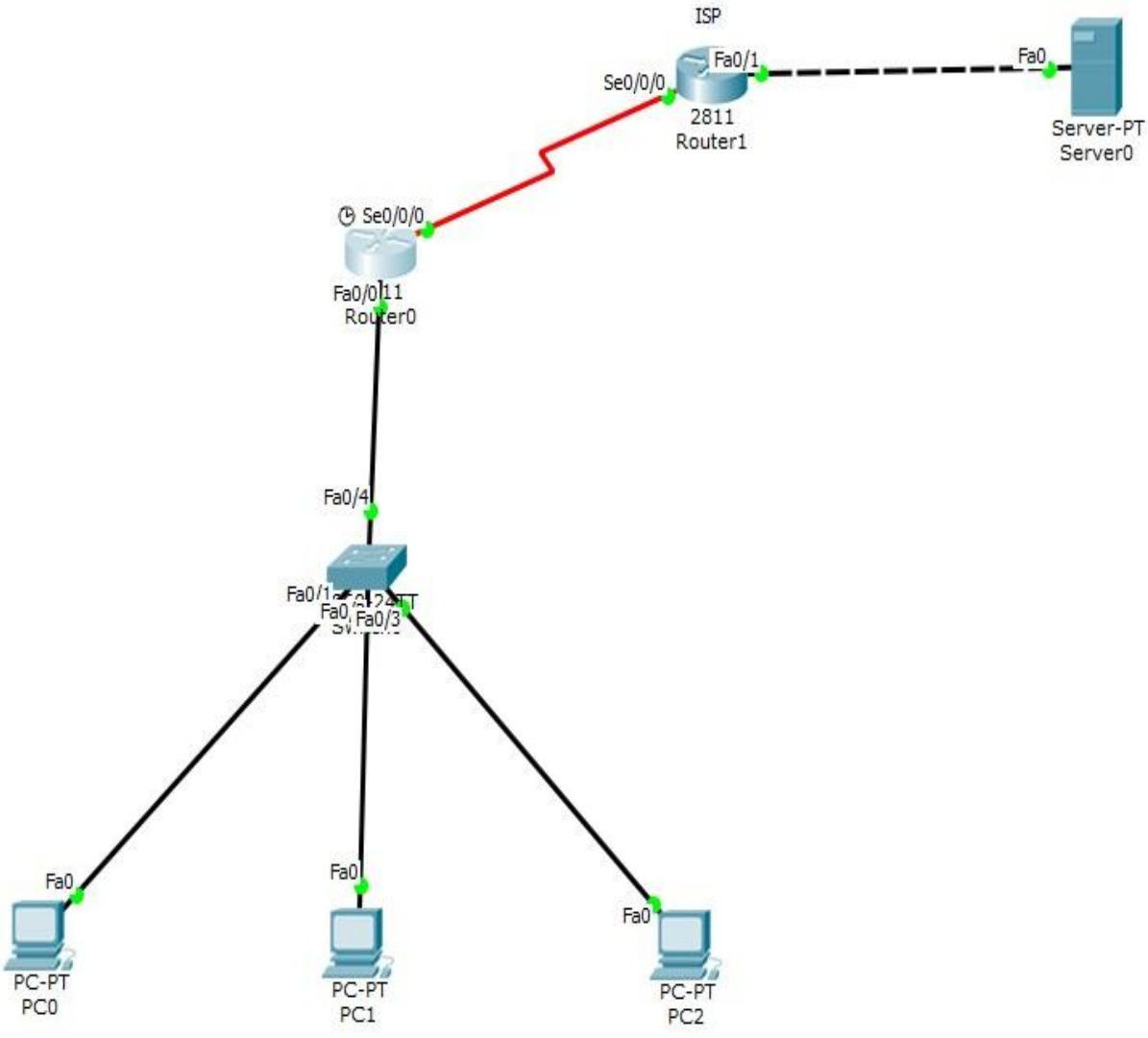
Router(config)#**ip nat pool** NAT-POOL 209.165.200.226 209.165.200.240 netmask 255.255.255.224
Router(config)#**access-list 1 permit** 192.168.1.0 0.0.0.255
Router(config)#**ip nat inside source list 1 pool** NAT-POOL **overload**
Router(config)#interface fa0/0
Router(config-if)#**ip nat inside**
Router(config-if)#exit
Router(config)#interface se0/0/0
Router(config-if)#**ip nat outside**
Router(config-if)#exit
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#copy run start
Destination filename [startup-config]?
Building configuration...

Η μόνη διαφορά με το dynamic NAT είναι η προσθήκη του OVERLOAD στο τέλος της εντολής *ip nat inside source list 1 pool NAT-POOL* ***overload.***

Άσκηση: Στήνουμε το δίκτυο της εικόνας χρησιμοποιώντας ένα server στον οποίο δίνουμε πραγματική διεύθυνση 200.200.200.200 . Στήνουμε PAT στο router που βρίσκεται στην άκρη του δικτύου μας (192.168.1.0) . Ελέγχουμε την επικοινωνία των υπολογιστών με τον server κάνοντας ping και tracert στη διεύθυνση 200.200.200.200

Μεταξύ των 2 router χρησιμοποιούμε το υποδίκτυο 209.165.200.0 με subnetmask 255.255.255.252.(δες static nat) Και στα 2 router δίνουμε default route με την εντολή **ip route 0.0.0.0 0.0.0.0 *[exit-interface]***

Σημείωση: Προσοχή στα καλώδια που χρησιμοποιούμε για τη σύνδεση των 2 router αλλά και την απευθείας σύνδεση του router με τον server



Κεφάλαιο 10ο

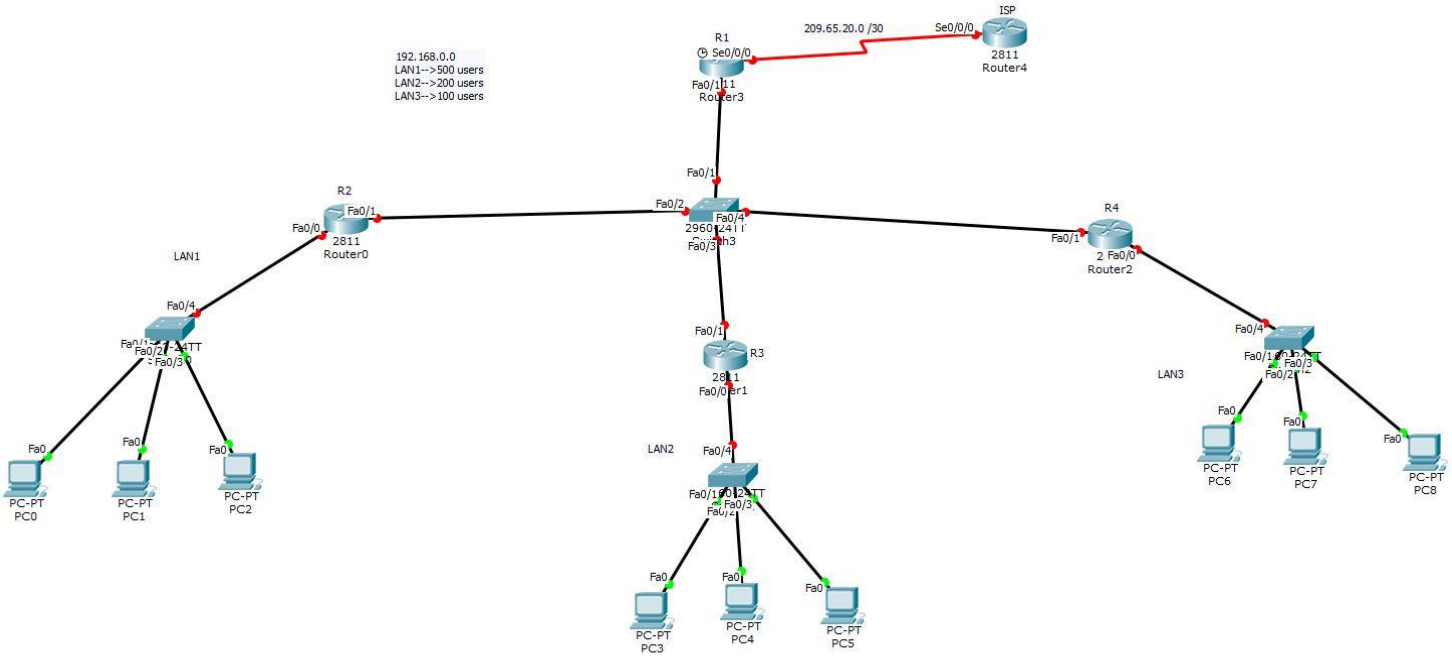
Τελικό Project

Ζητείται να σχεδιαστεί και να υλοποιηθεί το δίκτυο υπολογιστών μίας εταιρίας. Η εταιρία στεγάζεται σε τριώροφο κτήριο που στον κάθε όροφο στεγάζεται διαφορετικό τμήμα που χρειάζεται το δικό του δίκτυο. Να υλοποιηθεί το σχήμα της εικόνας.

Οι ανάγκες του LAN1 είναι για 500 χρήστες, του LAN2 για 220 χρήστες και του LAN3 για 100 χρήστες. Έχουμε τη διεύθυνση δικτύου 192.168.0.0. Να γίνει subnetting για τα 3 δίκτυα αλλά και για το δίκτυο μεταξύ των router.

Να υλοποιηθεί basic configuration σε όλα τα switch και routers.

Ο R1 να υλοποιεί DHCP για όλα τα δίκτυα. Επίσης να υλοποιηθεί NAT-PAT. Ο ISP συνδέεται με τον R1 με μεταξύ τους δίκτυο το 209.65.20.0 . Η δημόσια διεύθυνση που θα δίνει το NAT είναι η 65.32.10.124



Κεφάλαιο 3ο

Easygenerator

Για την δημιουργία του δικού μας εκπαιδευτικού υλικού θα χρησιμοποιήσουμε την πλατφόρμα Easygenerator. Η πλατφόρμα αυτή μας δίνει τη δυνατότητα της flipped διδασκαλίας όπως απαιτείται από το δικό μας στόχο.

Μας δίνει επίσης τη δυνατότητα να εξάγουμε το υλικό μας σε μορφή HTML5 , flash, SCORM , αλλά ακόμα και να χρησιμοποιήσουμε την cloud υπηρεσία ώστε να παραδώσουμε το υλικό στους εκπαιδευόμενους. Αυτό καθιστά το Easygenarator ιδιαίτερα βολικό καθώς είναι συμβατό με πολλά συστήματα διαχείρισης μαθημάτων.

