Υλοποίηση Δικτυακών Υποδομών και Υπηρεσιών: Υπηρεσία Ηλεκτρονικού Ταχυδρομείου - SMTP

Δρ. Απόστολος Γκάμας

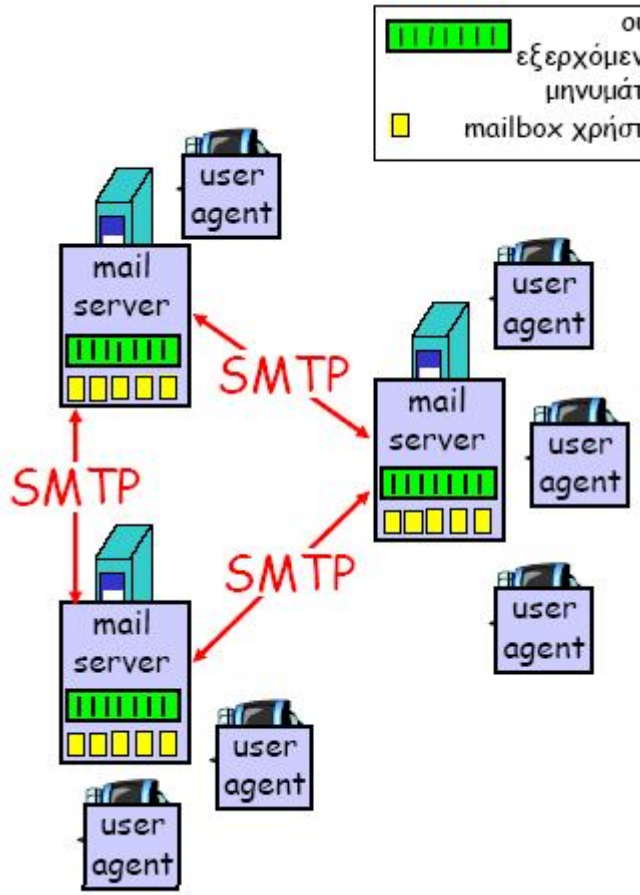
Διδάσκων (407/80)

gkamas@uop.gr

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

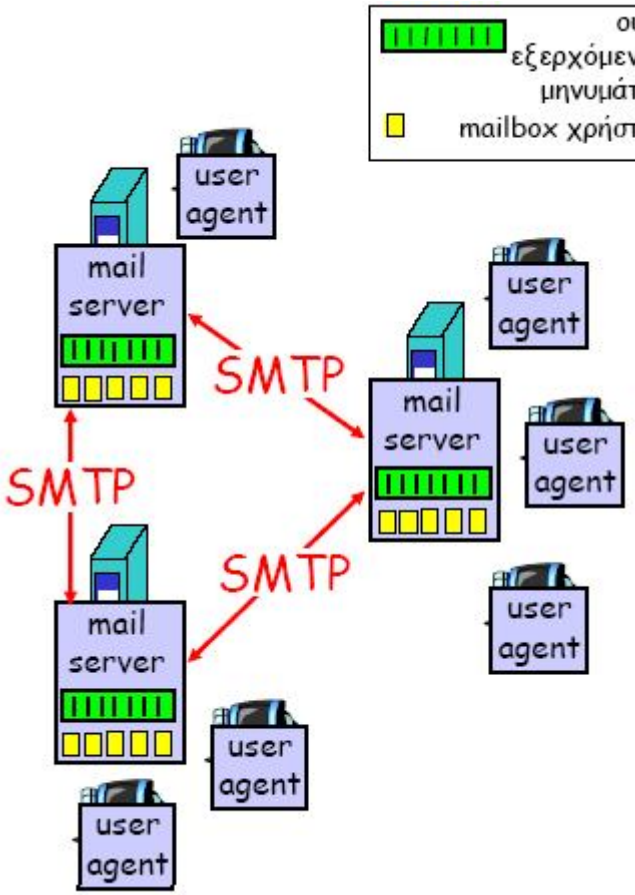
Ηλεκτρονικό Ταχυδρομείο

- Αποτελείται από τρία κύρια στοιχεία
  - User agents
  - Mail servers
  - SMTP: Simple Mail Transfer Protocol
- User Agent ή "mail reader"
  - Σύνθεση, ανάγνωση μηνυμάτων ηλεκτρονικού ταχυδρομείου
  - π.χ. Outlook, elm, pico
  - Εισερχόμενα και εξερχόμενα μηνύματα αποθηκεύονται στον mail server



