FUNDAMENTOS DE REDES
CAPA DE APLICACIÓN

Daniel Barragán C.
daniel.barragan@correounivalle.edu.co
Edificio 331 Oficina 2114

Universidad del Valle

Capa de aplicación

"El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en un caja de Titanio, encerrado en un búnker de concreto, rodeado por gas venenoso y cuidado por guardias muy armados y muy bien pagados. Aun así no apostaría mi vida por él"

Eugene Spafford

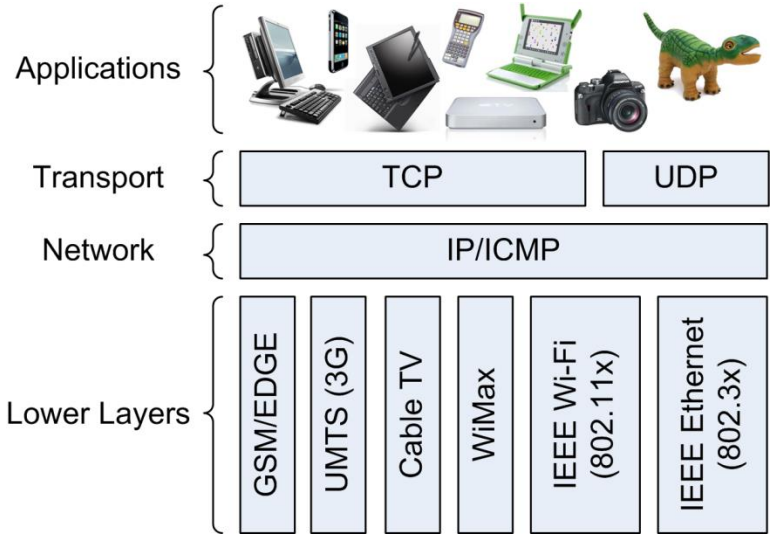
Capa de aplicación

Agenda

- Introducción
- Servicios
- HTTP (Hypertext Transfer Protocol)
- FTP (File Transfer Protocol)
- Correo Electrónico
- DNS (Domain Name System)*
- Programación con Sockets
- Programando un Servidor Web

Introducción

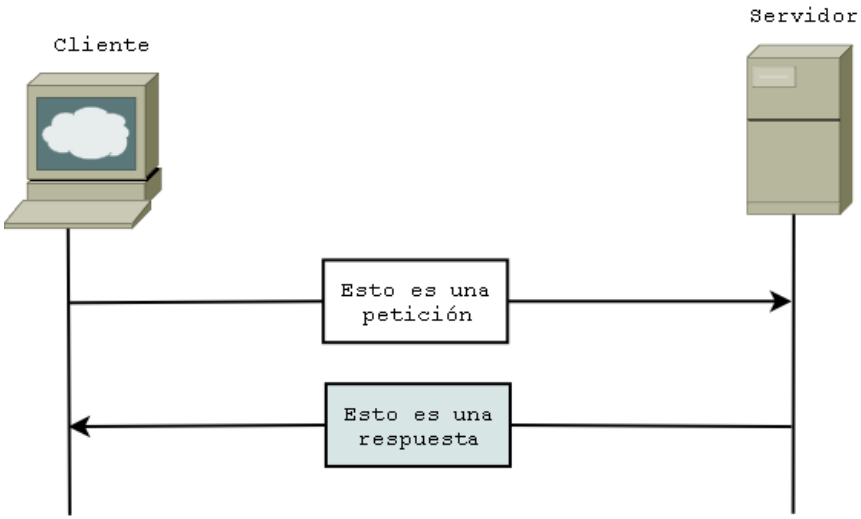
Las aplicaciones de red son la razón de ser de una red de comunicación. Las aplicaciones de red trabajan con protocolos de la capa de aplicación



Introducción

Protocolos de la capa de aplicación

Los protocolos de la capa de aplicación definen el formato y el orden en que los mensajes se intercambian entre procesos, así como las acciones a realizar al transmitir o recibir un mensaje



Introducción

Protocolos de la capa de aplicación

El correo electrónico y la web son aplicaciones de red compuestas por distintos componentes

Introducción

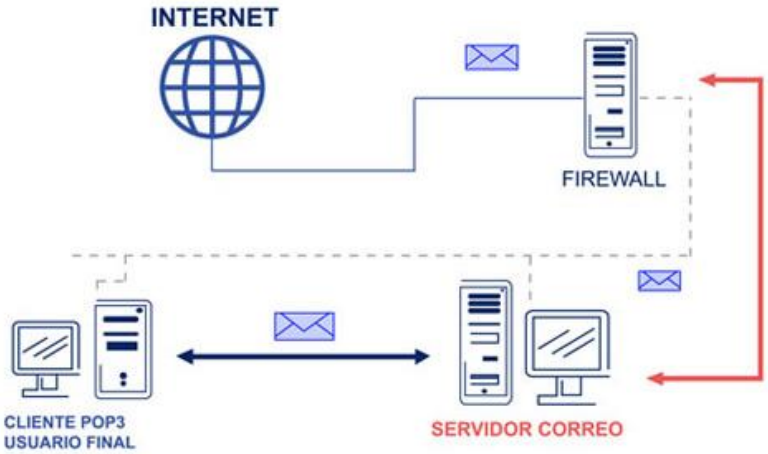
Protocolos de la capa de aplicación

Algunos componentes de la web son: el estándar HTML, los navegadores web, los servidores web y el protocolo HTTP

Introducción

Protocolos de la capa de aplicación

Algunos componentes del correo electrónico son: servidores de correo, clientes de correo, el estándar MIME (Multipurpose Internet Mail Extensions) y el protocolo SMTP (Simple Mail Transfer Protocol)



Introducción

Protocolos de la capa de aplicación

Un protocolo de la capa de aplicación define:

- Tipos de mensajes: mensajes de solicitud y respuesta
- Sintaxis de los mensajes (campos en los mensajes)
- Semántica de los campos (significado de los campos)
- Reglas de cuando y cómo se procesan mensajes de solicitud y respuesta

Introducción

Comunicación a través de la red

Una aplicación de red involucra dos o mas procesos que se comunican entre ellos

Introducción

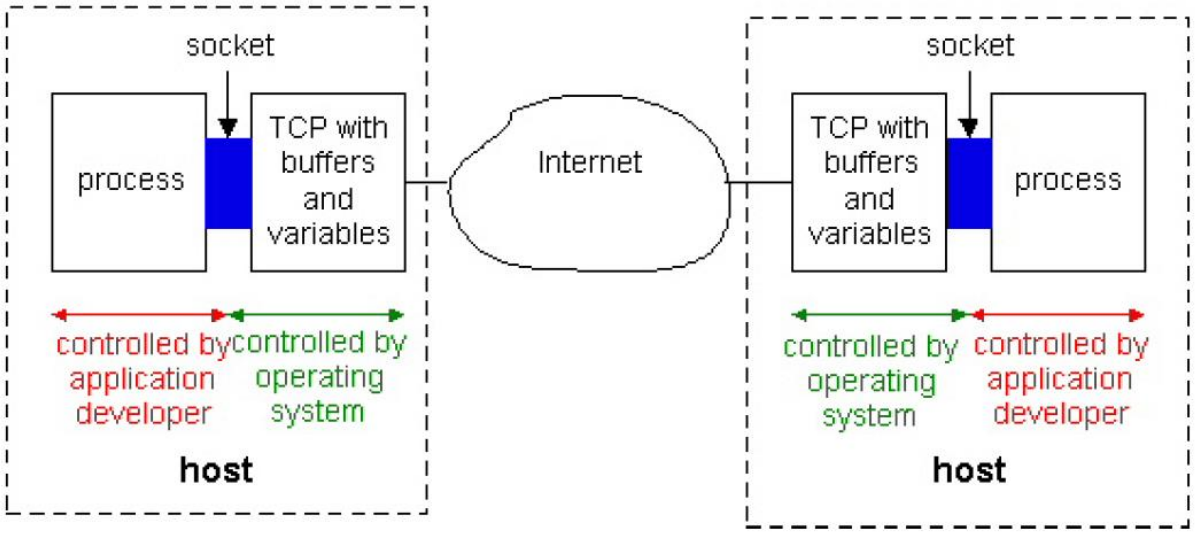
Comunicación a través de la red

Los procesos envían y reciben mensajes a través de sockets. Los procesos asumen que existe una infraestructura entre los sockets involucrados en la comunicación

