ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Οπτικοποίηση των αιτήσεων και αποκρίσεων των πρωτοκόλλων της σουίτας TCP/IP»

Του φοιτητή
Αθανασίου Χρήστου
Αρ. Μητρώου: 144265

Επιβλέπων
Αμανατιάδης Δημήτριος

Ημερομηνία 31/05/2025

Τίτλος Δ.Ε: Οπτικοποίηση των αιτήσεων και αποκρίσεων των πρωτοκόλλων της σουίτας TCP/IP
Κωδικός Δ.Ε. 23120
Ονοματεπώνυμο φοιτητή/τών Αθανασίου Χρήστος
Ονοματεπώνυμο εισηγητή Αμανατιάδης Δημήτριος
Ημερομηνία ανάληψης Δ.Ε. 23-02-2024
Ημερομηνία περάτωσης Δ.Ε. 31-5-2024

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

«Αφιέρωνω την πτυχιακή μου εργασία στην οικογένια μου που με στήριξε και με βοήθησε όταν αύτο χρεαζόταν »

Πρόλογος

Η παρούσα πτυχιακή εργασία πραγματεύεται την οπτικοποίηση των αιτήσεων και αποκρίσεων των βασικών πρωτοκόλλων της σουίτας TCP/IP, με στόχο τη διευκόλυνση της κατανόησης των μηχανισμών επικοινωνίας στο Διαδίκτυο. Η λειτουργία των πρωτοκόλλων δικτύου, αν και θεμελιώδης για την ψηφιακή εποχή, παραμένει συχνά αφηρημένη και δυσνόητη για τους εκπαιδευόμενους. Για τον λόγο αυτό, η εργασία επικεντρώνεται στη δημιουργία εκπαιδευτικού υλικού με μορφή κινούμενων εικόνων (animations), το οποίο αποδίδει με απλό και οπτικά κατανοητό τρόπο τη ροή δεδομένων και πακέτων στο δίκτυο.

Μέσα από θεωρητική ανάλυση και πρακτική εφαρμογή, επιχειρείται η σύνδεση της τεχνικής γνώσης με την οπτική αναπαράσταση, δίνοντας έμφαση στην εκπαιδευτική αξία της απεικόνισης. Η εργασία στοχεύει να αποτελέσει ένα χρήσιμο εργαλείο τόσο για φοιτητές όσο και για εκπαιδευτικούς στον τομέα των δικτύων υπολογιστών.

Περίληψη

Στα πλαίσια της πτυχιακής εργασίας αναπτύχθηκε μια σειρά από βίντεο για εκπαιδευτικούς σκοπούς τα οποία απλοποιούν σύνθετες δικτυακές διεργασίες και διευκολύνουν την κατανόηση της λειτουργίας του διαδικτύου. Η σουίτα πρωτοκόλλων TCP/IP επιτρέπει την επικοινωνία τύπου client-server με τρόπο αξιόπιστο, δομημένο και αποτελεσματικό, μέσα από πρωτόκολλα όπως TCP (για σύνδεση) και HTTP (για δεδομένα εφαρμογής). Στο θεωρητικό κομμάτι περιγράφεται το πώς λειτουργεί η επικοινωνία μεταξύ **πελάτη (client)** και **εξυπηρετητή (server)**, μέσω των πρωτοκόλλων **TCP, HTTP (Hypertext Transfer Protocol), ARP , DNS** και **DHCP**, χρησιμοποιώντας το μοντέλο **αίτησης-απόκρισης** (*request-response*).

Το σενάριο με το οποίο ασχολείται η πτυχιακή εργασία είναι ότι ο χρήστης πληκτρολογεί τη διεύθυνση μιας ιστοσελίδας, π.χ. https://www.example.com, στον browser του. Ο υπολογιστής του (client) πρέπει να βρει την IP διεύθυνση που αντιστοιχεί στο όνομα www.example.com, οπότε κάνει ένα DNS query στον τοπικό DNS server για να μετατρέψει το όνομα σε IP. Ο DNS server απαντά ότι η διεύθυνση IP για www.example.com είναι 93.184.216.34. Αφού ο client αποκτήσει την IP, ξεκινά τη διαδικασία σύνδεσης με τον server μέσω του TCP three-way handshake. Ο client στέλνει ένα πακέτο SYN στον server για να ξεκινήσει τη σύνδεση. Ο server απαντά με ένα SYN-ACK, επιβεβαιώνοντας την αποδοχή της σύνδεσης και ο client στέλνει ένα ACK, ολοκληρώνοντας τη σύνδεση. Ακολούθως, εάν η σύνδεση είναι ασφαλής (HTTPS), ακολουθεί ένα TLS handshak**e** για να καθιερωθεί μια κρυπτογραφημένη σύνδεση μεταξύ του client και του server. Μόλις η σύνδεση είναι έτοιμη, ο client στέλνει το HTTP request για τη συγκεκριμένη ιστοσελίδα και ο server απαντά με τα απαιτούμενα δεδομένα (HTML, εικόνες, κ.λπ.). Όλη αυτή η διαδικασία που διαρκεί συνήθως λιγότερο από ένα δευτερόλεπτο, διασφαλίζει την αξιόπιστη και ασφαλή μεταφορά δεδομένων, επιτρέποντας στον χρήστη να δει την ιστοσελίδα στον browser του.

« Visualization of Requests and Responses in the TCP/IP Protocol Suite »

«Athanasiou Christos»

Abstract

This thesis focuses on the visualization of request and response processes of core protocols in the TCP/IP suite, aiming to enhance the comprehension of network communication mechanisms. Although protocols such as DHCP, DNS, ARP, TCP, HTTP, and ICMP are fundamental to modern network infrastructures, their internal operation is often challenging to grasp through theory alone. To address this issue, the present work combines theoretical analysis with visual representations in the form of animated videos.

Each protocol is presented through a structured animation that illustrates the exchange of messages, including packet direction, header information, timing, and address resolution. For instance, the DHCP process is visualized step-by-step (Discover, Offer, Request, Acknowledgment), while the TCP handshake shows the full sequence of SYN, SYN-ACK, and ACK messages. The animations were developed using Microsoft PowerPoint and exported as video, enabling intuitive and accessible understanding for learners.

The final result is an educational tool that supports students and instructors in computer networking courses. By translating abstract packet flows into visually structured sequences, the material helps bridge the gap between theory and practice. The animations can be used both independently and as supplementary teaching material in academic or training environments.

The outcome of this work demonstrates that visualization significantly contributes to the clarity and retention of complex technical concepts. Future improvements could include expanding the material to additional application-layer protocols or integrating interactivity into the video content.

Περιεχόμενα

Συντομογραφίες

ARP – Address Resolution Protocol

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

FTP – File Transfer Protocol

ICMP – Internet Control Message Protocol

IP – Internet Protocol

LAN – Local Area network

MAC – Medium Access Control

POP – Post Office Protocol

RARP – Reverse Address Resolution Protocol

SMTP – Simple Mail Transfer Protocol

TCP – Transmission Control Protocol

TLS – Transfer Layer Security

UDP - User Datagram Protocol

PPP – Point to Point

HTTP – HyperText Transfer Protocol

HTTPS – HyperText Transfer Protocol Secure

DORA – Discover Offer Request Acknowledge

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1ο: Εισαγώγη

1.1. Εισαγωγή κεφαλαίου

Η τεχνολογία των δικτύων υπολογιστών αποτελεί σήμερα βασικό θεμέλιο της σύγχρονης ψηφιακής κοινωνίας. Από την αποστολή ενός απλού μηνύματος ηλεκτρονικού ταχυδρομείου, έως την παρακολούθηση πολυμέσων και την απομακρυσμένη εργασία μέσω cloud υπηρεσιών, οι περισσότερες δραστηριότητες βασίζονται σε κάποιο είδος δικτυακής επικοινωνίας. Πίσω από κάθε διαδικτυακή ενέργεια — όσο απλή κι αν φαίνεται στον τελικό χρήστη — ενεργοποιείται ένα πολύπλοκο σύνολο πρωτοκόλλων και τεχνολογιών που εξασφαλίζουν την αξιόπιστη, ασφαλή και αποδοτική μεταφορά δεδομένων.

Το παρόν κεφάλαιο εισάγει το γενικό πλαίσιο της πτυχιακής εργασίας, η οποία επικεντρώνεται στην ανάλυση της διαδικασίας επικοινωνίας μεταξύ ενός client και ενός server κατά την πρόσβαση σε μια ιστοσελίδα. Αρχικά, γίνεται μια ιστορική αναδρομή της εξέλιξης του Διαδικτύου και των βασικών τεχνολογιών που το διαμόρφωσαν. Στη συνέχεια, τονίζεται η σημασία της κατανόησης των βασικών διαδικτυακών πρωτοκόλλων και των επιπέδων ενθυλάκωσης, τα οποία, αν και λειτουργούν στο παρασκήνιο, παίζουν κρίσιμο ρόλο σε κάθε δικτυακή συναλλαγή.

1.2. Ιστορική αναδρομή του Διαδικτύου

Η δημιουργία του Διαδικτύου [1] βασίζεται σε μια σειρά τεχνολογικών εξελίξεων που ξεκίνησαν τη δεκαετία του 1960, σε ένα πλαίσιο στρατηγικής και επιστημονικής καινοτομίας. Η πρώτη κρίσιμη πρόοδος ήρθε με την έννοια της μεταγωγής πακέτου (packet switching), η οποία αντικατέστησε την παραδοσιακή μεταγωγή κυκλώματος, προσφέροντας μεγαλύτερη ευελιξία και αποδοτικότητα στη μετάδοση δεδομένων.

Το ARPANET, που δημιουργήθηκε στα τέλη της δεκαετίας του 1960 από την αμερικανική DARPA, αποτέλεσε τον πρώτο λειτουργικό πρόγονο του σημερινού Διαδικτύου. Μέσα σε λίγα χρόνια, το ARPANET συνδέθηκε με πανεπιστήμια και ερευνητικά κέντρα, αποτελώντας το πρώτο δίκτυο που χρησιμοποίησε την αρχή της αποκέντρωσης και της δικτύωσης χωρίς κεντρικό έλεγχο.

Κατά τη δεκαετία του 1980, θεμελιώθηκε η χρήση του πρωτοκόλλου TCP/IP (Transfer Control Protocol / Internet Protocol), το οποίο έγινε το πρότυπο επικοινωνίας στο Διαδίκτυο. Παράλληλα, αναπτύχθηκε το DNS (Domain Name System), που επέτρεψε την εύκολη αντιστοίχιση ονομάτων σε IP διευθύνσεις, καθιστώντας πιο φιλική τη χρήση του δικτύου.

Η δεκαετία του 1990 σηματοδότησε την εκρηκτική ανάπτυξη του Web. Με την κυκλοφορία των πρώτων γραφικών προγραμμάτων πλοήγησης (browsers), το Διαδίκτυο έγινε προσβάσιμο στο ευρύ κοινό και άρχισε να αποκτά εμπορικό χαρακτήρα. Οι εφαρμογές επεκτάθηκαν από την απλή ανταλλαγή πληροφοριών σε ηλεκτρονικό εμπόριο, ειδήσεις, ψυχαγωγία και εκπαίδευση. Η χρήση πρωτοκόλλων όπως HTTP (Hypertext Transfer Protocol), TCP, UDP (User Datagram Protocol) και DHCP (Dynamic Host Configuration Protocol) αποτέλεσαν ορόσημα στην αποτελεσματική λειτουργία του παγκόσμιου ιστού.

Από το 2000 και μετά, το Διαδίκτυο ενσωματώθηκε σε κάθε πτυχή της καθημερινότητας. Η ασύρματη πρόσβαση (Wi-Fi), τα κινητά δίκτυα (4G, 5G) και η ανάδυση των κοινωνικών δικτύων μετέτρεψαν το Διαδίκτυο σε ένα παγκόσμιο εργαλείο επικοινωνίας, έκφρασης και πληροφόρησης.

1.3. Η Σημασία κατανόησης των Βασικών Διαδικτυακών Πρωτοκόλλων

Η γνώση της εσωτερικής λειτουργίας των βασικών πρωτοκόλλων δικτύου είναι ιδιαίτερα σημαντική για τους φοιτητές και τους επαγγελματίες του τομέα της πληροφορικής. Πίσω από την απλή ενέργεια πληκτρολόγησης μιας διεύθυνσης ιστοσελίδας στον browser, ενεργοποιείται μια σειρά από τεχνολογίες και μηχανισμούς που συνεργάζονται αρμονικά: η απόκτηση IP μέσω του DHCP, η αντιστοίχιση του domain name σε IP μέσω DNS, η εγκαθίδρυση σύνδεσης TCP μέσω του three-way handshake και, σε περιβάλλοντα ασφαλούς περιήγησης, η δημιουργία κρυπτογραφημένης συνεδρίας μέσω του TLS (Transport Layer Security). Όλα αυτά εκτελούνται αυτόματα και χωρίς ορατή παρέμβαση από τον χρήστη, ωστόσο αποτελούν κρίσιμους πυλώνες πάνω στους οποίους στηρίζεται η λειτουργία του Διαδικτύου.

Στο πλαίσιο αυτό, η παρούσα πτυχιακή εργασία εστιάζει στην αναλυτική παρουσίαση της διαδικασίας που λαμβάνει χώρα από τη στιγμή που ένας χρήστης πληκτρολογεί τη διεύθυνση μιας ιστοσελίδας έως την τελική απόκριση του server και την εμφάνιση της ιστοσελίδας στην οθόνη του. Μέσα από ένα ενιαίο και ρεαλιστικό σενάριο, εξετάζονται τα πρωτόκολλα DHCP, DNS, IP, TCP, TLS και HTTP, περιγράφεται η διαδοχική ροή των πακέτων δεδομένων εντός του δικτύου και εξηγείται η ενθυλάκωση και αποενθυλάκωση της πληροφορίας μεταξύ των διαφορετικών επιπέδων του δικτυακού μοντέλου.

Προκειμένου να γίνει πιο κατανοητή αυτή η πολύπλοκη αλληλουχία διαδικασιών, η εργασία αξιοποιεί την οπτικοποίηση ως βασική εκπαιδευτική μέθοδο. Μέσα από τη χρήση διαγραμμάτων, κινούμενων απεικονίσεων (animations) και εποπτικών παραδειγμάτων, επιδιώκεται να αναδειχθεί η εσωτερική λειτουργία του Διαδικτύου με τρόπο προσιτό και ελκυστικό. Η οπτικοποίηση των πρωτοκόλλων και της ροής των δεδομένων επιτρέπει στον φοιτητή ή τον αναγνώστη να «δει» την αλληλουχία των ενεργειών, να αντιληφθεί τις σχέσεις ανάμεσα στα επίπεδα πρωτοκόλλων και να εμβαθύνει στη δομή των δικτυακών πακέτων. Έτσι, η μελέτη δεν περιορίζεται στη θεωρητική κατανόηση, αλλά επεκτείνεται και στην πρακτική, λειτουργική και διδακτική προσέγγιση.

Η εργασία αυτή φιλοδοξεί να αποτελέσει όχι μόνο μια τεχνική καταγραφή, αλλά και ένα διδακτικό εργαλείο με στόχο την κατανόηση του τι πραγματικά συμβαίνει πίσω από μια καθημερινή και φαινομενικά απλή πράξη, όπως η επίσκεψη σε μια ιστοσελίδα.

1.4. Επίλογος Κεφαλαίου

Το παρόν κεφάλαιο εισήγαγε το πλαίσιο της πτυχιακής εργασίας, αναδεικνύοντας τη σημασία της μελέτης των διαδικτυακών πρωτοκόλλων και των τεχνολογιών που υποστηρίζουν τη σύγχρονη δικτυακή επικοινωνία. Μέσα από μια ιστορική αναδρομή, παρουσιάστηκε η πορεία εξέλιξης του Διαδικτύου από την εποχή του ARPANET έως τη σημερινή εποχή της παγκόσμιας διασύνδεσης και της κινητής πρόσβασης. Παράλληλα, επισημάνθηκε η αναγκαιότητα κατανόησης της λειτουργίας των βασικών πρωτοκόλλων, όπως DHCP, DNS, TCP, IP και TLS, ιδιαίτερα για φοιτητές και επαγγελματίες του χώρου της Πληροφορικής.

Τονίστηκε επίσης ο ρόλος της οπτικοποίησης ως διδακτικό εργαλείο για την κατανόηση σύνθετων εννοιών και διαδικασιών, που εκτελούνται μεν στο παρασκήνιο, αλλά αποτελούν

θεμέλιο της καθημερινής εμπειρίας χρήσης του Διαδικτύου. Η εργασία επιδιώκει να προσφέρει μια αναλυτική και εκπαιδευτική προσέγγιση, αξιοποιώντας διαγράμματα, σενάρια και κινούμενη απεικόνιση της επικοινωνίας client–server, ώστε να ενισχύσει τη βαθύτερη κατανόηση των εννοιών.

Στα επόμενα κεφάλαια, θα παρουσιαστούν με λεπτομέρεια τα επιμέρους πρωτόκολλα και η αλληλουχία τους μέσα από το σενάριο επίσκεψης σε μια ιστοσελίδα, με στόχο την πλήρη χαρτογράφηση της διαδρομής ενός αιτήματος στο δίκτυο.

Κεφάλαιο 2ο: Αρχιτεκτονική Επιπέδων

2.1 Εισαγωγή

Η κατανόηση της αρχιτεκτονικής των δικτύων βασίζεται στην έννοια της πολυεπίπεδης σχεδίασης, σύμφωνα με την οποία η συνολική λειτουργικότητα του συστήματος επικοινωνίας χωρίζεται σε διακριτά επίπεδα. Κάθε επίπεδο έχει συγκεκριμένες αρμοδιότητες και αλληλεπιδρά μόνο με το αμέσως πάνω και κάτω από αυτό επίπεδο, διευκολύνοντας τον σχεδιασμό, την ανάπτυξη και την αντιμετώπιση προβλημάτων.

Στον χώρο των δικτύων, το πιο γνωστό και διαδεδομένο μοντέλο αναφοράς είναι το [4],[5] **μοντέλο OSI (Open Systems Interconnection)**, το οποίο αναπτύχθηκε από τον Διεθνή Οργανισμό Τυποποίησης (ISO) και οργανώνει τη λειτουργία της επικοινωνίας σε **επτά διακριτά επίπεδα**. Το μοντέλο OSI, έχει σημαντική παιδαγωγική και διδακτική αξία και εξακολουθεί να χρησιμοποιείται ευρέως για την κατανόηση της λειτουργίας των δικτύων υπολογιστών.

Παράλληλα, η στοίβα πρωτοκόλλων του Διαδικτύου, γνωστή και ως **TCP/IP stack**, βασίζεται σε παρόμοιες αρχές, αλλά με λιγότερα επίπεδα. Τα δύο αυτά μοντέλα παρουσιάζουν αντιστοιχίες και διαφορές, που είναι χρήσιμες για τη σύγκριση και την κατανόηση του τρόπου λειτουργίας των δικτυακών συστημάτων. Στο παρόν κεφάλαιο θα αναλυθούν τα επιμέρους επίπεδα του μοντέλου OSI, η δομή της στοίβας TCP/IP και η εννοιολογική σχέση μεταξύ τους.

2.2 Το μοντέλο OSI

Το μοντέλο OSI (Open Systems Interconnection) αποτελεί μια αφηρημένη θεώρηση της λειτουργίας των δικτύων υπολογιστών, οργανωμένη σε επτά ιεραρχικά επίπεδα. Κάθε επίπεδο παρέχει συγκεκριμένες υπηρεσίες στο αμέσως ανώτερο και βασίζεται στις υπηρεσίες του αμέσως κατώτερου. Η ανάλυση αυτή βοηθά στη διάκριση ρόλων, πρωτοκόλλων και τεχνολογιών κατά τη μεταφορά πληροφορίας από άκρο σε άκρο.

Εκτός από την κατανόηση του μοντέλου OSI, τα επίπεδα μοντέλου OSI είναι ιδιαίτερα χρήσιμα κατά την οπτικοποίηση της ροής δεδομένων από τον αποστολέα στον δέκτη. Οι περιγραφές των διαφόρων επιπέδων, καθώς και η αλληλεξάρτησή τους, διευκολύνουν τον εντοπισμό ζητημάτων δικτύωσης. Επίσης, οι προγραμματιστές μπορούν να χρησιμοποιήσουν το μοντέλο OSI για να κατανοήσουν καλύτερα πώς έρχονται τα δεδομένα από και προς τις εφαρμογές τους ή για να γράψουν συγκεκριμένο κώδικα για χρήση σε ορισμένα επίπεδα. Παρακάτω θα περιγραφούν τα 7 επίπεδα OSI [5], [6] «από πάνω προς τα κάτω» από το επίπεδο εφαρμογής, μέχρι το φυσικό επίπεδο.

2.2.1 Επίπεδο Εφαρμογής (Application Layer)

Το επίπεδο εφαρμογής χρησιμοποιείται από λογισμικό τελικού χρήστη, όπως προγράμματα περιήγησης ιστού και προγράμματα-πελάτες ηλεκτρονικού ταχυδρομείου. Παρέχει πρωτόκολλα που επιτρέπουν στο λογισμικό να στέλνει - λαμβάνει πληροφορίες και να παρουσιάζει δεδομένα στους χρήστες. Μερικά παραδείγματα πρωτοκόλλων επιπέδου εφαρμογής είναι το πρωτόκολλο μεταφοράς υπερκειμένου – HTTP, το πρωτόκολλο μεταφοράς αρχείων – FTP (File Transfer Protocol), το πρωτόκολλο ταχυδρομικού γραφείου – POP (Post Office Protocol), το πρωτόκολλο απλής μεταφοράς αλληλογραφίας – SMTP (Simple Mail Transfer Protocol) και το σύστημα ονομάτων τομέα DNS (Domain Name System).