Ηλεκτρονικό Ταχυδρομείο: mail servers

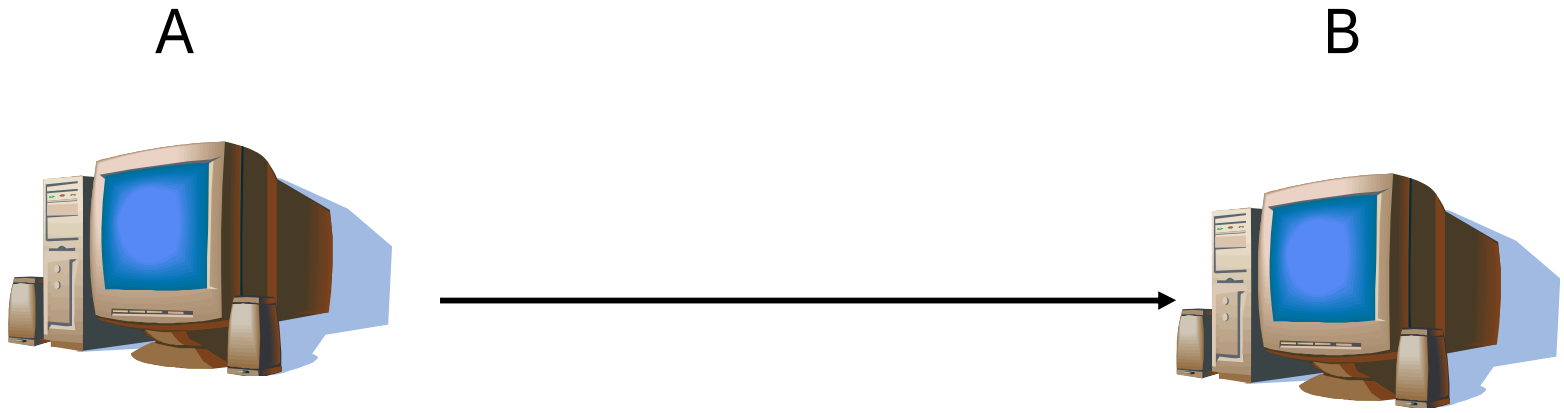
- **Mailbox:** περιέχει εισερχόμενα μηνύματα χρήστη
- Ουρά μηνυμάτων: περιέχει εξερχόμενα (προοριζόμενα για αποστολή) μηνύματα e-mail
- Πρωτόκολλο SMTP: αποστολή μηνυμάτων email μεταξύ mail servers
- Μοντέλο client/server
  - Client: αποστέλλων mail server
  - Server: παραλαμβάνων mail server
- Κάθε mail server τρέχει και την διεργασία client και την διεργασία server



Message Transfer Agent (MTA) ή Mail Servers

- Οι message transfer agent (MTA) είναι υπεύθυνοι για την μετάδοση των ηλεκτρονικών μηνυμάτων πάνω από TCP/IP δίκτυα.
  - Ένας MTA είναι υπεύθυνος να δρομολογήσει τα ηλεκτρονικά μηνύματα στους κατάλληλους προορισμούς.
  - Οι MTA χρησιμοποιούν το Mail Exchange (MX) record από ένα DNS server για να προσδιορίσουν τους παραλήπτες μηνυμάτων.
- Το SMTP ορίζει πως δύο MTAs επικοινωνούν πάνω από μια TCP σύνδεση.

