ΑΕΙ ΠΕΙΡΑΙΑ ΤΤ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «ΕΦΑΡΜΟΣΜΕΝΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σχεδιασμός και Ανάπτυξη Περιβάλλοντος Υποστήριξης Δικτυακών Πειραμάτων

Αρτέμιος Α. Σιγάλας

Εισηγητής: Δρ Γεώργιος Τσελίκης, Καθηγητής

ΑΘΗΝΑ
ΣΕΠΤΕΜΒΡΙΟΣ 2017

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σχεδιασμός και Ανάπτυξη Περιβάλλοντος Υποστήριξης Δικτυακών Πειραμάτων

Αρτέμιος Α. Σιγάλας
Α.Μ. AIS0064

Εισηγητής:

Δρ Γεώργιος Τσελίκης, Καθηγητής

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Αρτέμιος Σιγάλας, του Αντωνίου, με αριθμό μητρώου ais0064 φοιτητής του Τμήματος Μηχανικών Η/Υ Συστημάτων Τ.Ε. του Α.Ε.Ι. Πειραιά Τ.Τ. πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

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

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

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

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό των δικτύων ηλεκτρονικών υπολογιστών. Την προσπάθειά μου αυτή υποστήριξε ο επιβλέπων καθηγητής μου κ. Γεώργιος Τσελίκης, τον οποίο θα ήθελα να ευχαριστήσω.

Θα ήθελα επίσης να ευχαριστήσω, όλους του καθηγητές του μεταπτυχιακού για τις πολύτιμες γνώσεις που μου προσέφεραν.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία ασχολείται με τον σχεδιασμό και την ανάπτυξη περιβάλλοντος υποστήριξης δικτυακών πειραμάτων. Η εφαρμογή παρέχει τη δυνατότητα στο χρήστη να διεξάγει πειράματα με σκοπό να ελέγξει τις γνώσεις και τις ικανότητές του σε θέματα που σχετίζονται με την IP τεχνολογία. Η εφαρμογή μπορεί να αποτελέσει εργαλείο εκμάθησης και ελέγχου των γνώσεων συμμετεχόντων σε παρόμοια προγράμματα.

ABSTRACT

The present thesis concerns the design and development of an integrated environment to support network experiments. The application provides the user with the ability to perform experiments in order to test his knowledge and skills in topics related to the IP technology. The application may be used as a learning tool from candidates who participate in similar programs.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Δίκτυα Ηλεκτρονικών Υπολογιστών
ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Πρωτόκολλα Επικοινωνίας, Διαστρωμάτωση, IP, Πειράματα

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ADCCP	Advanced Data Communication Control Procedures
ASCII	American Standard Code for Information Interchange
EBCDIC	Extended Binary Coded Decimal Interchange Code
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
HDLC	High-Level Data Link Control
HTTP	Hypertext Transfer Protocol
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
MIME	Multipurpose Internet Mail Extensions
OSPF	Open Shortest Path First
PAN	Personal Area Network
SCSI	Small Computer System Interface
SCTP	Stream Control Transmission Protocol
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
XML	Extensible Markup Language

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

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

1.1 Κατηγορίες Δικτύων

Τα δίκτυα κατηγοριοποιούνται :

- Ανάλογα με το φυσικό μέσο διασύνδεσής τους χαρακτηρίζονται ως ενσύρματα ή ασύρματα.
- Ανάλογα με τον τρόπο πρόσβασης σε αυτά χαρακτηρίζονται ως δημόσια ή ιδιωτικά δίκτυα.
- Ανάλογα με την γεωγραφική κάλυψη του δικτύου χαρακτηρίζονται ως τοπικά (LAN και WLAN), μητροπολιτικά (MAN και WMAN), ευρείας κάλυψης (WAN και WWAN) και προσωπικά (PAN και WPAN).

Οι χαρακτηρισμοί με το πρόσθετο W ανταποκρίνονται στον ασύρματο (Wireless) τρόπο σύνδεσης [1].

1.2 Λογισμικό Δικτύων

Στα πλαίσια του λογισμικού των δικτύων, θα εξεταστούν τα εξής:

- Ιεραρχίες πρωτοκόλλων
- Ζητήματα σχεδίασης των επιπέδων
- Συνδεσμοστρεφείς και ασυνδεσμικές υπηρεσίες
- Θεμελιώδεις λειτουργίες υπηρεσιών
- Η σχέση των υπηρεσιών με τα πρωτόκολλα

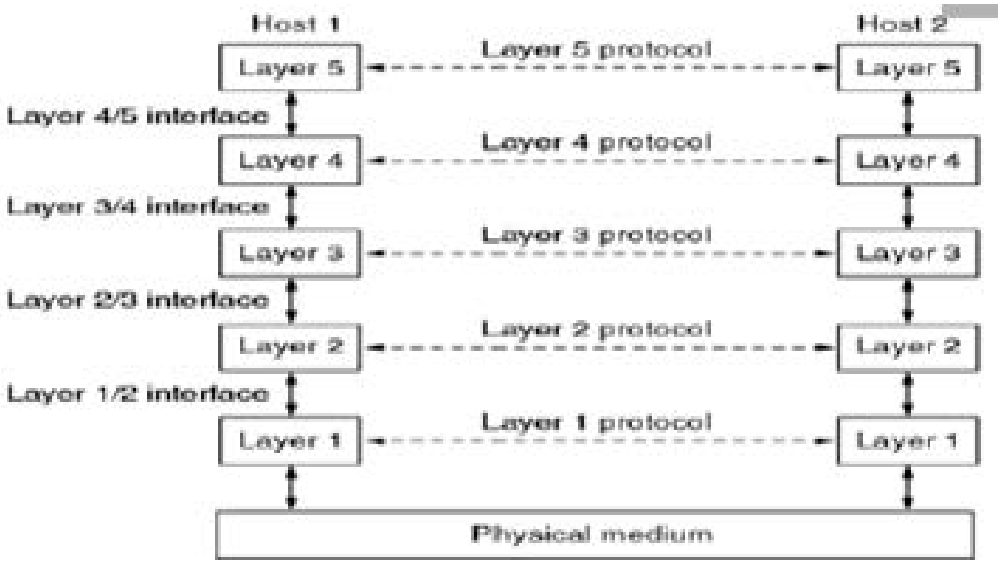
1.2.1 Ιεραρχίες πρωτοκόλλων

Για να μειωθεί η σχεδιαστική τους πολυπλοκότητα, τα περισσότερα δίκτυα οργανώνονται ως μια στοίβα επιπέδων (layers ή levels).

Κάθε επίπεδο προσφέρει ορισμένες υπηρεσίες στα ανώτερα επίπεδα, «κρύβοντας» από τα επίπεδα αυτά τις λεπτομέρειες υλοποίησης των παρεχομένων υπηρεσιών.

Το επίπεδο n σε μια οντότητα (π.χ. υπολογιστής) πραγματοποιεί συνομιλία με το επίπεδο n σε κάποια άλλη οντότητα. Οι κανόνες και οι συμβάσεις που χρησιμοποιούνται σε αυτή τη συνομιλία ονομάζονται συνολικά «πρωτόκολλο του επιπέδου n».

Οι οντότητες που υλοποιούν τα αντίστοιχα επίπεδα ονομάζονται ομότιμες (peers) και επικοινωνούν μεταξύ τους χρησιμοποιώντας το πρωτόκολλο.



Εικόνα 1-1: Ιεραρχία πρωτοκόλλων σε δίκτυο πέντε επιπέδων

Ανάμεσα σε κάθε ζεύγος γειτονικών επιπέδων υπάρχει μια διασύνδεση (interface), η οποία ορίζει τις στοιχειώδεις λειτουργίες και τις υπηρεσίες τις οποίες παρέχει το κατώτερο επίπεδο προς το ανώτερο επίπεδο.

Το σύνολο των επιπέδων και των πρωτοκόλλων ονομάζεται αρχιτεκτονική δικτύου (network architecture), οι προδιαγραφές της οποίας πρέπει να παρέχουν επαρκείς πληροφορίες ώστε να επιτρέπουν την ανάπτυξη/επιλογή λογισμικού/υλικού ώστε να εφαρμόζονται αξιόπιστα τα κατάλληλα πρωτόκολλα.

Οι λεπτομέρειες της υλοποίησης και οι προδιαγραφές των διασυνδέσεων δεν αποτελούν μέρος της αρχιτεκτονικής, αφού είναι κρυμμένες μέσα σε κάθε οντότητα και δεν είναι ορατές από τον έξω κόσμο. [2]

1.2.2 Ζητήματα σχεδίασης των επιπέδων

Κατά την σχεδίαση των επιπέδων προκύπτουν τα παρακάτω ζητήματα:

1. **Διευθυνσιοδότηση** (**Addressing**): μηχανισμός για την αναγνώριση των αποστολέων και των παραληπτών (απαιτείται κάποια μορφή διευθυνσιοδότησης και για τις οντότητες και τις διεργασίες).
2. **Κανόνες μεταφοράς δεδομένων** (**Directions for data transfer**): μονόδρομη (simplex), ημι-αμφίδρομη (half-duplex), πλήρως αμφίδρομη (full-duplex) επικοινωνία.
3. **Λογικά κανάλια (Logical channels):** τουλάχιστον δύο ανά σύνδεση (ένα για κανονικά δεδομένα και ένα για επείγοντα).
4. **Έλεγχος σφαλμάτων (Error control):** και τα δύο άκρα της σύνδεσης πρέπει να συμφωνήσουν στη χρήση των ίδιων κωδικών ανίχνευσης και διόρθωσης σφαλμάτων. Επιπλέον, ο παραλήπτης πρέπει να έχει ένα τρόπο ειδοποίησης του αποστολέα σχετικά με τα μηνύματα που έχει λάβει ορθά και το αντίθετο.
5. **Ακολουθία μηνυμάτων (Message sequencing or ordering):** προφανής λύση είναι να αριθμούνται τα μηνύματα, κάτι που όμως αφήνει ανοικτό το θέμα του τι πρέπει να γίνει με τα μηνύματα που φθάνουν σε εσφαλμένη σειρά.
6. **Έλεγχος ροής (Flow control):** στόχος είναι η αποτροπή του γρήγορου αποστολέα από το να κατακλύσει έναν αργό παραλήπτη με δεδομένα. Συχνά απαιτείται κάποιου είδους ανάδραση από τον παραλήπτη.
7. **Μηχανισμοί κατακερματισμού, μετάδοσης και ανασυναρμολόγησης μηνυμάτων (Mechanisms for disassembling, transmitting, and reassembling messages):** Υπάρχει αδυναμία πολλών διεργασιών να δεχθούν αυθαίρετα μεγάλα μηνύματα. Σχετικό ζήτημα είναι το πρόβλημα του τι πρέπει να γίνεται όταν οι διεργασίες επιμένουν να μεταδίδουν δεδομένα σε τόσο μικρές ομάδες ώστε η χωριστή αποστολή τους να είναι αποτελεσματική.
8. **Πολυπλεξία (Multiplexing):** όταν δεν είναι αποδοτική η εγκαθίδρυση ξεχωριστής σύνδεσης για κάθε ζεύγος διεργασιών που επικοινωνούν, το κατώτερο επίπεδο μπορεί να αποφασίσει να χρησιμοποιήσει την ίδια σύνδεση για πολλές ασυσχέτιστες συνδιαλέξεις (π.χ. λίγα φυσικά κυκλώματα χρησιμοποιούνται για όλες τις εικονικές συνδέσεις).

9. **Δρομολόγηση (Routing):** αφορά την επιλογή της βέλτιστης διαδρομής ανάμεσα στον αποστολέα και τον παραλήπτη. Η απόφαση αυτή συχνά εμπλέκει δύο ή και περισσότερα επίπεδα.

1.2.3 Συνδεσμοστρεφείς και ασυνδεσμικές υπηρεσίες

Η **συνδεσμοστρεφής (connection-oriented)** υπηρεσία έχει ως μοντέλο το τηλεφωνικό σύστημα. Στην ουσία, η σύνδεση δρα ως σωλήνας: ο αποστολέας ωθεί αντικείμενα (bits) από το ένα άκρο και ο παραλήπτης τα λαμβάνει από το άλλο άκρο συνήθως με την ίδια σειρά. Οι συνδεσμοστρεφείς υπηρεσίες είναι κατάλληλες όταν η επικοινωνία μεταξύ δύο μερών έχει μεγάλη διάρκεια.

Η **ασυνδεσμική (connectionless)** υπηρεσία έχει ως μοντέλο το ταχυδρομικό σύστημα. Κάθε μήνυμα φέρει την πλήρη διεύθυνση προορισμού και δρομολογείται ανεξάρτητα. Η σειρά παράδοσης των μηνυμάτων δεν είναι γνωστή/εγγυημένη. Οι ασυνδεσμικές υπηρεσίες είναι κατάλληλες για την αποστολή σύντομων μηνυμάτων [2].

1.2.4 Ποιότητα υπηρεσιών

Αξιόπιστες χαρακτηρίζονται οι υπηρεσίες που δεν χάνουν ποτέ δεδομένα. Αυτό μπορεί να υλοποιηθεί υποχρεώνοντας τον παραλήπτη να επιβεβαιώνει τη λήψη κάθε μηνύματος. Αυτό όμως εισάγει επιπλέον επιβαρύνσεις και καθυστερήσεις στην επικοινωνία, οι οποίες συχνά αξίζουν το κόπο αλλά κάποιες φορές είναι ανεπιθύμητες (αναξιόπιστες υπηρεσίες).

Παραδείγματα

Η αξιόπιστη συνδεσμοστρεφής υπηρεσία είναι κατάλληλη για τη μεταφορά αρχείων, όπου στόχος είναι η έλλειψη σφαλμάτων.

Η αναξιόπιστη συνδεσμοστρεφής υπηρεσία είναι κατάλληλη για τη μετάδοση ψηφιοποιημένης φωνής, όπου οι καθυστερήσεις δεν είναι αποδεκτές.

Η αξιόπιστη ασυνδεσμική υπηρεσία ή υπηρεσία αυτοδύναμων πακέτων με επιβεβαίωση (acknowledged datagram service) είναι κατάλληλη για τη μετάδοση συστημένων e-mails.

Η αναξιόπιστη ασυνδεσμική υπηρεσία ή υπηρεσία αυτοδύναμων πακέτων (datagram service) είναι κατάλληλη για το electronic junk mail (παρέχοντας υψηλή πιθανότητα αλλά όχι και εγγύηση της παράδοσης του μηνύματος).

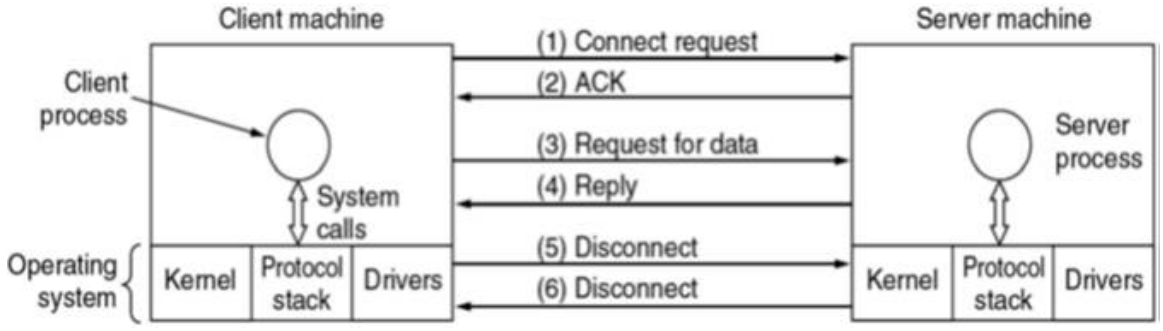
Άλλη μια ασυνδεσμική υπηρεσία είναι η υπηρεσία αίτησης-απάντησης (request-reply), η οποία χρησιμοποιείται συχνά για την υλοποίηση της επικοινωνίας στο μοντέλο client-server.

1.2.5 Θεμελιώδεις λειτουργίες υπηρεσιών

Η υπηρεσία ορίζεται τυπικά με τον προσδιορισμό ενός συνόλου από θεμελιώδεις λειτουργίες (primitives), οι οποίες διατίθενται στις διεργασίες των χρηστών ώστε να προσπελάσουν την υπηρεσία. Αυτές οι θεμελιώδεις λειτουργίες ζητούν από την υπηρεσία είτε να εκτελέσει κάποια ενέργεια, είτε να δώσει αναφορά σχετικά με ενέργεια που έγινε από ομότιμη οντότητα.

Πίνακας 1-1: Πέντε θεμελιώδεις λειτουργίες υπηρεσίας για την υλοποίηση απλής συνδεσμοστραφούς υπηρεσίας

Θεμελιώδης λειτουργία	Σημασία
LISTEN	Μπλοκάρισμα για αναμονή μιας εισερχόμενης σύνδεσης
CONNECT	Εγκαθίδρυση σύνδεσης με ομότιμη οντότητα που βρίσκεται σε αναμονή
RECEIVE	Μπλοκάρισμα για αναμονή εισερχόμενου μηνύματος
SEND	Αποστολή μηνύματος σε ομότιμη οντότητα
DISCONNECT	Τερματισμός σύνδεσης



Εικόνα 1-2: Τα πακέτα που αποστέλλονται σε μια απλή αλληλεπίδραση πελάτη-διακομιστή σε συνδεσμοστρεφές δίκτυο

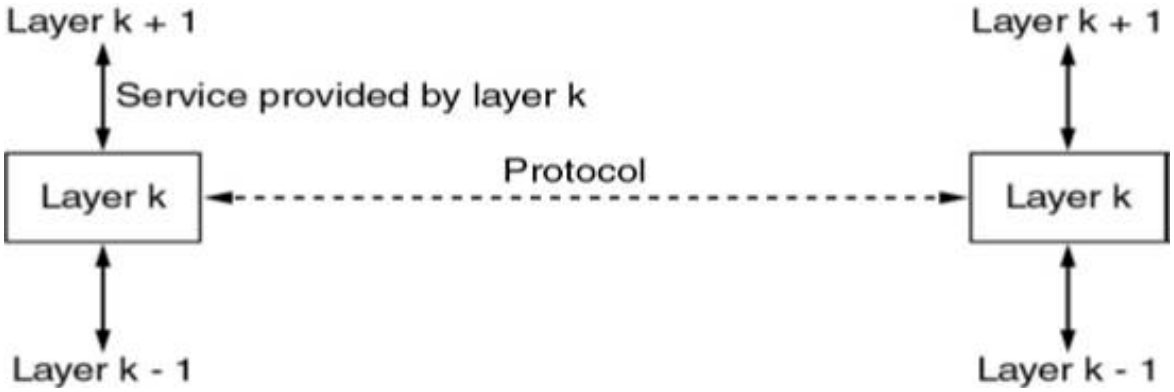
1.2.6 Η σχέση των υπηρεσιών με τα πρωτόκολλα

Οι υπηρεσίες και τα πρωτόκολλα είναι διακριτές έννοιες που δεν πρέπει να συγχέονται.

Η υπηρεσία (service) είναι ένα σύνολο θεμελιωδών λειτουργιών που παρέχονται από ένα επίπεδο στο αμέσως ανώτερο. Η υπηρεσία καθορίζει ποιες

λειτουργίες είναι προετοιμασμένο να εκτελέσει το επίπεδο εκ μέρους των χρηστών του, αλλά δε λέει τίποτα για το πώς υλοποιούνται αυτές.

Το πρωτόκολλο (protocol) είναι ένα σύνολο κανόνων που καθορίζουν τη μορφή και τη σημασία των πακέτων/μηνυμάτων που ανταλλάσσονται μεταξύ των ομότιμων οντοτήτων ενός επιπέδου. Οι οντότητες αυτές χρησιμοποιούν πρωτόκολλα για να υλοποιήσουν τον ορισμό των υπηρεσιών τους. Η αλλαγή του πρωτοκόλλου δεν είναι ορατή στους χρήστες της υπηρεσίας, καθώς η υπηρεσία παραμένει η ίδια.



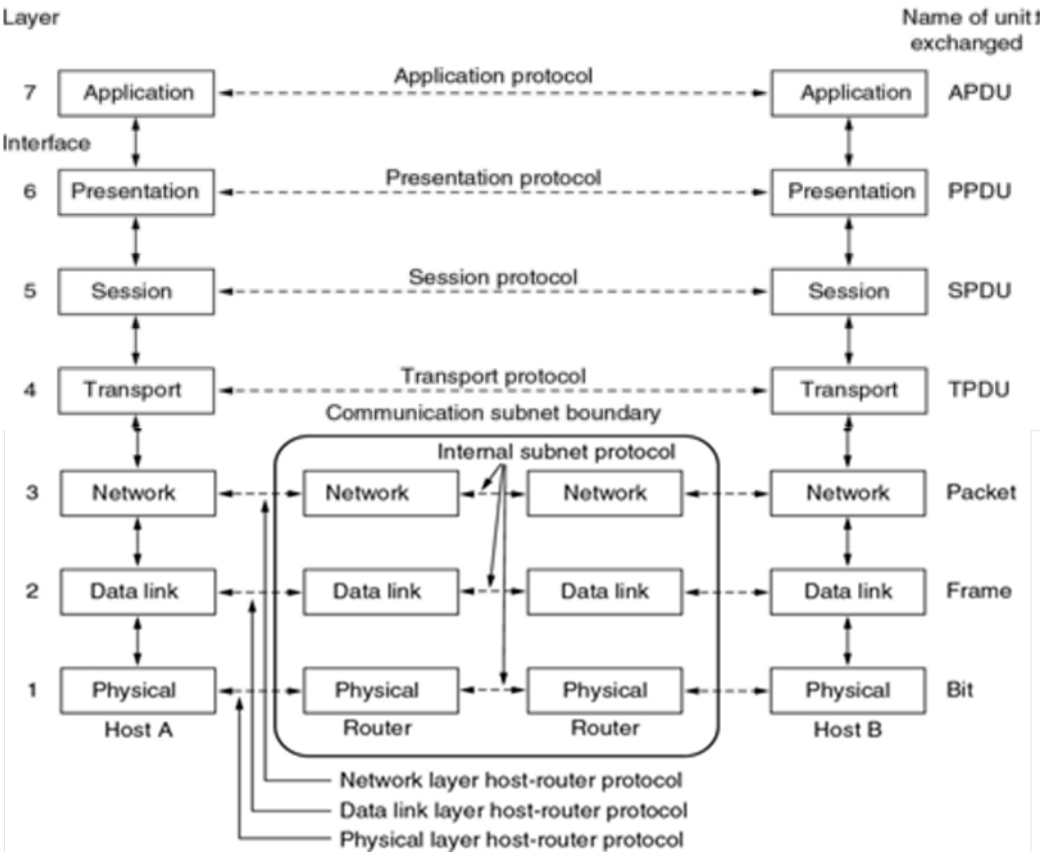
Εικόνα 1-3: Σχέση ανάμεσα σε μία υπηρεσία και ένα πρωτόκολλο

1.3 Μοντέλα Αναφοράς

Το μοντέλο αναφοράς OSI και το μοντέλο αναφοράς TCP/IP είναι δύο σημαντικές αρχιτεκτονικές δικτύων. Τα πρωτόκολλα που σχετίζονται με το μοντέλο OSI πλέον χρησιμοποιούνται σπάνια ενώ επειδή είναι αρκετά γενικό εξακολουθεί να είναι έγκυρο. Το μοντέλο TCP/IP έχει ευρεία εφαρμογή, κυρίως σε IP δίκτυα.

1.3.1 Το μοντέλο αναφοράς OSI

Το μοντέλο OSI βασίζεται σε μια πρόταση, που ανέπτυξε ο Οργανισμός Διεθνών Προτύπων ISO, ως ένα πρώτο βήμα προς την κατεύθυνση της διεθνούς προτυποποίησης των πρωτοκόλλων που χρησιμοποιούνται στα διάφορα στρώματα. Το μοντέλο αποκαλείται μοντέλο αναφοράς OSI (Open Systems Interconnection) του ISO, επειδή αφορά ανοικτά συστήματα, δηλαδή συστήματα ανοικτά στην επικοινωνία με άλλα συστήματα.



Εικόνα 1-4: Το μοντέλο αναφοράς OSI

Το μοντέλο αυτό έχει επτά στρώματα καθένα από τα οποία εκτελεί συγκεκριμένες λειτουργίες και επικοινωνεί με τα επίπεδα που είναι ακριβώς από πάνω και από κάτω του. Τα ανώτερα επίπεδα ασχολούνται κυρίως με τις υπηρεσίες, εφαρμογές και δραστηριότητες χρηστών και τα κατώτερα στρώματα ασχολούνται κυρίως με την μετάδοση των δεδομένων. Αυτά είναι από πάνω προς τα κάτω:

Επίπεδο 7: Εφαρμογών (applicatıon layer)

Το επίπεδο εφαρμογών παρέχει στον χρήστη τη δυνατότητα να επικοινωνήσει με άλλους δικτυακούς χρήστες μέσω κατάλληλων εφαρμογών (π.χ. εφαρμογή ηλεκτρονικού ταχυδρομείου, εφαρμογή μεταφοράς αρχείων, πλοηγός Διαδικτύου). [3]

Επίπεδο 6: Παρουσίασης (presentation layer)

Το επίπεδο παρουσίασης μετασχηματίζει τα δεδομένα στη μορφή που την αναμένει το επίπεδο εφαρμογών. Στο επίπεδο αυτό τα δεδομένα υφίστανται

κρυπτογράφηση, συμπίεση, κωδικοποίηση και όποια άλλη διαμόρφωση απαιτεί η μορφή δεδομένων ή ο σχεδιαστής του πρωτοκόλλου. [3]

Επίπεδο 5: Συνόδου (session layer)

Το επίπεδο συνόδου ελέγχει τις συνόδους (δηλαδή τις ανταλλαγές δεδομένων) μεταξύ δύο υπολογιστών, του Α και του Β. Εγκαθιστά, διαχειρίζεται και τερματίζει τη σύνδεση μεταξύ μιας τοπικής και μιας απομακρυσμένης εφαρμογής. [3]

Επίπεδο 4: Μεταφοράς (transport layer)

Το επίπεδο μεταφοράς διεκπεραιώνει τη μεταφορά των δεδομένων από χρήστη σε χρήστη, απαλλάσσοντας έτσι τα ανώτερα επίπεδα από κάθε ευθύνη να παρέχουν 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). [3]

Επίπεδο 3: Δικτύου (network layer)

Το επίπεδο δικτύου παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά δεδομένων μεταβλητού μήκους από τον αποστολέα στον 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. [3]

Επίπεδο 2: Ζεύξης Δεδομένων (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. [3]

Επίπεδο 1: Φυσικό (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). [3]

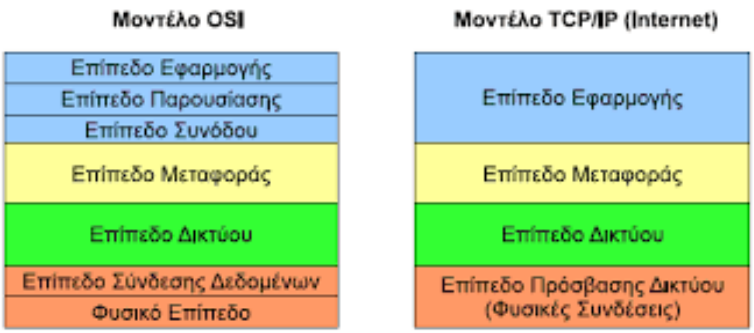
1.3.2 Το μοντέλο αναφοράς TCP/IP

Βασικοί στόχοι σχεδίασης του μοντέλου TCP/IP είναι:

1. Η ικανότητα διασύνδεσης πολλών δικτύων με διαφανή τρόπο.
2. Η ικανότητα επιβίωσης μετά από απώλεια στο υλικό του υποδικτύου, χωρίς να τερματίζονται οι υπάρχουσες συνομιλίες.
3. Μια ευέλικτη αρχιτεκτονική που να υποστηρίζει διαφορετικές και αποκλίνουσες απαιτήσεις, από μεταφορά αρχείων έως μετάδοση ομιλίας σε πραγματικό χρόνο.

