

Comunicacións e Sistemas Multimedia



Alberto Alonso Ruibal

alberto@alonsoruibal.com

<http://www.alonsoruibal.com>

Twitter: [@albertoruibal](https://twitter.com/albertoruibal)

O Servizo DNS (Domain Name System)

Introducción

- O DNS utilízase principalmente para a resolución de nomes, isto é, averiguar qué dirección IP pertence a determinado nome completo de host
- É unha base de datos distribuída e xerárquica
- É o primeiro que se consulta antes de facer unha petición a un servidor web ou de correo

Funcións do DNS

- **Resolución de nomes:** Dado o nome completo dun host (por exemplo `www.aulaestudio.com`), obte-lo seu enderezo IP
- **Resolución inversa de direccións:** É o mecanismo inverso o anterior. Consiste en, dado un enderezo IP, obte-lo nome asociado ó mesmo
- **Resolución de servidores de correo:** Dado un nome de dominio (por exemplo `gmail.com`) obter o servidor a través do cal debe realizarse a entrega do correo electrónico

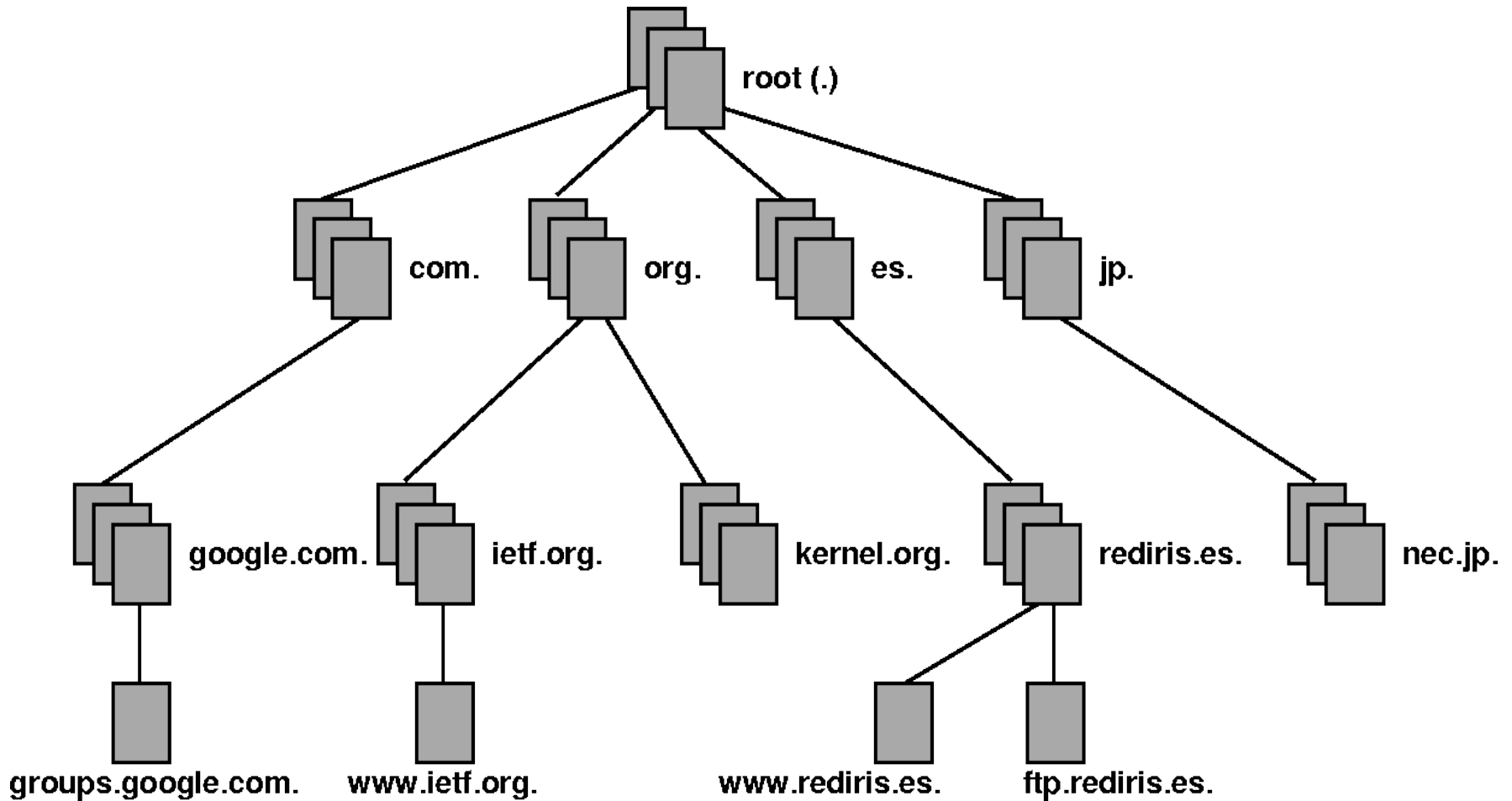
Terminoloxía