Τρόπος λειτουργίας του SMTP

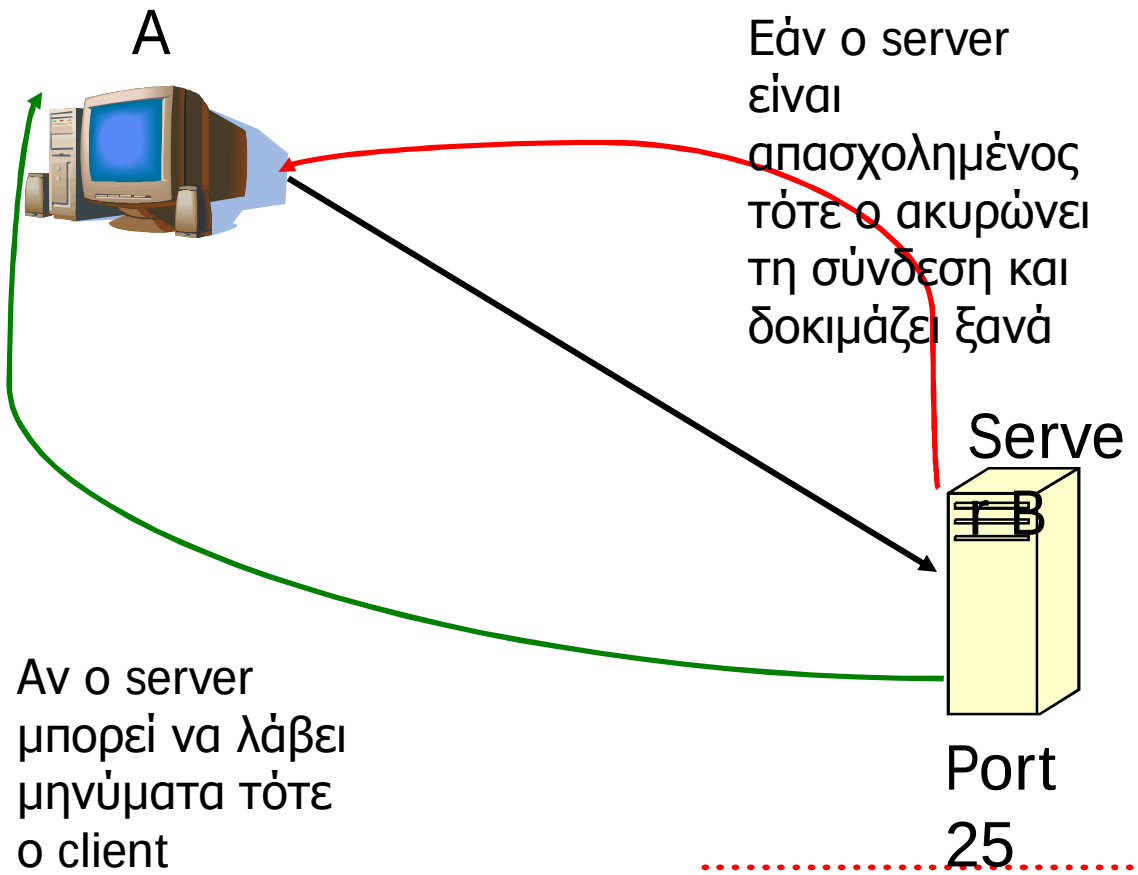


Έστω ότι θέλουμε να στείλουμε ένα ηλεκτρονικό μήνυμα από τον σταθμός εργασίας Α στο σταθμό εργασίας Β

