Livello Applicazione

.

Davide Quaglia

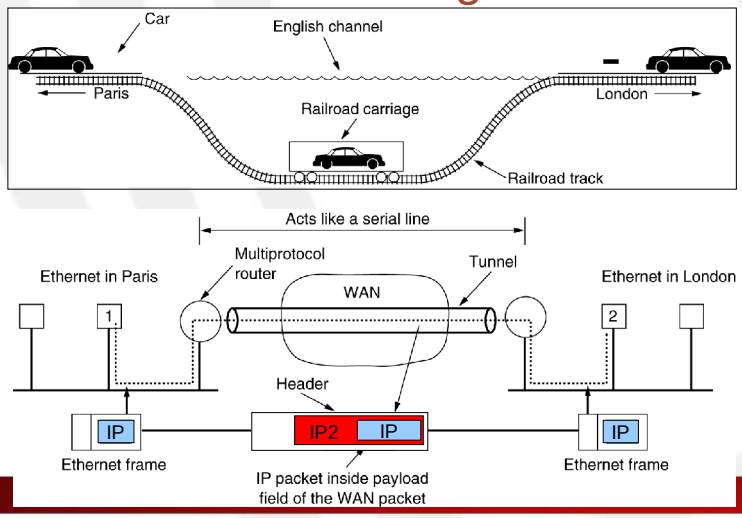
Motivazione

- Nell'architettura ibrida TCP/IP sopra il livello trasporto esiste un unico livello che si occupa di:
  - Gestire il concetto di sessione di lavoro
    - Autenticazione
    - Ripresa dopo una interruzione
  - Cifrare i dati o garantirne l'autenticità
  - Compiti di gestione: nomi e cfg interfacce
  - Costruire le applicazioni utili alle persone
    - Posta, Web, FTP, ecc...

Virtual Private Network (VPN)

- Scopo
- Servizi
  - Autenticazione
  - Riservatezza
  - Integrità
  - Non ripudio

Tunneling



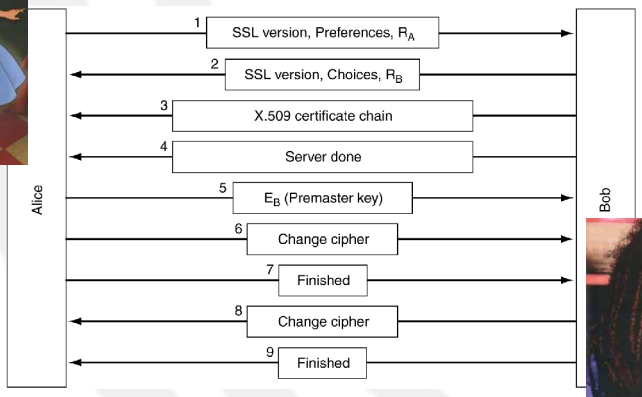
Protocolli per VPN

- IP Security (IPSec)
  - Incaspula pacchetti IP cifrati in pacchetti IP in chiaro
- Secure Socket Layer (SSL) e Transport Layer Security (TLS)
  - Utilizzano TCP
  - Rivestono vari protocolli applicativi rendendoli sicuri
    - HTTPS, Secure SMTP, Secure POP3, ecc...

SSL

Application (HTTP)
Security (SSL)
Transport (TCP)
Network (IP)
Data link (PPP)
Physical (modem, ADSL, cable TV)

SSL (2)



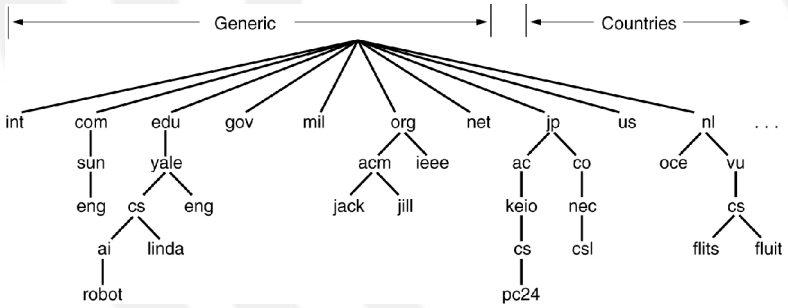
Domain Name System (DNS)

- Motivazioni
  - E' più facile ricordare nomi che indirizzi IP
  - Un server può cambiare IP pur mantenendo lo stesso nome
  - Raggrupp. logico diverso da raggr. topologico
- Il servizio DNS associa nomi di host e destinazioni di posta elettronica a indirizzi IP:
  - Basato su UDP
  - Modello client/server: richiesta → risposta
  - Organizzazione gerarchica dei nomi
  - Database distribuito per aumentare robustezza e manutenibilità

