

Δίκτυα Υπολογιστών II
Παπαδόπουλος Κωνσταντίνος, Α.Ε.Μ. 8677

Δίκτυα Υπολογιστών II (8ο εξάμηνο)
Experimental Virtual Lab

REPORT

του φοιτητή
Παπαδόπουλου Κωνσταντίνου (8677)

Απρίλιος 2018

Τμήμα Ηλεκτρολόγων Μηχανικών Πολυτεχνική Σχολή ΑΠΘ

Συλλογή μετρήσεων και παρουσίαση αποτελεσμάτων

Ζητούμενα:

[E]

(α)

Σύντομα σχόλια/παρατηρήσεις

Στην εκφώνηση:

- σελ.7, υποσημείωση 5
Διαπιστώνουμε ότι μόνο ο κωδικός σταθμού τηλεμετρήσεων “T00” αποκρίνεται σε αιτήματα αποστολής μετρήσεων θερμοκρασίας.
- σελ.9, υποσημείωση 9 και 10
- Ορισμένες φορές οι συνθήκες επικοινωνίας οδηγούν τον server στη διαπίστωση της ανάγκης επανάληψης του ίδιου πακέτου για περισσότερες από δύο φορές.

Η απώλεια πακέτων οφείλεται είτε σε σφάλματα στη μετάδοση δεδομένων, συνήθως σε ασύρματα δίκτυα είτε σε συμφόρηση δικτύου.

Τα ασύρματα δίκτυα είναι ευάλωτα σε διάφορους παράγοντες που μπορούν να καταστρέψουν ή να χάσουν πακέτα υπό διαμετακόμιση, όπως παρεμβολές ραδιοσυχνοτήτων (RFI), ραδιοσήματα που είναι πολύ αδύναμα εξαιτίας εξασθένησης από την απόσταση ή λόγω πολλαπλών διαδρομών, ελαττωματικού εξοπλισμού δικτύωσης ή ελαττωματικά προγράμματα οδήγησης δικτύου.

Τα ασύρματα δίκτυα μπορούν να αντιμετωπίσουν απώλεια πακέτων που προκαλείται από το “υψηλό ποσοστό σφαλμάτων δυαδικών ψηφίων” (BER), τα χαρακτηριστικά ασταθούς καναλιού και την κινητικότητα των χρηστών.

Η συμφόρηση του δικτύου είναι επίσης αιτία απώλειας πακέτων που μπορεί να επηρεάσει όλους τους τύπους δικτύων. Όταν το περιεχόμενο φθάνει για παρατεταμένο χρονικό διάστημα σε ένα συγκεκριμένο δρομολογητή ή σε ένα τμήμα δικτύου με ρυθμό μεγαλύτερο από ό, τι είναι δυνατόν να αποσταλεί, δεν υπάρχει άλλη επιλογή από το να εγκαταλείψουμε πακέτα.

Το Internet Protocol επιτρέπει στους δρομολογητές να απορρίψουν απλά πακέτα εάν ο δρομολογητής ή ένα τμήμα δικτύου είναι πολύ απασχολημένος για την έγκαιρη παράδοση των δεδομένων ή εάν το πρωτόκολλο ελέγχου IPv4 δείχνει ότι το πακέτο έχει καταστραφεί.

Σε περιπτώσεις όπου η ποιότητα της υπηρεσίας περιορίζει την ταχύτητα μιας σύνδεσης, τα πακέτα ενδέχεται να πέσουν σκόπιμα προκειμένου να επιβραδυνθούν συγκεκριμένες υπηρεσίες για να εξασφαλιστεί το διαθέσιμο εύρος ζώνης για άλλες υπηρεσίες με μεγαλύτερη σημασία (όπως αυτές που χρησιμοποιούνται στον leaky bucket algorithm αλγόριθμο). Για το λόγο αυτό, η απώλεια πακέτων δεν αποτελεί αναγκαστικά ένδειξη κακής αξιοπιστίας σύνδεσης ή σημείων συμφόρησης εύρους ζώνης.

- Γνωρίζουμε ότι η ρυθμαπόδοση (throughput) μπορεί να δοθεί από τη σχέση $R = L / x_{\text{noise}}$. Άρα, όσο μεγαλύτερο L έχουμε τόσο μεγαλύτερη θα είναι και η ταχύτητα μετάδοσης της εικόνας (βέβαια τόσο πιο ευάλωτα είναι ενδεχομένως τα πακέτα στο θόρυβο).