2.2.2 Επίπεδο Παρουσίασης (Presentation Layer)

Το επίπεδο παρουσίασης προετοιμάζει δεδομένα για το **επίπεδο εφαρμογής**. Καθορίζει τον τρόπο με τον οποίο δύο συσκευές θα πρέπει να κωδικοποιούν, να κρυπτογραφούν και να συμπιέζουν δεδομένα ώστε να λαμβάνονται σωστά από την άλλη άκρη. Το επίπεδο παρουσίασης λαμβάνει όλα τα δεδομένα που μεταδίδονται από το επίπεδο εφαρμογής και τα προετοιμάζει για μετάδοση μέσω του επιπέδου περιόδου λειτουργίας.

2.2.3 Επίπεδο Συνεδρίας (Session Layer)

Το επίπεδο συνεδρίας δημιουργεί κανάλια επικοινωνίας, που ονομάζονται συνεδρίες, μεταξύ συσκευών. Είναι υπεύθυνο για το άνοιγμα των συνεδριών, τη διασφάλιση ότι παραμένουν ανοιχτές και λειτουργικές κατά τη μεταφορά των δεδομένων και το κλείσιμό τους όταν τελειώνει η επικοινωνία. Το επίπεδο συνεδρίας μπορεί επίσης να ορίσει σημεία ελέγχου κατά τη διάρκεια μιας μεταφοράς δεδομένων, όπου σε περίπτωση που διακοπεί η συνεδρία, οι συσκευές μπορούν να συνεχίσουν τη μεταφορά δεδομένων από το τελευταίο σημείο ελέγχου.

2.2.4 Επίπεδο Μεταφοράς (Transport Layer)

Το επίπεδο μεταφοράς λαμβάνει μηνύματα επιπέδου εφαρμογής, τα διασπά σε μικρότερα τμήματα (segments) και τα μεταφέρει από άκρο σε άκρο (end – to – end), δηλαδή μεταφορά μυνημάτων ανάμεσα σε δύο εφαρμογές που εκτελούνται σε διαφορετικούς υπολογιστές. Είναι υπεύθυνο για τη συναρμολόγηση των τμημάτων στο άκρο λήψης, μετατρέποντάς τα ξανά σε δεδομένα που μπορούν να χρησιμοποιηθούν από το ανώτερο επίπεδο. Το επίπεδο μεταφοράς μπορεί να προσφέρει αξιόπιστη μεταφορά δεδομένων, όπου γίνονται οι κατάλληλοι έλεγχοι για την αποστολή των τμημάτων με τη σωστή σειρά και την αντιμετώπιση σφαλμάτων σε περίπτωση που προκύψουν, αλλά προσφέρει επίσης, μεταφορά χωρίς ελέγχους που δεν εγγυάται την αξιόπιστη μεταφορά των τμημάτων και μπορεί να υπάρξουν απώλειες.

2.2.5 Επίπεδο Δικτύου (Network Layer)

Το επίπεδο δικτύου είναι υπεύθυνω για τη μεταφορά πακέτων επιπέδου δικτύου, τα οποία ονομάζονται δεδομενογράμματα (datagrams) από έναν υπολογιστή σε έναν άλλον. Η κύρια αποστολή του είναι η **δρομολόγηση (routing)** των datagrams από τον αποστολέα προς τον παραλήπτη, ακόμη και αν αυτοί βρίσκονται σε απομακρυσμένες τοπολογίες. Το επίπεδο δικτύου περιλαμβάνει το πρωτόκολλο **IP** το οποίο ορίζει τα πεδία των datagrams και το πως αυτά επεξεργάζονται από τους υπολογιστές και τους δρομολογητές. Επίσεις περιλαμβάνει τα πρωτόκολλα δρομολόγησης RIP (Routing Information Protocol), OSPF (Open Shortest Path First) κ.α., τα οποία καθορίζουν τις διαδρομές που ακολουθούν τα datagrams από την προέλευση έως τον προορισμό.

2.2.6 Επίπεδο Ζεύξης (Link Layer)

Το επίπεδο ζεύξης αποτελεί το ενδιάμεσο στάδιο μεταξύ του φυσικού επιπέδου και των ανωτέρων λογικών επιπέδων. Εξασφαλίζει την αξιόπιστη και σωστή μεταφορά των δεδομένων από μια συσκευή σε μία άλλη. Τα πακέτα σε αυτό το επίπεδο ονομάζονται «πλαίσια» και κάποια από τα πρωτόκολλα είναι το Ethernet, WiFi, PPP (Point-to-Point), κ.α..

2.2.7 Φυσικό Επίπεδο (Physical Layer)

Το φυσικό επίπεδο μεταφέρει την πληροφορία σε μορφή bit (0-1). Τα πρωτόκολλα σε αυτό το επίπεδο εξαρτώνται από τη ζεύξη και από το μέσο μετάδωσεις, όπως είναι το χάλκινο καλώδιο crossover, ομοαξονικό καλώδιο, οπτική ίνα ή ασύρματη σύνδεση.

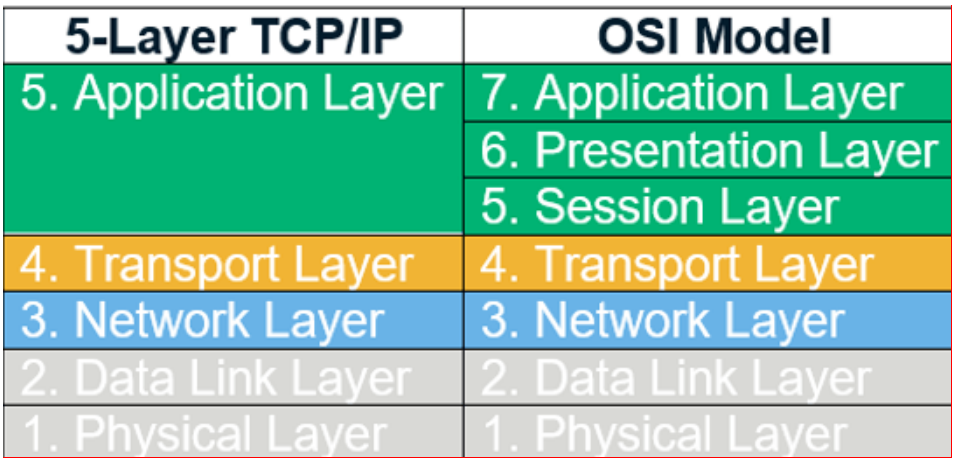
2.3 Σύγκριση Μοντέλου OSI με το TCP/IP

Το μοντέλο TCP/IP είναι το πρότυπο που χρησιμοποιείται ευρέως και εφαρμόζεται στην καθημερινή λειτουργία των δικτύων, σε αντίθεση με το OSI το οποίο προσφέρει μια καθαρή διαίρεση της επικοινωνίας σε επτά διακριτά επίπεδα, αλλά στη πράξη δεν εφαρμόζεται σχεδόν ποτέ αυτούσιο στο διαδίκτυο. Το TCP/IP αναπτύχθηκε στα τέλη της δεκαετίας του 1970 και αρχές του 1980 από τους Vint Cerf και Robert Kahn, [5], [6] είναι ένα πρακτικό μοντέλο που αντιμετωπίζει συγκεκριμένες προκλήσεις επικοινωνίας και βασίζεται σε τυποποιημένα πρωτόκολλα.

Η διαφορά των δύο μοντέλων είναι ότι το TCP/IP μοντέλο συγχωνεύει το επίπεδο Παρουσίασης και το επίπεδο Συνόδου στο επίπεδο Εφαρμογής.

2.3.1 Δομή TCP/IP

- **Επίπεδο Εφαρμογής (Application Layer):** Περιλαμβάνει όλα τα πρωτόκολλα εφαρμογών όπως HTTP, FTP, SMTP, DNS, κ.α.. Αντιστοιχεί στα επίπεδα Εφαρμογής-Παρουσίασης-Συνόδου του OSI.
- **Επίπεδο Μεταφοράς (Transport Layer):** Χρησιμοποιεί πρωτόκολλα όπως TCP (Transmission Control Protocol) και UDP (User Datagram Protocol), προσφέροντας μεταφορά δεδομένων μεταξύ εφαρμογών.
- **Επίπεδο Δικτύου (Network Layer):** Υπεύθυνο για τη δρομολόγηση και τη διευθυνσιοδότηση με το πρωτόκολλο IP.
- **Επίπεδο Ζεύξης (Link Layer):** Αυτό το επίπεδο εξασφαλίζει την τοπική μετάδοση δεδομένων μεταξύ δύο συσκευών συνδεδεμένων στο ίδιο φυσικό μέσο.
- **Φυσικό Επίπεδο (Physical Layer):** Το Φυσικό επίπεδο είναι υπεύθυνο για τη φυσική μετάδοση των bits μέσω των φυσικών μέσων επικοινωνίας.



Σχήμα 1.1: TCP/IP vs OSI

2.4 **Επίλογος Κεφαλαίου**

Στο παρόν κεφάλαιο παρουσιάστηκε αναλυτικά η αρχιτεκτονική του μοντέλου OSI καθώς και η πρακτική του αντιστοιχία με το μοντέλο TCP/IP, το οποίο εφαρμόζεται στην πραγματική λειτουργία του Διαδικτύου. Μέσα από τη μελέτη των επιμέρους επιπέδων, έγινε κατανοητή η πολυεπίπεδη προσέγγιση που χρησιμοποιείται για την επικοινωνία μεταξύ υπολογιστικών συστημάτων, όπου κάθε επίπεδο έχει διακριτό ρόλο. Η κατανόηση των επιπέδων αυτών είναι απαραίτητη για την πλήρη αντίληψη της ροής των δεδομένων στο δίκτυο και για την ανάλυση των λειτουργιών που πραγματοποιούνται κατά τη μετάδοση μιας πληροφορίας από έναν υπολογιστή σε έναν άλλο.

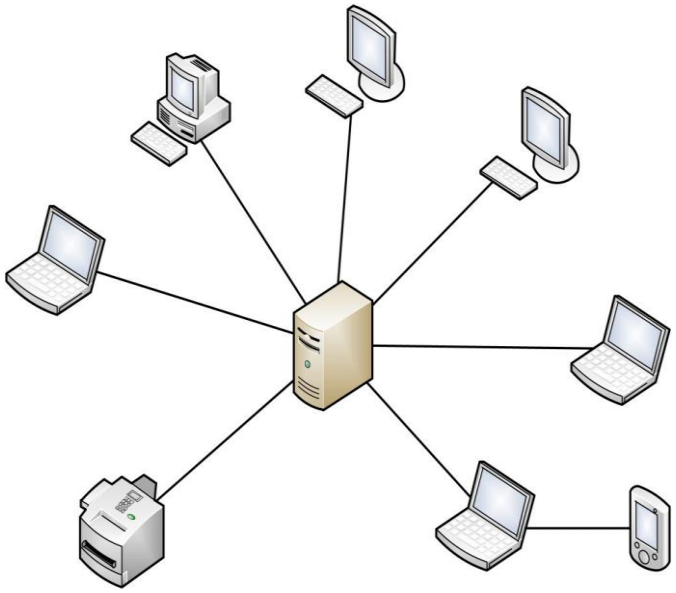
Κεφάλαιο 3ο: Client Server

3.1 Εισαγωγή

Το μοντέλο πελάτη-διακομιστή (Client-Server Model) είναι μια θεμελιώδης αρχιτεκτονική στην πληροφορική και τις τηλεπικοινωνίες, που χρησιμοποιείται ευρέως για τη διαχείριση και την ανταλλαγή δεδομένων μεταξύ συστημάτων. Η αρχιτεκτονική αυτή βασίζεται στη διακριτή σχέση μεταξύ του πελάτη (client), ο οποίος αιτείται δεδομένα ή υπηρεσίες και του διακομιστή (server), που επεξεργάζεται τα αιτήματα και παρέχει τις ζητούμενες υπηρεσίες. Το μοντέλο αυτό έχει συμβάλει σημαντικά στην ανάπτυξη του διαδικτύου, των βάσεων δεδομένων, των επιχειρηματικών εφαρμογών και πολλών άλλων τεχνολογικών συστημάτων. Θα αναλυθούν οι βασικές αρχές του μοντέλου πελάτη-διακομιστή, η λειτουργία του, τα χαρακτηριστικά, τα πλεονεκτήματα και τα μειονεκτήματά του, καθώς και η εφαρμογή του σε διάφορους τομείς των Δικτύων.

3.2 Client-Server

Το μοντέλο client-server (πελάτη-διακομιστή) [2] υποδηλώνει μια σχέση μεταξύ συνεργαζόμενων προγραμμάτων σε μια εφαρμογή, που αποτελείται από πελάτες που ξεκινούν αιτήματα για υπηρεσίες και διακομιστές που παρέχουν αυτήν τη λειτουργία ή την υπηρεσία.



Σχήμα 2.1: Μοντέλο Client-Server

Το μοντέλο client-server είναι μια έννοια στα δίκτυα που ρυθμίζει την αλληλεπίδραση μεταξύ πελάτη και διακομιστή μέσω της σαφής κατανομής των εργασιών σε ένα δίκτυο.

Ο **διακομιστής** παρέχει τους απαραίτητους πόρους και υπηρεσίες για άλλους υπολογιστές ή προγράμματα για τον πελάτη. Αυτό περιλαμβάνει την εκτέλεση των υπηρεσιών και την παροχή της αναμενόμενης απάντησης.

Ο **πελάτης** είναι υπεύθυνος για την επικοινωνία, χρησιμοποιεί τις παρεχόμενες υπηρεσίες και τις ζητά. Είναι επομένως ο παραλήπτης των απαντήσεων από τον διακομιστή. Ο διακομιστής εξυπηρετεί πολλούς πελάτες και επομένως επεξεργάζεται πολλά αιτήματα.

Το μοντέλο client-server επιτρέπει την αποτελεσματική διανομή υπηρεσιών και πόρων σε ένα δίκτυο. Προωθεί την επεκτασιμότητα, καθώς οι διακομιστές μπορούν να προστεθούν ή να ενημερωθούν όπως απαιτείται. Αποτελεί λοιπόν τη βάση για πολλές εφαρμογές πληροφορικής, π.χ. πρόσβαση σε ιστοσελίδες σε διακομιστή ιστού, διαχείριση επισκεψιμότητας email ή μεταφορά αρχείων. Το μοντέλο διευκολύνει έτσι την κεντρική διαχείριση των πόρων.

Οι βασικές αρχές που διέπουν το μοντέλο πελάτη-διακομιστή περιλαμβάνουν:

- **Κατανομή εργασιών**: Οι πελάτες εκτελούν τοπικά τις διεπαφές χρήστη και διαχειρίζονται τη διαμόρφωση των αιτημάτων, ενώ οι διακομιστές αναλαμβάνουν την αποθήκευση και επεξεργασία δεδομένων.
- **Ανεξαρτησία κόμβων**: Ο πελάτης και ο διακομιστής μπορούν να λειτουργούν ανεξάρτητα, εφόσον υπάρχει δικτυακή σύνδεση μεταξύ τους.
- **Κλιμάκωση (Scalability)**: Το σύστημα μπορεί να επεκταθεί είτε με την προσθήκη περισσότερων διακομιστών (horizontal scaling) είτε με την αναβάθμιση του υπάρχοντος διακομιστή (vertical scaling).

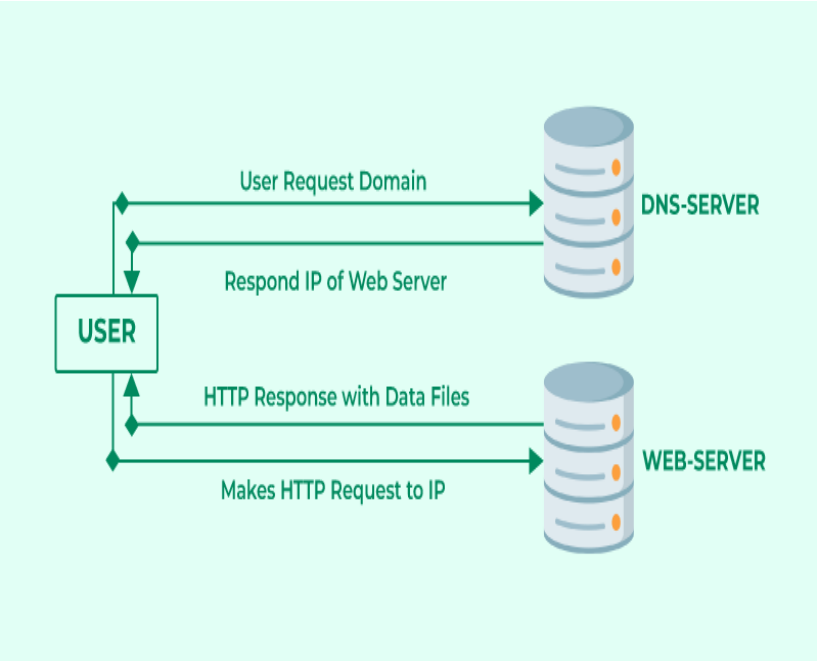
3.3 Τι είναι ένα δίκτυο client-server

Ένα δίκτυο client-server [3] είναι το μέσο μέσω του οποίου οι πελάτες έχουν πρόσβαση σε πόρους και υπηρεσίες από έναν κεντρικό υπολογιστή, είτε μέσω ενός τοπικού δικτύου (LAN), είτε μέσω Διαδίκτυου. Ένας μοναδικός διακομιστής που ονομάζεται daemon server μπορεί να χρησιμοποιηθεί με μοναδικό σκοπό την αναμονή αιτημάτων πελάτη, οπότε η σύνδεση δικτύου ξεκινά μέχρι να εκπληρωθεί το αίτημα πελάτη.

Η κίνηση δικτύου κατηγοριοποιείται ως πελάτη-προς-διακομιστή ή από διακομιστή-προς-διακομιστή. Οι δημοφιλείς υπηρεσίες δικτύου περιλαμβάνουν το ηλεκτρονικό ταχυδρομείο, την κοινή χρήση αρχείων και τον Παγκόσμιο Ιστό. Ένα σημαντικό πλεονέκτημα του δικτύου client-server είναι η κεντρική διαχείριση εφαρμογών και δεδομένων.

Στον κόσμο του Διαδικτύου, πολλές τεχνολογίες έχουν τις ρίζες τους στο μοντέλο πελάτη-διακομιστή. Σε αυτό το μοντέλο, ένας κεντρικός υπολογιστής (ο διακομιστής) παρέχει υπηρεσίες σε άλλους υπολογιστές (τους πελάτες). Αυτές οι υπηρεσίες περιλαμβάνουν πρόσβαση σε πόρους όπως αρχεία, περιεχόμενο, επεξεργαστική ισχύ και διαχείριση εξουσιοδότησης χρήστη. Αυτή η προσέγγιση διαφοροποιείται από την ομότιμη δικτύωση όπου όλοι οι υπολογιστές (ομότιμοι) μοιράζονται πόρους με όλους τους άλλους.

Οι πελάτες εκκινούν αιτήματα στον διακομιστή και ο διακομιστής απαντά με την επιθυμητή υπηρεσία. Είναι σημαντικό να σημειωθεί ότι ο πελάτης είναι συνήθως μια συσκευή χρήστη, όπως ένας επιτραπέζιος υπολογιστής, που χρησιμοποιεί σύνδεση στο Διαδίκτυο και πρόγραμμα περιήγησης για να συνδεθεί στον διακομιστή.



Εικόνα 2.2: Client Server-Request model

3.4 Βασικά Χαρακτηριστικά Αρχιτεκτονικής Client-Server

Το μοντέλο αρχιτεκτονικής πελάτη-διακομιστή ακολουθεί βασικά πρότυπα: το αίτημα-απόκριση και το αίτημα σύνδεσης. Αυτό σημαίνει ότι η ραχοκοκαλιά του μοντέλου βρίσκεται στους πελάτες που κάνουν αιτήματα σε έναν διακομιστή ενώ ο διακομιστής ερμηνεύει αυτά τα αιτήματα και στέλνει πίσω μια κατάλληλη απάντηση.

Ακολουθούν ορισμένα πρόσθετα χαρακτηριστικά αυτής της αρχιτεκτονικής:

- **Δυνατότητα απεριόριστης χωρητικότητας αποθήκευσης**: Με την κλιμάκωση της δομής της εφαρμογής, οι διακομιστές μπορούν ενδεχομένως να χειριστούν περισσότερες χωρητικότητες αποθήκευσης. Αυτό εξαρτάται από τη διαχείριση του διακομιστή και τη χωρητικότητα φόρτωσης του δικτύου διακομιστή πελάτη.
- **Διαδικασίες από την πλευρά του διακομιστή**: Πρόκειται για διεργασίες που πραγματοποιούνται στον διακομιστή, μακριά από την πλευρά του πελάτη. Ένα απλό παράδειγμα μπορεί να είναι τα σενάρια από την πλευρά του διακομιστή που αποδίδουν δυναμικό περιεχόμενο σε ιστοσελίδες.
- **Διακεκριμένοι πελάτες**: Με την αρχιτεκτονική διακομιστή πελάτη, πολλοί διαφορετικοί πελάτες μπορούν να έχουν πρόσβαση σε έναν μόνο διακομιστή χωρίς να δημιουργούν επιπλέον κίνηση.

