

«Εφαρμογές Διαδικτύου»

Πρόσβαση στο Διαδίκτυο
Υπηρεσίες του Διαδικτύου
Ασφάλεια στο Διαδίκτυο

Πρόσβαση στο Διαδίκτυο

- τηλεφωνική dial-up
- καλωδιακή
- ασύρματη
- δορυφορική
- μέσω κινητού τηλεφώνου

Συνδέσεις dial-up

- απλή τηλεφωνική γραμμή
- αναλογική μετάδοση σήματος
- μετατροπή του σήματος:
ψηφιακό $\leftrightarrow$ αναλογικό $\leftrightarrow$ ψηφιακό
- modem
 - modulator διαμορφωτής
 - demodulator αποδιαμορφωτής

Συνδέσεις dial-up

- ISP – Internet Service Provider
πάροχος υπηρεσιών διαδικτύου
 - ιδιωτικές εταιρίες
π.χ. otenet, forthnet, vivodi, ...
 - δημόσιοι φορείς
π.χ. πανεπιστήμια

Συνδέσεις dial-up

- Διαδικασία σύνδεσης
 - ο χρήστης καλεί τον ISP από τον Η/Υ του μέσω ενός modem
 - αστική κλήση
 - ΕΠΑΚ - Ενιαίου Πανελλαδικού Αριθμού Κλήσης
 - ΠΕΑΚ - Περιοχικού Αριθμού Κλήσης
 - αποκαθίσταται επικοινωνία με τον ISP και ελέγχεται η ταυτότητα του χρήστη
 - ξεκινά η σύνδεση στο Διαδίκτυο

Συνδέσεις dial-up

- Μέγιστες ταχύτητες
 - 56 kbps για σύνδεση PSTN
 - 128 kbps για σύνδεση ISDN
- + :
 - προσβασιμότητα παντού όπου υπάρχει μία τηλεφωνική συσκευή
- — :
 - αργή διαδικασία σύνδεσης
 - χαμηλές ταχύτητες
 - σχετικά υψηλό κόστος

Καλωδιακές συνδέσεις

- ευρυζωνικές (broadband)
- πραγματοποιούνται με
 - ομοαξονικά καλώδια
 - οπτικές ίνες
 - χάλκινα σύρματα
- ADSL
Asymmetric Digital Subscriber Line
ασύμμετρη ψηφιακή γραμμή συνδρομητή
 - φορείς δεδομένων
 - χάλκινα σύρματα τηλεφωνικής γραμμής (Ελλάδα)
 - ομοαξονικά καλώδια καλωδιακής τηλεόρασης (αλλού...)
 - ταυτόχρονη μετάδοση αναλογικού και ψηφιακού σήματος

Καλωδιακές συνδέσεις

- ADSL:

διαφορετικές ταχύτητες download/upload
π.χ. 2048/256 kbps

- Ταχύτητα download με *30€/μήνα*

- Ελλάδα 1 Mbps

- Γαλλία 28 Mbps + 100 κανάλια tv +...

Ασύρματες συνδέσεις

- χρησιμοποιούνται κατάλληλοι πομποδέκτες
- Wi-Fi (Wireless Fidelity)
 - το πιο διαδεδομένο σύστημα σήμερα
 - βασίζεται στο πρότυπο IEEE 802.11
 - Εμβέλεια: 100 m
 - Μέγιστη ταχύτητα 54 Mbps
- Οι περισσότεροι φορητοί Η/Υ έχουν σήμερα Wi-Fi
- Με βάση το Wi-Fi μπορούν εύκολα να συσταθούν ασύρματα τοπικά δίκτυα (WLAN – Wireless LAN) τα οποία συνδέονται έπειτα στο Διαδίκτυο

Ασύρματες συνδέσεις

- Wireless Hotspots
περιοχές όπου προσφέρεται
ασύρματη πρόσβαση στο Διαδίκτυο
 - αεροδρόμια, δημόσιοι χώροι, café, εμπορικά κέντρα, ...
 - πολλές φορές είναι δωρεάν
 - Πανεπιστήμιο Ιωαννίνων:
 - κυλικείο Εστιών Β΄
 - βιβλιοθήκη
 - αναγνωστήριο Τμήματος Φυσικής
 - ...

Ασύρματες συνδέσεις

■ WiMax

- εμβέλεια μερικών χιλιομέτρων
- κάλυψη μεγάλων αποστάσεων
- δημιουργία μητροπολιτικών ασυρμάτων δικτύων

<http://www.awmn.net/?id=communities>

Δορυφορικές συνδέσεις

- Προσφέρονται σε ειδικές περιπτώσεις
 - απουσία επίγειας πρόσβασης
 - σε μέρη που μετακινούνται (π.χ. πλοία)
- Τρόποι σύνδεσης
 - μονόδρομη πολυεκπομπή (one-way multicast)
 - μονόδρομη με επίγεια επιστροφή (one-way with terrestrial return)
 - αμφίδρομη (two-way satellite access)

Συνδέσεις μέσω κινητής τηλεφωνίας

- Κινητή τηλεφωνία
 - βασίζεται στην μετάδοση ψηφιακού σήματος
 - εκτός των δεδομένων φωνής μπορεί να μεταδώσει και πακέτα δεδομένων
 - GPRS
General Packet Radio Services
- Πρόσβαση κινητών τηλεφώνων
 - στο WWW μέσω WAP
 - στο ηλεκτρονικό ταχυδρομείο μέσω IMAP

