Diritto dell'Informatica

Modulo Tecnico

A.A. 2014-2015

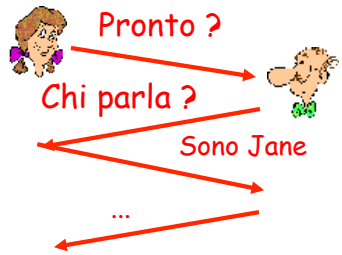
Melchiorre Monaca
melchiorre.monaca@unirc.it

Reti di Telecomunicazione

- Le reti di telecomunicazione
- Internet
- Il web
- Applicazioni

I problemi da risolvere

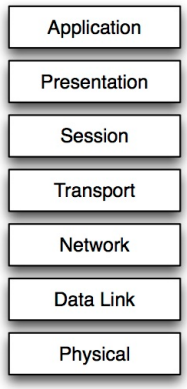
Facciamo una telefonata



Scomponiamo il problema

- Collegamento fisico
- Indirizzamento
- Instradamento
- Trasporto dei dati
- Gestione della connessione
- Servizi

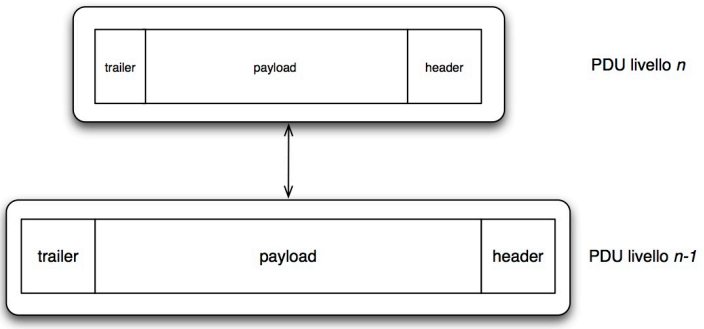
Il modello ISO/OSI



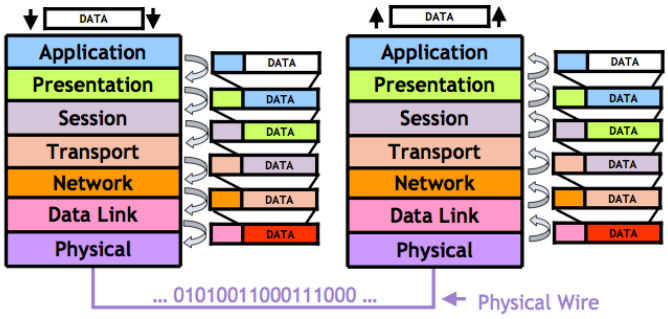
Incapsulamento

- Tante “buste”
- Header
- Payload
- Protocol Data Unit (PDU)
- Ogni livello gestisce l’header di sua competenza

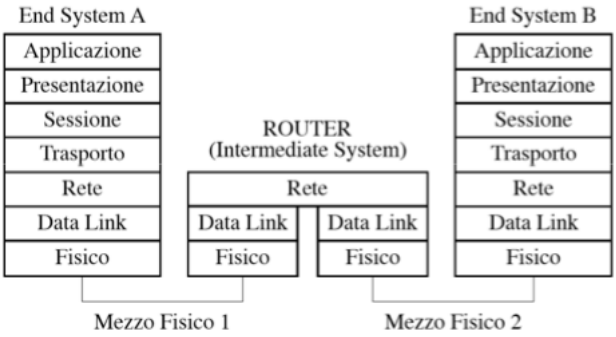
Incapsulamento



Il modello ISO/OSI

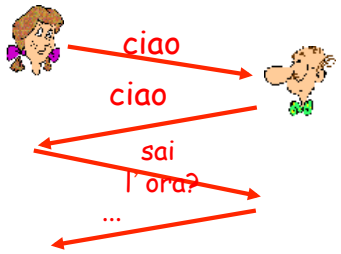


Il modello ISO/OSI



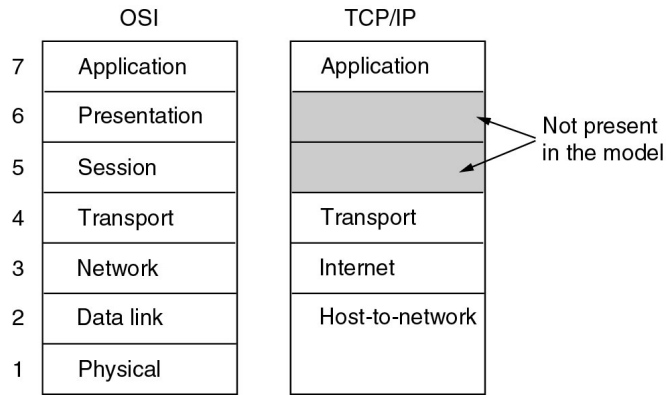
I Protocolli

Conversazione



Connessione di rete

Il TCP/IP



Livello fisico: il mezzo trasmissivo

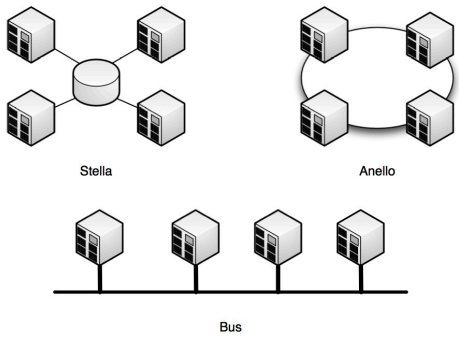
- Cavo elettrico
- Onde radio
- Fibra ottica
- Laser

Classifichiamo

- PAN (Personal area network)
- LAN (Local area network)
- MAN (metropolitan area network)
- WAN (wide area network)

Livello fisico: topologia

- Point to Point
  - Stella
  - Anello
- Broadcast
  - Bus

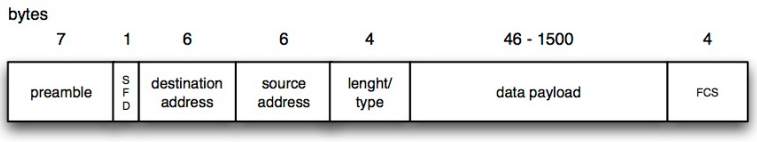


Livello Data Link

- Frammentazione
- Indirizzamento
- Controllo dell'errore
- Controllo di flusso

Livello Data Link: Ethernet

- Frame
- MAC ADDRESS



Livello Network

- Indirizzamento
- Routing
- Internetworking

Livello Network: IP

- Indirizzi IP
- Sottoreti
- Classi di Indirizzi
- Unicast, Broadcast, Multicast

Livello Network: IP

- Indirizzo host 1.2.3.4
  00000001.00000010.00000011.00000100
- Indirizzo network 1.2.3.0
  00000001.00000010.00000011.00000000
- Indirizzo broadcast 1.2.3.255
  00000001.00000010.00000011.11111111
- NetMask 255.255.255.0
  11111111. 11111111. 11111111. 00000000

Livello Network: IP

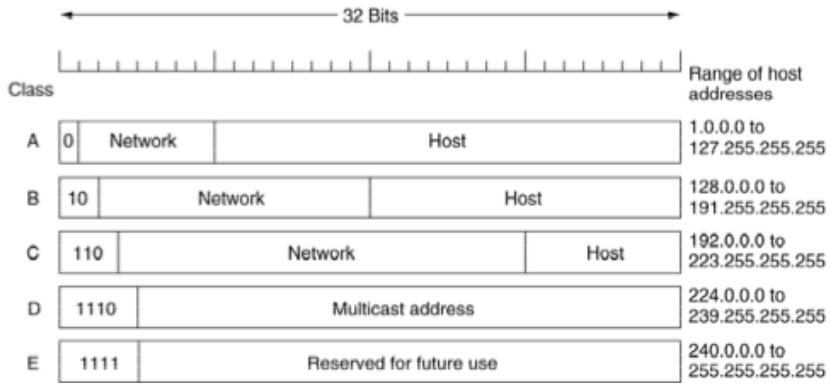
- Ind. host 1.2.3.4 AND netmask 255.255.255.0