3.5 Πλεονεκτήματα-Μειονεκτήματα

Ένα από τα κύρια πλεονεκτήματα του μοντέλου πελάτη-διακομιστή [4] είναι η συγκέντρωση του. Η ύπαρξη κεντρικού διακομιστή διευκολύνει τη διαχείριση και την ενημέρωση δεδομένων και υπηρεσιών. Αυτό το μοντέλο επιτρέπει επίσης βελτιωμένη επεκτασιμότητα, καθώς μπορούν να προστεθούν

περισσότεροι πελάτες χωρίς να επηρεαστεί η απόδοση του διακομιστή. Η υψηλότερη ασφάλεια είναι ένα άλλο πλεονέκτημα καθώς όλα τα δεδομένα αποθηκεύονται στην πλευρά του διακομιστή.

Από την άλλη πλευρά, το μοντέλο πελάτη-διακομιστή έχει ένα μόνο σημείο αποτυχίας. Εάν ο διακομιστής πέσει, επηρεάζεται ολόκληρο το δίκτυο. Επίσης, η μεγάλη κίνηση δικτύου μπορεί να υπερφορτώσει τον διακομιστή, οδηγώντας σε χαμηλότερη απόδοση. Τέλος, λόγω της συγκεντρωτικής φύσης του, το μοντέλο στερείται της ευρωστίας που υπάρχει σε κατανεμημένα δίκτυα όπως το peer-to-peer.

Από αρχιτεκτονικής άποψης, το μοντέλο πελάτης-διακομιστής παρέχει έναν σαφή καταμερισμό εργασίας—οι διακομιστές διαχειρίζονται πόρους ενώ οι πελάτες παρέχουν διεπαφές για την αλληλεπίδραση με τον χρήστη. Αυτός ο διαχωρισμός επιτρέπει την ευκολότερη ανάπτυξη και διαχείριση εφαρμογών.

Ωστόσο, αυτή η αρχιτεκτονική μπορεί να γίνει εμπόδιο όταν αντιμετωπίζουμε μεγάλους όγκους χρηστών ή μεγάλα σύνολα δεδομένων. Η απόδοση και η χωρητικότητα του διακομιστή μπορούν να περιορίσουν ολόκληρο το σύστημα και η αυξημένη κίνηση δικτύου μπορεί να επηρεάσει αρνητικά τη συνολική απόδοση του συστήματος.

Συμπερασματικά, ενώ το μοντέλο πελάτη-διακομιστή προσφέρει ορισμένα ισχυρά πλεονεκτήματα, οι περιορισμοί του είναι αξιοσημείωτοι. Η επιλογή χρήσης αυτού του μοντέλου πρέπει να βασίζεται σε μια προσεκτική αξιολόγηση των απαιτήσεων της εφαρμογής και της επεκτασιμότητας που θα έχει στο μέλλον.

3.6 Πώς λειτουργεί το μοντέλο Client-Server

Για να περιγραφεί η διαδικασία, ο πελάτης στέλνει ένα αίτημα υπηρεσίας στον διακομιστή, ο οποίος στη συνέχεια επεξεργάζεται το αίτημα και επιστρέφει την κατάλληλη υπηρεσία ή δεδομένα.

Αυτή η ροή επικοινωνίας ακολουθεί ένα συγκεκριμένο πρωτόκολλο, όπου ο πελάτης δημιουργεί πρώτα μια σύνδεση με τον διακομιστή (η διαδικασία σύνδεσης) πριν από την έναρξη των αιτημάτων υπηρεσίας. Τα ακριβή βήματα ποικίλλουν ανάλογα με το πρωτόκολλο και την εφαρμογή που εμπλέκονται, αλλά το βασικό μοτίβο παραμένει το ίδιο.

Σε βάθος, η επικοινωνία πελάτη-διακομιστή μπορεί να συνοψιστεί σε τρία βήματα:

Αίτημα πελάτη: Εδώ, ο πελάτης εκκινεί ένα αίτημα υπηρεσίας μέσω μιας αλληλεπίδρασης, όπως το κλικ σε ένα κουμπί σε μια ιστοσελίδα ή η εισαγωγή διαπιστευτηρίων σύνδεσης. Μια τέτοια ενέργεια οδηγεί σε ένα μορφοποιημένο μήνυμα - ουσιαστικά, ένα σύνολο εντολών σε πακέτα δικτύου - που αποστέλλεται στον διακομιστή.

Επεξεργασία διακομιστή: Κατά τη λήψη του αιτήματος, ο διακομιστής ερμηνεύει τα ληφθέντα πακέτα και εκτελεί τις απαραίτητες ενέργειες. Αυτό μπορεί να περιλαμβάνει την εκτέλεση προγραμματισμού από την πλευρά του διακομιστή, την πρόσβαση σε πόρους ή ακόμη πιο περίπλοκες ενέργειες, όπως η διαχείριση της εξουσιοδότησης χρήστη.

Απόκριση διακομιστή: Μετά την επεξεργασία του αιτήματος του πελάτη, ο διακομιστής στέλνει πίσω ένα μήνυμα απάντησης στον πελάτη. Αυτό το μήνυμα μπορεί να κυμαίνεται από περιεχόμενο έως ιστοσελίδες, μηνύματα σφάλματος ή πρόσβαση στους ισχύοντες πόρους.

3.7 Τύποι Client και Server

Οι πελάτες, γνωστοί και ως αιτητές υπηρεσιών, είναι κομμάτια υλικού υπολογιστή ή λογισμικού διακομιστή που ζητούν πόρους και υπηρεσίες που διατίθενται από έναν διακομιστή. Η υπολογιστική ισχύς του πελάτη ταξινομείται ως Thick, Thin ή Hybrid.

- **Thick Client**: ένας πελάτης που παρέχει πλούσια λειτουργικότητα, εκτελεί μόνος του το μεγαλύτερο μέρος της επεξεργασίας δεδομένων και βασίζεται πολύ ελαφρά στον διακομιστή.
- **Thin Client**: ένας διακομιστής thin-client είναι ένας ελαφρύς υπολογιστής που βασίζεται σε μεγάλο βαθμό στους πόρους του κεντρικού υπολογιστή -- ένας διακομιστής εφαρμογών εκτελεί την πλειοψηφία οποιασδήποτε απαιτούμενης επεξεργασίας δεδομένων.
- **Hybrid Client**: διαθέτοντας ένα συνδυασμό χαρακτηριστικών thin client και thick client, ένας υβριδικός πελάτης βασίζεται στον διακομιστή για την αποθήκευση μόνιμα δεδομένων, αλλά είναι ικανός για τοπική επεξεργασία.

Ο διακομιστής είναι μια συσκευή ή ένα πρόγραμμα υπολογιστή που παρέχει λειτουργικότητα για άλλες συσκευές ή προγράμματα. Οποιαδήποτε ηλεκτρονική διαδικασία που μπορεί να χρησιμοποιηθεί ή να κληθεί από έναν πελάτη για κοινή χρήση πόρων και διανομή εργασίας είναι διακομιστής. Μερικά κοινά παραδείγματα διακομιστών περιλαμβάνουν:

- **Διακομιστής εφαρμογών**: φιλοξενεί εφαρμογές Ιστού που μπορούν να χρησιμοποιήσουν οι χρήστες στο δίκτυο χωρίς να χρειάζονται δικό τους αντίγραφο.
- Υπολογιστικός διακομιστής: μοιράζεται έναν τεράστιο όγκο πόρων υπολογιστή με δικτυωμένους υπολογιστές που απαιτούν περισσότερη ισχύ CPU και RAM από ό,τι είναι συνήθως διαθέσιμο για έναν προσωπικό υπολογιστή.
- **Διακομιστής βάσεων δεδομένων**: διατηρεί και μοιράζεται βάσεις δεδομένων για οποιοδήποτε πρόγραμμα υπολογιστή που απορροφά καλά οργανωμένα δεδομένα, όπως λογισμικό λογιστικής και υπολογιστικά φύλλα.
- **Διακομιστής Ιστού**: φιλοξενεί ιστοσελίδες και διευκολύνει την ύπαρξη του Παγκόσμιου Ιστού.

3.8 Άλλα μοντέλα

Άλλα μοντέλα σχέσεων προγράμματος [4] περιλαμβάνουν peer-to-peer (P2P) και πρωτεύον/δευτερον. Στο μοντέλο P2P, κάθε κόμβος στο δίκτυο μπορεί να λειτουργήσει και ως πελάτης και ως διακομιστής. Στο πρωτεύον/δευτερεύον μοντέλο, η κύρια συσκευή ή διεργασία ελέγχει μία ή περισσότερες άλλες δευτερεύουσες συσκευές ή διεργασίες. Μόλις το δίκτυο δημιουργήσει την πρωτεύουσα/δευτερεύουσα σχέση, η κατεύθυνση του ελέγχου είναι πάντα από το πρωτεύον προς το δευτερεύον.

Το μοντέλο Client-Server διαφέρει από το Peer-to-Peer (P2P), στο οποίο κάθε κόμβος μπορεί να λειτουργήσει τόσο ως πελάτης όσο και ως διακομιστής. Αντίθετα, στο Client-Server, οι ρόλοι είναι αυστηρά διαχωρισμένοι.

	Client-Server	**Peer-to-Peer (P2P)**
Δομή	Κεντρική διαχείριση	Αποκεντρωμένη
Ασφάλεια	Υψηλή λόγω κεντρικού ελέγχου	Χαμηλότερη, λόγω αποκεντρωμένης φύσης
Αποδοτικότητα	Υψηλή αλλά με κίνδυνο bottle-neck	Μοιρασμένος φόρτος εργασίας
Ανθεκτικότητα	Ευάλωτο σε αποτυχία του διακομιστή	Ανθεκτικότερο, καθώς δεν υπάρχει κεντρικός κόμβος

Πίνακας 3.1 Σύγκριση των μοντέλων Client Server και P2P

Κεφάλαιο 4ο: Πρωτόκολλα του TCP/IP Μοντέλου

4.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα εξεταστούν με μεγαλύτερη λεπτομέρεια τα βασικά πρωτόκολλα που υλοποιούν τις λειτουργίες κάθε επιπέδου. Τα πρωτόκολλα αυτά αποτελούν την «καρδιά» της δικτυακής επικοινωνίας, καθορίζοντας τη δομή των πακέτων, τη ροή των δεδομένων, την αξιοπιστία της μετάδοσης και την ταυτοποίηση των τελικών συσκευών. Τα πρωτόκολλα του μοντέλου TCP/IP που θα αναλυθούν είναι:

- **Επίπεδο εφαρμογής**: DHCP, DNS, HTTP, HTTPS
- **Επίπεδο Μεταφοράς**: UDP, TCP
- **Επίπεδο Δικτύου**: IP
- **Επίπεδο Ζεύξης**: ARP, Ethernet

Η κατανόηση της λειτουργίας των πρωτοκόλλων είναι πολύ σημαντική για τη διάγνωση προβλημάτων, τη διασφάλιση της αποδοτικότητας των δικτύων και την κατανόηση της ροής των πληροφοριών.

4.2 DHCP (Επίπεδο Εφαρμογής)

Κάθε συσκευή για να συνδεθεί σε ένα δίκτυο χρειάζεται μια διεύθυνση IP η οποία θα αναλυθεί σε επόμενο κεφάλαιο. Τις διευθύνσεις αυτές μπορεί να τις δώσει χειροκίνητα ο διαχειριστής του δικτύου (Static IP) ή μπορεί να χρησιμοποιήσει το DHCP.

Το DHCP [5],[6] είναι πρωτόκολλο του επιπέδου εφαρμογής και χρησιμοποιείται για τη δυναμική-αυτόματη εκχώρηση διευθύνσεων IP (Dynamic IP) σε κάθε δικτυακή συσκευή στο δίκτυο ενός οργανισμού. Μερικά παραδείγματα περιλαμβάνουν επιτραπέζιους υπολογιστές και φορητούς υπολογιστές, thin clients και προσωπικές συσκευές.

Το DHCP επιπλέον εκχωρεί διευθύνσεις συστήματος ονομάτων τομέα (DNS), μάσκες υποδικτύου και προεπιλεγμένες πύλες. Όλα αυτά επιτρέπουν στις συσκευές να επικοινωνούν με το Διαδίκτυο και μεταξύ τους εντός των ορίων του δικτύου.

4.2.1 DHCP Components

Τα κύρια στοιχεία DHCP περιλαμβάνουν: διακομιστή DHCP (DHCP Server), DHCP πελάτη (DHCP Client) και DHCP relay.

- **Διακομιστής DHCP:** Ένας διακομιστής DHCP είναι αυτό που χρησιμοποιεί το σύστημα για να παρέχει αυτόματα διευθύνσεις IP και πρόσθετες παραμέτρους δικτύου στις συσκευές που συνδέονται στο δίκτυό. Είναι σε θέση να παρέχει προσωρινές ή δυναμικές διευθύνσεις IP που λαμβάνονται από μια ομάδα διαθέσιμων διευθύνσεων.
- **Client DHCP:** Ένας πελάτης DHCP είναι μια συσκευή που λειτουργεί ως κεντρικός υπολογιστής και λαμβάνει τις πληροφορίες που αποστέλλονται από τον διακομιστή DHCP. Αυτό περιλαμβάνει οποιαδήποτε συσκευή μπορεί να συνδεθεί στο δίκτυο και χρειάζεται δεδομένα από τον διακομιστή DHCP για να αλληλεπιδράσει με το δίκτυο.

- **Relay DHCP:** Ένα DHCP relay αναφέρεται σε οποιοδήποτε κεντρικό υπολογιστή πρωτοκόλλου ελέγχου μετάδοσης (TCP/IP) που προωθεί μηνύματα DHCP μεταξύ διακομιστών και πελατών. Ένα DHCP relau παίζει ουσιαστικό ρόλο, για παράδειγμα, όταν ένα δίκτυο αποτελείται από πολλά υποδίκτυα. Σε αυτήν την περίπτωση, ένα DHCP relay επιτρέπει σε έναν διακομιστή DHCP να παρέχει τις απαραίτητες πληροφορίες σε όλους τους πελάτες τόσο στο κύριο δίκτυο όσο και στο υποδίκτυο.

4.2.2 Dynamic IP VS Static IP

1. **Dynamic IP**
    - Ανατίθεται αυτόματα μέσω του πρωτοκόλλου DHCP.
    - Η διεύθυνση δίνεται προσωρινά και ενδέχεται να αλλάξει κάθε φορά που η συσκευή συνδέεται στο δίκτυο.
    - Εύκολη διαχείριση από τον διαχειριστή του δικτύου.
    - Ιδανική για οικιακά δίκτυα, Wi-Fi ή περιβάλλοντα με πολλές συσκευές.

2. **Static IP**
    - Ορίζεται χειροκίνητα από τον διαχειριστή του δικτύου.
    - Η IP παραμένει σταθερή ανεξάρτητα από το πόσες φορές επανεκκινείται ή αποσυνδέεται η συσκευή.
    - Χρήσιμη σε εξυπηρετητές (servers), εκτυπωτές, κάμερες IP και VPN (virtual private network).

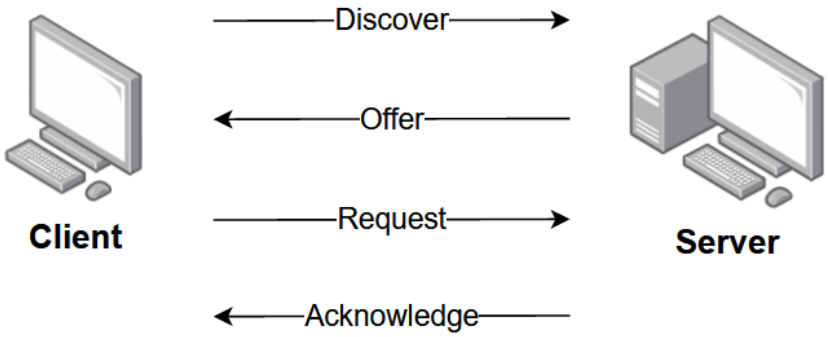
Τομέας	Dynamic IP	Static IP
Απόδοση IP	Αυτόματη μέσω DHCP	Χειροκίνητα
Διάρκεια	Προσωρινή	Μόνιμη
Διαχείριση	Αυτόματη	Απαιτεί ρύθμιση
Ασφάλεια	Μεγαλύτερη	Πιο ευάλωτη
Χρήση	Οικιακά δίκτυα/κινητές συσκευές	Servers, VPN, IP κάμερες

Πίνακας 3.2: Σύγκριση Dynamic IP - Static IP

4.2.3 Διαδικασία DORA(Discovery-Offer-Request-Ack)

Για να αποκτήσει διεύθυνση IP μία συσκευή με τη χρήση του πρωτοκόλλου DHCP, πρέπει να εκτελεστούν τέσσερα βήματα στο παρασκήνιο:

1. **DHCP Discover Message:** Ο Client που θέλει να αποκτήσει μια διεύθυνση IP, δεν γνωρίζει την ύπαρξη κάποιου DHCP server στο δίκτυο, οπότε θα στείλει σε όλους ένα μήνυμα (Broadcast) DHCP Discover Message για να ανακαλύψει τους διαθέσιμους DHCP Servers.
2. DHCP Offer Message: Ένας ή περισσότεροι DHCP servers απαντούν με DHCP Offer Message, προσφέροντας μια διεύθυνση IP και τις υπόλοιπες παραμέτρους που χρείαζεται ο Client.
3. **DHCP Request Message:** Ο Client επιλέγει μία από τις προσφορές που έλαβε και στέλνει ένα DHCP Request Message ως επιβεβαίωση. Αυτό το μήνυμα ενημερώνει και τους υπόλοιπους DHCP servers ότι απορρίπτει τις δικές τους προσφορές.
4. **DHCP ACK Message:** Ο DHCP server επιβεβαιώνει την ανάθεση της IP με ένα DHCP ACK Message. Από αυτό το σημείο, ο client μπορεί να χρησιμοποιήσει κανονικά τη διεύθυνση IP που επέλεξε.



Σχήμα 4.1: DHCP DORA

4.3 DNS (Επίπεδο Εφαρμογής)

Το Domain Name System (DNS) [7] αποτελεί σημαντικό θεμέλιο της λειτουργίας του Διαδικτύου, καθώς επιτρέπει την αντιστοίχιση ευκολομνημόνευτων ονομάτων υπολογιστών σε διευθύνσεις IP. Οι άνθρωποι χρησιμοποιούν ονόματα (π.χ. www.example.com), ενώ το ίδιο το δίκτυο βασίζεται σε αριθμητικές διευθύνσεις. Το DNS είναι :

1. μια κατανεμημένη, ιεραρχική αρχιτεκτονική εξυπηρετών DNS (DNS Servers). Οι εξυπηρετητές DNS αποθηκεύουν εγγραφές που περιλαμβάνουν αντιστοιχίσεις μεταξύ ονομάτων και διευθύνσεων IP.
2. ¨Ενα πρωτόκολλο επιπέδου εφαρμογής με το οποίο υπολογιστές και DNS servers μπορούν να υποβάλουν ερωτήματα στην κατανεμημένη βάση.

4.3.1 Τύποι DNS Server

Το DNS στηρίζεται σε μια ιεραρχική και κατανεμημένη αρχιτεκτονική, η οποία περιλαμβάνει **τρεις βασικούς τύπους εξυπηρετητών** που συνεργάζονται για την επίλυση ενός ερωτήματος DNS. Κάθε τύπος παίζει καθοριστικό ρόλο στη διαδικασία αντιστοίχισης ενός domain name με μια διεύθυνση IP.

1) Εξυπηρέτης Root DNS

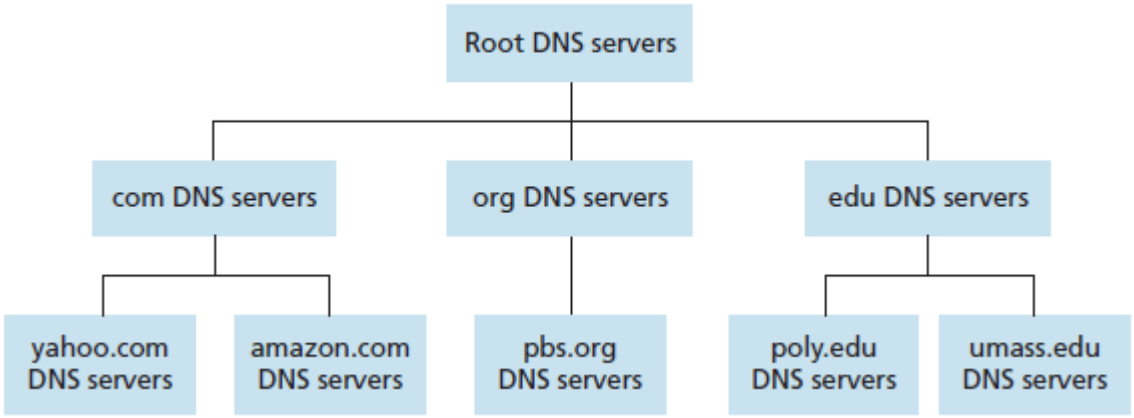
Οι Root DNS servers βρίσκονται στην κορυφή της ιεραρχίας του DNS. Υπάρχουν 13 κύριοι root servers στον κόσμο (ονομάζονται από A ως M), ο κάθε ένας από αυτούς αποτελείται από ένα σύμπλεγμα αντιγράφων εξυπηρετών για λόγους αξιοπιστίας και ασφάλειας. Οι root servers δεν γνωρίζουν την IP ενός domain name, αλλά παρέχουν πληροφορίες για τους εξυπηρετητές του επόμενου επιπέδου – δηλαδή τους TLD servers.