Introducción

Comunicación a través de la red

Un socket es una interfaz entre un proceso y el protocolo de transporte



Introducción

Direccionamiento

En la tarea de enviar un mensaje se requiere identificar de forma única los procesos que participan en la comunicación

Existen dos tipos de direcciones: la dirección del equipo (dirección IP) y la dirección o identificador del proceso (Número de puerto)

Servicios

Al desarrollar una aplicación de red empleando sockets, se debe escoger el protocolo de la capa de transporte a utilizar

Servicios

Los servicios que una aplicación de red requiere de un protocolo de la capa de transporte pueden ser clasificados de acuerdo a tres dimensiones:

Perdida de información: algunas aplicaciones pueden presentar perdida de información y otras no

Ancho de banda: algunas aplicaciones deben transmitir información a una velocidad constante. Las técnicas de codificación adaptativa permiten adaptarse a las condiciones del canal

Tiempo: algunas aplicaciones tienen restricciones de tiempo muy ajustadas para la entrega de información

Servicios

Servicios TCP

TCP provee un servicio orientado a conexión y de transferencia confiable de información

En un servicio orientado a conexión las partes negocian el establecimiento de la comunicación. Cuando la transmisión de información termina, el cliente cierra la conexión

La transferencia confiable implica que las partes pueden confiar en que TCP entregará todos los mensajes sin error y en el orden correcto

TCP provee control de la congestión

Servicios

Servicios UDP

UDP provee un servicio no orientado a conexión y de transferencia de información no confiable

En un servicio no orientado a conexión las partes no negocian el establecimiento de la conexión

La transferencia no confiable no garantiza que los mensajes lleguen a su destino (socket receptor), ni que lleguen en orden

UDP no provee control de la congestión

HTTP

Introducción

Una página WEB se compone de objetos. Un objeto puede ser: un archivo HTML, una imagen, un audio, un video, etc

El archivo HTML base referencia a los otros objetos por medio de URLs. Una URL se compone del ***hostname*** del servidor y la ruta al objeto

www.univalle.edu.co/imagenes/logounivalle261x31.gif

HTTP

Características

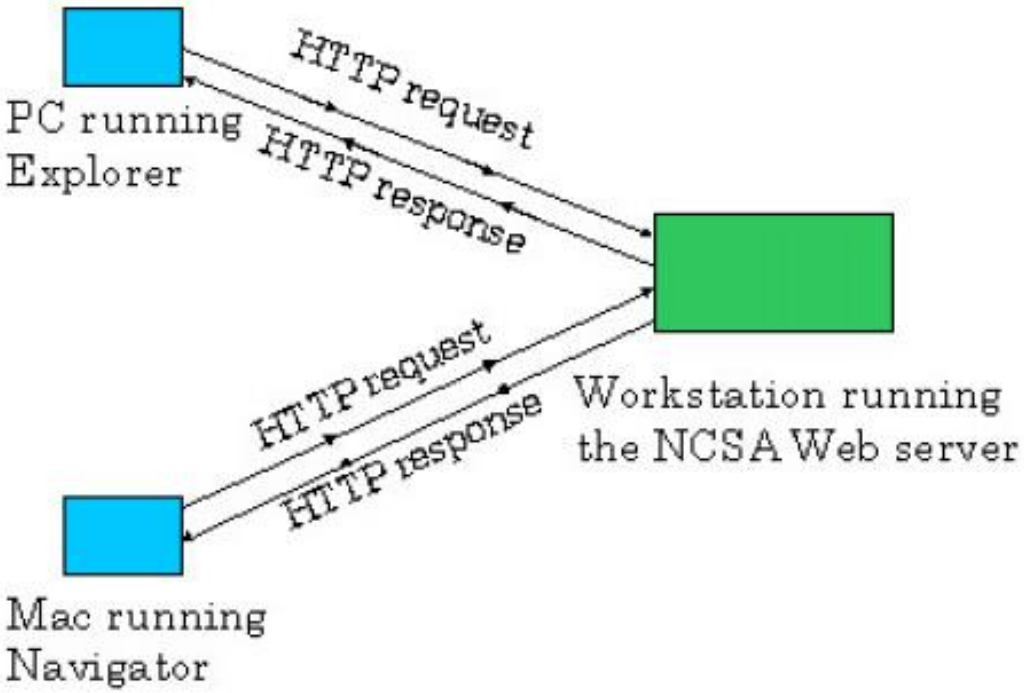
HTTP se implementa como dos programas:

- Programa cliente
- Programa servidor

HTTP define:

- Forma en que se comunican cliente y servidor
- Estructura de los mensajes entre cliente y servidor

HTTP


HTTP request
HTTP response
PC running
Explorer
HTTP request
HTTP response
Workstation running
the NCSA Web server
Mac running
Navigator

HTTP

Características

HTTP/1.0, HTTP/1.1 y HTTP/1.2 usan como protocolo en la capa de transporte a TCP. Cliente y Servidor intercambian información a través de sockets

HTTP emplea una sola conexión TCP para el control de la conexión y el envío de información (***in-band***)

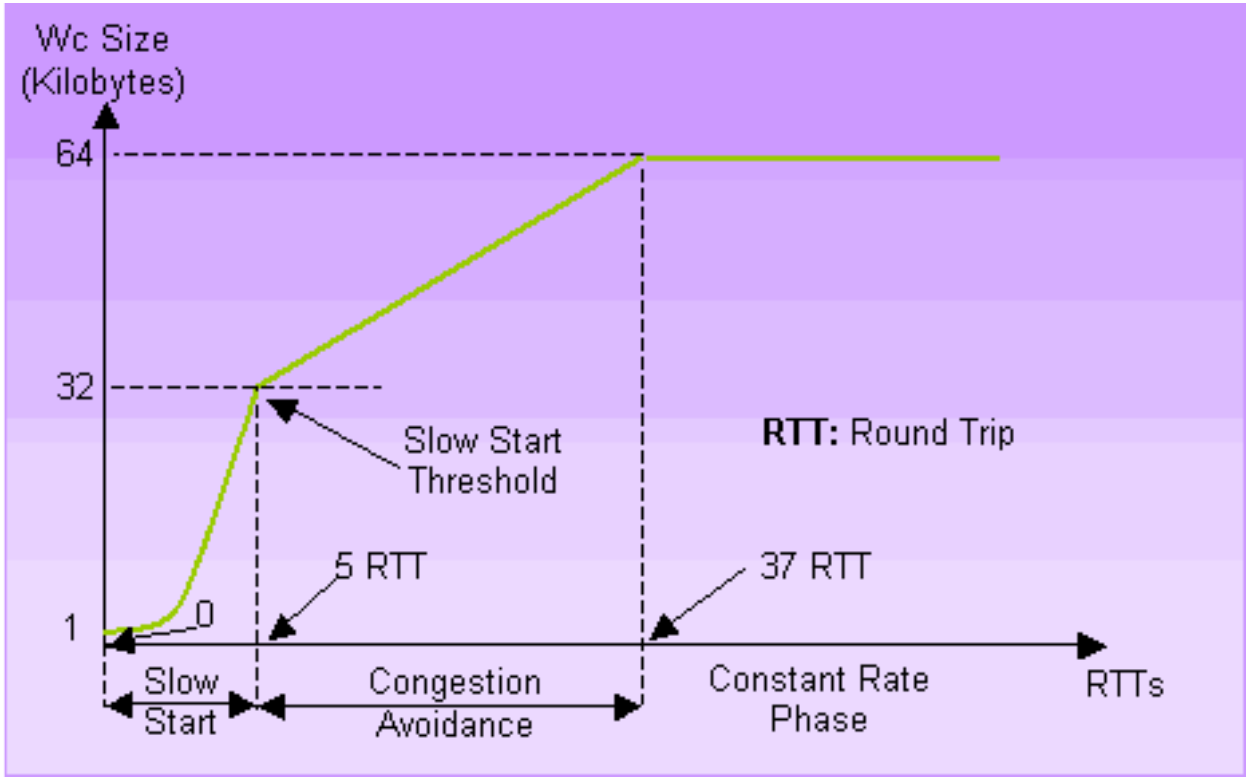
El modo de funcionamiento de HTTP es obtener información que alguien almacena en un servidor (***pull protocol***)