- σελ.11, υποσημείωση 12 και 13

- Μία σημαντική σχέση για το συντελεστή β είναι $d_i = \Delta_i / \beta$. Όταν $\beta > 1$, τότε το Δ_i μεγαλώνει, δηλαδή μεγαλώνει η διαφορά μεταξύ δύο διαδοχικών βημάτων, δίνοντας έτσι πιο “οξύ”, αλλά και πιο “αφύσικο” ήχο (χειρότερης ποιότητας).

- Όταν το βήμα κβάντισης Q γίνει 16, χειροτερεύει η ποιότητα του ήχου.

- σελ.14, υποσημείωση 14

Πραγματοποιήθηκε από τον φοιτητή μία μικρή πειραματική εφαρμογή που δημιουργεί έναν σύνδεσμο TCP προς τη θύρα 80 για τη μελέτη της συμπεριφοράς ενός web sever.

Κατασκευάστηκε επιπλέον ένας Apache HTTP Web Server για την περαιτέρω μελέτη του μοντέλου client-server.

ΠΕΙΡΑΜΑΤΙΚΗ ΕΦΑΡΜΟΓΗ – TCP STREAM TO PORT 80 OF WEB SERVER

```
import java.io.DataOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.net.InetAddress;
import java.net.Socket;
import java.net.UnknownHostException;

import org.omg.CORBA.portable.OutputStream;

public class Request {

    public static void main(String[] args) throws IOException {

        int portNumber = 80;

        byte[] addressArray = { (byte)155, (byte)207, (byte)18, (byte)208 };
                                // address of Ithaki

                                // 185.140.165.12 -> contra.gr

                                // 79.107.217.65 -> my IP

        Socket s = null;
```

```
        try {
            s = new Socket(InetAddress.getByAddress(addressArray),
portNumber);
        } catch (IOException e) {
            e.printStackTrace();
        }

        byte[] input = new byte[1024];

        //DataOutputStream out = null;
        try (DataOutputStream out = new
DataOutputStream(s.getOutputStream())) { //this is called "try with resources"
and it flushes the stream automatically
            //out = new DataOutputStream(s.getOutputStream());
            out.write("GET /index.html HTTP/1.0\r\n\r\n".getBytes());

            InputStream in = s.getInputStream();
            //int BytesAvailable = in.available();
            //byte[] input = new byte[BytesAvailable];
            //in.read(input, 0, BytesAvailable);
            in.read(input);
            String message = new String(input, 0, 1024);
            System.out.println("HERE IS THE RESPONSE FROM THE
SERVER ... \n" + message);
        } catch (IOException e) {
            e.printStackTrace();
        }

        /*
        try {
            InputStream in = s.getInputStream();
            in.read(input);
            String message = new String(input, 0, 1024);
```