Όλοι οι παραπάνω στόχοι οδήγησαν στην επιλογή ενός δικτύου μεταγωγής πακέτων (packet-switching) βασιζόμενο σε ένα ασυνδεσμικό επίπεδο διαδικτύου, που ονομάζεται internet layer.

Εικόνα 1-5: Το μοντέλο αναφοράς TCP/IP



Εικόνα 1-6: OSI και TCP/IP

Επίπεδο 4: Εφαρμογής

Το επίπεδο εφαρμογής χρησιμοποιείται από την πλειοψηφία των δικτυομένων προγραμμάτων. Το πρόγραμμα παραδίδει τα δεδομένα σε μια μορφή που ορίζει το ίδιο.

Εφ' όσον το TCP/IP δεν παρέχει επίπεδα μεταξύ των επιπέδων εφαρμογής και μεταφοράς, όλες οι λειτουργίες παρουσίασης και συνεδρίας (μοντέλο OSI) πρέπει να υλοποιηθούν σ' αυτό το επίπεδο. Αυτή η διαδικασία διευκολύνεται με τη χρήση βιβλιοθηκών . [4]

Επίπεδο 3: Μεταφοράς

Το επίπεδο μεταφοράς είναι υπεύθυνο για την μεταφορά μηνυμάτων, ανεξαρτήτως του υποκείμενου δικτύου, με έλεγχο σφαλμάτων (error control), κατάτμηση (fragmentation) και ρύθμιση ροής (flow control). Η μετάδοση μηνυμάτων μεταξύ δυο οντοτήτων μπορεί να κατηγοριοποιηθεί ως εξής:

- Συνδεσμοστρεφείς (connection-oriented), π.χ. TCP
- Ασυνδεσμικές (connectionless), π.χ. UDP

Η λειτουργία του επιπέδου αυτού μπορεί να συγκριθεί με αυτή οποιουδήποτε μηχανισμού - μέσου μεταφοράς, π.χ. ένα όχημα που πρέπει να εξασφαλίζει την πλήρη και ασφαλή διακίνηση του φορτίου του. Το επίπεδο μεταφοράς παρέχει αυτή την υπηρεσία σύνδεσης εφαρμογών μεταξύ τους, κάνοντας χρήση θυρών (ports). Καθώς το IP προσφέρει μόνο παράδοση όσο το δυνατόν καλύτερα (best effort delivery), το επίπεδο μεταφοράς είναι το πρώτο επίπεδο όπου λαμβάνεται υπόψιν το θέμα της αξιοπιστίας. [4]

Επίπεδο 2: Δικτύου

Ο σκοπός του επιπέδου δικτύου είχε αρχικά καθοριστεί ως η μεταφορά πακέτων μέσω ενός ενιαίου δικτύου.

Με την εμφάνιση πιο σύνθετων μορφών δικτύων, προστέθηκαν επιπλέον χαρακτηριστικά στο επίπεδο αυτό, έτσι ώστε ο ρόλος του να είναι πια η διακίνηση δεδομένων από το δίκτυο-αποστολέα στο δίκτυο-παραλήπτη. Αυτό προϋποθέτει συνήθως τη δρομολόγηση πακέτων διαμέσου ενός δικτύου δικτύων (internetwork).

Στην σουίτα πρωτοκόλλων Διαδικτύου, το IP μεταφέρει τα πακέτα δεδομένων από τον αποστολέα στον παραλήπτη. Το IP μπορεί να εξυπηρετήσει διάφορα πρωτόκολλα ανωτέρων επιπέδων (upper layer protocols), το καθένα τους προσδιορίζεται με έναν αποκλειστικό αριθμό πρωτοκόλλου: π.χ. το ICMP και το IGMP έχουν τους αριθμούς 1 και 2 αντίστοιχα. [4]

Επίπεδο 1: Διασύνδεσης Δικτύου

Το επίπεδο αυτό, ρόλος του οποίου είναι η διακίνηση πακέτων του επιπέδου δικτύου μεταξύ δυο οντοτήτων, δεν είναι στην ακρίβεια μέρος της σουίτας πρωτοκόλλων Διαδικτύου, διότι το IP λειτουργεί με διάφορα επίπεδα συνδέσμου. Η διαδικασία διαβίβασης πακέτων σε ένα συγκεκριμένο επίπεδο συνδέσμου μπορεί να ελέγχεται είτε από τον οδηγό του interface, είτε το firmware ή σύνολο εξειδικευμένων κυκλωμάτων (chipsets), είτε τέλος από ένα συνδυασμό των προαναφερθέντων. Αυτά θα εκτελέσουν τις λειτουργίες σύνδεσης δεδομένων (data link), όπως π.χ. την πρόσθεση επικεφαλίδας (packet header) πριν την αποστολή, την ίδια τη διαβίβαση του πλαισίου (frame) με τη χρήση ενός φυσικού μέσου.

Το επίπεδο συνδέσμου είναι επίσης το επίπεδο όπου τα πακέτα μπορούν να αναχαιτιστούν για να σταλθούν σ' ένα Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network, VPN). Σ' αυτήν την περίπτωση, τα δεδομένα του επιπέδου αυτού αντιμετωπίζονται ως δεδομένα εφαρμογής, και "ξανακατεβαίνουν" τη στοίβα πρωτοκόλλων Διαδικτύου για να σταλθούν. Στη λαμβάνουσα πλευρά, τα δεδομένα ανεβαίνουν δυο φορές τη στοίβα (μια για το VPN και μια δεύτερη για τη δρομολόγηση).

Το φυσικό επίπεδο, που αποτελείται από τα φυσικά στοιχεία του δικτύου (π.χ. hubs, repeaters, καλώδια δικτύου, οπτικές ίνες, ομοαξονικά καλώδια, κάρτες δικτύων) και τις προδιαγραφές χαμηλού επιπέδου των σημάτων (τάση, συχνότητα, κλπ.), θεωρείται συχνά ως μέρος του επιπέδου συνδέσμου. [4]

1.3.3 Σύγκριση των μοντέλων αναφοράς OSI και TCP/IP

Θεμελιώδεις ομοιότητες και διαφορές των μοντέλων OSI και TCP/IP

Και τα δύο μοντέλα βασίζονται στην έννοια της στοίβας ανεξαρτήτων πρωτοκόλλων.

Η λειτουργικότητα των επιπέδων είναι σε γενικές γραμμές η ίδια.

Στο επίκεντρο του μοντέλου OSI βρίσκονται τρεις έννοιες:

1. Υπηρεσίες: οι οποίες καθορίζουν τι κάνει το επίπεδο και όχι πώς γίνεται η προσπέλασή του από τα ανώτερα επίπεδα ή πώς αυτό δουλεύει.
2. Διασυνδέσεις: οι οποίες δηλώνουν στις διεργασίες που βρίσκονται στο αμέσως ανώτερο επίπεδο πώς να το προσπελάσουν (ήτοι, προσδιορίζει ποιες είναι οι παράμετροι και τα αναμενόμενα αποτελέσματα), ενώ δεν περιλαμβάνει τίποτα σχετικά με τον τρόπο εσωτερικής λειτουργίας του επιπέδου.
3. Πρωτόκολλα: τα οποία χρησιμοποιούνται μεταξύ ομότιμων οντοτήτων για να υλοποιηθούν οι παρεχόμενες υπηρεσίες, ενώ αφορούν μόνο ένα επίπεδο.

Το μοντέλο OSI έκανε σαφή τη διάκριση ανάμεσα στις τρεις αυτές έννοιες. Το μοντέλο TCP/IP δεν παρέχει κάποιον αντίστοιχο σαφή διαχωρισμό.

Το μοντέλο OSI επινοήθηκε πριν σχεδιαστούν τα αντίστοιχα πρωτόκολλα, ενώ ακριβώς το αντίθετο ισχύει για το μοντέλο TCP/IP.

Το μοντέλο OSI έχει επτά επίπεδα, ενώ το μοντέλο TCP/IP έχει μόνο τέσσερα.

Το μοντέλο OSI υποστηρίζει και συνδεσμοστρεφή και ασυνδεσμική επικοινωνία στο επίπεδο δικτύου, αλλά μόνον συνδεσμοστρεφή στο επίπεδο μεταφοράς. Το μοντέλο TCP/IP έχει μόνον έναν τρόπο λειτουργίας στο επίπεδο διαδικτύου (ασυνδεσμικό), αλλά υποστηρίζει και τους δύο τρόπους λειτουργίας στο επίπεδο μεταφοράς.

1.3.4 Παραδείγματα δικτύων

1.3.4.1 Το Internet

ARPANET

Το ARPANET αποτελεί δημιούργημα της ARPA (Advanced Research Projects Agency) του υπουργείου Εθνικής Αμύνης των Η.Π.Α.

Μεγάλο μέρος της τρέχουσας γνώσης μας σχετικά με τα δίκτυα υπολογιστών οφείλεται και αποτελεί άμεσο επακόλουθο του προγράμματος ARPANET.

Οι τεχνολογίες που χρησιμοποιήθηκαν στο ARPANET ήταν:

1. Μίνι υπολογιστές ονόματι: Επεξεργαστές Μηνυμάτων Διασύνδεσης ή IMP (Interface Message Processor).
2. Οι IMPs ήταν συνδεδεμένοι με γραμμές μετάδοσης των 56 kbps ή 230.4 kbps (μισθωμένες γραμμές). Αρχικά, κάθε IMP μπορούσε να υποστηρίξει από έναν έως τέσσερεις hosts, ενώ στη συνέχεια δεκάδες hosts και εκατοντάδες τερματικά ταυτόχρονα. [2]

TCP/IP

Το TCP/IP σχεδιάστηκε ειδικά για να χειρίζεται την επικοινωνία πάνω από διαδίκτυα, ιδιαίτερα για να αντιμετωπίσει τον τεράστιο αριθμό δικτύων που συνδέονταν με το ARPANET.

Για να διευκολυνθεί η ανεύρεση hosts στο ARPANET, δημιουργήθηκε το Σύστημα Ονομάτων Περιοχής ή DNS (Domain Name System) με στόχο να οργανώσει τις μηχανές σε περιοχές και να αντιστοιχίσει τα ονόματα των υπολογιστών υπηρεσίας σε διευθύνσεις IP. [2]

NSFNET

Στα τέλη της δεκαετίας του 1970, η NSF (National Science Foundation) των Η.Π.Α. δημιούργησε το NSFNET για να παράσχει υπηρεσίες δικτύωσης σε όλη την επιστημονική κοινότητα των Η.Π.Α. (και ιδιαίτερα σε αυτούς που δεν είχαν πρόσβαση στο ARPANET, κάτι που απαιτούσε τη σύναψη κάποιου ερευνητικού συμβολαίου με το DoD).

Το NSFNET χτίστηκε γύρω από ένα μηχάνημα (NSFNET-RELAY) στο BBN το οποίο υποστήριζε γραμμές dial-up (PHONENET) και είχε συνδέσεις με το ARPANET και άλλα δίκτυα (π.χ., X.25, CYPRESS).

Στις υπηρεσίες που προσέφερε περιλαμβάνονται: το ηλεκτρονικό ταχυδρομείο (e-mails), η μεταφορά αρχείων (file transfer) και η τηλεσύνδεση (remote login).

Internet

Μετά τη διασύνδεση του ARPANET με το NSFNET (χρησιμοποιώντας το TCP/IP ως το μοναδικό επίσημο πρωτόκολλο), πολλά περιφερειακά δίκτυα συνδέθηκαν ανά τον κόσμο.

Κάπου στα μέσα της δεκαετίας του 1980, ο κόσμος άρχισε να αντιμετωπίζει αυτή τη συλλογή δικτύων σαν ένα διαδίκτυο και αργότερα σαν το Διαδίκτυο ή Internet.

Τον Ιανουάριο του 1992, συστάθηκε η Internet Society με στόχο να προωθήσει τη χρήση του Internet.

Ο συνδετικός ιστός του Internet είναι το μοντέλο αναφοράς TCP/IP και η στοίβα πρωτοκόλλων TCP/IP.

Έτσι όταν μια μηχανή είναι συνδεδεμένη στο Internet σημαίνει ότι:

- τρέχει τη στοίβα πρωτοκόλλων TCP/IP,
- έχει μια διεύθυνση IP και
- έχει την ικανότητα να στέλνει πακέτα IP σε όλες τις άλλες μηχανές στο Internet. [2]

1.3.4.2 Ethernet

Το **ethernet** είναι το συνηθέστερα χρησιμοποιούμενο πρότυπο δίκτυο υπολογιστών ενσύρματης τοπικής δικτύωσης υπολογιστών. Αναπτύχθηκε από την εταιρεία Xerox κατά τη δεκαετία του '70 και έγινε δημοφιλές αφότου η Digital Equipment Corporation και η Intel, από κοινού με τη Xerox, προχώρησαν στην προτυποποίησή του το 1980. Το 1985 το Ethernet έγινε αποδεκτό επίσημα από τον οργανισμό IEEE ως το πρότυπο 802.3 για ενσύρματα τοπικά δίκτυα (LAN).

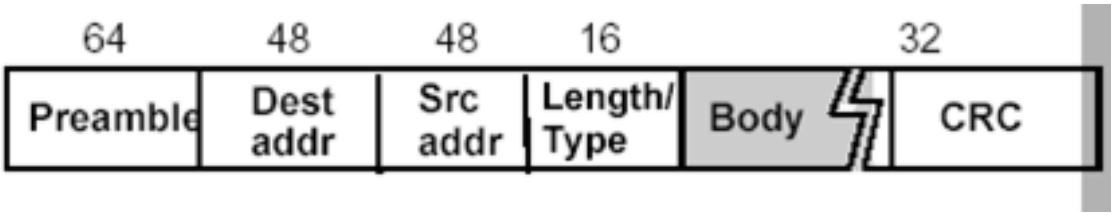
Το αρχικό Ethernet επέτρεπε ονομαστικούς ρυθμούς μετάδοσης δεδομένων της τάξης των 3 Mbps, μέσω ενός ομοαξονικού καλωδίου στο οποίο συνδέονταν οι επιμέρους υπολογιστές του δικτύου (σύνδεση token ring). Τη διασύνδεση αναλάμβανε μία κάρτα δικτύου Ethernet προσαρτημένη σε κάθε κόμβο, με κάθε κάρτα να χαρακτηρίζεται από μία μοναδική, εργοστασιακή 48-bit διεύθυνση MAC. Σήμερα η σύνδεση token ring έχει εγκαταλειφθεί ολοκληρωτικά και οι επιμέρους

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

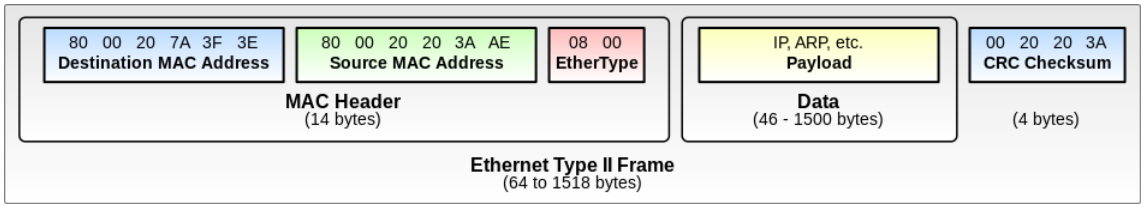
- **Ethernet** (10MBps)
- **Fast Ethernet** (100 Mbps)
- **Gigabit Ethernet** (1 Gbps)
- **10 Gigabit Ethernet** (10Gbps)

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

Πρακτικά, το Ethernet χρησιμοποιεί τη μέθοδο μετάδοσης δεδομένων σε μορφή πακέτων (packet switching) μέγιστου μεγέθους (Maximum Transmission Unit, MTU) 1500 bytes και ελάχιστου 46 bytes. Για το σκοπό αυτό, δεδομένα με μήκος μεγαλύτερο των 1500 bytes κατατέμνονται σε πακέτα των 46-1500 bytes (το λεγόμενο payload) τα οποία αποστέλλονται διαδοχικά στη γραμμή επικοινωνίας. Αν το payload έχει μήκος μικρότερο των 46 bytes, προστίθενται επιπλέον κενά bytes ώστε αυτό να αποκτήσει το επιθυμητό ελάχιστο μήκος. Επιπλέον του payload, προστίθενται πληροφορίες όπως ο σειριακός αριθμός της κάρτας Ethernet, οι φυσικές διευθύνσεις (MAC addresses) αποστολέα και παραλήπτη, το μήκος του payload, καθώς και δεδομένα για έλεγχο σφαλμάτων κατά τη μετάδοση. [5]



Εικόνα 1-7: Ethernet πλαίσιο (frame format)



Εικόνα 1-8: Ethernet II

Διεύθυνση MAC

Μία διεύθυνση Media Access Control - ελέγχου προσπέλασης στο μέσο (διεύθυνση MAC), που καλείται επίσης και φυσική διεύθυνση ή διεύθυνση υλικού, είναι μία μοναδική ταυτότητα που αποδίδεται στις διασυνδέσεις δικτύου (network interfaces) για την επικοινωνία στο φυσικό τμήμα του δικτύου. Οι διευθύνσεις MAC χρησιμοποιούνται σαν διευθύνσεις δικτύου στις περισσότερες IEEE 802 τεχνολογίες δικτύου, συμπεριλαμβανομένων του Ethernet και του WIFI. Οι διευθύνσεις MAC χρησιμοποιούνται στο υποεπίπεδο ελέγχου πρόσβασης στο μέσο (media access control) του μοντέλου αναφοράς OSI.

Οι διευθύνσεις MAC αποδίδονται από τον κατασκευαστή του ελεγκτή διασύνδεσης στο δίκτυο (Network Interface Controller, NIC), έχουν μήκος 48 bits (6 Bytes) και αποθηκεύονται στο hardware της διασύνδεσης στη ROM (μνήμη μόνο ανάγνωσης).

ΚΕΦΑΛΑΙΟ 2

ΠΡΩΤΟΚΟΛΛΑ IP ΤΕΧΝΟΛΟΓΙΑΣ

2.1 Πρωτόκολλα

2.1.1 Internet Protocol

Το Πρωτόκολλο Διαδικτύου (IP) , αποτελεί το κύριο πρωτόκολλο επικοινωνίας για τη μετάδοση δεδομενογραμμάτων (datagrams), δηλαδή πακέτων δεδομένων, σε ένα διαδίκτυο, και είναι τμήμα της Σουίτας Πρωτοκόλλων Διαδικτύου. Το Πρωτόκολλο IP είναι υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων ανάμεσα στα διάφορα δίκτυα, ανεξάρτητα από την υποδομή τους, και αποτελεί το κύριο πρωτόκολλο πάνω στο οποίο είναι βασισμένο το Διαδίκτυο.

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

Το Πρωτόκολλο IP εισήχθη από τους Vint Cerf και Bob Kahn το 1974. Συνδέεται στενά με το Πρωτόκολλο Ελέγχου Μετάδοσης (TCP), με αποτέλεσμα ολόκληρη η σουίτα των πρωτοκόλλων του Διαδικτύου να αναφέρεται απλά ως σουίτα TCP/IP.

Η πρώτη μεγάλης κλίμακας έκδοση του Πρωτοκόλλου IP, ήταν η έκδοση 4 (IPv4) η οποία επικρατεί μέχρι και σήμερα σε όλο το Διαδίκτυο. Ωστόσο, λόγω του ότι δεν επαρκούν πλέον οι διευθύνσεις, τα τελευταία χρόνια, έχει αναπτυχθεί η διάδοχη έκδοση του πρωτοκόλλου, η έκδοση 6 (IPv6), η οποία είναι εν ενεργεία και χρησιμοποιείται εξαπλωνόμενη σε όλο τον κόσμο. Οι τελευταίες διευθύνσεις IPv4 παραδόθηκαν σε ειδική τελετή, στις 3 Φεβρουαρίου του 2011, στο Μαϊάμι.

Υπηρεσίες του Πρωτοκόλλου IP

Το Πρωτόκολλο IP, είναι υπεύθυνο για τη διευθυνσιοδότηση των κόμβων και την δρομολόγηση των πακέτων από έναν υπολογιστή προς έναν τελικό προορισμό, κατά μήκος ενός ή περισσότερων δικτύων. Για το σκοπό αυτό, το

πρωτόκολλο IP, καθορίζει ένα σύστημα διευθυνσιοδότησης, το οποίο έχει δύο λειτουργίες. Έτσι κάθε πακέτο IP, αποτελείται από μια κεφαλίδα και στη συνέχεια ακολουθούν τα δεδομένα. Στη κεφαλίδα αυτή εμπεριέχονται πληροφορίες: πρώτον, για τα δεδομένα που εμπεριέχονται στο πακέτο και δεύτερον, οι διευθύνσεις αφετηρίας και προορισμού. Η διαδικασία προσθήκης της κεφαλίδας σε ένα πακέτο δεδομένων ονομάζεται ενθυλάκωση.

Το Πρωτόκολλο IP είναι μια υπηρεσία χωρίς σύνδεση, είναι ανεξάρτητο από την τεχνολογία του υλικού, που χρησιμοποιείται σε κάθε δίκτυο, και δεν χρειάζεται να την γνωρίζει πριν την μετάδοση.

Αξιοπιστία

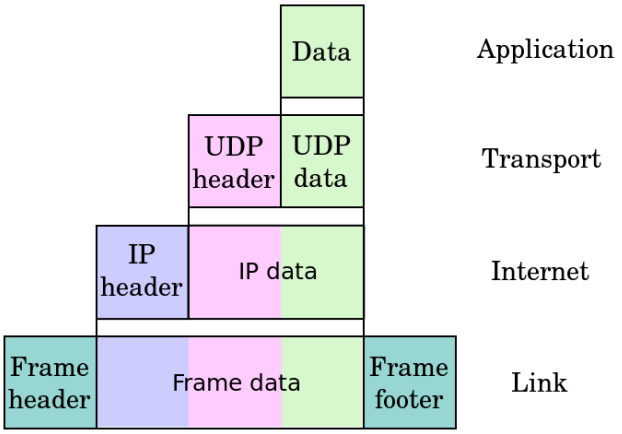
Εκτός από τον ορισμό της μορφής των αυτοδύναμων πακέτων, το Πρωτόκολλο IP ορίζει τη σημασιολογία της επικοινωνίας, και χρησιμοποιεί τον όρο βέλτιστη προσπάθεια, για να περιγράψει την υπηρεσία που παρέχει. Ουσιαστικά το πρότυπο αυτό ορίζει, ότι παρ' όλο που το πρωτόκολλο IP κάνει τη βέλτιστη δυνατή προσπάθεια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

- Αλλοίωση δεδομένων
- Απώλεια αυτοδύναμου πακέτου
- Επανάληψη αυτοδύναμου πακέτου
- Επίδοση με καθυστέρηση ή εκτός σειράς.

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

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

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



Εικόνα 2-1: Ενθυλάκωση των δεδομένων (πράσινο χρώμα) μιας εφαρμογής

Μορφή Πακέτου

Ένα IP πακέτο αποτελείται από το τμήμα της επικεφαλίδας και το τμήμα δεδομένων.

Επικεφαλίδα

Η επικεφαλίδα στο IPv4 αποτελείται από 14 πεδία, από τα οποία τα 13 είναι απαραίτητα. Το 14 πεδίο είναι προαιρετικό (με το κόκκινο φόντο στον πίνακα) και ονομάζεται: Επιλογές. Τα πεδία στην επικεφαλίδα πακετάρονται με το περισσότερο σημαντικό πεδίο εμπρός και για το διάγραμμα και τη συζήτηση, τα περισσότερο σημαντικά bit βρίσκονται μπροστά. Έτσι το 0 είναι το “περισσότερο σημαντικό bit” MSB), έτσι ‘ώστε για παράδειγμα το πεδίο «έκδοση» βρίσκεται στα 4 περισσότερο σημαντικά bit του πρώτου Byte.

Μορφή Επικεφαλίδας +IPv4																															
Offsets	**Octet**	**0**								**1**								**2**								**3**							
Octet	**Bit**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
0	**0**	*Έκδοση*				*IHL*				*DSCP*						*ECN*		*Συνολικό Μήκος*															
4	**32**	*Αναγνώριση*																*Flags*			*Δείκτης Εντοπισμού Τμήματος*											
8	**64**	*Χρόνος Ζωής*								*Αριθμός Πρωτοκόλλου*								*Άθροισμα Ελέγχου Επικεφαλίδας*															
12	**96**	*IP Διεύθυνση Πηγής*																															
16	**128**	*IP Διεύθυνση Προορισμού*																															
20	**160**	*IP Επιλογές (Εάν Μήκος Επικεφαλίδας > 5)*																															

Εικόνα 2-2: IP Επικεφαλίδα

Έκδοση

Το πρώτο πεδίο της επικεφαλίδας σε ένα IP πακέτο είναι το πεδίο της έκδοσης του πρωτοκόλλου, μήκους 4-bit. Για το IPv4 αυτό έχει την τιμή 4 (απ' όπου και προέρχεται το όνομα IPv4)

Μήκος Επικεφαλίδας (IHL)

Το δεύτερο πεδίο (4-bits) είναι το μήκος της επικεφαλίδας (IHL, Internet Header Length). Αυτό μας δίνει το μήκος της επικεφαλίδας σε λέξεις των 32 bit. Επειδή η επικεφαλίδα του IPv4 μπορεί να περιέχει μεταβλητό αριθμό επιλογών, αυτό το πεδίο παρέχει το μήκος της επικεφαλίδας. Η μικρότερη τιμή του πεδίου είναι 5 (RFC 791), που σημαίνει ότι το μήκος είναι 5×32 = 160 bits = 20 bytes. Επειδή το πεδίο είναι 4 bit, το μέγιστο μήκος είναι 24-1=15 λέξεις (15×32 bits) ή 480 bits = 60 bytes.

Συνολικό Μήκος

Το πεδίο αυτό έχει μήκος16-bits. Καθορίζει το συνολικό μήκος του κομματιού (fragment) σε bytes, συμπεριλαμβανομένων της επικεφαλίδας και των δεδομένων. Το ελάχιστο μήκος του πακέτου είναι 20 bytes (20 bytes επικεφαλίδα +0 bytes δεδομένα) και το μέγιστο μήκος είναι 216-1=65535 bytes, καθότι το μήκος του πεδίου Συνολικό Μήκος είναι 16 bits.