DNS: funzionamento

- L'applicativo chiama una procedura del sistema operativo chiamata RISOLUTORE
- Il risolutore invia un pacchetto UDP a un server DNS locale
  - La propria macchina deve conoscere l'indirizzo IP del server DNS locale (ad es. in Unix in /etc/resolv.conf)
  - Il server DNS cerca il nome e restituisce l'indirizzo IP al risolutore, che a sua volta lo restituisce al chiamante.
  - A questo punto si può stabilire una connessione TCP con la destinazione o inviarle pacchetti UDP

Lo spazio dei nomi: domini



L'assegnamento dei nomi e' assolutamente indipendente dall'indirizzamento IP !

I domini NON coincidono con le reti IP !!!

DNS (3)

- Circa 200 domini di primo livello
- Ogni dominio copre diversi host
- Ogni dominio controlla come allocare i domini sottostanti
- Gli host si identificano col percorso completo dei nomi dei domini attraversati
  - Da sx a dx: dal più specifico al più generale
  - Separati da punti

Resource Records

- A ciascun nodo dell'albero è associato uno o più Resource Record
- Il Resource Record è una quintupla:
  - *Domain_name:* dominio
  - *Time_to_live:* indicatore stabilità
  - *Class:* per Internet IN
  - *Type:* SOA, A, MX, NS, etc.
  - *Value:* string di ASCII

Resource Records (2)

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

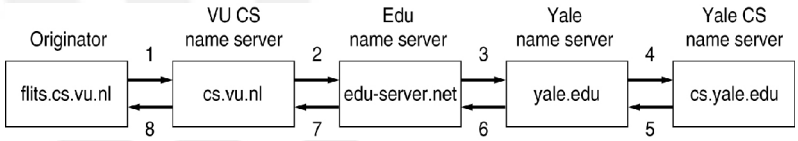
Resource Records (3): esempio

```
; 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
```

I server dei nomi

- Lo spazio dei nomi è diviso in zone non sovrapposte
- Ogni zona contiene il proprio server dei nomi
- Il risolutore si rivolge sempre al server locale
  - Se il nome richiesto è di competenza del server locale viene restituita una risposta AUTHORITATIVE
  - Altrimenti il server locale chiede al server di livello successivo o al server di primo livello
- La richiesta arriva fino al server del dominio del host richiesto e la risposta segue il percorso inverso
- Il server locale mantiene una cache delle risposte
  - Le risposte in cache non sono AUTHORITATIVE

I server dei nomi (2)

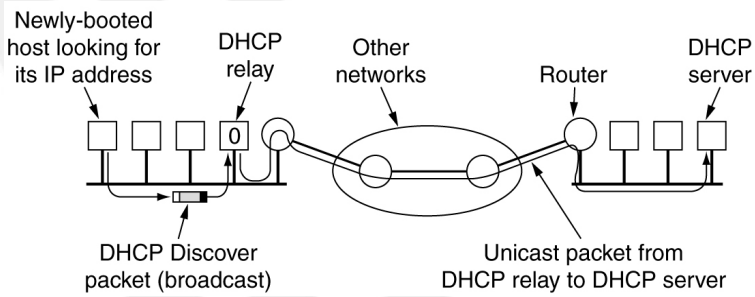


L'host `flirts.cs.vu.nl` vuole conoscere l'IP dell'host `linda.cs.yale.edu`

Dynamic Host Configuration Protocol (DHCP)

- Usato per configurare automaticamente tutte le interfacce di una rete
- Assegna
  - IP/netmask
  - Default gateway
  - Domain Name Server
  - (opzionale) altri server (Domini Windows, centralino, VoIP, ecc…)