Ακόμα μας δίνει αρκετές επιλογές στην παρουσίαση του εκπαιδευτικού μας υλικού. Μπορούμε να χρησιμοποιήσουμε πολυμεσικό υλικό όπως βίντεο, ηχογραφήσεις, εικόνες. Μπορούμε ακόμα να χρησιμοποιήσουμε βίντεο από το Youtube , το Vimeo και το SoundCloud και να τα ενσωματώσουμε στο υλικό του μαθήματος μας.

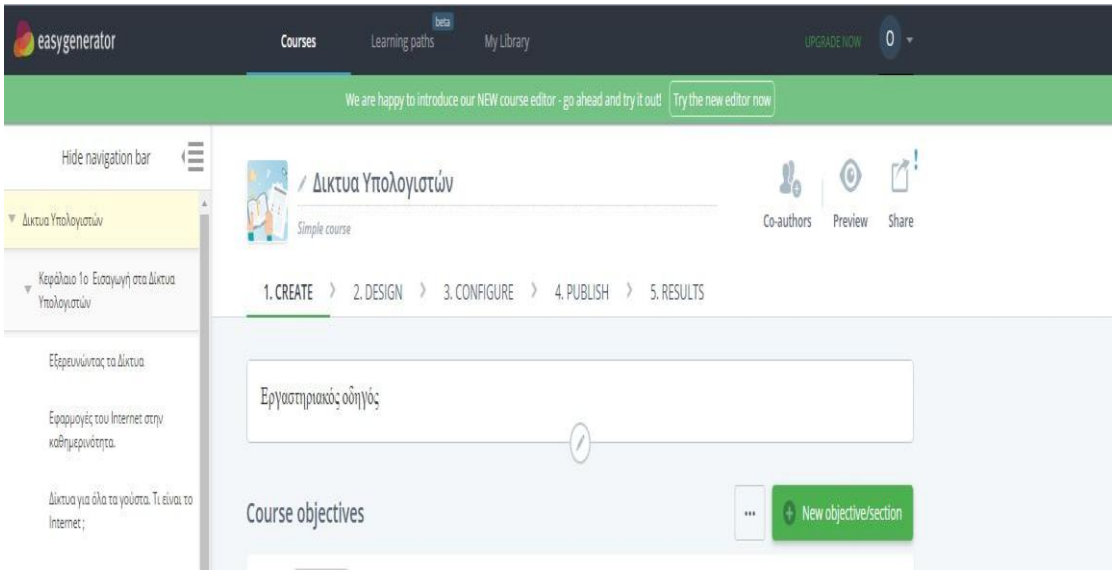
Το Easygenarator προσφέρει μία μεγάλη γκάμα από ερωτήσεις, quizzes και διαδραστικών παιχνιδιών ώστε να εξασφαλίζεται η κατανόηση και η αφομοίωση από τους μαθητές του μαθήματος. Υπάρχει η δυνατότητα των ερωτήσεων πολλαπλής επιλογής, συμπλήρωσης κενών, σχεδιασμού δικών μας ερωτήσεων και πολλά άλλα.

Δημιουργία του Elearning υλικού με το Easygenarator

Δημιουργούμε λογαριασμό ώστε να έχουμε τη δυνατότητα να χρησιμοποιήσουμε το easygenarator. Η πλατφόρμα μας αφήνει για δεκατέσσερις ημέρες να χρησιμοποιήσουμε το ολοκληρωμένο πακέτο

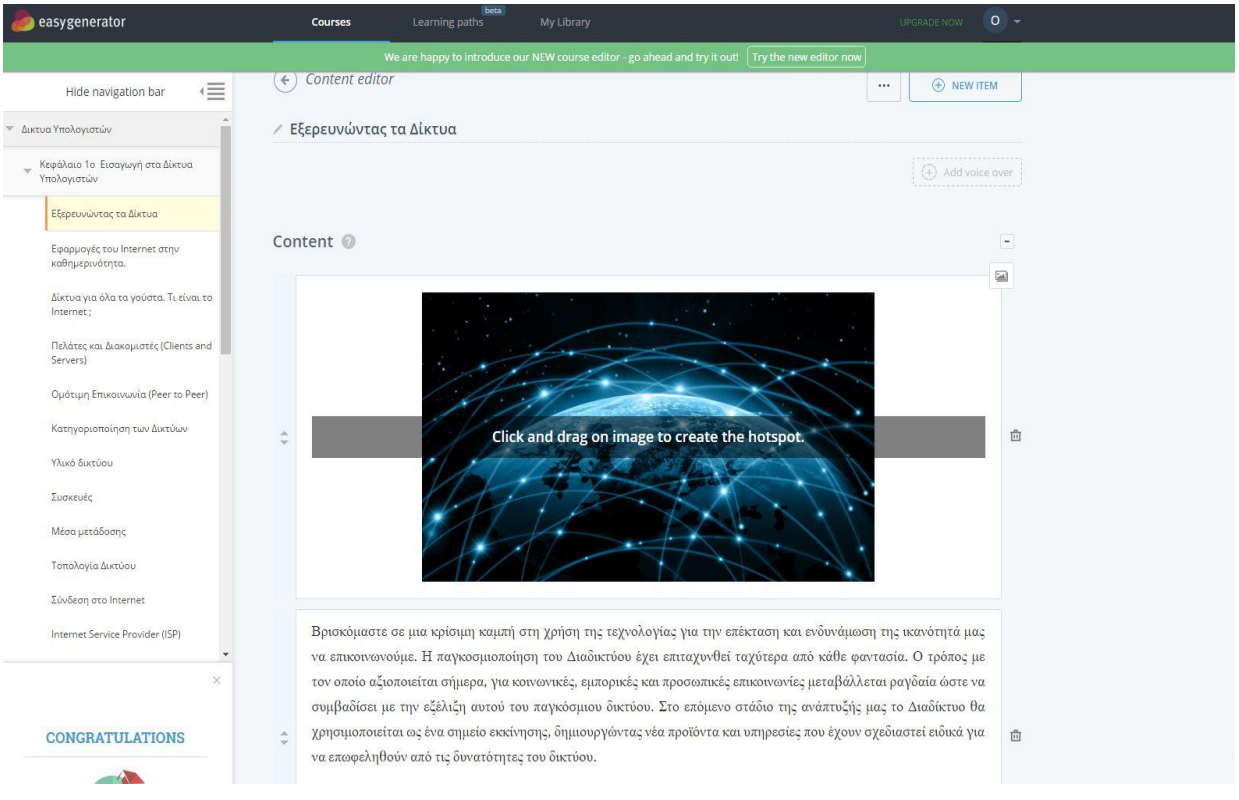
(το οποίο δεν είναι δωρεάν), στο οποίο δεν υπάρχει κανένας περιορισμός για την δημιουργία του υλικού μας.

Κάνοντας σύνδεση μπαίνουμε στην πλατφόρμα ανάπτυξης του διαδικτυακού υλικού. Δίνουμε όνομα στο μάθημα που θέλουμε να δημιουργήσουμε καθώς και υπότιτλο.

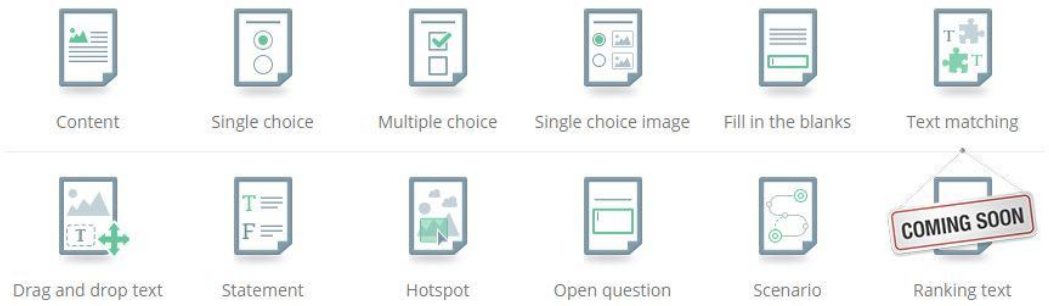


Στη συνέχεια επιλέγουμε το new objective/section ώστε να δημιουργήσουμε την παρουσίαση του μαθήματος.

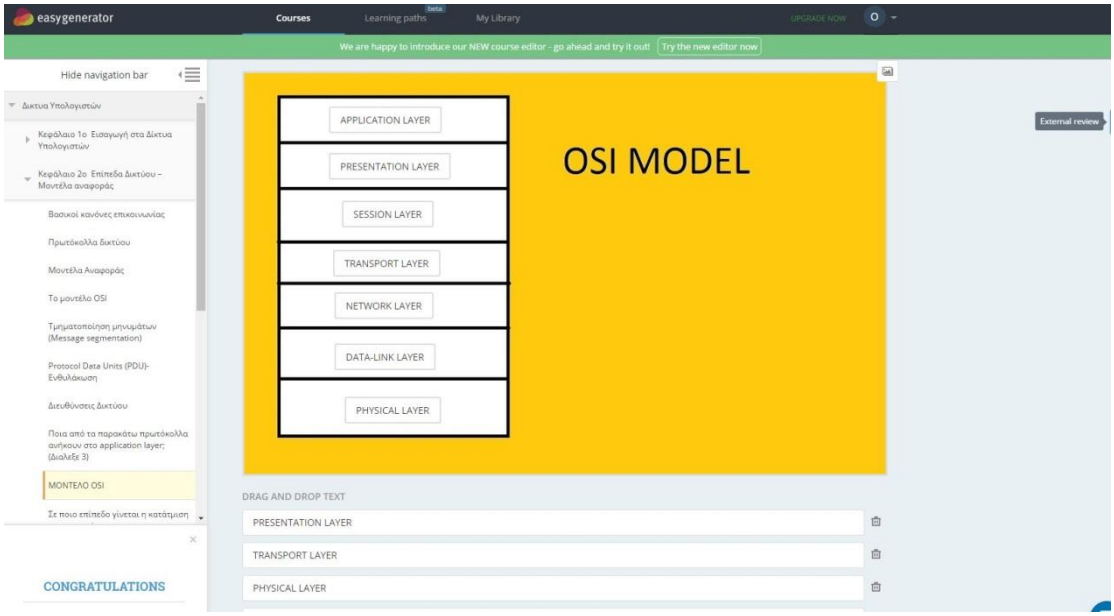
Όπως είπαμε και παραπάνω μπορούμε να κάνουμε ενδιαφέρον το υλικό μας χρησιμοποιώντας εικόνες, βίντεο και άλλα πολυμέσα.