2) TLD DNS Servers

Οι TLD (Top-Level-Domain) servers είναι υπεύθυνοι για τα domains που τελειώνουν με συγκεκριμένες καταλήξεις (Top-Level Domains), όπως .com, .edu, .net, κ.ά, καθώς επίσης και για όλους τους τομείς ανωτάτου επιπέδου χωρών όπως .gr, .de, .uk, κ.α.. Κάθε TLD server γνωρίζει τις διευθύνσεις IP των αυθεντικών DNS εξυπηρετών που είναι υπεύθυνοι για τα επιμέρους domain names εντός του TLD.

3) Αυθεντικοί Εξυπηρετητές DNS

Ο αυθεντικός DNS εξυπηρετητής είναι ο μόνος που περιέχει την τελική και επίσημη καταχώρηση για το domain name που ζητείται. Αυτός ο εξυπηρετητής επιστρέφει την τελική διεύθυνση IP που αντιστοιχεί στο πλήρες domain (π.χ. www.example.com).



Εικόνα 4.2: Ιεραρχική Δομή DNS

4.5.2 Τρόπος Λειτουργίας του DNS

Το **DNS** λειτουργεί ως ένας **κατάλογος του Διαδικτύου** που μεταφράζει **ονομασίες ιστοσελίδων** (όπως www.example.com) σε **διευθύνσεις IP** που μπορούν να καταλάβουν οι υπολογιστές.

Η διαδικασία περιλαμβάνει τα εξής βήματα:

1. **Ο υπολογιστής (client)** θέτει ένα ερώτημα DNS, ζητώντας την IP ενός domain (π.χ. www.example.com).
2. Το ερώτημα αποστέλλεται στον **τοπικό DNS εξυπηρετητή** (local DNS server), ο οποίος βρίσκεται στο τοπικό δίκτυο, αν γνωρίζει την απάντηση (μέσω cache), δηλαδή αν υπάρχει η αντιστοιχία στη μνήμη του τοπικού DNS server από πρόσφατη αναζήτηση, την επιστρέφει αμέσως.
3. Αν δεν έχει την απάντηση, ξεκινάει η **ιεραρχική αναζήτηση**:
    - **Root DNS servers** → δίνουν πληροφορία για το ποιοι είναι οι TLD servers (π.χ. για .com).

- **TLD DNS servers** → δίνουν τον αυθεντικό εξυπηρετητή για το example.com.
- **Αυθεντικοί DNS servers** → δίνουν την τελική διεύθυνση IP του www.example.com.

4. Ο τοπικός DNS εξυπηρετητής **αποθηκεύει την απάντηση** στη μνήμη του (DNS cache) για μελλοντικά αιτήματα.
5. Η **διεύθυνση IP επιστρέφεται** στον υπολογιστή του χρήστη.

4.4 HTTP (Επίπεδο Εφαρμογής)

Το πρωτόκολλο HTTP (HyperText Transfer Protocol) [8] αποτελεί τον θεμέλιο λίθο της επικοινωνίας στο Διαδίκτυο. Πρόκειται για ένα πρωτόκολλο επιπέδου εφαρμογής που επιτρέπει τη μεταφορά υπερκειμένου (hypertext) και άλλων τύπων δεδομένων μεταξύ ενός client που συνήθως είναι ένας φυλλομετρητής (browser) και ενός web server. Είναι το βασικό πρωτόκολλο που χρησιμοποιείται για την πρόσβαση σε ιστοσελίδες και υπηρεσίες του Παγκόσμιου Ιστού (World Wide Web). Με την εξέλιξη των τεχνολογιών του Διαδικτύου, το HTTP έχει επίσης εξελιχθεί ώστε να καλύπτει αυξημένες ανάγκες σε ταχύτητα, ασφάλεια και αποδοτικότητα.

4.4.1 Βασικά Χαρακτηριστικά HTTP

Το HTTP λειτουργεί βάσει της αρχής **αιτήματος-απόκρισης (request-response) και του μοντέλου client-server**. Ο client αποστέλλει ένα αίτημα (HTTP request) στον web server ζητώντας κάποιον πόρο, όπως ένα HTML αρχείο ή μια εικόνα. Ο server απαντά με ένα μήνυμα απόκρισης (HTTP response), το οποίο περιλαμβάνει τον ζητούμενο πόρο ή έναν κωδικό κατάστασης (status code) που υποδεικνύει την επιτυχία ή αποτυχία του αιτήματος.

Η επικοινωνία βασίζεται κυρίως στις εξής αρχές:

- **Ανεξαρτησία καταστάσεων (statelessness):** Κάθε αίτημα HTTP αντιμετωπίζεται ως ανεξάρτητο και δεν υπάρχει διατήρηση πληροφορίας μεταξύ διαδοχικών αιτημάτων, εκτός αν χρησιμοποιηθούν τεχνολογίες όπως cookies ή sessions.
- **Χρήση TCP:** Το HTTP λειτουργεί πάνω από το TCP, διασφαλίζοντας την αξιόπιστη παράδοση των δεδομένων.
- **Πρωτόκολλο κειμένου (text-based):** Τα αιτήματα και οι αποκρίσεις του HTTP είναι αναγνώσιμα από άνθρωπο, καθώς αποτελούνται από απλό κείμενο.

4.4.2 Παραμένουσες vs Μη Παραμένουσες Συνδέσεις

Στο πλαίσιο της επικοινωνίας client-server μέσω του HTTP, ένα κρίσιμο σημείο διαφοροποίησης είναι ο τρόπος με τον οποίο διαχειρίζεται η σύνδεση TCP κατά την ανταλλαγή αιτήσεων και αποκρίσεων. Υπάρχουν δύο βασικές κατηγορίες: οι **μη παραμένουσες** (non-persistent) και οι **παραμένουσες** (persistent) συνδέσεις.

Μη Παραμένουσες Συνδέσεις (Non-persistent HTTP)

Στην παλαιότερη αυτή μορφή λειτουργίας, κάθε HTTP αίτημα απαιτεί μια νέα σύνδεση TCP. Η διαδικασία περιλαμβάνει:

1. Δημιουργία σύνδεσης TCP.
2. Αποστολή HTTP αιτήματος.
3. Λήψη HTTP απόκρισης.

4. Τερματισμός της σύνδεσης TCP.

Για κάθε αντικείμενο (π.χ., HTML αρχείο, εικόνες, CSS), ο client πρέπει να δημιουργήσει ξεχωριστή TCP σύνδεση. Αυτό σημαίνει πως για τη φόρτωση μιας ιστοσελίδας με πολλαπλά στοιχεία, απαιτείται μεγάλος αριθμός συνδέσεων, οδηγώντας σε σημαντική επιβάρυνση του χρόνου απόκρισης λόγω των καθυστερήσεων σύνδεσης και αποσύνδεσης.

Παραμένουσες Συνδέσεις (Persistent HTTP)

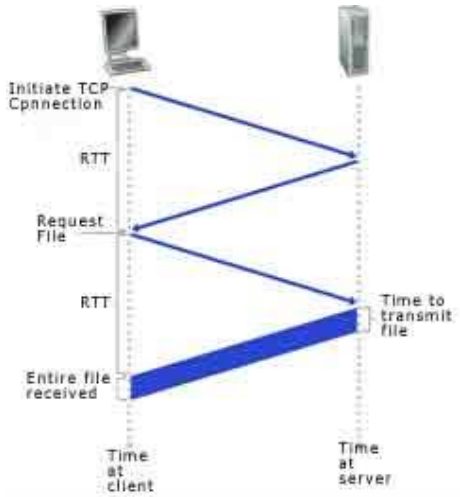
Η εισαγωγή του **HTTP/1.1** επέτρεψε την υποστήριξη παραμενουσών συνδέσεων, γνωστών και ως **HTTP keep-alive**. Σε αυτό το μοντέλο:

1. Η σύνδεση TCP παραμένει ενεργή μετά την πρώτη αίτηση/απόκριση.
2. Πολλαπλά HTTP αιτήματα μπορούν να σταλούν στην ίδια σύνδεση χωρίς να χρειάζεται επανεγκαθίδρυση.

Αυτό μειώνει τα επιπλέον RTT (round-trip time), δηλαδή τον που απετείται από την στιγμή που ο client κάνει ένα request στον server, μέχρι τη στιγμή που θα λάβει την απάντηση. Αυτό έχει ως αποτέλεσμα να μειωθεί ο φόρτος του server και στο δίκτυο.

Τομέας	Μη Παραμένουσα Σύνδεση	Παραμένουσα Σύνδεση
Σύνδεση TCP	Για κάθε αίτημα	Μία σύνδεση για πολλά αιτήματα
Απόδοση	Χαμηλότερη (πολλαπλά RTT)	Υψηλότερη (λιγότερα RTT)
Επιβάρυνση Δικτύου	Υψηλή	Μειωμένη

Πίνακας 4.1: Παραμένουσες vs Μη Παραμένουσες Συνδέσεις.



Σχήμα 4.3: Αίτημα HTTP

4.4.3 Web Cache

Το **Web cache** [9] είναι ένας ενδιάμεσος μηχανισμός που αποθηκεύει προσωρινά αντίγραφα ιστοσελίδων και άλλων διαδικτυακών πόρων. Όταν ένας χρήστης ζητά μια ιστοσελίδα, ο υπολογιστής ή ο διακομιστής μεσολάβησης (proxy) ελέγχει αν έχει ήδη ένα αποθηκευμένο αντίγραφο της σελίδας

στη μνήμη cache. Αν υπάρχει και είναι έγκυρο, το παραδίδει απευθείας στον χρήστη χωρίς να χρειαστεί να επικοινωνήσει με τον απομακρυσμένο εξυπηρετητή.

Πλεονεκτήματα:

- **Ταχύτερη απόκριση**: Μειώνεται ο χρόνος φόρτωσης της σελίδας για τον χρήστη.
- **Μείωση φόρτου εξυπηρετητών**: Λιγότερα αιτήματα αποστέλλονται στον Web server.
- **Οικονομία εύρους ζώνης (bandwidth)**: Εξοικονομείται κίνηση στο δίκτυο.

4.5 UDP (Επίπεδο Μεταφοράς)

Πρωτού αναλυθούν τα δύο πρωτόκολλα μεταφοράς (UDP, TCP), είναι σημαντικό να αναφερθεί οι όροι Segment, με τον οποίο ορίζονται τα πακέτα στο επίπεδο μεταφοράς και ο όρος Segmentation που είναι η διαδικασία διαίρεσης των μηνυμάτων εφαρμογής σε μικρότερα κομμάτια (segments).

Το **UDP [10]** είναι ένα πρωτόκολλο επιπέδου μεταφοράς το οποίο παρέχει έναν απλό και γρήγορο τρόπο αποστολής δεδομένων μεταξύ εφαρμογών σε διαφορετικούς υπολογιστές. Το UDP δεν παρέχει μηχανισμούς για την εξασφάλιση αξιόπιστης παράδοσης, σειράς ή επανεμετάδοσης πακέτων. Αυτό το καθιστά **πιο ελαφρύ και αποδοτικό** για εφαρμογές όπου η ταχύτητα προτιμάται από την αξιοπιστία, όπως η ροή πολυμέσων (streaming), το VoIP και τα διαδικτυακά παιχνίδια.

Η βασική λειτουργία του UDP βασίζεται στη μετάδοση **segments** χωρίς να απαιτείται η εγκαθίδρυση σύνδεσης μεταξύ αποστολέα και παραλήπτη. Ο αποστολέας απλώς στέλνει τα πακέτα, και ο παραλήπτης τα λαμβάνει όσο καλύτερα μπορεί, χωρίς επιβεβαίωση παραλαβής.

Παρά τον "ανεπίσημο" χαρακτήρα του, το UDP παραμένει κρίσιμο για εφαρμογές όπου ο χρόνος απόκρισης είναι σημαντικότερος από την ακεραιότητα των δεδομένων.

4.5.1 Χαρακτηριστικά UDP

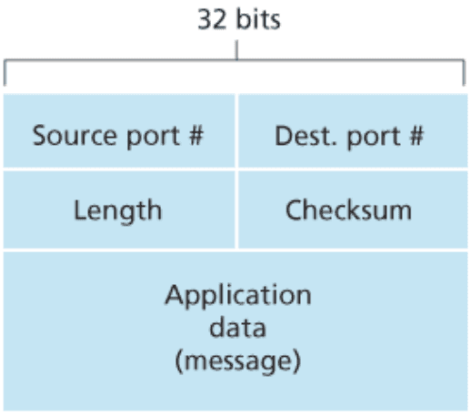
Το UDP σχεδιάστηκε με σκοπό την απλότητα και την ταχύτητα στη μεταφορά δεδομένων. Τα βασικά του χαρακτηριστικά είναι:

- **Μη συνδεσμοστραφές πρωτόκολλο:** Το UDP δεν απαιτεί την εγκαθίδρυση σύνδεσης πριν από τη μετάδοση των δεδομένων. Ο αποστολέας μπορεί να στείλει τα datagrams απευθείας, χωρίς προηγούμενη επικοινωνία με τον παραλήπτη.
- **Χωρίς επιβεβαίωση παραλαβής:** Δεν υπάρχει μηχανισμός αναγνώρισης ή επιβεβαίωσης ότι το πακέτο παραλήφθηκε επιτυχώς. Αν το πακέτο χαθεί ή φτάσει με λάθος, δεν υπάρχει προσπάθεια επαναποστολής.
- **Χωρίς έλεγχο ροής ή συμφόρησης:** Το UDP δεν περιλαμβάνει μηχανισμούς για τη ρύθμιση του ρυθμού αποστολής πακέτων ή για την αποφυγή συμφόρησης στο δίκτυο.
- **Ανεξάρτητα πακέτα (Segments):** Κάθε UDP segment αντιμετωπίζεται ανεξάρτητα και μπορεί να φτάσει με διαφορετική σειρά από την οποία εστάλει.
- **Μικρή επικεφαλίδα (header):** Η επικεφαλίδα του UDP είναι μόνο 8 bytes, κάτι που το καθιστά αποδοτικό ως προς τον όγκο μεταφερόμενων δεδομένων.
- **Γρήγορη μετάδοση:** Λόγω της απλότητάς του, το UDP προσφέρει υψηλή απόδοση και χαμηλή καθυστέρηση, κάτι που είναι ιδιαίτερα χρήσιμο σε εφαρμογές πραγματικού χρόνου.

4.5.2 Δομή UDP Segment

Το UDP (User Datagram Protocol) χρησιμοποιεί μια απλή και ελαφριά δομή πακέτου, γνωστή ως *UDP segment*. Η επικεφαλίδα (header) του UDP είναι σταθερού μεγέθους και αποτελείται από **μόλις 64bits**, χωρισμένα σε τέσσερα βασικά πεδία:

- **Source Port (16 bits):** Η θύρα του αποστολέα. Καθορίζει ποια εφαρμογή έστειλε το πακέτο.
- **Destination Port (16 bits):** Η θύρα του παραλήπτη. Προσδιορίζει ποια εφαρμογή πρέπει να το παραλάβει**.**
- **Length (16 bits):** Το συνολικό μέγεθος του segment.
- **Checksum (16 bits):** Το πεδίο Checksum στο UDP χρησιμοποιείται για τον έλεγχο σφαλμάτων. Υπολογίζεται από τα περιεχόμενα του πακέτου και επιτρέπει στον παραλήπτη να εντοπίσει αλλοιώσεις που μπορεί να προκλήθηκαν κατά τη μετάδοση. Αν ο έλεγχος αποτύχει, το πακέτο απορρίπτεται.
- Στη συνέχεια ακολουθούν τα δεδομένα του segment.



Σχήμα 4.4: Δομή UDP Segment

Εν κατακλδείδι, το UDP δεν χρειάζεται να εγκαθυδρίσει σύνδεση με τον παραλήπτη, οπότε στέλνει μηνύματα χώρις κάποιον έλεγχο για το αν φτάνουν τα μηνύματα στον προορισμό τους και αν φτάνουν, αυτά έχουν τη σωστή σειρά.

4.6 TCP (Επίπεδο Μεταφοράς)

Το **TCP** [11] αποτελεί ένα από τα βασικότερα πρωτόκολλα του Διαδικτύου και βρίσκεται στο επίπεδο μεταφοράς της στοίβας TCP/IP. Σκοπός του είναι να εξασφαλίσει την αξιόπιστη και ακριβή μεταφορά δεδομένων μεταξύ δύο υπολογιστικών συστημάτων που επικοινωνούν μέσω δικτύου. Παρέχει τις βασικές λειτουργίες που απαιτούνται για την εγκαθίδρυση, διατήρηση και τερματισμό μίας σύνδεσης.

4.6.1 Χαρακτηριστικά TCP

- **Συνδεσμικό (Connection-oriented)**: Πριν τη μεταφορά δεδομένων, το TCP απαιτεί να δημιουργηθεί μια αξιόπιστη σύνδεση μέσω της διαδικασίας **three-way handshake,** η οποία θα αναλυθεί στη συνέχια. Αυτό διασφαλίζει ότι και τα δύο άκρα είναι έτοιμα να επικοινωνήσουν.
- **Αξιόπιστη μετάδοση δεδομένων:** Το TCP παρέχει μηχανισμούς επιβεβαίωσης παραλαβής (ACK), επανεκπομπής χαμένων πακέτων και αναδιάταξης των segments στην σωστή σειρά, ώστε να φτάνουν όλα τα δεδομένα ακέραια και με σωστή σειρά.
- **Έλεγχος ροής (Flow control):** Ο μηχανισμός αυτός διασφαλίζει ότι ο αποστολέας δεν θα υπερφορτώσει τον παραλήπτη με περισσότερα δεδομένα από όσα μπορεί να επεξεργαστεί, χρησιμοποιώντας το πεδίο *Window Size*.
- **Έλεγχος συμφόρησης (Congestion control):** Το TCP προσαρμόζει τη ροή των δεδομένων με βάση τη συμφόρηση στο δίκτυο, αποφεύγοντας την υπερφόρτωση των ενδιάμεσων δικτυακών κόμβων.

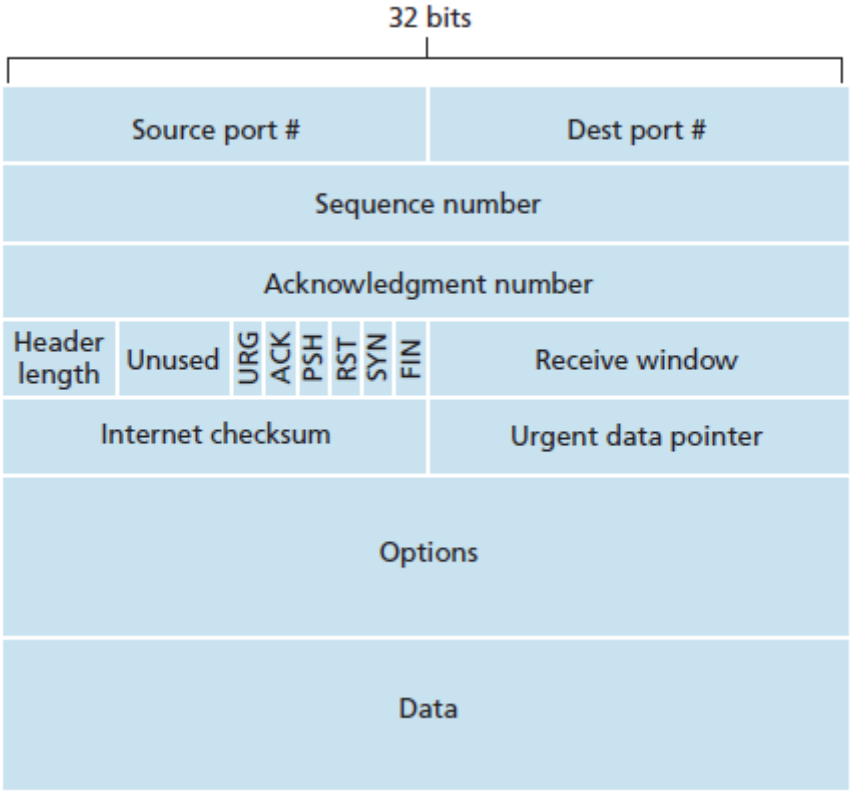
4.6.2 Δομή TCP Segment

Κάθε TCP segment [11] αποτελείται από δύο βασικά μέρη: **την κεφαλίδα (header)** και **τα δεδομένα (payload)**. Η κεφαλίδα περιέχει κρίσιμες πληροφορίες ελέγχου που χρησιμοποιούνται για τη διαχείριση της σύνδεσης και τη μετάδοση των δεδομένων.