- **Host Name:** O nome dun host é unha sola "palabra" (formada por letras, números e guións)
- **Fully Qualified Host Name (FQHN):** É o "nome completo" dun host. Está formado polo hostname, seguido dun punto e o seu correspondiente nome de dominio. Por exemplo, "hostname.dominio.com"
- **Domain Name:** O nome de dominio é unha sucesión de nomes concatenados por puntos
- **Top Level Domains (TLD):** Os dominios de nivel superior (root servers) son aqueles que non pertencen a outro dominio. Exemplos de este tipo son "com", "org", "es"...

Arquitectura (I)

- O sistema DNS funciona principalmente en base ó protocolo UDP (porto 53)
- O sistema está estruturado en forma de árbol. Cada nodo do árbol componse dun grupo de servidores que se encargan de resolver un conxunto de dominios (zona). Un servidor pode delegar en outro (ou outros) a autoridade sobre algunha das súas sub-zonas (esto é, algún subdominio da zona sobre a que él ten autoridade).
- Un subdominio pode verse como unha especialización dun dominio de nivel anterior

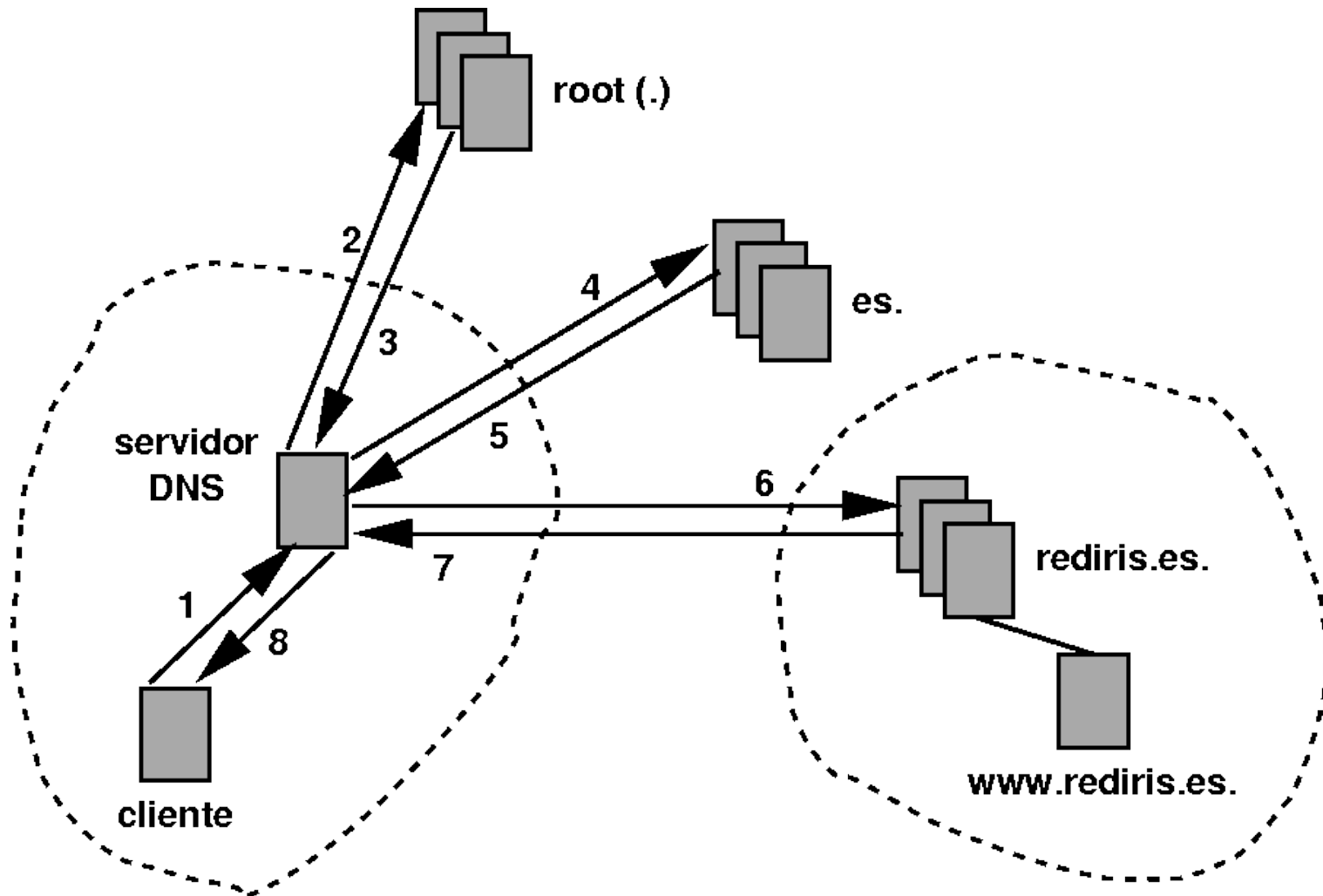
Arquitectura (II)