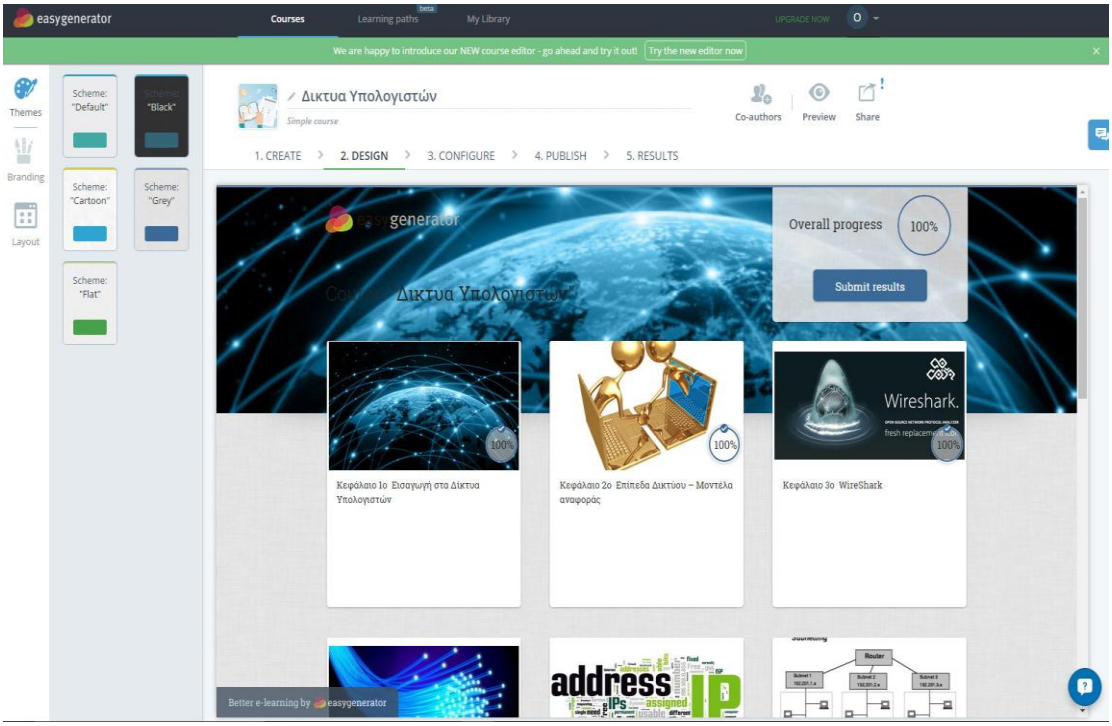
Με την επιλογή new item προσθέτουμε νέα σελίδα στην παρουσίαση μας, όπου και πάλι επιλέγουμε μέσα από ένα σύνολο templates. Με το new item μπορούμε να δημιουργήσουμε και τις ερωτήσεις στο τέλος του κάθε κεφαλαίου.



Παράδειγμα δημιουργίας ερώτησης



Με την ολοκλήρωση της δημιουργίας του υλικού , μπορούμε να ασχοληθούμε με το design του μαθήματος. Μέσα από μία γκάμα templates μπορούμε να διαλέξουμε αυτό που μας ταιριάζει. Ακόμα μπορούμε να δημιουργήσουμε διάφορες παραλλαγές, να βάλουμε εικόνες στο φόντο και άλλα πολλά.



Τέλος μπορούμε να εξάγουμε το υλικό μας σε διάφορε μορφές όπως είπαμε και παραπάνω. Μπορούμε να πάρουμε απλά ένα URL το οποίο μας οδηγεί στο cloud της easygenarator πλατφόρμας όπου είναι αποθηκευμένο (http://elearning.easygenerator.com/42b6628b-8777-415f-a925-29167ae4b552).

Ακόμα μας δίνεται η δυνατότητα να το εντάξουμε μέσα στην ιστοσελίδα μας με html κώδικα που θα δημιουργεί ένα frame μέσα στο οποίο θα προβάλλει το υλικό μας.

Παράδειγμα HTML κώδικα

<iframe width="930" height="700" src="http://elearning.easygenerator.com/42b6628b-8777-415f-a925-29167ae4b552" frameborder="0" allowfullscreen></iframe>

Μπορούμε να εξάγουμε το υλικό μας και να το «κατεβάσουμε» σε μορφή SCORM 1.2 ή HTML. Η μορφή SCORM μας βοηθά ώστε να το ανεβάσουμε σε κάποιο LMS ώστε να έχουν μέσω αυτού πρόσβαση οι εκπαιδευόμενοι, πχ open eclass. Για να είναι στο σωστό format κάθε πακέτο Scorm περιέχει ένα manifest αρχείο ώστε να συνδέεται με το αντίστοιχο LMS και να αλληλοτροφοδοτούνται με τις απαραίτητες πληροφορίες (βλ παραρτημα 1).

Πλατφόρμα open e-class

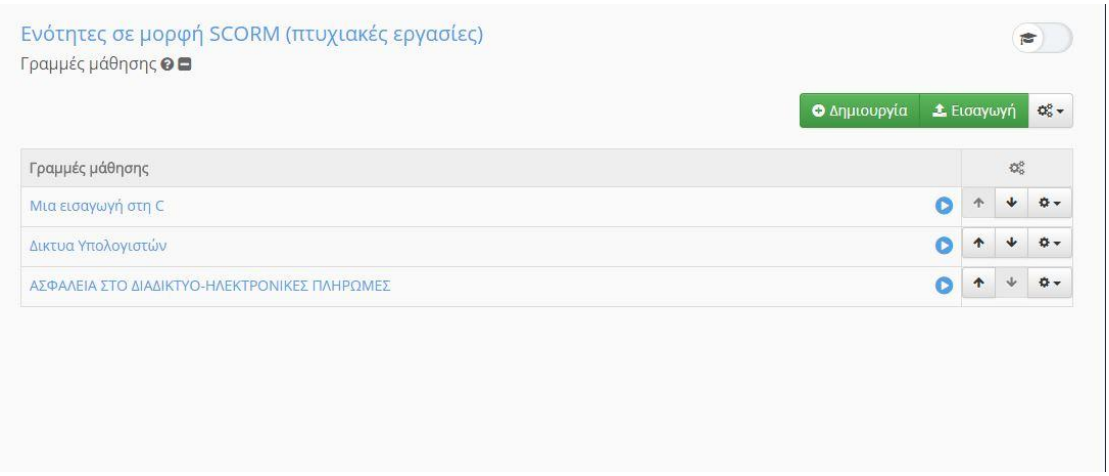
Εξάγοντας το υλικό μας σε μορφή SCORM μπορούμε να το ανεβάσουμε στην πλατφόρμα ηλεκτρονικής μάθησης που χρησιμοποιεί το ΤΕΙ Κρήτης,open e-class.

Η πλατφόρμα Open eClass είναι ένα ολοκληρωμένο Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων και συνιστά προσφορά του Ελληνικού Ακαδημαϊκού Διαδικτύου (GUnet) στην εκπαιδευτική και ακαδημαϊκή κοινότητα. Έχει σχεδιαστεί με προσανατολισμό την ενίσχυση της εκπαιδευτικής διαδικασίας, βασίζεται στη φιλοσοφία του λογισμικού ανοικτού κώδικα, υποστηρίζεται ενεργά από το GUnet και διανέμεται ελεύθερα. Βασική επιδίωξη της πλατφόρμας είναι η ενσωμάτωση των νέων τεχνολογιών και η εποικοδομητική χρήση του διαδικτύου στην εκπαιδευτική διαδικασία.

Είναι ιδιαίτερα εύχρηστη τόσο από τους εκπαιδευτές όσο και από τους εκπαιδευόμενους. Η πρόσβαση στην Open eClass γίνεται με τη χρήση ενός απλού φυλλομετρητή (web browser). Η πλατφόρμα Open eClass είναι πλήρως λειτουργική σε όλους τους φυλλομετρητές. Η πλατφόρμα Open eClass διαθέτει μοντέρνα και προσαρμοστική (responsive) διεπαφή χρήστη (user interface), που βασίζεται σε Bootstrap 3x, ώστε να προσαρμόζεται στις οθόνες διαφορετικών συσκευών, συμπεριλαμβανομένων ηλεκτρονικών υπολογιστών, tablets και smartphones.

Οι χρήστες μπορούν επίσης να έχουν απευθείας πρόσβαση στην Open eClass στο tablet ή το κινητό τους και μέσω των εφαρμογών για κινητές συσκευές με λειτουργικό iOS και Android.

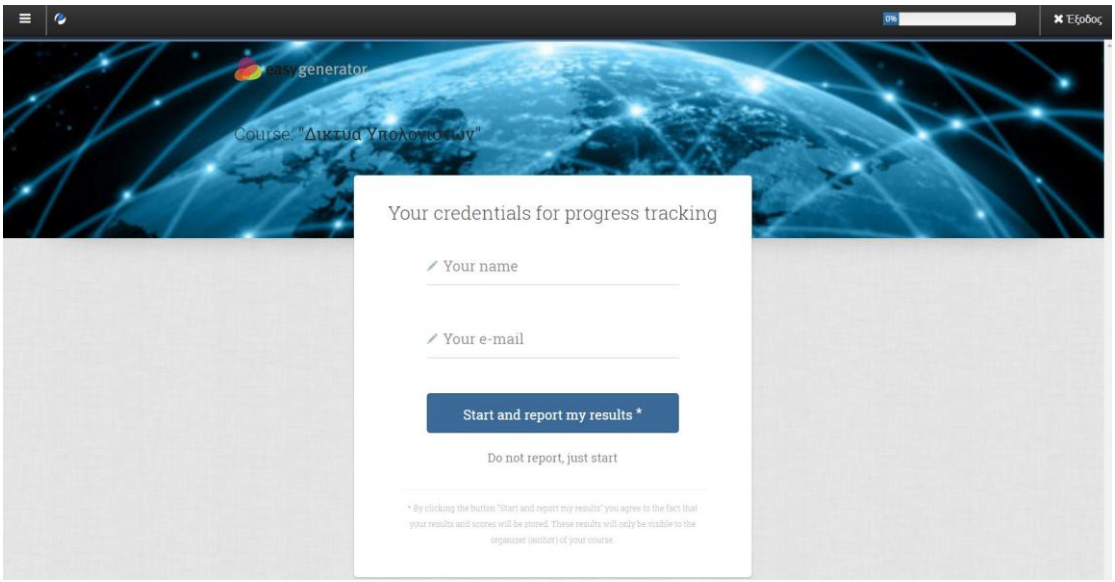
Βασικό της στοιχείο είναι η συμβατότητα της με διάφορα πρότυπα ηλεκτρονικής μάθησης όπως το SCORM πράγμα που εξασφαλίζει την επαναχρησιμοποίηση, την προσβασιμότητα και την ανθεκτικότητα του εκπαιδευτικού υλικού στις τεχνολογικές μεταβολές, καθώς και την διαλειτουργικότητα μεταξύ συστημάτων ηλεκτρονικής μάθησης.