Διάφορες συσκευές και μερικές φορές τα υποδίκτυα μπορεί να επιβάλλουν περιορισμούς στο μέγεθος των αυτοδύναμων πακέτων, τα οποία σ' αυτήν την περίπτωση πρέπει να σπάσουν σε μικρότερα κομμάτια. Στο IPv4 η διάσπαση μπορεί να γίνει στους σταθμούς εργασίας ή στους δρομολογητές.

Αναγνώριση

Το πεδίο αυτό είναι ένα πεδίο ταυτότητας και χρησιμεύει για τον μοναδικό προσδιορισμό των κομματιών (fragments) που ανήκουν στο ίδιο αρχικό IP αυτοδύναμο πακέτο.

Σημαίες (Flags)

Αυτό είναι ένα πεδίο των τριών bit και χρησιμεύει να ελέγχει ή να προσδιορίζει τα κομμάτια. Αυτά είναι (κατά σειρά από το περισσότερο σημαντικό προς το λιγότερο):

- bit 0: Δεσμευμένο, πρέπει να είναι 0
- bit 1: Απαγόρευσης διάσπασης του αυτοδύναμου πακέτου (DF=Don't Fragment)
- bit 2:Ένδειξης ύπαρξης περισσότερων κομματιών (MF=More Fragments)

Εάν η σημαία DF έχει τεθεί στο 1 και για την δρομολόγηση του πακέτου είναι απαραίτητη η διάσπασή του, τότε το πακέτο απορρίπτεται. Αυτό θα μπορούσε να χρησιμοποιηθεί κατά την αποστολή πακέτων σε σταθμούς εργασίας, οι οποίοι δεν έχουν επαρκείς πόρους για τον χειρισμό της διάσπασης. Επίσης μπορεί να χρησιμοποιηθεί για την αυτόματη ανίχνευση της Μέγιστης Μονάδας Μεταφοράς κατά Μήκος της Διαδρομής (Path MTU Discovery) είτε αυτόματα από το software των σταθμών εργασίας, είτε χειροκίνητα με την χρήση διαγνωστικών εργαλείων, όπως τα ping και traceroute. Σε πακέτα που δεν έχουν διασπαστεί η σημαία MF είναι 0. Για διασπασμένα πακέτα όλα τα κομμάτια έχουν το MF=1, εκτός από το τελευταίο πού έχει το MF=0. Το τελευταίο κομμάτι έχει μη μηδενικό πεδίο Δείκτη εντοπισμού τμήματος, το οποίο το διακρίνει από ακκομάτιαστα πακέτα.

Δείκτης εντοπισμού τμήματος

Ο δείκτης εντοπισμού τμήματος είναι 13-bit και απαριθμεί σε οκτάδες Byte. Προσδιορίζει την θέση ενός συγκεκριμένου κομματιού, από την αρχή του αρχικού ακκομάτιαστου αυτοδύναμου πακέτου. Το πρώτο κομμάτι έχει δείκτη εντοπισμού τμήματος 0. Αυτό επιτρέπει έναν μέγιστο αριθμό θέσεων (213 – 1) × 8 = 65,528 bytes, το οποίο και ξεπερνά το μέγιστο μήκος του IP πακέτου, που είναι 65535 bytes, εάν συμπεριλάβουμε και το μήκος της επικεφαλίδας (65,528 + 20 = 65,548 bytes).

Χρόνος Ζωής

Το πεδίο αυτό οριοθετεί το χρόνο ζωής του αυτοδύναμου πακέτου. Έχει μήκος 8 bit και χρησιμεύει στο να καταστρέφονται αυτοδύναμα πακέτα που για

διάφορους λόγους περιφέρονται άσκοπα στο Internet. Δίνεται σε δευτερόλεπτα, αλλά χρόνοι μικρότεροι από 1s στρογγυλεύονται στο 1 s. Στην πράξη έχει καταντήσει μετρητής αναπηδήσεων: Όταν ένα αυτοδύναμο πακέτο φτάσει σε έναν δρομολογητή, ο δρομολογητής μειώνει το πεδίο TTL κατά 1. Όταν μηδενιστεί, ο δρομολογητής απορρίπτει το πακέτο και στέλνει ένα μήνυμα τέλους χρόνου του πρωτοκόλλου μηνυμάτων ελέγχου του Internet(ICMP Time Exceeded) μήνυμα στον αποστολέα. Το πρόγραμμα traceroute χρησιμοποιεί το μήνυμα τέλους χρόνου του ICMP. για να εκτυπώσει τους δρομολογητές που χρησιμοποιούνται από τα πακέτα στη διαδρομή τους από την πηγή στον προορισμό.

Αριθμός πρωτοκόλλου

Το πεδίο αυτό προσδιορίζει την έκδοση του πρωτοκόλλου IP που χρησιμοποιείται από το αυτοδύναμο πακέτο. Η Internet Assigned Numbers Authority διατηρεί έναν κατάλογο αριθμών πρωτοκόλλου IP, ο οποίος αρχικά είχε καθοριστεί στο RFC 790.

Άθροισμα ελέγχου επικεφαλίδας

Το 16-bits άθροισμα ελέγχου της επικεφαλίδας, χρησιμοποιείται για έλεγχο σφαλμάτων της επικεφαλίδας. Μόλις ένα πακέτο φτάσει σε έναν δρομολογητή, ο δρομολογητής υπολογίζει το άθροισμα ελέγχου της επικεφαλίδας και το συγκρίνει με το πεδίο αθροίσματος ελέγχου της επικεφαλίδας. Εάν δεν ταιριάζουν, τότε ο δρομολογητής απορρίπτει το πακέτο. Σφάλματα στο πεδίο δεδομένων πρέπει να διαχειριστούν από το ενθυλακωμένο πρωτόκολλο. Και το UDP και το TCP έχουν πεδία αθροισμάτων ελέγχου.

Όταν ένα πακέτο φτάσει σε έναν δρομολογητή, ο δρομολογητής μειώνει το πεδίο χρόνου ζωής (TTL). Συνεπώς ο δρομολογητής πρέπει να υπολογίσει το νέο άθροισμα ελέγχου. Η RFC 1071 καθορίζει τον τρόπο υπολογισμού του αθροίσματος:

Το πεδίο αθροίσματος ελέγχου είναι το 16 bit συμπλήρωμα ως προς ένα, του αθροίσματος των συμπληρωμάτων ως προς 1 των 16 bit λέξεων της επικεφαλίδας. Για τον υπολογισμό του αθροίσματος, το πεδίο άθροισμα ελέγχου επικεφαλίδας θεωρείται 0.

Ας θεωρήσουμε για παράδειγμα την Δεκαεξαδική Επικεφαλίδα: 45000030442240008006000008c7c19acae241e2b (20 bytes IP Επικεφαλίδα):

- Βήμα 1) 4500 + 0030 + 4422 + 4000 + 8006 + 0000 + 8c7c + 19ac + ae24 + 1e2b = 2BBCF (16-bit Άθροισμα)
- Βήμα 2) 2 + BBCF = BBD1 = 1011101111010001 (Συμπλήρωμα ως προς 1 του 16-bit Αθροίσματος)
- Βήμα 3) ~BBD1 = 0100010000101110 = 442E (Συμπλήρωμα ως προς 1 του 16-bit Αθροίσματος)

Για τον έλεγχο αθροίσματος ελέγχου της επικεφαλίδας, μπορεί να χρησιμοποιηθεί ο ίδιος αλγόριθμος: το άθροισμα ελέγχου μιας επικεφαλίδας, που περιέχει ένα σωστό άθροισμα, είναι μηδέν (τιμή 0):

2BBCF + 442E = 2FFFD. 2 + FFFD = FFFF. the 1'S of FFFF = 0.

IP Διεύθυνση πηγής

Αυτό το πεδίο είναι η IPv4 διεύθυνση του αποστολέα του πακέτου. Η διεύθυνση αυτή μπορεί να αλλάξει κατά την διέλευση από μία συσκευή μετάφρασης διεύθυνσης δικτύου (NAT)

IP Διεύθυνση προορισμού

Αυτό το πεδίο είναι η IPv4 διεύθυνση του παραλήπτη του πακέτου. Η διεύθυνση αυτή μπορεί να αλλάξει κατά την διέλευση από μία συσκευή μετάφρασης διεύθυνσης δικτύου (NAT).

IP Επιλογές

Το πεδίο IP Επιλογές δεν χρησιμοποιείται συχνά.

Διάσπαση και επανασύνδεση

Το IP καθιστά δυνατό το να επικοινωνεί το ένα δίκτυο με το άλλο. Ο σχεδιασμός προβλέπει την συνύπαρξη δικτύων διαφόρων τύπων. Το πρωτόκκολο είναι ανεξάρτητο από την φύση της υποκείμενης τεχνολογίας μετάδοσης του επιπέδου σύνδεσης. Τα δίκτυα με διαφορετικό υλικό συνήθως διαφέρουν όχι μόνο στην μέγιστη ταχύτητα μετάδοσης, αλλά επίσης και στη μέγιστη μονάδα μετάδοσης (MTU). Όταν ένα δίκτυο θέλει να στείλει αυτοδύναμα πακέτα σε δίκτυα με μικρότερο MTU, μπορεί να κομματιάσει το αυτοδύναμο πακέτο. Στο IPv4 αυτή η

λειτουργία είναι τοποθετημένη στο επίπεδο internet και εκτελείται στο IPv4 από τους δρομολογητές. Αντίθετα το IPv6, η επόμενη γενιά του πρωτοκόλλου Internet, δεν επιτρέπει στους δρομολογητές να κάνουν διάσπαση. Οι σταθμοί εργασίας πρέπει να προσδιορίσουν το MTU της διαδρομής, προτού αποστείλουν τα αυτοδύναμα πακέτα.

Δεδομένα

Το τμήμα δεδομένων του πακέτου, δεν συμπεριλαμβάνεται στο Άθροισμα Ελέγχου, το οποίο και γι' αυτό αποκαλείται Άθροισμα Ελέγχου Επικεφαλίδας. Ο τρόπος αναπαράστασης των περιεχομένων του βασίζεται στην τιμή που υπάρχει στο πεδίο «Αριθμός Πρωτοκόλλου» της επικεφαλίδας. [6]

2.1.2 ARP: Address Resolution Protocol (Πρωτόκολλο Ανάλυσης Διευθύνσεων)

Το Address Resolution Protocol (ARP) (πρωτόκολλο επίλυσης διευθύνσεων) ορίστηκε στο RFC 826 το 1982 και χρησιμοποιείται για να βρεθεί μια διεύθυνση του επιπέδου συνδέσμου (link layer) ή διεύθυνση υλικού (hardware address) ενός ξένου υπολογιστή με βάση μια διεύθυνση του επιπέδου επικοινωνίας (network layer). Αν και το συναντάμε κυρίως με τα πρωτόκολλα IPv4 και Ethernet (το RFC 826 το ονομάζει πρωτόκολλο επίλυσης διευθύνσεων Ethernet (Ethernet Address Resolution Protocol)), το ARP μπορεί να χρησιμοποιηθεί με το IP πάνω στο ATM ή το FDDI.

Η λειτουργία του ARP μπορεί να χωριστεί σε 4 κατηγορίες:

1. Όταν ένας ξένος υπολογιστής θέλει να στείλει ένα πακέτο σ'έναν άλλο ξένο υπολογιστή που βρίσκεται στο ίδιο δίκτυο
2. Όταν οι δυο ξένοι υπολογιστές βρίσκονται σε διαφορετικά δίκτυα και επικοινωνούν μέσω μιας πύλης/δρομολογητή (gateway/router): π.χ. A → B
3. Όταν ένας δρομολογητής πρέπει να προωθήσει ένα πακέτο ενός host μέσω άλλου δρομολογητή: π.χ. B → C
4. Όταν ένας δρομολογητής πρέπει να προωθήσει ένα πακέτο ενός ξένου υπολογιστή προς έναν άλλο, ο οποίος βρίσκεται στο ίδιο δίκτυο: π.χ. C → D

Η πρώτη περίπτωση ισχύει όταν δυο host βρίσκονται στο ίδιο φυσικό δίκτυο (physical network, π.χ. συνδεδεμένοι με ένα καλώδιο Ethernet), κατά συνέπεια επικοινωνούν απευθείας, χωρίς την μεσολάβηση δρομολογητή. Οι υπόλοιπες τρεις είναι οι πιο κοινές στο Διαδίκτυο εφ'όσον δυο ξένοι υπολογιστές χωρίζονται σχεδόν πάντα από πάνω από τρεις κόμβους.

Δομή πακέτων:

Τύπος υλικού (hardware type)

Ένας αριθμός προσδιορίζεται σε κάθε πρωτόκολλο του στρώματος συνδέσμου, π.χ. 1 για το Ethernet, και γράφεται στο πεδίο αυτό.

Τύπος πρωτόκολλου (protocol type)

Ένας αριθμός προσδιορίζεται σε κάθε πρωτόκολλο, π.χ. 0x0800 για το IPv4, που αντιγράφετε στο πεδίο αυτό.

Μέγεθος τύπου υλικού (hardware length)

Μέγεθος σε bytes της διεύθυνσης υλικού, π.χ. 6 για διευθύνσεις Ethernet.

Μέγεθος τύπου πρωτόκολλου

Μέγεθος σε bytes της διεύθυνσης λογικού τύπου, π.χ. 4 για διευθύνσεις IPv4.

Ενέργεια (operation)

Καθορίζει την ενέργεια που εκτελεί ο αποστολέας: 1 για ερώτημα και 2 για απάντηση.

Διεύθυνση υλικού αποστολέα (sender hardware address)

Διεύθυνση υλικού του αποστολέα. Το μέγεθος του πεδίου αυτού δεν είναι σταθερό ˙ εξαρτάται από το υλικό που χρησιμοποιείται.

Διεύθυνση πρωτοκόλλου αποστολέα (sender protocol address)

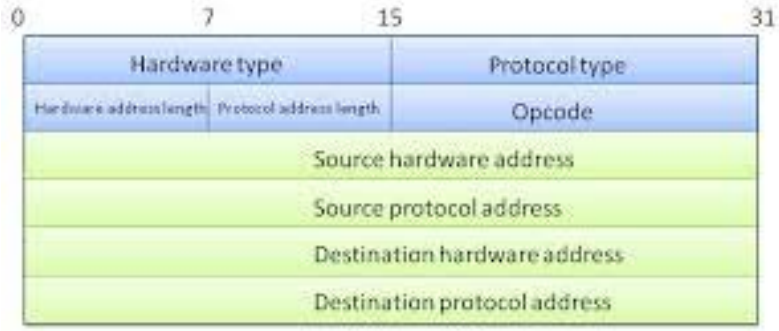
Διεύθυνση πρωτοκόλλου του αποστολέα. Το μέγεθος του πεδίου αυτού δεν είναι σταθερό ˙ εξαρτάται από το πρωτόκολλο που χρησιμοποιείται.

Διεύθυνση υλικού παραλήπτη (target hardware address)

Διεύθυνση υλικού του τελικού παραλήπτη. Το μέγεθος του πεδίου αυτού δεν είναι σταθερό ˙ εξαρτάται από το υλικό που χρησιμοποιείται. Εαν η ενέργεια είναι ερώτημα, το πεδίο αυτό είναι άγνωστο και εξ ορισμού τιμή είναι 0.

Διεύθυνση πρωτοκόλλου παραλήπτη (target protocol address)

Διεύθυνση πρωτοκόλλου του τελικού παραλήπτη. Το μέγεθος του πεδίου αυτού δεν είναι σταθερό ˙ εξαρτάται από το πρωτόκολλο που χρησιμοποιείται.



Εικόνα 2-3: Δομή ARP Πακέτου

Λειτουργία

Κάθε ξένος υπολογιστής που είναι συνδεδεμένος σ'ένα δίκτυο που βασίζεται στο ARP κρατάει έναν κατάλογο (ARP table) ζευγών του τύπου Διεύθυνση πρωτοκόλλου → Αντίστοιχη διεύθυνση υλικού (π.χ. ο δρομολογητής μπορεί να έχει το ζεύγος 192.168.0.30 → 30:30:30:30:30:30 για τον host C). Στην περίπτωση που, για ένα συγκεκριμένο χρονικό διάστημα, δεν υπάρχει επικοινωνία με έναν ξένο υπολογιστή που βρίσκεται στον κατάλογο, το ζεύγος που τον αναφέρει αφαιρείται.

Τα ερωτήματα ARP στέλνονται με broadcast, που σημαίνει πως διάφοροι ξένοι υπολογιστές τα λαμβάνουν. Παρακάτω δίνεται η λίστα των βημάτων που ακολουθεί ένας ξένος υπολογιστής όταν λάβει ένα ερώτημα ARP:

1. Αν το ζεύγος πεδίο ΔΠΑ → πεδίο ΔΥΑ δεν βρίσκεται στον κατάλογο, το προσθέτουμε
2. Αν ο κατάλογος περιέχει ένα ζεύγος με διεύθυνση πρωτοκόλλου ίδια με το πεδίο ΔΠΠ, απαντάμε με τα ανάλογα στοιχεία στον αποστολέα...

3. ... αλλιώς, αν το πεδίο ΔΠΠ αντιστοιχεί σε μια από τις διευθύνσεις πρωτοκόλλου του host, απαντάμε με τα ανάλογα στοιχεία στον αποστολέα...
4. ... αλλιώς απορρίπτουμε το πακέτο. [7]

2.1.3 TCP (Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς

Το TCP (Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς) είναι ένα από τα κυριότερα πρωτόκολλα της Σουίτας Πρωτοκόλλων Διαδικτύου. Βρίσκεται πάνω από το IP protocol (πρωτόκολλο IP). Οι κύριοι στόχοι του πρωτοκόλλου TCP είναι να επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων, επίσης να μεταφέρονται τα δεδομένα χωρίς λάθη μεταξύ του στρώματος δικτύου (network layer) και του στρώματος εφαρμογής (application layer) και, φτάνοντας στο πρόγραμμα του στρώματος εφαρμογής, να έχουν σωστή σειρά. Οι περισσότερες σύγχρονες υπηρεσίες στο Διαδίκτυο βασίζονται στο TCP. Για παράδειγμα το SMTP (port 25), το παλαιότερο (και μη-ασφαλές) Telnet (port 23), το FTP και πιο σημαντικό το HTTP (port 80), γνωστό ως υπηρεσίες World Wide Web (WWW - Παγκόσμιος Ιστός). Το TCP χρησιμοποιείται σχεδόν παντού, για αμφίδρομη επικοινωνία μέσω δικτύου.

Αρχικά το Transmission ήταν Transfer, ένας όρος που προσδιόριζε την μεταβίβαση του ελέγχου στα άκρα του δικτύου TCPIP πριν αποσπαστεί το IP.

TCP Επικεφαλίδα

Τα πακέτα του πρωτοκόλλου TCP καλούνται segments (τμήματα)[1]. Ένα από τα κυριότερα μέρη ενός segment είναι η TCP επικεφαλίδα (TCP header), η οποία παρέχει συγκεκριμένες πληροφορίες για το πρωτόκολλο TCP. Το ελάχιστο μέγεθος της επικεφαλίδας είναι 5 words και το μέγιστο 15 words (απουσία ή παρουσία όλων των options αντίστοιχα).

+	Bits 0 - 3	4 - 9	10 - 15	16 - 31
0	**Source Port** Θύρα Προέλευσης			**Destination Port** Θύρα Προορισμού
32	**Sequence Number** Αριθμός ακολουθίας			
64	**Acknowledgment Number** Αριθμός επιβεβαίωσης			
96	**Data Offset**	**Reserved**	**Flags** Σημαίες	**Window** Παράθυρο
128	**Checksum** Άθροισμα ελέγχου			**Urgent Pointer** Επείγοντα δεδομένα
160	**Options** Επιλογές (προαιρετικές)			
160/192+	**Data** Δεδομένα			

Εικόνα 2-4:TCP Επικεφαλίδα

Source Port

Αυτό το πεδίο προσδιορίζει την port (θύρα) του αποστολέα

Destination Port

Αυτό το πεδίο προσδιορίζει την port (θύρα) του παραλήπτη

Sequence Number

Ο sequence number (αριθμός ακολουθίας) έχει διπλό ρόλο:

- Εαν υπάρχει η SYN flag (SYN σημαία) τότε είναι ο αρχικός αριθμός ακολουθίας (ISN - initial sequence number) και η πρώτη octet δεδομένων του πακέτου είναι ο ISN+1.
- Αλλιώς, εαν δεν υπάρχει η SYN flag, τότε η πρώτη octet δεδομένων είναι ο αριθμός ακολουθίας.

Acknowledgment number

Όταν υπάρχει η ACK flag η τιμή αυτού του πεδίου δείχνει τον επόμενο sequence number (αριθμό ακολουθίας) που αναμένει ο αποστολέας.

Data offset

Είναι ο αριθμός από words μεγέθους 32 bit στην επικεφαλίδα TCP (TCP header). Καθορίζει το μέγεθος της επικεφαλίδας (πολλαπλάσιο του 32) και επομένως δείχνει και την αρχή των δεδομένων.

Reserved

Πεδίο 6 bit "κρατημένων" (αγγλ. reserved) για μελλοντική χρήση. Η τιμή των bit πρέπει να είναι 0.

Flags (επίσης γνωστό ως bits ελέγχου - Control bits)

Περιέχει 6 bit - σημαίες:

Πίνακας 2-1: Σημαίες Flags

Σημαία	Σημασία	Προέλευση ονομασίας
URG	Το πεδίο urgent pointer είναι σημαντικό	**URG**ent
ACK	Το πεδίο επιβεβαίωσης είναι σημαντικό	**ACK**nowledgment
PSH	Λειτουργία ώθησης	**P**u**SH**
RST	Επαναρύθμιση σύνδεσης	**R**e**S**e**T**
SYN	Συγχρονισμός αριθμών ακολουθίας	**SYN**chronize
FIN	Ο αποστολέας δεν στέλνει άλλα δεδομένα	**FIN**ish

Window

Ο αριθμός από octets δεδομένων (bytes) που επιθυμεί να δεχτεί ο αποστολέας του πακέτου, αρχίζοντας από εκείνη που δείχνει το πεδίο επιβεβαίωσης (acknowledgment field).

Checksum

Το πεδίο checksum μεγέθους 16 bit χρησιμοποιείται για έλεγχο λαθών στην επικεφαλίδα και στα δεδομένα. Το checksum υπολογίζεται πάνω σε ψευδο-κεφαλίδα.

Options

Μεταβλητή, η οποία καθορίζει ειδικές επιλεγόμενες ρυθμίσεις και μπορεί να καταλάβει χώρο στο τέλος της επικεφαλίδας TCP (TCP header). Το μήκος τους είναι πολλαπλάσιο των 8 bit και σε το περιεχόμενο της επικεφαλίδας μετά την τελευταία επιλογή πρέπει να γεμίζει (πχ. με μηδενικά - 0). Με αυτόν τον τρόπο το data offset θα δείχνει σωστά την αρχή των δεδομένων.

Urgent pointer

Εάν είναι ενεργοποιημένο το URG bit ελέγχου, τότε αυτό το πεδίο δείχνει τον αριθμό ακολουθίας (sequence number) της octet που βρίσκεται αμέσως μετά το τελευταίο byte από τα επείγοντα δεδομένα. Έτσι παρουσιάζει τη θέση του τελευταίου byte με επείγοντα δεδομένα.

Τρόπος λειτουργίας

Το πρωτόκολλο ελέγχου μεταφορών (TCP) είναι connection oriented, δηλαδή η μεταφορά δεδομένων γίνεται μέσω σύνδεσης, η οποία οριοθετείται από ένα σήμα έναρξης και ένα σήμα τέλους ή διακοπής.

Έναρξη - Τριμερής χειραψία / 3-way handshake

Πριν να προσπαθήσει ένα πρόγραμμα-πελάτης (client) να συνδεθεί με έναν server, ο server πρέπει πρώτα να δεσμεύσει μια port και να την ανοίξει ώστε να δέχεται συνδέσεις: αυτό καλείται passive open. Όταν γίνει αυτό, ο client μπορεί να αρχίσει τη σύνδεση (active open). Για να γίνει μια σύνδεση, γίνεται μια "χειραψία" ανάμεσα στα συμμετέχοντα μέρη, το λεγόμενο three-way handshake:

Έναρξη της σύνδεσης με three-way handshake

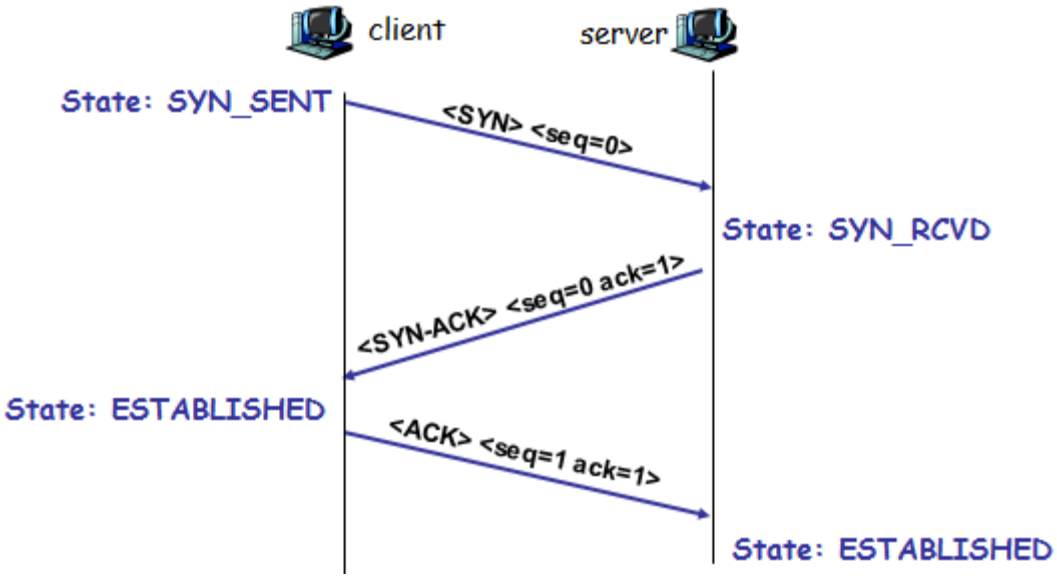
1. Αρχικά αποστέλεται ένα πακέτο[1] με το SYN bit ενεργοποιημένο. Ο client θέτει το πεδίο αριθμού ακολουθίας στην TCP επικεφαλίδα (TCP header) στον αρχικό αριθμό ακολουθίας του (ISN - initial sequence number).
2. server στο άλλο άκρο απαντάει:

είτε με SYN (για να στείλει και το δικό του ISN) και ACK (που έχει το ISN+1 του client) του πρώτου πακέτου του client για να αποδεχτεί τη σύνδεση,

ή SYN/RST για να ενημερώσει τον client ότι αρνείται τη σύνδεση και η διαδικασία σταματά.

3. Όταν ο client πάρει ένα πακέτο SYN/ACK απαντάει, αυτή τη φορά, με ένα πακέτο ACK. Σε αυτό το σημείο, τα δύο μέρη συνδέονται και μπορούν πλέον να σταλούν τα δεδομένα.