Τρόπος λειτουργίας του SMTP

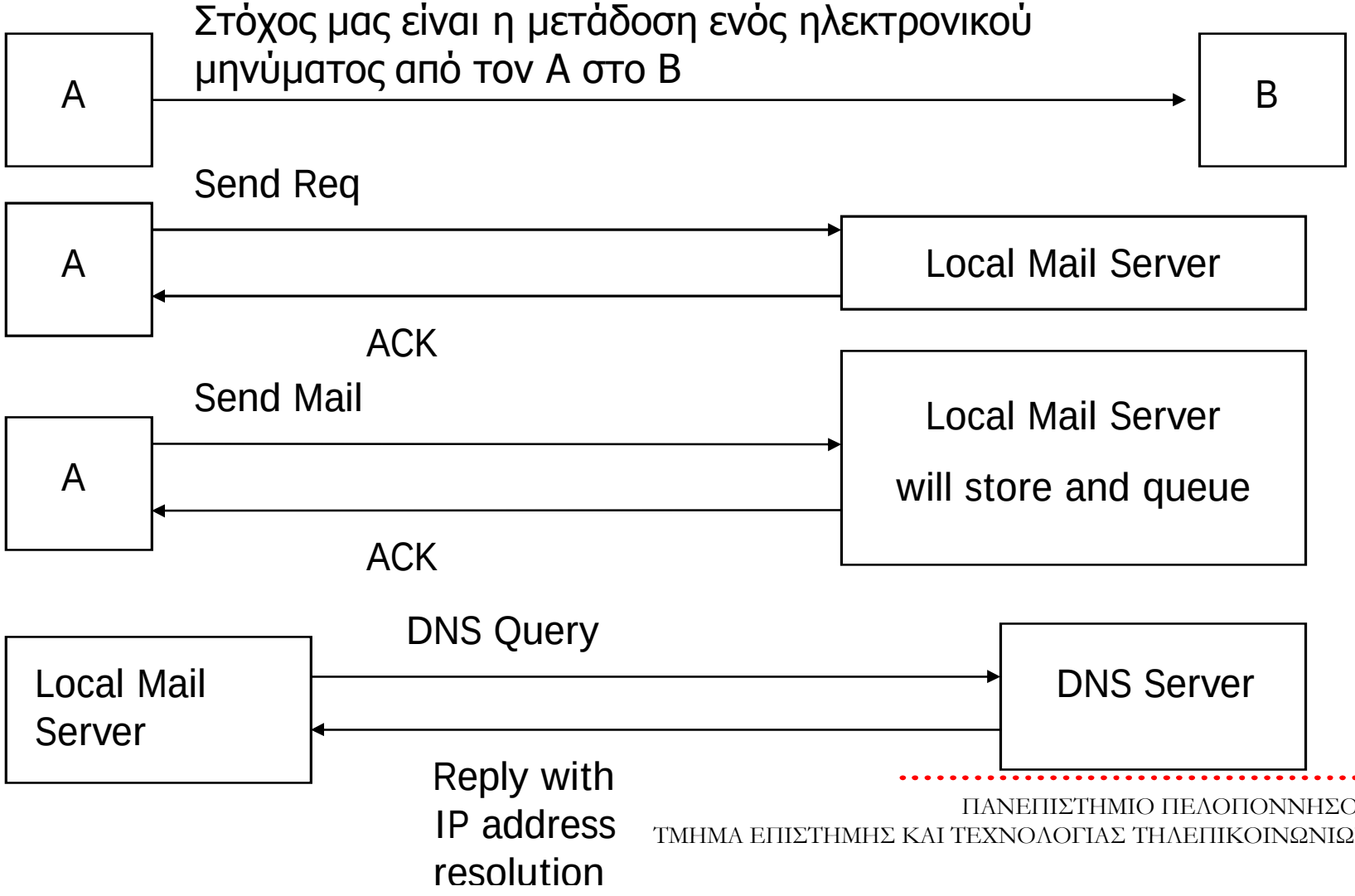
Ο Α υποβάλει το source και destination. Εάν και τα δύο είναι σωστά ο server δίνει το go-ahead signal