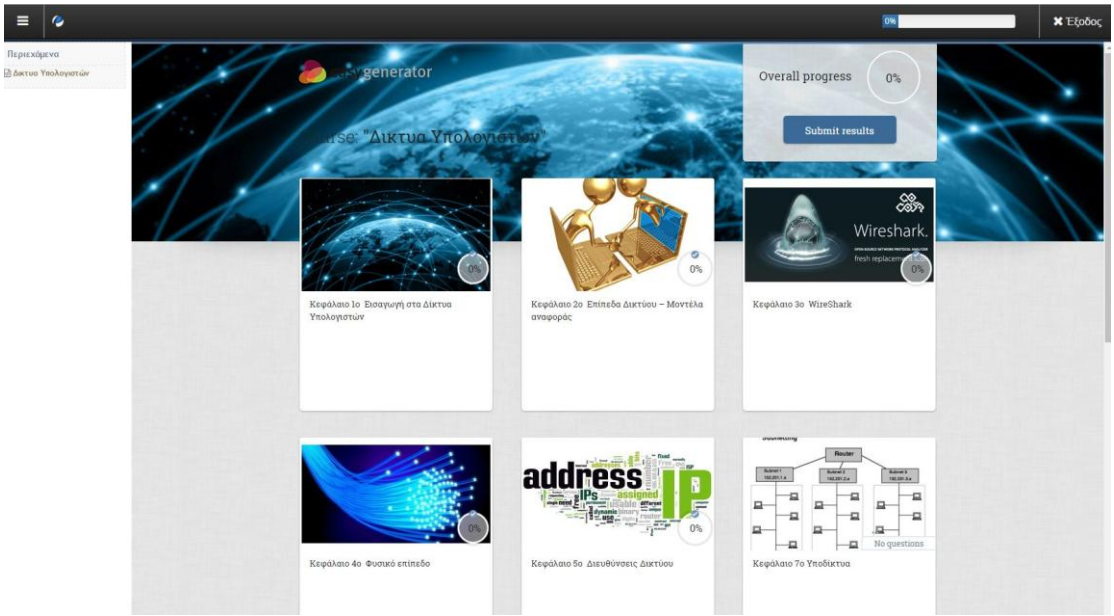
Για την δημιουργία νέου μαθήματος όπως φαίνεται και στην εικόνα παραπάνω επιλέγουμε «δημιουργία» ενώ για την εισαγωγή έτοιμου υλικού σε μορφή SCORM την επιλογή “Εισαγωγή».

Χρήση του υλικού μας

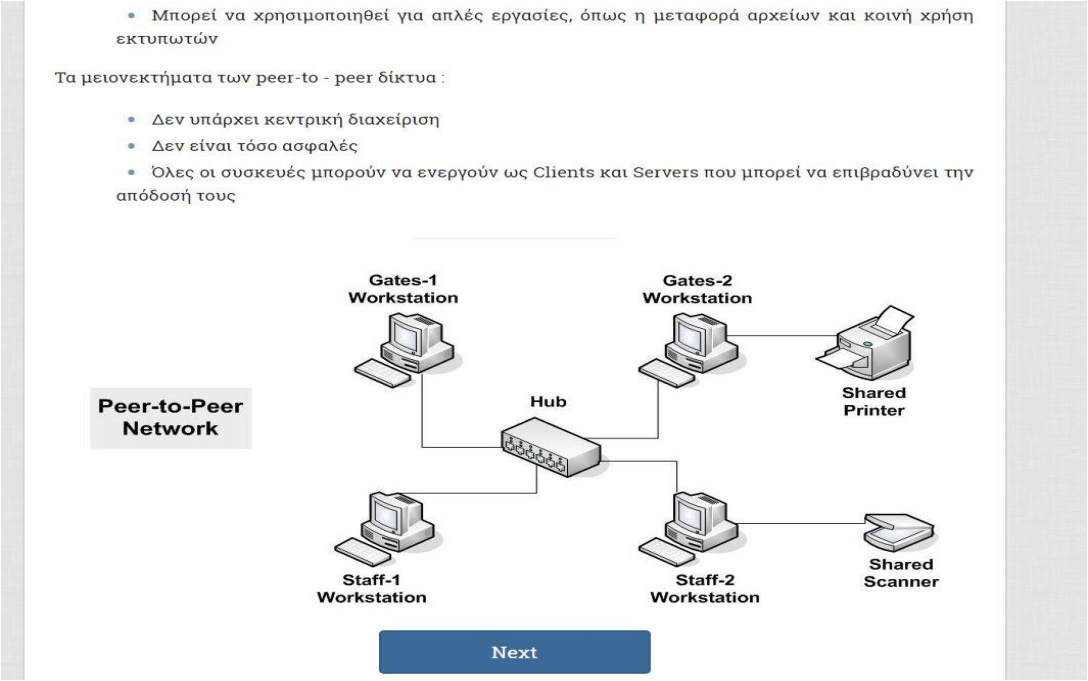
Με το που επιλέξουμε το μάθημα δίκτυα υπολογιστών μας δίνεται η δυνατότητα να εισάγουμε τα στοιχεία μας ώστε να πάρουμε στο e-mail μας feedback για την πορεία μάθησης και τα αποτελέσματα με βάση της ασκήσεις



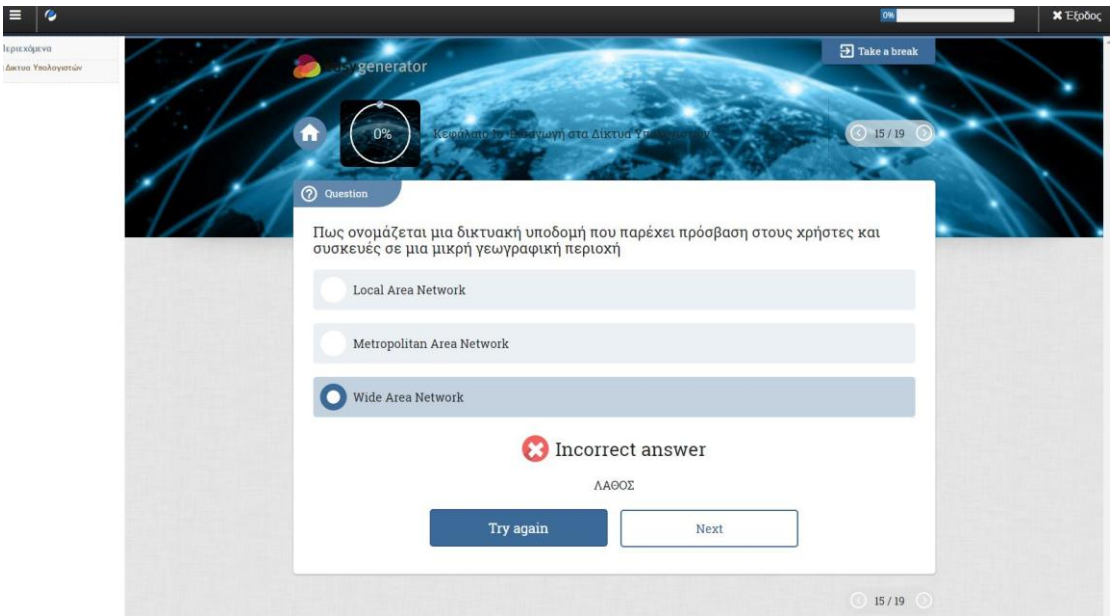
Στη συνέχεια εμφανίζεται το σύνολο των κεφαλαίων που περιέχει το μάθημα.



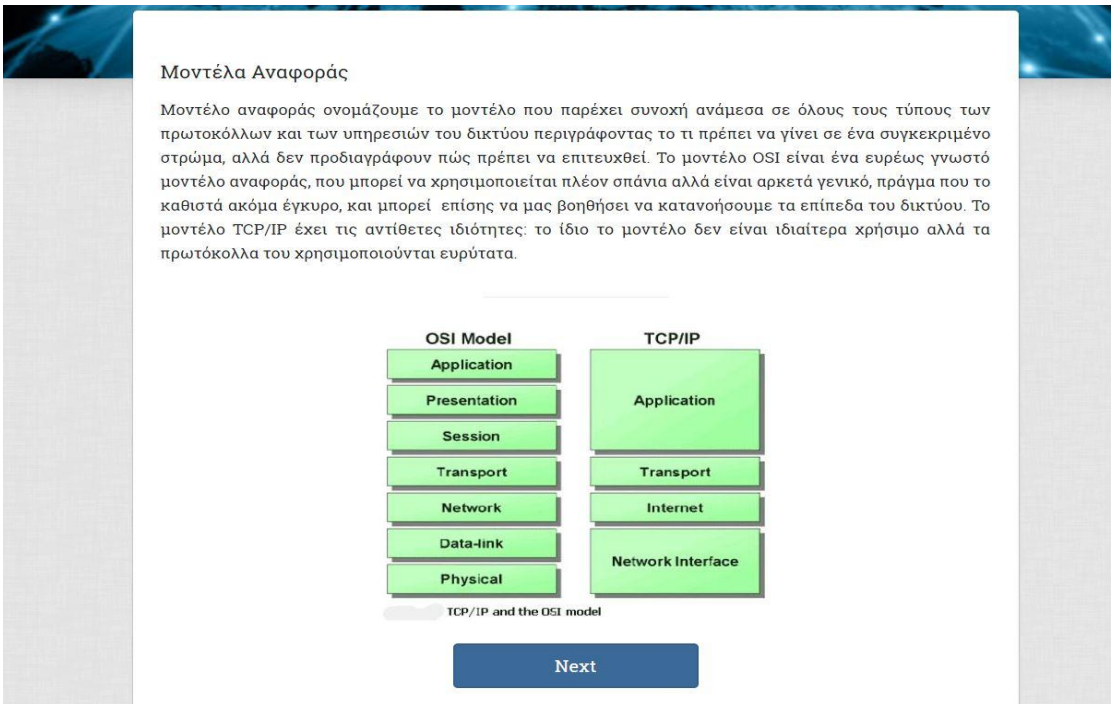
Στο 1^{ο} κεφάλαιο πραγματοποιείται μία εισαγωγή στο μάθημα δίκτυα υπολογιστών ενώ στο τέλος του ακολουθούν ερωτήσεις κατανόησης.