Κατά τη διάρκεια του three-way handshake, τα δύο μέρη διαπραγματεύονται επίσης όλες τις ειδικές επιλογές που θα χρησιμοποιηθούν κατά τη διάρκεια της σύνδεσης TCP, όπως ECN κ.α.



Εικόνα 2-5: Έναρξη της σύνδεσης με three-way handshake

Μεταφορά δεδομένων

Μόλις ανταλλαχθούν οι ISNs, οι εφαρμογές μπορούν να διαβιβάσουν δεδομένα η μια στην άλλη. Η ανάλυση του τρόπου με τον οποίο γίνεται η μεταφορά δεδομένων, απαιτεί εξέταση για

- έλεγχο ροής (flow control) και
- τεχνικές ελέγχου συμφόρησης (congestion avoidance).

Σε μια απλή υλοποίηση του TCP, χωρίς τους προαναφερθέντες ελέγχους, η εφαρμογή θα στείλει πακέτα στο δίκτυο προς τον παραλήπτη, εφ' όσον υπάρχουν δεδομένα να σταλούν και εφ' όσον ο αποστολέας δεν υπερβαίνει το window που του έχει υποδείξει ο παραλήπτης. Όταν ο παραλήπτης δέχεται πακέτα TCP, στέλνει επιβεβαιώσεις (acknowledgement), δείχνοντας σε ποιο σημείο του

ρεύματος από byte (byte stream) βρίσκεται. Αυτές οι επιβεβαιώσεις περιέχουν επίσης το επόμενο window (παράθυρο) που καθορίζει πόσα byte επιθυμεί να δεχτεί στη συνέχεια ο παραλήπτης.

Εάν ορισμένα δεδομένα αναπαράγονται ή χάνονται, μπορεί να δημιουργηθεί ένα κενό στο ρεύμα από byte (byte stream). Ο παραλήπτης θα συνεχίσει να επιβεβαιώνει την νεότερη θέση που βρίσκεται, στο ρεύμα από byte που έχει δεχτεί.

Εάν δεν υπάρχουν δεδομένα για να σταλούν, ο αποστολέας θα βρίσκεται σε αδράνεια αναμένοντας την εφαρμογή να βάλει δεδομένα στο byte stream ή να παραλάβει δεδομένα από το άλλο άκρο της σύνδεσης.

Έλεγχος ροής

Ο έλεγχος ροής απαιτεί την επιβεβαίωση λήψης (acknowledgment) κάθε πακέτου από τον απόμακρο host πριν να σταλεί το επόμενο. Οι αλγόριθμοι για το sliding window [3], που χρησιμοποιούνται από το TCP, επιτρέπουν σε πολλαπλά πακέτα δεδομένων να μεταφέρονται ταυτόχρονα για να χρησιμοποιείται αποδοτικότερα το εύρος ζώνης (bandwidth) ενός δικτύου.

Για παράδειγμα, εαν ένας υπολογιστής Α στείλει 4 byte με αριθμό ακολουθίας (sequence number) 100 - συνεπώς, τα 4 bytes έχουν αριθμό ακολουθίας 100, 101, 102 και 103 - τότε ο παραλήπτης πρέπει να απαντήσει με επιβεβαίωση (acknowledgement) που φέρει sequence number 104. Αυτό πρόκειται να είναι το επόμενο byte που περιμένει στο επόμενο πακέτο. Εαν για κάποιο λόγο, τα τελευταία δύο bytes περιέχουν σφάλματα τότε η τιμή της επιβεβαίωσης θα είναι 102, εφόσον τα bytes με αριθμό 100 και 101 έχουν φτάσει με επιτυχία.

Έλεγχος συμφόρησης

Αν και το TCP συνήθως δεν ενδιαφέρεται για όσα συμβαίνουν στο διαδίκτυο (αυτό είναι εργασία που εκτελείται από IP protocol στο 3ο επίπεδο του μοντέλου OSI) πρέπει να είναι αρκετά "έξυπνο", ώστε να αντιληφθεί και να χειριστεί κατάλληλα μια συμφόρηση στο δίκτυο. Το TCP δεν μπορεί να αγνοήσει τι συμβαίνει στο διαδίκτυο μεταξύ των δύο συνδεδεμένων άκρων.

Για αυτόν τον λόγο, το TCP περιλαμβάνει διάφορους συγκεκριμένους αλγορίθμους που έχουν ως σκοπό είτε να αποφύγουν εξ αρχής τη συμφόρηση, είτε να ανταποκριθούν σε αυτή. Χρησιμοποιούνται διάφοροι μηχανισμοί για να επιτευχθεί υψηλή απόδοση και να μην υπερφορτωθεί το δίκτυο. Αυτοί οι μηχανισμοί περιλαμβάνουν:

- τον αλγόριθμο slow-start,
- τον αλγόριθμο congestion avoidance,
- τον αλγόριθμο fast retransmit και
- τον αλγόριθμο fast recovery

όπως αναφέρεται στο RFC 2001.

Τερματισμός

Η σύνδεση τερματίζεται με ένα four-way handshake, με την κάθε πλευρά να τερματίζει ανεξάρτητα:

1. Όταν κάποιο άκρο επιθυμεί να κλείσει τη σύνδεση από πλευράς του, στέλνει ένα πακέτο με το FIN ενεργοποιημένο,
2. Το πακέτο αυτό επιβεβαιώνει η άλλη πλευρά με ένα ACK και
3. στη συνέχεια, στέλνει το ένα πακέτο FIN
4. Η πλευρά που ξεκίνησε τον τερματισμό, μπορεί να το επιβεβαιώσει στέλνοντας ένα πακέτο ACK.

Με αυτόν τον τρόπο, για έναν τυπικό τερματισμό χρειάζεται ένα ζεύγος πακέτων FIN και ACK για κάθε άκρο στη σύνδεση TCP. Μια σύνδεση μπορεί να είναι "half-open", δηλαδή η μία πλευρά να έχει τερματίσει, όχι όμως και η άλλη. Η πλευρά που έχει τερματίσει δεν μπορεί να στείλει πλέον δεδομένα, ενώ η άλλη μπορεί.

Τέλος, είναι δυνατό, αν και λιγότερο πιθανό, οι δύο host να στείλουν ταυτόχρονα ένα πακέτο FIN ο ένας στον άλλο. Στη συνέχεια ο καθένας επιβεβαιώνει το FIN που δέχτηκε με ένα πακέτο ACK. Στο σημείο αυτό και οι δύο διακόπτουν τη σύνδεση. [8]

2.1.4 UDP User Datagram Protocol

Το πρωτόκολλο User Datagram Protocol (UDP) είναι ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο. Μία εναλλακτική ονομασία του πρωτοκόλλου είναι Universal Datagram Protocol. Διάφορα προγράμματα χρησιμοποιούν το πρωτόκολλο UDP για την αποστολή σύντομων μηνυμάτων (γνωστών και ως datagrams) από τον έναν υπολογιστή στον άλλον μέσα σε ένα δίκτυο υπολογιστών.

Ένα από τα κύρια χαρακτηριστικά του UDP είναι ότι δεν εγγυάται αξιόπιστη επικοινωνία. Τα πακέτα UDP που αποστέλλονται από έναν υπολογιστή μπορεί να φτάσουν στον παραλήπτη με λάθος σειρά, διπλά ή να μην φτάσουν καθόλου εάν το δίκτυο έχει μεγάλο φόρτο. Χρησιμοποιείται όταν η "γρήγορη" παράδοση των πακέτων είναι πιο σημαντική από την "ακριβή" παράδοση, π.χ στη μετάδοση ομιλίας και βίντεο.. Αντιθέτως, το πρωτόκολλο TCP διαθέτει όλους τους απαραίτητους μηχανισμούς ελέγχου και επιβολής της αξιοπιστίας και συνεπώς μπορεί να εγγυηθεί την αξιόπιστη επικοινωνία μεταξύ των υπολογιστών. Η έλλειψη των μηχανισμών αυτών από το πρωτόκολλο UDP το καθιστά αρκετά πιο γρήγορο και αποτελεσματικό, τουλάχιστον για τις εφαρμογές εκείνες που δεν απαιτούν αξιόπιστη επικοινωνία.

Οι εφαρμογές audio και video streaming χρησιμοποιούν κατά κόρον πακέτα UDP. Για τις εφαρμογές αυτές είναι πολύ σημαντικό τα πακέτα να παραδοθούν στον παραλήπτη σε σύντομο χρονικό διάστημα ούτως ώστε να μην υπάρχει διακοπή στην ροή του ήχου ή της εικόνας. Κατά συνέπεια προτιμάται το πρωτόκολλο UDP διότι είναι αρκετά γρήγορο, παρόλο που υπάρχει η πιθανότητα μερικά πακέτα UDP να χαθούν. Στην περίπτωση που χαθεί κάποιο πακέτο, οι εφαρμογές αυτές διαθέτουν ειδικούς μηχανισμούς διόρθωσης και παρεμβολής ούτως ώστε ο τελικός χρήστης να μην παρατηρεί καμία αλλοίωση ή διακοπή στην ροή του ήχου και της εικόνας λόγω του χαμένου πακέτου. Σε αντίθεση με το πρωτόκολλο TCP, το UDP υποστηρίζει broadcasting, δηλαδή την αποστολή ενός πακέτου σε όλους τους υπολογιστές ενός δικτύου, και multicasting, δηλαδή την αποστολή ενός πακέτου σε κάποιους συγκεκριμένους υπολογιστές ενός δικτύου. Η τελευταία δυνατότητα χρησιμοποιείται πολύ συχνά στις εφαρμογές audio και video streaming ούτως ώστε μία ροή ήχου ή εικόνας να μεταδίδεται ταυτόχρονα σε πολλούς συνδρομητές.

Μερικές σημαντικές εφαρμογές που χρησιμοποιούν πακέτα UDP είναι οι εξής: Domain Name System (DNS), IPTV, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) και τα παιχνίδια που παίζονται ζωντανά μέσω του Διαδικτύου.

Δομή UDP πακέτου

Η δομή ενός πακέτου UDP περιγράφεται αναλυτικά στο αντίστοιχο πρότυπο IETF RFC 768. Στην σουίτα πρωτοκόλλων του Διαδικτύου, το UDP βρίσκεται ανάμεσα στο επίπεδο δικτύου (network layer) και στο επίπεδο συνόδου (session layer) ή εφαρμογών (application layer).

Κάθε πακέτο UDP έχει μία κεφαλίδα (header) που αναφέρει τα χαρακτηριστικά του. Η κεφαλίδα περιλαμβάνει μονάχα 4 πεδία, τα οποία είναι πολύ λίγα εάν συγκριθούν με άλλα πρωτόκολλα, όπως το TCP. Δύο από τα τέσσερα πεδία είναι προαιρετικά (φαίνονται χρωματισμένα με ροζ).

+	Bits 0 - 15	16 - 31
0	Source Port	Destination Port
32	Length	Checksum
64	Data	

Εικόνα 2-6: UDP Κεφαλίδα

Source port

Η πόρτα του αποστολέα από την οποία προήλθε το πακέτο. Εάν ο παραλήπτης επιθυμεί να στείλει κάποια απάντηση, θα πρέπει να την στείλει στην πόρτα αυτήν. Το συγκεκριμένο πεδίο δεν είναι υποχρεωτικό και στις περιπτώσεις που δεν χρησιμοποιείται θα πρέπει να έχει την τιμή μηδέν.

Destination port

Η πόρτα του παραλήπτη στην οποία θα πρέπει να παραδοθεί το πακέτο.

Length

Το πεδίο αυτό έχει μέγεθος 16-bit και περιλαμβάνει το μέγεθος του πακέτου σε bytes. Το μικρότερο δυνατό μέγεθος είναι 8 bytes, αφού η κεφαλίδα αυτή καθ' αυτή καταλαμβάνει τόσο χώρο. Θεωρητικά, το μέγεθος του UDP πακέτου δεν μπορεί να ξεπερνάει τα 65,527 bytes, αλλά πρακτικά το όριο μειώνεται στα 65,507 bytes λόγω διαφόρων περιορισμών που εισάγει το πρωτόκολλο IPv4 στο επίπεδο δικτύου.

Checksum

Ένα πεδίο 16-bit το οποίο χρησιμοποιείται για επαλήθευση της ορθότητας του πακέτου στο σύνολό του, δηλαδή τόσο της κεφαλίδας όσο και των δεδομένων.

Στην συνέχεια το πακέτο UDP περνάει στο επίπεδο δικτύου, το οποίο αναλαμβάνει να το μεταδώσει στο δίκτυο υπολογιστών. Το επίπεδο αυτό τοποθετεί μία ακόμη κεφαλίδα στο πακέτο, η οποία διαφέρει ανάλογα με την έκδοση του πρωτοκόλλου που χρησιμοποιείται στο επίπεδο δικτύου (IPv4 ή IPv6).

Για IPv4, το πακέτο λαμβάνει την ακόλουθη μορφή:

+	Bits 0 - 7	8 - 15	16 - 23	24 - 31
0	Source address			
32	Destination address			
64	Zeros	Protocol	UDP length	
96	Source Port		Destination Port	
128	Length		Checksum	
160	Data			

Εικόνα 2-7: UDP (IPv4)

Source Address, Destination Address

Οι διευθύνσεις IP του αποστολέα και του παραλήπτη αντίστοιχα.

Zeros

Μία ακολουθία μηδενικών, η οποία δεν παίζει κανέναν ρόλο κατά την μετάδοση του πακέτου.

Protocol

Ένας χαρακτηριστικός αριθμός που αντιστοιχεί στο πρωτόκολλο που χρησιμοποιείται. Για το UDP η τιμή που παίρνει το πεδίο αυτό είναι 17.

UDP Length

Το συνολικό μέγεθος του πακέτου UDP.

Για IPv6, το πακέτο παίρνει την εξής μορφή:

+	Bits 0 - 7	8 - 15	16 - 23	24 - 31
0	Source address			
32				
64				
96				
128	Destination address			
160				
192				
256				
288	UDP length			
320	Zeros			Next Header
352	Source Port		Destination Port	
384	Length		Checksum	
416	Data			

Εικόνα 2-8: UDP (IPv6)

Source Address, Destination Address

Οι διευθύνσεις IP του αποστολέα και του παραλήπτη αντίστοιχα, οι οποίες όμως στην περίπτωση αυτή είναι τύπου IPv6, δηλαδή πολύ μεγαλύτερες (IPv4 - 32bit, IPv6 - 128bit).

UDP Length

Το συνολικό μέγεθος του πακέτου UDP, όπως και προηγουμένως.

Zeros

Μία ακολουθία μηδενικών, η οποία δεν παίζει κανέναν ρόλο κατά την μετάδοση του πακέτου.

Next Header

Το πεδίο αυτό παίρνει μία τιμή που είναι χαρακτηριστική για το πρωτόκολλο που χρησιμοποιείται. Στην περίπτωση του UDP, η τιμή αυτή είναι 17.

Στην περίπτωση IPv6 το πεδίο checksum του UDP πακέτου δεν είναι πλέον προαιρετικό, αλλά θα πρέπει υποχρεωτικά να συμπληρωθεί.

Εφαρμογές

Όπως αναφέρθηκε και προηγουμένως, οι εφαρμογές που χρησιμοποιούν το πρωτόκολλο UDP θα πρέπει να μπορούν να δεχτούν κάποια απώλεια πακετων ή διάφορα σφάλματα στα πακέτα τα οποία στέλνουν. Μερικές εφαρμογές, όπως για παράδειγμα το Trivial File Transfer Protocol (TFTP) υλοποιούν δικούς τους μηχανισμούς διασφάλισης της αξιοπιστίας της επικοινωνίας. Πάντως, τις περισσότερες φορές οι εφαρμογές που χρησιμοποιούν το UDP δεν επιβάλλουν επιπρόσθετους μηχανισμούς αξιοπιστίας διότι θα παρεμποδίζονται από αυτούς και χειροτερεύει η απόδοσή τους. Κλασικό παράδειγμα τέτοιων προγραμμάτων είναι οι εφαρμογές πραγματικού χρόνου (πχ. media streaming, παιχνίδια στο διαδίκτυο, VoIP κτλ). Στην περίπτωση πάντως που μία εφαρμογή χρειάζεται αξιόπιστη μετάδοση δεδομένων, δηλαδή η πλειοψηφία των εφαρμογών του διαδικτύου, θα προτιμήσει να χρησιμοποιήσει το πρωτόκολλο TCP αντί του UDP.

Σε ένα τυπικό δίκτυο υπολογιστών, η κίνηση που προέρχεται από την μετάδοση UDP πακέτων ανέρχεται σε ένα αρκετά μικρό ποσοστό. Παρόλα αυτά όμως, το πρωτόκολλο αυτό το χρησιμοποιούν πολύ σημαντικές εφαρμογές, στην σωστή

λειτουργία των οποίων βασίζεται το διαδίκτυο. Τέτοιες εφαρμογές είναι για παράδειγμα οι εξής: Domain Name System (DNS), Simple Network Management Protocol (SNMP), Dynamic Host Configuration Protocol (DHCP) και το Routing Information Protocol (RIP).

Διαφορές μεταξύ TCP και UDP

Το πρωτόκολλο TCP λειτουργεί εγκαθιδρύοντας συνδέσεις μεταξύ του αποστολέα και του παραλήπτη των πακέτων. Από την στιγμή που μία σύνδεση εγκαθιδρυθεί με επιτυχία, όλα τα δεδομένα αποστέλλονται από τον έναν υπολογιστή στον άλλο με την μορφή πακέτων χρησιμοποιώντας την σύνδεση αυτή. Τα κύρια χαρακτηριστικά του TCP είναι τα εξής:

- **Αξιοπιστία** - Το TCP χρησιμοποιεί διάφορους μηχανισμούς ούτως ώστε να διασφαλιστεί ότι τα πακέτα που μεταδίδονται από τον αποστολέα θα φτάσουν σίγουρα στον παραλήπτη και στην σωστή σειρά. Οι μηχανισμοί αυτοί περιλαμβάνουν την επιβεβαίωση λήψης πακέτου από τον παραλήπτη, την επαναποστολή πακέτων που χάθηκαν και τον καθορισμό ενός ελάχιστου χρονικού διαστήματος μέσα στο οποίο κάθε αποστελλόμενο πακέτο θα πρέπει να έχει παραληφθεί (timeout). Στην περίπτωση που χαθεί κάποιο πακέτο, ο αποστολέας προσπαθεί και πάλι να το ξαναστείλει. Επίσης, εάν ο παραλήπτης διαπιστώσει ότι ένα πακέτο δεν του έχει έρθει, τότε θα ζητήσει από τον αποστολέα να του το ξαναστείλει.
- **Σειρά πακέτων** - Εάν δύο πακέτα αποσταλούν σε μία σύνδεση το ένα μετά το άλλο, τότε το πρωτόκολλο TCP εγγυάται ότι θα φτάσουν στον παραλήπτη με την ίδια σειρά με την οποία στάλθηκαν. Στην περίπτωση που λείπει ένα πακέτο και έρθουν μελλοντικά πακέτα, τότε αυτά κατακρατούνται στην προσωρινή μνήμη (buffer) μέχρις ότου φτάσει το πακέτο που λείπει. Τότε αναδιατάσσονται και εμφανίζονται με την σωστή σειρά στον παραλήπτη.
- **Βαρύτητα** - Το πρωτόκολλο TCP θεωρείται ιδιαίτερα βαρύ, δεδομένου του γεγονότος ότι χρειάζονται τουλάχιστον 3 πακέτα για την εγκαθίδρυση της σύνδεσης, πριν ακόμη μεταδοθεί οποιοδήποτε πακέτο δεδομένων. Επίσης, οι μηχανισμοί αξιοπιστίας που υλοποιεί το κάνουν ακόμη πιο

βαρύ, πράγμα που έχει φυσικά σημαντικό αντίκτυπο στην ταχύτητα μετάδοσης δεδομένων.

Το UDP είναι ένα πιο απλό και ελαφρύ πρωτόκολλο, στο οποίο δεν υπάρχει η έννοια της σύνδεσης. Κάθε πακέτο UDP διανύει το δίκτυο ως μία ξεχωριστή αυτόνομη μονάδα και όχι ως μία σειρά πακέτων σε μία σύνδεση, όπως στο TCP. Τα κύρια χαρακτηριστικά του UDP είναι τα εξής:

- **Αναξιόπιστο** - Κατά την αποστολή ενός πακέτου, ο αποστολέας δεν είναι σε θέση να γνωρίζει εάν το πακέτο θα φτάσει σωστά στον προορισμό του ή εάν θα χαθεί μέσα στο δίκτυο. Δεν έχει προβλεφθεί η δυνατότητα επιβεβαίωσης λήψης πακέτου από τον παραλήπτη, ούτε η επαναμετάδοση ενός χαμένου πακέτου.
- **Δεν υπάρχει σειρά** - Τα πακέτα UDP, σε αντίθεση με το TCP, δεν αριθμούνται και κατά συνέπεια δεν υπάρχει κάποια συγκεκριμένη σειρά με την οποία θα πρέπει να φτάσουν στον παραλήπτη.
- **Ελαφρύ** - Το πρωτόκολλο αυτό καθ' αυτό είναι πολύ ελαφρύ σε σύγκριση με το TCP διότι δεν εφαρμόζει όλους τους μηχανισμούς αξιόπιστης επικοινωνίας που υπάρχουν στο δεύτερο. Αυτό έχει ως συνέπεια να είναι αρκετά πιο γρήγορο.
- **Datagrams** - Κάθε πακέτο UDP ονομάζεται επίσης και "datagram", θεωρείται δε ως μεμονωμένη οντότητα που θα πρέπει να μεταδοθεί ολόκληρη. Κατά συνέπεια δεν υφίσταται η έννοια της διοχέτευσης πακέτων μέσα σε ένα κανάλι / σύνδεση. [9]

ΚΕΦΑΛΑΙΟ 3

IP ΔΙΕΘΥΝΣΙΟΔΟΤΗΣΗ – ΥΠΟΔΙΚΤΥΑ - ΔΡΟΜΟΛΟΓΗΣΗ

3.1 Διεύθυνση IP

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

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

Domain names

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

Δυναμικές και στατικές διευθύνσεις IP

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

Δυναμικές IP

Οι δυναμικές διευθύνσεις IP δίνονται για να αναγνωρίζονται προσωρινές συσκευές όπως προσωπικοί υπολογιστές ή προγράμματα πελάτες (clients). Οι ISPs χρησιμοποιούν δυναμική κατανομή (οι διευθύνσεις IP κατανέμονται δυναμικά) για να ορίσουν διευθύνσεις από ένα μικρό πλήθος διαθέσιμων σε ένα μεγαλύτερο αριθμό πελατών. Αυτή η μέθοδος χρησιμοποιείται για σύνδεση μέσω τηλεφώνου (dial-up), WiFi και άλλες προσωρινές συνδέσεις, επιτρέποντας σε χρήστες φορητών υπολογιστών να συνδέονται αυτόματα σε μια ποικιλία υπηρεσιών χωρίς να χρειάζεται να γνωρίζουν λεπτομέρειες σχετικά με τη δρομολόγηση (routing) του κάθε δικτύου.

Οι χρήστες με δυναμικές διευθύνσεις IP πιθανόν να έχουν προβλήματα στο να τρέχουν δικό τους mail server (διακομιστή ηλεκτρονικού ταχυδρομείου) καθώς τα τελευταία χρόνια υπηρεσίες όπως το mail-abuse.org [1] έχουν συλλέξει λίστες από σειρές (ranges) διευθύνσεων IP (διευθύνσεις δηλαδή που έχουν ίδια κάποια αρχικά ψηφία) και τις έχουν μπλοκάρει.

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

Είναι σύνηθες να χρησιμοποιείται δυναμική κατανομή για ιδιωτικά δίκτυα. Δεδομένου ότι τα ιδιωτικά δίκτυα σπάνια παρουσιάζουν έλλειψη διευθύνσεων, είναι δυνατό να οριστεί η ίδια διεύθυνση στον ίδιο υπολογιστή με κάθε αίτηση

(request) ή να καθοριστεί ένας παρατεταμένος lease time. Αυτές οι δύο μέθοδοι μιμούνται την ανάθεση στατικής διεύθυνσης IP.

Στατικές IP

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

Εκδόσεις του IP

Το Πρωτόκολλο Διαδικτύου έχει δύο κύριες εκδόσεις σε χρήση, την IPv4 και την IPv6. Κάθε έκδοση έχει το δικό της ορισμό για την διεύθυνση IP. Λόγω της επικράτησής της, ο όρος «διεύθυνση IP» τυπικά αναφέρεται σε εκείνες που ορίζονται στο IPv4.

Οι διευθύνσεις IP που ορίζονται είναι αριθμοί της μορφής xxx.xxx.xxx.xxx (IPv4), όπου xxx ένας αριθμός από 0 εώς 255 ή xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.xxx.xxx.xxx.xxx (IPv6).

IPv4

Το IPv4 χρησιμοποιεί διευθύνσεις των 32-bit (4 byte), που περιορίζουν το πλήθος διευθύνσεων σε 4.294.967.296 (2^{32}) πιθανές μοναδικές διευθύνσεις. Εντούτοις, πολλές παρακρατούνται για ειδικούς λόγους, όπως για χρήση σε ιδιωτικά δίκτυα ή διευθύνσεις πολυδιανομής. Κατά αυτόν τον τρόπο, μειώνεται ο αριθμός που μπορεί να διατεθεί για δημόσιες διευθύνσεις Διαδικτύου και, καθώς ο αριθμός διαθέσιμων διευθύνσεων καταναλώνεται, η έλλειψη εμφανίζεται να είναι αναπόφευκτη μακροπρόθεσμα. Αυτός ο περιορισμός έχει συντελέσει στη στροφή προς το IPv6, που είναι αυτήν την περίοδο σε αρχικά στάδια επέκτασης και ο μόνος υποψήφιος αντικαταστάτης του IPv4.

IPv6

Στο IPv6, το νέο standard (αλλά όχι ακόμα εκτεταμένης χρήσης) Πρωτοκόλλο Διαδικτύου, οι διευθύνσεις έχουν μέγεθος 128 bit, το οποίο, ακόμη και με

γενναιόδωρη ανάθεση netblocks, θα είναι αρκετό για να επαρκέσει στο κοντινό μέλλον. Θεωρητικά, θα υπάρχουν ακριβώς 2128, ή περίπου 3,403 × 1038 μοναδικές διευθύνσεις για διεπιφάνειες διακομιστών (host interfaces). Ο ακριβής αριθμός είναι 340.282.366.920.938.463.463.374.607.431.768.211.456. Αυτό το μεγάλο πλήθος διευθύνσεων θα δεσμευτεί αραιά, γεγονός που καθιστά πιθανή την κωδικοποίηση περισσότερων πληροφοριών δρομολόγησης στις ίδιες τις διευθύνσεις.

Δημόσιες και ιδιωτικές διευθύνσεις

Δημόσια διεύθυνση (public IP) ονομάζεται κάθε IP διεύθυνση που είναι απευθείας ορατή στο Διαδίκτυο, για παράδειγμα η διεύθυνση που εμφανίζεται αν κάποιος προσπαθεί να κάνει ανώνυμη καταχώρηση στη Βικιπαίδεια. Αυτή είναι συνήθως η IP που δίνεται στο modem-router που χρησιμοποιείται και όχι η διεύθυνση που δίνει το modem-router στον υπολογιστή του χρήστη αυτού.