  00000001.00000010.00000011.00000100
  AND
  11111111.11111111.11111111.00000000

- Si ottiene indirizzo network 1.2.3.0

  00000001.00000010.00000011.00000000

Livello Network: IP - classi



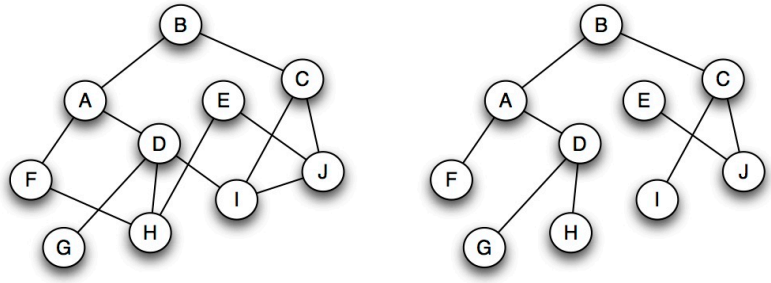
Livello Network: IP – indirizzi privati

Class	First address	Last address	How many
A	10.0.0.0	10.255.255.255	16.777.216
B	172.16.0.0	172.31.255.255	1.048.576
C	192.168.0.0	192.168.255.255	65.536

Livello Network: Routing

- Principio di ottimalità
- Routing statico
- Routing dinamico

Livello Network: Routing



Livello Network: Routing

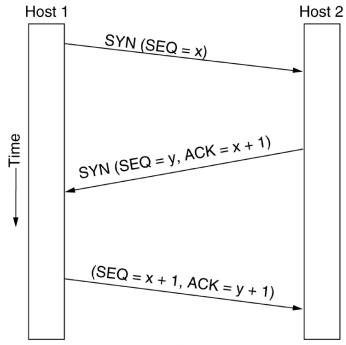
```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.167.111.254 to network 0.0.0.0

O    192.168.106.0/24 [110/2] via 192.167.111.12, 00:28:49, FastEthernet0/1
O    192.167.106.0/24 [110/2] via 192.167.111.12, 00:28:49, FastEthernet0/1
O    192.168.12.0/24 [110/11] via 192.167.111.254, 00:28:49, FastEthernet0/1
O    192.168.13.0/24 [110/11] via 192.167.111.254, 00:28:49, FastEthernet0/1
O    192.168.104.0/24 [110/2] via 192.167.111.16, 00:28:49, FastEthernet0/1
O    192.167.104.0/24 [110/2] via 192.167.111.16, 00:28:49, FastEthernet0/1
O    192.168.31.0/24 [110/28] via 192.167.111.254, 00:28:49, FastEthernet0/1
O    192.168.105.0/24 [110/2] via 192.167.111.16, 00:28:49, FastEthernet0/1
O    192.167.105.0/24 [110/2] via 192.167.111.16, 00:28:49, FastEthernet0/1
O    192.168.8.0/24 [110/25] via 192.167.111.254, 00:28:49, FastEthernet0/1
O    192.168.110.0/24 [110/2] via 192.167.111.16, 00:28:49, FastEthernet0/1
O    192.167.110.0/24 [110/2] via 192.167.111.96, 00:28:49, FastEthernet0/1
     192.168.111.0/30 is subnetted, 6 subnets
C       192.168.111.4 is directly connected, Serial0/0.1
O       192.168.111.0 [110/24] via 192.167.111.254, 00:28:49, FastEthernet0/1
O       192.168.111.12 [110/24] via 192.167.111.254, 00:28:49, FastEthernet0/1
O       192.168.111.8 [110/24] via 192.167.111.254, 00:28:49, FastEthernet0/1
O       192.168.111.16 [110/24] via 192.167.111.254, 00:28:49, FastEthernet0/1
O       192.168.111.96 [110/24] via 192.167.111.254, 00:28:49, FastEthernet0/1
C    192.167.111.0/24 is directly connected, FastEthernet0/1
O    192.167.108.0/24 [110/2] via 192.167.111.20, 00:28:58, FastEthernet0/1
C    192.168.109.0/24 is directly connected, FastEthernet0/0
C    192.167.109.0/24 is directly connected, FastEthernet0/0
......
```

Livello Transport

- Controllo della connessione
  - Connection less (UDP)
  - Connection oriented (TCP)
- Controllo di flusso
- Riordino dei TPDU

Livello Transport: TCP

- Three-way handshake



Livello Transport: TCP

- Socket

Port	Protocol	Use
21	FTP	File transfer
23	Telnet	Remote login
25	SMTP	E-mail
69	TFTP	Trivial File Transfer Protocol
79	Finger	Lookup info about a user
80	HTTP	World Wide Web
110	POP-3	Remote e-mail access
119	NNTP	USENET news

Applicazioni

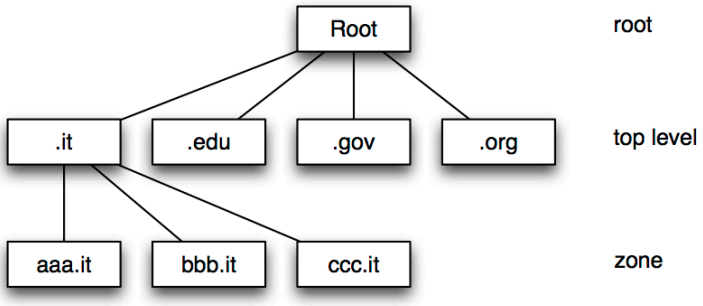
- Dns
- Web
- E-MAIL
- Motori di ricerca
- Content delivery
- Peer to Peer
- Ip Telephony e Videoconferenza
- Chat
- Streaming

DNS – The Domain Name System

- The DNS Name Space
- Resource Records
- Name Servers

The DNS Name Space

A sample of the Internet domain name space.



Resource Records

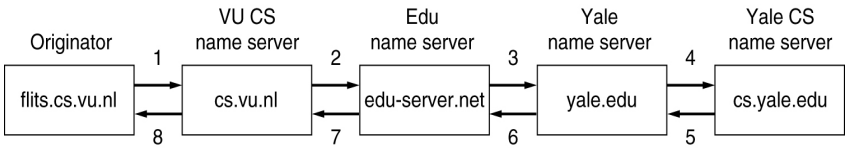
The principal DNS resource records types.

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

Resource Records (2)

```
; Authoritative data for cs.vu.nl
cs.vu.nl.          86400  IN  SOA     star boss (952771,7200,7200,2419200,86400)
cs.vu.nl.          86400  IN  TXT     "Divisie Wiskunde en Informatica."
cs.vu.nl.          86400  IN  TXT     "Vrije Universiteit Amsterdam."
cs.vu.nl.          86400  IN  MX      1 zephyr.cs.vu.nl.
cs.vu.nl.          86400  IN  MX      2 top.cs.vu.nl.

flits.cs.vu.nl.    86400  IN  HINFO   Sun Unix
flits.cs.vu.nl.    86400  IN  A       130.37.16.112
flits.cs.vu.nl.    86400  IN  A       192.31.231.165
flits.cs.vu.nl.    86400  IN  MX      1 flits.cs.vu.nl.
flits.cs.vu.nl.    86400  IN  MX      2 zephyr.cs.vu.nl.
flits.cs.vu.nl.    86400  IN  MX      3 top.cs.vu.nl.
www.cs.vu.nl.      86400  IN  CNAME   star.cs.vu.nl
ftp.cs.vu.nl.      86400  IN  CNAME   zephyr.cs.vu.nl

rowboat                   IN  A       130.37.56.201
                          IN  MX      1 rowboat
                          IN  MX      2 zephyr
                          IN  HINFO   Sun Unix

little-sister             IN  A       130.37.62.23
                          IN  HINFO   Mac MacOS

laserjet                  IN  A       192.31.231.216
                          IN  HINFO   "HP Laserjet IIISi" Proprietary
```

Name Servers (2)



How a resolver looks up a remote name in eight steps.

Electronic Mail

- Architecture and Services
- The User Agent
- Message Formats
- Message Transfer
- Final Delivery

Electronic Mail (2)

Some smileys. They will not be on the final exam :-).