HTTP

- HTTP y TCP -

TCP emplea un mecanismo de control de congestión que obliga a iniciar la transmisión a una tasa baja (***slow start***) y dependiendo de las condiciones de la red (congestión) pasar a una tasa mayor

HTTP


Wc Size
(Kilobytes)
64
32
1
0
Slow Start
Threshold
5 RTT
37 RTT
RTT: Round Trip
Slow
Start
Congestion
Avoidance
Constant Rate
Phase
RTTs

HTTP

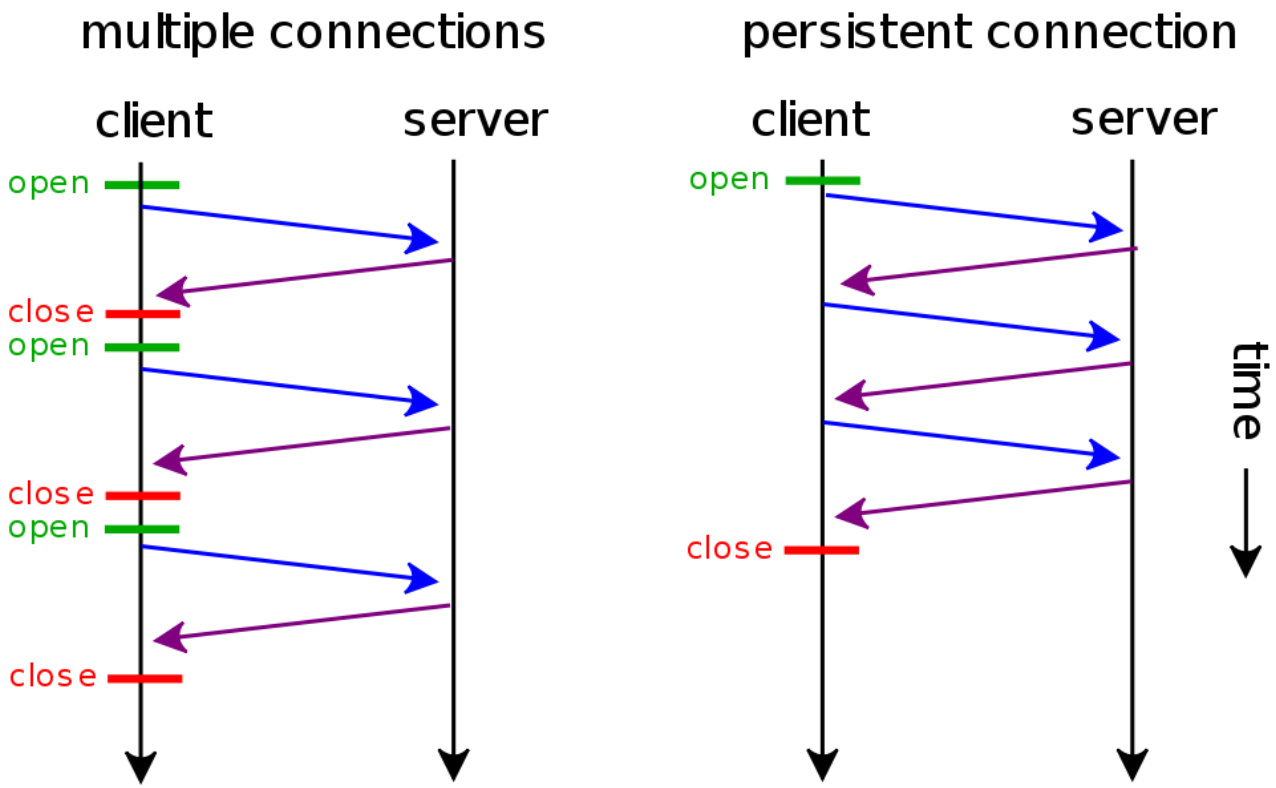
Características

HTTP es un protocolo sin estado (***stateless***). El servidor reenvía un objeto en caso de ser solicitado dos o mas veces (Sin cache)

HTTP puede usar conexiones persistentes (una sola conexión TCP) o no persistentes (múltiples conexiones TCP). Las conexiones persistentes pueden ser de dos tipos: con ***pipelining*** o ***sin pipelining***

Por defecto: HTTP/1.0 (no persistentes), HTTP/1.1 (persistentes)

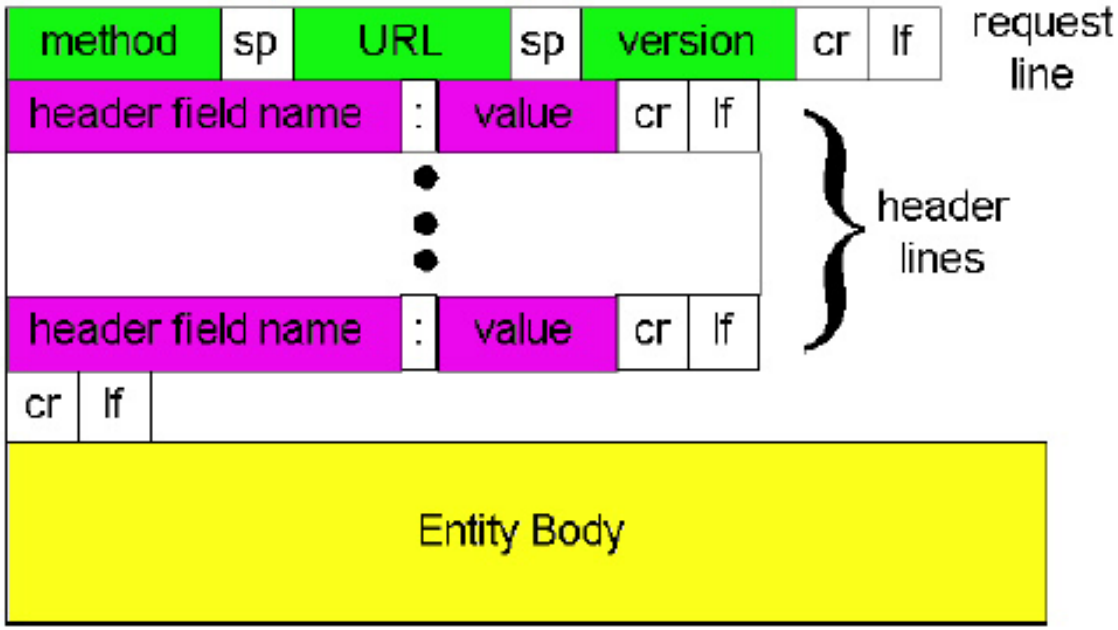
HTTP


multiple connections
client
server
open
close
open
close
open
close
persistent connection
client
server
open
close
time

HTTP

Comunicación - Formato de Mensajes

Un mensaje de solicitud presenta el siguiente formato:



HTTP

Comunicación - Formato de Mensajes

Un ejemplo de un mensaje de solicitud es el siguiente:

GET /somedir/page.html/ HTTP/1.1

Connection: close

User-agent: Mozilla/4.0

Accept: text/html, image/gif, image/jpeg

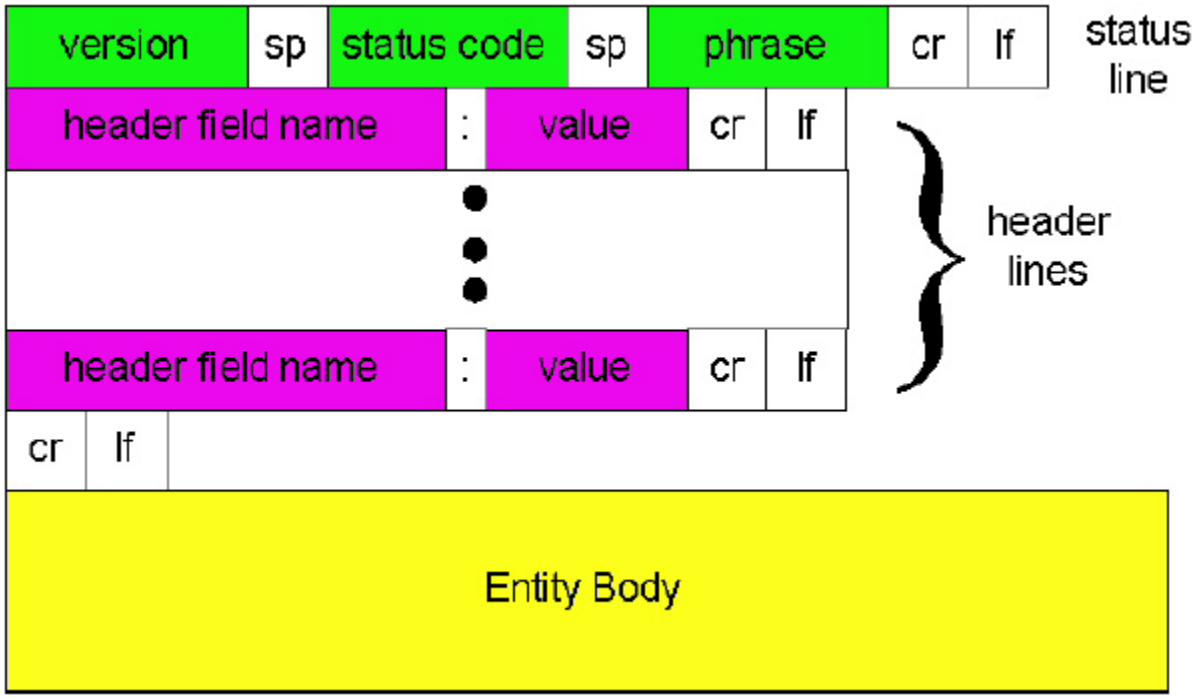
Accept-language: fr

(retorno de carro y nueva línea adicional)

HTTP

Comunicación - Formato de Mensajes

Un mensaje de respuesta presenta el siguiente formato:



HTTP

Comunicación - Formato de Mensajes

Un ejemplo de un mensaje de respuesta es el siguiente:

HTTP/1.1 200 OK

Connection: close

Date: Thu, 06 Aug 1998 12:00:15 GMT

Server: Apache/1.3.0 (Unix)

Last-Modified: Mon, 22 Jun 1998 09:23:24 GMT

Content-Length: 6821

Content-Type: text/html

data data data ...

HTTP

Comunicación – Estados Comunes

Algunos estados comunes y frases asociadas son:

200 OK

301 Moved Permanently

400 Bad Request

404 Not Found

505 HTTP Version Not Supported

HTTP

Comunicación (Ejercicio)

1. Inicie la ejecución de la maquina virtual proporcionada
2. Desde un cliente digitar lo siguiente:

>telnet 175.40.0.2 80

GET /index.html HTTP/1.0

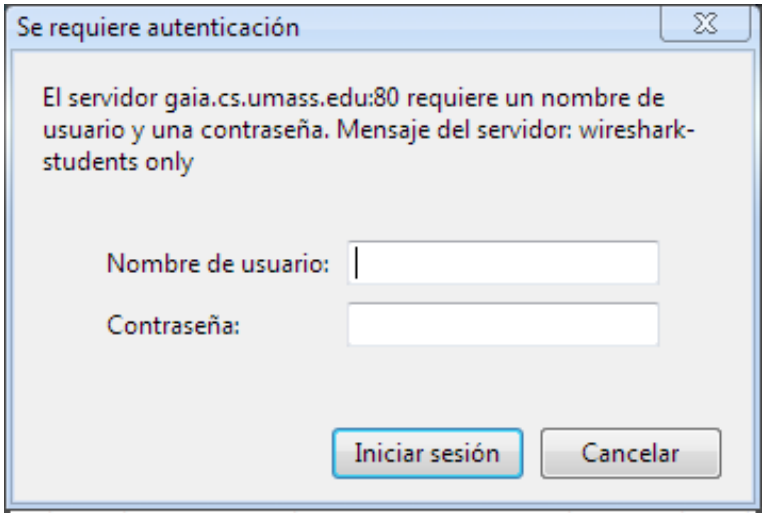
*Presionar ENTER dos veces después de escribir la segunda línea

3. Por medio de ***Wireshark*** hacer seguimiento de los mensajes que se intercambian en la red

HTTP

Autenticación y Cookies

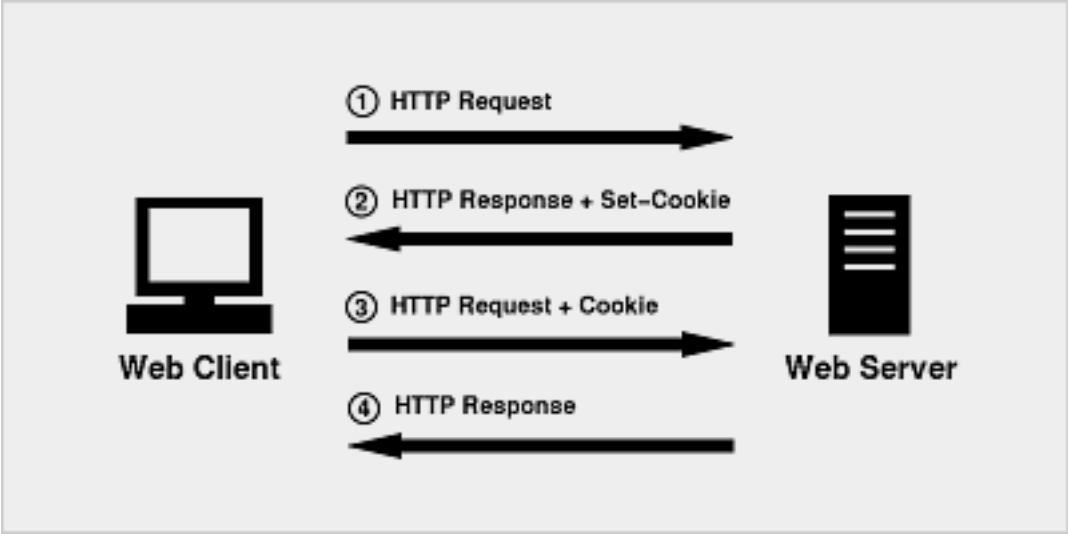
Algunos sitios requieren un usuario y contraseña para el acceso a la información. HTTP provee códigos de estado y cabeceras para realizar autenticación



HTTP

Autenticación y Cookies

Las cookies son una alternativa para llevar un seguimiento de los usuarios.