Dynamic Host Configuration Protocol

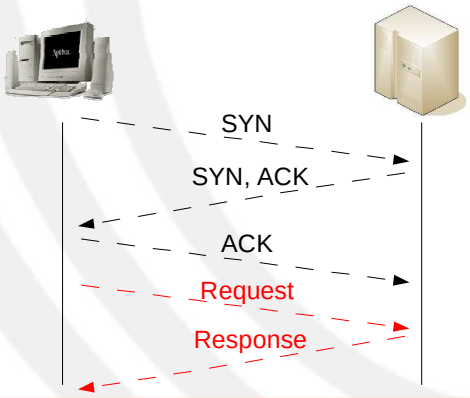


Broadcast
IP+ liv 2

Modello client/server

Browser Web (client)
IP: 157.27.12.5 Porta TCP: 3500

Server Web (server)
IP: 130.192.16.20 Porta TCP: 80



Well-known ports

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

World Wide Web

World Wide Web

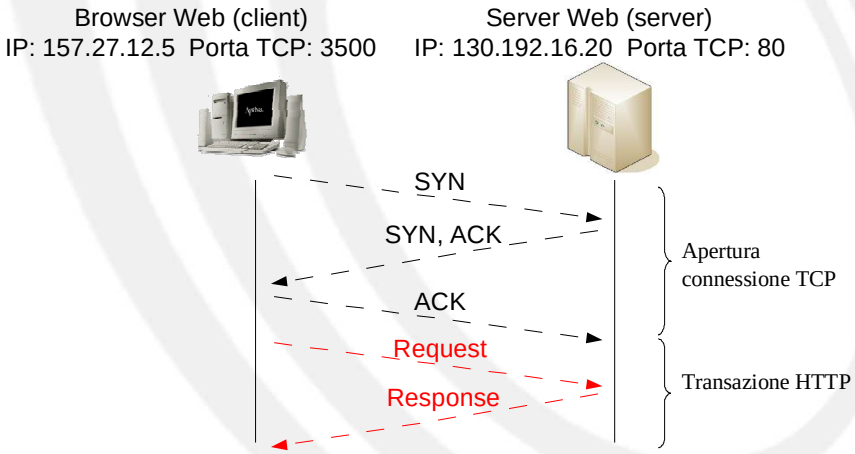
- Inventato da Tim Berners-Lee al CERN di Ginevra nel 1989
- Client (web browser) accedono a documenti HTML, immagini, ecc. contenuti su vari server
- I contenuti digitali possono essere
  - Statici: pagine, immagini, video
  - Dinamici: risultati di calcoli, query a DB

Il funzionamento del WWW

1. Il browser determina l'URL (o digitata I clicckata)
2. Il browser chiede al DNS locale l'IP di www.ietf.org
3. Il DNS risponde con 64.170.9[illegible]
4. Il browser apre una conn T[illegible]
5. Il browser **richiede** la pagin[illegible]
6. Il server **invia** la pagina HTML e ch[illegible]
7. Il browser chiude la conn TCP e visualizza la pagina HTML
8. Il browser **richiede** al server, **riceve** e visualizza le immagini contenute nella pagina

Le richieste e le risposte sono regolate dal protocollo di livello applicazione chiamato Hyper Text Transfer Protocol

Hyper Text Transfer Protocol (HTTP)



Esempio di dialogo: client request

GET / HTTP/1.1
Host: 130.192.16.20
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11
Accept: text/xml,application/xml,text/html
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Esempio di dialogo: server response

HTTP/1.1 200 OK
Date: Wed, 04 Feb 2009 11:17:10 GMT
Server: Apache/2.0.52 (Debian GNU/Linux)
Last-Modified: Wed, 10 Nov 2004 11:40:38 GMT
Content-Length: 1457
Content-Type: text/html
Content-Language: en

Header

<html>
...
</html>

Payload

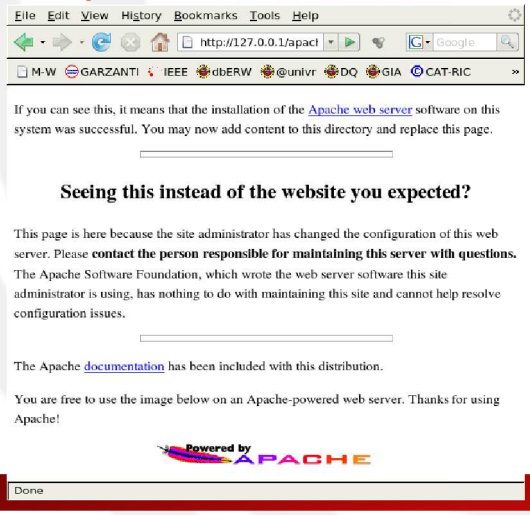
Esempio: server response: payload (1)

```
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>Test Page for Apache Installation</title>
</head>
<!-- Background white, links blue (unvisited), navy (visited), red
(active) -->
<body bgcolor="#FFFFFF" text="#000000" link="#0000FF" vlink="#000080" alink="#FF0000">
<p>If you can see this, it means that the installation of the
<a href="http://www.apache.org/foundation/preFAQ.html">Apache web server</a>
software on this system was successful. You may now add content to this directory
and replace this page.</p>

<hr width="50%" size="8" />
<h2 align="center">Seeing this instead of the website you expected?</h2>

...
```