Συνδέσεις μέσω κινητής τηλεφωνίας

- Χρήση ενός κινητού ως modem
 - σύνδεση Η/Υ με το κινητό
 - καλώδιο USB
 - bluetooth
 - Σύνδεση στο Διαδίκτυο μέσω GPRS
- Μειονεκτήματα
 - ιδιαίτερα ακριβό
 - ιδιαίτερα αργό (~ 32 kbps)
ανάπτυξη νέων τεχνολογιών (π.χ. UMTS, HSDPA) → 1.5 Mbps

Υπηρεσίες του Διαδικτύου

- Απομακρυσμένες συσκευές
- Μεταφορά αρχείων
- Απομακρυσμένα τερματικά
- Ηλεκτρονικό ταχυδρομείο
- Εφαρμογές πραγματικού χρόνου
- Παγκόσμιος Ιστός – WWW
- Υπολογιστικό Πλέγμα – GRID
- ...

Υπηρεσίες του Διαδικτύου

Πρόσβαση σε απομακρυσμένες συσκευές

- δικτυακοί σκληροί δίσκοι
- δικτυακοί εκτυπωτές
- webcams
- ...
- Χρησιμοποιούμενες εφαρμογές
 - SAMBA
διασύνδεση υπηρεσιών αρχείων και εκτυπωτών
MS windows με άλλα λειτουργικά συστήματα
 - NFS (Network File System)
δικτυακό σύστημα αρχείων
 - AFS (Andrews' File System)
κι άλλο ένα δικτυακό σύστημα αρχείων

Υπηρεσίες του Διαδικτύου

Μεταφορά αρχείων

- FTP – File Transfer Protocol
 - client-server
 - μεταφορά αρχείων από/προς κάποιον εξυπηρετητή
 - δεν παρέχει ασφάλεια επικοινωνίας
 - συνήθως χρησιμοποιείται για τη λήψη ελεύθερου λογισμικού
 - θύρα TCP = 21
- Μπορεί να χρησιμοποιηθεί
 - από τη γραμμή εντολών
 - από φυλλομετρητές WWW
 - από γραφικές εφαρμογές (GUI) όπως το WS_FTP

Υπηρεσίες του Διαδικτύου

Μεταφορά αρχείων

```
ftp ftp.uoi.gr
Connected to ftp.uoi.gr.
220 ProFTPD 1.2.10 Server (NOC UOI ANONYMOUS FTP SERVER) [195.130.120.38]
User (ftp.uoi.gr:(none)): anonymous
331 Anonymous login ok, send your complete email address as your password.
Password:***
230 Anonymous access granted, restrictions apply.
ftp> cd /mirror/apache/httpd/docs/
250 CWD command successful
ftp> dir httpd-docs-*.en.*
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-rw-r-- 1 root root 3455650 Oct 16 2005 httpd-docs-2.0.54.en.pdf
-rw-rw-r-- 1 root root 1211788 Apr 27 2006 httpd-docs-2.0.58.en.chm
-rw-rw-r-- 1 root root 915363 Apr 27 2006 httpd-docs-2.0.58.en.maff.zip
-rw-rw-r-- 1 root root 711718 Apr 27 2006 httpd-docs-2.0.58.en.war
226 Transfer complete.
ftp: 654 bytes received in 0,00Seconds 654000,00Kbytes/sec.
ftp> get httpd-docs-2.0.54.en.pdf
200 PORT command successful
150 Opening ASCII mode data connection for httpd-docs-2.0.54.en.pdf (3455650 bytes)
226 Transfer complete.
ftp: 3532080 bytes received in 16,28Seconds 216,93Kbytes/sec.
ftp> bye
221 Goodbye.
```

Υπηρεσίες του Διαδικτύου

Μεταφορά αρχείων

- **SFTP** (secure FTP), **SCP** (secure copy)
 - client-server
 - μεταφορά αρχείων από/προς κάποιον εξυπηρετητή
 - παρέχει ασφάλεια επικοινωνίας μέσω της κρυπτογραφημένης μετάδοσης δεδομένων
 - βασίζονται στο πρωτόκολλο SSH (θύρα TCP 22) (secure shell)
- Η χρήση του SFTP μοιάζει με αυτή του FTP
- Η χρήση του SCP μοιάζει με το πρόγραμμα αντιγραφής cp
π.χ.
`scp /path/myfile.doc user@pc1.domain.gr:/path2/`
- Υπάρχουν και γραφικές εφαρμογές (GUI) για την πιο φιλική χρήση των πρωτοκόλλων αυτών, όπως π.χ. το WinSCP

Υπηρεσίες του Διαδικτύου

Απομακρυσμένα τερματικά

- ανάγκη πρόσβασης σε απομακρυσμένους Η/Υ
- χρήση σαν να ήταν κανείς άμεσα συνδεδεμένος
- Πρωτόκολλα / προγράμματα
 - TELNET
 - SSH
 - VNC
 - Remote desktop
 - ...

Υπηρεσίες του Διαδικτύου

Απομακρυσμένα τερματικά - TELNET

- TELetype NETwork
 - client-server
 - δεν παρέχει ασφάλεια → εγκαταλείπεται
 - χρησιμοποιείται για επικοινωνία με συσκευές
 - θύρα TCP = 23

Υπηρεσίες του Διαδικτύου

Απομακρυσμένα τερματικά - SSH

■ Secure SHell

- λειτουργεί όμοια με το TELNET
- παρέχει ασφάλεια μέσω κρυπτογραφημένης μετάδοσης δεδομένων
- θύρα TCP = 22
- επιτρέπει την ταυτόχρονη προώθηση δεδομένων πέραν αυτών του τερματικού, π.χ. του συστήματος γραφικών X11, μέσα από το ίδιο κανάλι SSH.