HTTP

Autenticación y Cookies

Cuando un usuario visita un lugar que emplea cookies, la respuesta del servidor incluye una cabecera especial y un número de identificación:

Set-cookie: 1678453

El cliente almacena el numero de identificación y el hostname en un archivo. En nuevas solicitudes el cliente incluye en el mensaje la siguiente línea:

Cookie: 1678453

HTTP

Autenticación y Cookies (Ejercicio)

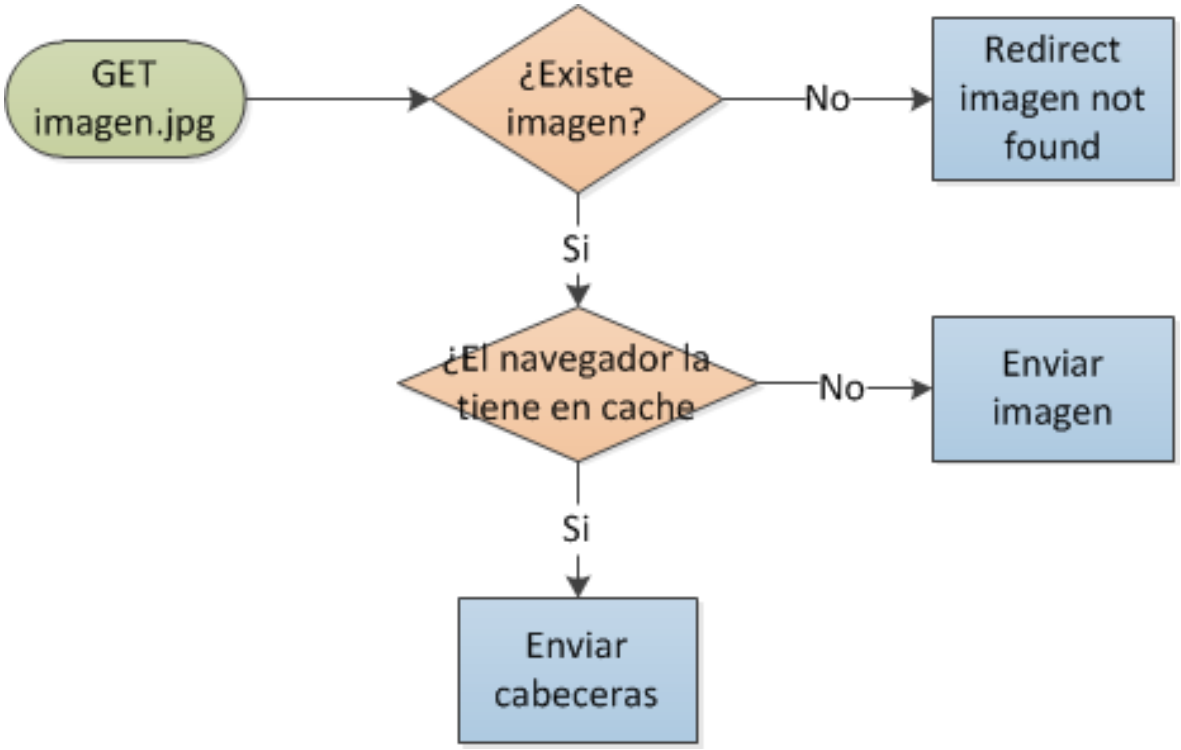
1. Inicie la ejecución de la maquina virtual proporcionada
2. Ingrese en la URL 175.40.0.2/ejemplos/cookies/cookies.php
3. Verifique por medio de **Wireshark** como la cookie conserva la opción de color seleccionada tras un nuevo acceso

HTTP

Cache

Almacenando los objetos devueltos se reduce el tráfico Web en Internet. Los caches Web pueden estar en el cliente o en un servidor de cache

HTTP


GET
imagen.jpg
¿Existe
imagen?
No
Redirect
imagen not
found
Si
¿El navegador la
tiene en cache
No
Enviar
imagen
Si
Enviar
cabeceras

HTTP

Cache

HTTP tiene un mecanismo para actualizar la información del cache una vez es modificada en el servidor. Este mecanismo se llama ***conditional GET***

HTTP

Cache - Conditional GET (Ejemplo)

Mensaje de solicitud

GET /fruit/kiwi.gif HTTP/1.0

User-agent: Mozilla/4.0

Accept: text/html, image/gif, image/jpeg

HTTP

Cache - Conditional GET (Ejemplo)

Mensaje de respuesta

HTTP/1.0 200 OK

Date: Wed, 12 Aug 1998 15:39:29

Server: Apache/1.3.0 (Unix)

Last-Modified: Mon. 22 Jun 1998 09:23:24

Content-Type: image/gif

data data data …

HTTP

Cache - Conditional GET (Ejemplo)

Mensaje de solicitud

GET /fruit/kiwi.gif HTTP/1.0

User-agent: Mozilla/4.0

Accept: text/html, image/gif, image/jpeg

If-modified-since: Mon, 22 Jun 1998 09:23:24

HTTP

Cache - Conditional GET (Ejemplo)

Mensaje de respuesta

HTTP/1.0 304 Not Modified

Date: Wed, 19 Aug 1998 15:39:29

Server: Apache/1.3.0 (Unix)

(empty entity body)

HTTP

Cache - Conditional GET (Ejercicio)

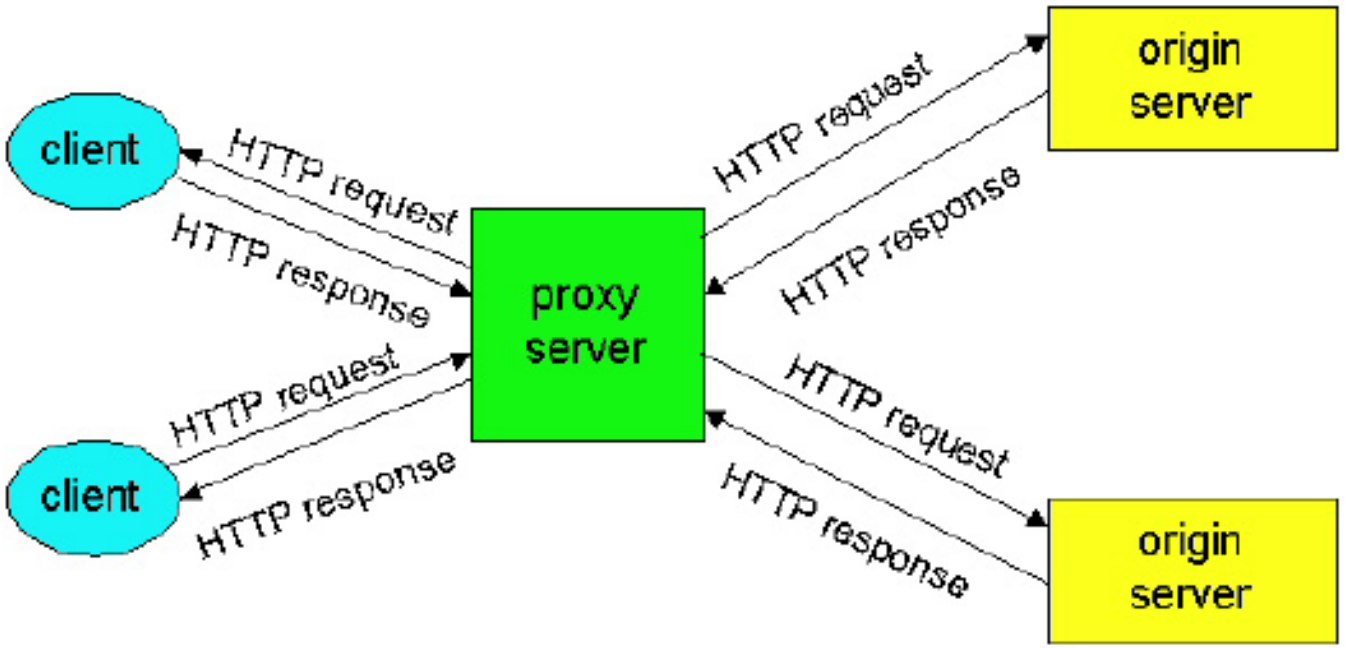
1. Inicie la ejecución de la maquina virtual proporcionada
2. Ingrese en la URL 175.40.0.2/ejemplos/cache/index.html
3. Verifique por medio de **Wireshark** que al cargar nuevamente la pagina no se envían la imagen