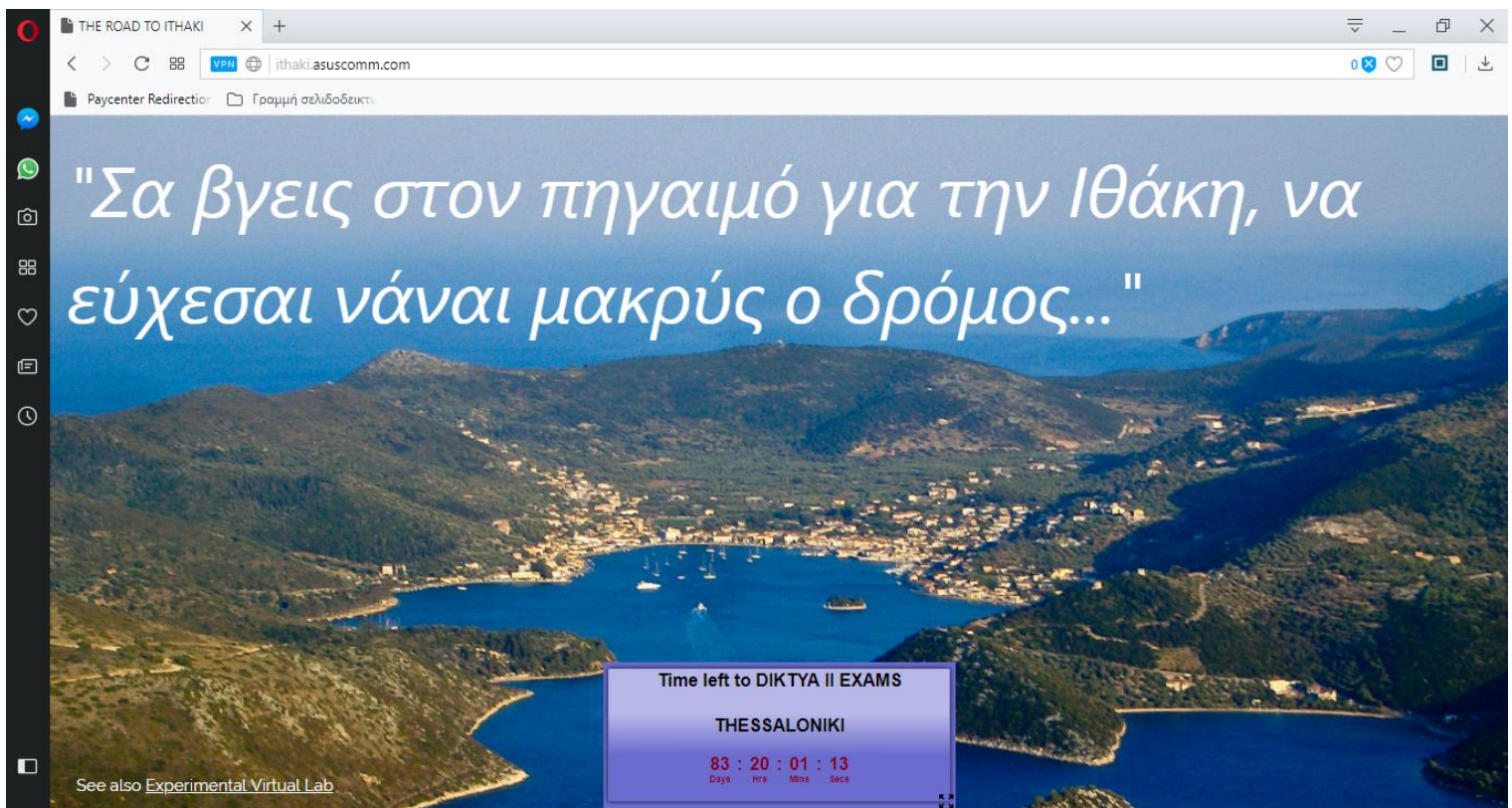
```
        System.out.println("HERE IS THE RESPONSE FROM THE  
SERVER ... \n" + message);  
    } catch (IOException e) {  
        e.printStackTrace();  
    }  
    */  
  
}  
  
}
```

APACHE HTTP “HOME” WEB SERVER

Ο server θα τρέχει κάθε Σάββατο 16.00-17.00 ή μετά από αίτημα ενός χρήστη στο email konserpap@auth.gr (το QoS [uptime του server] είναι χαμηλό λόγω της συχνής απουσίας του φοιτητή από το σπίτι και για λόγους ασφαλείας).

Ο server παρέχει υπηρεσία αντίστροφης μέτρησης μέχρι την ημέρα της εξέτασης του μαθήματος Δίκτυα II, στις 29 Ιουνίου 2018, στις 12.00.

Screenshot του ιστότοπου <http://ithaki.asuscomm.com> που κάνει hosting ο server



(β)

Γενικά για το UDP

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

Το UDP είναι το δεύτερο πρωτόκολλο επιπέδου μεταφοράς (το πρώτο είναι το TCP) και ουσιαστικά κάνει τα ελάχιστα που μπορεί να κάνει ένα πρωτόκολλο επιπέδου μεταφοράς. Το UDP είναι ασυνδεσμικό, δηλαδή δεν προσφέρει εγγυημένη παράδοση μηνυμάτων στη σωστή σειρά ή επιβεβαιώσεις παράδοσης, κανένα έλεγχο ροής και συμφόρησης και δε χρειάζεται ειδική διαδικασία εγκαθίδρυσης σύνδεσης πριν την ανταλλαγή μηνυμάτων (παρέχει δηλαδή μια υπηρεσία “καλύτερης προσπάθειας” χωρίς σύνδεση (connectionless), είναι μια μινιμαλιστική επέκταση της υπηρεσίας “best-effort” του IP). Πρακτικά η μόνη υπηρεσία που παρέχει είναι η πολύπλεξη μέσω του μηχανισμού των θυρών οπότε μια εφαρμογή που χρησιμοποιεί το UDP είναι σαν να χρησιμοποιεί το επίπεδο Διαδικτύου απευθείας.