O proceso de resolución (I)

- O cliente consulta ó servidor de nomes inicial
- O servidor de nomes inicial consulta a un dos servidores raíz (do cal debe coñecer previamente a dirección IP)
- Este devolve o nome do servidor a quen teña delegada a sub-zona
- O servidor inicial interroga o novo servidor
- O proceso repítese novamente se hai unha sub-zona delegada
- Ó obter o nome do servidor con autoridade sobre a zona en cuestión, o servidor inicial o interroga
- O servidor resolve o nome correspondiente, se este existe
- O servidor inicial informa ó cliente do nome resolto

O proceso de resolución (II)



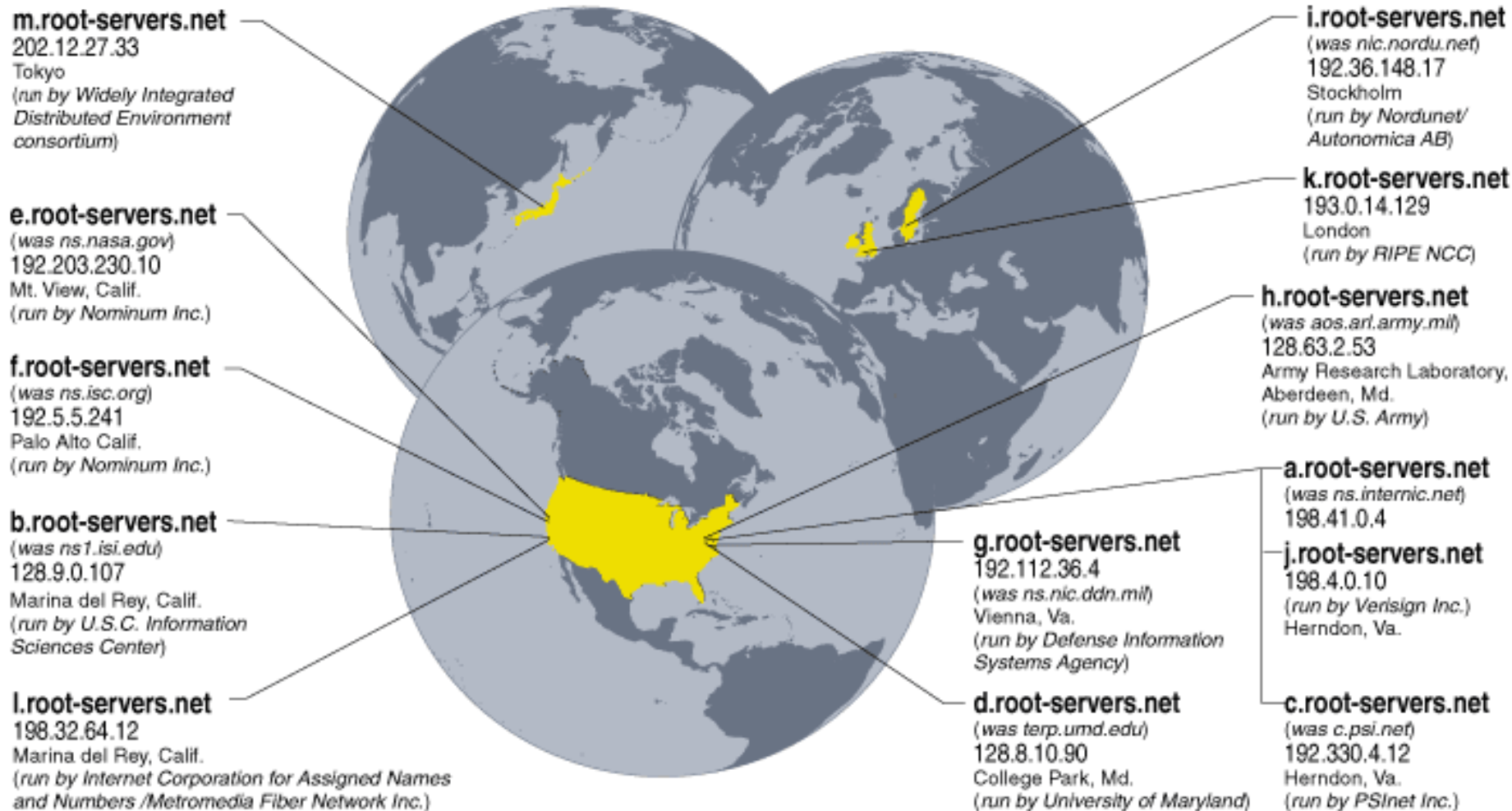
Tipos de entradas

- **A (Address):** Este rexistro se utiliza para traducir nomes de hosts do dominio en cuestión a direccións IP
- **CNAME (Canonical Name):** É un alias para un host determinado. (Non define unha dirección IP, senón un novo nome)
- **NS (Name Server):** Especifica o servidor (ou servidores) de nomes para un dominio. Tamén serve para delegar zonas.
- **MX (Mail Exchange):** Define o(s) servidor(es) encargado(s) de recibi-lo correo electrónico para o dominio
- **PTR (Pointer):** Especifica un "rexistro inverso", á inversa do rexistro A, permitindo a traducción de direccións IP a nomes