HTTP

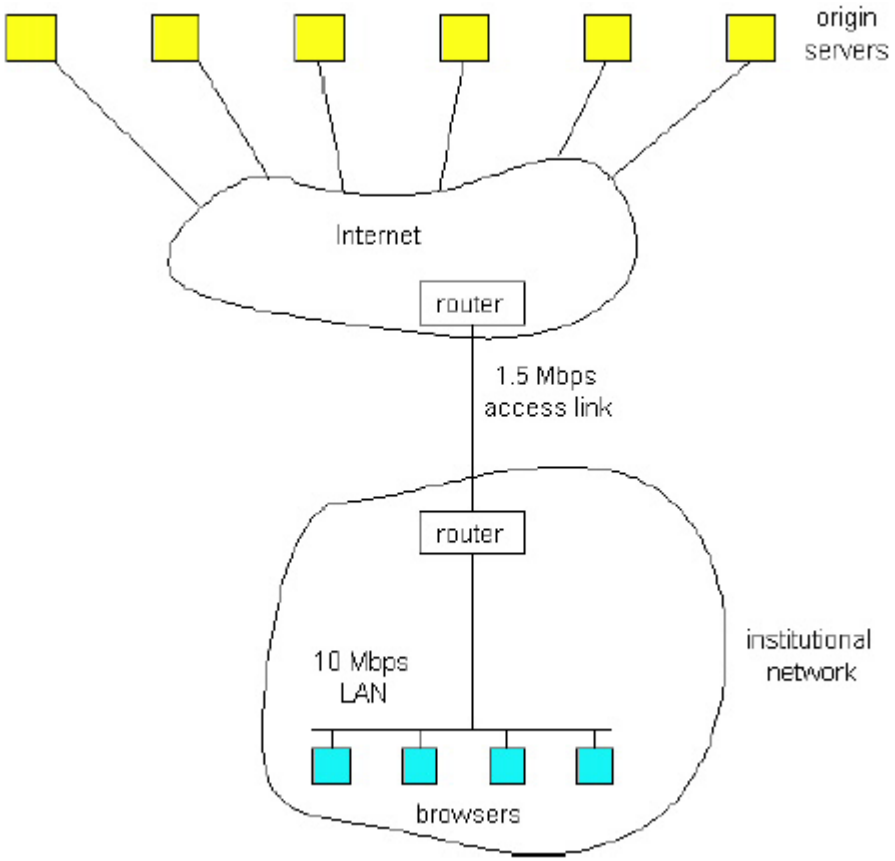
Cache Web o Servidor Proxy

Un servidor proxy almacena copias de objetos solicitados recientemente. Las peticiones desde los navegadores son redirigidas al servidor proxy

HTTP


client
client
proxy server
origin server
origin server
HTTP request
HTTP response
HTTP request
HTTP response
HTTP request
HTTP response
HTTP request
HTTP response

HTTP


origin
servers
Internet
router
1.5 Mbps
access link
router
10 Mbps
LAN
institutional
network
browsers

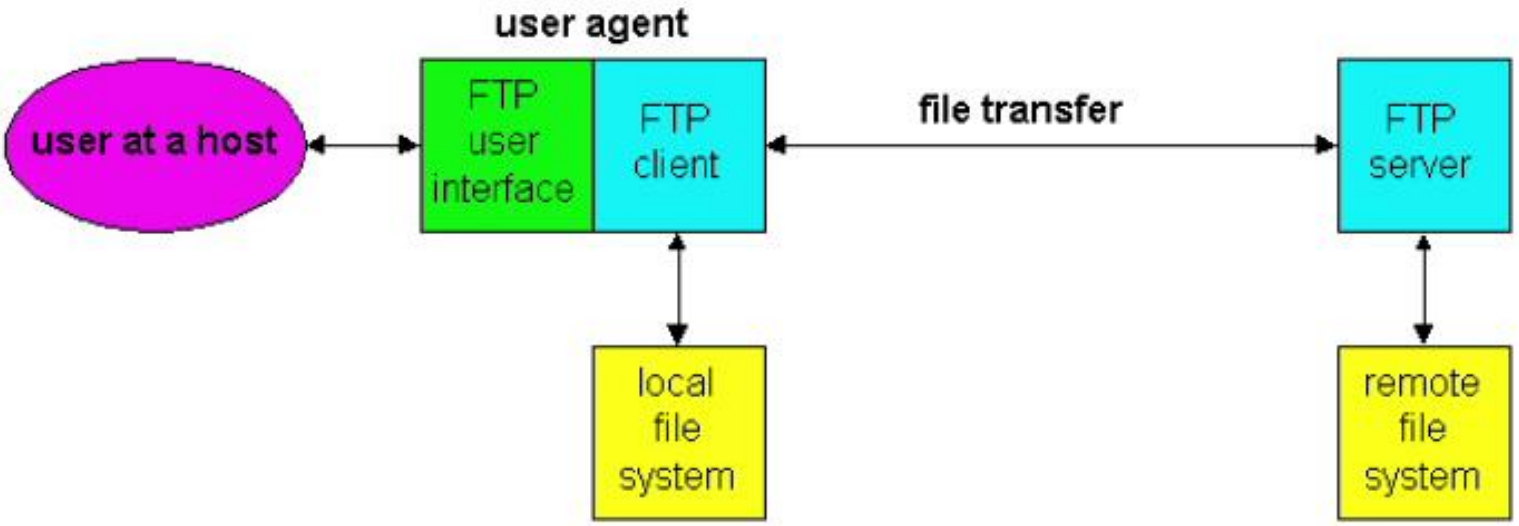
FTP

Introducción

Es un protocolo para la transferencia de archivos

Es una sesión FTP el usuario se autentica (nombre de usuario, contraseña) y transfiere archivos de un sistema local a un sistema remoto

FTP


user agent
user at a host
FTP user interface
FTP client
file transfer
FTP server
local file system
remote file system

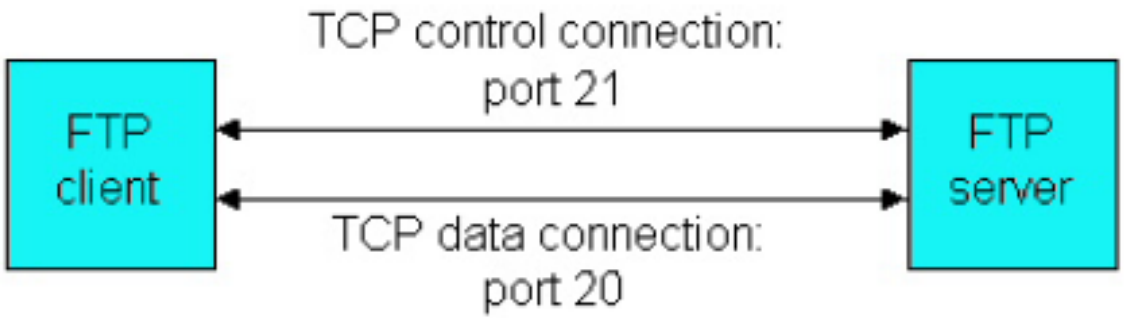
FTP

Características

FTP usa como protocolo de la capa de transporte a TCP

FTP emplea dos conexiones TCP paralelas para la transferencia de un archivo. Una de ellas para el control de la conexión y otra para la información (***out-of-band***)