Esempio: server response: payload (2)

```
...

<p>This page is here because the site administrator has changed the
configuration of this web server. Please <strong>contact the person
responsible for maintaining this server with questions.</strong>
The Apache Software Foundation, which wrote the web server software
this site administrator is using, has nothing to do with
maintaining this site and cannot help resolve configuration issues.</p>

<hr width="50%" size="8" />
<p>The Apache <a href="/manual/">documentation</a> has been included
with this distribution.</p>

<p>You are free to use the image below on an Apache-powered web
server. Thanks for using Apache!</p>

<div align="center"><img src="apache_pb.gif" alt="" /></div>
</body>
</html>
```

Esempio: risultato sul client



Contenuti restituiti dal server web

- I contenuti restituiti possono essere
  - Statici: pagine, immagini, video
  - Dinamici: risultati di calcoli, query a database
- Molti tipi di applicazioni possibili
  - Documentazione statica
  - Commercio elettronico
  - Lettura di posta elettronica
  - Elaborazione distribuita con chiamata remota di metodi (SOAP)
  - Applicazioni collaborative
    - Forum
    - Content/Document Management System (CMS/DMS)
    - Wiki

Tipi di richieste HTTP

Method	Description
GET	Request to read a Web page
HEAD	Request to read a Web page's header
PUT	Request to store a Web page
POST	Append to a named resource (e.g., a Web page)
DELETE	Remove the Web page
TRACE	Echo the incoming request
CONNECT	Reserved for future use
OPTIONS	Query certain options

Versione cifrata di HTTP

- Versione sicura su SSL/TLS con porta 443
- Autenticazione mediante certificati (chiave pubblica/privata)
- Cifratura mediante chiave simmetrica con validità di sessione

Posta elettronica

Aspetti del problema

- Formato del messaggio di posta
- Spedizione del messaggio
- Archiviazione presso una mailbox
- Lettura del messaggio arrivato

Formato del messaggio

- RFC 822: testo ASCII
  - Coppie *chiave : valore*
  - campi intestazione + riga vuota + corpo del messaggio
- MIME (Multipurpose Internet Mail Extensions)
  - Coppie *chiave : valore*
  - Nuove intestazioni tra cui *Content-type* per descrivere il formato del contenuto
    - Testo, immagini, video, pdf, ecc...

Intestazioni RFC 822

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

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

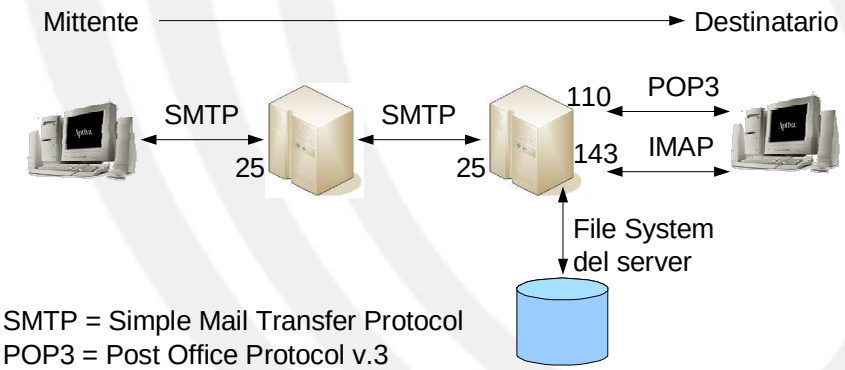
Intestazioni MIME

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

Codifica di contenuti non testuali

- La posta elettronica in origine prevedeva messaggi di testo su 7 bit
  - Impossibile inserire immagini e altri allegati
- Codifica Base64
  - Gruppi di 24 bit vengono suddivisi in 4 unità di 6 bit
  - Ogni unità è rappresentata come un carattere ASCII

Trasporto dei messaggi



SMTP = Simple Mail Transfer Protocol
POP3 = Post Office Protocol v.3
IMAP = Internet Message Access Protocol

Trasporto dei messaggi (2)

- POP3 scarica la posta sul client
- IMAP mantiene la posta sul server
- Esistono le versioni su SSL/TLS di SMTP, POP3 e IMAP (usano porte server diverse)

Altri protocolli applicativi

- File Transfer Protocol (FTP)
- Secure SHell (SSH)
- Session Initiation Protocol (SIP)
- Simple Network Management Prot (SNMP)
- Real Time Streaming Protocol (RTSP)
- Realtime Transfer Protocol (RTP)
- Network File System (NFS)
- Ecc...