Βασικά πεδία TCP Header (20 bytes + options):

1. **Source Port (16 bits):** Η θύρα του αποστολέα. Καθορίζει ποια εφαρμογή έστειλε το πακέτο.
2. **Destination Port (16 bits):** Η θύρα του παραλήπτη. Προσδιορίζει ποια εφαρμογή πρέπει να το παραλάβει.
3. **Sequence Number (32 bits):** Ο αύξων αριθμός ακολουθίας του πρώτου byte που αποστέλλεται με αυτό το segment.
4. **Acknowledgment Number (32 bits):** Αν είναι ενεργοποιημένο το ACK flag, δείχνει τον αριθμό του επόμενου byte που ο αποστολέας αναμένει να λάβει.
5. **Header Length (4 bits):** Καθορίζει το μήκος της TCP κεφαλίδας. Απαραίτητο για να εντοπιστεί το σημείο που ξεκινούν τα δεδομένα.
6. **Flags :**
    a. **URG (Urgent):** Ένδειξη επειγόντων δεδομένων.
    b. **ACK (Acknowledgment):** Δηλώνει ότι ένα πακέτο έχει ληφθεί επιτυχώς.
    c. **PSH (Push):** Ζητά την άμεση παράδοση των δεδομένων στο επόμενο επίπεδο αμέσως.
    d. **SYN (Synchronize):** Χρησιμοποιείται κατά την έναρξη μιας TCP σύνδεσης (στο three-way handshake).
    e. **RST:** Διακόπτει απότομα μια σύνδεση TCP.
    f. **FIN (Finish):** Χρησιμοποιείται για να τερματιστεί η σύνδεση TCP με ασφαλή τρόπο.
7. **Receive Window (16bits):** Χρησιμοποιείται στον έλεγχο ροής. Δηλώνει πόσα bytes είναι ο παραλήπτης έτοιμος να δεχτεί.

8. **Checksum (16 bits):** Έλεγχος σφαλμάτων. Ελέγχει την ακεραιότητα των δεδομένων και της κεφαλίδας.
9. **Urgent Pointer (16 bits):** Χρησιμοποιείται όταν είναι ενεργοποιημένο το URG flag. Δηλώνει το τέλος των επειγόντων δεδομένων.
10. **Options (μεταβλητό μήκος):** Περιέχει επιλογές όπως το Maximum Segment Size (MSS), timestamps και άλλα χαρακτηριστικά που επεκτείνουν τη λειτουργία του TCP.
11. **Data: Τα δεδομένα που μεταφέρονται στο συγκεκριμένο segment.**



Σχήμα 4.5: Δομή TCP Segment

4.6.3 Three-Way-Handshake

Το **Three-Way Handshake** είναι μια διαδικασία τριών βημάτων που επιτρέπει σε έναν client και έναν server να:

- **συγχρονίσουν αριθμούς ακολουθίας (sequence numbers)**
- **επιβεβαιώσουν τη διαθεσιμότητά τους για επικοινωνία**
- **ξεκινήσουν μια αξιόπιστη αμφίδρομη σύνδεση TCP**

Τα Τρία Βήματα του Handshake:

1. **SYN (Synchronize) – Αίτημα σύνδεσης Ο client στέλνει ένα TCP segment με το SYN flag ενεργό (SYN = 1), δηλώνοντας την πρόθεσή του να ξεκινήσει σύνδεση. Το segment περιέχει:**
- **έναν αρχικό αριθμό ακολουθίας (Sequence Number), που προτείνεται από τον client (π.χ. Seq = m)**

4.7 SYN-ACK – Αποδοχή και συγχρονισμός από τον server

Ο server, αφού λάβει το SYN, απαντά με ένα segment όπου:

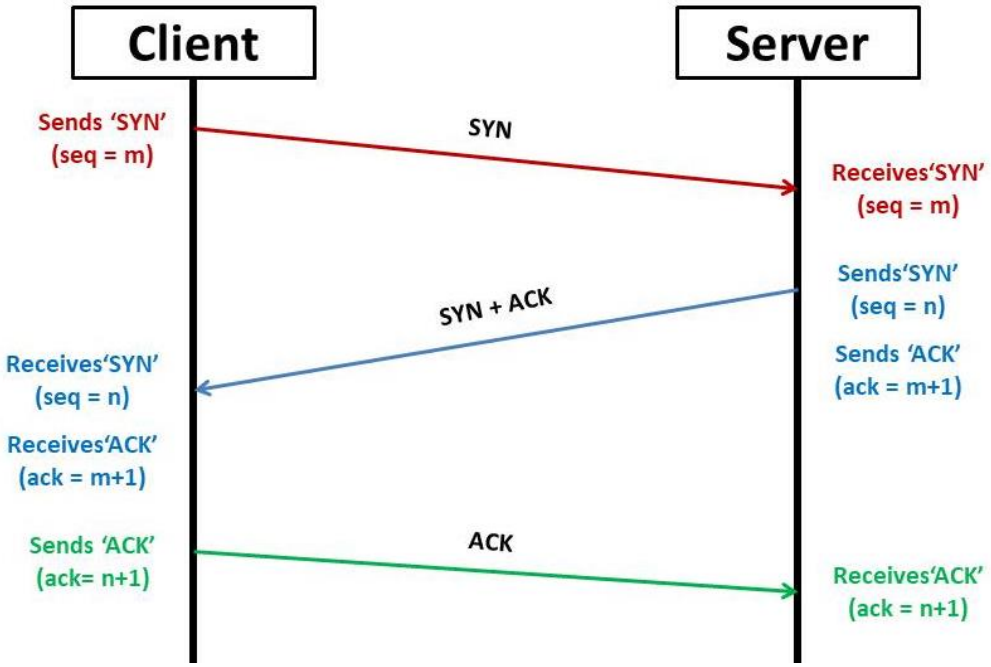
- **ενεργοποιούνται και τα SYN και ACK flags (SYN = 1, ACK = 1)**
- **ο server στέλνει τον δικό του αριθμό ακολουθίας (π.χ. Seq = n)**
- **επιβεβαιώνει τη λήψη του SYN του client στέλνοντας Ack = m + 1**

4.8 ACK – Επιβεβαίωση από τον client

Ο client απαντά στέλνοντας ένα TCP segment με:

- **μόνο το ACK flag ενεργό (ACK = 1)**
- **Ack = n + 1 επιβεβαιώνοντας τον αριθμό του server**

Μετά από αυτό το βήμα, η σύνδεση θεωρείται ενεργή, και μπορεί να ξεκινήσει η αποστολή δεδομένων.



Σχήμα 4.6: Three-Way-Handshake

4.6.4 Έλεγχος Ροής στο TCP (Flow Control)

Ο **έλεγχος ροής** [12] στο TCP είναι ένας μηχανισμός που αποσκοπεί στο να αποτρέψει την αποστολή δεδομένων με ρυθμό μεγαλύτερο από αυτόν που μπορεί να διαχειριστεί ο παραλήπτης. Ειδικά σε εφαρμογές με υψηλό ρυθμό μετάδοσης, όπως η μεταφορά αρχείων ή η ροή πολυμέσων, είναι κρίσιμο ο αποστολέας να γνωρίζει πόσα δεδομένα μπορεί να λάβει και να αποθηκεύσει προσωρινά ο παραλήπτης.

Για τον σκοπό αυτό, το TCP χρησιμοποιεί την υπηρεσία **ελέγχου ροής** (flow-control service), η οποία βασίζεται σε μια μεταβλητή γνωστή ως **παράθυρο λήψης** (receive window - rwnd). Το rwnd υποδεικνύει στον αποστολέα πόσα bytes μπορεί να αποστείλει, χωρίς να υπερβεί τη χωρητικότητα του ενταμιευτή λήψης (receive buffer) του παραλήπτη.

Το TCP προσαρμόζεται δυναμικά στις συνθήκες του παραλήπτη. Αν η εφαρμογή του παραλήπτη δεν προλαβαίνει να διαβάζει από τον ενταμιευτή λήψης, τότε αυτός γεμίζει και το rwnd μειώνεται. Αντίστροφα, όταν η εφαρμογή διαβάζει γρήγορα τα δεδομένα, δημιουργείται ελεύθερος χώρος και το rwnd αυξάνεται.

Η τιμή του παραθύρου λήψης αποστέλλεται στον αποστολέα μέσα στα πεδία της κεφαλίδας TCP. Αν ο αποστολέας λάβει τιμή rwnd = 0, οφείλει να διακόψει προσωρινά τη μετάδοση δεδομένων μέχρι να λάβει ενημερωμένο rwnd με θετική τιμή.

Ο έλεγχος ροής διασφαλίζει ότι κανένας αποστολέας TCP δεν θα υπερφορτώσει τον παραλήπτη με δεδομένα, προστατεύοντας έτσι τη σταθερότητα και την αξιοπιστία της επικοινωνίας.

4.6.5 Έλεγχος Συμφόρησης TCP

Ο **έλεγχος συμφόρησης** (congestion control) [13] αποτελεί έναν από τους βασικούς μηχανισμούς του πρωτοκόλλου TCP. Επειδή η αποστολή πακέτων TCP πραγματοποιείται πάνω από το αναξιόπιστο και μη εγγυημένο πρωτόκολλο IP, το TCP πρέπει να διαχειρίζεται προσεκτικά την ποσότητα των δεδομένων που διοχετεύει στο δίκτυο. Σε αντίθετη περίπτωση, ενδέχεται να προκληθεί συμφόρηση σε κόμβους ή ενδιάμεσες διαδρομές, οδηγώντας σε καθυστερήσεις, απώλειες πακέτων και υποβάθμιση της ποιότητας επικοινωνίας.

Το TCP χρησιμοποιεί έναν μηχανισμό βασισμένο στην παρακολούθηση και προσαρμογή του ρυθμού μετάδοσης των πακέτων. Αντί να αποστέλλει όλα τα δεδομένα αμέσως, το πρωτόκολλο περιορίζει την ταχύτητα αποστολής με βάση τις συνθήκες του δικτύου. Εάν ο αποστολέας διαπιστώσει απώλεια πακέτων ή καθυστερήσεις, μειώνει τον ρυθμό. Εάν αντίθετα δεν εντοπίζει προβλήματα, αυξάνει προοδευτικά τον όγκο των δεδομένων που αποστέλλονται.

Αργή Εκκίνηση (Slow Start)

Η αργή εκκίνηση είναι ο αρχικός μηχανισμός ελέγχου συμφόρησης του TCP, ο οποίος ενεργοποιείται όταν ξεκινά μια νέα σύνδεση. Στόχος της είναι να αποφευχθεί η υπερφόρτωση του δικτύου κατά την αρχική αποστολή δεδομένων. Επειδή δεν υπάρχει αρχική γνώση για την κατάσταση του δικτύου, το TCP ξεκινά προσεκτικά με μικρό ρυθμό αποστολής και τον αυξάνει σταδιακά, παρακολουθώντας τα σήματα επιβεβαίωσης (ACK) που λαμβάνει.

Η μεταβλητή-κλειδί της διαδικασίας είναι το παράθυρο συμφόρησης cwnd, το οποίο ελέγχει πόσα byte μπορούν να σταλούν χωρίς επιβεβαίωση. Στην αφετηρία, η τιμή του cwnd είναι συνήθως 1 MSS (Maximum Segment Size), δηλαδή το μέγιστο μέγεθος τμήματος TCP που μπορεί να μεταδοθεί.

Για κάθε επιβεβαίωση (ACK) που λαμβάνει ο αποστολέας, η τιμή του cwnd αυξάνεται κατά 1 MSS. Έτσι, κάθε γύρος μετάδοσης διπλασιάζει τον όγκο των δεδομένων που αποστέλλονται. Αυτή η εκθετική αύξηση συνεχίζεται έως ότου:

- παρατηρηθεί απώλεια πακέτου ή
- το cwnd φτάσει μια τιμή-κατώφλι που ονομάζεται ssthresh (slow start threshold).

Όταν φτάσει το όριο ssthresh, η αργή εκκίνηση τερματίζεται και το TCP περνά στη φάση αποφυγής συμφόρησης (congestion avoidance), όπου η αύξηση γίνεται πιο αργά και γραμμικά.

Ο μηχανισμός της αργής εκκίνησης επιτρέπει στο πρωτόκολλο να "δοκιμάσει" σταδιακά τα όρια του δικτύου, αυξάνοντας τον ρυθμό αποστολής μέχρι να παρατηρήσει κάποιο σημάδι συμφόρησης (όπως καθυστέρηση ή απώλεια), προκειμένου να εξισορροπήσει την απόδοση και τη σταθερότητα. Αν συμβεί απώλεια πακέτου, το TCP μειώνει σημαντικά το cwnd και συνήθως επανεκκινεί τη διαδικασία από χαμηλότερο σημείο.

Η αργή εκκίνηση, παρόλο που ονομάζεται "αργή", στην πραγματικότητα επιτρέπει γρήγορη αύξηση του ρυθμού αποστολής, υπό ελεγχόμενες συνθήκες, εξασφαλίζοντας όμως ότι το δίκτυο δεν θα κορεστεί ξαφνικά από μαζική αποστολή δεδομένων.

Αποφυγή Συμφόρησης

Σε αντίθεση με την αργή εκκίνηση, όπου το cwnd διπλασιάζεται εκθετικά με κάθε γύρο RTT, στην αποφυγή συμφόρησης η αύξηση είναι γραμμική, για κάθε επιβεβαίωση που λαμβάνει ο αποστολέας, αυξάνει το cwnd κατά ένα κλάσμα του MSS (συνήθως MSS × (MSS/cwnd)), ώστε στο τέλος κάθε

γύρου να έχει αυξηθεί κατά περίπου 1 MSS. Η πιο συντηρητική αύξηση αποσκοπεί στο να διατηρεί τη ροή δεδομένων σε ένα επίπεδο ασφαλές για το δίκτυο, χωρίς να προκληθεί υπερφόρτωση. Εάν εντοπιστεί **απώλεια πακέτου**, αυτό αποτελεί ένδειξη συμφόρησης. Το TCP τότε **μειώνει δραστικά** το παράθυρο συμφόρησης και, ανάλογα με την αιτία ανίχνευσης της απώλειας (είτε timeout είτε τριπλό ACK), εφαρμόζει διαφορετικές πολιτικές προσαρμογής. Για παράδειγμα:

- Αν εντοπιστεί απώλεια μέσω **καθυστέρησης**, το cwnd συνήθως επαναφέρεται στην αρχική τιμή (1 MSS), και το ssthresh μειώνεται στο μισό της προηγούμενης τιμής του cwnd.
- Αν εντοπιστεί μέσω **τριπλού ACK** (τριπλή παραλαβή ACK για το ίδιο τμήμα), εφαρμόζεται η μέθοδος **fast recovery** (ταχεία ανάκαμψη), η οποία επιτρέπει πιο ήπια μείωση και ταχύτερη επαναφορά.

Η αποφυγή συμφόρησης σε συνδυασμό με την αργή εκκίνηση δημιουργούν ένα **δυναμικό σύστημα ελέγχου**, που προσαρμόζει τον ρυθμό αποστολής με βάση τις συνθήκες του δικτύου, πετυχαίνοντας ισορροπία ανάμεσα στην αξιοπιστία, την αποδοτικότητα και τη σταθερότητα της σύνδεσης.

Ταχεία Ανάκαμψη

Όταν ο αποστολέας λάβει **τρεις επαναλαμβανόμενες ACKs**, θεωρεί ότι ένα πακέτο έχει χαθεί, χωρίς όμως να έχει διακοπεί πλήρως η επικοινωνία (καθώς λαμβάνει ακόμα ACKs για μεταγενέστερα πακέτα). Αντί να περιμένει το χρονόμετρο λήξης χρόνου (timeout), το TCP προχωρά σε **γρήγορη επαναμετάδοση** του χαμένου πακέτου και εισέρχεται στη φάση **ταχείας ανάκαμψης**.

Βήματα Ταχείας Ανάκαμψης

1. **Ρύθμιση τιμής ssthresh:** Το TCP μειώνει το **ssthresh** (slow start threshold) στο **μισό του congestion window** που ίσχυε όταν εντοπίστηκε η απώλεια.
2. **Αποστολή επαναμετάδοσης:** Το TCP προχωρά σε **γρήγορη επαναμετάδοση** του πακέτου που θεωρείται χαμένο, δηλαδή του πακέτου στο οποίο αναφέρονται τα επαναλαμβανόμενα ACKs.
3. **Προσωρινή αύξηση του congestion window:** Αντί να μειωθεί απότομα το cwnd, το TCP το **αυξάνει προσωρινά** κατά ένα MSS για κάθε επαναλαμβανόμενο ACK που λαμβάνει, θεωρώντας ότι το δίκτυο εξακολουθεί να μπορεί να μεταφέρει κάποια ποσότητα δεδομένων.
4. **Έξοδος από την ταχεία ανάκαμψη:** Όταν ο αποστολέας λάβει ένα νέο ACK που επιβεβαιώνει **όλο το χαμένο τμήμα**, η τιμή του **ssthresh** τίθεται στο μισό της τιμής του cwnd όταν συνέβη η απώλεια, το **cwnd** τίθεται σε 1 MSS και επιστρέφει στη φάση **αποφυγής συμφόρησης**.

Τα πλεονεκτήματα του είναι:

1. **Αποτρέπει περιττή επαναφορά στην αργή εκκίνηση**, διατηρώντας υψηλότερη απόδοση.
2. **Αντιδρά ταχύτερα στην απώλεια**, χωρίς να περιμένει λήξη χρονικού ορίου (timeout).
3. **Διατηρεί τη ροή των δεδομένων ενεργή**, αφού συνεχίζει να αποστέλλει νέα τμήματα.

4.6.6 TCP vs UDP

Έπειτα από την αναλυτική παρουσίαση των πρωτοκόλλων TCP και UDP στα προηγούμενα κεφάλαια, κρίνεται σκόπιμο να παρατεθούν οι βασικές διαφορές μεταξύ τους. Αν και ανήκουν στο ίδιο επίπεδο του μοντέλου TCP/IP, υλοποιούν διαφορετικές προσεγγίσεις ως προς τη μεταφορά των δεδομένων.

Μορφή Επικοινωνίας

- Το **TCP** είναι **συνδεσμικό** (connection-oriented). Πριν από οποιαδήποτε μεταφορά δεδομένων, απαιτείται εγκαθίδρυση σύνδεσης μέσω της διαδικασίας *three-way handshake*.

- Το **UDP** είναι **ασυνδεσμικό** (connectionless). Τα πακέτα στέλνονται χωρίς προηγούμενη συνεννόηση μεταξύ αποστολέα και παραλήπτη.

Αξιοπιστία

- Το **TCP** εξασφαλίζει **αξιόπιστη μεταφορά**: ελέγχει την ακεραιότητα, την ακολουθία και την παράδοση των δεδομένων μέσω αριθμών ακολουθίας, επιβεβαιώσεων (ACKs), και επανεκπομπών.
- Το **UDP δεν παρέχει μηχανισμούς επιβεβαίωσης ή επαναμετάδοσης**. Η αξιοπιστία επαφίεται στην εφαρμογή.

Ταχύτητα και Απόδοση

- Το **TCP** είναι **πιο βαρύ**, λόγω των μηχανισμών αξιοπιστίας, αλλά κατάλληλο για εφαρμογές που απαιτούν πλήρη και σωστή παράδοση, όπως το HTTP, FTP και email.
- Το **UDP** είναι **ταχύτερο**, με ελάχιστη καθυστέρηση και μικρότερη επικεφαλίδα (8 bytes), γεγονός που το καθιστά ιδανικό για εφαρμογές πραγματικού χρόνου όπως video streaming, VoIP και online gaming.

Έλεγχος Ροής και Συμφόρησης

- Το **TCP** ενσωματώνει **έλεγχο ροής** και **έλεγχο συμφόρησης**, για σταθερή απόδοση και προστασία του δικτύου.
- Το **UDP δεν έχει τέτοιους μηχανισμούς**, στέλνει δεδομένα χωρίς να λαμβάνει υπόψη την κατάσταση του δικτύου ή του παραλήπτη.

Κατάλληλες Εφαρμογές

- Το **TCP** χρησιμοποιείται για εφαρμογές που απαιτούν **υψηλή αξιοπιστία και ακρίβεια**: περιήγηση στο web (HTTP/HTTPS), μεταφορά αρχείων (FTP), email (SMTP).
- Το **UDP** προτιμάται σε εφαρμογές όπου η **καθυστέρηση είναι κρίσιμη και η απώλεια πακέτων είναι ανεκτή**: DNS, VoIP, video conferencing, gaming.

4.7 IP (Επίπεδο Δικτύου)

Το **Πρωτόκολλο Διαδικτύου (IP)** [14] είναι η μέθοδος για την αποστολή δεδομένων από τη μια συσκευή στην άλλη μέσω του Διαδικτύου. Κάθε συσκευή έχει μια διεύθυνση IP που την προσδιορίζει μοναδικά και της επιτρέπει να επικοινωνεί και να ανταλλάσσει δεδομένα με άλλες συσκευές που είναι συνδεδεμένες στο Διαδίκτυο. Θεωρείται το πρότυπο για γρήγορη και ασφαλή επικοινωνία απευθείας μεταξύ κινητών συσκευών.