Υπηρεσίες του Διαδικτύου

Απομακρυσμένα τερματικά - VNC

- Virtual Network Computing
 - εφαρμογή GUI, client-server
 - διανομή της επιφάνειας εργασίας ενός Η/Υ (Α) σε έναν άλλο απομακρυσμένο (Β)
 - μετάδοση των γεγονότων πληκτρολογίου και ποντικιού από τον Β στον Α
 - ανανέωση της οθόνης γραφικών του Β όποτε υπάρχουν αλλαγές
- ο βασικός κώδικας του VNC είναι ελεύθερος
- διατίθενται πολλές δωρεάν εκδόσεις του (π.χ. <http://www.realvnc.com>)

Υπηρεσίες του Διαδικτύου

Απομακρυσμένα τερματικά – Remote desktop

- σύνδεση σε απομακρυσμένους Η/Υ που τρέχουν MS windows
- υπάρχουν servers μόνο για τα windows
- φιλοσοφία όμοια με αυτή του VNC
- υπάρχουν clients για όλα τα λειτουργικά συστήματα (π.χ. το rdesktop στο linux)

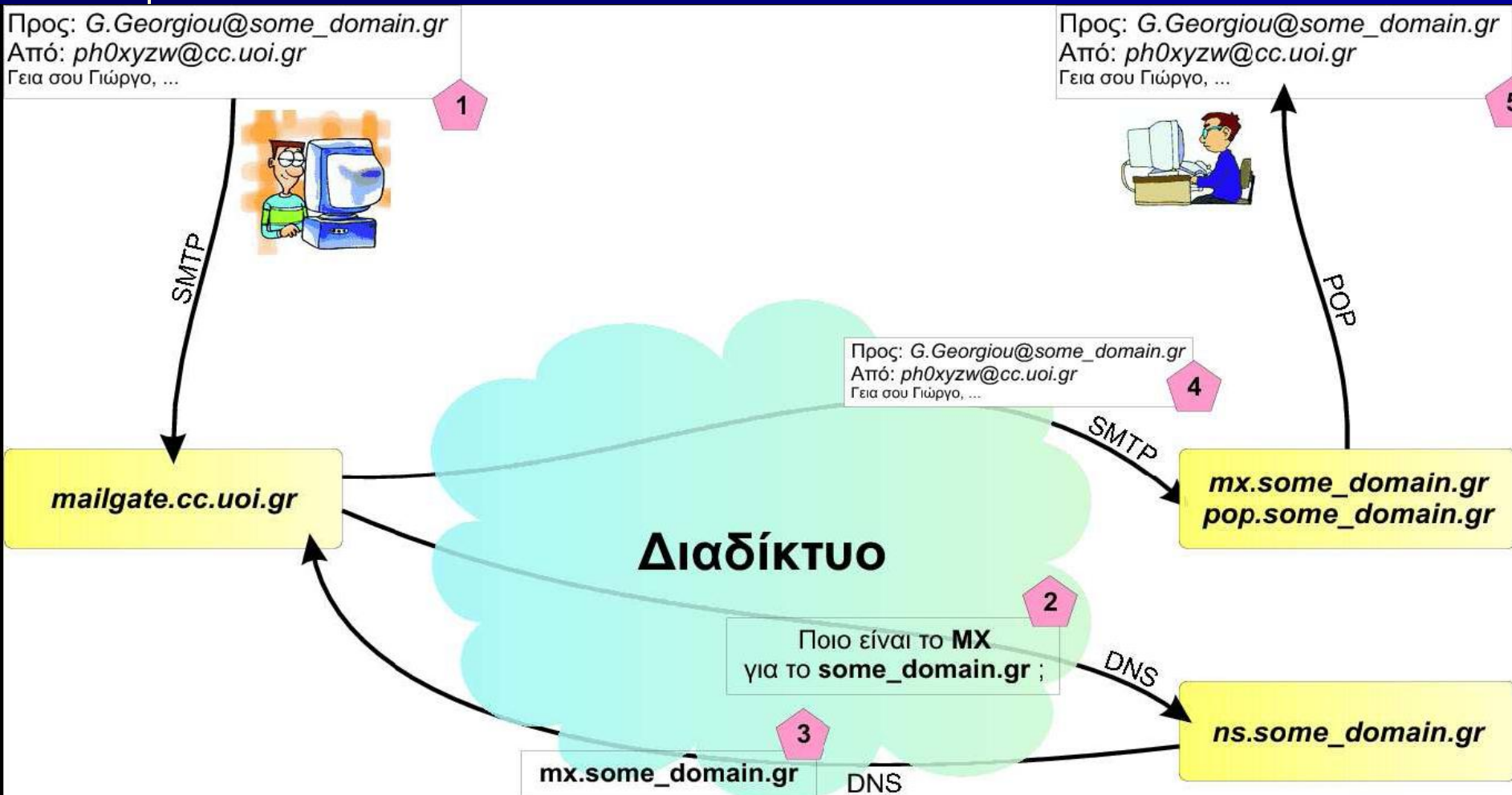
Υπηρεσίες του Διαδικτύου

Ηλεκτρονικό ταχυδρομείο

- e-mail ή email
- από τις κυριότερες εφαρμογές του διαδικτύου
- Αποστολή και λήψη μηνυμάτων
 - απλού κειμένου
 - μορφοποιημένου κειμένου (με HTML)
 - δυνατότητα επισύναψης αρχείων
- βασίζεται στο πρωτόκολλο SMTP
Simple Mail Transfer Protocol