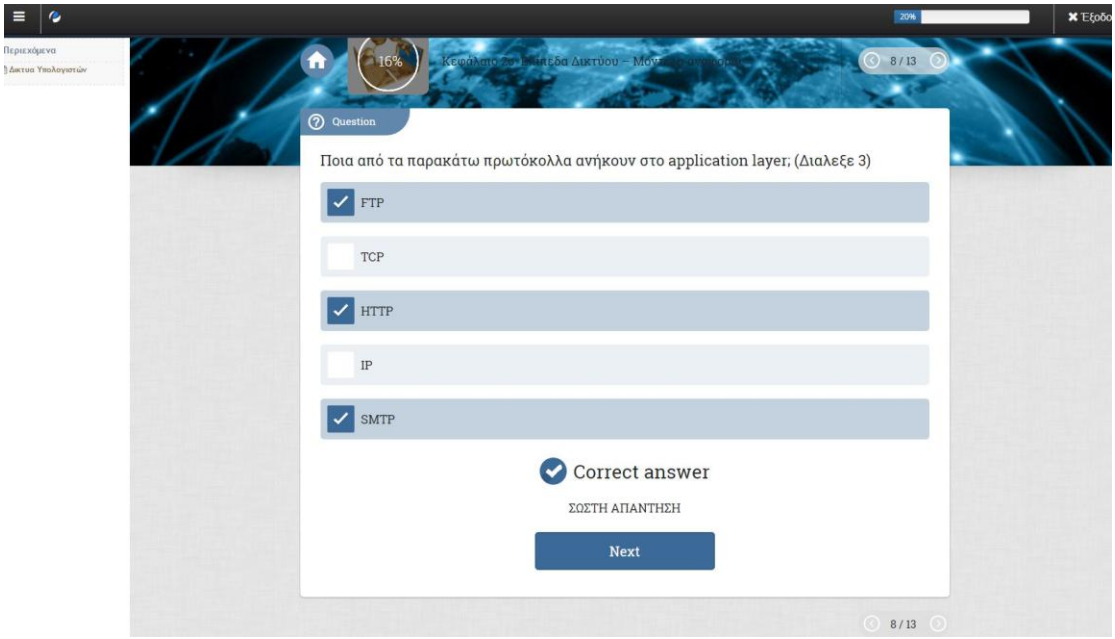


Προχωράμε τις διαφάνειες επιλέγοντας το next ενώ υπάρχει και η δυνατότητα να γυρίζουμε προς τα πίσω. Στις ερωτήσεις κατανόησης ο χρήστης ενημερώνεται άμεσα για μία λάθος απάντηση και του δίνεται η δυνατότητα να ξαναπροσπαθήσει.

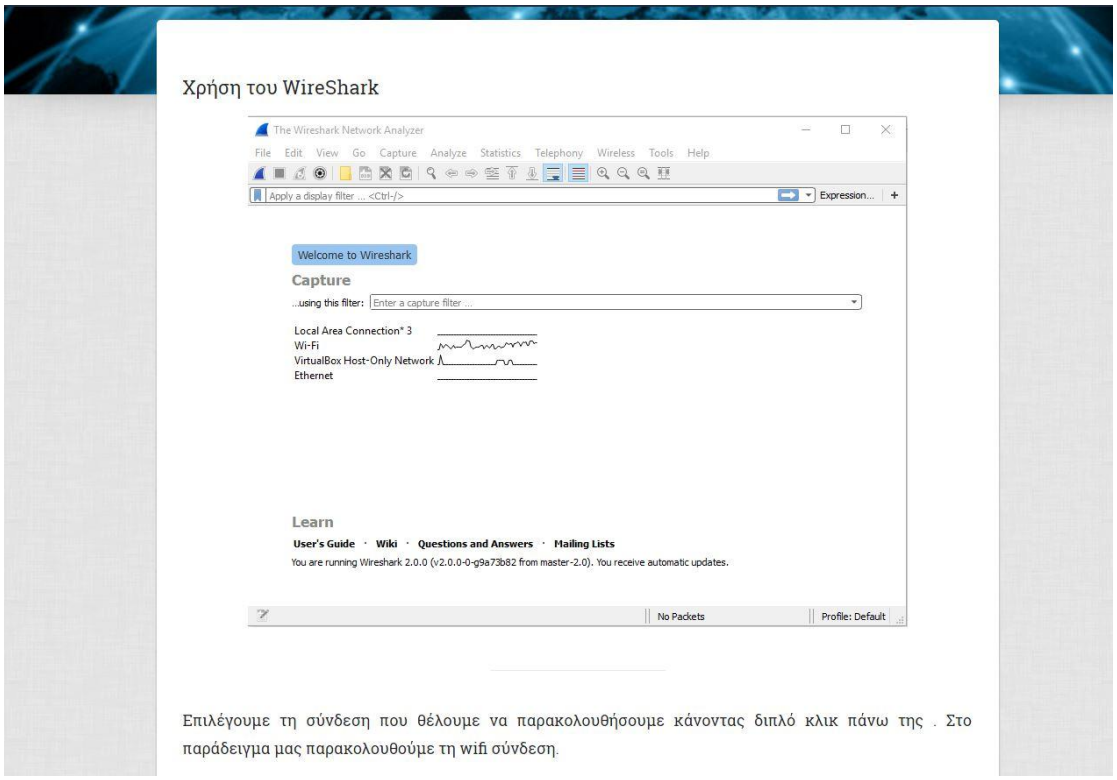


Στο 2^{ο} κεφάλαιο ασχολούμαστε με τα επίπεδα του δικτύου και τα μοντέλα αναφοράς. Και εδώ ακολουθούν ερωτήσεις κατανόησης με το τέλος των διαφανειών της θεωρίας.

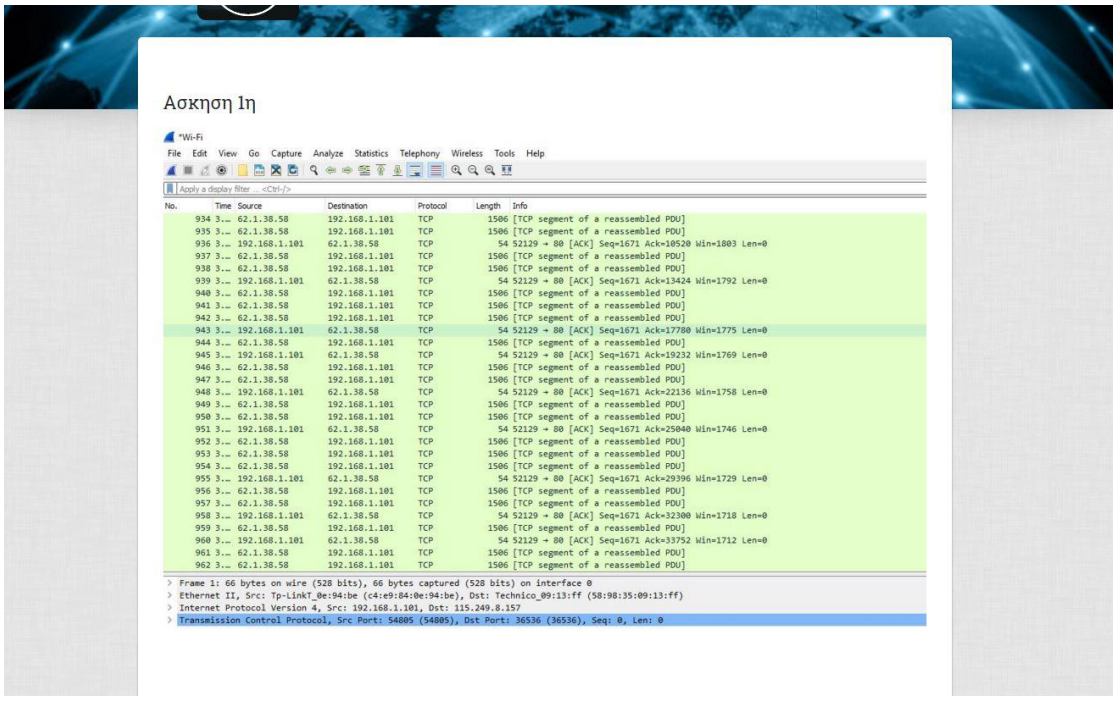




Στο 3^{ο} κεφάλαιο ασχολούμαστε με την εγκατάσταση και χρήση του προγράμματος Wireshark.



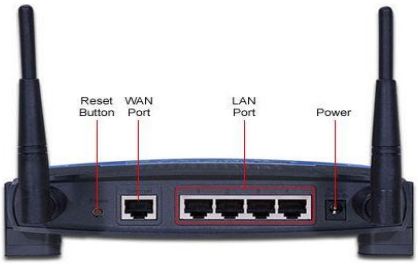
Επιλέγουμε τη σύνδεση που θέλουμε να παρακολουθήσουμε κάνοντας διπλό κλικ πάνω της . Στο παράδειγμα μας παρακολουθούμε τη wifi σύνδεση.



Στο 4^{ο} κεφάλαιο αναφερόμαστε στο φυσικό επίπεδο. Αναλυτικά κουβεντιάζουμε για τα μέσα μετάδοσης αλλά και την συνδεσμολογία των συσκευών του δικτύου.

Για να συνδέσουμε τερματικές συσκευές μεταξύ τους , είτε πρόκειται για ένα τοπικό δίκτυο, είτε για να συνδεθούμε σε ένα server στην άλλη άκρη του κόσμου, χρειάζεται πρώτα να εγκατασταθεί μία φυσική σύνδεση. Μία φυσική σύνδεση μπορεί να είναι ενσύρματη χρησιμοποιώντας καλώδια αλλά μπορεί να είναι και ασύρματη χρησιμοποιώντας ραδιοκύματα.

Στο σπίτι μας συνδιάζουμε την ενσύρματη με την ασύρματη σύνδεση καθώς το router μας λειτουργεί ταυτόχρονα και σαν switch αλλά και σαν wireless access point!

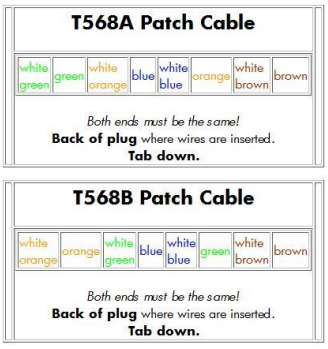


Next

Straight-through : Το πιο κοινό καλώδιο, αυτό που συνδέει ένα χρήστη στο switch , το switch με το router.