Και τα δύο πρωτόκολλα IP (v4 και v6) έχουν περιοχές διευθύνσεων (υποδίκτυα - subnets) τα οποία προορίζονται για ιδιωτική χρήση. Οι ιδιωτικές διευθύνσεις για το IPv4 σύμφωνα με το RFC 1918 είναι:

Πίνακας 3-1:IANA-ιδιωτικές διευθύνσεις IPv4

IANA-ιδιωτικές διευθύνσεις IPv4			
	Αρχή	**Τέλος**	**Αρ. διευθύνσεων**
24-bit Block (/8 prefix, 1 × A)	10.0.0.0	10.255.255.255	16.777.216
20-bit Block (/12 prefix, 16 × B)	172.16.0.0	172.31.255.255	1.048.576
16-bit Block (/16 prefix, 256 × C)	192.168.0.0	192.168.255.255	65.536

Σύμφωνα με το RFC 3330:

Η διεύθυνση 127.0.0.1 συνήθως χρησιμοποιείται για τον τοπικό υπολογιστή και, όπως και ολόκληρο το υποδίκτυο 127.0.0.0/8, δεν "βγαίνει" ούτε στο τοπικό υποδίκτυο.

Οι διευθύνσεις του υποδικτύου 39.0.0.0/8 χρησιμοποιήθηκαν το 1995 και του 24.0.0.0/8 το 1996 για ειδικούς σκοπούς αλλά πλέον περιλαμβάνονται στις δημόσιες διευθύνσεις.

Οι ίδιες ιδιωτικές διευθύνσεις βρίσκονται σε διάφορα υποδίκτυα παγκοσμίως και δεν "περνούν" μέσα από τους δρομολογητές (routers). Για να μπορέσει ένας υπολογιστής να βγει στο Διαδίκτυο χρησιμοποιείται, συνήθως, ο πίνακας αντικαταστάσεων NAT. [10]

Αταξική Δρομολόγηση Δικτυακών Περιοχών

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

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

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

IP υποδίκτυα

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

Ο καθορισμός των υποδικτύων γίνεται από τον διαχειριστή του δικτύου, ο οποίος ανάλογα με τις ανάγκες του οργανισμού, την ήδη υπάρχουσα οργάνωσή του, την τοπολογία του δικτύου και τις μελλοντικές απαιτήσεις ανάπτυξης επιλέγει

την κατάλληλη μορφή υποδικτύωσης. Για την επικοινωνία των υποδικτύων είναι απαραίτητη η χρήση δρομολογητή.

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

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

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

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

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

Πίνακας 3-2:Μάσκες υποδικτύων

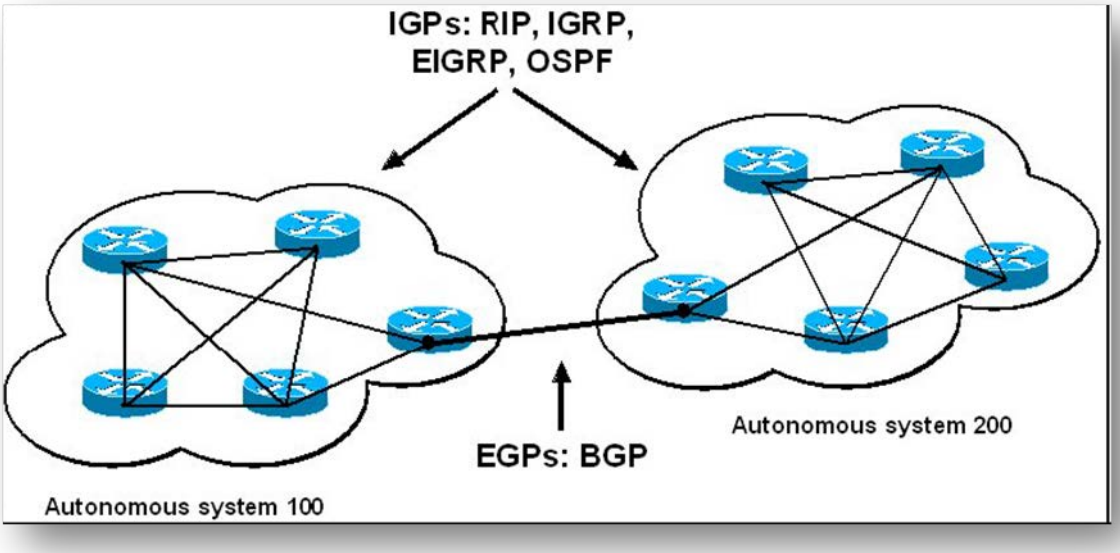
Μάσκα	CIDR value	Μάσκα	CIDR value
255.0.0.0	/8	255.255.240.0	/20
255.128.0.0	/9	255.255.248.0	/21
255.192.0.0	/10	255.255.252.0	/22
255.224.0.0	/11	255.255.254.0	/23
255.240.0.0	/12	255.255.255.0	/24
255.248.0.0	/13	255.255.255.128	/25
255.252.0.0	/14	255.255.255.192	/26
255.254.0.0	/15	255.255.255.224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

3.2 Τα πρωτόκολλα δρομολόγησης (routing protocols)

Τα πρωτόκολλα δρομολόγησης (routing protocols) είναι υπεύθυνα για την επιλογή του καλύτερου δρόμου προς οποιοδήποτε δίκτυο/υποδίκτυο προορισμού, την κατάλληλη ενημέρωση των πινάκων δρομολόγησης και την ανταλλαγή πληροφοριών δρομολόγησης μεταξύ των δρομολογητών ενός δικτύου.

Υπάρχουν δυο βασικά πρωτόκολλα δρομολόγησης:

1. **τα εσωτερικά πρωτόκολλα πύλης IGP (Interior Gateway Protocols)** τα οποία χρησιμοποιούνται για την επικοινωνία των δρομολογητών και την ανταλλαγή των πινάκων δρομολόγησης τους σε ένα **αυτόνομο σύστημα (autonomous system).** (π.χ RIP, OSPF) *Αυτόνομο σύστημα είναι ένα σύνολο δικτύων που εποπτεύονται από μια κοινή αρχή διαχείρησης.*
2. **τα εξωτερικά πρωτόκολλα πύλης EGP (Exterior Gateway Protocols)** τα οποία χρησιμοποιούνται για την επικοινωνία των δρομολογητών και την ανταλλαγή των πινάκων δρομολόγησης τους μεταξύ αυτόνομων συστημάτων. (π.χ BGP).



Εικόνα 3-1: Πρωτόκολλα Δρομολόγησης

Βασική λειτουργία των πρωτοκόλλων δρομολόγησης είναι η εύρεση και η επιλογή του καλύτερου δρόμου για τα δίκτυα προορισμού με τη χρήση κατάλληλων αλγορίθμων δρομολόγησης (routing algorithms). Ο αλγόριθμος δρομολόγησης δημιουργεί έναν αριθμό, τον οποίο ονομάζουμε τιμή κόστους (metric), για κάθε διαδρομή στο δίκτυο. Η διαδρομή με το μικρότερο κόστος για

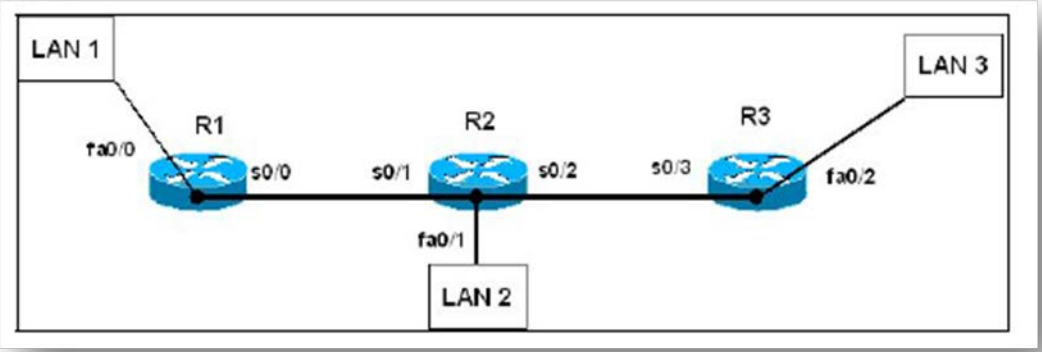
τον ίδιο προορισμό καταχωρείται τελικά στον πίνακα δρομολόγησης. Ανάλογα με την υλοποίηση, ως κόστος μπορεί να χρησιμοποιηθεί ο αριθμός των δρομολογητών (hop count) που περνά το μήνυμα μέχρι να φτάσει στον προορισμό του, το εύρος ζώνης της γραμμής (bandwidth), η καθυστέρηση (delay), το φορτίο της γραμμής (load) και μια σειρά άλλων παραμέτρων ή ένας συνδυασμός από αυτές. Οι αλγόριθμοι δρομολόγησης χωρίζονται σε δυο κατηγορίες:

- **αλγόριθμοι διανύσματος απόστασης (Distance Vector Algorithms),** όπου οι πίνακες δρομολόγησης αποτελούνται από μια σειρά από προορισμούς (vectors) και κόστη τις αποστάσεις (distances) που διανύονται για την προσέγγιση του προορισμού.
- **αλγόριθμοι της κατάστασης της σύνδεσης (Link State Algorithms)**

3.3 Routing Information Protocol (RIP)

Το πρωτόκολλο RIP χρησιμοποιεί τον αλγόριθμο διανύσματος απόστασης και είναι κατάλληλο για τη λειτουργία μικρών δικτύων. Στους πίνακες δρομολόγησης που προκύπτουν υπάρχουν πληροφορίες για το δρόμο και το κόστος της απόστασης προς τα δίκτυα προορισμού. Ως κόστος χρησιμοποιείται ο αριθμός των ενδιάμεσων δρομολογητών μέχρι να φτάσουμε στο δίκτυο προορισμού **(hop count)**. Ο αριθμός των ενδιάμεσων δρομολογητών μέχρι το δίκτυο προορισμού μπορεί να είναι μέχρι 15. Στο πρωτόκολλο RIP οι δρομολογητές περιοδικά (κάθε 30 δευτερόλεπτα), ανακοινώνουν ολόκληρο το περιεχόμενο του πίνακα δρομολόγησής τους, στους άμεσα γειτονικούς δρομολογητές. Ο πίνακας δρομολόγησης μπορεί να μεταδοθεί κι όταν υπάρξει κάποια αλλαγή στην τοπολογία του δικτύου. Έτσι επιτρέπεται στο κάθε δρομολογητή να βλέπει το δίκτυο του γειτονικού δρομολογητή και να προσθέτει το ανάλογο κόστος στην απόσταση που έχει ήδη προσθέσει ο δεύτερος. Το μειονέκτημα της προσέγγισης αυτής είναι ότι καθώς το δίκτυο μεγαλώνει, ανταλλάσσεται ένα μεγάλο ποσό πληροφορίας ανά τακτά χρονικά διαστήματα, ακόμα κι όταν η τοπολογία του δικτύου δεν έχει αλλάξει, με αποτέλεσμα να περιορίζεται το διαθέσιμο εύρος ζώνης και να αυξάνεται ο χρόνος σύγκλισης.

Ως χρόνος σύγκλισης (**convergence time**), ορίζεται ο χρόνος που περνά μέχρι όλοι οι δρομολογητές να συμφωνήσουν σχετικά με την τοπολογία του δικτύου, από τη στιγμή που θα προκύψει μια αλλαγή. Όταν αλλάζει η τοπολογία του δικτύου, εκτελείται ο αλγόριθμος δρομολόγησης και σταματά η κίνηση των δεδομένων που μεταφέρει ο δρομολογητής προς τα διάφορα interfaces του, γιατί δεν γνωρίζει αν το δίκτυο προορισμού είναι διαθέσιμο ή όχι. Άρα, όσο πιο γρήγορα γίνεται η σύγκλιση τόσο πιο γρήγορα θα μεταφερθούν τελικά τα δεδομένα προς τον προορισμό τους.



Εικόνα 3-2: Δρομολόγηση RIP

Σύμφωνα με τα παραπάνω οι πίνακες δρομολόγησης που προκύπτουν στο παραπάνω δίκτυο θα είναι:

Πίνακας 3-3: Πίνακας Δρομολόγησης

R1		
network	**next hop router**	**metric**
LAN1	connected	0
LAN2	R2	1
LAN3	R3	2
R2		
network	**next hop router**	**metric**
LAN1	R1	1
LAN2	connected	0
LAN3	R3	1
R3		
network	**next hop router**	**metric**
LAN1	R2	2
LAN2	R2	1
LAN3	connected	0

3.4 OSPF (Open Shortest Path First)

Το OSPF είναι πρωτόκολλο δρομολόγησης IP δικτύων τύπου IGP(Interior Gateway Protocol), δηλαδή διανέμει την πληροφορία εντός ενός αυτόνομου συστήματος παρότι μπορεί να στείλει και να λάβει διαδρομές και από άλλα. Βασίζεται στον αλγόριθμο του Dijkstra. Δεν υπάρχει περιορισμός στον αριθμό των hops, ενώ το RIP περιορίζεται στα 15 hops. Έχει τη δυνατότητα να σπάσει το IP δίκτυο σε πολλά υποδίκτυα διαφόρων μεγεθών, παρέχοντας μεγαλύτερη ευελιξία στον διαχειριστή και επίσης παρέχει λειτουργία αυθεντικοποίησης των μηνυμάτων δρομολόγησης. Τέλος επιτρέπει τη μεταφορά και το μαρκάρισμα των διαδρομών οι οποίες εισάγονται σε ένα αυτόνομο σύστημα από εξωτερικά πρωτόκολλα.

3.5 Σύγκριση RIP v OSPF

Οι RIP routers μαζεύουν μεγάλο ποσό άχρηστης πληροφορίας και δημιουργούνται λανθασμένες δρομολογήσεις λόγω της μεγάλης καθυστέρησης

σύγκλισης. Οι ενημερώσεις στέλνονται περιοδικά ανά 30 sec, αφορούν όλη την πληροφορία δρομολόγησης και γίνονται με broadcast μετάδοση.

Το γεγονός αυτό αυτόματα κάνει το RIP ακατάλληλο για χρήση σε ασύρματα δίκτυα και για μεγάλα δίκτυα ή δίκτυα που αλλάζουν αρκετά γρήγορα και συχνά

Οι αποφάσεις δρομολόγησης λαμβάνονται με βάση μόνο των αριθμό των συνδέσεων και όχι το κόστος – εύρος της κάθε σύνδεσης. Έτσι προτιμάται μια κοντινή διαδρομή έστω και αν υπάρχει μακρύτερη με περισσότερο εύρος.

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

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

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

Επίσης απαιτείται περισσότερη επεξεργαστική ισχύς και μνήμη στους δρομολογητές.

ΚΕΦΑΛΑΙΟ 4

ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΑΝΑΠΤΥΞΗ ΤΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΥΠΟΣΤΗΡΙΞΗΣ ΔΙΚΤΥΑΚΩΝ ΠΕΙΡΑΜΑΤΩΝ

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

Επίσης θα γίνει πλήρης παρουσίαση του περιβάλλοντος και των λειτουργιών που υποστηρίζει.

4.1 Η εφαρμογή quiz

4.1.1 Γενικά

Το αντικείμενο μελέτης για αυτήν την διπλωματική εργασία όπως προδίδει και ο τίτλος της, ήταν ο Σχεδιασμός και Ανάπτυξη Περιβάλλοντος Υποστήριξης Δικτυακών Πειραμάτων.

Πρόκειται για μια PHP εφαρμογή με την οποία μπορούμε να δημιουργήσουμε online κουίζ και τεστ καθώς και να πάρουμε αποτελέσματα από αυτά.

Η προτεινόμενη εφαρμογή λαμβάνει υπ’ όψη της τη δυνατότητα πρόσβασης σε αυτή από πλήθος συσκευών όπως Η/Υ, ταμπλέτες, έξυπνα τηλέφωνα κ.α. μέσω ενός φυλλομετρητή (browser). Η εφαρμογή μπορεί να εγκατασταθεί στο διαδίκτυο ή ακόμα και σε ένα τοπικό δίκτυο.

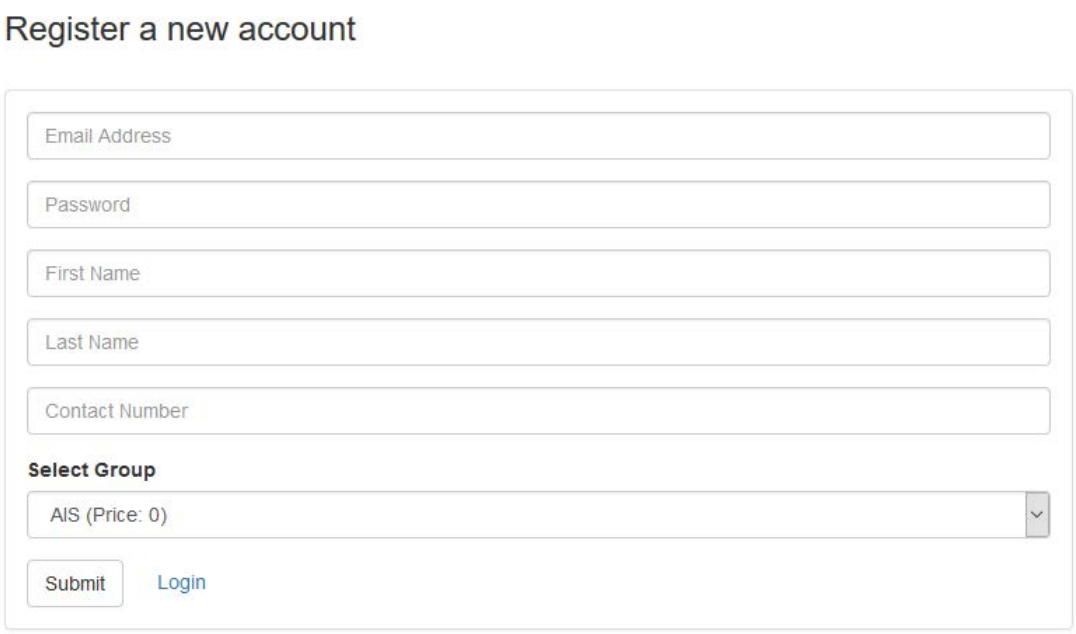
Οι ελάχιστες απαιτήσεις για την εκτέλεση της εφαρμογής είναι:

- PHP 5+
- MySql Database (v5+)
- Linux or Windows server
- 35 MB Disk space (web space)

Η εφαρμογή υποστηρίζει δύο επίπεδα πρόσβασης:

1. Διαχειριστής
2. Απλός χρήστης

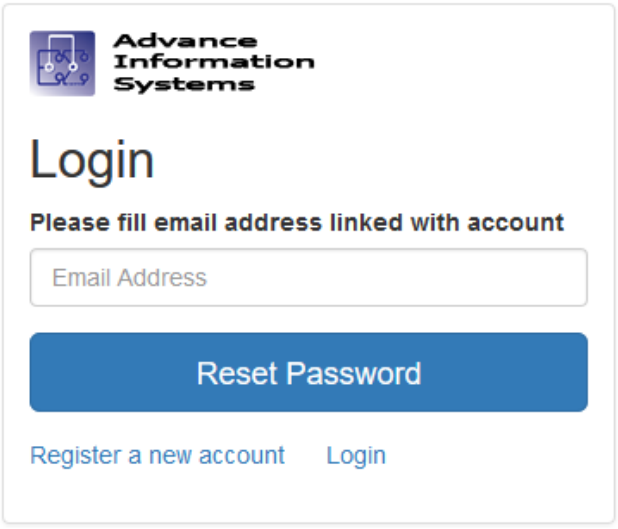
4.1.2 Εγγραφή νέου Χρήστη (Register a new account)



Εικόνα 4-1: Εγγραφή νέου Χρήστη

Από την επιλογή αυτή μπορεί να εγγραφεί ένας νέος χρήστης αφού συμπληρώσει τα στοιχεία του στα σχετικά πεδία.

4.1.3 Ξέχασα τον κωδικό μου (Forgot password)



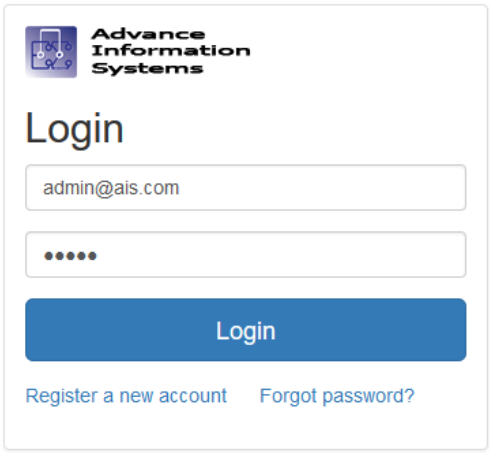
Εικόνα 4-2: Επαναφορά Κωδικού

Από την επιλογή αυτή μπορούμε να κάνουμε επαναφορά του κωδικού μας αφού το σύστημα θα μας στείλει στο email μας το σχετικό σύνδεσμο.

4.2 Η εφαρμογή από την πλευρά του Διαχειριστή

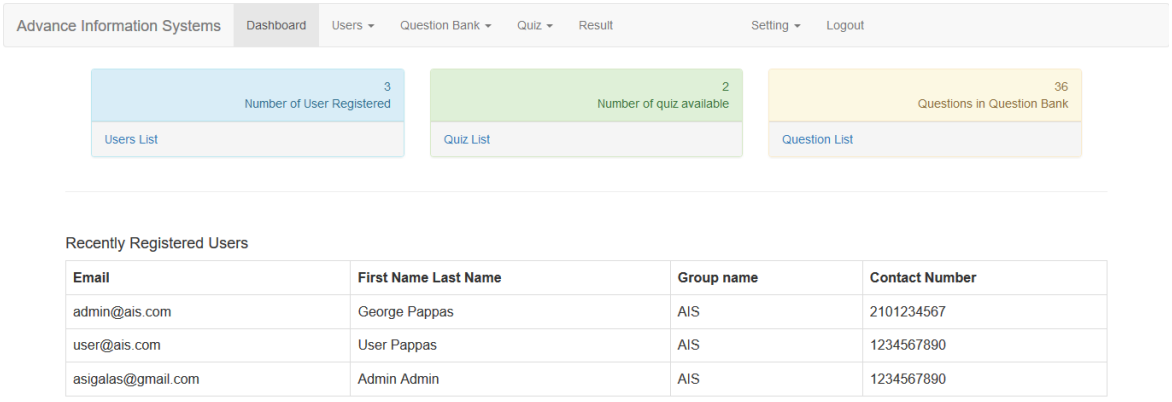
4.2.1 Η οθόνη σύνδεσης

Για την σύνδεση των διαχειριστών στην εφαρμογή απαιτείτε το email του διαχειριστή και ο κωδικός του.



Εικόνα 4-3: Σύνδεση Διαχειριστή

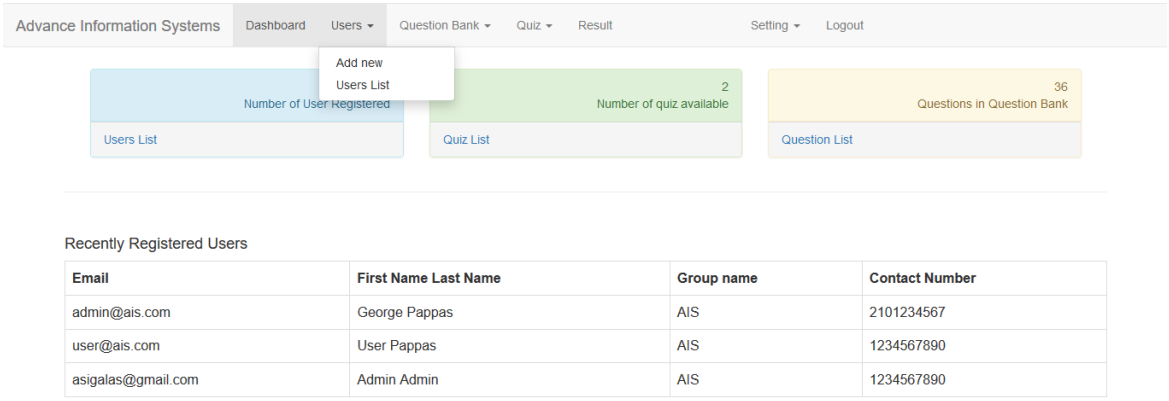
4.2.2 Η αρχική οθόνη Διαχειριστή (Dashboard)



Εικόνα 4-4: Αρχική οθόνη Διαχειριστή

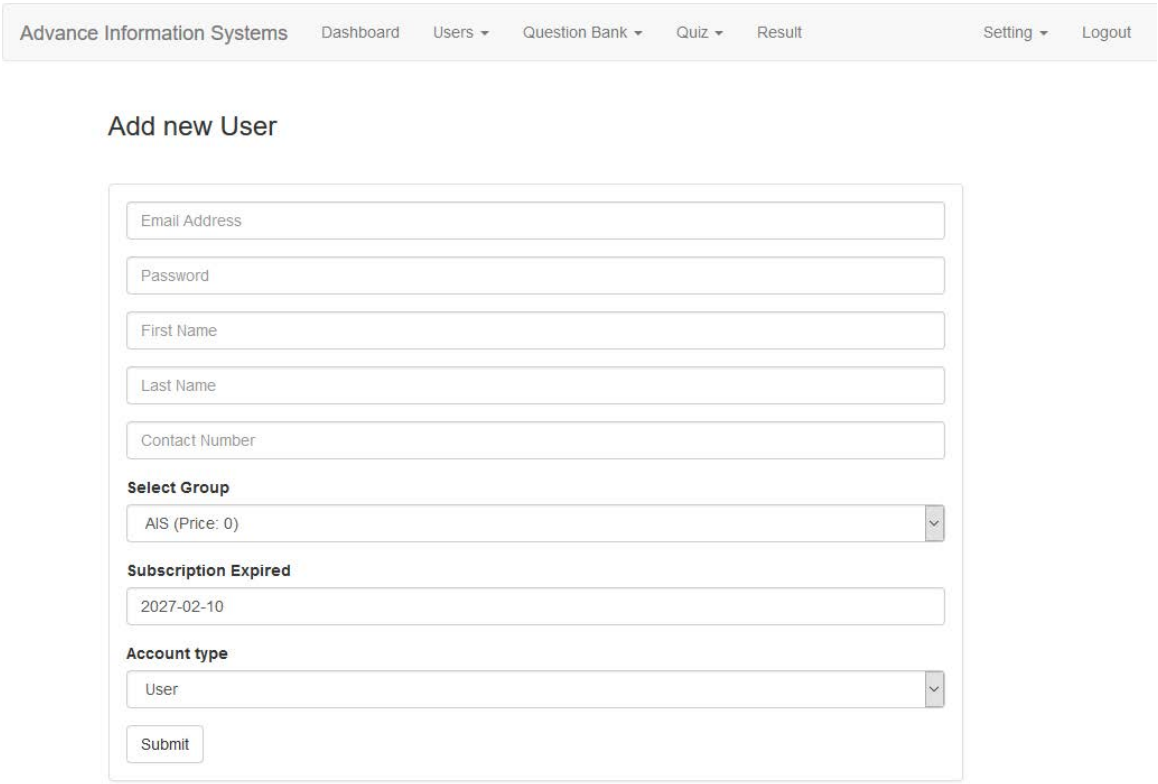
Στην αρχική οθόνη ο Διαχειριστής βλέπει το πλήρες μενού της εφαρμογής και επιπλέον πληροφορίες για τον αριθμό εγγεγραμμένων χρηστών, τον αριθμό των τεστ και των αριθμό των ερωτήσεων που υπάρχουν στην εφαρμογή.