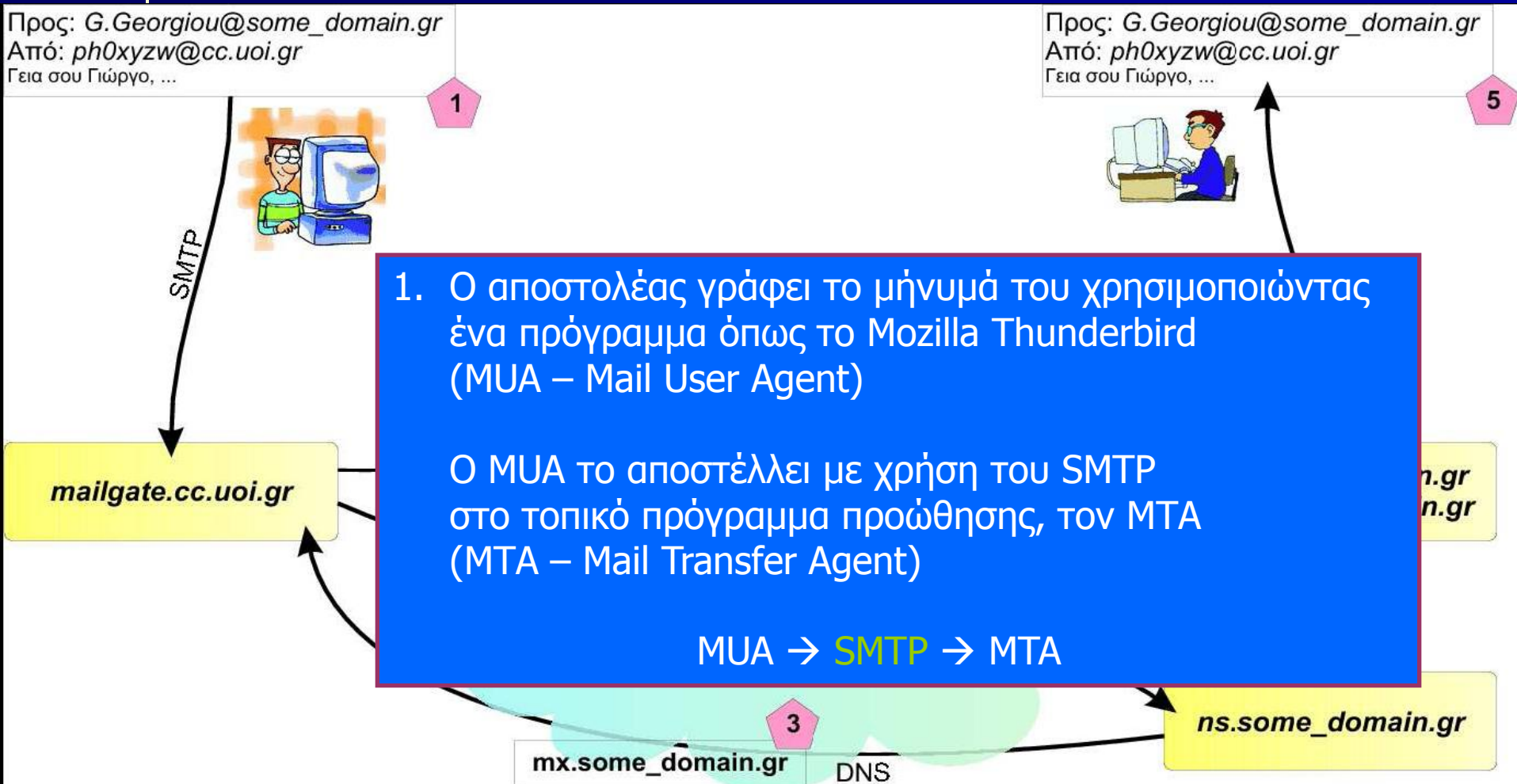
Υπηρεσίες του Διαδικτύου

Ηλεκτρονικό ταχυδρομείο



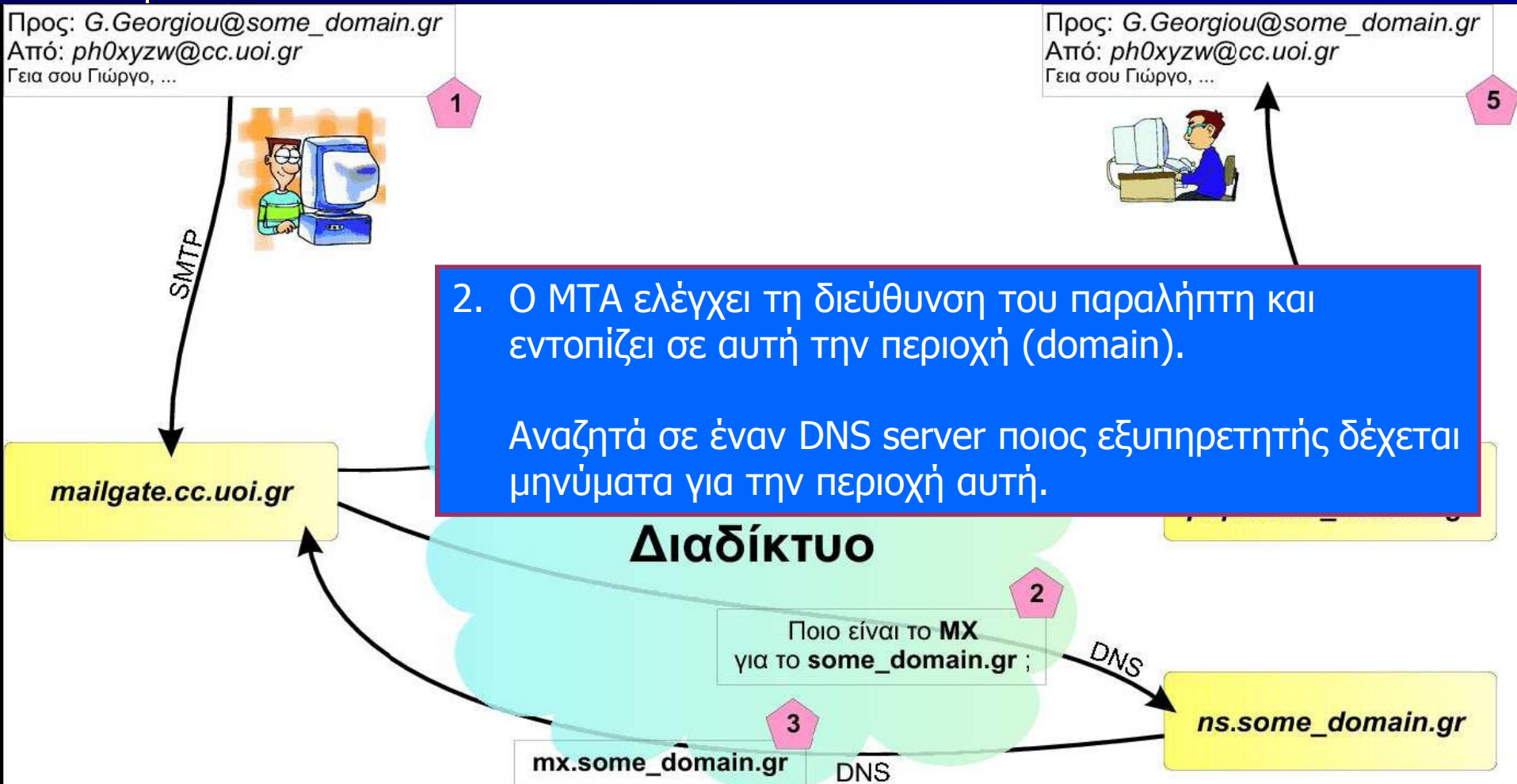
Υπηρεσίες του Διαδικτύου

Ηλεκτρονικό ταχυδρομείο



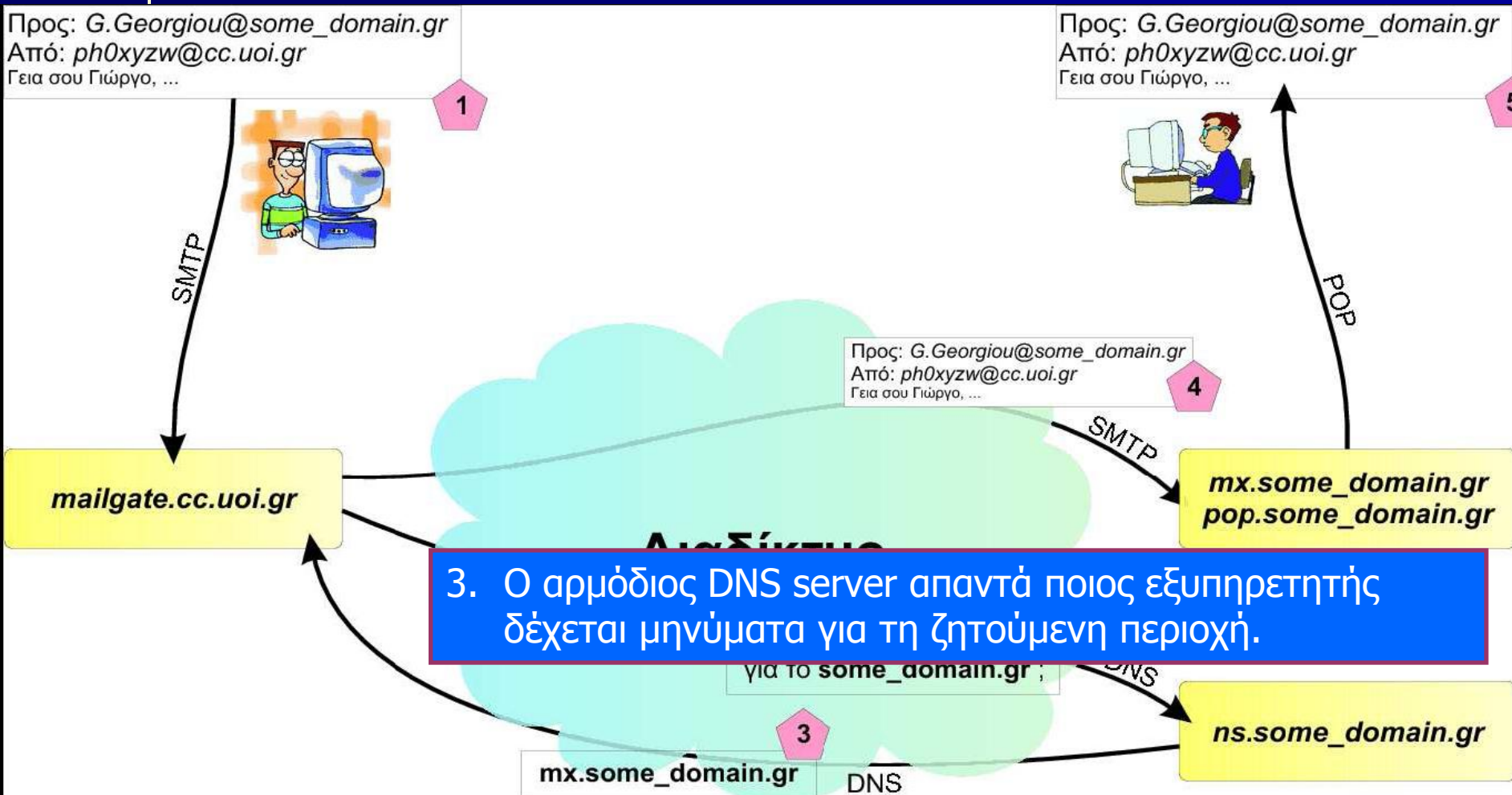
Υπηρεσίες του Διαδικτύου

Ηλεκτρονικό ταχυδρομείο



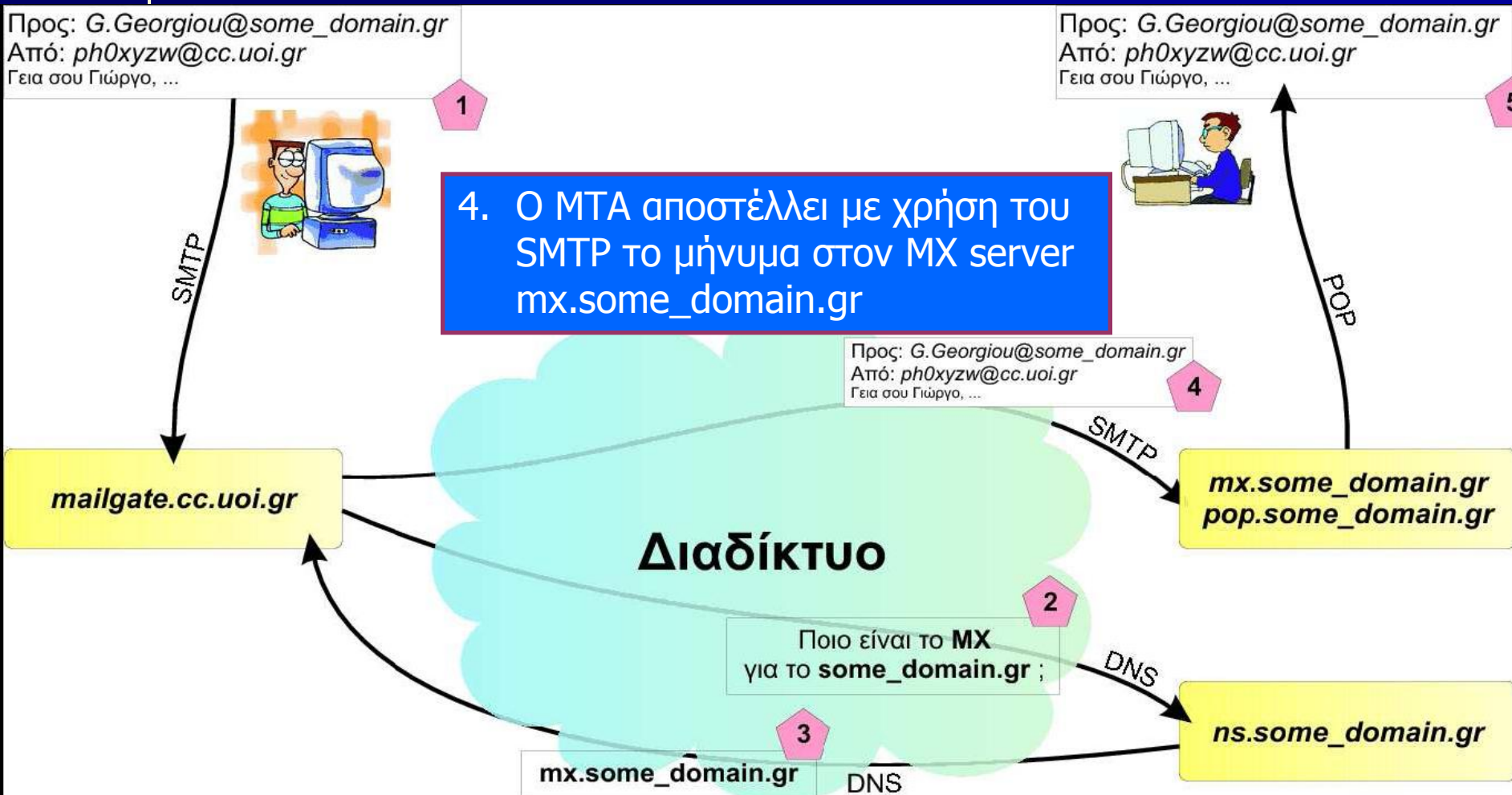