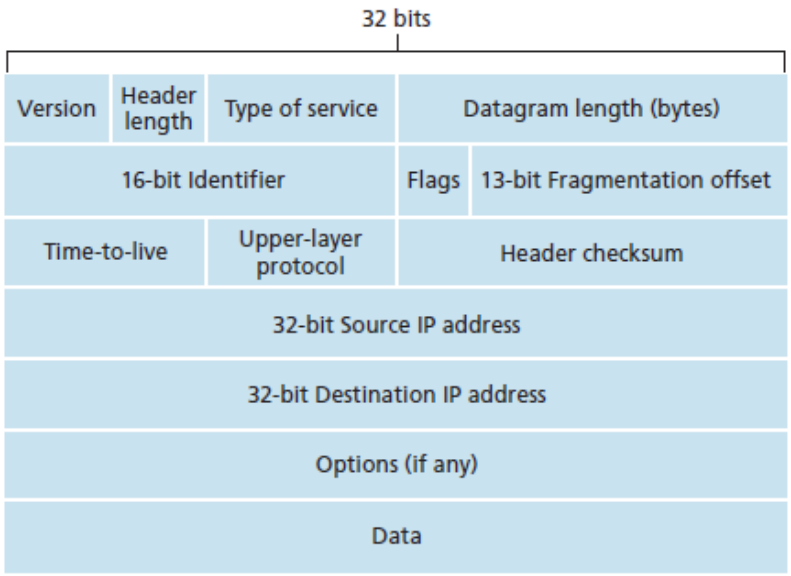
Η IP είναι υπεύθυνη για τον καθορισμό του τρόπου με τον οποίο οι εφαρμογές και οι συσκευές ανταλλάσσουν πακέτα δεδομένων μεταξύ τους. Είναι το κύριο πρωτόκολλο επικοινωνίας που είναι υπεύθυνο για τις μορφές και τους κανόνες για την ανταλλαγή δεδομένων και μηνυμάτων μεταξύ υπολογιστών σε ένα μόνο δίκτυο ή σε πολλά δίκτυα συνδεδεμένα στο Διαδίκτυο. Αυτό το κάνει μέσω του TCP/IP Suite, μιας ομάδας πρωτοκόλλων επικοινωνίας που χωρίζονται σε τέσσερα επίπεδα αφαίρεσης.

Το IP είναι το κύριο πρωτόκολλο στο επίπεδο Δικτύου του TCP/IP. Ο κύριος σκοπός του είναι να παραδίδει πακέτα δεδομένων μεταξύ της εφαρμογής πηγής ή της συσκευής και του προορισμού χρησιμοποιώντας μεθόδους και δομές που τοποθετούν ετικέτες, όπως πληροφορίες διεύθυνσης, μέσα σε πακέτα δεδομένων.

4.7.1 Δεδομενόγραμμα IPv4 (Datagram IPv4)

Το δεδομενόγραμμα IPv4 είναι ένα πακέτο επιπέδου δικτύου, στο οποίο ενθυλακόνεται το πακέτο του ανωτέρου επιπέδου, δηλαδή όταν το πακέτο του ανωτέρου επιπέδου φτάσει στο επίπεδο δικτύου, μπαίνει η επικεφαλίδα του πρωτοκόλλου IP από μπροστά η οποία παρέχει τις βασικές πληροφορίες που χρειάζονται οι συσκευές του διαδικτύου για να κατευθύνουν το πακέτο προς τον προορισμό του. Η κεφαλίδα του δεδομενογράμματος IPv4 αποτελείται από 20 έως 60 bytes και η μορφή του δεδομενογράμματος είναι η εξής:

1. **Έκδοση (4 bits):** Υποδηλώνει την έκδοση του IP που χρησιμοποιήται (IPv4 ή IPv6).
2. **(4 bits):** Με αυτή τη τιμή ο παραλήπτης αντιλαμβάνετε που ακριβώς ξεκινάνε τα δεδομένα καθώς το μέγεθος της κεφαλίδας μεταβάλεται ανάλογα με το αν το πεδίο επιλογών είναι κενό ή όχι.
3. **Τύπος υπηρεσίας (TOS – type of service) (8 bits):** Υποδηλώνει το πόσο σημαντικό είναι το πακέτο και τη προτεραιότητα του.
4. **Μήκος δεδομενογράμματος (16 bits):** Το συνολικό μέγεθος του δεδομενογράμματος σε bytes.
5. **Ταυτότητα (16 bits):** Βοηθάει στην αναγνώριση του πακέτου όταν αυτό κόβεται σε μικρότερα τμήματα (Κατάτμηση).
6. **Σημαίες (3 bits):** Ρυθμίσεις σχετικά με την κατάτμηση.
7. **Μετατόπηση κατάτμησης (13 bits):** Υποδηλώνει τη θέση ενός τμήματος μέσα στο αρχικό δεδομενόγραμμα.
8. **Διάρκεια ζωής (8 bits):** Αυτό το πεδίο είναι ένας μετρητής ο οποίος μειώνεται κατά ένα κάθε φορά που περνάει από έναν δρομολογητή και όταν μηδενίσει απορρίπτεται έτσι ώστε να μην υπάρχει περίπτωση να κυκλωφορεί για πάντα στο διαδίκτυο.
9. **Πρωτόκολλο (8 bits):** Αυτό το πεδίο δηλώνει σε ποιό πρωτόκολλο μεταφοράς ανήκουν τα δεδομένα.
10. **Άθροισμα ελέγχου (16 bits):** Ένας αριθμός ελέγχου για τον εντοπισμό τυχόν αλλοίωσης στην επικεφαλίδα. Σε περίπτωση που εντοπιστεί σφάλμα ο δρομολογητής απορρίπτει το δεδομενόγραμμα.
11. **Διεύθυνση προέλευσης (32 bits):** Η διεύθυνση **αποστολέα** του δεδομενογράμματος.
12. **Διεύθυνση παραλήπτη (32 bits):** Η διεύθυνση **παραλήπτη** του δεδομενογράμματος.
13. **Επιλογές (μεταβλητού μήκους – αν υπάρχουν):** Επιπλέον πληροφορίες για ειδικές περιπτώσεις.
14. **Δεδομένα:** Περιέχει το τμήμα που ενθυλακώνεται στο δεδομενόγραμμα.



Σχήμα 4.7: IPv4 Datagram

4.7.2 Διεύθυνση IPv4

Μια διεύθυνση IP βοηθά τις συσκευές να αναγνωρίζουν η μία την άλλη μέσα στο δίκτυο. Μια διεύθυνση IP δεν είναι τυχαία. Η δημιουργία μιας διεύθυνσης IP έχει τη βάση των μαθηματικών. Το Internet Assigned Numbers Authority (IANA) εκχωρεί τη διεύθυνση IP και τη δημιουργία της. Όπως αναφέρθηκε προηγουμένος, αποτελείται από 32 bits και το πλήρες εύρος της μπορεί να κυμαίνεται από 0.0.0.0 έως 255.255.255.255. Με τη μαθηματική αντιστοίχιση μιας διεύθυνσης IP, μπορεί να γίνει η μοναδική αναγνώριση για να πραγματοποιηθεί μια σύνδεση με έναν προορισμό.

Η IPv4 διεύθυνση χωρίζεται σε δύο μέρη:

- **Το τμήμα του δικτύου (network part):** Προσδιορίζει σε ποιο δίκτυο ανήκει η συσκευή.
- **Το τμήμα του host (host part):** Προσδιορίζει ποια συγκεκριμένη συσκευή (υπολογιστής, εκτυπωτής, κλπ.) είναι μέσα στο δίκτυο αυτό.

Ο διαχωρισμός γίνεται με τη χρήση της **μάσκας υποδικτύου (subnet mask),** η οποία δείχνει ποιά bits στη διεύθυνση στη διεύθυνση του host αντιστοιχούν στο δίκτυο και ποιά στον host. Για παράδειγμα, έστω ότι:

- IP: 192.168.1.0
- Subnet mask: 255.255.255.0

τότε τα πρώτα 24 bits της IP αντιστοιχούν στο δίκτυο και τα 8 τελευταία είναι ελεύθερα να δωθούν στους hosts του δικτύου.

4.7.3 IPv6

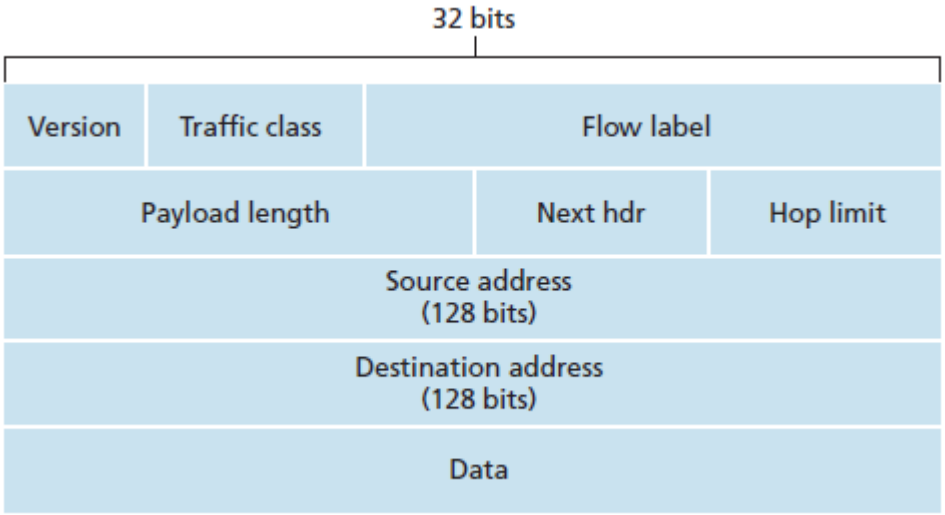
Η συνεχής ανάπτυξη του Διαδικτύου έφερε μαζί και την ανάγκη για περισσότερες διευθύνσεις. Το IPv4 υποστιρίζει 2^32 (4.294.967.296) διεθύνεσεις οι οποίες με τον καιρό άρχισαν να καλύπτονται. Για τη λύση αυτού του προβλήματος δημιουργήθηκε το **IPv6**.

Το **IPv6** [15] χρησιμοποιεί 128 bits στις διευθύνσεις του, που σημαίνει ότι υποστιρίζει 2^128, ένας αριθμός που στα σημερινά δεδομένα είναι σχεδόν απίθανο να καλυφθεί.

Η **κεφαλίδα του IPv6** αποτελείται από 40 bytes εκ των οποίων τα 32 bytes είναι οι διευθύνσεις του αποστολέα και του παραλήπτη. Η μορφή της είναι η εξής:

1. **Έκδοση (4 bits):** Υποδηλώνει την έκδοση του IP που χρησιμοποιήται.
2. **Κλάση κίνησης (8 bits):** Χρησιμοποιείται για την κατηγοριοποίηση και για προτεραιότητες μετάδοσης, κάτι αντίστοιχο με το **TOS.**
3. **Ετικέτα ροής (20 bits):** Επιτρέπει στον αποστολέα να επισημάνει πακέτα που ανήκουν στην ίδια ροή (flow) — χρήσιμο για πολυμέσα ή real-time εφαρμογές.
4. **Μήκος ωφέλιμου φορτίου (16 bits):** Ο αριθμός των byte που ακολουθούν μετά την κεφαλίδα.
5. **Επόμενη κεφαλίδα (8 bits):** Προσδιορίζει το πρωτόκολλο στο οποίο θα παραδοθούν τα δεδομένα που κουβαλάει το δεδομενόγραμμα (TCP, UDP κ.α.).
6. **Όριο αλμάτων (8 bits):** Έχει την ίδια λειτουργία με το πεδίο «Διάρκεια ζωής» στο IPv4.
7. **Διεύθυνση προέλευσης (128 bits):** Η διεύθυνση **αποστολέα** του δεδομενογράμματος.
8. **Διεύθυνση παραλήπτη (128 bits):** Η διεύθυνση **παραλήπτη** του δεδομενογράμματος.

Στη συνέχεια, όπως και στο IPv4 ακολουθούν τα δεδομένα.



Σχήμα 4.8: Δεδομενόγραμμα IPv6

4.7.4 Δημόσια και Ιδιωτική διεύθυνση IP

Οι διευθύνσεις IP χωρίζονται σε δύο κατηγορίες, τις **Δημόσιες (Public)** και τις **Ιδιωτικές (Private)**. Ο λόγος για τον οποίο συμβαίνει αυτό είναι ότι κάθε συσκευή πρέπει να βγαίνει στο διαδίκτυο με μία **μοναδική διεύθυνση** που δεν μπορεί να υπάρχει σε καμία άλλη. Καθώς όμως εξαντλούνται οι διευθύνσεις έπρεπε να αντιμετωπιστεί αυτό το πρόβλημα. Έτσι κάποιες διευθύνσεις χαρακτηρίστηκαν ως ιδιωτικές και χρησιμοποιούνται στους hosts των τοπικών δικτύων. Από την άλλη μεριά, οι δημόσιες διευθύνσεις μοιράζονται από **τους πάροχο υπηρεσιών Διαδικτύου (ISP – Internet Service Provider)** στούς πελάτες και μέσω αυτών μπορεί να επικοινωνίσει μια συσκευή του τοπικού δικτύου με το Διαδίκτυο. Αυτό γίνεται με τη χρήση του πρωτοκκόλου **NAT (Network Address Translation)** το οποίο όπως λέει και το όνομα του, **μεταφράζει – αντιστοιχεί** την ιδιωτική διεύθυνση του host σε μία δημόσια που έχει παραχορηθεί από τον ISP.

Από	Έως
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Πίνακας 4.2: Ιδιωτικές Διευθύνσεις

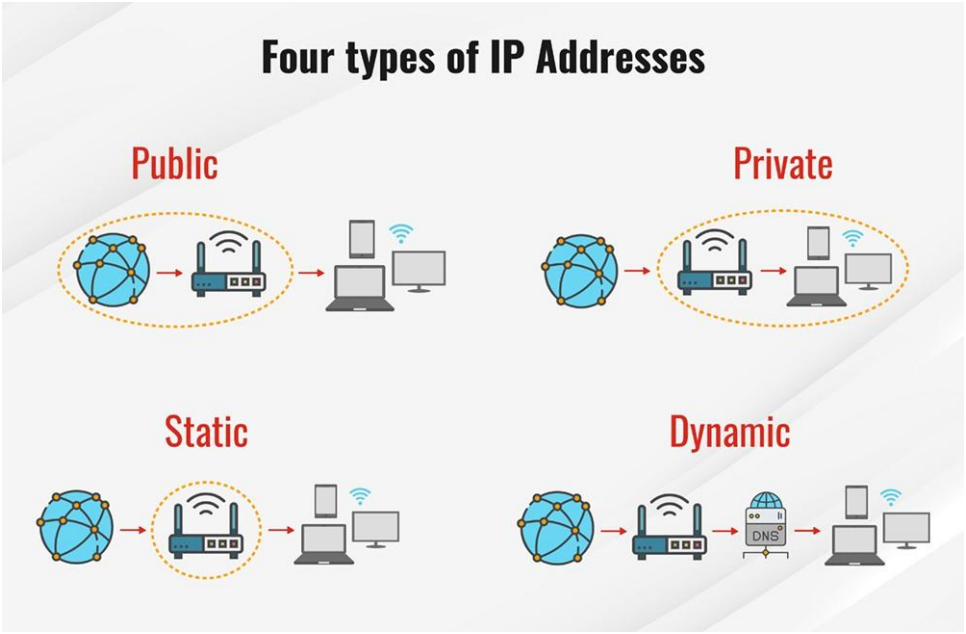
4.7.5 Στατική και Δυναμική Διεύθυνση IP

Μία ακόμη κατηγοροποίηση των διευθύνσεων IP είναι αυτή ανάναμεσα στις **Στατικές διευθύνσεις (Static IP address)** και τις **Δυναμικές διευθύνσεις (Dynamic IP address)**. Μια διεύθυνση IP που ένα άτομο διαμορφώνει και διορθώνει με μη αυτόματο τρόπο σε μία συσκευή στο δίκτυο αναφέρεται ως **στατική διεύθυνση IP**. Βασικοί λόγοι χρήσης της στατικής IP είναι:

- Κάποιος Server ή οποιαδήποτε συσκευή που πρέπει να είναι προσβάσιμη ανά πάσα ώρα και στιγμή και για να γίνει αυτό, η διεύθυνση του πρέπει να είναι σταθερή, καθώς όπως είναι λογικό αν άλλαζε συνεχώς η διεύθυνση του δεν θα την γνώριζαν οι χρήστες.
- Ευκολότερη διαχείριση του δικτύου από τον διαχειριστή του, μπορεί να το διαμορφώσει στα μέτρα του ανάλογα με τις ανάγκες.

Μια δυναμική διεύθυνση IP εκχωρείται αυτόματα σε ένα δίκτυο όταν ρυθμίζεται ένας δρομολογητής. Το πρωτόκολλο DHCP εκχωρεί τη διανομή αυτού του δυναμικού συνόλου διευθύνσεων IP. Το DHCP μπορεί να «τρέχει» στον δρομολογητή του δικτύου σε ένα σπίτι ή έναν οργανισμό. Κάθε φορά που ένας νέος χρήστης συνδέεται στο δίκτυο, του παρέχεται μια διεύθυνση IP από τη δεξαμενή των διαθέσιμων διευθύνσεων IP (που δεν έχουν εκχωρηθεί προς το παρόν) για ένα χρονικό διάστημα **(lease time)** και σε περίπτωση που λήξει ή του παραχωρείται μια νέα διεύθυνση ή ανανεώνει το lease time. Ο βασικός λόγος χρήσης των δυναμικών διευθύνσεων είναι:

- Η **εξοικονώμιση χρόνου**: Ο διαχειριστής του δικτύου δεν χρειάζεται να ασχοληθεί καθόλου με την καταχώρησει διευθύνσεων στους hosts, το αναλαμβάνει εξωλοκλήρου το DHCP.



Σχήμα 4.9: Τύποι IP Διευθύνσεων

4.8 **Πρωτόκολλο ICMP (Επίπεδο Δικτύου)**

Η νούμερο ένα χρήση του **πρωτοκόλλου ICMP** (Internet Control Message Protocol) [16] είναι για την αναφορά σφαλμάτων. Κάθε φορά που δύο συσκευές συνδέονται μέσω του Διαδικτύου, το ICMP μπορεί να χρησιμοποιηθεί για τη δημιουργία σφαλμάτων που μπορούν να μεταβούν από τη συσκευή λήψης στη συσκευή αποστολής, εάν ορισμένα από τα δεδομένα δεν έφτασαν όπως αναμενόταν. Για παράδειγμα, εξαιρετικά μεγάλα πακέτα δεδομένων μπορεί να είναι πολύ μεγάλα για να τα διαχειριστεί ένας δρομολογητής. Σε αυτήν την περίπτωση, ο δρομολογητής θα απορρίψει το πακέτο δεδομένων και θα μεταδώσει ένα μήνυμα ICMP στον αποστολέα που τον ενημερώνει για το πρόβλημα.

Μια άλλη κοινή χρήση του ICMP είναι ως διαγνωστικό εργαλείο για την αξιολόγηση της απόδοσης ενός δικτύου. Τόσο το traceroute όσο και το ping χρησιμοποιούν ICMP. Το Traceroute και το ping είναι μηνύματα που αποστέλλονται σχετικά με το εάν τα δεδομένα μεταδόθηκαν επιτυχώς. Όταν χρησιμοποιείται το traceroute, οι συσκευές από τις οποίες πέρασε ένα πακέτο δεδομένων για να φτάσει στον προορισμό του εμφανίζονται στην αναφορά. Αυτό περιλαμβάνει τους φυσικούς δρομολογητές που χειρίστηκαν τα δεδομένα.

Το traceroute δείχνει πόσος χρόνος χρειάστηκε για να μεταφερθούν τα δεδομένα από τη μια συσκευή στην άλλη. Κάθε φορά που τα δεδομένα περνούν μεταξύ των δρομολογητών, το ταξίδι αναφέρεται ως hop. Οι πληροφορίες που αποκαλύπτονται από το traceroute μπορούν να χρησιμοποιηθούν για να καταλάβουμε ποιες συσκευές κατά μήκος της διαδρομής προκαλούν καθυστερήσεις.

Ένα ping είναι παρόμοιο με ένα traceroute αλλά πιο απλό. Αναφέρει πόσο χρόνο χρειάζεται για να περάσουν τα δεδομένα μεταξύ δύο σημείων. Το ICMP διευκολύνει το ping δεδομένου ότι το αίτημα ηχούς ICMP και η απάντηση ηχούς χρησιμοποιούνται κατά τη διαδικασία ping.

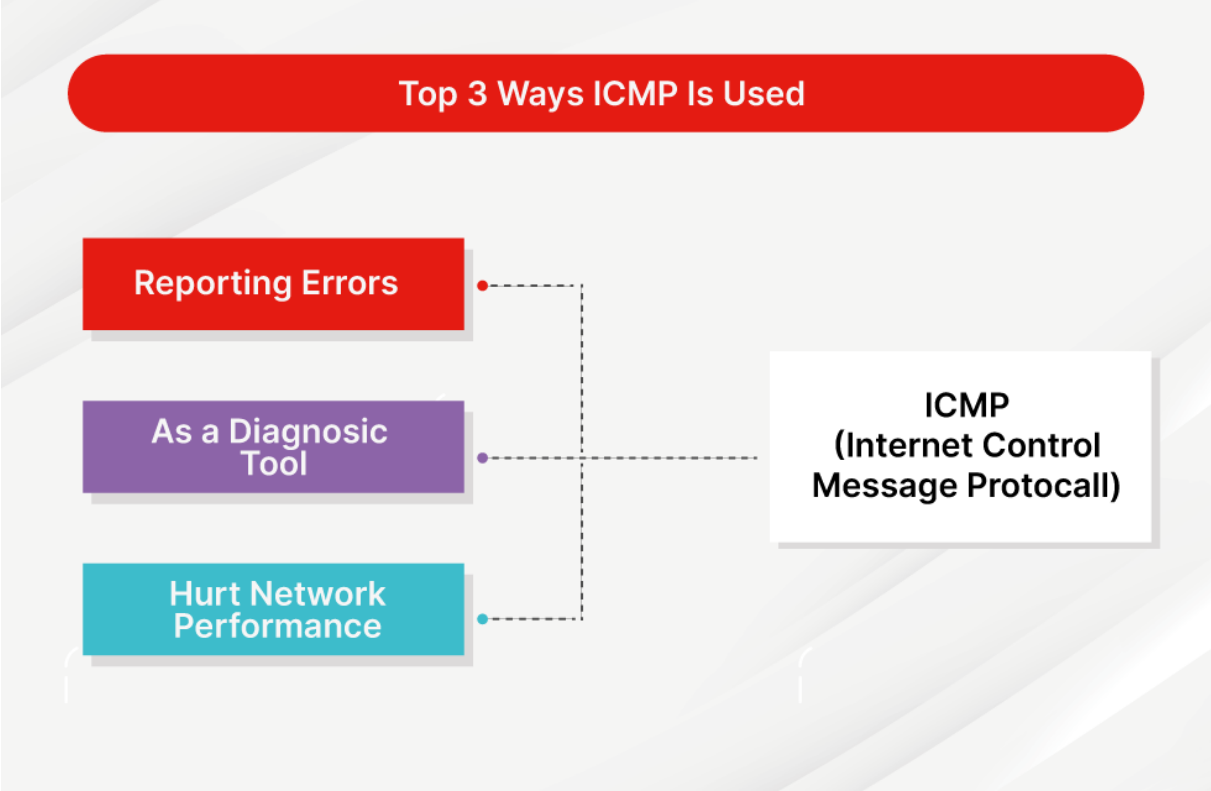
4.8.1 Τρόπος Λειτουργίας ICMP

Το ICMP είναι διαφορετικό από το Πρωτόκολλο Ελέγχου Μετάδοσης (TCP) ή το Πρωτόκολλο Δεδομένων Χρήστη (UDP). Ως αποτέλεσμα, δεν χρειάζεται να συνδεθεί μια συσκευή με μια άλλη πριν από την αποστολή μηνύματος ICMP.