- **TXT (Text):** Permite asociar información adicional a un dominio. Isto é utilizado para outros fins, como o almacenamiento de claves de cifrado, "DomainKeys" o "Sender Policy Framework"
- **SOA (Start Of Address):** Contén información do servidor dns principal, o correo do administrador e os tempos de vida por defecto

A caché no DNS

- Cada vez que un servidor de nomes envía unha resposta, faino adxuntando o tempo de validez da mesma (TTL o "tempo de vida"). Isto posibilita que o receptor, ante a necesidade de volver a resolve-la mesma consulta, poida utilizar a información previamente obtida en vez de realizar unha nova petición
- Isto provoca un “Tempo de propagación de DNS”

Os servidores DNS raíz



Consultando ó DNS

Utilizaremos o comando **dig**:

dig [@server] [-p port#] [name] [type]

- **@server**: nome ou dirección IP do servidor DNS ó que se lle fai a consulta. Se non se especifica, consulta os servidores que se listan no ficheiro `/etc/resolv.conf`
- **-p port**: serve para indicar un porto de servidor distinto do de por defecto (53)
- **name**: nome do rexistro que se desexa consultar
- **type**: tipo do rexistro de a consultar: ANY, A, MX, etc. Se non se especifica nengún, por defecto é de tipo A.