4.2.3 Το μενού Χρήστες (Users)



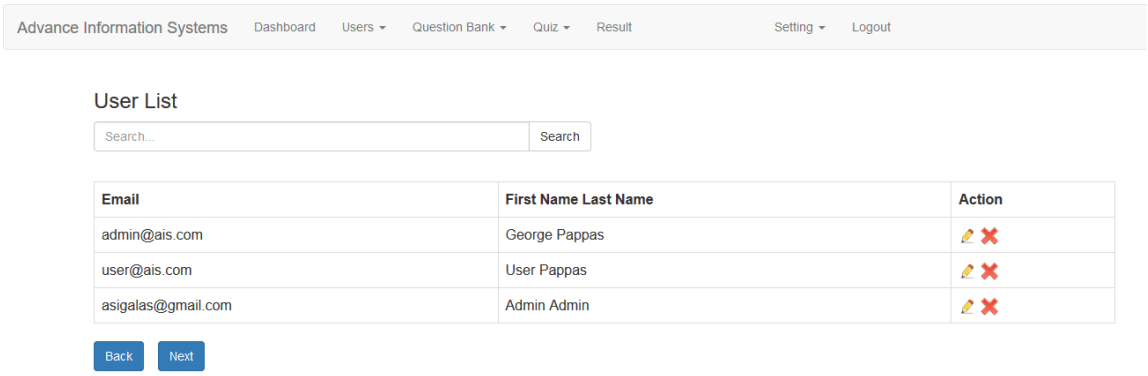
Εικόνα 4-5: Μενού Χρήστες (Users Menu)

Από το μενού Users έχουμε την επιλογή προσθήκης νέου χρήστη (**Add new**) και την επιλογή προβολής της λίστας των ήδη εγγεγραμμένων χρηστών (**Users List**).



Εικόνα 4-6: Προσθήκη νέου χρήστη

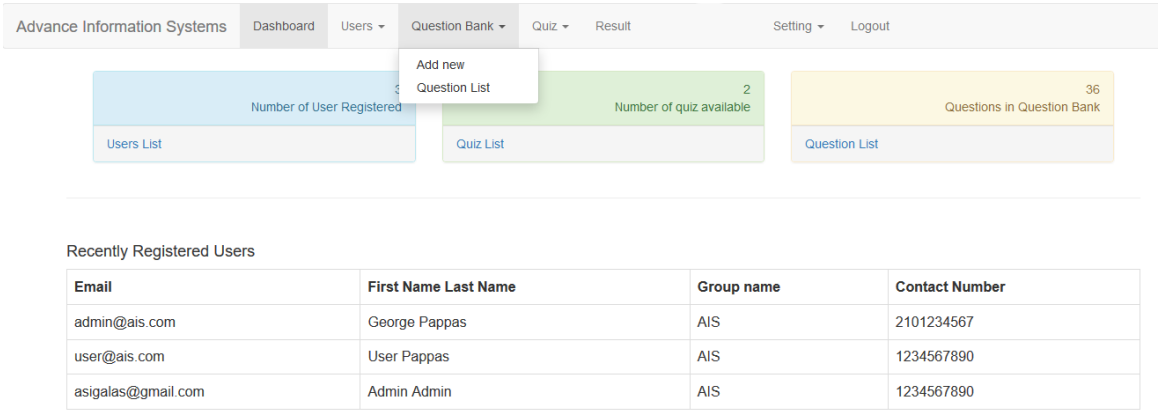
Στην προσθήκη νέου χρήστη καταχωρούμε το email του το οποίο χρησιμοποιείται και ως user name, τον κωδικό πρόσβασης στην εφαρμογή, τα στοιχεία του, την ομάδα χρηστών στην οποία ανήκει, την ημερομηνία λήξης της πρόσβασης του στην εφαρμογή και τον τύπο χρήστη (χρήστης ή διαχειριστής).



Εικόνα 4-7: Λίστα χρηστών (Users List)

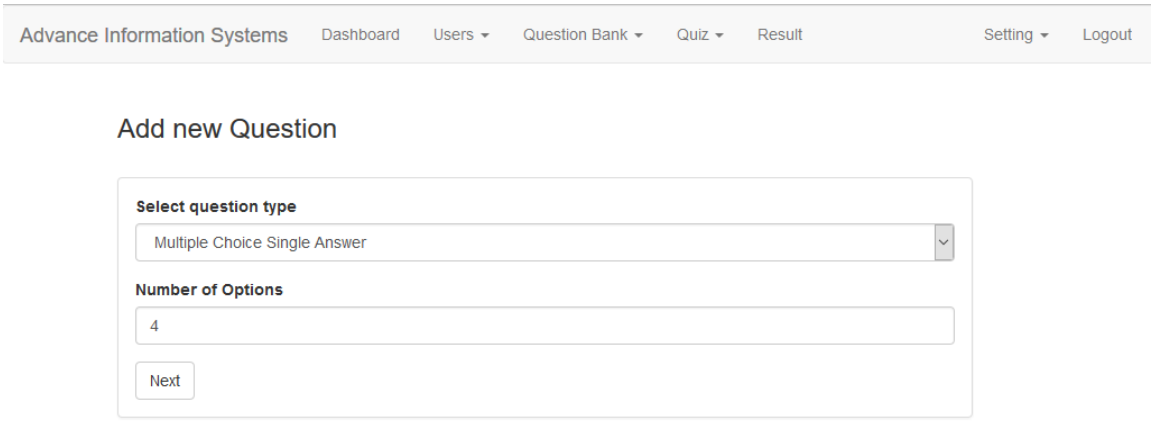
Από την λίστα χρηστών μπορούμε να διαγράψουμε ένα χρήστη ή να επεξεργαστούμε τα στοιχεία του.

4.2.4 Το μενού ερωτήσεις (Question Bank)



Εικόνα 4-8: Το μενού ερωτήσεις (Question Bank)

Από το μενού **Question Bank** έχουμε την επιλογή προσθήκης νέας ερώτησης (**Add new**) και την επιλογή προβολής της λίστας των ήδη καταχωρημένων ερωτήσεων (**Question List**).

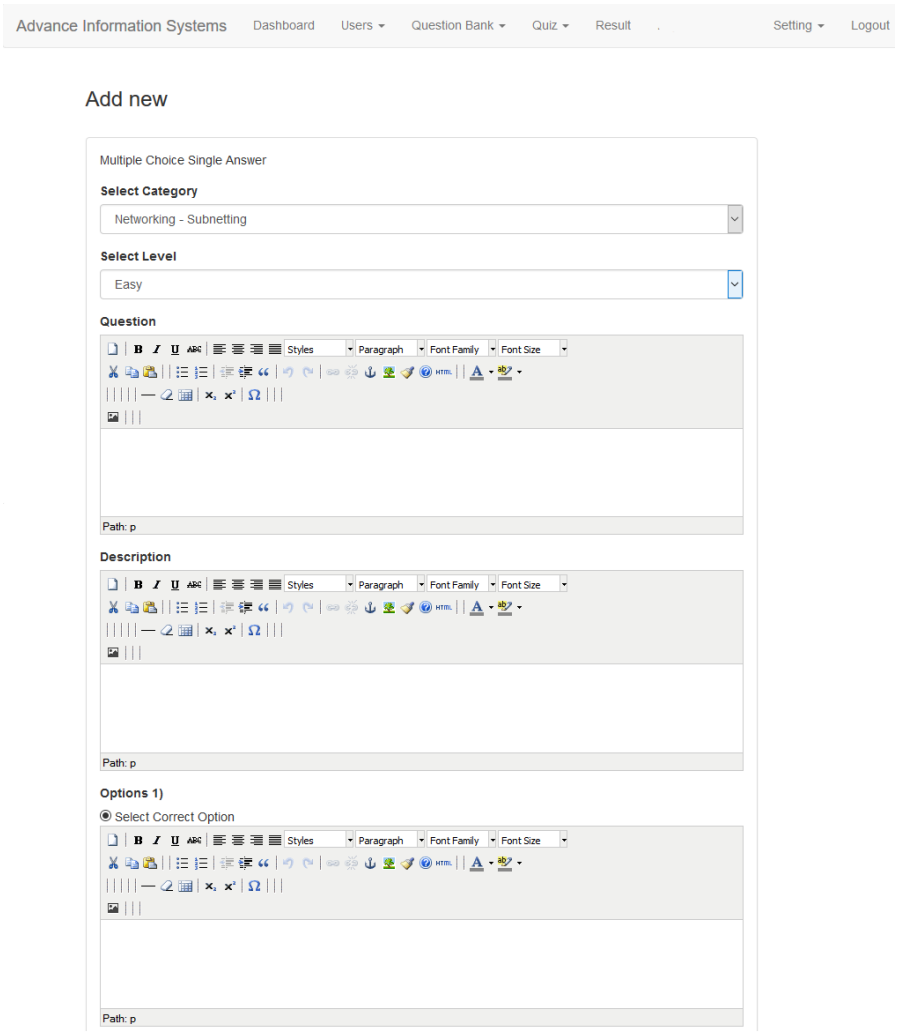


Εικόνα 4-9: Επιλογή τύπου ερώτησης

Στη διαδικασία προσθήκης νέας ερώτησης επιλέγουμε τον τύπο της ερώτησης ο οποίος είναι ένας από τους παρακάτω:

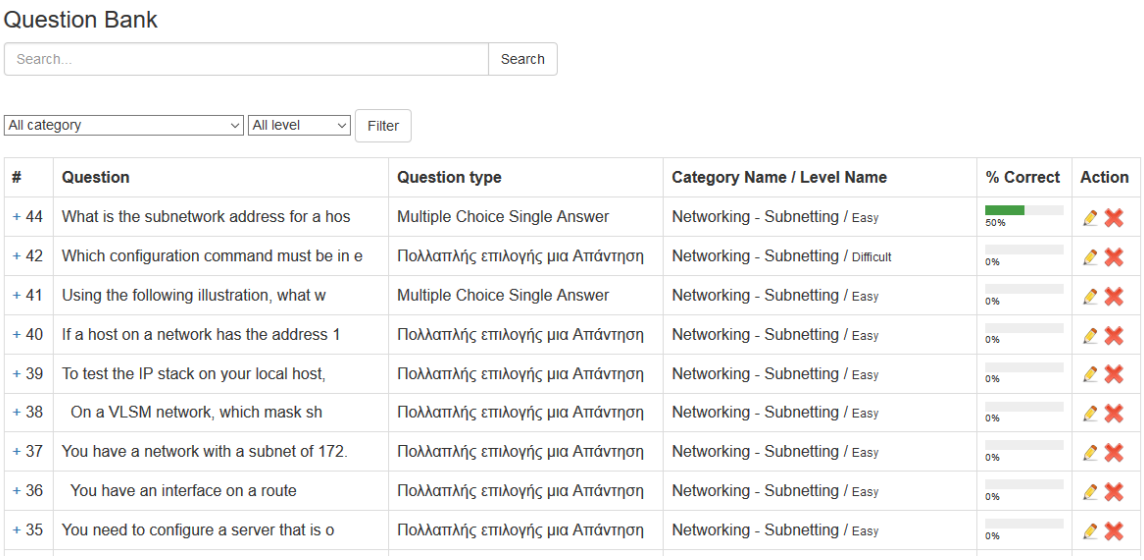
- Πολλαπλής Επιλογής Μία Απάντηση (Multiple Choice Single Answer)
- Πολλαπλής Επιλογής Πολλαπλές Απαντήσεις (Multiple Choice Multiple Answers)
- Αντιστοίχιση (Match the Column)
- Σύντομη Απάντηση (Short Answer)
- Εκτεταμένη Απάντηση (Long Answer)

Επιλέγουμε και το αριθμό των επιλογών που θα έχουμε στην ερώτηση.



Εικόνα 4-10: Καταχώρηση Ερώτησης

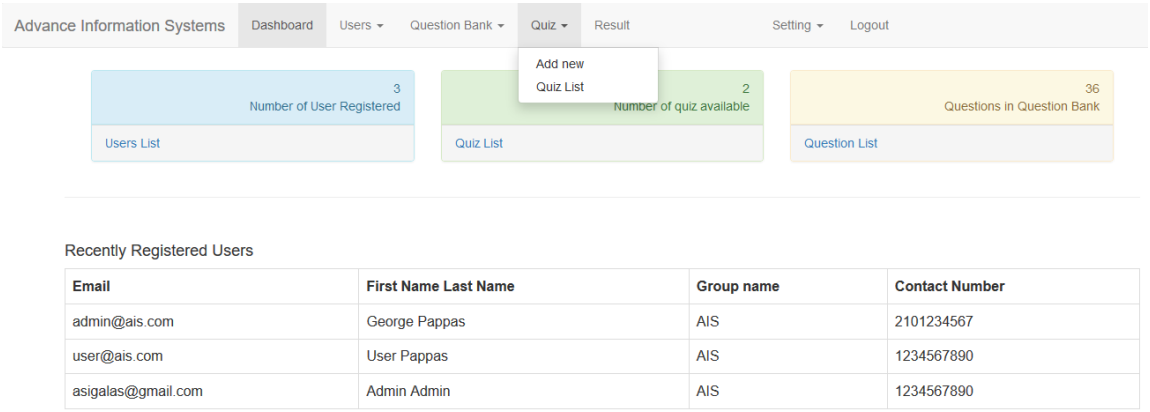
Κατόπιν επιλέγουμε την κατηγορία και το επίπεδο δυσκολίας στην οποία ανήκει η ερώτηση και καταχωρούμε την ερώτηση και τις επιλογές της επιλέγοντας την σωστή ή τις σωστές επιλογές.



Εικόνα 4-11: Λίστα Ερωτήσεων (Question List)

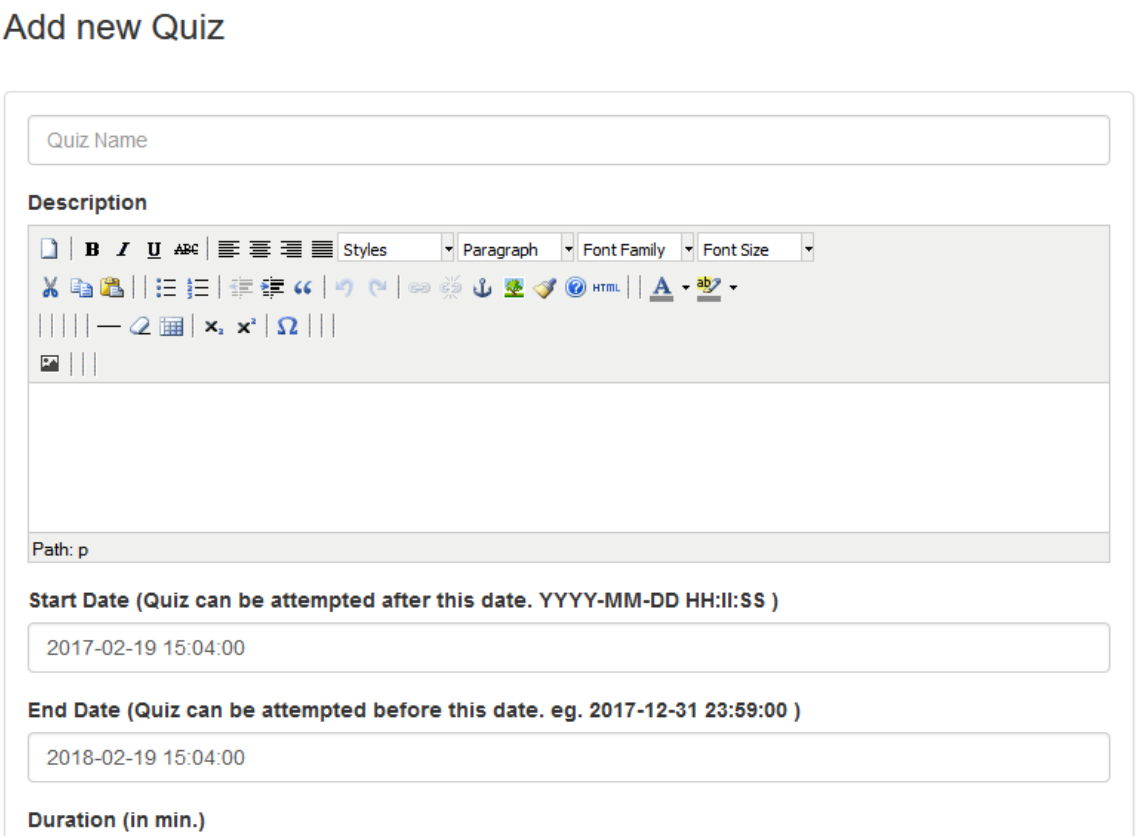
Από την λίστα ερωτήσεων μπορούμε να διαγράψουμε ή να επεξεργαστούμε τα στοιχεία μίας ερώτησης.

4.2.5 Το μενού Τεστ (Quiz)



Εικόνα 4-12: Το μενού τεστ (Quiz)

Από το μενού **Quiz** έχουμε την επιλογή προσθήκης νέου τεστ (**Add new**) και την επιλογή προβολής της λίστας των ήδη καταχωρημένων quiz (τεστ) (**Quiz List**).

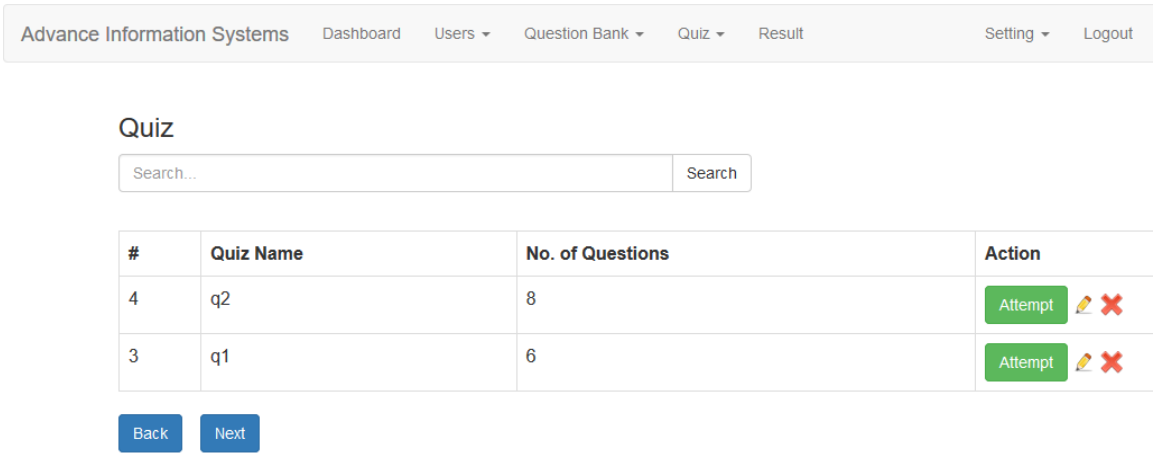


Εικόνα 4-13: Προσθήκη τεστ

Στη διαδικασία προσθήκης νέου quiz (τεστ) συμπληρώνουμε τα εξής πεδία:

- Όνομα quiz
- Περιγραφή
- Ημερομηνία και ώρα έναρξης
- Ημερομηνία και ώρα λήξης
- Διάρκεια σε λεπτά
- Μέγιστες προσπάθειες ανά χρήστη
- Επί της 100 ποσοστό για να περάσει κάποιος το τεστ
- Το σκορ για κάθε σωστή απάντηση (1)
- Το σκορ για κάθε λάθος απάντηση (0)
- Τα IP που μπορούν να συνδεθούν για το τεστ
- Αν επιτρέπεται να βλέπουμε τις σωστές απαντήσεις μετά από την τελική υποβολή του
- Την ομάδα χρηστών που μπορεί να κάνει το τεστ
- Τον τρόπο προσθήκης των ερωτήσεων (Αυτόματα ή με επιλογή)
- Αν θέλουμε να εκδοθεί πιστοποιητικό

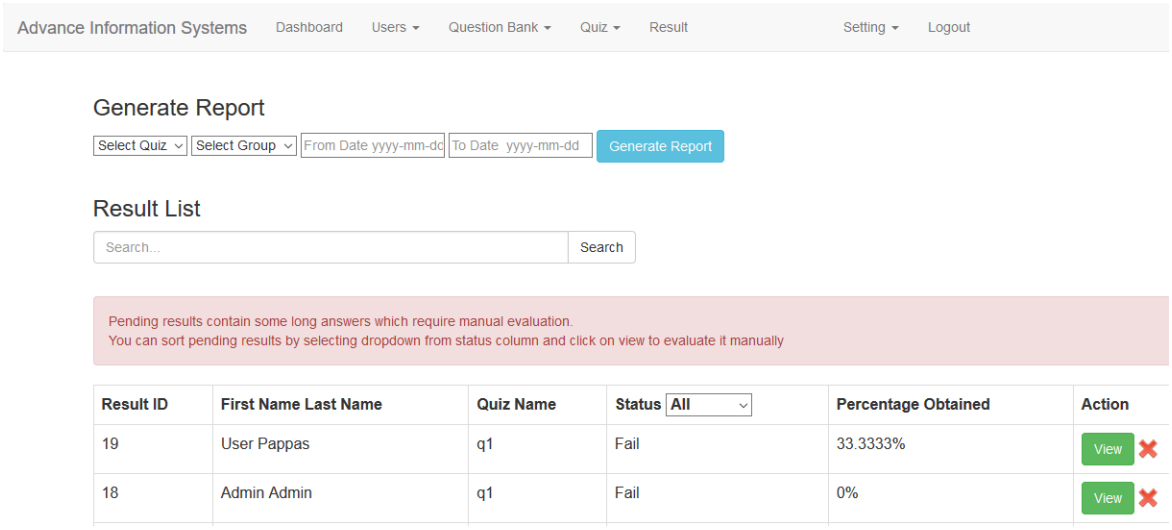
Διαλέγοντας τον αυτόματο τρόπο διαλέγουμε την κατηγορία ερωτήσεων, τον βαθμό δυσκολίας, τον αριθμό των ερωτήσεων που θα προστεθούν και η εφαρμογή κάνει τυχαία επιλογή ερωτήσεων ανάλογα με τα κριτήρια. Ενώ αν διαλέξουμε να επιλέξουμε εμείς τις ερωτήσεις τότε εμφανίζετε η λίστα των ερωτήσεων από την οποία μπορούμε να προσθέσουμε ερωτήσεις στο τεστ που δημιουργούμε.



Εικόνα 4-14: Λίστα Τεστ (Quiz List)

Από την επιλογή Quiz List μπορούμε να δούμε την λίστα των quiz (τεστ) που έχουν δημιουργηθεί και έχουμε την επιλογή να κάνουμε το τεστ, να το επεξεργαστούμε ή να το διαγράψουμε.

4.2.6 Το μενού Result (Αποτέλεσμα)

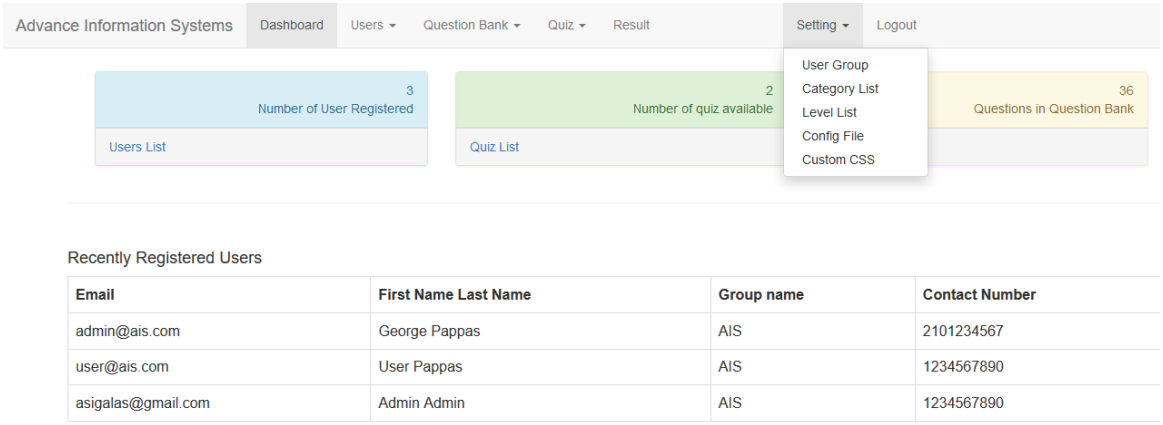


Εικόνα 4-15: Το μενού Result (Αποτέλεσμα)

Από το μενού αυτό μπορούμε να δούμε τα αποτελέσματα των τεστ που έχουν γίνει από τους χρήστες.

Από την επιλογή View μπορούμε να δούμε το αποτέλεσμα αναλυτικά και να το εκτυπώσουμε σε pdf μορφή ή να διαγράψουμε το αποτέλεσμα από την επιλογή X.