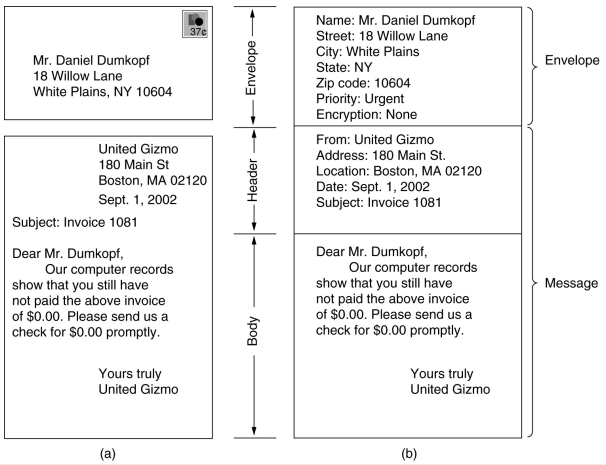
Smiley	Meaning	Smiley	Meaning	Smiley	Meaning
:-)	I'm happy	=|:-)	Abe Lincoln	:+)	Big nose
:-(	I'm sad/angry	=):-)	Uncle Sam	:-))	Double chin
:-|	I'm apathetic	*<:-)	Santa Claus	:-{)	Mustache
;-)	I'm winking	<:-(	Dunce	#:-)	Matted hair
:-(O)	I'm yelling	(-:	Australian	8-)	Wears glasses
:-(*)	I'm vomiting	:-)X	Man with bowtie	C:-)	Large brain

E-Mail Architecture and Services

Basic functions

- Composition
- Transfer
- Reporting
- Displaying
- Disposition

The User Agent



Reading E-mail

Reading E-mail

```
Return-Path: it_it_ndt_bounces@insideapple.apple.com
Received: from mta.unime.it (LHLO mta.unime.it) (192.167.101.20) by
 mail1.unime.it with LMTP; Wed, 14 Mar 2012 08:52:02 +0100 (CET)
Received: from localhost (localhost [127.0.0.1])
     by mta.unime.it (Postfix) with ESMTP id 3D6E6120DA912
     for <monaca@unime.it>; Wed, 14 Mar 2012 08:52:02 +0100 (CET)
X-Spam-Flag: NO
X-Spam-Score: -1.313
X-Spam-Level:
X-Spam-Status: No, score=-1.313 tagged_above=-10 required=10 tests=[AWL=0.689,
     BAYES_00=-2.599, HTML_IMAGE_RATIO_06=0.001, HTML_MESSAGE=0.001,
     SPF_HELO_PASS=-0.001, SPF_SOFTFAIL=0.596]
Received: from mta.unime.it ([127.0.0.1])
     by localhost (mta.unime.it [127.0.0.1]) (amavisd-new, port 10024)
     with ESMTP id ibJHXOPT9FCg for <monaca@unime.it>;
     Wed, 14 Mar 2012 08:52:00 +0100 (CET)
Received: from smtp1.unime.it (smtp.unime.it [192.167.101.11])
     by mta.unime.it (Postfix) with ESMTP id 6FB7712090C1A
     for <melchiorre.monaca@unime.it>; Wed, 14 Mar 2012 08:52:00 +0100 (CET)
Received: from smtp1.unime.it (localhost.localdomain [127.0.0.1])
     by localhost (Email Security Appliance) with SMTP id 5AD98101E47C_F604E20B
     for <melchiorre.monaca@unime.it>; Wed, 14 Mar 2012 07:52:00 +0000 (GMT)
Received: from msbadger0102.apple.com (msbadger0102.apple.com [17.254.6.109])
     by smtp1.unime.it (Sophos Email Appliance) with ESMTP id 2EAAD1018AB5_F604E1EF
     for <melchiorre.monaca@unime.it>; Wed, 14 Mar 2012 07:51:57 +0000 (GMT)
DKIM-Signature: v=1; a=rsa-sha1; d=new.itunes.com; s=itunes; c=relaxed/simple;
     q=dns/txt; i=@new.itunes.com; t=1331711517;
     h=From:Subject:Date:To:MIME-Version:Content-Type;
     bh=cdEntTColDlRPDGUy0el70w60k4=;
     b=RMIKXvkLn1BFm6uyqeBbInpD3XJmQL8TxGPMlDQj9nrEb5kPKFEHK//DtNcd0fnX
     mH7VOcnDyRFFIEmpZEyN4g==;
Date: Wed, 14 Mar 2012 00:51:57 -0700
From: iTunes <itunes_it@new.itunes.com>
To: melchiorre.monaca@unime.it
```

Message Formats – RFC 822

RFC 822 header fields

Header	Meaning
To:	E-mail address(es) of primary recipient(s)
Cc:	E-mail address(es) of secondary recipient(s)
Bcc:	E-mail address(es) for blind carbon copies
From:	Person or people who created the message
Sender:	E-mail address of the actual sender
Received:	Line added by each transfer agent along the route
Return-Path:	Can be used to identify a path back to the sender

Message Formats – RFC 822 (2)

Header	Meaning
Date:	The date and time the message was sent
Reply-To:	E-mail address to which replies should be sent
Message-Id:	Unique number for referencing this message later
In-Reply-To:	Message-Id of the message to which this is a reply
References:	Other relevant Message-Ids
Keywords:	User-chosen keywords
Subject:	Short summary of the message for the one-line display

MIME – Multipurpose Internet Mail Extensions

Problems with international languages:

- Languages with accents (French, German).
- Languages in non-Latin alphabets (Hebrew, Russian).
- Languages without alphabets (Chinese, Japanese).
- Messages not containing text at all (audio or images).

MIME (2)

RFC 822 headers added by MIME.

Header	Meaning
MIME-Version:	Identifies the MIME version
Content-Description:	Human-readable string telling what is in the message
Content-Id:	Unique identifier
Content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Type:	Type and format of the content

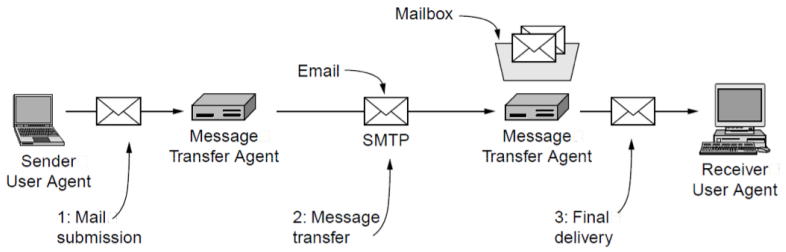
MIME (3)

Type	Subtype	Description
Text	Plain	Unformatted text
	Enriched	Text including simple formatting commands
Image	Gif	Still picture in GIF format
	Jpeg	Still picture in JPEG format
Audio	Basic	Audible sound
Video	Mpeg	Movie in MPEG format
Application	Octet-stream	An uninterpreted byte sequence
	Postscript	A printable document in PostScript
Message	Rfc822	A MIME RFC 822 message
	Partial	Message has been split for transmission
	External-body	Message itself must be fetched over the net
Multipart	Mixed	Independent parts in the specified order
	Alternative	Same message in different formats
	Parallel	Parts must be viewed simultaneously
	Digest	Each part is a complete RFC 822 message

MIME (4)

```
From: elinor@abcd.com
To: carolyn@xyz.com
MIME-Version: 1.0
Message-Id: <0704760941.AA00747@abcd.com>
Content-Type: multipart/alternative; boundary=qwertyuiopasdfghjklzxcvbnm
Subject: Earth orbits sun integral number of times

This is the preamble. The user agent ignores it. Have a nice day.

--qwertyuiopasdfghjklzxcvbnm
Content-Type: text/enriched

Happy birthday to you
Happy birthday to you
Happy birthday dear <bold> Carolyn </bold>
Happy birthday to you

--qwertyuiopasdfghjklzxcvbnm
Content-Type: message/external-body;
        access-type="anon-ftp";
        site="bicycle.abcd.com";
        directory="pub";
        name="birthday.snd"

content-type: audio/basic
content-transfer-encoding: base64
--qwertyuiopasdfghjklzxcvbnm--
```

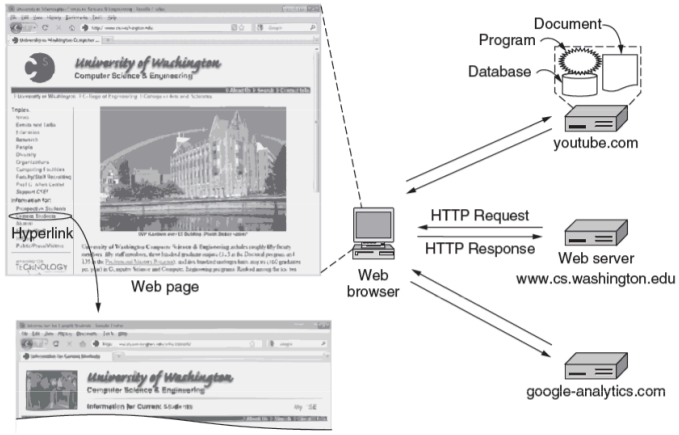
E-mail Delivery



Fetch E-mail

- POP 3
- IMAP

The World Wide Web



URLs – Uniform Resource Locators

Some common URLs.