Κύρια χαρακτηριστικά του UDP

Τα κύρια **χαρακτηριστικά του UDP** είναι τα εξής:

- Αναξιόπιστο** - Κατά την αποστολή ενός πακέτου, ο αποστολέας δεν είναι σε θέση να γνωρίζει εάν το πακέτο θα φτάσει σωστά στον προορισμό του ή εάν θα χαθεί μέσα στο δίκτυο. Δεν έχει προβλεφθεί η δυνατότητα επιβεβαίωσης λήψης πακέτου από τον παραλήπτη, ούτε η επαναμετάδοση ενός χαμένου πακέτου.
- Δεν υπάρχει σειρά** - Τα πακέτα UDP, σε αντίθεση με το TCP, δεν αριθμούνται και κατά συνέπεια δεν υπάρχει κάποια συγκεκριμένη σειρά με την οποία θα πρέπει να φτάσουν στον παραλήπτη.
- Ελαφρύ** - Το πρωτόκολλο αυτό καθ' αυτό είναι πολύ ελαφρύ σε σύγκριση με το TCP διότι δεν εφαρμόζει όλους τους μηχανισμούς αξιόπιστης επικοινωνίας που υπάρχουν στο δεύτερο. Αυτό έχει ως συνέπεια να είναι αρκετά πιο γρήγορο.

•**Datagrams** - Κάθε πακέτο UDP ονομάζεται επίσης και "datagram", θεωρείται δε ως μεμονωμένη οντότητα που θα πρέπει να μεταδοθεί ολόκληρη. Κατά συνέπεια δεν υφίσταται η έννοια της διοχέτευσης πακέτων μέσα σε ένα κανάλι/σύνδεση.

Δομή UDP πακέτου

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

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

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

Ακολουθεί μία συνοπτική εξήγηση των πεδίων:

Source port

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

Destination port

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

Length

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

Checksum

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

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

➤ Για IPv4, το πακέτο λαμβάνει την ακόλουθη μορφή:

Source Address, Destination Address

Οι διευθύνσεις IP του αποστολέα και του παραλήπτη αντίστοιχα.

Zeros

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

Protocol

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

UDP Length

Το συνολικό μέγεθος του πακέτου UDP.

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

➤ Για IPv6, το πακέτο παίρνει την εξής μορφή:

Source Address, Destination Address

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

UDP Length

Το συνολικό μέγεθος του πακέτου UDP, όπως και προηγουμένως.

Zeros

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

Next Header

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

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

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

UDP έναντι TCP

Γιατί να επιλέξει κάποιος για την εφαρμογή του το πρωτόκολλο UDP αφού δεν παρέχει όλες τις χρήσιμες υπηρεσίες του TCP;

Οι κυριότεροι λόγοι είναι:

- η πολύ **μικρή καθυστέρηση** αποστολής και η άμεση ανταλλαγή μηνυμάτων εξαιτίας της πολύ μικρής επικεφαλίδας και του μη καθορισμού σύνδεσης
- η **εξοικονόμηση πόρων** στα τερματικά επειδή δεν χρειάζεται η διατήρηση κατάσταση σύνδεσης
- ο **καλύτερος έλεγχος από την εφαρμογή** του ποια δεδομένα αποστέλονται και πότε, κυρίως επειδή δεν υπάρχει υποχρεωτική επαναμετάδοση πακέτων και αγνοούνται οι συνθήκες συμφόρησης του δικτύου.

Τυπικά το UDP χρησιμοποιείται από εφαρμογές που ανταλλάσσουν περιορισμένο αριθμό μηνυμάτων (πχ DNS) οπότε δεν υπάρχει λόγος δημιουργίας σύνδεσης, ή από εφαρμογές που είναι ευαίσθητες στην καθυστέρηση (πχ VoIP, video conference) όπου το TCP με όλους τους μηχανισμούς του είναι μη αποδοτικό.

Εφαρμογές

Σε αντίθεση με το πρωτόκολλο TCP, το UDP υποστηρίζει broadcasting, δηλαδή την αποστολή ενός πακέτου σε όλους τους υπολογιστές ενός δικτύου, και multicasting, δηλαδή την αποστολή ενός πακέτου σε κάποιους συγκεκριμένους υπολογιστές ενός δικτύου. Η τελευταία δυνατότητα χρησιμοποιείται πολύ συχνά στις εφαρμογές audio και video streaming ούτως ώστε μία ροή ήχου ή εικόνας να μεταδίδεται ταυτόχρονα σε πολλούς συνδρομητές.