Υπηρεσίες του Διαδικτύου

Ηλεκτρονικό ταχυδρομείο



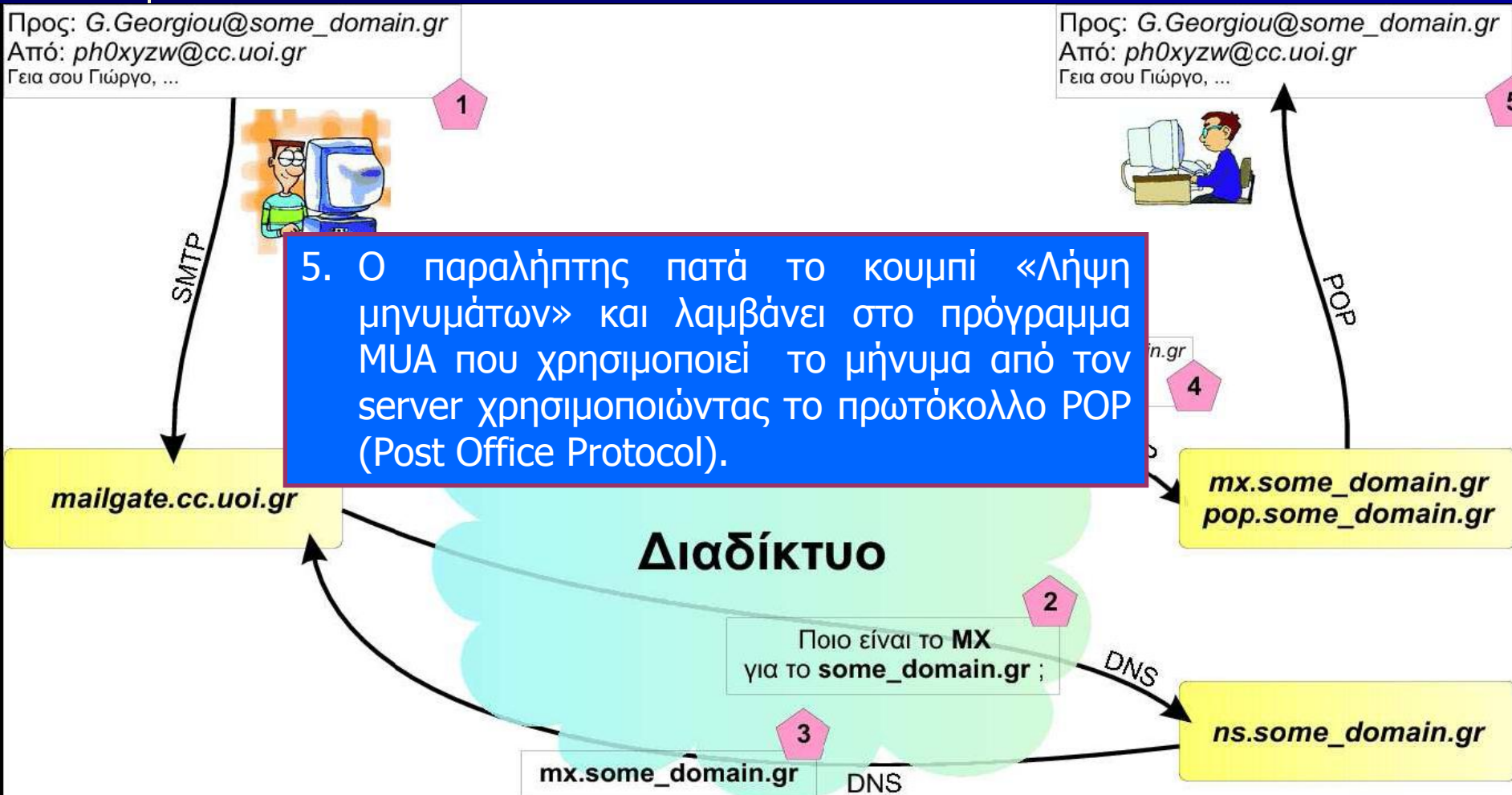
Υπηρεσίες του Διαδικτύου

Ηλεκτρονικό ταχυδρομείο



Υπηρεσίες του Διαδικτύου

Ηλεκτρονικό ταχυδρομείο



Υπηρεσίες του Διαδικτύου

Ηλεκτρονικό ταχυδρομείο

- MUA Mail User Agent
- SMTP Simple Mail Transfer Protocol
- MTA Mail Transfer Agent