O servidor de nomes BIND

- Prácticamente o único software utilizado nos servidores de nomes de Internet é **BIND** ("Berkeley Internet Name Domain"),
- Este programa, distribuido baixo unha licenza libre, é utilizado en prácticamente tódolos sistemas Unix do mundo
- Nos sistemas linux se chama **named**, e se arranca/para con

```
/etc/init.d/bind9 start
```

```
/etc/init.d/bind9 stop
```

Crear unha zona no BIND (I)

- Instalar o servidor de nomes named con apt-get:

```
apt-get install bind9
```

- Edita-lo arquivo `/etc/bind/named.conf.local`

```
zone "aulaestudio.com" {  
    type master;  
    file "/etc/bind/db.aulaestudio";  
};
```

Crear unha zona no BIND (II)

```
• /etc/bind/db.aulaestudio
```

```
$TTL 86400
```

```
@      IN      SOA    ns.aulaestudio.com. admin.aulaestudio.com. (
```

```
        200403031
```

```
        28800
```

```
        7200
```

```
        604800
```

```
        86400 )
```

```
        NS    ns.aulaestudio.com.
```

```
        MX    10 mail.aulaestudio.com.
```

```
ns      A      192.168.1.1
```

```
mail    A      192.168.1.2
```

```
www     CNAME   ns
```


Delegación de zonas DNS

- A delegación dunha zona se fai introducindo un rexistro NS apuntando ó servidor DNS que vai xestionar a zona delegada
- A xerarquía DNS fórmase por sucesivas delegacións de zonas

Internationalized Domain Name

- É un nome de dominio de Internet que pode conter caracteres non ASCII
- Foi implantado no 2005
- Exemplo de codificación:

Ñandú.cl -> xn--and-6ma2c.cl

As URLs (Uniform Resource Locator)

As URLs

- Serven para dar a ubicación dun recurso numha rede
- Teñen o formato xenérico:

esquema://máquina/directorio/arquivo

- Os esquemas poden ser: http, https, ftp, mailto, file...
- O formato pode ser máis específico:

esquema://usuario:contraseña@máquina:porto/directorio(s)
/arquivo

O Servizo HTTP (HyperText Transfer Protocol)

Introducción

- É o protocolo que se utiliza para o acceso a maior parte do contido que hai en Internet (páxinas web)
- HTTP foi desenvolvido polo World Wide Web Consortium e a Internet Engineering Task Force, colaboración que culminou en 1999 coa publicación dunha serie de RFCs
- Protocolo baseado en mensaxes de texto plano (se pode simular utilizando a aplicación telnet)
- Os servidores HTTP escoitan normalmente na porta TCP 80 (HTTPS no 443)

Exemplo de petición HTTP

- Isto é un exemplo do que envía o noso navegador a un servidor web cando pide a páxina web <http://www.aulaestudio.com/index.php>

GET /index.php HTTP/1.1

Host: www.aulaestudio.com

User-Agent: nome-cliente

[liña en branco]

Exemplo de resposta HTTP

HTTP/1.1 200 OK

Date: Fri, 21 Dec 200 22:00:00 GMT

Content-Type: text/html

Content-Length: 1024

<html>

<body>

<h1>Título</h1>

...

</body>

</html>

Anatomía da petición HTTP

- A petición HTTP está composta por
TIPO_PETICION RECURSO PROTOCOLO
<Cabeceiras>

<Datos>

- TIPO_PETICION: pode ser GET ou POST, esta última leva contido na parte <Datos>
- RECURSO: nome do recurso
- PROTOCOLO: normalmente “HTTP/1.1”

Anatomía da resposta HTTP

- A resposta HTTP está composta por
PROTOCOLO CODIGO_DE_RESPOSTA MENSAXE
<Cabeceiras>

<Datos>

- PROTOCOLO: normalmente “HTTP/1.1”
- Código de resposta: explicando o resultado da petición
- MENSAXE: explicando o código de resposta

Códigos de resposta HTTP

- 2xx: Peticións correctas:
 - 200: OK
- 3xx: Redireccións
 - 302: Movido Temporalmente
- 4xx: Erros do cliente
 - 401: Non autorizado
 - 403: Prohibido
 - 404: Non atopado
- 5xx: Erros de servidor
 - 500: Erro interno

Cabeceiras HTTP

- Teñen seguinte formato:

Clave: valor

- Exemplos de cabeceiras da petición

Host: `www.aulaestudio.com`

User-Agent: `Mozilla/5.0 (X11; U; Linux i686; gl; rv:1.9.2.2) Gecko/20100316 Firefox/2.0.0.3`