Αρχικά επιχειρούμε να συνδεθούμε με τον απομακρυσμένο server για να διαπιστώσουμε εάν λαμβάνει μηνύματα

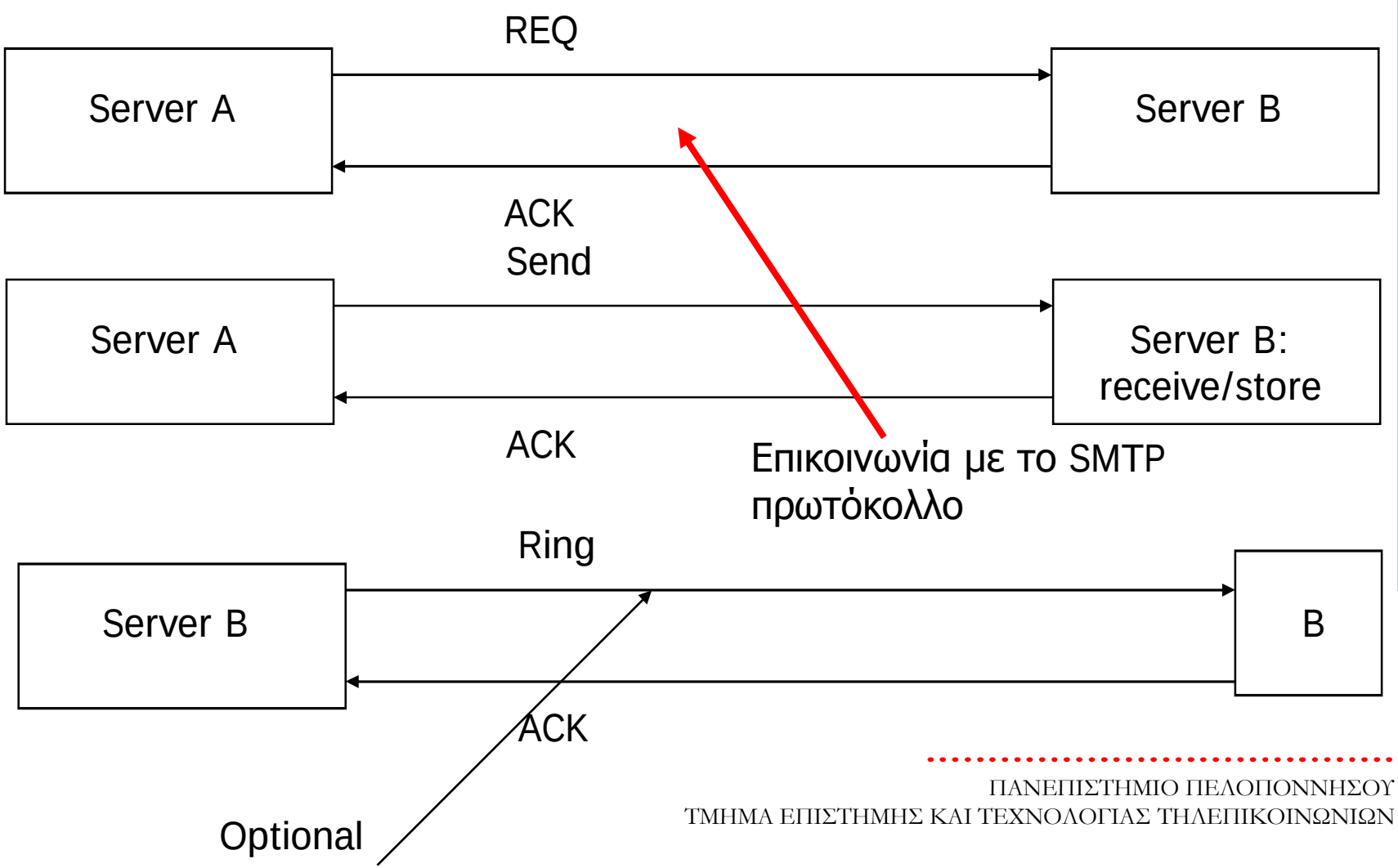


Αν ο server μπορεί να λάβει μηνύματα τότε ο client αποστέλλει το μήνυμα

Τρόπος λειτουργίας του SMTP



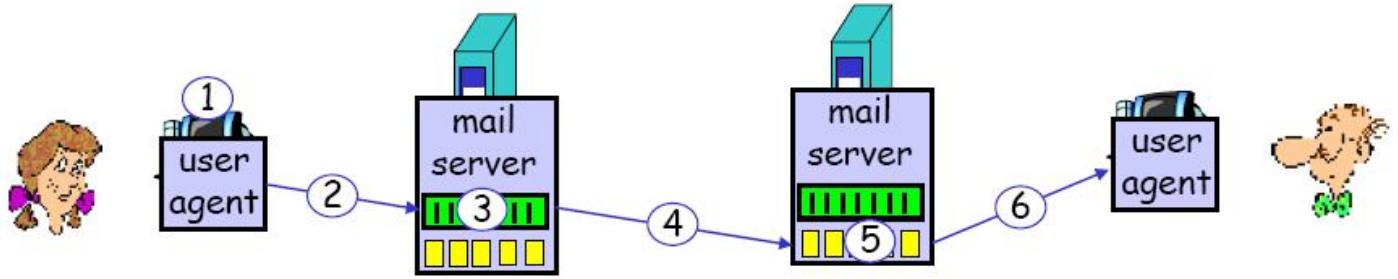
Τρόπος λειτουργίας του SMTP



Σενάριο: Η Άννα στέλνει μήνυμα στον Κώστα

1. Η Άννα χρησιμοποιεί τον **user agent (UA)** για να συνθέσει μήνυμα με διεύθυνση kostas@cti.gr
2. Ο **UA** της Άννας στέλνει το μήνυμα στον **mail server** της όπου τοποθετείται στην ουρά εξερχόμενων μηνυμάτων
3. Ο **SMTP client** ανοίγει σύνδεση **TCP** με τον **mail server** του Κώστα
4. Ο **SMTP client** στέλνει το μήνυμα της Άννας μέσω της σύνδεσης **TCP**
5. Ο **mail server** του Κώστα τοποθετεί το μήνυμα στο **mailbox** του Κώστα
6. Ο Κώστας χρησιμοποιεί τον **user agent** του για να διαβάσει το μήνυμα

— Εάν ο **mail server** του Κώστα δεν είναι σε λειτουργία, τότε το μήνυμα παραμένει στον **mail server** της Άννας ο οποίος επιχειρεί ξανά αργότερα



RFC 821

- Αποτελεί μια περιγραφή του SMTP
  - Στόχος είναι η αξιόπιστη και αποτελεσματική μεταφορά μηνυμάτων
- Σημεία με ενδιαφέρον
  - Αποστολή
  - Προώθηση
  - Relaying
  - Άνοιγμα / κλείσιμο

RFC 821

- Το RFC 821 επίσης παρέχει:
  - Εξακρίβωση
  - SMTP εντολές και σύνταξη
  - Διαγράμματα κατάστασης
  - Αλληλουχίες εντολών και αποκρίσεις
- Επεκτάσεις:
  - RFC 1869
    - HELO εντολή
  - MAIL, RCPT, DATA μπορούν να πάρουν επιπλέον τιμές.