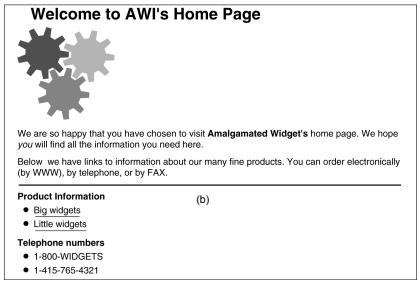
Name	Used for	Example
http	Hypertext (HTML)	http://www.cs.vu.nl/~ast/
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
file	Local file	file:///usr/suzanne/prog.c
news	Newsgroup	news:comp.os.minix
news	News article	news:AA0134223112@cs.utah.edu
gopher	Gopher	gopher://gopher.tc.umn.edu/11/Libraries
mailto	Sending e-mail	mailto:JohnUser@acm.org
telnet	Remote login	telnet://www.w3.org:80

HTML

- HyperText Markup Language

```
<html>
<head><title> AMALGAMATED  WIDGET, INC. </title> </head>
<body> <h1> Welcome to AWI's Home Page</h1>
<img src="http://www.widget.com/images/logo.gif" ALT="AWI Logo"> <br>
We are so happy that you have chosen to visit <b> Amalgamated Widget's </b>
home page.We hope <i> you </i> will find all the information you need here.
<p>Below we have links to information about our many fine products.
You can order electronically (by WWW), by telephone, or by fax. </p>
<hr>
<h2> Product information </h2>
<ul>
   <li> <a href="http://widget.com/products/big"> Big widgets </a>
   <li> <a href="http://widget.com/products/little"> Little widgets </a>
</ul>
<h2> Telephone numbers</h2>
<ul>
   <li> By telephone: 1-800-WIDGETS
   <li> By fax: 1-415-765-4321
</ul>
</body>
</html>
```

(a)

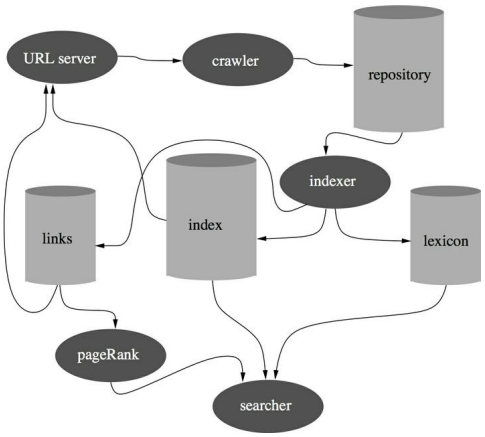


(b)

HTML (2)

Tag	Description
<html> ... </html>	Declares the Web page to be written in HTML
<head> ... </head>	Delimits the page's head
<title> ... </title>	Defines the title (not displayed on the page)
<body> ... </body>	Delimits the page's body
<h *n*> ... </h*n*>	Delimits a level *n* heading
...	Set ... in boldface
...	Set ... in italics
...	Center ... on the page horizontally
...	Brackets an unordered (bulleted) list
...	Brackets a numbered list
	Starts a list item (there is no)
 	Forces a line break here
<p>	Starts a paragraph
<hr>	Inserts a Horizontal rule
<img src="...">	Displays an image here
 ... 	Defines a hyperlink

Search Engines



Sicurezza

- **Integrità**
  - protezione da modifiche (o cancellazioni) non autorizzate dei dati trasmessi
  - garantire l'integrità di un messaggio significa assicurare che il messaggio ricevuto sia esattamente quello spedito dal mittente.
- **Autenticazione**
  - chi sei? Possibilità di identificare in modo certo e univoco chi invia e riceve i dati
  - può essere semplice (solo mittente) o mutua (sia mittente che destinatario)
- **Non ripudio**
  - prova formale, utilizzabile anche a termine di legge, per dimostrare che una certa persona ha sottoscritto (firmato) un documento

- **Integrità e autenticazione sono condizioni necessarie per garantire che mittente e destinatario non possano negare di aver inviato e ricevuto il documento firmato**

Sicurezza

- **Autorizzazione**
  - cosa puoi fare?
  - capacità di controllare le operazioni che un utente autenticato può effettuare e le risorse a cui può accedere
- **Riservatezza**
  - protezione da letture non autorizzate dei dati
  - ha lo scopo di impedire l'utilizzo illegittimo di informazioni riservate
- **Disponibilità**
  - capacità di garantire l'accesso all'infrastruttura e la fruizione dei servizi agli utenti autorizzati

Attacchi alla sicurezza

- **Attacchi passivi**
  - Obiettivo: entrare in possesso di informazioni riservate
  - Compromettono la riservatezza e l'autenticazione
  - È più facile intervenire con la prevenzione che rilevarne la presenza
- **Attacchi attivi**
  - Obiettivo: alterare le informazioni e/o danneggiare le risorse
  - Compromettono l'integrità e la disponibilità
  - Molto spesso gli attacchi passivi sono effettuati per ottenere le informazioni necessarie a iniziare un attacco attivo

Attacchi alla sicurezza

- **Attacchi passivi**
  - Mapping e port scanning (esplorazione della rete)
  - Sniffing (analisi del traffico)
- **Attacchi attivi**
  - Spoofing (sostituzione)
  - Exploit (sfruttamento di software bug)
  - Malicious software
  - DoS: Denial of Service (negazione del servizio)
  - Phishing

Mapping e port scanning

Obiettivo: determinare quali sono gli host attivi in una rete e quali sono i servizi offerti

- **Mapping**
  - ricostruzione di quali sono gli indirizzi IP attivi di una stessa rete
  - Es. Uso del ping o di altre utility per l'esplorazione di una rete
- **Port scanning**
  - Contatto sequenziale dei numeri di porta di uno stesso host per vedere cosa succede
  - I numeri di porta sono contattati sia con segmenti TCP (es. con telnet) che con segmenti UDP
  - Es. Uso di telnet o di di altre utility per la scansione delle porte

Sniffing

- **Lettura dei pacchetti destinati ad un altro nodo della rete**
  - Quando i dati viaggiano su una rete a mezzo condiviso (come sono tipicamente le LAN) è possibile da un qualsiasi punto della rete intercettare i pacchetti in transito destinati ad altri host
- **L'intercettazione dei dati è fatta attraverso appositi programmi, detti sniffer, che:**
  - mettono la scheda di rete Ethernet in modalità promiscua
  - convertono i dati raccolti in una forma leggibile ricostruendo i pacchetti dei protocolli di livello più alto
  - filtrano i pacchetti in base a criteri definibili dall'utente

User account spoofing

- **L'identità elettronica degli utenti può essere sostituita intercettando le credenziali di autenticazione**
  - sia al di fuori del sistema (social enginering)
  - sia sfruttando vulnerabilità dei sistemi interni (malware)
  - sia mentre queste credenziali transitano sulla rete
- **I problemi più gravi si hanno**
  - quando l'abuso produce gravi violazioni alle norme vigenti
  - quando l'abuso avviene in un contesto commerciale e dà origine a obblighi per la persona la cui identità è stata utilizzata impropriamente
  - quando viene carpita l'identità dell'amministratore del sistema
- **Sono colpiti: l'autenticazione, l'integrità, il non ripudio e la riservatezza**

Address spoofing

- **IP spoofing**
  - Falsificazione dell'indirizzo di rete del mittente
  - Il sistema che effettua l'attacco si spaccia per un diverso IP
  - Il sistema che subisce l'attacco invia le risposte all'host effettivamente corrispondente all'IP utilizzato per lo spoofing
- **DNS spoofing**
  - Falsificazione del nome simbolico
  - La richiesta di una pagina web o di un altro servizio è fatta al fornitore sbagliato
  - Basato sulla modifica del DNS server a cui la vittima si rivolge (direttamente o indirettamente)

Data spoofing

- **Alterazione dei dati nel corso di una comunicazione**
  - Si utilizza uno dei meccanismi di spoofing precedentemente descritti
  - Si prende il controllo di un canale di comunicazione e su questo si inseriscono, cancellano o modificano dei pacchetti

Malicious software

- **Virus**
  - pezzo di codice in grado di riprodursi nel sistema, attaccandosi ai programmi già esistenti, agli script, sostituendosi al settore di avvio di un disco o di una partizione, o inserendosi all'interno di file di dati che prevedono la presenza di macro istruzioni
- **Worm**
  - programmi che utilizzano i servizi di rete per propagarsi da un sistema all'altro programma ospite
- **Cavalli di Troia**
  - programmi apparentemente innocui che una volta eseguiti, effettuano operazioni diverse da quelle per le quali l'utente li aveva utilizzati e tipicamente dannose

Phishing

- **truffa** via Internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili
  - attività illegale che sfrutta una tecnica di ingegneria sociale
  - attraverso l'invio casuale di messaggi di posta elettronica che imitano la grafica di siti bancari o postali, un malintenzionato cerca di ottenere dalle vittime la password di accesso al conto corrente, le password che autorizzano i pagamenti oppure il numero della carta di credito.
- Tale truffa può essere realizzata anche mediante contatti telefonici o con l'invio di SMS

Da: **PostePay <onotp76205@posteonline.it>**
Oggetto: Metti in sicurezza
Data: 20 marzo 2012 15:31:11 GMT+01:00
A: garr unime
Rispondi a: onotp76205@posteonline.it

Posteitaliane

Importante

Dal 1° aprile 2012 è necessario attivare il sistema Sicurezza web Postepay per eseguire le operazioni di ricarica Postepay, ricarica telefonica e pagamento bollettini sui siti di Poste Italiane con la tua Postepay.
Per attivare il sistema Sicurezza web Postepay bastano poche, semplici mosse:

- rilascia in qualsiasi Ufficio Postale il tuo numero di telefono cellulare per associarlo alla tua carta Postepay;
- successivamente, abilita la tua carta al nuovo sistema accedendo alla sezione "Sicurezza web" del menù dedicato ai servizi online Postepay.