CrossOver : Είναι καλώδιο που χρησιμοποιείται ώστε να συνδέει παρόμοιες συσκευές όπως ένα switch με ένα άλλο switch, ένα υπολογιστή με ένα άλλο κλπ. Χρησιμοποιείται επίσης για να συνδέσουμε απευθείας πάνω στο router ένα PC (Προσοχή στο σπίτι μας έχουμε layer 3 switch και όχι router και για αυτό χρησιμοποιούμε Straight-through!!).

T568A T568B Cable Color Code



Next

Στο κεφάλαιο 5 μιλάμε για τις διευθύνσεις δικτύου. Μαθαίνουμε να ξεχωρίζουμε το δικτυακό μέρος από το μέρος του χρήστη, να δουλεύουμε με δυαδικό σύστημα κ.α.

χωριζονται μεταξυ τους απο μια τελεια. Για παραδειγμα μια διευθυνση δικτυου σε δυαδικη μορφη ειναι η εξής:

11000000.10101000.00001010.00000001

Το να δουλεύουμε και να επεξεργαζόμαστε τις IP σε δυαδικό σύστημα είναι δύσκολο. Γι αυτό και μετατρέπουμε τις IP σε δεκαδικό σύστημα ώστε να μπορούμε να τις επεξεργαζόμστε πιο εύκολα. Ετσι η παραπ[άνω διεύθυνση μεταφράζεται σε δεκαδικό:

192.168.10.1

Χρειαζόμαστε όμως να μπορούμε να μετατρέπουμε από δεκαδικό σε δυαδικό οπότε θα δώσουμε λίγο βάρος στο πως θα κάνουμε αυτή τη διαδιακασία εύκολη!

Μετατροπή δυαδικού σε δεκαδικό

Για να κάνουμε εύκολη τη μετατροπή από δεκαδικό σε δυαδικό χρειάζεται να έχουμε στο μυαλό μας τις δυνάμεις του 2.

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Αντιστοιχίζοντας τον παραπάνω πίνακα σε 8 bit που έχει ο κάθε τομέας μπορούμε να δούμε ότι:

Ο 1ος τομέας του παραδείγματος IP που δώσαμε παραπάνω αντιστοιχει:

Δημόσιες και ιδιωτικές IPv4 διευθύνσεις

Το σύνολο των IPv4 διευθύνσεων είναι από 0.0.0.0 έως 255.255.255.255 εκ των οποίων κάποιες είναι δεσμευμένες από ερευνητικούς οργανισμούς, μεγάλες εταιρίες, το στρατό, μυστικές υπηρεσίες κ.α. Αυτό μας δίνει ένα σύνολο 2^32 διευθύνσεων, κάτι λιγότερο από 4,3 δισεκατομμύρια!

Μπορεί να φαίνονται πάρα πολλές αλλά η πραγματικότητα το διαψεύδει. Με τόσες συσκευές που πλέον συνδέονται στο internet, από υπολογιστές, tablet, smartphones, μέχρι και οικιακές συσκευές καταλαβαίνουμε ότι ο αριθμός αυτός δεν επαρκεί. Αυτό είχε λυθεί ως ένα βαθμό προσωρινά με το διαχωρισμό των IPv4 διευθύνσεων σε ψεύτικες και πραγματικές, ιδιωτικές-δημόσιες. Ακόμα και με αυτό το διαχωρισμό όμως οι IPv4 διευθύνσεις έχουν εξαντληθεί από το Φλεβάρη του 2011! Στη συνέχεια του κεφαλαίου θα δούμε πως έχει λυθεί αυτό το πρόβλημα. Προς το παρόν θα ασχοληθούμε με τις πραγματικές και ψεύτικες διευθύνσεις.

Τι είναι όμως μια ψεύτικη διεύθυνση και τι μια πραγματική; Είπαμε πριν ότι κάθε συσκευή που βρίσκεται μέσα σε ένα δίκτυο έχει μία διεύθυνση που την καθορίζει μονοσήμαντα. Αυτό μας δίνει τη δυνατότητα σε 2 συσκευές που βρίσκονται σε διαφορετικά δίκτυα να έχουν την ίδια IP(ψεύτική-ιδιωτική) όσο επικοινωνούν με άλλες συσκευές στο ίδιο με αυτές δίκτυο, αλλά θα χρειάστούν ξεχωριστή (πραγματική -δημόσια) όταν «βγουν» στο internet.

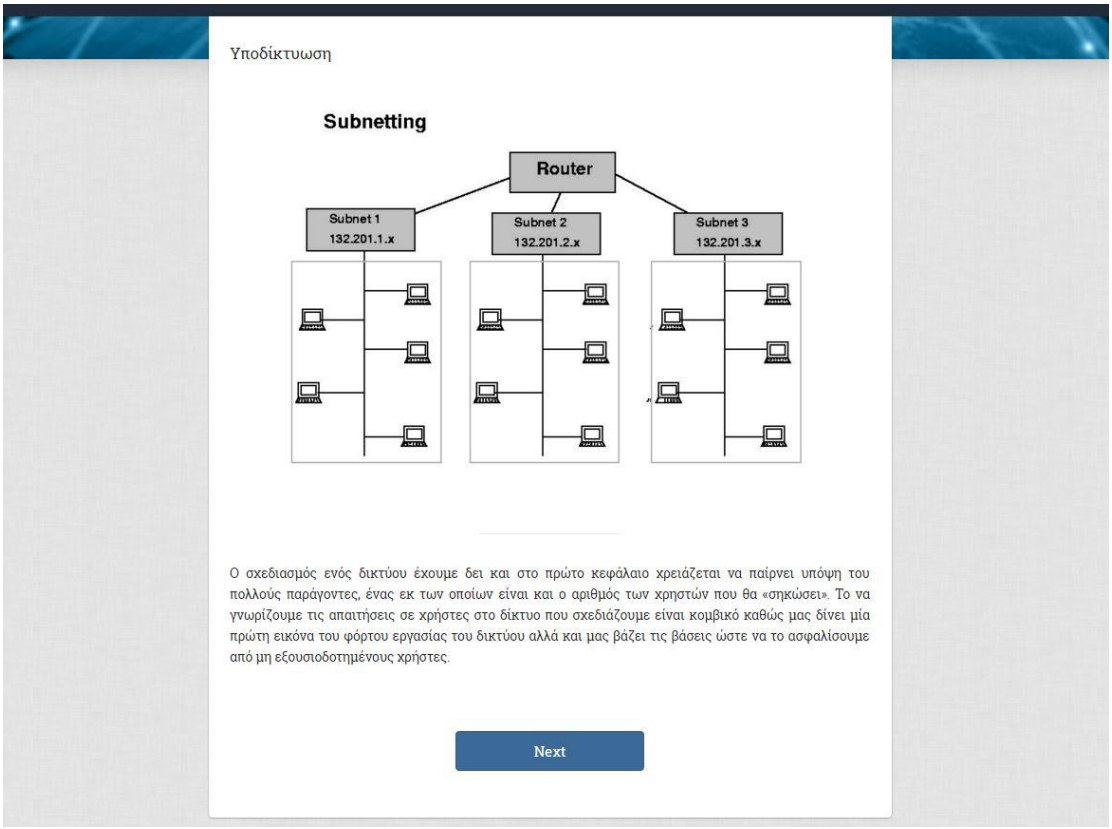
Με αυτό το σκεπτικό ένα κομμάτι των IPv4 διευθύνσεων έχουν ξεχωριστεί και θεωρούνται ψεύτικες, δεν αναγνωρίζονται στο internet. Τα μπλοκ των ψεύτικων διευθύνσεων είναι:

- 24-bit Block (/8 prefix,) 10.0.0.0 - 10.255.255.255
- 20-bit Block (/12 prefix) 172.16.0.0 - 172.31.255.255
- 16-bit Block (/16 prefix) 192.168.0.0 - 192.168.255.255

Όλες οι υπόλοιπες διευθύνσεις είναι πραγματικές και χρησιμοποιούνται από τις συσκευές μόλις «βγαίνουν» στο internet. Πραγματικές διευθύνσεις μας δίνουν οι ISP.

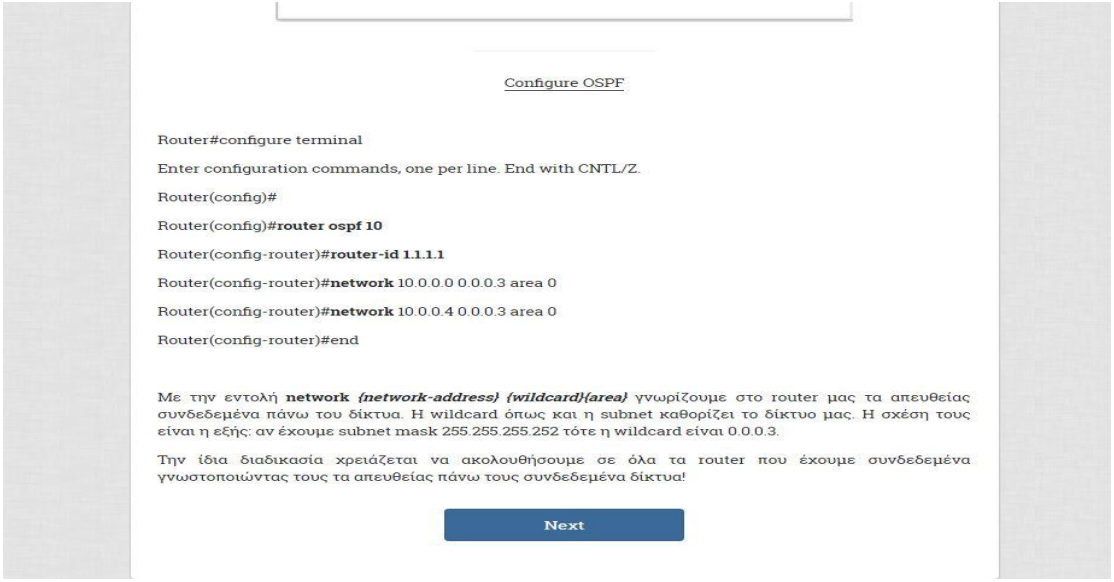
Next

Στο 6ο κεφάλαιο μαθαίνουμε να κάνουμε subnetting.



Στο 7ο κεφάλαιο ασχολούμαστε με το DHCP και μαθαίνουμε πως να το στήνουμε σε ένα routrer.

Στο 8^{ο} κεφάλαιο μιλάμε για routing protocols και μαθαίνουμε πως στήνεται το OSPF πρωτόκολλο στο δίκτυο μας.