SMTP εντολές

- MAIL command
  - Κάνει clear buffer και είναι προετοιμασία για λήψη μηνύματος
  - Δίνει το sender ID
- RCPT command
  - Δίνει τα στοιχεία του παραλήπτη
- DATA command
  - Στέλνει τα δεδομένα

RFC 822

- Περιγράφει την δομή των μηνυμάτων του SMTP.
  - Το RFC 822 είναι το πρότυπο για την μορφή των μηνυμάτων κειμένου στο Διαδίκτυο.
  - RFC 2822: Νέο πρότυπο
- Σημεία με ενδιαφέρον
  - Μορφή μηνυμάτων
  - Μορφή ώρας / ημερομηνίας
  - Μορφή διευθύνσεων
  - Διάφορες RFC επεκτάσεις

Ηλεκτρονικό ταχυδρομείο: SMTP (RFC 2821)

- Το SMTP χρησιμοποιεί TCP για τη μεταφορά μηνυμάτων ηλεκτρονικού ταχυδρομείου από τον client στο server (θύρα 25)
- Απευθείας μεταφορά μηνυμάτων από mail server αποστολέα σε mail server παραλήπτη
- Μετά την εγκαθίδρυση σύνδεσης TCP ακολουθούν τρεις φάσεις μεταφοράς:
  - Χαιρετισμός (greeting)
  - Μεταφορά μηνυμάτων
  - Τερματισμός
- Αλληλουχία εντολών / αποκρίσεων
  - Εντολές (commands): κείμενο ASCII
  - Αποκρίσεις (responses): κώδικας και φράση κατάστασης
- Τα μηνύματα πρέπει να είναι σε 7-bit ASCII

Παρατηρήσεις σχετικά με το SMTP

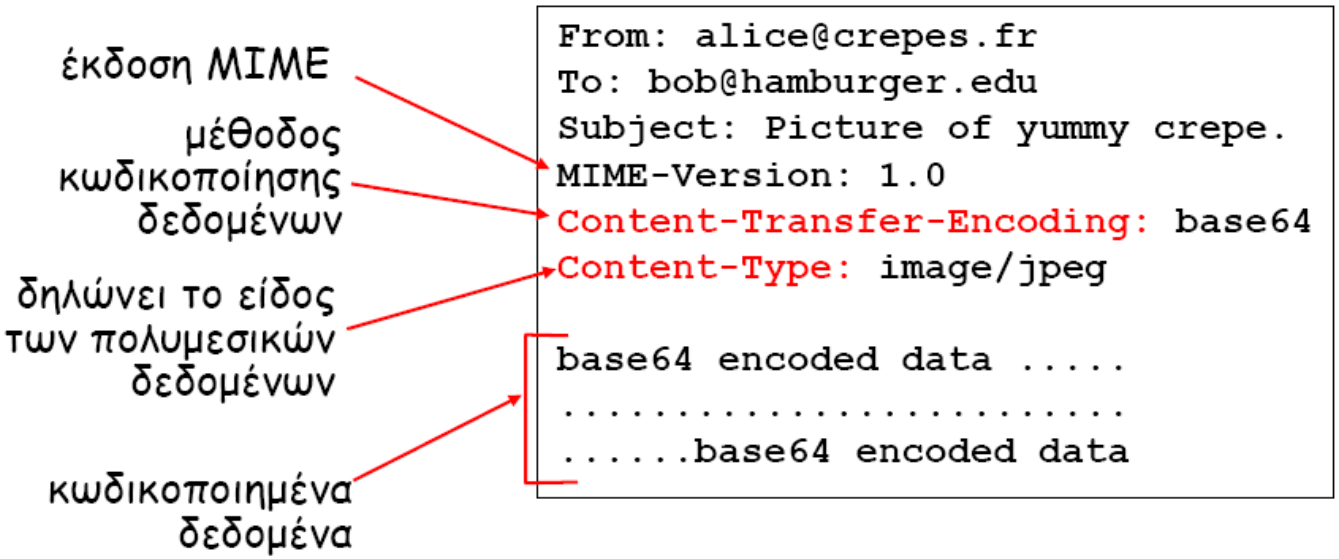
- Το SMTP χρησιμοποιεί παραμένουσες (persistent) συνδέσεις TCP
- Το SMTP απαιτεί το μήνυμα (επικεφαλίδα και σώμα) να είναι σε 7-bit ASCII
- Ο SMTP server χρησιμοποιεί CRLF. CRLF για να προσδιορίσει το τέλος ενός μηνύματος

Μορφή μηνύματος ηλεκτρονικού ταχυδρομείου (κείμενο)

- SMTP: πρωτόκολλο για την ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου
- RFC 822: πρότυπο για τη μορφή (format) μηνύματος κειμένου:
  - Γραμμές επικεφαλίδας (header lines) π.χ. To, From, Subject οι οποίες είναι διαφορετικές από τις SMTP εντολές
  - Σώμα (body): το «κυρίως» μήνυμα, χαρακτήρες ASCII μόνο