FTP


TCP control connection:
port 21
FTP
client
FTP
server
TCP data connection:
port 20

FTP

Comunicación

Cuando un usuario inicia una sesión FTP con un equipo remoto, primero se establece una conexión TCP de control en el puerto 21 del equipo remoto

A través de esta conexión se envía información como: usuario, contraseña, comandos para cambiar el directorio remoto, comando para obtener un archivo (get) ó subir un archivo (put)

FTP

Comunicación

Al momento de transferir un archivo FTP establece una conexión TCP en el puerto 20 del equipo remoto. FTP envía únicamente un archivo y luego cierra la conexión de datos (la conexión de control permanece activa durante la sesión)

FTP es un protocolo con estado (***state***). FTP asocia la conexión de control con un usuario y debe realizar un seguimiento de los cambios en el equipo remoto (estructura de archivos)

FTP

Comunicación – Comandos Comunes

USER username: se emplea para enviar el usuario

PASS password: se emplea para enviar la contraseña

LIST : se emplea para listar los archivos del directorio actual

RETR filename: se emplea para obtener un archivo

STOR filename: se emplea para subir un archivo

FTP

Comunicación – Respuestas Comunes

331 Username OK, password required

125 Data connection already open; transfer starting

425 Can’t open data connection

425 Error writing file

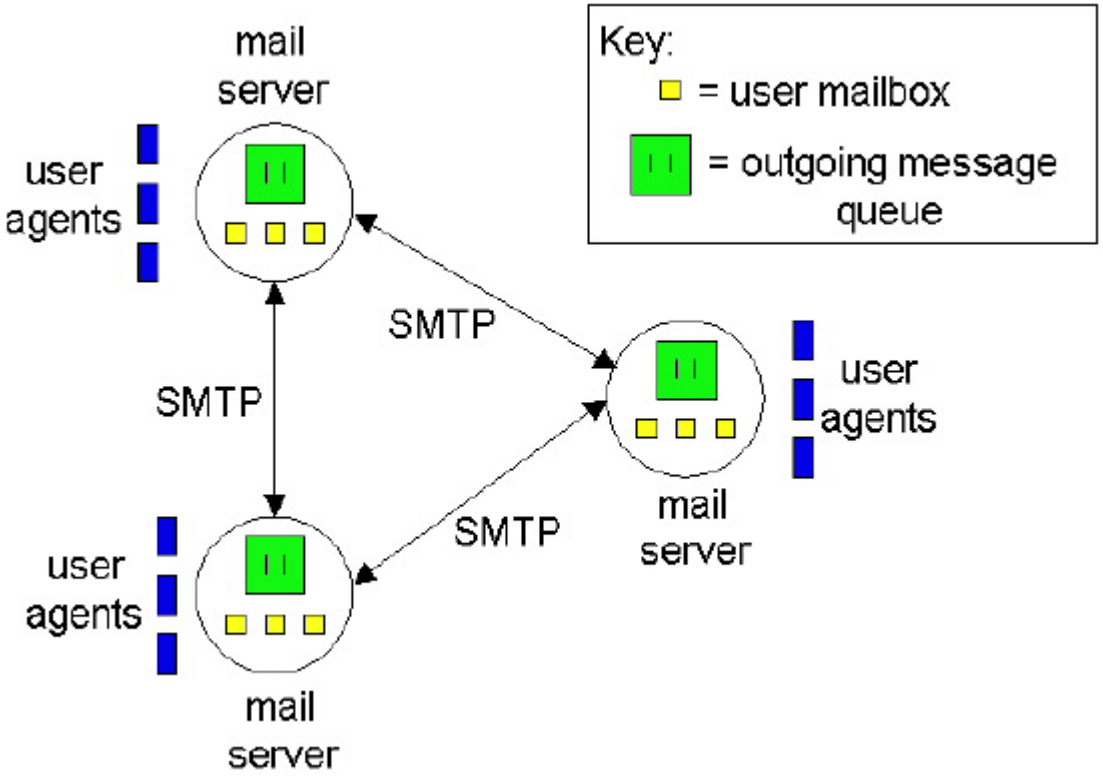
Correo Electrónico

Introducción SMTP

El servicio de correo electrónico tiene 3 componentes principales: los agentes de usuario (thunderbird, outlook), los servidores de correo y el protocolo de transferencia de correo SMTP (Simple Mail Transfer Protocol)

SMTP transfiere mensajes entre servidores de correo. Es mas antiguo que HTTP

Correo Electrónico



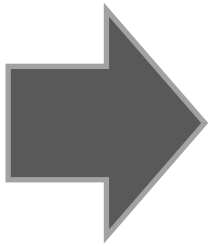
Correo Electrónico

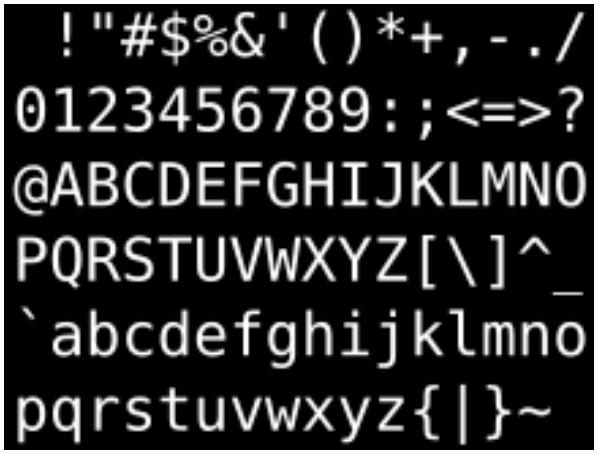
Características SMTP

SMTP restringe el cuerpo de los mensajes de correo a ASCII de 7 bits

SMTP desde su concepción restringe el cuerpo de los mensajes de correo a ASCII de 7 bits. Las aplicaciones de hoy requieren transmitir contenido multimedia (información binaria) por lo cual para estos casos se codifica la información multimedia en ASCII antes de ser enviada

Correo Electrónico





Correo Electrónico

Comunicación SMTP (Ejemplo)

>telnet hamburguer.edu 25

S: 220 hamburguer.edu

C: HELO crepes.fr

S: 250 Hello crepes.fr, pleased to meet you

C: MAIL FROM: <alice@crepes.fr>

S: 250 alice@crepes.fr … Sender ok

C: RCPT TO: <bob@hamburguer.edu>

S: 250 bob@hamburguer.edu... Recipient ok

Correo Electrónico

Comunicación SMTP (Ejemplo)

C: DATA

S: 354 Enter mail, end with "." on a line by itselft

C: Do you like ketchup?

C: How about pickles?

C: .

S: 250 Message accepte for delivery

C: QUIT

S: 221 hamburguer.edu closing connection

Correo Electrónico

Comunicación SMTP (Ejercicio)

Por medio del software ***Wireshark*** hacer seguimiento de los mensajes que se intercambian en la red

1. Inicie la ejecución de la maquina virtual proporcionada
2. Desde un cliente digitar lo siguiente:

>telnet 175.40.0.2 25

```
Trying 175.40.0.2...
Connected to 175.40.0.2.
Escape character is '^]'.
220 localhost.localdomain ESMTP Postfix
HELO
501 Syntax: HELO hostname
MAIL FROM: jacinto@facebook.com
250 2.1.0 Ok
RCPT TO: vagrant@localhost
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Hola mundo
.
250 2.0.0 Ok: queued as 85E386C027C
QUIT
221 2.0.0 Bye
```

Correo Electrónico

Características SMTP

El modo de funcionamiento de SMTP es enviar información hacia un servidor de correo receptor (***push protocol***)

SMTP emplea conexiones persistentes

SMTP encapsula todos los objetos a enviar en un solo mensaje

Correo Electrónico

Formato de Mensajes (DATA)

En un mensaje (información que se ingresa después de digitar el comando DATA) la cabecera y el cuerpo están separados por una línea.