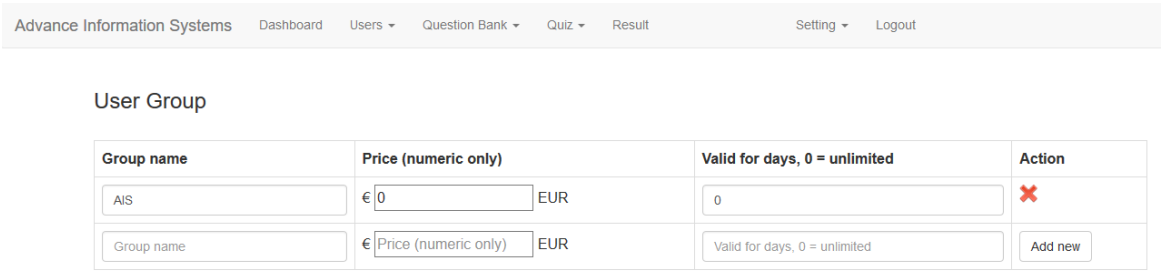
4.2.7 Το μενού Setting (Ρύθμιση)



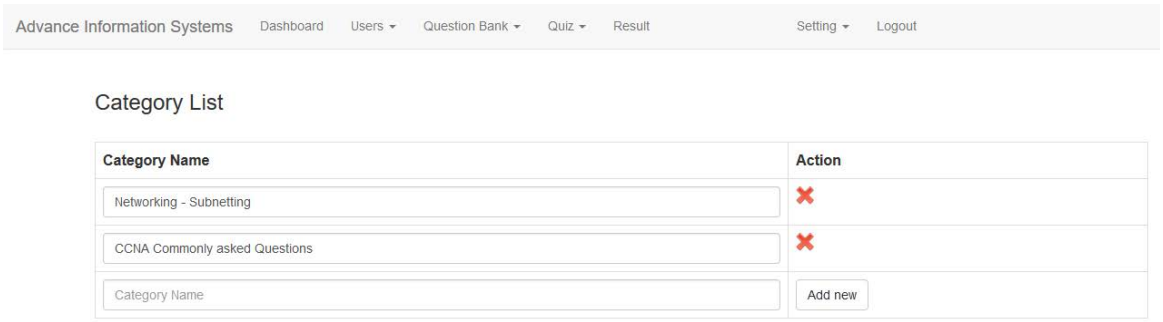
Εικόνα 4-16: Το μενού Setting (Ρύθμιση)

Από το μενού Setting μπορούμε:

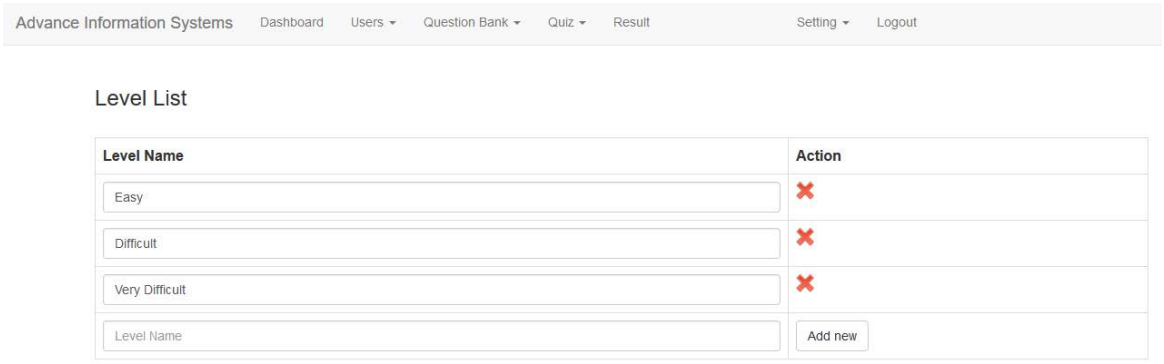
- Να διαχειριστούμε τις ομάδες χρηστών (User Group)
- Να διαχειριστουμε τις κατηγορίες ερωτήσεων (Category List)
- Να διαχειριστούμε τα επίπεδα δυσκολίας (Level List)
- Να παραμετροποιήσουμε το αρχείο config της εφαρμογής
- Να τροποποιήσουμε το αρχείο Custom CSS



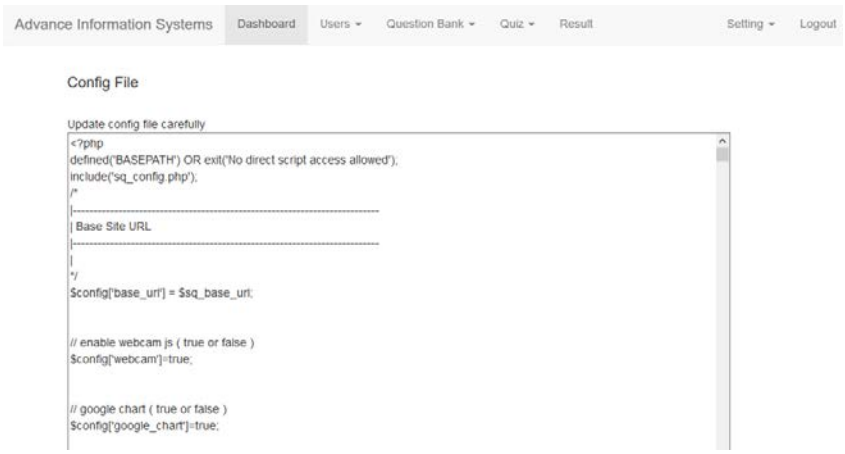
Εικόνα 4-17: User Group



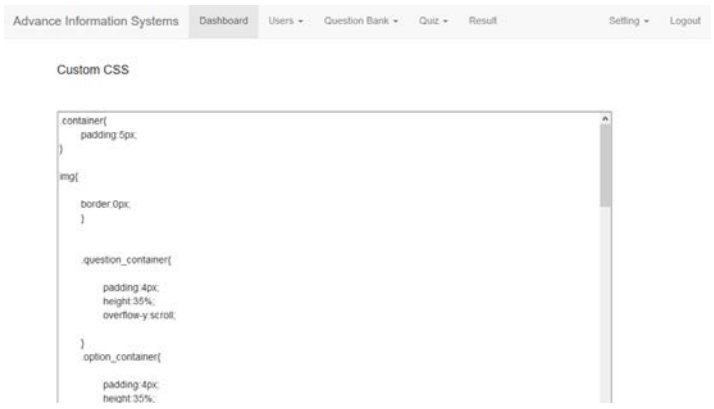
Εικόνα 4-18: Category List



Εικόνα 4-19: Level List



Εικόνα 4-20: Config File



Εικόνα 4-21: Custom CSS

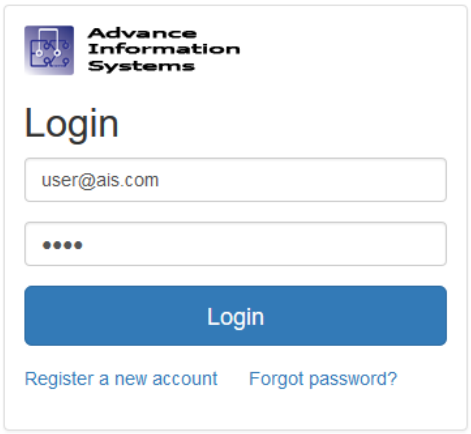
4.2.8 Το μενού Logout (Έξοδος)

Από την επιλογή Logout γίνεται η έξοδος από την εφαρμογή

4.3 Η εφαρμογή από την πλευρά του Χρήστη

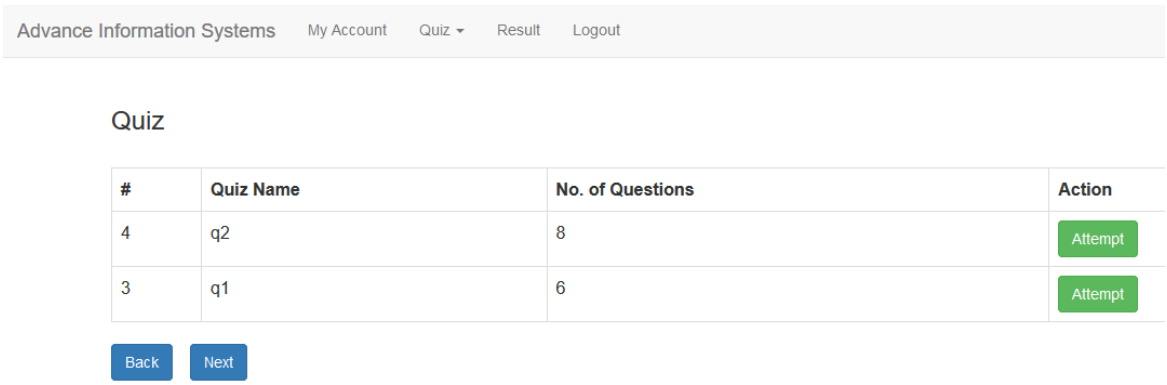
4.3.1 Η οθόνη σύνδεσης

Για την σύνδεση των χρηστών στην εφαρμογή απαιτείτε το email του χρήστη και ο κωδικός του.



Εικόνα 4-22: Σύνδεση Χρήστη

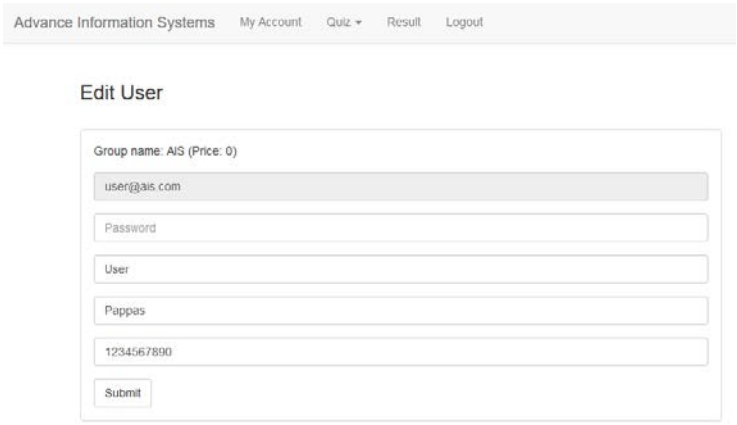
4.3.2 Η αρχική οθόνη Χρήστη (Dashboard)



Εικόνα 4-23: Αρχική οθόνη Χρήστη

Στην αρχική οθόνη ο Χρήστης βλέπει το πλήρες μενού της εφαρμογής και τα quiz (τεστ) που μπορεί να κάνει πατώντας το Action **Attempt**.

4.3.3 Το μενού My Account (Ο λογαριασμός μου)



Εικόνα 4-24: Το μενού My Account

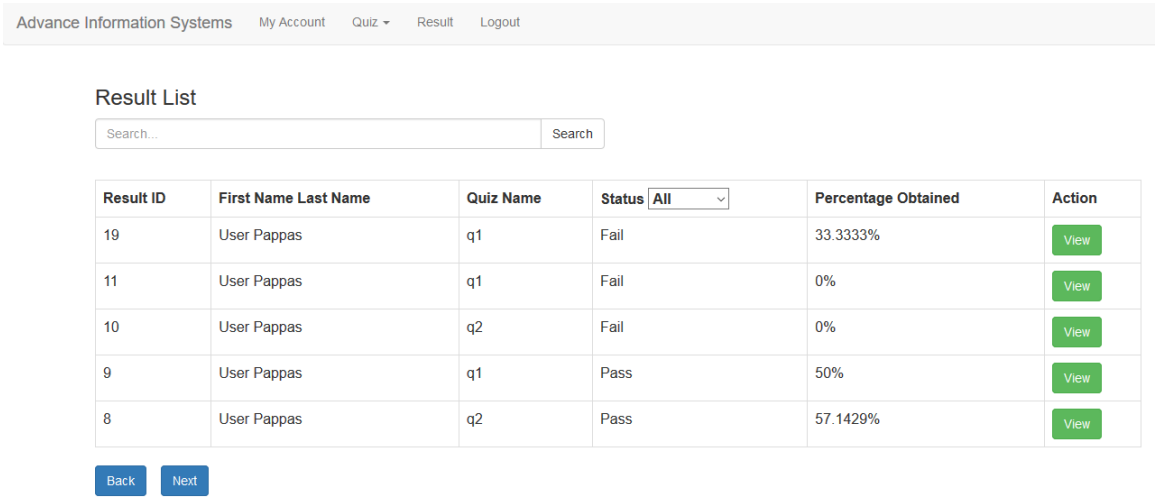
Από το μενού My Account ο χρήστης μπορεί να επεξεργαστεί τα στοιχεία του στο σύστημα και να αλλάξει τον κωδικό πρόσβασής του.

4.3.4 Το μενού Quiz

Από το μενού Quiz ο χρήστης μπορεί να δει τη λίστα των τεστ στα οποία έχει πρόσβαση.

4.3.5 Το μενού Result

Από το μενού Result ο χρήστης μπορεί να δει αναλυτικά τα αποτελέσματα των τεστ που έχει ολοκληρώσει.



Εικόνα 4-25: Αποτελέσματα Χρήστη

ΚΕΦΑΛΑΙΟ 5

ΣΥΜΠΕΡΑΣΜΑΤΑ

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

5.1 Open source Software (Λογισμικό ανοικτού κώδικα)

Για την ανάπτυξη της εφαρμογής χρησιμοποιήθηκε λογισμικό ανοικτού κώδικα. Το λογισμικό ανοικτού κώδικα διατίθεται με ειδικές άδειες, οι οποίες επιτρέπουν στους χρήστες να μελετήσουν, να τροποποιήσουν και να βελτιώσουν το λογισμικό.

Σαν περιβάλλον ανάπτυξης χρησιμοποιήθηκε το NetBeans IDE και το Notepad++.

Για την εκτέλεση της εφαρμογής χρησιμοποιήθηκε το περιβάλλον Xampp που υποστηρίζει PHP 5+, MySql Database (v5+) και Apache web server που καλύπτει της ελάχιστες απαιτήσεις της.

5.2 CodeIgniter

Το CodeIgniter [11] είναι ένα ισχυρό PHP framework, μικρό σε μέγεθος πακέτο εργαλείων, το οποίο είναι μια καλή βάση για την δημιουργία εφαρμογών διαδικτύου.

Είναι συμβατό με PHP και υποστηρίζει διάφορες βάσεις δεδομένων όπως την MySql.

Στηριζεται στο Model-View-Controller (MVC), ένα αρχιτεκτονικό μοτίβο που χωρίζει μια εφαρμογή σε τρία βασικά λογικά κομμάτια:

- το μοντέλο (Model) που διαχειρίζεται τα δεδομένα της εφαρμογής
- την προβολή (View) που έχει να κάνει με την διεπαφή χρήστη
- τον ελεγκτή (Controller) που ενεργεί ως διεπαφή μεταξύ του μοντέλου και της προβολής για να επεξεργαστεί τις ενέργειες του χρήστη και τα δεδομένα ώστε να παράξει το τελικό αποτέλεσμα.

5.3 Bootstrap

Το Bootstrap [12] είναι μια συλλογή εργαλείων ανοιχτού κώδικα (Ελεύθερο λογισμικό) για τη δημιουργία ιστοσελίδων και διαδικτυακών εφαρμογών. Περιέχει

HTML και CSS για τις μορφές τυπογραφίας, κουμπιά πλοήγησης και άλλων στοιχείων του περιβάλλοντος, καθώς και προαιρετικές επεκτάσεις JavaScript. Είναι το πιο δημοφιλές πρόγραμμα στο GitHub και έχει χρησιμοποιηθεί από τη NASA και το MSNBC, μεταξύ άλλων.

Το Bootstrap έχει σχετικά ελλιπή υποστήριξη για HTML5 και CSS, αλλά είναι συμβατό με όλους τους φυλλομετρητές (browsers). Βασικές πληροφορίες συμβατότητας των ιστοσελίδων ή εφαρμογές είναι διαθέσιμες για όλες τις συσκευές και τα προγράμματα περιήγησης.

Από την έκδοση 2.0 υποστηρίζει επίσης ανταποκρίσιμο σχεδιασμό (responsive design). Αυτό σημαίνει ότι η διάταξη των ιστοσελίδων προσαρμόζεται δυναμικά, λαμβάνοντας υπόψη τα χαρακτηριστικά της συσκευής που χρησιμοποιείται (PC, tablet, κινητό τηλέφωνο).

5.4 TinyMCE

Ο TinyMCE (Tiny Moxiecode Content Editor) [13] είναι ένας WYSIWYG συντάκτης περιεχομένου ανοικτού κώδικα σε γλώσσα javascript. Είναι συμβατός με τους περισσότερους φυλλομετρητές όπως τους Internet Explorer, Mozilla Firefox, Safari, Opera και Google Chrome. Προσφέρει εργαλεία μορφοποίησης HTML, όπως έντονη γραφή, πλάγια γραφή, υπογράμμιση, ταξινομημένες και μη ταξινομημένες λίστες, διαφορετικούς τύπους ευθυγράμμισης, in-line τοποθέτηση των εικόνων και βίντεο, κ.λπ. Επιτρέπει στους χρήστες να επεξεργάζονται έγγραφα HTML σε απευθείας σύνδεση. Έχει πλήθος επιλογών που μπορούν να ρυθμιστούν κατά την ενσωμάτωση του σε ένα πρόγραμμα.

5.5 Μελλοντικές προσθήκες για στην εφαρμογή

Η εφαρμογή quiz, παρέχει στο χρήστη τη δυνατότητα δημιουργίας τεστ ερωτοαπαντήσεων για εκπαιδευτικούς σκοπούς. Η αυξανόμενη τάση για χρήση της τεχνολογίας στην εκπαίδευση δημιουργεί την ανάγκη για τη δημιουργία και εξέλιξη αυτού του είδους των εφαρμογών.

Αν και η εφαρμογή διαθέτει δυνατότητα χρήσης πολλαπλών μεταφράσεων μέσω των σχετικών αρχείων γλώσσας σε μελλοντική επέκταση θα μπορούσε η επιλογή γλώσσας να γίνεται από το περιβάλλον χρήσης της.

Μια επίσης καλή ιδέα για λειτουργικότητα, θα ήταν η δυνατότητα να μπορούν οι χρήστες να επικοινωνήσουν μέσω προσωπικών μηνυμάτων μέσα από το

περιβάλλον της εφαρμογής. Να γίνει δηλαδή η εφαρμογή ένα σημείο επικοινωνίας μεταξύ των χρηστών της.

Επίσης μελλοντικά θα μπορούσε να προστεθεί σύστημα ανακοινώσεων με δυνατότητα σύναψης αρχείων στα μηνύματα, χωρισμένες ίσως ανά ομάδα χρηστών. Έτσι θα μπορούσε να υπάρχει μαζική πληροφόρηση για εκπαιδευτικούς σκοπούς.

Τέλος μια σημαντική προσθήκη στην εφαρμογή θα ήταν η δυνατότητα αποστολής σύντομων μηνυμάτων στο κινητό των χρηστών. Το περιεχόμενο του μηνύματος θα μπορούσε να είναι, η δημιουργία ενός νέου τεστ που αφορά στον χρήστη, ο χρόνος στον οποίο πρέπει να έχει ολοκληρωθεί, πλήθος άλλων πληροφοριών και τέλος τα αποτελέσματα του τεστ.

ΠΑΡΑΡΤΗΜΑ Α’

Στο παράρτημα αυτό παρατίθενται μερικές από τις ερωτήσεις που έχουν αρχικά καταχωρηθεί στην εφαρμογή.

Networking Basics

1. How long is an IPv6 address?

A. 32 bits
B. 128 bytes
C. 64 bits
D. 128 bits
Answer: Option D

Explanation: An IPv6 address is 128 bits long.

2. What flavor of Network Address Translation can be used to have one IP address allow many users to connect to the global Internet?

A. NAT
B. Static
C. Dynamic
D. PAT
Answer: Option D

Explanation: Port Address Translation (PAT) allows a one-to-many approach to network address translation.

3. What are the two main types of access control lists (ACLs)?

1. Standard
2. IEEE
3. Extended
4. Specialized

A. 1 and 3
B. 2 and 4
C. 3 and 4
D. 1 and 2
Answer: Option A

Explanation: Standard and extended access control lists (ACLs) are used to configure security on a router.

4. What command is used to create a backup configuration?

A. copy running backup
B. copy running-config startup-config
C. config mem
D. wr mem
Answer: Option B

Explanation: The command to back up the configuration on a router is copy running-config startup-config.

5. You have 10 users plugged into a hub running 10Mbps half-duplex. There is a server connected to the switch running 10Mbps half-duplex as well. How much bandwidth does each host have to the server?

A. 100 kbps
B. 1 Mbps
C. 2 Mbps
D. 10 Mbps
Answer: Option D

Explanation: Each device has 10 Mbps to the server

6. Which WLAN IEEE specification allows up to 54Mbps at 2.4GHz?

A. A
B. B
C. G
D. N
Answer: Option C

Explanation: IEEE 802.11B is 2.4GHz, but with a maximum of only 11Mbps. IEEE 802.11G is in the 2.4GHz range, with a top speed of 54Mbps.

7. Which of the following is the valid host range for the subnet on which the IP address 192.168.168.188 255.255.255.192 resides?

A. 192.168.168.129-190
B. 192.168.168.129-191
C. 192.168.168.128-190
D. 192.168.168.128-192
Answer: Option A

Explanation: 256 - 192 = 64. 64 + 64 = 128. 128 + 64 = 192. The subnet is 128, the broadcast address is 191, and the valid host range is the numbers in between, or 129-190.

8. To back up an IOS, what command will you use?

A. backup IOS disk
B. copy ios tftp
C. copy tftp flash
D. copy flash tftp
Answer: Option D

Explanation: The command copy flash tftp will prompt you to back up an existing IOS in flash to a TFTP host.

9. What protocol does PPP use to identify the Network layer protocol?

A. NCP
B. ISDN
C. HDLC
D. LCP
Answer: Option A

Explanation: Network Control Protocol is used to help identify the Network layer protocol used in the packet.

10. Which of the following commands will allow you to set your Telnet password on a Cisco router?

A. line telnet 0 4
B. line aux 0 4
C. line vty 0 4
D. line con 0
Answer: Option C

Explanation: The command line vty 0 4 places you in a prompt that will allow you to set or change your Telnet password.

11. Which protocol does DHCP use at the Transport layer?

A. IP
B. TCP
C. UDP
D. ARP
Answer: Option C

Explanation: User Datagram Protocol is a connection network service at the Transport layer, and DHCP uses this connectionless service.

12. Which command is used to determine if an IP access list is enabled on a particular interface?

A. show access-lists
B. show interface
C. show ip interface
D. show interface access-lists
Answer: Option C

Explanation: The show ip interface command will show you if any outbound or inbound interfaces have an access list set.

13. Where is a hub specified in the OSI model?

A. Session layer
B. Physical layer
C. Data Link layer
D. Application layer
Answer: Option B

Explanation: Hubs regenerate electrical signals, which are specified at the Physical lay

14. What does the passive command provide to dynamic routing protocols?

A. Stops an interface from sending or receiving periodic dynamic updates.
B. Stops an interface from sending periodic dynamic updates but not from receiving updates.
C. Stops the router from receiving any dynamic updates.
D. Stops the router from sending any dynamic updates.
Answer: Option B

Explanation: The passive command, short for passive-interface, stops regular updates from being sent out an interface. However, the interface can still receive updates.

15. Which protocol is used to send a destination network unknown message back to originating hosts?

A. TCP
B. ARP
C. ICMP
D. BootP
Answer: Option C

Explanation: ICMP is the protocol at the Network layer that is used to send messages back to an originating router.

16. How often are BPDUs sent from a layer 2 device?

A. Never
B. Every 2 seconds
C. Every 10 minutes
D. Every 30 seconds
Answer: Option B

Explanation: Every 2 seconds, BPDUs are sent out from all active bridge ports by default.

17. How many broadcast domains are created when you segment a network with a 12-port switch?

A. 1
B. 2
C. 5
D. 12
Answer: Option A

Explanation: By default, switches break up collision domains but are one large broadcast domain.

18. What does the command routerA(config)#line cons 0 allow you to perform next?

A. Set the Telnet password.
B. Shut down the router.
C. Set your console password.
D. Disable console connections.
Answer: Option C

Explanation: The command line console 0 places you at a prompt where you can then set your console user-mode password.

19. Which router command allows you to view the entire contents of all access lists?

A. show all access-lists
B. show access-lists
C. show ip interface
D. show interface
Answer: Option B

Explanation: To see the contents of all access lists, use the show access-lists command.

20. Which class of IP address has the most host addresses available by default?

A. A
B. B
C. C
D. A and B
Answer: Option A

Explanation: Class A addressing provides 24 bits for host addressing.

21. In a network with dozens of switches, how many root bridges would you have?
A. 1
B. 2
C. 5
D. 12
Answer: Option A

Explanation: You should have only one root bridge per network

22. What PPP protocol provides dynamic addressing, authentication, and multilink?
A. NCP
B. HDLC
C. LCP
D. X.25
Answer: Option C

Explanation: Link Control Protocol in the PPP stack provides dynamic addressing, authentication, and multilink.

23. What is a stub network?
A. A network with more than one exit point.
B. A network with more than one exit and entry point.
C. A network with only one entry and no exit point.
D. A network that has only one entry and exit point.
Answer: Option D

Explanation: Stub networks have only one connection to an internetwork. Only default routes can be set on a stub network or network loops may occur.

24. If your router is facilitating a CSU/DSU, which of the following commands do you need to use to provide the router with a 64000bps serial link?
A. RouterA(config)#bandwidth 64
B. RouterA(config-if)#bandwidth 64000
C. RouterA(config-if)#clock rate 64
D. RouterA(config-if)#clock rate 64000
Answer: Option D

Explanation: The clock rate command is two words, and the speed of the line is in bps.

25. Which one of the following is true regarding VLANs?
A. Two VLANs are configured by default on all Cisco switches.
B. VLANs only work if you have a complete Cisco switched internetwork. No off-brand switches are allowed.
C. You should not have more than 10 switches in the same VTP domain.
D. VTP is used to send VLAN information to switches in a configured VTP domain.
Answer: Option D

Explanation: Switches do not propagate VLAN information by default; you must configure the VTP domain. VLAN Trunking Protocol (VTP) is used to propagate VLAN information across a trunk link.

26. What does a VLAN do?
A. Acts as the fastest port to all servers.
B. Provides multiple collision domains on one switch port.
C. Breaks up broadcast domains in a layer 2 switch internetwork.
D. Provides multiple broadcast domains within a single collision domain.
Answer: Option C

Explanation: VLANs break up broadcast domains at layer 2

27. What is the main reason the OSI model was created?
A. To create a layered model larger than the DoD model.
B. So application developers can change only one layer's protocols at a time.
C. So different networks could communicate.
D. So Cisco could use the model.
Answer: Option C

Explanation: The primary reason the OSI model was created was so that different networks could inter-operate.

28. How many collision domains are created when you segment a network with a 12-port switch?
A. 1
B. 2
C. 5
D. 12
Answer: Option D

Explanation: Layer 2 switching creates individual collision domains.

29. What command will display the line, protocol, DLCI, and LMI information of an interface?
A. sh pvc
B. show interface
C. show frame-relay pvc
D. show run
Answer: Option B

Explanation: The show interface command shows the line, protocol, DLCI, and LMI information of an interface.

30. Which protocol does Ping use?
A. TCP
B. ARP
C. ICMP
D. BootP
Answer: Option C

Explanation: ICMP is the protocol at the Network layer that is used to send echo requests and replies.

31. Which command is used to upgrade an IOS on a Cisco router?
A. copy tftp run
B. copy tftp start
C. config net
D. copy tftp flash
Answer: Option D

Explanation: The copy tftp flash command places a new file in flash memory, which is the default location for the Cisco IOS in Cisco routers.

32. If you wanted to delete the configuration stored in NVRAM, what would you type?
A. erase startup
B. erase nvram
C. delete nvram
D. erase running
Answer: Option A

Explanation: The command erase startup-config deletes the configuration stored in NVRAM.

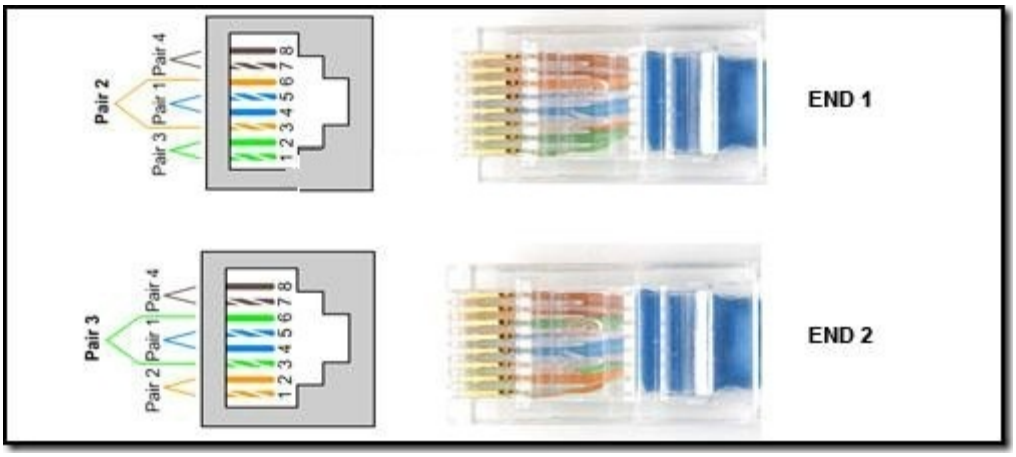
33. What protocols are used to configure trunking on a switch?