Για παράδειγμα, στο TCP, οι δύο συσκευές που επικοινωνούν πρώτα πραγματοποιούν μια χειραψία που απαιτεί πολλά βήματα. Μετά την ολοκλήρωση της χειραψίας, τα δεδομένα μπορούν να μεταφερθούν από τον αποστολέα στον παραλήπτη. Αυτές οι πληροφορίες μπορούν να παρατηρηθούν χρησιμοποιώντας ένα εργαλείο όπως το tcpdump.

Το ICMP είναι διαφορετικό. Δεν δημιουργείται σύνδεση. Το μήνυμα απλά αποστέλλεται. Επίσης, σε αντίθεση με το TCP και το UDP, που υπαγορεύουν τις θύρες στις οποίες αποστέλλονται οι

πληροφορίες, δεν υπάρχει τίποτα στο μήνυμα ICMP που να τις κατευθύνει σε μια συγκεκριμένη θύρα της συσκευής που θα τις λάβει.



Σχήμα 4.10: ICMP Applications

4.9 Address Resolution Protocol (Επίπεδο Ζεύξης)

Στο επίπεδο ζεύξης οι συσκευές χρησιμοποιούν **διευθύνσεις MAC (Media Access Control)**, ενώ στο επίπεδο δικτύου χρησιμοποιούν **IP address.** Για να μπορέσει μία συσκευή να στείλει δεδομένα σε μια άλλη, θα πρέπει να γίνει η αντιστοίχηση αυτών των δύο. Το ρόλο αυτό αναλαμβάνει το πρωτόκολλο **ARP** [17].

4.9.1 Mac Address

Η **MAC address** είναι ένας **μοναδικός αριθμός** που αντιστοιχεί σε κάθε κάρτα δικτύου (NIC) μιας συσκευής. Είναι για μια **φυσική διεύθυνση** που εκχωρείται από τον κατασκευαστή της NIC και έχει σταθερό μήκος 48 bits. Συνήθως γράφεται σε μορφή έξι ζευγών δεκαεξαδικών ψηφίων, π.χ.: 2F:A8:E9:C3:D1:7B. Η MAC address χρησιμοποιείται για να αναγνωρίζονται οι συσκευές **μέσα στο τοπικό δίκτυο**. Δηλαδή, η IP δείχνει ποιόν θέλει να βρεί κάποιος στον διαδίκτυο, η MAC λέει ποια συσκευή είναι ποιά μέσα στο τοπικό δίκτυο (π.χ. σε ένα σπίτι ή γραφείο).

4.9.2 Λειτουργία ARP

Όταν ένας νέος υπολογιστής ενταχθεί σε ένα τοπικό δίκτυο (LAN), θα λάβει μια μοναδική διεύθυνση IP για χρήση, για αναγνώριση και επικοινωνία. Τα πακέτα δεδομένων φτάνουν σε μια πύλη, που προορίζεται για μια συγκεκριμένη μηχανή υποδοχής. Η πύλη ή το κομμάτι υλικού σε ένα δίκτυο που επιτρέπει τη ροή δεδομένων από το ένα δίκτυο στο άλλο, ζητά από το πρόγραμμα ARP να βρει μια διεύθυνση MAC που ταιριάζει με τη διεύθυνση IP. Η κρυφή μνήμη ARP διατηρεί μια λίστα με κάθε διεύθυνση IP και την αντίστοιχη διεύθυνση MAC της.

Η κρυφή μνήμη ARP είναι δυναμική, αλλά οι χρήστες σε ένα δίκτυο μπορούν επίσης να διαμορφώσουν έναν στατικό πίνακα ARP που περιέχει διευθύνσεις IP και διευθύνσεις MAC. Οι κρυφές μνήμες ARP διατηρούνται σε όλα τα λειτουργικά συστήματα σε ένα δίκτυο Ethernet IPv4. Κάθε φορά που μια συσκευή ζητά μια διεύθυνση MAC για να στείλει δεδομένα σε μια άλλη συσκευή που είναι συνδεδεμένη στο LAN, η συσκευή επαληθεύει την προσωρινή μνήμη ARP για να δει εάν η σύνδεση IP σε MAC διεύθυνσης έχει ήδη ολοκληρωθεί. Εάν υπάρχει, τότε ένα νέο αίτημα δεν είναι απαραίτητο.

Ωστόσο, εάν η μετάφραση δεν έχει ακόμη πραγματοποιηθεί, τότε αποστέλλεται το αίτημα για διευθύνσεις δικτύου και εκτελείται το ARP. Το μέγεθος της κρυφής μνήμης ARP περιορίζεται από το σχεδιασμό και οι διευθύνσεις τείνουν να παραμένουν στην κρυφή μνήμη μόνο για λίγα λεπτά. Καθαρίζεται τακτικά για να ελευθερωθεί χώρος. Αυτός ο σχεδιασμός προορίζεται επίσης για το απόρρητο και την ασφάλεια για την αποτροπή κλοπής ή πλαστογράφησης διευθύνσεων IP από κυβερνοεπιτιθέμενους. Ενώ οι διευθύνσεις MAC είναι σταθερές, οι διευθύνσεις IP ενημερώνονται συνεχώς.

Κατά τη διαδικασία εκκαθάρισης, οι μη χρησιμοποιημένες διευθύνσεις διαγράφονται. Το ίδιο ισχύει και για τυχόν δεδομένα που σχετίζονται με ανεπιτυχείς προσπάθειες επικοινωνίας με υπολογιστές που δεν είναι συνδεδεμένοι στο δίκτυο ή που δεν είναι καν ενεργοποιημένοι.

4.9.3 Τύποι ARP

Υπάρχουν διαφορετικές εκδόσεις και περιπτώσεις χρήσης του ARP.

Proxy ARP: Το ARP μεσολάβησης είναι μια τεχνική με την οποία μια συσκευή διακομιστή μεσολάβησης σε ένα δεδομένο δίκτυο απαντά στο αίτημα ARP για μια διεύθυνση IP που δεν βρίσκεται σε αυτό το δίκτυο. Ο διακομιστής μεσολάβησης γνωρίζει την τοποθεσία του προορισμού της κυκλοφορίας και προσφέρει τη δική του διεύθυνση MAC ως προορισμό.

Gratuitous ARP: Το δωρεάν ARP είναι σχεδόν σαν μια διοικητική διαδικασία, που πραγματοποιείται ως ένας τρόπος για έναν κεντρικό υπολογιστή σε ένα δίκτυο να ανακοινώνει ή να ενημερώνει απλώς τη διεύθυνση IP-to-MAC του. Το δωρεάν ARP δεν ζητείται από ένα αίτημα ARP για τη μετάφραση μιας διεύθυνσης IP σε μια διεύθυνση MAC.

Reverse ARP (RARP): Οι κεντρικές μηχανές που δεν γνωρίζουν τη δική τους διεύθυνση IP μπορούν να χρησιμοποιήσουν το Πρωτόκολλο Ανάλυσης Αντίστροφης Διεύθυνσης (RARP) για ανακάλυψη.

4.10 Επίλογος

Σε αυτό το κεφάλαιο εξετάστηκαν τα βασικότερα πρωτόκολλα που αποτελούν τον πυρήνα της επικοινωνίας στο Διαδίκτυο. Κάθε ένα από αυτά εξυπηρετεί έναν συγκεκριμένο ρόλο μέσα στην πολύπλοκη διαδικασία μεταφοράς και διαχείρισης δεδομένων, από τη στιγμή που ένας χρήστης εισάγει μια διεύθυνση στον φυλλομετρητή του, μέχρι την τελική εμφάνιση του περιεχομένου στην οθόνη του.

Το **HTTP** αναλύθηκε ως το βασικό πρωτόκολλο που διέπει τη μεταφορά ιστοσελίδων και περιεχομένου από web servers σε πελάτες. Το **DNS** εξηγεί τον τρόπο με τον οποίο οι συμβολικές διευθύνσεις αντιστοιχίζονται σε αριθμητικές IP διευθύνσεις. Το **DHCP** παρουσιάστηκε ως η αυτόματη μέθοδος εκχώρησης IP διευθύνσεων σε συσκευές, εξασφαλίζοντας σύνδεσή τους στο δίκτυο.

Στο επίπεδο μεταφοράς, το **TCP** και το **UDP** έδειξαν δύο διαφορετικές προσεγγίσεις στη μεταφορά δεδομένων: το TCP με έμφαση στην αξιοπιστία και τη διαχείριση ροής, και το UDP με έμφαση στην ταχύτητα και την απλότητα. Το **IP**, ως βασικό πρωτόκολλο του επιπέδου δικτύου, αποτελεί το μέσο

δρομολόγησης των πακέτων από άκρο σε άκρο,το ICMP ως ένα διαγνωστικό εργαλείο και αναφοράς σφαλμάτων, ενώ το **ARP** εξασφαλίζει την αντιστοίχιση μεταξύ των IP διευθύνσεων και των MAC διευθύνσεων στο τοπικό δίκτυο.

Όλα μαζί συνεργάζονται με αποδοτικό τρόπο για να επιτυγχάνεται η σωστή λειτουργία του δικτύου και κατ' επέκταση του Διαδικτύου.

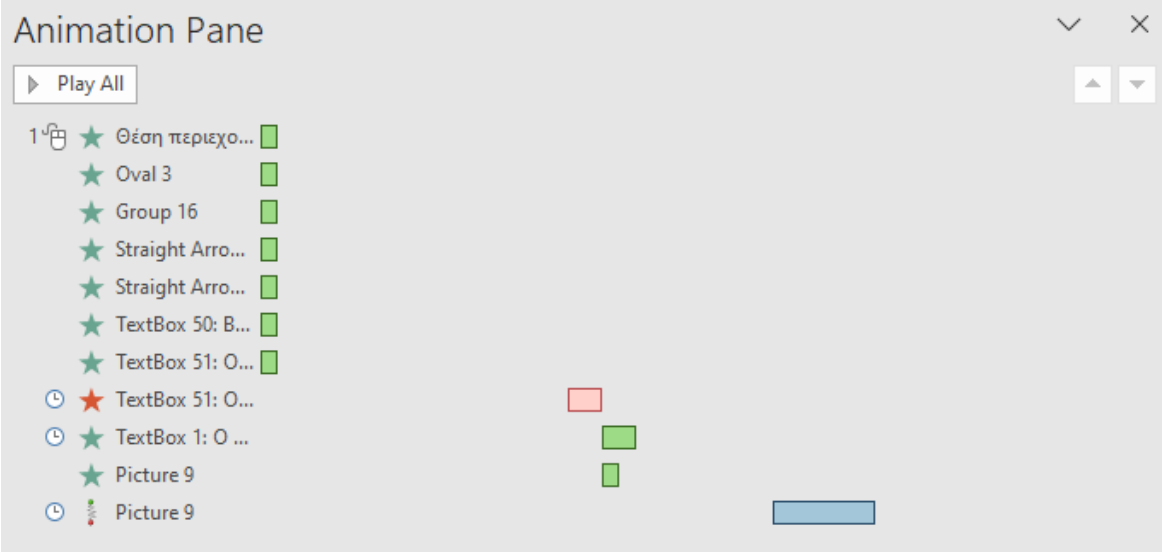
Κεφάλαιο 5ο: Οπτικοποίηση αιτήσεων

5.1 Εισαγωγή

Σε αυτήν την ενότητα περιγράφεται το πρακτικό κομμάτι της πτυχιακής. Πιο συγκεκριμένα δημιουργήθηκε μια σειρά από βίντεο, όπου παρουσιάζονται όλα τα βήματα για την οπτικοποίηση των αιτήσεων και αποκρίσεων της σουίτας πρωτοκόλλων TCP/IP. Ως στόχο έχει την καλύτερη κατανόηση των διαδικασιών που εκτελούνται στο παρασκήνιο έτσι ώστε να ολοκληρωθεί μια φαινομενικά απλή διαδικασία όπως είναι η εμφάνιση μιας ιστοσελίδας.

5.2 Εργαλείο ανάπτυξης γραφικών στοιχείων

Για την υλοποίηση του πρακτικού μέρους της εργασίας επιλέχθηκε το **Microsoft PowerPoint** ως βασικό εργαλείο δημιουργίας των γραφικών στοιχείων και animations. Το PowerPoint έχει ένα ευέλικτο περιβάλλον παρουσίασης, το οποίο επιτρέπει την αναπαράσταση της ροής με διαδοχικά καρέ και χρονικά συγχρονισμένες κινήσεις.



Σχήμα 5.1: Animation Pane

Βασικοί λόγοι επιλογής του PowerPoint:

- Δημιουργία σχημάτων και αντικειμένων
- **Χρήση animations** για την κίνηση των πακέτων στο δίκτυο.
- **Χρονοπρογραμματισμός (timing)** των κινήσεων ώστε να παρουσιάζεται η λογική σειρά των βημάτων.
- **Προσθήκη επεξηγηματικών κειμένων**, ώστε να είναι σαφής η λειτουργία κάθε βήματος.
- Δυνατότητα εξαγωγής του τελικού αποτελέσματος σε **μορφή βίντεο (.MP4).**

5.3 Σουίτα Πρωτοκόλλων TCP/IP – Επίπεδα & Πρωτόκολλα

Επίπεδο Εφαρμογής (Application Layer)

➤ Πρωτόκολλα: HTTP, HTTPS, FTP, SMTP, DNS, κ.ά.

➤ Παρέχει διεπαφή για τις εφαρμογές.

Επίπεδο Μεταφοράς (Transport Layer)

➤ Πρωτόκολλα: TCP, UDP

➤ Εγγυάται αξιόπιστη μεταφορά (TCP) ή γρήγορη χωρίς εγγύηση (UDP).

Επίπεδο Δικτύου/Διαδικτύου (Internet Layer)

➤ Πρωτόκολλο: IP (IPv4/IPv6)

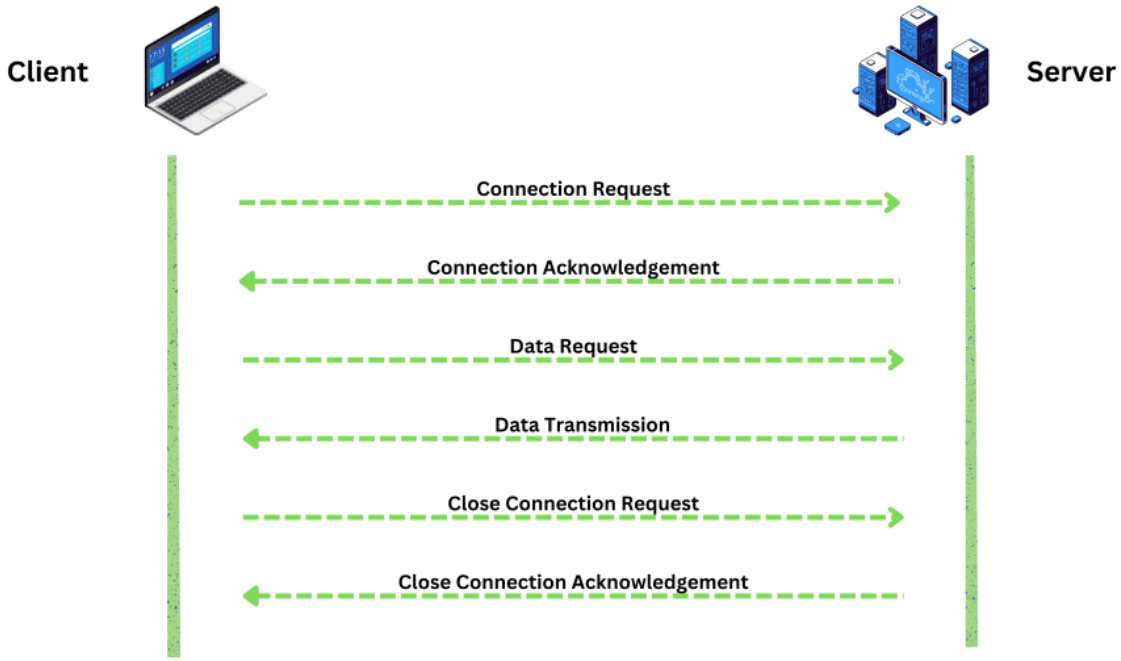
➤ Διαχείριση δρομολόγησης πακέτων.

Σύνδεσης Δεδομένων (Link Layer)

➤ Π.χ. Ethernet, Wi-Fi

➤ Ανταλλαγή δεδομένων μεταξύ συσκευών στο ίδιο δίκτυο.

Στην παρακάτω επικοινωνία παρουσιάζεται παράδειγμα client-server επικοινωνίας.



Σχήμα 5.2: Επικοινωνία Client Server

Παράδειγμα Οπτικοποίησης: Αίτηση HTTP μέσω TCP/IP

Χρήστης ανοίγει έναν browser και πληκτρολογεί www.example.com

[Application Layer - HTTP]

Client: GET /index.html HTTP/1.1

Server: HTTP/1.1 200 OK (αποστολή της σελίδα)

[Transport Layer - TCP]

Client: SYN → Server

Server: SYN-ACK → Client

Client: ACK → Server → (Εγκαθίδρυση σύνδεσης)

Μετά μεταφέρεται το HTTP request/response

[Internet Layer - IP]

Το πακέτο αποκτά IP headers και δρομολογείται προς το server

[Link Layer - Ethernet/WiFi]

Πακέτο φεύγει από την κάρτα δικτύου με MAC διευθύνσεις

Επίπεδο	**Πρωτόκολλα**	**Περιγραφή**
Εφαρμογής	HTTP, DNS	HTTP request/response, DNS για όνομα σε IP
Μεταφοράς	TCP	Εγγυάται τη σωστή παράδοση των πακέτων
Διαδικτύου	IP	Μεταφορά πακέτων μέσω IP διευθύνσεων
Σύνδεσης Δεδομένων	Ethernet/Wi-Fi, ARP	MAC διευθύνσεις, ARP για εύρεση gateway

Πίνακας 5.1: Αίτηση HTTP μέσω TCP/IP

‘Όπως περιγράφεται στον παραπάνω πίνακα στο Ε**πίπεδο Σύνδεσης**

ARP – Address Resolution Protocol (Επίπεδο Σύνδεσης Δεδομένων)

ARP Request

Ο client δεν γνωρίζει τη MAC διεύθυνση του server ή της default gateway.

Στέλνει broadcast αίτημα στο τοπικό δίκτυο:

"Ποιος έχει τη διεύθυνση IP X; Στείλε μου τη MAC σου!"

ARP Reply

Ο server (ή το router) απαντά με τη MAC διεύθυνσή του.

Πλέον, ο client μπορεί να στείλει Ethernet frame προς αυτόν.

Στη συνέχεια στο **Επίπεδο Εφαρμογής**

DNS – Domain Name System (Επίπεδο Εφαρμογής μέσω UDP)

DNS Request

Ο client στέλνει αίτηση στο DNS server για να μετατρέψει το fi.ps.ihu.gr σε IP.

DNS Response

Ο DNS server απαντά με την αντίστοιχη IP διεύθυνση του domain.

TCP – Transmission Control Protocol (**Επίπεδο Μεταφοράς)**

TCP SYN

Ο client ξεκινά το 3-way handshake με SYN πακέτο για να δημιουργήσει σύνδεση.

TCP SYN-ACK

Ο server απαντά με SYN-ACK (δέχεται σύνδεση και απαντά πίσω).

TCP ACK

Ο client απαντά με ACK και η σύνδεση είναι έτοιμη για αποστολή δεδομένων.

HTTP – Hypertext Transfer Protocol (**Επίπεδο Εφαρμογής**)

HTTP Request

Ο client στέλνει HTTP αίτημα τύπου GET για μια σελίδα (π.χ. /index.html).