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

(Υ)

Γενικά για το Audio Streaming

Η τεχνολογία του «streaming audio» μεταδίδει τον ήχο συνεχόμενα και μπορεί να δώσει την ηχητική εμπειρία που περιμένουν οι περισσότεροι άνθρωποι. Το streaming ανταποκρίνεται πολύ περισσότερο στις ανάγκες των χρηστών απ' ότι προηγούμενες τεχνολογίες αφού προσφέρει μια αίσθηση αμεσότητας στους χρήστες ενώ δίνει και ένα δυνατό όπλο στα χέρια των επαγγελματιών του δικτύου αφού μπορεί να προσελκύσει το ενδιαφέρον των χρηστών στις σελίδες τους περισσότερο χρόνο. Μια άλλη ενδιαφέρουσα χρήση της τεχνολογίας «streaming» είναι οι τηλεφωνικές υπηρεσίες μέσω δικτύου. Το τηλέφωνο μέσω δικτύου δίνει τη δυνατότητα στους χρήστες να κάνουν αμέτρητες υπεραστικές και διεθνής συνδιαλέξεις με κόστος, το κόστος μιας δικτυακής σύνδεσης.

Για να καταλάβει κανείς πως λειτουργεί η τεχνολογία του streaming audio βοηθάει να γνωρίζει τα εξής:

- Τύπους του streaming audio
- Κωδικοποίηση ήχου
- Πρωτόκολλα χρησιμοποιούμενα για το streaming audio

Τύποι του streaming audio

On demand: Αποθηκευμένα αρχεία ήχου που λαμβάνονται από τους χρήστες

Live: Μετάδοση γεγονότων καθώς αυτά συμβαίνουν

Συμπίεση/Κωδικοποίηση ήχου

Τα αρχεία ήχου είναι σχετικά μεγάλα. Για να μεταφέρεις τέτοια αρχεία ακόμη και μέσω σύνδεσης απαιτείται τα αρχεία να είναι συμπιεσμένα. Έτσι είναι απαραίτητο ο ήχος πριν τη μετάδοσή του να κωδικοποιείται και να συμπιέζεται.

Κάθε εταιρεία χρησιμοποιεί δικούς της τρόπους συμπίεσης και αποσυμπίεσης. Τα προγράμματα κωδικοποίησης παίρνουν ένα αρχικό αρχείο(.wav,.au,.snd,.aiff) και μειώνουν το μέγεθος του πετώντας κάποια πληροφορία που εκείνα θεωρούν άχρηστη ή

μη ζωτικής σημασίας για το τελικό αποτέλεσμα. Το συμπιεσμένο αρχείο που παράγουν είναι πολύ μικρότερο σε μέγεθος και χαμηλότερης ποιότητας ήχου σε σχέση με το αρχικό. Επίσης το αρχείο ήχου δίνεται σε μια μορφή (format) ανάλογα με τον προμηθευτή του αντίστοιχου προγράμματος. Τα προγράμματα κωδικοποίησης επιτρέπουν τον έλεγχο της ποιότητας του ήχου που θα παράγουμε. Φυσικά όσο καλύτερη είναι η ποιότητα του ήχου και όσο μεγαλύτερη η συχνότητα δειγματοληψίας τόσο μεγαλύτερο θα είναι το μέγεθος του τελικού αρχείου.

Όλα τα προϊόντα του streaming audio απαιτούν έναν κωδικοποιητή (encoder) και ένα αποκωδικοποιητή (player). Ο κωδικοποιητής ταυτόχρονα εκτελεί και χρέη server, δηλαδή συμπιέζει τα πακέτα ήχου ώστε να ταιριάζουν στο εύρος ζώνης του δικτύου με το οποίο είναι συνδεδεμένοι οι χρήστες. Ο αποκωδικοποιητής αποσυμπιέζει τα πακέτα ήχου και με τη βοήθεια της κάρτας ήχου του υπολογιστή μας ακούμε το μεταδιδόμενο σήμα.

Ενδεικτικά αναφέρονται ορισμένα πρωτόκολλα και τεχνικές όπως MPEG-2, AAC (Advanced Audio Codec), MP3, PCM (Pulse Code Modulation), DPCM (Differential Pulse Code Modulation), ADPCM (Adaptive Differential Pulse Code Modulation) και AQ-DPCM (Adaptive Quantiser - Differential Pulse Code Modulation).