Μορφή μηνύματος ηλεκτρονικού ταχυδρομείου: επεκτάσεις για πολυμέσα

- MIME: Multipurpose Internet Mail Extensions, RFC 2045, 2046
- Πρόσθετες γραμμές στην επικεφαλίδα (header) του μηνύματος δηλώνουν το είδος του περιεχομένου



MIME types

- Content-Type: type/subtype; parameters
- Type: Text – Subtype: π.χ. plain, html
- Type: Image – Subtype: π.χ. Jpeg, gif
- Type: Audio – Subtype: π.χ. Basic, 32kadpcm
- Type: Video – Subtype: π.χ. Mpeg, quicktime
- Application: άλλου είδους δεδομένα τα οποία πρέπει να επεξεργαστεί μια εφαρμογή για να μπορούν να χρησιμοποιηθούν από τον χρήστη

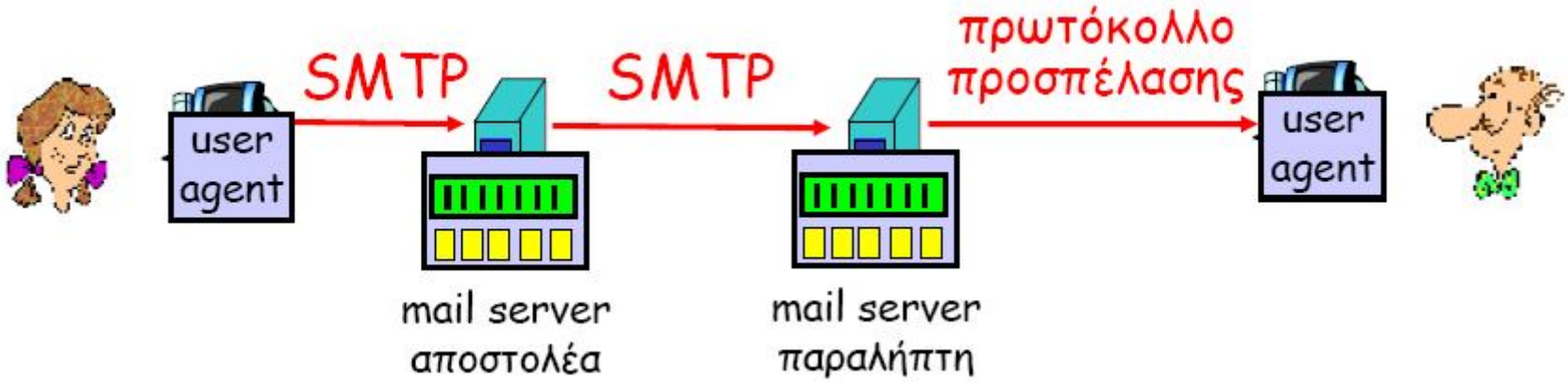
Multipart Type

```
From: alice@crepes.fr
To: bob@hamburger.edu
Subject: Picture of yummy crepe.
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=StartOfNextPart

--StartOfNextPart
Dear Bob, Please find a picture of a crepe.
--StartOfNextPart
Content-Transfer-Encoding: base64
Content-Type: image/jpeg
base64 encoded data .....
.........................
......base64 encoded data
--StartOfNextPart
Do you want the recipe?
--StartOfNextPart
```

Πρωτόκολλα προσπέλασης ηλεκτρονικού ταχυδρομείου (mail access)

- SMTP: παράδοση/αποθήκευση στον mail server του παραλήπτη
- Mail access protocol: ανάκτηση από τον mail server
  - POP: Post Office Protocol (RFC 1939) – εξουσιοδότηση (agent – server) και download
  - IMAP: Internet Mail Access Protocol (RFC 1730)
    - Περισσότερες δυνατότητες (πιο πολύπλοκο)
    - Διαχείριση αποθηκευμένων μηνυμάτων στον server
  - HTTP: Hotmail, Yahoo! Mail κλπ



POP3 και IMAP

- POP3
  - Στο προηγούμενο παράδειγμα χρησιμοποιείται ο τρόπος «download and delete»
  - Ο Κώστας δεν μπορεί να ξαναδιαβάσει το e-mail εάν αλλάξει client
  - «Download and keep»: αντίγραφα των μηνυμάτων σε διαφορετικούς clients
  - Το POP3 είναι "stateless" από σύνοδο (session) σε σύνοδο
- IMAP
  - Διατηρεί όλα τα μηνύματα στο ίδιο μέρος: τον server
  - Επιτρέπει στον χρήστη να οργανώσει τα μηνύματα σε φακέλους (folders)
  - Το IMAP διατηρεί την «κατάσταση» του χρήστη μεταξύ συνόδων: Ονόματα φακέλων, ποια μηνύματα σχετίζονται με ποίους φακέλους