- DNS Domain Name System
- MX Mail eXchange
- POP Post Office Protocol
- IMAP Internet Message Access Protocol

Υπηρεσίες του Διαδικτύου

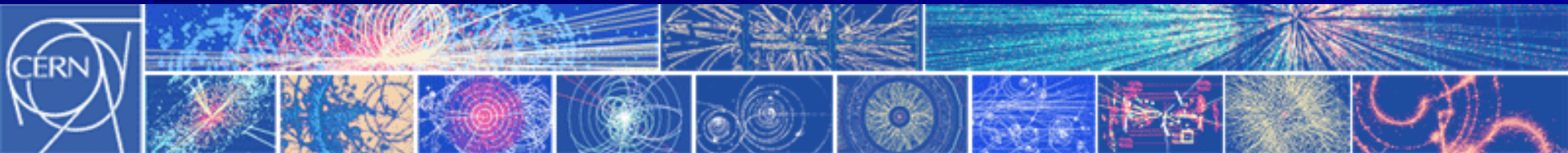
Εφαρμογές πραγματικού χρόνου

- real-time computing systems
 - περιορισμοί ως προς τη χρονική απόκριση
 - λογισμικό και υλικό ιδιαίτερων προδιαγραφών
- τηλεπικοινωνίες
 - Τηλεφωνία, τηλεδιασκέψεις
 - VoIP (Voice over IP)
 - Skype
 - VRVS, EVO
 - Διαδικτυακή τηλεόραση και ραδιόφωνο
- Ιατρική
 - παρακολούθηση ασθενών από απόσταση
 - εκτέλεση εγχειρήσεων από απόσταση
 - χρήση ρομπότ για την εγχείρηση
 - ο χειρουργός βλέπει σε μία οθόνη και χρησιμοποιεί χειριστήρια που κατευθύνουν το ρομπότ