Διεθνή Πρότυπα Audio Streaming

Ο όρος streaming media (audio/video) αναφέρεται σε περιεχόμενο που «καταναλώνεται» κατά τη διάρκεια της αποστολής του. Δηλαδή δεν είναι απαραίτητο να «κατέβει» όλο το αρχείο στον τοπικό υπολογιστή ή κινητή συσκευή (PDA, κινητό...) προκειμένου να τα δούμε ή να το ακούσουμε. Αρκεί να συνδεθούμε σε έναν server που να μας στέλνει μια «ροή» δεδομένων. Πολύ διαδεδομένες εφαρμογές τύπου streaming είναι η τηλεσυνδιάσκεψη, το internet radio και voice over IP (VoIP). Επίσης πολλοί είναι πλέον αυτοί που χρησιμοποιούν VoIP προγράμματα (πχ Skype) για να μειώσουν αισθητά ή και να εκμηδενίσουν τα τηλεπικοινωνιακά τους κόστη. Υπό το πρίσμα αυτό λοιπόν παρουσιάζει εξαιρετικό ενδιαφέρον μια αναφορά στα διεθνή πρότυπα audio streaming που χρησιμοποιούνται σήμερα.

Γενικά, η χρήση διαφόρων προτύπων audio streaming δεν σημαίνει πως καθένα από αυτά χρησιμοποιεί και το δικό του πρωτόκολλο μεταφοράς δεδομένων. Τα πιο πολλά από αυτά είναι «χτισμένα» πάνω στα πρωτόκολλα TCP, UDP και HTTP. Αξίζει να

σημειωθεί, όμως, ότι πρωτόκολλα και εφαρμογές που βασίζονται στο UDP αντιμετωπίζουν συχνά προβλήματα με τα firewalls.

Real-time Transport Protocol (RTP)

Το RTP καθορίζει ένα προτυποποιημένο τύπο πακέτων δεδομένων αποκλειστικά για μετάδοση ήχου και βίντεο μέσω του Διαδικτύου. Πρώτη φορά εμφανίστηκε το 1996. Το RTP δεν χρησιμοποιεί κάποια συγκεκριμένη θύρα UDP ή TCP. Ο μόνος κανόνας στον οποίο υπακούει είναι ότι οι επικοινωνίες UDP γίνονται σε θύρες (ports) με ζυγούς αριθμούς και οι TCP σε αυτές με περιττούς αριθμούς. Παρόλο που δεν είναι υποχρεωτικό συνήθως χρησιμοποιεί τις θύρες 16384 έως 32767. Το RTP σχεδιάστηκε αρχικά ως πρωτόκολλο multicast αλλά τελικά χρησιμοποιείται κυρίως σε unicast εφαρμογές. Συχνά χρησιμοποιείται σε συστήματα streaming media (σε συνδυασμό με το πρωτόκολλο RTSP), όπως επίσης και σε συστήματα τηλεδιάσκεψης και push-to-talk (σε συνδυασμό με το H.323 ή το SIP). Το γεγονός αυτό το κάνει την βάση της VoIP «βιομηχανίας». Συνδέεται άμεσα με το RTCP και είναι χτισμένο πάνω στο πρωτόκολλο UDP (στο OSI model).

Real-time Control Protocol (RTCP)

Το RTCP είναι το «αδελφό» πρωτόκολλο του RTP. Παρέχει πληροφορίες ελέγχου για μια ροή δεδομένων τύπου RTP. Συνεργάζεται με το RTP για το «πακετάρισμα» και την διανομή δεδομένων πολυμέσων αλλά το ίδιο δεν ασχολείται με την μεταφορά αυτών. Χρησιμοποιείται για να εκπέμπει κατά διαστήματα πακέτα ελέγχου στους συμμετέχοντες σε μια σύνοδο πολυμέσων. Ο κύριος σκοπός του είναι να παρέχει πληροφορίες για την ποιότητα και επίδοση της επικοινωνίας που παρέχει το RTP. Συγκεντρώνει στατιστικά στοιχεία για την σύνδεση και τη μετάδοση των δεδομένων (πχ σταλμένα bytes, σταλμένα πακέτα, χαμένα πακέτα, θόρυβος γραμμής, ανάδραση και καθυστέρηση). Τα στοιχεία αυτά μπορούν να χρησιμοποιηθούν από την εκάστοτε εφαρμογή για να αυξηθεί η ποιότητα της επικοινωνίας με διάφορους τρόπους, όπως: περιορισμός ροής ή χρήση αλγορίθμου υψηλότερης συμπίεσης για τα πολυμεσικά δεδομένα. Γενικά δηλαδή το RTCP χρησιμοποιείται για αναφορά QoS (Quality of Service).