- Exemplos de cabeceiras da resposta

Content-Type: `text/html`

Content-Length: `7839`

Servidores multidominio

- Permiten aloxar múltiples dominios sobre un só enderezo IP
- Distinguen os dominios que aloxan segundo a cabeceira “Host”
- Só e posible con Http v1.1
- Non funciona co protocolo seguro HTTPs

O servidor HTTP Apache

- É o servidor HTTP máis usado en Internet, de código aberto e dispoñible para case todos os sistemas operativos
- A fundación Apache mantén ademais outros moitos proxectos de software libre (Tomcat, Jakarta...)
- <http://www.apache.org>



A configuración do Apache (I)

Divídese en distintos ficheiros:

- **`/etc/apache2/apache2.conf`**: ficheiro principal de configuración
- **`/etc/apache2/conf.d/`**: directorio con ficheiros de configuración adicional
- **`/etc/apache2/mods-enabled/`**: directorio con enlaces simbólicos os arquivos no outro directorio `mods-available/` para activar uns módulos ou outros
- **`/etc/apache2/sites-enabled/`**: idem, pero coa configuración dos VirtualHosts

A configuración do Apache (II)

As directivas de configuración agrúpanse en distintos niveis indicados dentro de “tags”:

- <VirtualHost>: para configurar un host virtual
- <Directory>: para engadir configuracións asociadas a un directorio do servidor
- <Location>: para configuracións asociadas a unha “ubicación” dentro do dominio
- <Files>: para facer configuracións relativas a un conxunto de ficheiros

A configuración do Apache (III)

Algunhas directivas de configuración:

- Listen: A porta na que escoita o servidor
- DocumentRoot: o directorio do servidor cos arquivos a servir
- ServerAdmin: o enderezo de correo do administrador do servidor
- ServerName: no nome de dominio se devolverá ós clientes
- CustomLog: arquivo onde se gardará o rexistro de accesos
- LogFormat: define o formato para o ficheiro de rexistro
- ErrorLog: arquivo onde se gardará o rexistro de error
- ErrorDocument: asociación dun documento a un tipo de erro
- Include: inclúe outro ficheiro de configuración
- ...

Os módulos de Apache

Apache dispón de distintos módulos que amplían súa funcionalidade básica

- Alias: Permite usar a directiva Alias para engadir ligazóns
- Auth*: autenticación de usuarios
- Cgi: permite executar CGI's
- Gzip: permite a compresión do contido antes de envialo ó cliente
- PHP: permite a execución de scrips PHP
- Proxy: permite facer funcións de proxy
- Rewrite: reescritura de URL's e redireccións
- SSL: permite usar o Apache como un servidor HTTPS
- ...

Proxies HTTP

- Fan de punto intermedio nas peticións HTTP entre o noso navegador e o servidor HTTPD final
- Para o servidor final as peticións HTTP proceden do servidor proxy
- Función de caché, balance de carga, control de acceso ou tamén para mellorar a privacidade
- Os máis usados son o ISA Server ou o Squid (<http://www.squid-cache.org/>)

O Correo Electrónico

O correo electrónico

- Servizo que permite os usuarios enviar e recibir mensaxes
- Baseado en protocolos de texto plano
- Os enderezos de correo teñen o formato:

usuario@servidor

Utilízase unha @ para separar o nome de usuario do servidor no que aloxa o seu correo

- Os dominios de correo son resoltos coas entradas MX no DNS

Protocolos de correo electrónico

Para envío:

- SMTP: Simple Mail Transfer Protocol

Para recollida:

- POP: Post Office Protocol
- IMAP: Internet Message Access Protocol

Todos estes protocolos teñen o seu equivalente sobre unha conexión segura (SSL)

O protocolo SMTP

- Escoita na porta TCP 25 por defecto
- Defínese no RFC 821
- Comandos básicos:
 - HELO: identifica o host cliente ante o servidor
 - MAIL FROM: indica o enderezo de correo do remitente
 - RCPT TO: indica o(s) destinatario(s) do correo
 - DATA: permite especificar o corpo da mensaxe
 - QUIT: pecha a conexión

Códigos de resposta SMTP

A cada comando o servidor resposta cunha mensaxe con formato “CODIGO MENSAXE”, no que código toma os seguintes valores:

- 2XX éxito
- 3XX a orde foi aceptada, pero o servidor esta pendente de que o cliente lle envíe novos datos para termina-la operación
- 4XX erro, pero espera que se repita a instrucción
- 5XX, erro permanente, polo que non debe repetirse a orde

Exemplo de Comunicación

S: 220 Servidor ESMTTP

C: HELO miequipo.midominio.com

S: 250 Hello, please to meet you

C: MAIL FROM: <proba@aulaestudio.com>

S: 250 Ok

C: RCPT TO: <destinatario@aulaestudio.com>

S: 250 Ok

C: DATA

S: 354 End data with <CR><LF>.<CR><LF>

C: Subject: Asunto do correo electrónico

C: From: proba@aulaestudio.com

C: To: destinatario@aulaestudio.com

C:

C: Esto é unha proba

C:

C: .

S: 250 Ok: queued as 4321

C: QUIT

S: 221 Bye

O formato MIME das mensaxes

- Unha mensaxe pode ter múltiples partes anidadas: distintas presentacións da mensaxe, arquivos adxuntos, etc.
- Cada unha de estas partes ten cabeceiras (semellantes as de HTTP) e contido separadas por unha liña en branco
- Or arquivos binarios se codifican en base64, esto implica un aumento de tamaño cando se envían

Exemplo de mensaxe MIME

MIME-Version: 1.0

Content-Type: multipart/mixed; boundary="frontier"

This is a message with multiple parts in MIME format.

--frontier

Content-Type: text/plain

This is the body of the message.

--frontier

Content-Type: application/octet-stream

Content-Transfer-Encoding: base64

PGh0bWw+CiAgPGhIYWQ+CiAgPC9oZWFKPgogIDxib2R5PgogICAgaPHA+VGhpcyBpcyB0aGUg
Ym9keSBvZiB0aGUgbWVzc2FnZS48L3A+CiAgPC9ib2R5Pgo8L2h0bWw+Cg==

--frontier--

O problema do SPAM

- O SPAM ou “correo basura” é o principal problema do correo electrónico hoxe en día
- Múltiples “solucións” a nivel de servidor
 - Sistemas de filtrado (Ex: SpamAssassin)
 - Sistemas de greylisting (Ex: PostGrey)
 - Hai quen propón que se mude o protocolo SMTP
- Tamén se empregan filtros antispam a nivel de cliente



O protocolo POP

- Servizo que escoita no porto TCP 110
- Permite a descarga de correo dun servidor
- Se utiliza na súa versión 3, polo que vemos indistintamente POP/POP3
- Definido no RFC 1393
- No servidor hai un único buzón no que se atopan tódalas mensaxes

Os comandos do POP

- USER <nome> Identificación de usuario
- PASS <password> Envía a contrasinal
- STAT Da o número de mensaxes non borradas no buzón e a súa lonxitude total
- LIST Amosa tódalas mensaxes non borradas
- RETR <número_mensaxe> Solicita unha mensaxe (non a borra)
- TOP <número_mensaxe> <líneas> amosa a cabeceira e o número de liñas requerido da mensaxe
- DELE <número_mensaxe> Borra a mensaxe especificada
- RSET Recupera as mensaxes borradas
- UIDL <número_mensaxe> Devolve unha cadea identificativa da mensaxe
- QUIT remata a conexión

O protocolo IMAP

- Servizo que escoita na porta TCP 143
- Alternativa moderna ó protocolo POP
- Definido no RFC 3501
- Menos usado por ter máis requisitos tanto computacionais como de espazo de aloxamento no servidor
- Admite extensións

Ventaxas de IMAP sobre POP

- Admite carpetas no servidor
- Un usuario pode conectarse con varios clientes simultaneamente a unha mesma conta dun mesmo servidor
- Permite obter unha mensaxe de forma parcial
- O servidor pode realizar pesquisas
- ...

Servidores SMTP

Hay moitísimos servidores SMTP

- Sendmail: o primeiro en sistemas UNIX, pero moi complicado de configurar
- Postfix: alternativa máis sinxela que se está impondo en Linux
- Exim: moi bó para facer configuracións moi avanzadas do correo
- Qmail
- Exchange: suite integrada de Microsoft, inclúe tamén calendario, contactos, tarefas, etc.
- Lotus Notes: similar ó exchange pero de IBM
- ...