Υπηρεσίες του Διαδικτύου

Παγκόσμιος Ιστός – WWW

- WorldWide Web
- World-Wide Web
- World Wide Web
- the Web



Γεννήθηκε στο **CERN** το 1990

<http://info.cern.ch>

Αποτελεί την κυριότερη εφαρμογή του Διαδικτύου

Υπηρεσίες του Διαδικτύου

Παγκόσμιος Ιστός – WWW

- Σύστημα αλληλοσυνδεόμενων αρχείων υπερ-κειμένου (hypertext)
- Ιστοσελίδες
 - εμφάνιση με φυλλομετρητές (browsers)
 - περιέχουν
 - μορφοποιημένο κείμενο (HTML)
 - εικόνες
 - πολυμέσα
 - υπερσυνδέσμους (hyperlinks)

Υπηρεσίες του Διαδικτύου

Πλέγμα – GRID

- GRID: ένα βήμα πέρα από τον Ιστό
- Εκτός από πληροφορίες, οι χρήστες έχουν πρόσβαση και σε άλλους πόρους
 - σε υπολογιστική ισχύ
 - σε αποθηκευτικούς πόρους
 - σε δικτυακές συσκευές
 - σε ανιχνευτές, συσκευές λήψης δεδομένων, ...

Υπηρεσίες του Διαδικτύου

Πλέγμα – GRID

- Ένας χρήστης «βλέπει» το GRID σαν **έναν** υπερυπολογιστή
- Επιμέρους κατηγορίες
 - υπολογιστικά πλέγματα (computational grids)
 - πλέγματα δεδομένων (data grids)
 - πλέγματα εξοπλισμού (equipment grids)

Υπηρεσίες του Διαδικτύου

Πλέγμα – GRID

- **EGEE**

όταν ξεκίνησε:

Enabling Grids for E-science in Europe

τώρα πια αποτελεί παγκόσμια συνεργασία:

Enabling Grids for E-science

- Η Ελλάδα είναι μέλος του EGEE-SEE (EGEE – South Eastern Europe)

- Στο εργαστήριο ΦΥΕ του Τμήματος Φυσικής είναι υπό κατασκευή ένας κόμβος GRID που σύντομα θα συνδεθεί στο Πλέγμα

Ασφάλεια στο Διαδίκτυο

- Τα περισσότερα πρωτόκολλα που είδαμε έως τώρα δεν εξασφαλίζουν το απόρρητο
 - δυνατότητα υποκλοπής πακέτων κατά τη δρομολόγησή τους από τρίτους
- Ανάγκη ανάπτυξης πρωτοκόλλων που εξασφαλίζουν το απόρρητο της επικοινωνίας

Ασφάλεια στο Διαδίκτυο

πρωτόκολλο TLS/SSL

- Κρυπτογραφικά πρωτόκολλα
 - SSL – Secure Sockets Layer
 - TLS – Transport Layer Security
- Χρησιμοποιούνται ως ενδιάμεσα πρωτόκολλα μεταξύ του επιπέδου εφαρμογών και του επιπέδου μεταφοράς

Ασφάλεια στο Διαδίκτυο

πρωτόκολλο TLS/SSL

- TLS v1.0
 - βασίζεται στο SSL v3.0,
με το οποίο είναι ουσιαστικά ίδιο
οπότε αναφέρεται ως **TLS/SSL**
- client – server
- Συνήθως γίνεται έλεγχος της ταυτότητας του εξυπηρετητή
 - ο πελάτης γνωρίζει με ποιον έχει συνδεθεί
 - η επικοινωνία είναι κρυπτογραφημένη

Ασφάλεια στο Διαδίκτυο

πρωτόκολλο TLS/SSL

- Σε ανώτερο επίπεδο ασφαλείας, έλεγχος τόσο της ταυτότητας του πελάτη όσο και του εξυπηρετητή
 - γίνεται με τη χρήση της υποδομής PKI
Public Key Infrastructure

Ασφάλεια στο Διαδίκτυο

πρωτόκολλο TLS/SSL

- λειτουργία σε τρεις φάσεις
 - διαπραγμάτευση για τους υποστηριζόμενους αλγορίθμους
 - ανταλλαγή κλειδιών
 - κρυπτογράφηση δημοσίου κλειδιού (public key encryption)
 - αυθεντικότητα βασισμένη σε πιστοποιητικά
 - ανταλλαγή κρυπτογραφημένων δεδομένων
 - κρυπτογράφηση συμμετρικής φράσης (symmetric cipher)

Ασφάλεια στο Διαδίκτυο

πρωτόκολλο **TLS/SSL**

- Μπορεί να χρησιμοποιηθεί από οποιοδήποτε πρωτόκολλο εφαρμογής πριν το πρωτόκολλο μεταφοράς (π.χ. TCP)
- Συνήθως χρησιμοποιείται σε συνδυασμό με το HTTP:
HTTPS (secure HTTP) = HTTP + TLS/SSL