Real Time Streaming Protocol (RTSP)

Το RTSP εμφανίστηκε το 1998 και είναι ένα πρωτόκολλο για χρήση σε συστήματα streaming media. Το βασικό του χαρακτηριστικό είναι ότι επιτρέπει τον απομακρυσμένο έλεγχο ενός media server με εντολές παρόμοιες με αυτές ενός βίντεο. Μερικοί RTSP servers χρησιμοποιούν το πρωτόκολλο μεταφοράς RTP, ενώ άλλοι το πρωτόκολλο RDT της RealNetworks. Οι εντολές αυτές αφορούν την περιγραφή του αρχείου προς μετάδοση, τον έλεγχο της αναπαραγωγής και τον τερματισμό της συνόδου με τον server. Οι αιτήσεις επικοινωνίας RTSP βασίζονται στο πρωτόκολλο HTTP. Δηλαδή ο client «μιλάει» στον server μέσω HTTP και TCP, ενώ ο server στον client σε RTP ή RDT. Σπανιότερα ο server χρειάζεται να στείλει κάποιο μήνυμα στον client και τότε το στέλνει και αυτός σε HTTP.

Real Data Transport (RDT)

Το RDT είναι ένα ιδιόκτητο πρωτόκολλο μεταφοράς της RealNetworks. Δημιουργήθηκε κατά τη δεκαετία του '90 και χρησιμοποιείται κυρίως στο πρόγραμμα αναπαραγωγής δεδομένων ροής RealPlayer. Χρησιμοποιείται συνήθως σε συνδυασμό με κάποιο πρωτόκολλο ελέγχου όπως το RTSP, που παρουσιάστηκε προηγουμένως.

Unicast

Ο όρος αναφέρεται περισσότερο στον τρόπο μετάδοσης των δεδομένων ροής παρά σε ένα πρωτόκολλο μετάδοσης. Πρόκειται ουσιαστικά για την μετάδοση δεδομένων από έναν συγκεκριμένο server σε έναν συγκεκριμένο χρήστη, σε αντίθεση με την τεχνολογία multicast. Δηλαδή ο server στέλνει σε κάθε χρήστη ένα ξεχωριστό media stream. Αυτή η υλοποίηση είναι απλή αλλά μπορεί να οδηγήσει σε άσκοπα μεγάλη αύξηση της κίνησης σε ένα δίκτυο!

Multicast

Με τον όρο Multicast αναφερόμαστε στην μετάδοση πληροφορίας ταυτόχρονα σε ένα πλήθος παραλήπτων. Η μετάδοση γίνεται με την πιο αποδοτική στρατηγική για την διανομή των πακέτων σε κάθε παραλήπτη και τη δημιουργία αντιγράφων μόνο όταν η διαδρομή προς τους παραλήπτες διασπάται, «χωρίζει». Δηλαδή μεταξύ δύο κόμβων ενός δικτύου διακινείται μόνο ένα media stream, κάτι που μειώνει την κίνηση του δικτύου σε σχέση με την unicast μετάδοση. Τελικά σε κάθε παραλήπτη παραδίδεται από ένα

αντίγραφο των δεδομένων και αυτό μπορεί να έχει ως αποτέλεσμα την υπερβολική αύξηση του όγκου των δεδομένων που συνολικά διακινούνται. Πολλά δημοφιλή πρωτόκολλα πάντως, όπως το XMPP, δέχονται αυτό το μειονέκτημα και περιορίζουν το μέγιστο πλήθος των παραληπτών.

Η μετάδοση multicast υποστηρίζεται από και χρησιμοποιεί διάφορα πρωτόκολλα. Μερικά από αυτά αναφέρονται: Real-Time Transport Protocol (RTP) για πολυσυμμετοχικές τηλεδιασκέψεις, Scalable Reliable Multicast (SRM), Uniform Reliable Group Communication Protocol (URGC), Multicast File Transfer Protocol (MFTP), Log-Based Receiver-reliable Multicast (LBRM) και STORM (STructure-Oriented Resilient Multicast).

Ενδεικτικά αναφέρονται επιπλέον και τα Shoutcast, QuickTime και Macromedia Flash.

(δ)

Ρυθμίσεις:

➤ IP

The screenshot shows the 'LAN IP' configuration page. At the top, there are tabs for 'LAN IP', 'DHCP Server', 'Route', 'IPTV', and 'Switch Control'. The 'LAN IP' tab is selected. Below the tabs, the title 'LAN - LAN IP' is displayed. A subtitle reads 'Configure the LAN setting of DSL-N14U.' Below this, there are two input fields: 'IP Address' with the value '192.168.1.254' and 'Subnet Mask' with the value '255.255.255.0'. At the bottom right, there is an 'Apply' button.