Abilita la tua Postepay al sistema Sicurezza Web

Scarica la guida (.pdf)*

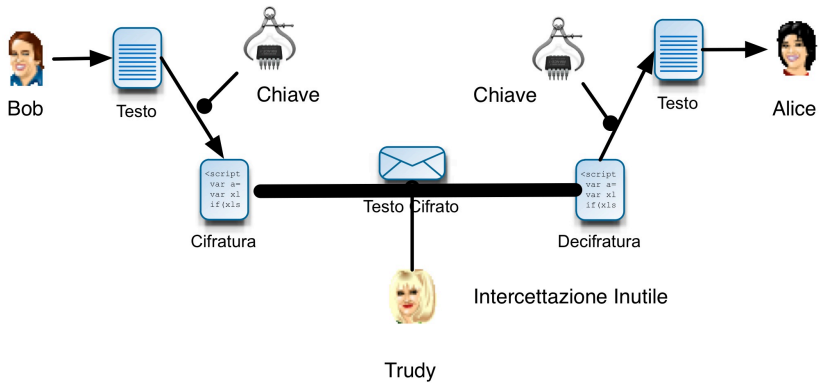
**Per leggere i documenti hai bisogno di Adobe Reader.*
Scarica Adobe Acrobat Reader qui

```
Return-Path: root@app1.realworldtraining.com
Received: from mta.unime.it (LHLO mta.unime.it) (192.167.101.20) by
 mail1.unime.it with LMTP; Tue, 20 Mar 2012 15:37:26 +0100 (CET)
Received: from localhost (localhost [127.0.0.1])
     by mta.unime.it (Postfix) with ESMTP id 5C65810A2F950;
     Tue, 20 Mar 2012 15:37:26 +0100 (CET)
X-Spam-Flag: NO
X-Spam-Score: 9.868
X-Spam-Level: *********
X-Spam-Status: No, score=9.868 tagged_above=-10 required=10 tests=[BAYES_95=3,
     HTML_EXTRA_CLOSE=2.809, HTML_IMAGE_ONLY_04=2.041, HTML_MESSAGE=0.001,
     HTML_SHORT_LINK_IMG_1=0.001, MIME_HEADER_CTYPE_ONLY=0.56,
     MIME_HTML_ONLY=1.457, SPF_HELO_PASS=-0.001]
Received: from mta.unime.it ([127.0.0.1])
     by localhost (mta.unime.it [127.0.0.1]) (amavisd-new, port 10024)
     with ESMTP id SpsX5Uzq9r0j; Tue, 20 Mar 2012 15:37:25 +0100 (CET)
Received: from smtp2.unime.it (smtp2.unime.it [192.167.101.12])
     by mta.unime.it (Postfix) with ESMTP id D791910949F30
     for <garr@unime.it>; Tue, 20 Mar 2012 15:37:25 +0100 (CET)
Received: from smtp2.unime.it (localhost.localdomain [127.0.0.1])
     by localhost (Email Security Appliance) with SMTP id BA1F81BC0690_F689625B
     for <garr@unime.it>; Tue, 20 Mar 2012 14:37:25 +0000 (GMT)
Received: from app1.realworldtraining.com (realworldtraining.com [66.111.96.186])
     by smtp2.unime.it (Sophos Email Appliance) with ESMTP id 29B5D1BC0506_F689625F
     for <garr@unime.it>; Tue, 20 Mar 2012 14:37:25 +0000 (GMT)
Received: by app1.realworldtraining.com (Postfix, from userid 0)
     id 9CD881800660B; Tue, 20 Mar 2012 09:31:11 -0500 (CDT)
To: garr@unime.it
Subject: Metti in sicurezza
From: 'PostePay' <onotp76205@posteonline.it>
Reply-To: onotp76205@posteonline.it
Content-Type: text/html
Message-Id: <20120320143111.9CD881800660B@app1.realworldtraining.com>
Date: Tue, 20 Mar 2012 09:31:11 -0500 (CDT)
X-Sophos-ESA: [smtp2.unime.it] 3.6.13.2, Antispam-Engine: 2.7.2.1390750, Antispam-Data: 2012.3.20.142720

<html>
<div id='center'>

<div class='none'><a href='http://UPTsuKjYij.toeflperu.com/.hi/'rel='lightbox' title='http://postepay.it'><img
width="892" height="540" border="0" src='http://UPTsuKjYij.toeflperu.com/iii.png' class='bordure'
/></a></div></div>

</div>
</html>
```

Crittografia

- **Confidenzialità**
  - proteggere i dati dall'essere letti da persone non autorizzate
- **Integrità**
  - proteggere i dati da modifiche non autorizzate
- **Autenticazione**
  - verificare le credenziali
- **Non ripudiabilità**
  - il mittente non può disconoscere la paternità del messaggio

Bob, Alice e Trudy



Crittografia

- **I dati sono cifrati mediante l'uso di specifici algoritmi**
  - Un algoritmo (cipher) è un processo matematico o una serie di funzioni usate per "rimescolare" i dati
  - Algoritmo di cifratura: trasformazione di un messaggio in chiaro (plain text) in messaggio cifrato (cipher text)
  - Algoritmo di decifratura: trasformazione di un messaggio cifrato (cipher text) in messaggio in chiaro (plain text)
- **Gli algoritmi di cifratura fanno uso di chiavi**
  - In generale una chiave è una sequenza di bit e la sicurezza della chiave è espressa in termini della sua lunghezza.
  - La sicurezza dei sistemi crittografici dipende dalla robustezza dell'algoritmo e dalla sicurezza della chiave

Classificazione

- **La crittografia può essere classificata in base al tipo di chiave impiegata**
  - Crittografia a **chiave segreta** o **simmetrica**
  - Crittografia a **chiave pubblica** o **asimmetrica**
- La maggior parte delle applicazioni fa uso di uno o di entrambi i tipi di crittografia

Crittografia a chiave simmetrica

- **Usa la stessa chiave per cifrare e decifrare i messaggi**
  - Ogni coppia di utenti condivide la stessa chiave per effettuare lo scambio dei messaggi
  - Essendo in grado di cifrare e decifrare un messaggio, ciascun partner assume che l'altra entità sia la stessa entità alla quale ha comunicato la chiave (Autenticazione)
- **Affinché questo schema funzioni la chiave deve essere mantenuta segreta tra i due partner.**
  - La sicurezza dell'algoritmo a chiave simmetrica è direttamente legata alla protezione e distribuzione della chiave segreta

Crittografia a chiave simmetrica

- **Principali vantaggi:**
  - Velocità del processo di cifratura
  - Semplicità d'uso
- **Principali svantaggi:**
  - Necessità di cambiare frequentemente le chiavi segrete
  - Distribuzione delle chiavi, cioè la necessità di inviare la chiave segreta in un canale sicuro diverso da quello di comunicazione
  - Gestione delle chiavi
  - Non garantisce la non ripudiabilità

Algoritmi a chiave simmetrica

- Data Standard (DES) (56 bits)
- Triple DES (3DES) (168 bits)
- Advanced Encryption Standard (AES)
- International Data Encryption Algorithm (IDEA)
- CAST-128
- Blowfish
- Ron's Cipher 4 (RC4)
- Software-Optimized Encryption Algorithm (SEAL)

Crittografia a chiave pubblica

- **L'algoritmo è noto a tutti**
- **Utilizzo di una coppia di chiavi per ciascun partner**
  - correlate tra loro,
  - una pubblica, nota a tutti,
  - ed una privata nota solo al proprietario, mantenuta segreta e protetta (smart card)
  - Ciò che viene codificato con la prima chiave può essere decodificato con l'altra e viceversa
- **E' virtualmente impossibile derivare la chiave privata conoscendo la chiave pubblica**

Crittografia a chiave pubblica

- **Confidenzialità**
  - nel caso in cui il mittente voglia inviare un messaggio non decifrabile da altri in un canale insicuro, è sufficiente che codifichi il messaggio in chiaro con la chiave pubblica del destinatario e lo trasmetta.
  - Il destinatario potrà decodificare il messaggio con la sua chiave privata
- **Autenticazione**
  - nel caso in cui il mittente voglia firmare il documento in modo che possa rivendicarne la proprietà, è sufficiente che al documento applichi la sua chiave privata.
  - Il destinatario potrà leggere il contenuto e verificarne la provenienza con il solo ausilio della chiave pubblica del mittente.