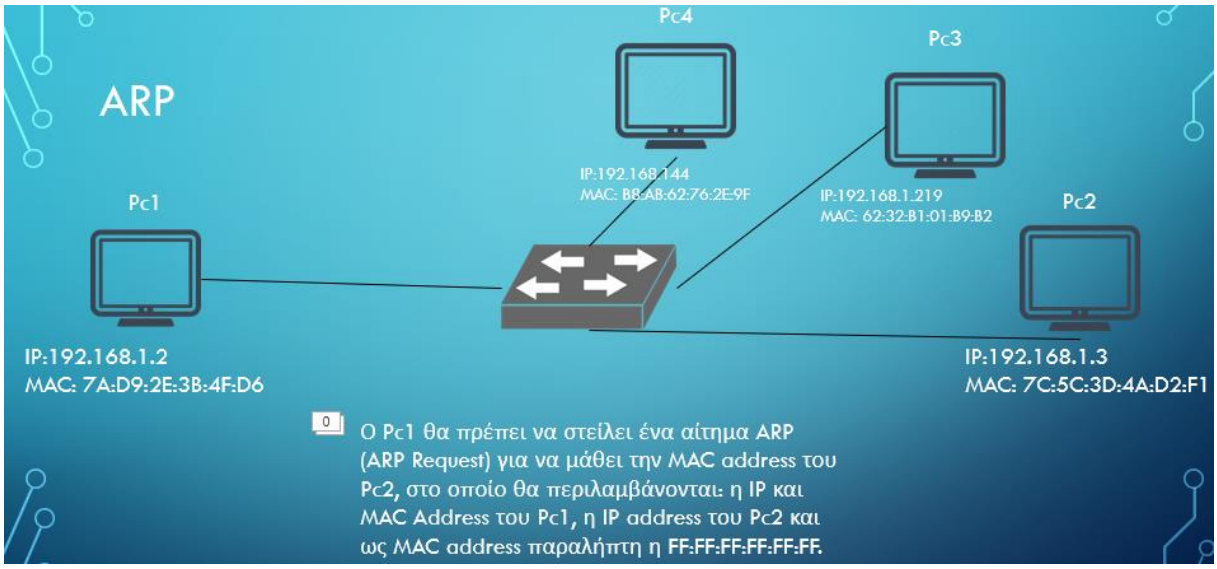
HTTP Response

Ο server απαντά με HTTP/1.1 200 OK και επιστρέφει τα δεδομένα της σελίδας (HTML, CSS, JS κ.λπ.)

5.4 Videos

Σε αυτήν την ενότητα παρουσιάζονται τα videos και οι παρουσιάσεις που αναπτύχθηκαν στα πλαίσια της υλοποίησης της διπλωματικής εργασίας.

5.4.1 Address Resolution Protocol



Σχήμα 5.3: ARP Address Resolution Protocol

Επισυνάπτονται τα αρχεία ARP.pptx & ARP.mp4. Το βίντεο παρουσιάζει τον τρόπο λειτουργίας του πρωτοκόλλου ARP.

Το παράδειγμα που παρουσιάζεται είναι

Παράδειγμα:

Έστω ότι ο **Υπολογιστής Α** θέλει να στείλει δεδομένα στον **Υπολογιστή Β**.

- IP του A: 192.168.1.10
- MAC του A: AA:AA:AA:AA:AA:AA
- IP του B: 192.168.1.20
- MAC του B: 12:AF:EC:4A:35:B1

Βήματα που ακολουθεί το ARP:

1. Ο υπολογιστής Α θέλει να στείλει πακέτο στον 192.168.1.20 αλλά **δεν γνωρίζει τη MAC διεύθυνσή** του.
2. Στέλνει ένα **ARP Request (broadcast)**:

"Ποιος έχει IP 192.168.1.20; απάντησε στο 192.168.1.10!"

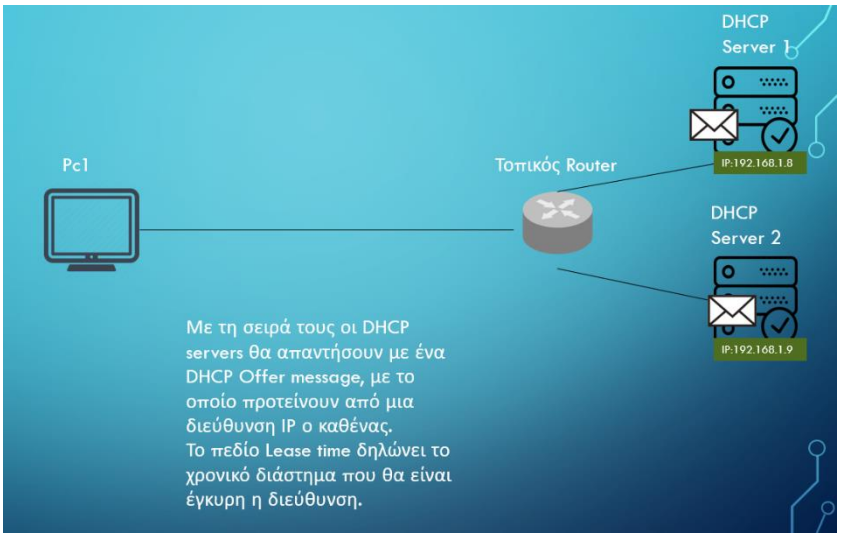
Αυτό το πακέτο φτάνει σε **όλες** τις συσκευές στο LAN.

3. Ο υπολογιστής Β λαμβάνει το αίτημα και απαντά με **ARP Reply (unicast)**:

"Η IP 192.168.1.20 ανήκει σε MAC 12:AF:EC:4A:35:B1"

4. Ο υπολογιστής Α αποθηκεύει τη διεύθυνση MAC στη **ARP cache** και στέλνει το πακέτο απευθείας στον Β.

5.4.2 DHCP Dynamic Host Configuration Protocol



Σχήμα 5.4: DHCP Dynamic Host Configuration Protocol.

Επισυνάπτονται τα αρχεία DHCP.pptx & DHCP.mp4. Το βίντεο παρουσιάζει τον τρόπο λειτουργίας του πρωτοκόλλου DHCP.

Σενάριο :

Έστω ότι ένας νέος υπολογιστής (Pc1) μπαίνει σε ένα δίκτυο και **δεν του έχει δωθεί μία στατική IP**.

Βήματα Επικοινωνίας :

DHCP Discover (Broadcast)
Ο client φωνάζει:

"Υπάρχει κάποιος DHCP Server; Χρειάζομαι IP!"

DHCP Offer (Broadcast)
Ο DHCP1 server απαντά:

"Σου προσφέρω την IP 192.168.1.50, για χρήση για 24 ώρες."

Ο DHCP1 server απαντά:

"Σου προσφέρω την IP 192.168.2.55, για χρήση για 24 ώρες."

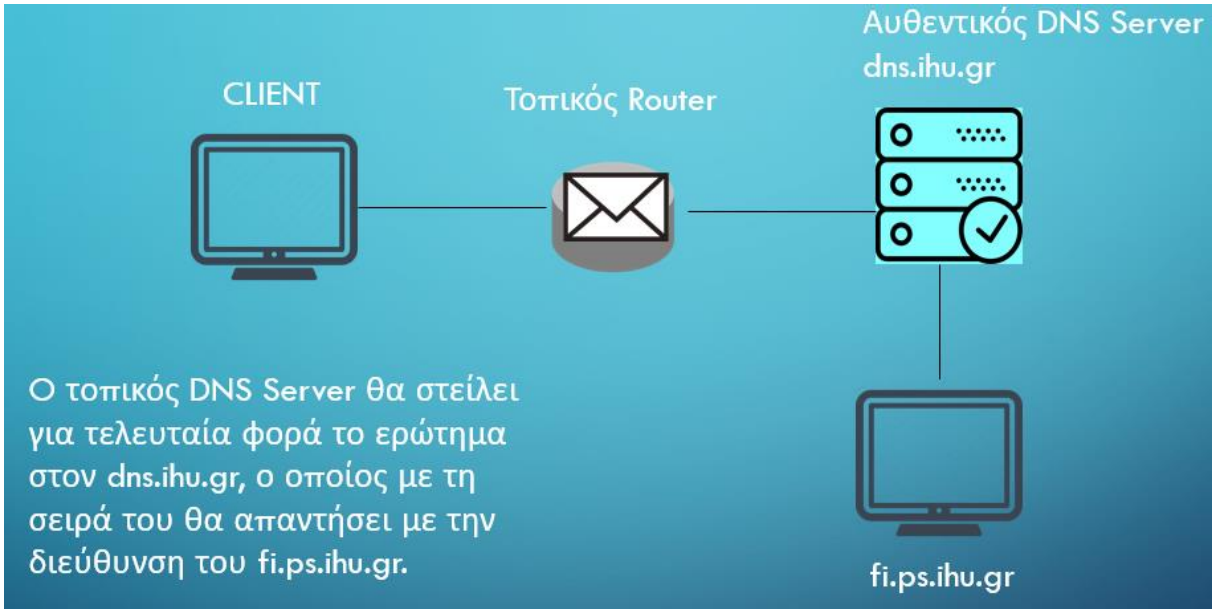
DHCP Request
Ο client απαντά:

"Ναι, αποδέχομαι την IP 192.168.1.50!"

DHCP Acknowledgment (ACK)
Ο server επιβεβαιώνει:

"Η IP 192.168.1.50 είναι δική σου."

5.4.3 DNS Domain Name System



Σχήμα 5.5: DNS Domain Name System

Επισυνάπτονται τα αρχεία DNS.pptx & DNS.mp4. Το βίντεο παρουσιάζει τον τρόπο λειτουργίας του πρωτοκόλλου DNS.

Έστω ότι ο χρήστης ανοίγει τον browser και πληκτρολογεί: **fi.ps.ihu.gr**

Βήματα DNS Αναζήτησης:

Ο υπολογιστής κοιτάζει το τοπικό cache:

- Έχει ξαναεπισκεφτεί το fi.ps.ihu.gr
  Αν ναι, χρησιμοποιεί την IP που είναι ήδη αποθηκευμένη.
- Αν όχι, προχωρά στο επόμενο βήμα.

Ερωτάται ο τοπικός DNS resolver (συνήθως ο router ή ο ISP):

"Ποια είναι η IP για fi.ps.ihu.gr;"

Αν δεν τη γνωρίζει, κάνει ιεραρχική αναζήτηση:

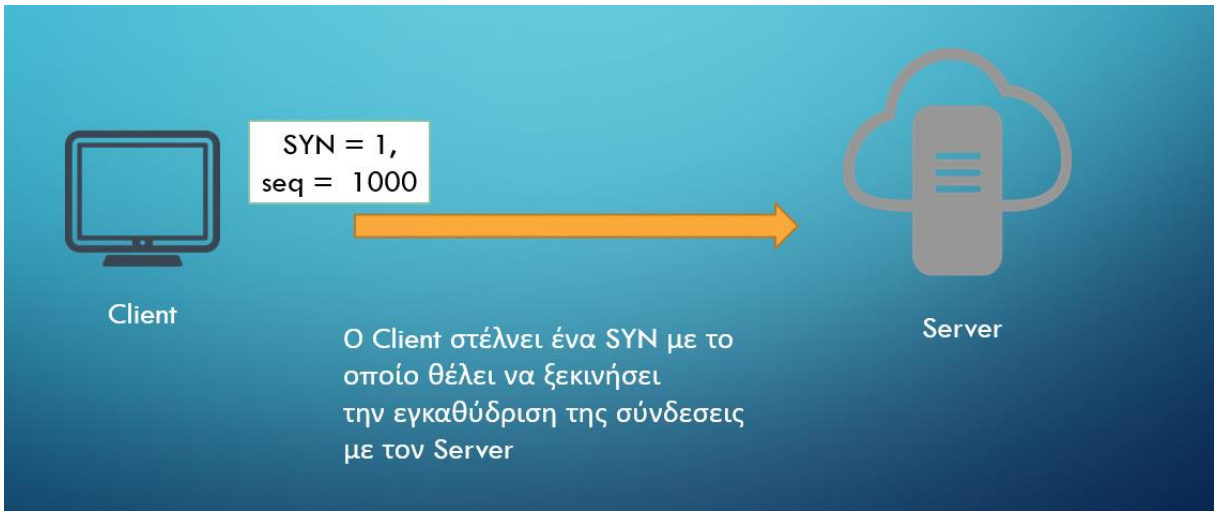
- **Root DNS server** → παραπέμπει σε
- **Top-Level Domain (TLD) DNS server** (.com) → παραπέμπει σε
- **Authoritative DNS server για example.com** → απαντά:

  " fi.ps.ihu.gr = "IP Address"

Η απάντηση επιστρέφει στον υπολογιστή και πλέον μπορεί να συνδεθεί στην IP address που αντιστοιχεί στο όνομα fi.ps.ihu.gr.

Η IP αποθηκεύεται προσωρινά (DNS caching) για επόμενες χρήσεις

5.4.4 TCP Transmission Control Protocol



Σχήμα 5.6: TCP Transmission Control Protocol

Επισυνάπτονται τα αρχεία TCP.pptx & TCP.mp4. Το βίντεο παρουσιάζει τον τρόπο λειτουργίας του πρωτοκόλλου TCP.

Παράδειγμα Σενάριο:

Ο Χρήστης φορτώνει μια ιστοσελίδα (www.example.com)

Βήματα TCP Επικοινωνίας (Τριπλή Χειραψία - Three-way Handshake):

Υπολογιστής Client → Server

SYN → Ο client ξεκινά σύνδεση:

"Θέλω να ξεκινήσουμε TCP σύνδεση. Το αρχικό μου sequence number είναι 1000."

SYN-ACK ← Ο server απαντά:

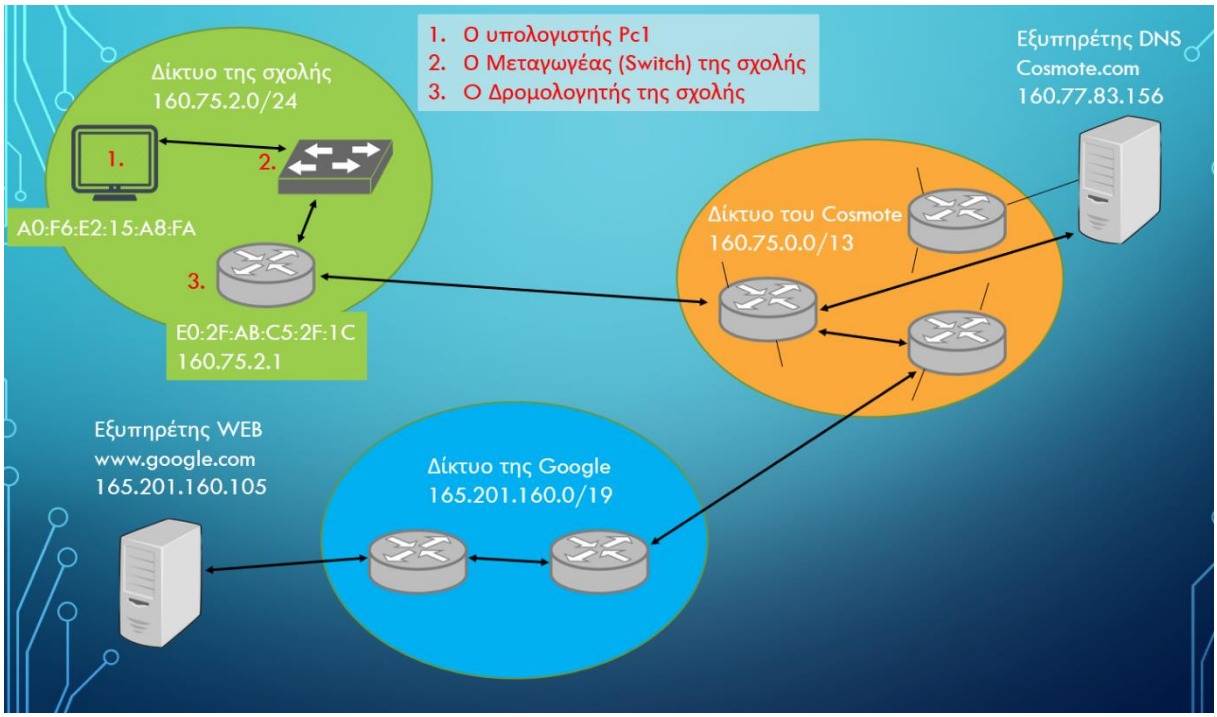
"Δεκτό! Το δικό μου sequence number είναι 2000 και επιβεβαιώνω το δικό σου 1001."

ACK → Ο client επιβεβαιώνει:

"OK, είμαστε έτοιμοι!"

Πλέον η σύνδεση είναι **καθιερωμένη** και μπορεί να ξεκινήσει ανταλλαγή δεδομένων (HTTP Request → Response κ.λπ.).

5.2.5 Ολοκληρωμένο παράδειγμα TCP/IP - HTTP



Σχήμα 5.7: TCP-HTTP οπτικοποίηση αίτησης.

Στο συγκεκριμένο βίντεο απεικονίζεται η πορεία που ακολουθεί μία αίτηση που κάνει ένας χρήστης για μία ιστοσελίδα από την αρχή που θα συνδεθεί στο τοπικό δίκτυο, μέχρι τη στιγμή που θα εμφανιστεί η ιστοσελίδα στην οθόνη του. Ουσιαστικά συνχωνεύονται όλα τα βίντεο σε ένα και παρουσιάζουν μια αρκετά ρεαλιστική κατάσταση ενός συνηθυσμένου αιτήματος Http.

Κεφάλαιο 6ο: Συμπεράσματα ή/και προτάσεις βελτίωσης

Συνοψίζοντας, όταν ένας client επιχειρεί να επισκεφτεί μια ιστοσελίδα, ενεργοποιείται μια ολόκληρη αλυσίδα πρωτοκόλλων και μηχανισμών του διαδικτύου. Αρχικά, μέσω του DHCP για την απόκτηση διεύθυνσης, έπειτα το DNS, το φιλικό όνομα της ιστοσελίδας μετατρέπεται σε μια αριθμητική IP διεύθυνση. Στη συνέχεια, το TCP φροντίζει για την αξιόπιστη σύνδεση μεταξύ client και server. Τέλος, μέσω του HTTP, πραγματοποιείται η πραγματική ανταλλαγή περιεχομένου που καταλήγει στην προβολή της ιστοσελίδας στον browser.

Σε όλη τη διάρκεια του βίντεο, παρακολουθήσαμε μεθοδικά πώς λειτουργεί το διαδίκτυο «πίσω από τα φώτα», όταν ένας χρήστης – δηλαδή ένας client – επιχειρεί να επισκεφτεί μια ιστοσελίδα. Αν και για τον τελικό χρήστη η διαδικασία μοιάζει απλή και άμεση, στην πραγματικότητα ενεργοποιείται μια πολύπλοκη αλλά απόλυτα συντονισμένη σειρά μηχανισμών και πρωτοκόλλων, τα οποία συνεργάζονται για να προσφέρουν την εμπειρία που όλοι γνωρίζουμε και χρησιμοποιούμε καθημερινά.

Ως προς το πρακτικό μέρος της εργασίας μπορεί να εμπλουτιστεί περαιτέρω με την ενσωμάτωση **διαδραστικών στοιχείων**. Για παράδειγμα, θα μπορούσαν να προστεθούν σενάρια στα οποία το DHCP server δεν απαντά ή εμφανίζεται καθυστέρηση στην απόκριση DNS, δίνοντας στον θεατή τη δυνατότητα να αντιληφθεί την πρακτική σημασία των αποκρίσεων των πρωτοκόλλων. Επιπλέον, μπορεί να ενσωματωθεί **αφήγηση** για την ενίσχυση της προσβασιμότητας του υλικού, αλλά και για την υποστήριξη διαφορετικών μαθησιακών προφίλ. Ιδιαίτερη αξία θα είχε επίσης η απεικόνιση πραγματικών πακέτων δεδομένων μέσω εργαλείων όπως το **Wireshark**, με αντίστοιχη απλοποιημένη μεταφορά τους σε animation για καλύτερη κατανόηση της δομής και λειτουργίας των πρωτοκόλλων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.60-66.

[2] H. S. Oluwatosin, "Client-Server model," IOSR Journal of Computer Engineering, vol. 16, no. 1, pp. 57–71, Jan. 2014, doi: 10.9790/0661-16195771. Available: https://doi.org/10.9790/0661-16195771

[3] Χ. Μανιφάβας, Κατανεμημένα συστήματα επικοινωνία - Client/Server. 2012. Available: https://eclass.hmu.gr/modules/document/file.php/TP183/%CE%98%CE%95%CE%A9%CE%A1%CE%99%CE%91/01.%CE%94%CE%B9%CE%B1%CF%86%CE%AC%CE%BD%CE%B5%CE%B9%CE%B5%CF%82/DS-1213E-slides/DS-L9b-05-Client-Server-Model.pdf

[4] P. Duchessi and I. Chengalur-Smith, "Client/server benefits, problems, best practices," Communications of the ACM, vol. 41, no. 5, pp. 87–94, May 1998, doi: 10.1145/274946.274961. Available: https://doi.org/10.1145/274946.274961

[5] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.52-53.

[6] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.345-349.

[7] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.130-139.

[8] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.98-103.

[9] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.110-114.

[10] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.198-204.

[11] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.230-233.

[12] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.250-252.

[13] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.269-277.

[14] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.331-352.

[15] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.356-359.

[16] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.353-355.

[17] Kurose, J. and Ross, K., Computer Networking A Top-Down Approach - Sixth Edition. New Jersey: Pearson Education, 2012, pp.462-469.