LAN IP	DHCP Server	Route	IPTV	Switch Control
LAN - LAN IP				
Configure the LAN setting of DSL-N14U.				
IP Address	192.168.1.254			
Subnet Mask	255.255.255.0			
Apply				

The screenshot shows the 'Manually Assigned IP around the DHCP list (Max Limit : 32)' section. It contains a table with three columns: 'MAC Address', 'IP Address', and 'Add / Delete'. The first row is empty, with input fields for MAC and IP, and a '+' button. The second row contains the MAC address '4C:BB:58:E3:3D:CC', the IP address '192.168.1.10', and a '-' button. At the bottom right, there is an 'Apply' button.

Manually Assigned IP around the DHCP list (Max Limit : 32)		
MAC Address	IP Address	Add / Delete
<input type="text"/>	<input type="text"/>	
4C:BB:58:E3:3D:CC	192.168.1.10	
Apply		

➤ DNS/DHCP

The screenshot displays the ASUS DSL-N14U web interface. The top navigation bar includes 'Logout', 'Reboot', and 'English' (language dropdown). Below this, the 'Firmware Version: 1.0.9.7' and 'SSID: WND_PmC004' are shown. The left sidebar contains a 'General' section with links to 'Network Map', 'Guest Network', 'Traffic Manager', 'Parental Controls', 'USB Application', and 'AiCloud'. Below this is an 'Advanced Settings' section with links to 'Wireless', 'LAN' (highlighted), 'WAN', 'IPv6', 'VPN', 'Firewall', and 'Administration'. The main content area is titled 'LAN - DHCP Server' and includes a description of DHCP. It features a 'Basic Config' section with a radio button to 'Enable the DHCP Server' (set to 'Yes'), and input fields for 'IP Pool Starting Address' (192.168.1.2), 'IP Pool Ending Address' (192.168.1.253), 'Lease Time' (86400 seconds), and 'Default Gateway'. Below this is a 'DNS and WINS Server Setting' section with input fields for 'DNS Server' and 'WINS Server'. At the bottom, there is a 'Manually Assigned IP around the DHCP list (Max Limit : 32)' table with columns for 'MAC Address', 'IP Address', and 'Add / Delete'. The table contains one entry with MAC address '4C:BB:58:1E:31:30' and IP address '192.168.1.10'.

MAC Address	IP Address	Add / Delete
4C:BB:58:1E:31:30	192.168.1.10	+

➤ NAT

WAN - NAT Passthrough

Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.

PPTP Passthrough	Enable ▾
L2TP Passthrough	Enable ▾
IPSec Passthrough	Enable ▾
RTSP Passthrough	Enable ▾
H.323 Passthrough	Enable ▾
SIP Passthrough	Enable ▾
Enable PPPoE Relay	Disable ▾

Apply

➤ PORT

The screenshot shows the WAN configuration page for port forwarding. The left sidebar contains various settings categories, with 'WAN' selected. The main content area includes a 'Basic Config' section with options to enable port forwarding and select server lists. Below this is a 'Port Forwarding List' table with columns for Service Name, Source IP, Port Range, Local IP, Local Port, Protocol, and Add/Delete actions. An 'Apply' button is at the bottom.

USB Application

AiCloud

Advanced Settings

Wireless

LAN

WAN

IPv6

VPN

Firewall

Administration

System Log

Network Tools

forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network.
If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200-10300), the LAN IP address, and leave the Local Port empty.

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with DSL-N14U's web user interface.
- When you set 20-21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with DSL-N14U's native FTP server.

[Virtual Server / Port Forwarding FAQ](#)

Basic Config

Enable Port Forwarding ☐ Yes ☒ No

Famous Server List

Famous Game List

FTP Server Port

Port Forwarding List (Max Limit : 32)

Service Name	Source IP	Port Range	Local IP	Local Port	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="button" value="⊕"/>
Ithaki	155.207.18.208	48000:48032	192.168.1.8		UDP	<input type="button" value="⊖"/>

Παραπομπές-Πηγές

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

<https://networking-basics.wikispaces.com/Επίπεδο+Μεταφοράς+%28Πρωτόκολλα+TCP+και+UDP%29>

<http://www.it.uom.gr/project/MultimediaTechnologyNotes/extra/append6.htm>

<http://repository.library.teimes.gr/xmlui/bitstream/handle/>

http://ikee.lib.auth.gr/record/290038/files/Διπλωματική-Στέφανος_Βάτσικας-4102.pdf

<https://tools.ietf.org/html/rfc768>

Stallings William, Ασύρματες Επικοινωνίες και Δίκτυα

Tanenbaum Andrew S., Δίκτυα υπολογιστών