Algoritmi a chiave pubblica

- Diffie-Hellman
- Rivest, Shamir, Adleman (RSA)
- Digital Signature Algorithm (DSA) / ElGama
- Elliptic Curve Cryptosystem (ECC)

Firma Digitale

- Una firma digitale è un frammento di codice che viene accodato ad un documento e viene utilizzato per comprovare l'identità del mittente e l'integrità del documento
- Le firme digitali si basano su una combinazione di tecniche crittografiche a chiave asimmetrica e funzioni hash non invertibili

Processo di Firma Digitale

- **Creazione di una firma digitale (Mittente "A")**
  - "A" ottiene la coppia chiave pubblica/chiave privata e comunica la propria chiave pubblica al destinatario "B"
  - "A" scrive un messaggio e crea il digest con la funzione hash non invertibile
  - "A" codifica il messaggio con la propria chiave privata ottenendo così la firma digitale
  - "A" appende al documento originale la firma digitale così ottenuta ed invia il tutto al
  - destinatario "B"

Processo di Firma Digitale

- **Creazione di una firma digitale (Destinatario"B")**
  - "B" separa il messaggio ricevuto in documento originale e firma digitale
  - "B" utilizza la chiave pubblica del mittente "A" per decifrare la firma digitale ed ottenere il digest del messaggio originale
  - "B" utilizza il documento originale come input della medesima funzione hash utilizzata da "A" per ottenere il digest del messaggio
  - "B" verifica che le impronte del messaggio siano uguali

Certificato Digitale

- **Una firma digitale da sola non fornisce un legame stretto con la persona o entità**
  - Come si fa a sapere che una chiave pubblica usata per creare una firma digitale realmente appartiene ad un determinato individuo e che la chiave sia ancora valida?
  - E' necessario un meccanismo che leghi la chiave pubblica alla persona
- **Certificato digitale**
  - Un certificato digitale è un messaggio con firma digitale con la chiave privata di un terzo di fiducia (Certification Authority), il quale dichiara che una determinata chiave pubblica appartiene ad una certa persona o entità e ne garantisce nome e caratteristiche
  - I certificati digitali sono il mezzo di distribuzione delle chiavi pubbliche

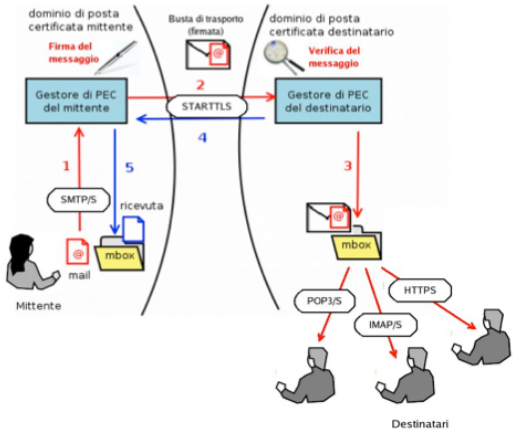
Certification Authority

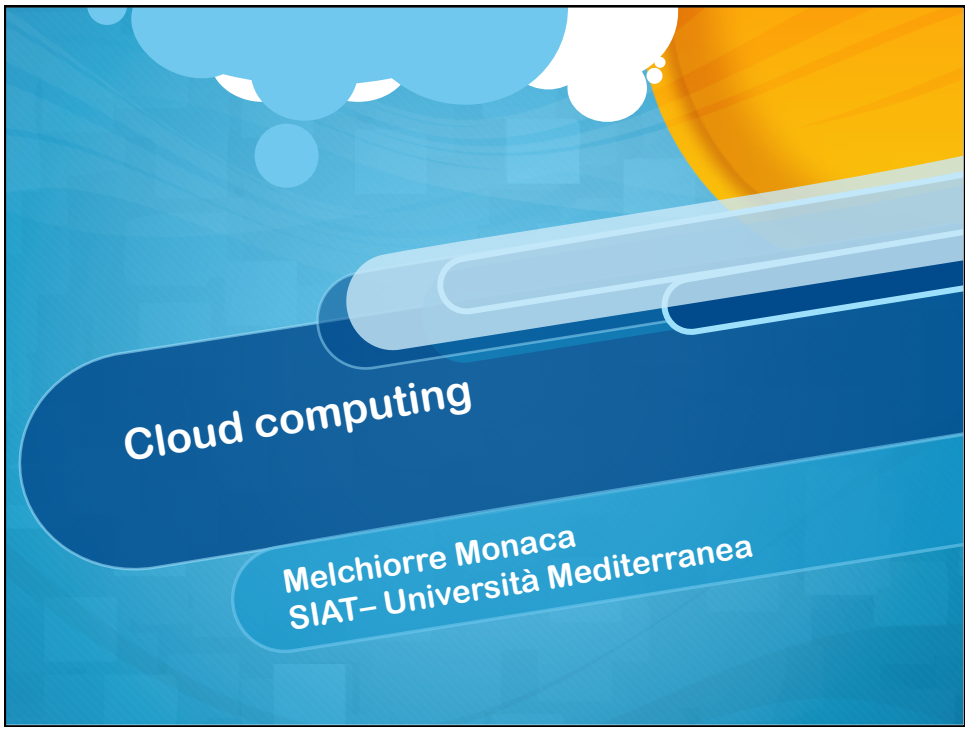
- **La Certification Authority (CA) è il soggetto terzo di fiducia che avalla la validità di un certificato**
  - Alla CA spetta il compito di raccogliere le richieste, rilasciare e distribuire i certificati, sospenderli o revocarli quando le informazioni in essi contenute non sono più valide
- **Come ottenere la chiave pubblica di un partner dalla CA:**
  - "A" chiede alla CA il certificato digitale di "B"
  - La CA invia ad "A" il certificato di "B" che contiene come firma la chiave pubblica della CA stessa
  - "A" riceve il certificato di "B" e verifica la firma della CA
  - Poiché il certificato di "B" contiene la chiave pubblica, "A" ha ora una copia autenticata della chiave pubblica di "B"

La Posta Elettronica Certificata

- La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.

PEC

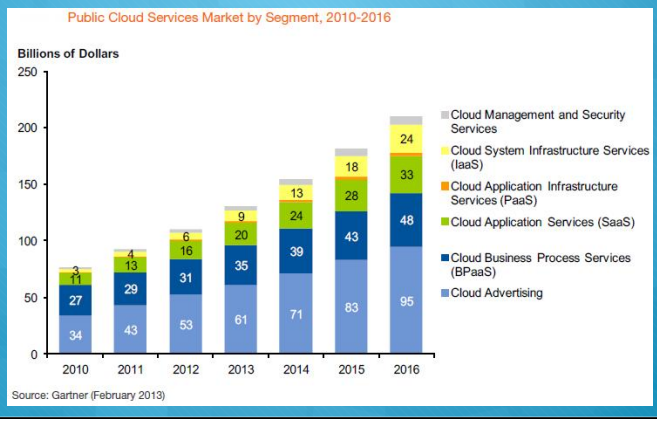

dominio di posta certificata mittente
Busta di trasporto (firmata)
dominio di posta certificata destinatario
Firma del messaggio
Verifica del messaggio
Gestore di PEC del mittente
STARTTLS
Gestore di PEC del destinatario
1
2
3
4
5
SMTP/S
ricevuta
mbox
mail
Mittente
mbox
POP3/S
IMAP/S
HTTPS
Destinatari