Configure OSPF

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

Router(config)#**router ospf 10**

Router(config-router)#**router-id 1.1.1.1**

Router(config-router)#**network** 10.0.0.0 0.0.0.3 area 0

Router(config-router)#**network** 10.0.0.4 0.0.0.3 area 0

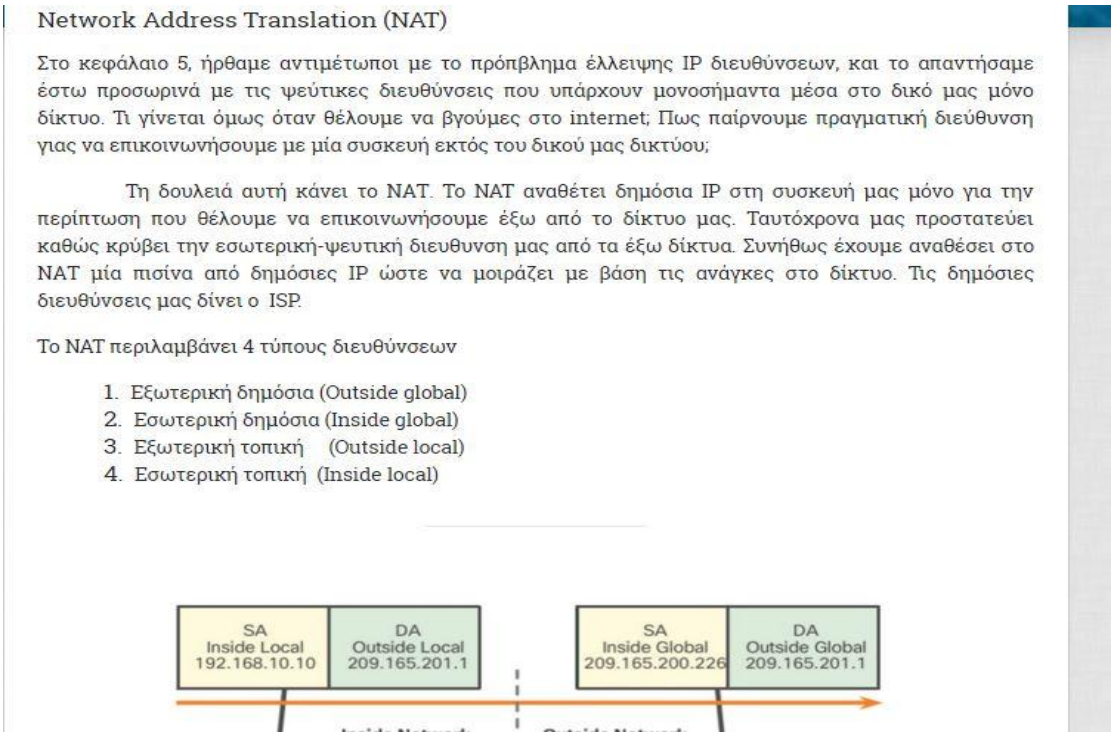
Router(config-router)#end

Με την εντολή **network** ***{network-address} {wildcard}{area}*** γνωρίζουμε στο router μας τα απευθείας συνδεδεμένα πάνω του δίκτυα. Η wildcard όπως και η subnet καθορίζει το δίκτυο μας. Η σχέση τους είναι η εξής: αν έχουμε subnet mask 255.255.255.252 τότε η wildcard είναι 0.0.0.3.

Την ίδια διαδικασία χρειάζεται να ακολουθήσουμε σε όλα τα router που έχουμε συνδεδεμένα γνωστοποιώντας τους τα απευθείας πάνω τους συνδεδεμένα δίκτυα!

Next

Στο κεφάλαιο 9 βλέπουμε τη χρήση του NAT αλλά και το που και πως στήνεται.



Network Address Translation (NAT)

Στο κεφάλαιο 5, ήρθαμε αντιμέτωποι με το πρόβλημα έλλειψης IP διευθύνσεων, και το απαντήσαμε έστω προσωρινά με τις ψεύτικες διευθύνσεις που υπάρχουν μονοσήμαντα μέσα στο δικό μας μόνο δίκτυο. Τι γίνεται όμως όταν θέλουμε να βγούμες στο internet; Πως παίρνουμε πραγματική διεύθυνση γιας να επικοινωνήσουμε με μία συσκευή εκτός του δικού μας δικτύου;

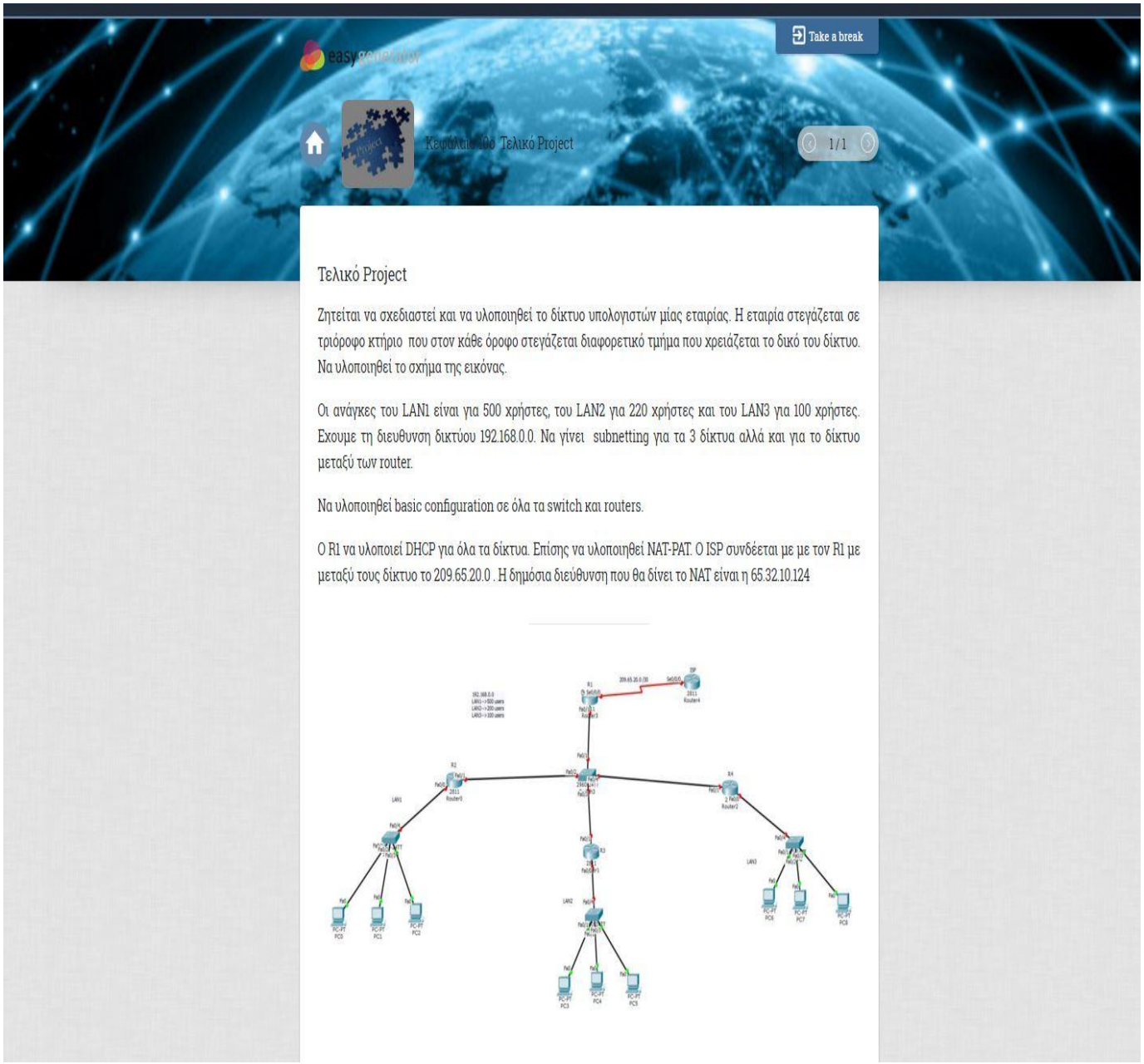
Τη δουλειά αυτή κάνει το NAT. Το NAT αναθέτει δημόσια IP στη συσκευή μας μόνο για την περίπτωση που θέλουμε να επικοινωνήσουμε έξω από το δίκτυο μας. Ταυτόχρονα μας προστατεύει καθώς κρύβει την εσωτερική-ψευτική διευθυνση μας από τα έξω δίκτυα. Συνήθως έχουμε αναθέσει στο NAT μία πισίνα από δημόσιες IP ώστε να μοιράζει με βάση τις ανάγκες στο δίκτυο. Τις δημόσιες διευθύνσεις μας δίνει ο ISP.

Το NAT περιλαμβάνει 4 τύπους διευθύνσεων

1. Εξωτερική δημόσια (Outside global)
2. Εσωτερική δημόσια (Inside global)
3. Εξωτερική τοπική (Outside local)
4. Εσωτερική τοπική (Inside local)

SA Inside Local 192.168.10.10 | DA Outside Local 209.165.201.1 | SA Inside Global 209.165.200.226 | DA Outside Global 209.165.201.1

Το τελευταίο κεφάλαιο περιέχει ένα project που ενσωματώνει τις γνώσεις που έχουν αποκτηθεί από τα μέχρι τώρα μαθήματα.



Συμπεράσματα

Την παρούσα πτυχιακή θα μπορούσαμε να την χωρίσουμε σε δύο βασικά μέρη. Το 1^{ο} μέρος έχει να κάνει με την επιλογή της ύλης και την συγγραφή του εργαστηριακού οδηγού, ενώ το 2^{ο} με την δημιουργία του υλικού ηλεκτρονικής μάθησης. Και τα δύο αυτά μέρη ήταν αρκετά διδακτικά.

Η συγγραφή του υλικού αντικειμενικά απασχόλησε το μεγαλύτερο μέρος του χρόνου που αφιερώθηκε στην εκπόνηση της εργασίας. Χρειάστηκε συστηματική μελέτη ώστε να επιλεχθούν τα κεφάλαια και η ύλη. Η δομή των κεφαλαίων προσπάθησα να καλύπτει τις γνώσεις που χρειάζονται για το σχεδιασμό, την υλοποίηση και την υποστήριξη ενός δικτύου υπολογιστών σε μία μετρίου μεγέθους εταιρία. Στο τέλος του κάθε κεφαλαίου υπάρχουν ασκήσεις κατανόησης αλλά και άσκηση σε Wireshark και packet tracer. Ιδιαίτερο με το δεύτερο οι ασκήσεις προσπαθούν να προσομοιάσουν πραγματικές καταστάσεις και ανάγκες που έχει ένα δίκτυο υπολογιστών.