Servidores IMAP/POP3

Tamén nos atopamos con gran variedade de servidores IMAP/POP3

- Courier: o buque insignia do Maildir
- Dovecot
- VPopMail
- Exchange
- Lotus Notes
- ...

Formas de almacena-lo correo

Nos servidores de correo hai dúas formas de almacena-las mensaxes

- **Mbox:** un único ficherio con tódalas mensaxes separadas por liñas en branco
- **Maildir:** As mensaxes almacénanse nun directorio, cun ficheiro con cada unha das mensaxes. Máis óptimo para indexación, concurrencia...

Config. servidor de correo

Para un servidor de correo modelo con **Postfix e Courier** habería que seguir os seguintes pasos

- Instalación do Postfix e do Courier
- Creación dos Maildir dos usuarios
- Configuración do Postfix para que entregue o correo no Maildir do usuario

Creación dos directorios Maildir/

- O correo vai ser entregado na carpeta “Maildir/” de cada un dos usuarios, para que funcione é preciso creala previamente
- Para isto, o Courier instálanos unha utilidade que se chama “maildirmake”

```
# sudo su usuario1
```

```
# cd
```

```
# maildirmake Maildir
```

- Deberíase automatizar...

Configuración do Postfix

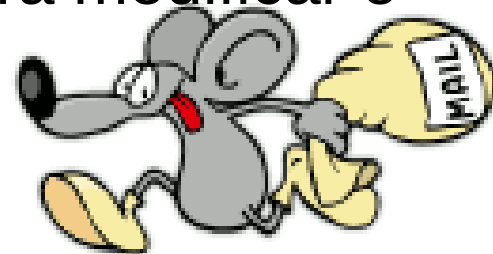
Para que o Postfix faga a entrega no directorio Mailbox no home do usuario, é preciso:

- Comentar a liña con **mailbox_command**
- Engadir:

```
home_mailbox=Maildir/
```

Ó poñerlle unha “/” ó final estamos a dicir que entregue o correo no directorio, isto é, usando Maildir

- Tamén podemos alterar **myhostname** para modificar o nome do servidor local



POSTFIX

A compartición de archivos



O Protocolo FTP

- Porta TCP 21, pero o FTP activo tamén utiliza máis portos
- É un protocolo Cliente-Servidor
- Foi a primeira forma de compartir ficheiros en Internet
- É inseguro, pero ten a súa variante sobre conexión SSL chamada FTPS
- Ten dous modos de transferencia, ASCII e binario

Os protocolos SFTP e SCP

- Porta TCP 22
- Funcionan sobre unha conexión SSH (Secure Shell Host), que é coma un telnet pero sobre unha conexión SSL
- Polo tanto cun só porto aberto podemos ter servizo de consola (SSH) e de transferencia de arquivos

Comandos FTP

Hai moitas interfaces gráficas para a utilización do FTP, pero tamén se pode utilizar o cliente de liña de comandos “ftp”, so seguintes comandos:

- open: abre unha conexión a un servidor FTP
- cd: cambia o directorio actual
- ls: lista os ficheiros do directorio actual
- pwd: devolve o directorio actual
- get, mget: obter un ficheiro ou varios ficheiros
- put, mput; subir un ficheiro ou varios
- del, mdel: borrado de ficheiros
- Mkdir, rmdir: creación e borrado de directorios
- binary: establece o modo de envío de arquivos binario

Cientes e Servidores FTP/SFTP

Cientes gráficos:

- FileZilla: Soporta FTP, FTPS e SFTP
- WinSCP

Servidores:

- VsFTPd
- PureFTPd
- ProFTPd
- IIS, o servidor HTTP de Microsoft tamén integra un servidor FTP

Outros protocolos...

- NFS (Network File System): É un sistema para compartir ficheiros entre S.O.'s UNIX. Válido só para redes locais
- SMB: é o protocolo que utilizan os Windows, tamén hay unha aplicación UNIX que permite interactuar con el (Samba). Tamén para redes locais
- TFTP (Trivial file transfer Protocol) Versión básica do FTP sobre UDP. Utilízase para transferir pequenos arquivos como por exemplo imaxes de arranque.
- WebDav: protocolo que funciona sobre HTTP