Un ejemplo de cabecera es el siguiente:

From: alice@crepes.fr

To: bob@hamburguer.edu

Subject: Searching for the meaning of life

Correo Electrónico

Extensión MIME

Las cabeceras normales no permiten enviar información distinta a texto en ASCII

Para enviar información diferente a texto se incluyen nuevas cabeceras.

Dos cabeceras MIME son:

Content-Type: indica el tipo de contenido

Content-Transfer-Encoding: indica el tipo de codificación

Correo Electrónico

Extensión MIME

Content-Type presenta el siguiente formato:

Content-Type: type/subtype ; parameters

Correo Electrónico

Extensión MIME

Para cada tipo hay un subtipo asociado. Algunos ejemplos de tipos y subtipos son:

Texto: text/plain; charset = “ISO-8859-1”

Imagen: image/jpeg

Audio: audio/midi

Video: video/mpeg

Aplicación: application/pdf

Correo Electrónico

Extensión MIME (Ejemplo Envío 1)

From: alice@crepes.fr

To: bob@hamburguer.edu

Subject: Picture of yummy crepe

MIME-Version: 1.0

Content-Transfer-Encoding: base 64

Content-Type: image/jpeg

base 64 encoded data…

Correo Electrónico

Extensión MIME (Ejemplo Envío 2)

From: alice@crepes.fr

To: bob@hamburguer.edu

Subject: Picture of yummy crepe with commentary

MIME-Version: 1.0

Content-Type: multipart/mixed; Boundary=StartOfNextPart

--StartOfNextPart

Dear Bob,

Please find a picture of an absolutely scrumptious crepe

Correo Electrónico

Extensión MIME (Ejemplo Envío 2)

// salto de línea

--StartOfNextPart

Content-Transfer-Encoding: base 64

Content-Type: image/jpeg

base 64 encoded data…

Correo Electrónico

Extensión MIME (Ejemplo Envío 2)

// salto de línea

--StartOfNextPart

Let me know if you would like the recipe.

.

// salto de línea

Correo Electrónico

Extensión MIME (Ejemplo Recepción 1)

Received: from crepes.fr by pizza.edu ; 12 Oct 98 15:27:39 GMT

From: alice@crepes.fr

To: bob@pizza.edu

Subject: Picture of yummy crepe

MIME-Version: 1.0

Content-Transfer-Encoding: base 64

Content-Type: image/jpeg

base 64 encoded data…

Correo Electrónico

Protocolos de Acceso al Correo

SMTP es un ***protocolo push***. Por tanto cuando el destinatario desea leer los correos almacenados en su servidor de correo debe emplear un protocolo que permita **extraer** los mensajes del servidor

Dos protocolos de acceso al correo son: POP3 e IMAP

Correo Electrónico

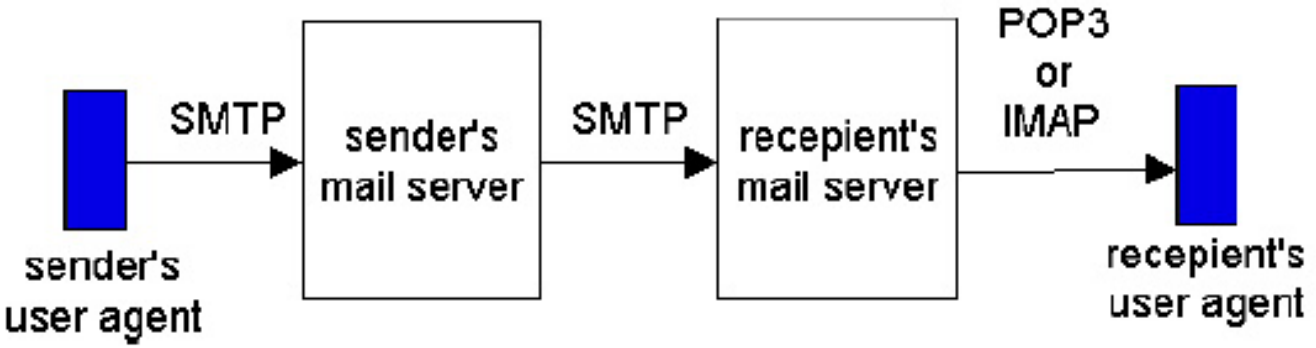


Figure 2.4-3: E-mail protocols and their communicating entities.

Correo Electrónico

POP3

POP3 se conecta al puerto TCP 110 del servidor de correo

POP3 permite crear carpetas y organizar mensajes en el equipo cliente pero no en el servidor de correo

POP3 presenta tres fases: autorización, transacción y actualización

Correo Electrónico

POP3 (Ejemplo)

>telnet mailServer 110

S: +OK POP3 server ready

C: user alice

S: +OK

C: pass hungry

S: +OK user successfully logged on

Correo Electrónico

POP3 (Ejemplo)

C: LIST

S: 1 498

S: 2 912

S: .

C: RETR 1

S: blah blah

C: DELE 1

C: QUIT

Correo Electrónico

POP3 (Ejercicio)

Por medio del software ***Wireshark*** hacer seguimiento de los mensajes que se intercambian en la red

1. Inicie la ejecución de la maquina virtual proporcionada
2. Desde un cliente digitar lo siguiente:

>telnet 175.40.0.2 110

S: +OK POP3 server ready

C: user vagrant

S: +OK

C: pass vagrant

S: +OK user successfully logged on

C: LIST

S: 1 498

S: .

C: RETR 1

S: blah blah

C: DELE 1

C: QUIT

Correo Electrónico

IMAP

IMAP se conecta al puerto TCP 143 del servidor de correo

IMAP permite crear carpetas y organizar mensajes en el servidor de correo: IMAP debe mantener el estado de la estructura de directorios de todos los usuarios

IMAP presenta cuatro fases: no autenticado, autenticado (permite seleccionar carpetas), seleccionado (permite modificar mensajes) y desconectado

Correo Electrónico

IMAP (Ejercicio)

Configure en una máquina virtual un servidor de correo (SMTP+postfix+dovecot)

Por medio del agente de usuario para correo electrónico Mozilla Thunderbird configure una conexión IMAP hacia el servidor correo

Correo Electrónico

HTTP

Cuando se emplea una pagina web de un proveedor de correo electrónico la conexión entre el cliente y el servidor de correo se realiza por medio de HTTP (no se emplea POP3 o IMAP)

Para la comunicación entre servidores de correo se emplea SMTP

Programación con Sockets

Fuentes

Cliente – Servidor con TCP

TCPServer.java

TCPClient.java

Cliente – Servidor con UDP

UDPServer.java

UDPClient.java

Programando un Servidor Web

Fuentes

Servidor Web en Java

Webserver.java

Bibliografía

Computer Networking: A Top-Down Approach
Sexta Edición (2012)
James F. Kurose and Keith W. Ross

Using Snort and Ethereal to Master The 8 Layers Of An Insecure Network
Primera Edición (2006)
Michael Gregg, Stephen Watkins, George Mays, Chris Ries, Ronald M. Bandes, Brandon Franklin

Enlaces Adicionales

RFC's

HTTP - http://tools.ietf.org/html/rfc2616

FTP – http://www.rfc-es.org/rfc/rfc0959-es.txt

Páginas WEB

http://code.google.com/p/dvwa/

http://atenlabs.com/blog/how-to-steal-facebook-authentication-cookies/

http://noclickemail.com/

http://www.hotcleaner.com/cookies.html

MIME Extensions - http://www.feedforall.com/mime-types.htm

Asesorías

daniel.barragan@correounivalle.edu.co

Edificio 331 – Oficina 2114

Miércoles 9:00 am – 12:00 am


ERROR:
404
ROAD NOT FOUND
??
Real life begins to adopt the more recognizable signage of the internet.