Διάλογος SMTP

από mail server `crepes.fr` σε mail server `hamburger.edu`

greeting
```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250  Hello crepes.fr, pleased to meet you
```
μεταφορά μηνύματος
```
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C:   How about pickles?
C: .
```
μήνυμα
κλείσιμο
```
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

Διάλογος POP3

φάση εξουσιοδότησης (authorization)

- εντολές client:
  - `user:` username
  - `pass:` password
- αποκρίσεις server:
  - +OK
  - -ERR

φάση συναλλαγής (transaction), client:

- `list:` παρέχει κατάλογο αριθμών μηνυμάτων
- `retr:` ανάκτηση μηνύματος με βάση τον αριθμό του
- `dele:` διαγραφή μηνύματος
- `quit`

φάση ενημέρωσης (update): mail server διαγράφει μηνύματα

```
S: +OK POP3 server ready
C: user bob
S: +OK
C: pass hungry
S: +OK user successfully logged on
```

```
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: <message 1 contents>
S: .
C: dele 1
C: retr 2
S: <message 2 contents>
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off
```

SMTP Εφαρμογές

- Υπάρχουν διάφορες SMTP υλοποιήσεις
- qmail
  - Τοποθετεί πολλά αρχεία στο root του συστήματος
  - Η άδεια χρήσης δεν επιτρέπει την διανομή τροποποιημένων εκδόσεων
  - Δεν υπάρχει άμεση ανταπόκριση από τον Developer/owner
- sendmail
  - Προηγούμενες και η τρέχουσα έκδοση έχουν προβλήματα ασφάλειας
  - Π.χ. Remote root exploits, etc.

SMTP Εφαρμογές

- Postfix
  - Έχει καλή απόδοση στην ασφάλεια
  - Είναι εύκολο στην ρύθμιση
  - Μπορεί να συνδεθεί με LDAP να επιλέξει νέους ή τροποποιημένους χρήστες
- Microsoft Exchange
  - Πολύ εύκολος στην χρήση για περιβάλλοντα Windows
  - Ενσωματώνει το Active Directory (LDAP)
  - Δεν έχει καλή απόδοση στην ασφάλεια

Θέματα απόδοσης και ασφάλειας

- Θέματα ασφάλειας
  - Όταν το SMTP αρχικά υλοποιήθηκε δεν δόθηκε μεγάλη έμφαση σε θέματα ασφάλειας
  - Σχεδιάστηκε βασισμένο σε πνεύμα συνεργασίας και εμπιστοσύνης ανάμεσα στου SMTP servers
  - Δεν υπήρχε πρόβλεψη του spam
- Mail Relay
  - Relay είναι η μετάδοση mail από ένα mail server σε ένα άλλο
  - Οι περισσότεροι SMTP servers δεν πιστοποιούν τους χρήστες

Θέματα απόδοσης και ασφάλειας

- Bulk mails
  - Αυθαίρετοι bulk mailers εκμεταλλεύονται τα παραπάνω
  - Η απόδοση μειώνεται για του χρήστες με δικαίωμα χρήση του mail server
- Relay Restrictions
  - Ελέγχει ότι ο υπολογιστής ανήκει στον τοπικό δίκτυο του mail server
  - Απαιτεί μία local domain return address
  - Δεν αποδέχεται mail από άλλους open relay servers

Θέματα απόδοσης και ασφάλειας

- Μια λύση θα ήταν η δημιουργία ενός νέου SMTP?
  - Πολύ πιθανό να δημιουργηθούν προβλήματα συμβατότητας
- Άλλα μέτρα ασφάλειας
  - Περιορισμένη χρήση εντολών
  - Περιορισμός μεγέθους email
  - Περιορισμός του αριθμού των emails που στέλνονται σε ένα χρονικό διάστημα
  - Αναλυτική καταγραφή (Log everything)
  - POP-before-SMTP Authentication
- Το SMTP δεν παρέχει μηχανισμούς κρυπτογράφησης
  - Αυτό θα πρέπει να γίνει σε υψηλότερα επίπεδα αν απαιτείται
  - Στις τρέχουσες υλοποιήσεις είναι application specific

Πιθανές λύσεις

- Sender Policy Framework (SPF)
  - Μόνο ορισμένοι server επιτρέπεται να κάνουν forward mail από ορισμένα domain names
- DNS Blackhole Lists
  - Περιορισμός αναγνωρισμένων invalid senders
  - Θα αποδώσει εάν υποστηρίζεται από πολλούς servers
- Spam Filtering
  - Ευφυές self-learning λογισμικό