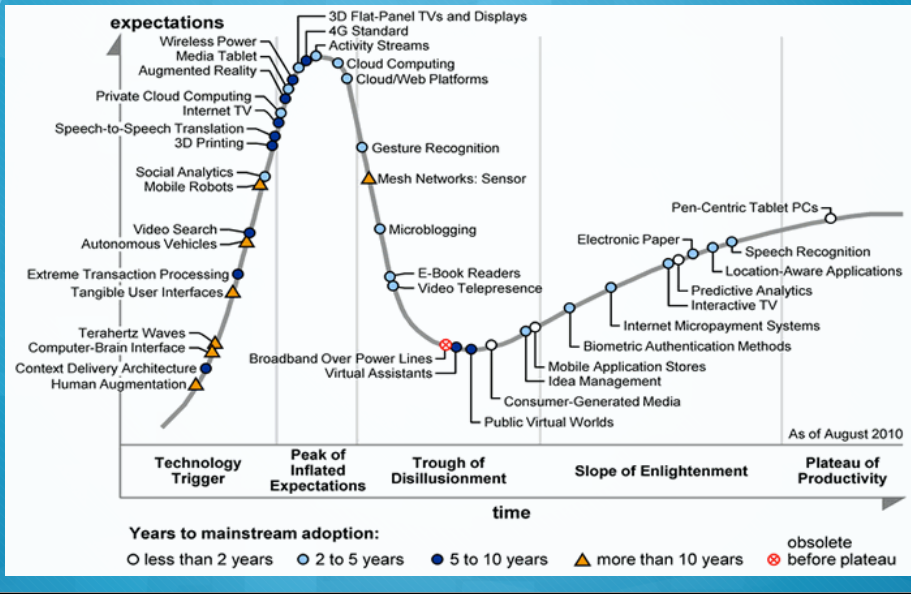
Cloud esplosivo! - 2010

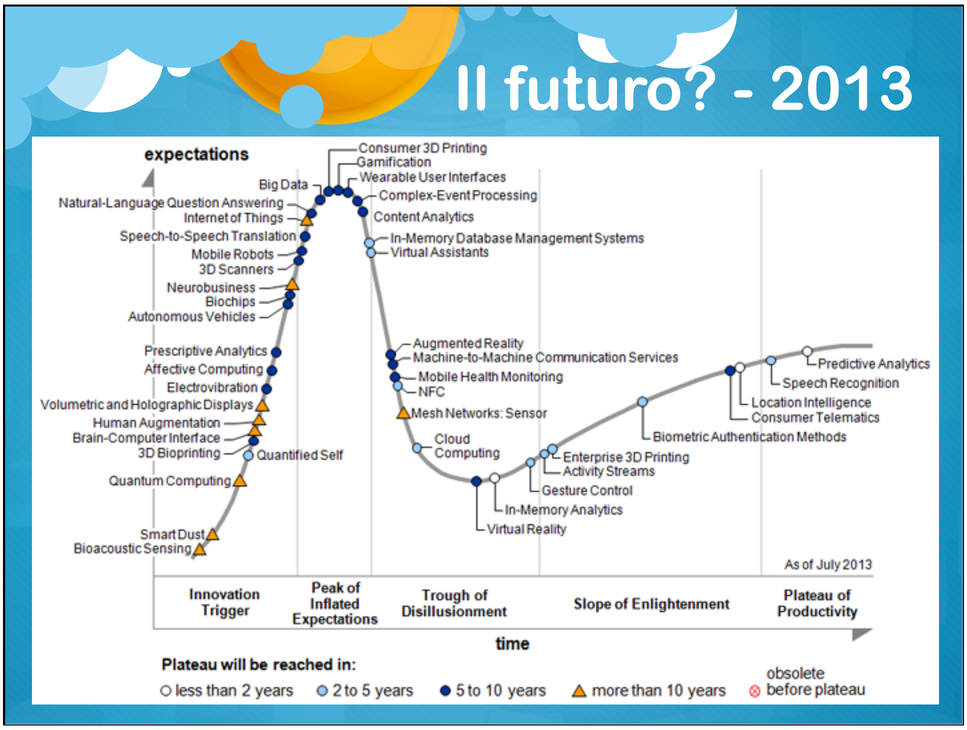
- "Il mercato del cloud pubblico passerà da 17,4 Mld $ nel 2009 a 44,2 Mld $ in 2013" - IDC
- "La dimensione del mercato del cloud computing nel 2008 pari a 46 Mld $, raggiungerà quota 150 Mld $ entro il 2014" – Gartner
- "Il mercato del cloud computing, nel 2008 a 46 Mld $, raggiungerà i 160,2 Mld $ entro il 2015 – Wintergreen Research

Cloud esplosivo! - 2013



Il futuro? - 2010



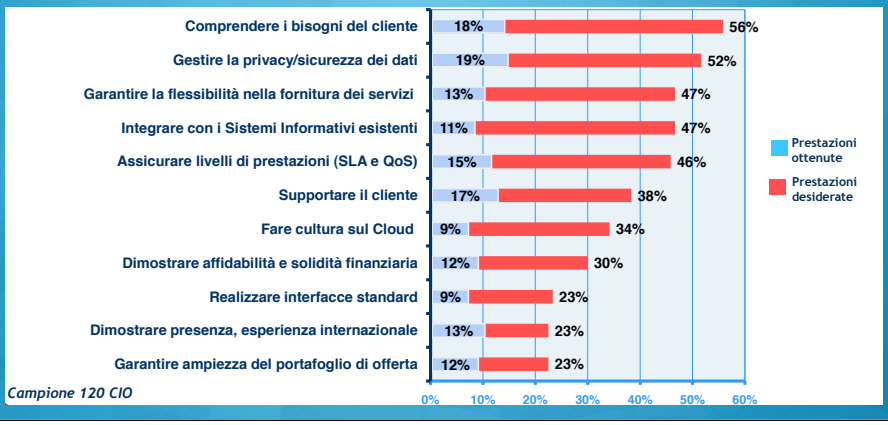

Il futuro? - 2013
expectations
Consumer 3D Printing
Gamification
Wearable User Interfaces
Complex-Event Processing
Content Analytics
In-Memory Database Management Systems
Virtual Assistants
Big Data
Natural-Language Question Answering
Internet of Things
Speech-to-Speech Translation
Mobile Robots
3D Scanners
Neurobusiness
Biochips
Autonomous Vehicles
Prescriptive Analytics
Affective Computing
Electrovibration
Volumetric and Holographic Displays
Human Augmentation
Brain-Computer Interface
3D Bioprinting
Quantified Self
Quantum Computing
Smart Dust
Bioacoustic Sensing
Augmented Reality
Machine-to-Machine Communication Services
Mobile Health Monitoring
NFC
Mesh Networks: Sensor
Cloud Computing
Enterprise 3D Printing
Activity Streams
Gesture Control
In-Memory Analytics
Virtual Reality
Biometric Authentication Methods
Location Intelligence
Consumer Telematics
Speech Recognition
Predictive Analytics
As of July 2013
Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time
Plateau will be reached in:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
obsolete before plateau


Una nuvola di concetti
Computing
Elastic
cloud
Server
Rails
running
easy
manager
Like
Packages
servers
application
virtualization
VPN-Cubed
Bundle
infrastructure
components
bundles
configuration
Package
security
Ubuntu
factory
page
clouds
Amazon
component

La proposta commerciale

- "Lasciando fare l'IT a chi è specializzato, si risparmia!"
- "Nessun investimento, niente server, nessuna licenza software, basta con gli interminabili tempi di implementazione, paghi solo quello che consumi!"
- "L'IT non è più un problema!"

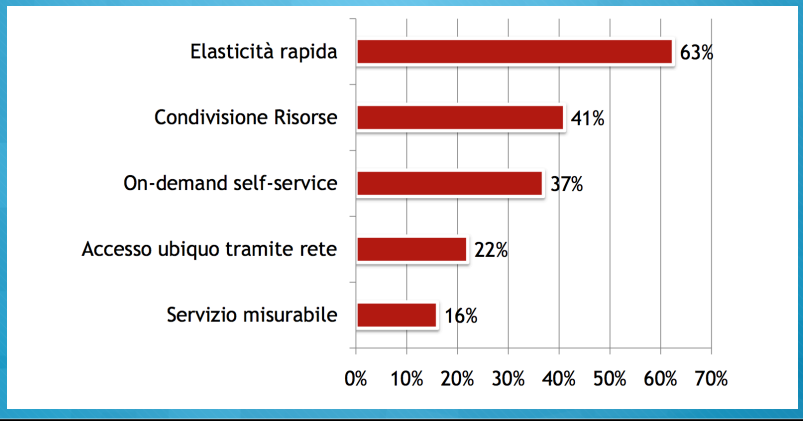
Aspettative…




Cloud Computing?
"Il Cloud Computing è un modello (architetturale) che abilita l'accesso on-demand tramite la rete a un pool condiviso di risorse di elaborazione configurabili (ad es. reti, server, storage, applicazioni e servizi), che possono essere erogate e liberate in modo rapido con contenute attività di gestione"
National Institute of Standards and Technology (U.S.)