Είναι λογικό ότι δεν θα μπορούσε ο εργαστηριακός αυτός οδηγός να καλύψει το σύνολο της ύλης όμως μία πιθανή επέκταση του θα μπορούσε να κάνει με το troubleshooting σε δίκτυα υπολογιστών.

Κεφάλαιο 4ο

Βιβλιογραφία

- Δίκτυα Υπολογιστών *ANDREW S. TANENBAUM*
- COMPUTER NETWORKING A Top-Down Approach *KUROSE ROSS*
- *www.easygenerator.com*
- *http://www.openeclass.org/*
- *https://en.wikipedia.org/wiki/Educational_technology*

Πηγή εικόνων

https://www.dynu.com/content/images/content/Blogs/StaticVSDynamicIP.jpg

http://images.slideplayer.com/20/6222823/slides/slide_11.jpg

http://www.windowsdevcenter.com/2007/06/12/graphics/IntroDHCP1.png

http://study-ccna.com/wp-content/images/dhcp_process_explained.jpg

https://upload.wikimedia.org/wikibooks/en/4/43/PAT.jpg

http://liomas.gr/external/eclass-images/Diktia_Hlektronikon_5.jpg

http://www.solplus.co.uk/wp-content/uploads/2013/03/projectManagement.jpg

http://www.nicwebdesign.com/blog/resources/site1/General/Blog%20Images/Netiquette.PNG

http://web1.muirfield-h.schools.nsw.edu.au/technology/resources/IPT/Karens%20stuff/IPT/HSC/Bernies/protocol_files/osi.gif

http://wiki.cas.mcmaster.ca/images/e/eb/Tcpmodel.jpg

http://www.learn44.com/wp-content/uploads/2013/06/Protocol-Data-Unit-PDU-and-Layer-Addressing-in-Data-Encapsulation-Cisco-Inter-networking.jpg

http://www.highteck.net/images/25-TCP-address.jpg

http://amtechcommunications.com/wp-content/uploads/2013/10/internet.jpg

http://www.adweek.com/socialtimes/files/2013/02/social-world.png

https://upload.wikimedia.org/wikipedia/commons/thumb/c/c9/Client-server-model.svg/2000px-Client-server-model.svg.png

https://www.webjunction.org/content/dam/WebJunction/Images/webjunction/img11019.jpg

http://www.microlink.co.in/wp-content/uploads/2014/05/Red_LAN.gif

https://upload.wikimedia.org/wikipedia/commons/9/9a/Wan_home1.png

http://storageareanetwork.info/wp-content/uploads/2013/08/storageareanetwork.png

http://www.conniq.com/images/intranet-extranet-internet.gif

http://www.highteck.net/images/12-network-services.jpg

http://img.directindustry.com/images_di/photo-g/4g-communication-router-mobile-26-ports-industrial-61501-6201751.jpg

http://www.tapscape.com/wp-content/uploads/2014/05/cox-residential-gigabit.jpg

https://www.edrawsoft.com/template/topology-diagram.png

https://krystalchisholm.files.wordpress.com/2010/10/access.jpg

http://netlab.ulusofona.pt/rc/book/1-introduction/1_04/01-07.jpg

http://cdn2.hubspot.net/hub/80068/file-15745649-jpg/images/scalabilty_(1).jpg?t=1445271589246

http://www3.alcatel-lucent.com/enrich/v1i22007/images/17_fig01.gif

https://www.flickr.com/photos/cocoia/2065184471

http://rack.3.mshcdn.com/media/ZgkyMDEzLzA0LzA5LzFkL0ZpYmVyLjYwYzMwLmpwZwpwCXRodW1iCTEyMDB4NjI3IwplCWpwZw/a6b5f72e/f0b/Fiber.jpg

http://cdn.instructables.com/F4S/17K7/GOHM3OB1/F4S17K7GOHM3OB1.MEDIUM.jpg

http://3.bp.blogspot.com/-1Yy9r5T3HAs/UVX3qBme6gI/AAAAAAAAMVs/LE2BQXucRCk/s1600/Capture.PNG

http://www.nktphotonics.com/wp-content/uploads/2015/06/Hollow_core_fiber_-_NKT_Photonics.png

http://rubyliuhuijun.blog.com/files/2015/06/Fiber-Optic-Common-Connector-types.jpg

http://www.a-store.gr/images/stories/virtuemart/product/cb84_3.jpg

https://www.dynu.com/content/images/content/Blogs/StaticVSDynamicIP.jpg

http://images.slideplayer.com/20/6222823/slides/slide_11.jpg

http://mars.netanya.ac.il/~unesco/cdrom/booklet/HTML/NETWORKING/IMAGES/subnet.gif

ΠΑΡΑΡΤΗΜΑ 1

Αρχείο manifest.json


```
{
 "name": "Simple course",
 "goal": "Teach",
 "shortDescription": "A basic eLearning course\n\nDetails:\nThe simple course will allow you to create a course that is divided into several parts (sections or learning objectives). Each section can contain both content items and questions. This way you can create a basic 'simple' eLearning course.",
 "thumbnail": "preview/thumbnail.png",
 "previewImages": [
  "preview/images/preview.jpg"
 ],
 "settingsUrls": {
  "design": {
   "layout": "settings/design/layout.html"
  },
  "configure": "settings/configure/configure.html"
 },
 "supports": [
  "branding"
 ],
 "presets": [
  {
   "title": "default",
   "settings": {
    "branding": {
     "logo": {
```

```
  "url": "//cdn.easygenerator.com/logo.png"
},
"colors": [
 {
  "key": "@text-color",
  "value": "#252728"
 },
 {
  "key": "@main-color",
  "value": "#43aaa3"
 },
 {
  "key": "@secondary-color",
  "value": "#2d9ec6"
 },
 {
  "key": "@button-text-color",
  "value": "#fff"
 },
 {
  "key": "@content-body-color",
  "value": "#fff"
 }
],
"background": {
 "header": {
```

```
        "brightness": 0,
        "color": null,
        "image": {
          "url": "//cdn.easygenerator.com/images/2.jpg",
          "option": "repeat"
        }
      },
      "body": {
        "enabled": true,
        "brightness": 0,
        "color": "#ececed",
        "texture": null
      }
    }
  }
},
{
  "title": "black",
  "settings": {
    "branding": {
      "logo": {
        "url": "//cdn.easygenerator.com/logo.png"
      },
      "colors": [
        {
```

```
    "key": "@text-color",
    "value": "#d7d7d7"
   },
   {
    "key": "@main-color",
    "value": "#336577"
   },
   {
    "key": "@secondary-color",
    "value": "#33b3e2"
   },
   {
    "key": "@button-text-color",
    "value": "#fff"
   },
   {
    "key": "@content-body-color",
    "value": "#232323"
   }
  ],
  "background": {
   "header": {
    "brightness": 0,
    "color": null,
    "image": {
     "url": "//cdn.easygenerator.com/images/11.jpg",
```

```
        "option": "repeat"
       }
      },
      "body": {
       "enabled": true,
       "brightness": 0,
       "color": null,
       "texture": "//cdn.easygenerator.com/textures/5.png"
      }
     }
    }
   }
},
{
 "title": "cartoon",
 "settings": {
  "branding": {
   "logo": {
    "url": "//cdn.easygenerator.com/logo.png"
   },
   "colors": [
    {
     "key": "@text-color",
     "value": "#252728"
    },
    {
```

```
    "key": "@main-color",
    "value": "#2fa6d1"
   },
   {
    "key": "@secondary-color",
    "value": "#e9d20b"
   },
   {
    "key": "@button-text-color",
    "value": "#fff"
   },
   {
    "key": "@content-body-color",
    "value": "#fff"
   }
  ],
  "background": {
   "header": {
    "brightness": 0,
    "color": null,
    "image": {
     "url": "//cdn.easygenerator.com/images/13.jpg",
     "option": "repeat"
    }
   },
   "body": {
```

```
        "enabled": true,
        "brightness": 0,
        "color": null,
        "texture": "//cdn.easygenerator.com/textures/3.png"
      }
     }
    }
   }
},
{
 "title": "grey",
 "settings": {
  "branding": {
   "logo": {
    "url": "//cdn.easygenerator.com/logo.png"
   },
   "colors": [
    {
     "key": "@text-color",
     "value": "#252728"
    },
    {
     "key": "@main-color",
     "value": "#3b6998"
    },
    {
```

```
    "key": "@secondary-color",
    "value": "#7596b7"
   },
   {
    "key": "@button-text-color",
    "value": "#fff"
   },
   {
    "key": "@content-body-color",
    "value": "#fff"
   }
  ],
  "background": {
   "header": {
    "brightness": 0,
    "color": null,
    "image": {
     "url": "//cdn.easygenerator.com/images/4.jpg",
     "option": "repeat"
    }
   },
   "body": {
    "enabled": true,
    "brightness": 0,
    "color": null,
    "texture": "//cdn.easygenerator.com/textures/16.png"
```

```
        }


      }
     }
    }
  },
  {
   "title": "flat",
   "settings": {
    "branding": {
     "logo": {
      "url": "//cdn.easygenerator.com/logo.png"
     },
     "colors": [
      {
       "key": "@text-color",
       "value": "#252728"
      },
      {
       "key": "@main-color",
       "value": "#46a24a"
      },
      {
       "key": "@secondary-color",
       "value": "#aed580"
      },
```

```
    {
      "key": "@button-text-color",
      "value": "#fff"
    },
    {
      "key": "@content-body-color",
      "value": "#fff"
    }
  ],
  "background": {
    "header": {
      "brightness": 0,
      "color": null,
      "image": {
        "url": "//cdn.easygenerator.com/images/12.jpg",
        "option": "repeat"
      }
    },
    "body": {
      "enabled": true,
      "brightness": 0,
      "color": null,
      "texture": "//cdn.easygenerator.com/textures/2.png"
    }
  }
}
```

```
    }
   }
  ],
  "languages": [
   {
    "code": "cn",
    "url": "lang/cn.json"
   },
   {
    "code": "nl",
    "url": "lang/nl.json"
   },
   {
    "code": "en",
    "url": "lang/en.json"
   },
   {
    "code": "fr",
    "url": "lang/fr.json"
   },
   {
    "code": "de",
    "url": "lang/de.json"
   },
   {
    "code": "it",
```

```
    "url": "lang/it.json"
   },
   {
    "code": "pt-br",
    "url": "lang/pt-br.json"
   },
   {
    "code": "tr",
    "url": "lang/tr.json"
   },
   {
    "code": "es",
    "url": "lang/es.json"
   },
   {
    "code": "ua",
    "url": "lang/ua.json"
   }
  ]
}
```