1. VLAN Trunking Protocol
2. VLAN
3. 802.1Q
4. ISL

A. 1 and 2
B. 3 and 4
C. 1 only
D. 2 only
Answer: Option B

Explanation: VTP is not right because it has nothing to do with trunking except that it sends VLAN information across a trunk link. 802.1Q and ISL are used to configure trunking on a port.

34. A student works in the lab and selects a cable as it appears. What links can successfully be done with this cable? (Choose two)



A. Connect a computer to the port console of a router

B. Connect two routers through the Ethernet ports

C. Connect two switches together with Gigabit speeds

D. Connect a computer with a switch with Gigabit speeds

E. Connect two devices with the same type of interface to Fast Ethernet speeds

Answer: Option B,E

Explanation: The cable is an Ethernet crossover type.

Subnetting

1. Your router has the following IP address on Ethernet0: 172.16.2.1/23. Which of the following can be valid host IDs on the LAN interface attached to the router?

1. 172.16.1.100
2. 172.16.1.198
3. 172.16.2.255
4. 172.16.3.0

A. 1 only
B. 2 and 3 only
C. 3 and 4 only
D. None of the above

Answer: Option C

Explanation: The router's IP address on the E0 interface is 172.16.2.1/23, which is 255.255.254.0. This makes the third octet a block size of 2. The router's interface is in the 2.0 subnet, and the broadcast address is 3.255 because the next subnet is 4.0. The valid host range is 2.1 through 3.254. The router is using the first valid host address in the range.

2. Which two statements describe the IP address 10.16.3.65/23?

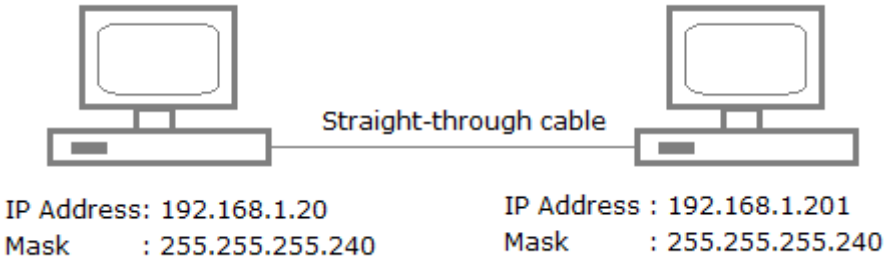
1. The subnet address is 10.16.3.0 255.255.254.0.
2. The lowest host address in the subnet is 10.16.2.1 255.255.254.0.
3. The last valid host address in the subnet is 10.16.2.254 255.255.254.0.
4. The broadcast address of the subnet is 10.16.3.255 255.255.254.0.

A. 1 and 3
B. 2 and 4
C. 1, 2 and 4
D. 2, 3 and 4

Answer: Option B

Explanation: The mask 255.255.254.0 (/23) used with a Class A address means that there are 15 subnet bits and 9 host bits. The block size in the third octet is 2 (256 - 254). So this makes the subnets in the interesting octet 0, 2, 4, 6, etc., all the way to 254. The host 10.16.3.65 is in the 2.0 subnet. The next subnet is 4.0, so the broadcast address for the 2.0 subnet is 3.255. The valid host addresses are 2.1 through 3.254.

3. A network administrator is connecting hosts A and B directly through their Ethernet interfaces, as shown in the illustration. Ping attempts between the hosts are unsuccessful. What can be done to provide connectivity between the hosts?



1. A crossover cable should be used in place of the straight-through cable.
2. A rollover cable should be used in place of the straight-through cable.
3. The subnet masks should be set to 255.255.255.192.
4. A default gateway needs to be set on each host.
5. The subnet masks should be set to 255.255.255.0.

A. 1 only
B. 2 only
C. 3 and 4 only
D. 1 and 5 only
E. 2 and 5 only

Answer: Option D

Explanation: First, if you have two hosts directly connected, as shown in the graphic, then you need a crossover cable. A straight-through cable won't work. Second, the hosts have different masks, which puts them in different subnets. The easy solution is just to set both masks to 255.255.255.0 (/24).

4. What is the maximum number of IP addresses that can be assigned to hosts on a local subnet that uses the 255.255.255.224 subnet mask?

A. 14
B. 15
C. 16
D. 30

Answer: Option D

Explanation: A /27 (255.255.255.224) is 3 bits on and 5 bits off. This provides 8 subnets, each with 30 hosts. Does it matter if this mask is used with a Class A, B, or C network address? Not at all. The number of host bits would never change.

5. You need to subnet a network that has 5 subnets, each with at least 16 hosts. Which classful subnet mask would you use?

A. 255.255.255.192
B. 255.255.255.224
C. 255.255.255.240
D. 255.255.255.248
Answer: Option B

Explanation: You need 5 subnets, each with at least 16 hosts. The mask 255.255.255.240 provides 16 subnets with 14 hosts-this will not work. The mask 255.255.255.224 provides 8 subnets, each with 30 hosts. This is the best answer.

6. You have a network that needs 29 subnets while maximizing the number of host addresses available on each subnet. How many bits must you borrow from the host field to provide the correct subnet mask?

A. 2
B. 3
C. 4
D. 5
Answer: Option D

Explanation: A 240 mask is 4 subnet bits and provides 16 subnets, each with 14 hosts. We need more subnets, so let's add subnet bits. One more subnet bit would be a 248 mask. This provides 5 subnet bits (32 subnets) with 3 host bits (6 hosts per subnet). This is the best answer.

7. If an Ethernet port on a router were assigned an IP address of 172.16.112.1/25, what would be the valid subnet address of this host?

A. 172.16.112.0
B. 172.16.0.0
C. 172.16.96.0
D. 172.16.255.0
Answer: Option A

Explanation: A /25 mask is 255.255.255.128. Used with a Class B network, the third and fourth octets are used for subnetting with a total of 9 subnet bits, 8 bits in the third octet and 1 bit in the fourth octet. Since there is only 1 bit in the fourth octet, the bit is either off or on-which is a value of 0 or 128. The host in the question is in the 0 subnet, which has a broadcast address of 127 since 128 is the next subnet.

8. You have an interface on a router with the IP address of 192.168.192.10/29. Including the router interface, how many hosts can have IP addresses on the LAN attached to the router interface?

A. 6
B. 8
C. 30
D. 32
Answer: Option A

Explanation: A /29 (255.255.255.248), regardless of the class of address, has only 3 host bits. Six hosts is the maximum number of hosts on this LAN, including the router interface.

9. What is the subnetwork number of a host with an IP address of 172.16.66.0/21?

A. 172.16.36.0
B. 172.16.48.0
C. 172.16.64.0
D. 172.16.0.0
Answer: Option C

Explanation: A /21 is 255.255.248.0, which means we have a block size of 8 in the third octet, so we just count by 8 until we reach 66. The subnet in this question is 64.0. The next subnet is 72.0, so the broadcast address of the 64 subnet is 71.255.

10. The network address of 172.16.0.0/19 provides how many subnets and hosts?

A. 7 subnets, 30 hosts each
B. 8 subnets, 8,190 hosts each
C. 8 subnets, 2,046 hosts each
D. 7 subnets, 2,046 hosts each
Answer: Option B

Explanation: A CIDR address of /19 is 255.255.224.0. This is a Class B address, so that is only 3 subnet bits, but it provides 13 host bits, or 8 subnets, each with 8,190 hosts.

11. You need to configure a server that is on the subnet 192.168.19.24/29. The router has the first available host address. Which of the following should you assign to the server?

A. 192.168.19.0 255.255.255.0
B. 192.168.19.33 255.255.255.240
C. 192.168.19.26 255.255.255.248
D. 192.168.19.31 255.255.255.248
Answer: Option C

Explanation: A /29 is 255.255.255.248, which is a block size of 8 in the fourth octet. The subnets are 0, 8, 16, 24, 32, 40, etc. 192.168.19.24 is the 24 subnet, and since 32 is the next subnet, the broadcast address for the 24 subnet is 31. 192.168.19.26 is the only correct answer.

12. You have an interface on a router with the IP address of 192.168.192.10/29. What is the broadcast address the hosts will use on this LAN?

A. 192.168.192.15
B. 192.168.192.31
C. 192.168.192.63

D. 192.168.192.127
Answer: Option A

Explanation: A /29 (255.255.255.248) has a block size of 8 in the fourth octet. This means the subnets are 0, 8, 16, 24, etc. 10 is in the 8 subnet. The next subnet is 16, so 15 is the broadcast address.

13. You have a network with a subnet of 172.16.17.0/22. Which is the valid host address?

A. 172.16.17.1 255.255.255.252
B. 172.16.0.1 255.255.240.0
C. 172.16.20.1 255.255.254.0
D. 172.16.18.255 255.255.252.0
Answer: Option D

Explanation: A Class B network ID with a /22 mask is 255.255.252.0, with a block size of 4 in the third octet. The network address in the question is in subnet 172.16.16.0 with a broadcast address of 172.16.19.255. Only option E even has the correct subnet mask listed, and 172.16.18.255 is a valid host.

14. On a VLSM network, which mask should you use on point-to-point WAN links in order to reduce the waste of IP addresses?

A. /27
B. /28
C. /29
D. /30
Answer: Option D

Explanation: A point-to-point link uses only two hosts. A /30, or 255.255.255.252, mask provides two hosts per subnet.

15. To test the IP stack on your local host, which IP address would you ping?

A. 127.0.0.0
B. 1.0.0.127
C. 127.0.0.1
D. 127.0.0.255
Answer: Option C

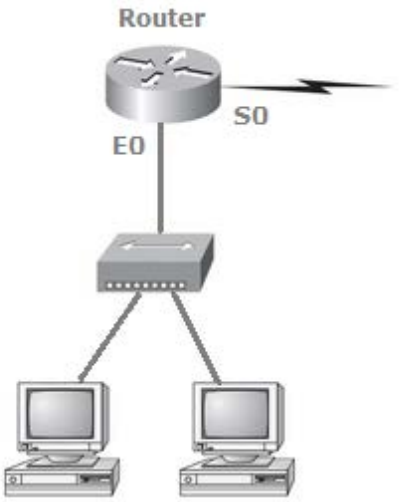
Explanation: To test the local stack on your host, ping the loopback interface of 127.0.0.1.

16. If a host on a network has the address 172.16.45.14/30, what is the subnetwork this host belongs to?

A. 172.16.45.0
B. 172.16.45.4
C. 172.16.45.8
D. 172.16.45.12
Answer: Option D

Explanation: A /30, regardless of the class of address, has a 252 in the fourth octet. This means we have a block size of 4 and our subnets are 0, 4, 8, 12, 16, etc. Address 14 is obviously in the 12 subnet.

17. Using the following illustration, what would be the IP address of E0 if you were using the eighth subnet? The network ID is 192.168.10.0/28 and you need to use the last available IP address in the range. The zero subnet should not be considered valid for this question.



A. 192.168.10.142
B. 192.168.10.66
C. 192.168.100.254
D. 192.168.10.143
E. 192.168.10.126
Answer: Option A

Explanation: A /28 is a 255.255.255.240 mask. Let's count to the ninth subnet (we need to find the broadcast address of the eighth subnet, so we need to count to the ninth subnet). Starting at 16 (remember, the question stated that we will not use subnet zero, so we start at 16, not 0), 16, 32, 48, 64, 80, 96, 112, 128, 144. The eighth subnet is 128 and the next subnet is 144, so our broadcast address of the 128 subnet is 143. This makes the host range 129-142. 142 is the last valid host.

18. Which configuration command must be in effect to allow the use of 8 subnets if the Class C subnet mask is 255.255.255.224?

A. Router(config)#ip classless
B. Router(config)#no ip classful
C. Router(config)#ip unnumbered
D. Router(config)#ip subnet-zero

Answer: Option D

Explanation: A Class C subnet mask of 255.255.255.224 is 3 bits on and 5 bits off (11100000) and provides 8 subnets, each with 30 hosts. However, if the command ip subnet-zero is not used, then only 6 subnets would be available for use.

19. Using the illustration from the previous question, what would be the IP address of S0 if you were using the first subnet? The network ID is 192.168.10.0/28 and you need to use the last available IP address in the range. Again, the zero subnet should not be considered valid for this question.

A. 192.168.10.24
B. 192.168.10.62
C. 192.168.10.30
D. 192.168.10.127

Answer: Option C

Explanation: A /28 is a 255.255.255.240 mask. The first subnet is 16 (remember that the question stated not to use subnet zero) and the next subnet is 32, so our broadcast address is 31. This makes our host range 17-30. 30 is the last valid host.

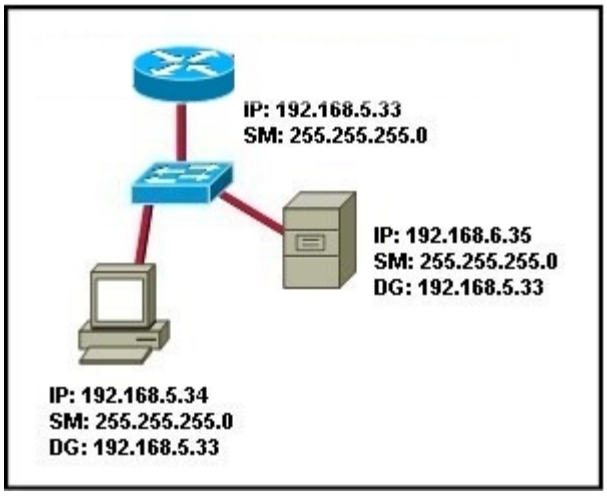
20. What is the subnetwork address for a host with the IP address 200.10.5.68/28?

A. 200.10.5.56
B. 200.10.5.32
C. 200.10.5.64
D. 200.10.5.0

Answer: Option C

Explanation: This is a pretty simple question. A /28 is 255.255.255.240, which means that our block size is 16 in the fourth octet. 0, 16, 32, 48, 64, 80, etc. The host is in the 64 subnet.

21. A computer user cannot connect to the server. All cables have been tested for proper operation as well as for connection to the devices. All devices have ip addresses. However, the user cannot connect to the server. The ping command does not respond. What can be blamed?

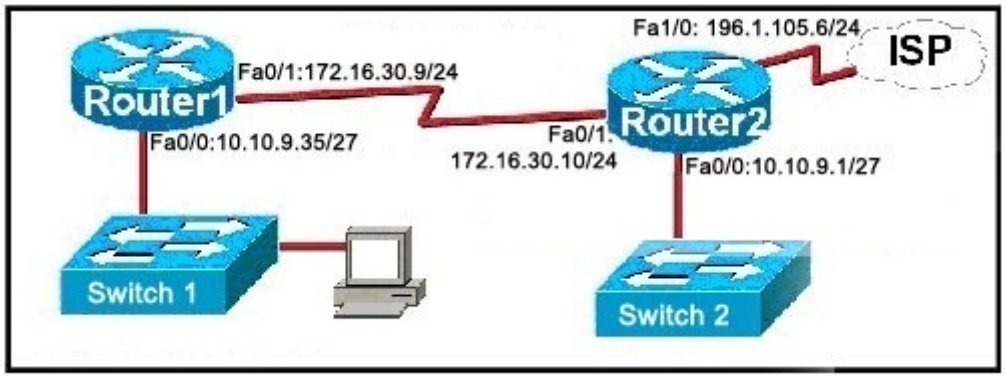


A. The router's interface is not configured with a default gateway.
B. The switch is not configured with an IP address and default gateway.
C. The pc and the server are on different logical networks.
D. The pc does not know the MAC address of the switch.

Answer: Option C

Explanation: The subnet mask /24 indicates that the user is on the 192.168.5.0 network and the server at 192.168.6.0

22. The User was disconnected from switch 2 and connected to switch 1. What combination of IP address, subnet mask, and default gateway should be declared on the user's Pc to allow it to work within the network?

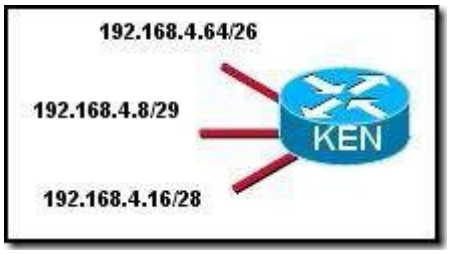


A. IP address: 10.10.9.37 Subnet mask: 255.255.255.240 Default gateway: 10.10.9.35
B. IP address: 10.10.9.37 Subnet mask: 255.255.255.224 Default gateway: 10.10.9.35
C. IP address: 10.10.9.29 Subnet mask: 255.255.255.248 Default gateway: 10.10.9.35
D. IP address: 10.10.9.32 Subnet mask: 255.255.255.224 Default gateway: 10.10.9.35
E. IP address: 10.10.9.37 Subnet mask: 255.255.255.224 Default gateway: 196.1.105.6
F. IP address: 10.10.9.63 Subnet mask: 255.255.255.224 Default gateway: 10.10.9.35

Answer: Option B

Explanation: Address 10.10.9.35 (00001010.00001010.00001001.00100011),
Netmask 255.255.255.224 = 27 (11111111.11111111.11111111.11100000),
Network 10.10.9.32/27 (**0**0001010.00001010.00001001.00100000),
Broadcast 10.10.9.63 (00001010.00001010.00001001.00111111),
First IP 10.10.9.33 (00001010.00001010.00001001.00100001),
Last IP 10.10.9.62 (00001010.00001010.00001001.00111110)

23. Which address is a broadcast address for one of the subnets shown in the image?



A. 192.168.4.3/29

B. 192.168.4.15/29

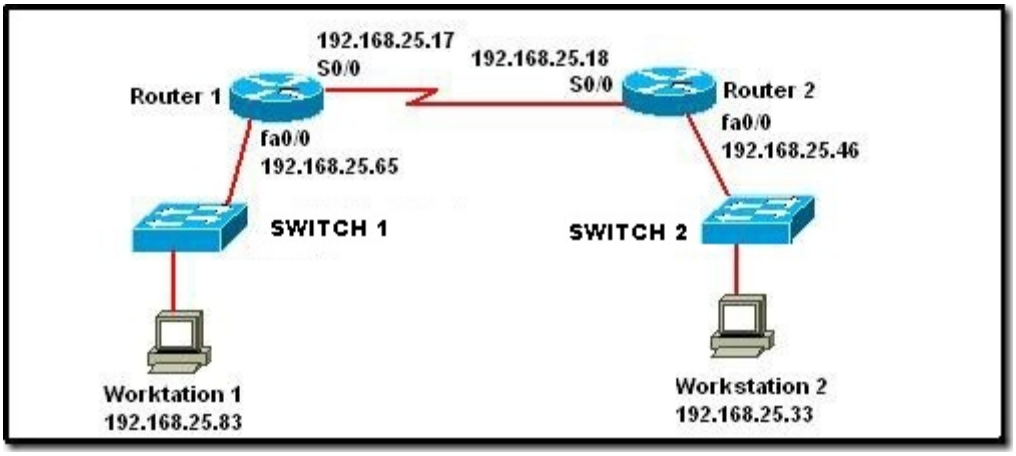
C. 192.168.4.65/26

D. 192.168.4.255/24

Answer: Option B

Explanation: Address 192.168.4.15 (11000000.10101000.00000100.00001111)
Netmask 255.255.255.248 = 29 (11111111.11111111.11111111.11111000)
The last 3 bits are all 1. So it's broadcast address after the mask is / 29.

24. A network administrator has configured a subnet network from the original 192.168.0.0/28 network. Workstation 1 is not able to communicate with Workstation 2. What is the cause of this loss of communications?



A. Workstation 1 and workstation 2 are on the same subnet

B. Serial connections use addresses from the LAN subnets.

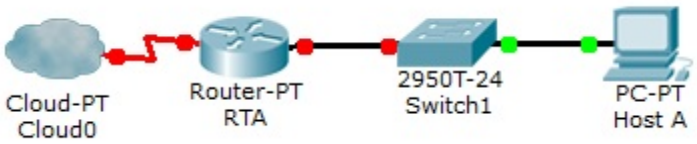
C. Workstation 1 is not on the same network with the Router 1 LAN interface

D. If routers are used on the network, there is no need for subnetworks.

Answer: Option C

Explanation: The last IP of the network is 192.168.25.78. So Workstation 1 is on another network.

25. User A in the shape has an IP address of 10.118.197.55/20. How many network devices can be added to the same subnet?



A. 253

B. 509

C. 1021

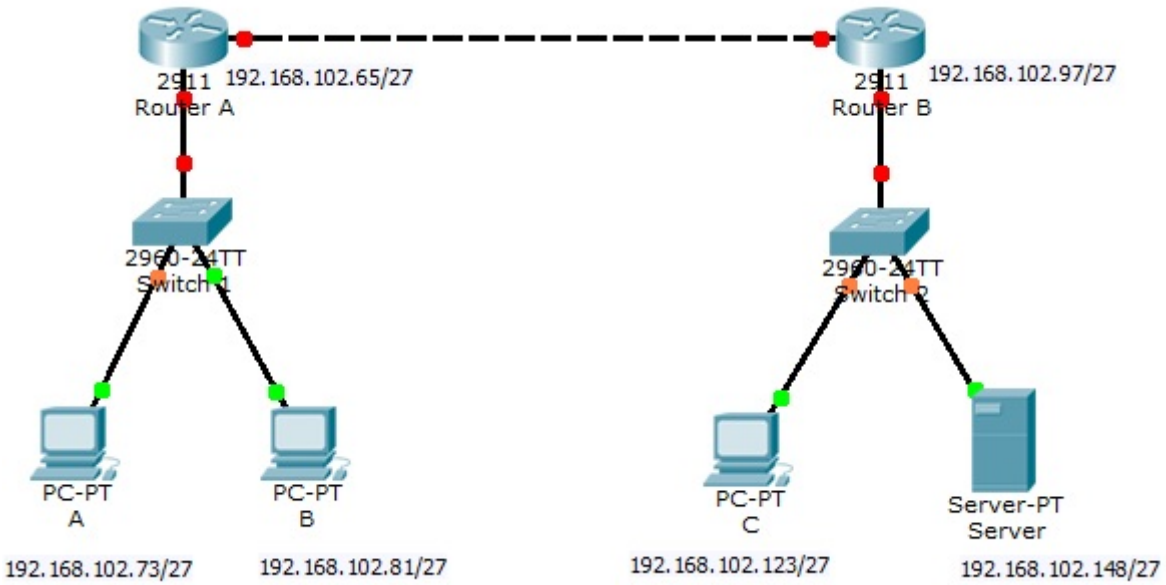
D. 2045

E. 4093

Answer: Option E

Explanation: The subnet mask / 20 can host 4096 IP addresses. Remove 1 for the network address, remove 1 for the broadcast address, and subtract one for User A already using an address. So 4093 addresses are available for use.

26. The devices are configured with a static IP address on the 192.168.102.0 network. All users can communicate with each other but can not communicate with the server. What causes the problem?



A. The IP address of the server is out of the subnet.

B. The IP address of the server is the broadcast address.

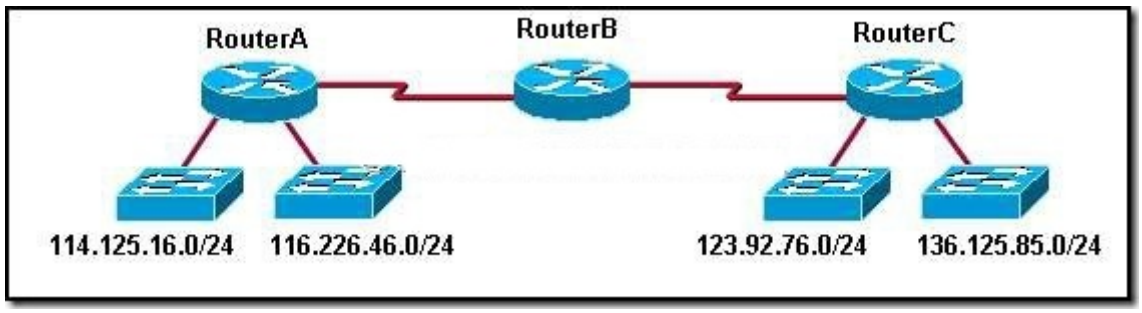
C. The IP address of the server is a network address.

D. The switch that the server connects to is not assigned an IP address.

Answer: Option A

Explanation: Using the subnet mask / 27 means that the networks will increase by 32. So the network addresses are: 192.168.102.0, 192.168.102.32, 192.168.102.64, 192.168.102.96, 192.168.102.128, 192.168.102.160, 192.168.102.192, 192.168 .102.224. Option A is correct because the IP address of the server 192.168.102.147 belongs to the 192.168.102.128 network rather than 192.168.102.96.

27. What actions will take place when RouterA loses network connection with 114.125.16.0? (Choose two)



A. RouterB will include 123.92.76.0 and 136.125.85.0 on the update to RouterA.

B. During the next update interval, RouterB will send an RIP update to both ports including the inaccessible network.

C. During the next update interval, RouterC will send an update to RouterB stating that the 114.125.16.0 network is accessible to 2 hops.

D. Router C will learn the loss of network connection 114.125.16.0 from RouterB.

E. RouterB will include the 123.92.76.0 and 136.125.85.0 network when updating of RouterC.

Answer: Option A,D

Explanation: A. The Router's A closest Router is RouterB. Therefore, in the next RIP update RouterA will learn the route from the RIP Update of RouterB.
D. In the same logic the closest to RouterC Router is RouterB.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] «Wikipedia:Δίκτυο_υπολογιστών,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/Δίκτυο_υπολογιστών. [Πρόσβαση 16 10 2016].

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

[3] «Wikipedia: Μοντέλο_αναφοράς_OSI,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/Μοντέλο_αναφοράς_OSI. [Πρόσβαση 16 10 2016].

[4] «Wikipedia: TCP/IP,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/TCP/IP. [Πρόσβαση 27 11 2017].

[5] «Wikipedia: Ethernet,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/Ethernet. [Πρόσβαση 2 1 2017].

[6] «Wikipedia: Διεύθυνση_IP,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/Διεύθυνση_IP. [Πρόσβαση 30 01 2017].

[7] «Wikipedia: ARP,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/Address_Resolution_Protocol. [Πρόσβαση 02 01 2017].

[8] «Wikipedia: Transmission_Control_Protocol,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/Transmission_Control_Protocol. [Πρόσβαση 22 01 2017].

[9] «Wikipedia: UDP,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/UDP. [Πρόσβαση 22 01 2017].

[10] «Wikipedia: Διεύθυνση_IP,» [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/Διεύθυνση_IP. [Πρόσβαση 30 01 2017].

[11] «codeingiter,» [Ηλεκτρονικό]. Available: https://codeigniter.com/.

[12] «Bootstrap,» [Ηλεκτρονικό]. Available: http://getbootstrap.com/.

[13] «TinyMCE,» [Ηλεκτρονικό]. Available: https://www.tinymce.com/.