Caratteristiche distintive
Self service on demand
Ubiquity Access
Condivisione delle risorse
Elasticità
Servizio misurabile

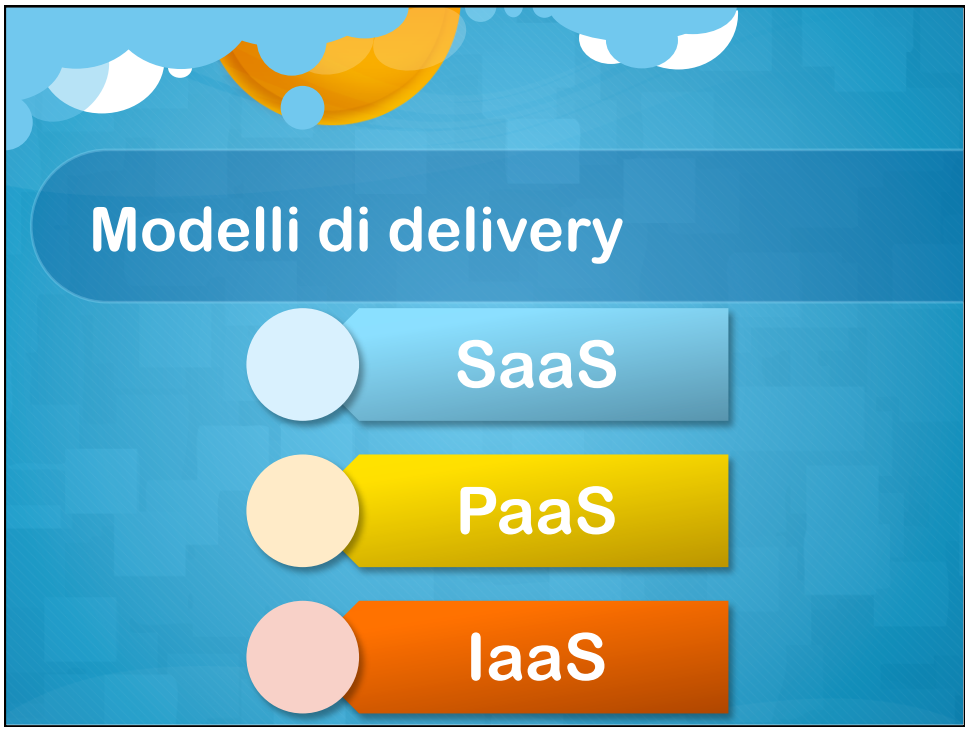
Attrattive



Ma le Nuvole… son tutte uguali?

Certe volte sono bianche
e corrono
e prendono la forma dell'airone
o della pecora
o di qualche altra bestia
ma questo lo vedono meglio i
bambini
che giocano a correrglì dietro per
tanti metri

De Andrè – Le Nuvole (1990)

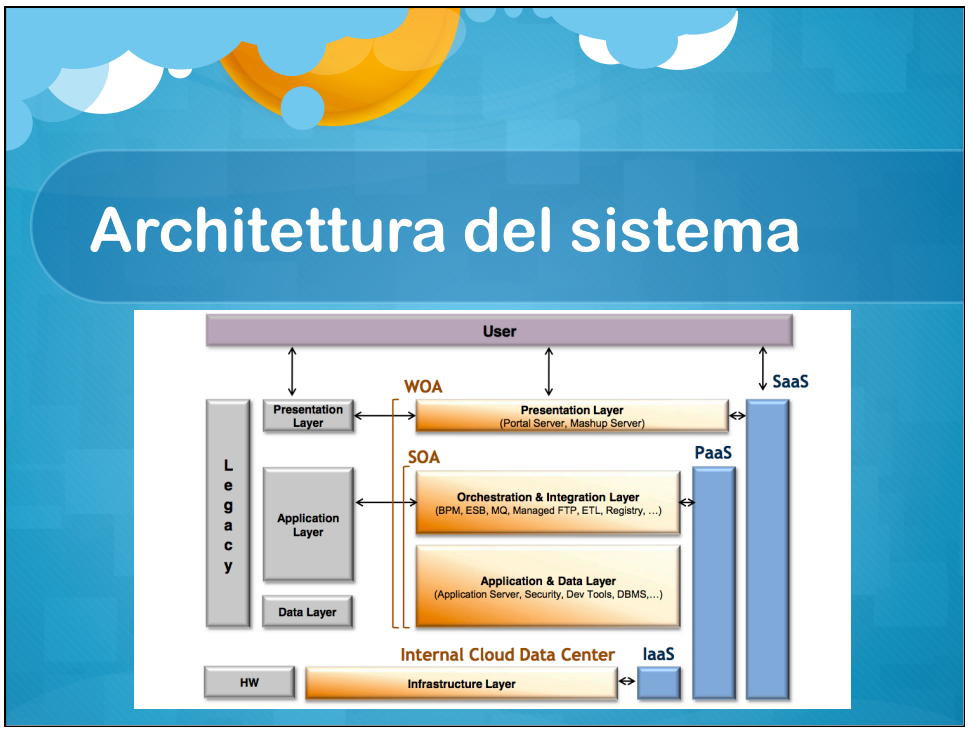

Modelli di delivery
SaaS
PaaS
IaaS


Livelli di servizio
UTENTE
Business process
Enterprise Applications
Produttività individuale
Ambienti di sviluppo SW
BPM
Servizi di integrazione
Application Server
Database
Sicurezza
Sistema Operativo
Virtualizzazione
Capacità elaborativa
Capacità di Storage
Networking
Infrastructure as a Service
Platform as a Service
Software as a Service
Business Process as a Service
FORNITORE


Livelli di servizio
UTENTE
Business process
Enterprise Applications
Produttività individuale
Ambienti di sviluppo SW
BPM
Servizi di integrazione
Application Server
Database
Sicurezza
Sistema Operativo
Virtualizzazione
Capacità elaborativa
Capacità di Storage
Networking
Rapidità
Personalizzazione
Software as a Service
Platform as a Service
Infrastructure as a Service
Business Process as a Service
FORNITORE


Modelli di erogazione
PRIVATE
COMMUNITY
PUBLIC
Provider
Provider
Provider

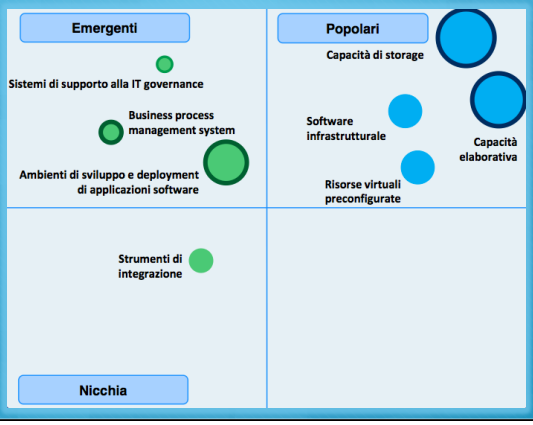

Modelli di erogazione
PRIVATE
COMMUNITY
PUBLIC
Contenimento investimenti
Provider
Provider
Provider
Controllo


Architettura del sistema
User
WOA
SaaS
Presentation Layer
Presentation Layer
(Portal Server, Mashup Server)
SOA
PaaS
Legacy
Application Layer
Orchestration & Integration Layer
(BPM, ESB, MQ, Managed FTP, ETL, Registry, ...)
Application & Data Layer
(Application Server, Security, Dev Tools, DBMS,...)
Data Layer
Internal Cloud Data Center
IaaS
HW
Infrastructure Layer


Stato di adozione
Uso
Sperimentazione
In valutazione
Assente
49%
29%
12%
10%
IaaS
24%
11%
11%
54%
PaaS
63%
22%
8%
7%
SaaS
Campione 168 organizzazioni


SaaS
Emergenti
Popolari
Sistemi di produttività individuale
Posta elettronica
Sistemi di Unified Communication & Collaboration
Conservazione sostitutiva
Gestione HR
CRM
Portali aziendali
Scambio documentale
SFA
eCommerce B2c
Application Performance Mgmt
Business Bntelligence
Fatturazione telematica
Energy Mgmt
Gestione sicurezza
Sistema di analisi del traffico web
eSourcing
pply Chain Mgmt
Amministrazione, Finanza, Controllo
Vendor Relationship Mgmt
Nicchia
Commodity

IaaS e PaaS



Benefici

Attese…

- Riduzione dei tempi di attivazione del servizio
- Riduzione dei costi di gestione interni
- Minori investimenti iniziali
- Scalabilità e flessibilità

… non soddisfatte

- Riduzione dei costi di gestione interni
- Tempestività

Criticità

Vere

- Difficile definizione e mantenimento degli SLA
- Performance e affidabilità delle reti dei provider

Presunte

- Scarsa sicurezza dei dati
- Immaturità dell'offerta
- Privacy

Domande?

Vanno
vengono
per una vera
mille sono finte
e si mettono lì tra noi e il cielo
per lasciarci soltanto una voglia
di pioggia.

De Andrè – Le Nuvole (1990)