# - Esquema de modelo OSI y su implementación TCP/IP con el nombre de los protocolos que se usan en cada nivel

El esquema OSI se separa en siete capas, Aplicación, Presentación, Sesión, Transporte, Red, Enlace de Red y Físico. Sin embargo, el modelo TCP/IP junta los de Aplicación, Presentación y Sesión, y los llama solamente Aplicación.

En la capa de Aplicación son conocidos los protocolos HTTP, TELNET, NTP, DHCP, y PING entre otros.

En Transporte, TCP y UDP

En Red, IP, ARP e ICMP

Por último, en Interfaz de Red, Ethernet, Router y Switches

# - Describe en detalle el nivel de Transporte de la implementación TCP/IP

Esta capa se encarga de garantizar que todos los paquetes que se envíen, lleguen a su destino, y además en el orden especificado. Esta comunicación se llama Punto a Punto (p2p).

# - Sobre IPV4 vs IPV6 resalta las diferencias.

Los protocolos de Internet V4 y V6 se diferencian básicamente en que la versión 4 utiliza una dirección de 32 bits, mientras que la 6 128 bits. La versión 6 nace para paliar el problema que tiene la 4, y es que en un futuro más o menos cercano puede quedarse sin direcciones válidas, y por eso se creó la 6, que puede guardar 340282366920938463463374607431768211456 ips (sí, muchas). Además de eso hay algunas diferencias técnicas más, como que IPV6 tiene cabeceras de paquetes más grandes, también una capa de seguridad de red incorporada, y más características.

# - Dime las redes privadas de clase A, B y C. ¿Cómo distinguirlas?

Las redes de clase A: 0.0.0.0 hasta 127.255.255.255 (128 redes y 16 777 214 host/red)

Las redes de clase B: 128.0.0.0 hasta 191.255.255.255 (16 384 redes y 65 534 host/red)

Las redes de clase C: 192.0.0.0 hasta 223.255.255.255 (2 097 152 redes y 254 host/red)

# - Protocolo HTTP

- Describe al URL de una Request.

https://www.techtarget.com/searchnetworking/search/query?q=URL

protocolo://subdominio.dominio/ruta/nomberArchivo/query

- Describe los 4 Métodos más usados

GET, para obtener información

POST, para subirla

DELETE, para eliminarla

PUT, para actualizar la ya existente

- HTTP Códigos de Response

1XX Informativo, 100 Continuar, 101 Cambio de protocolo, 102 Procesando

2XX Funcionamiento correcto, 200 OK, 201 Creado, 202 Aceptado, 204 sin contenido

3XX Redireccionamiento, 300 Multiples opciones, 301 movido permanentemente, 302 encontrado

4XX Error por parte del cliente, 400 consulta mal formulada, 401 sin autorización, 403 prohibido, 404 no encontrado

5XX Error por parte del servidor, 500 error interno de servidor, 501 no implementado, 503 servicio no disponible

# - Proxy: usos

Un servidor Proxy filtra los paquetes entre el cliente y el servidor de destino, así el servidor no conociendo la ip del cliente. A menudo se utiliza para acceder a contenido bloqueado regionalmente. También puede servir para navegar de forma más anónima, pero no hay que obviar que ellos tendrán los datos que utilices.

# - Que datos envía un servidor DHCP.

# - Servidor DNS: ¿Qué es?

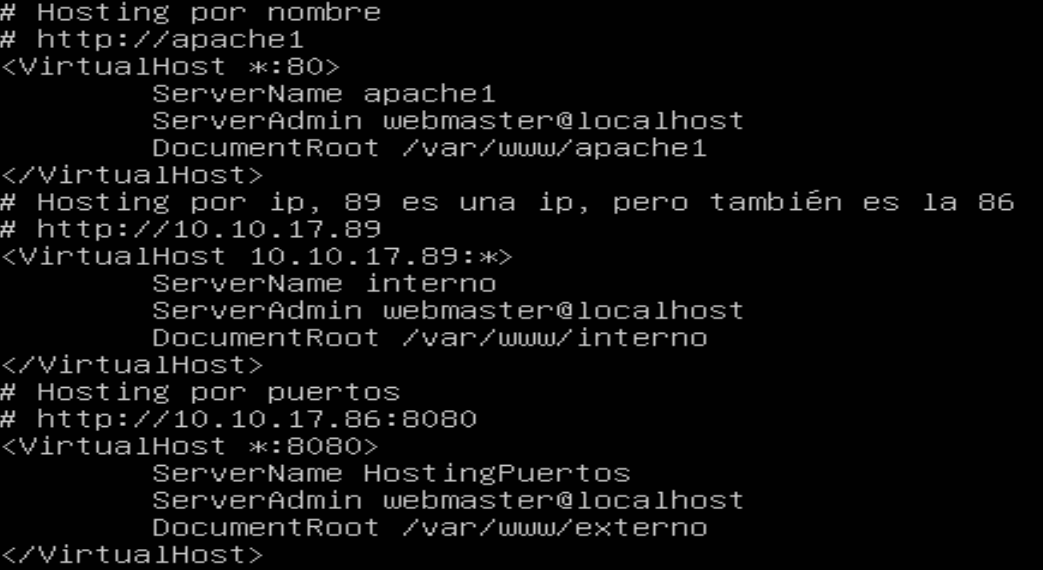
Es un sistema que se utiliza para transformar las IPs en nombres legibles, como traducir de 129.1.3.42 a pepito.com

# - Sobre APACHE

- Host Virtuales indicar que son y mostrar cómo se configuran. por IP/NAME/PORT

Los hosts virtuales son hosts que se crean en una máquina, para acceder a distintas webs en la misma máquina. Se pueden separar por ip, por nombre de dominio o por puertos.

Configuración:



- SSL cómo se configura

Hace falta conseguir el certificado para el servidor, desde una página como OPEN SSL.com

Luego se compila Apache con el módulo SSL, y se configura para que admita SSL.

wget http://www-us.apache.org/dist//httpd/httpd-2.4.25.tar.gz .

gunzip -c httpd-2.4.25.tar.gz | tar xvf –

./configure --enable-ssl –-enable-so

make

make install

LoadModule ssl\_module modules/mod\_ssl.so

Include conf/extra/httpd-ssl.conf

SSLCertificateFile "/usr/local/apache2/conf/ssl/certificate.crt"

SSLCertificateChainFile "/usr/local/apache2/conf/ssl/ca\_bundle.crt"

SSLCertificateKeyFile "/usr/local/apache2/conf/ssl/private.key"

ServerName chandan.io

cd /usr/local/apache2/bin

./apachectl stop

./apachectl start

Ahora debería poderse acceder a la dirección del servidor (en este caso chandan.io) con https

- Autenticación Basic/Digest

Son dos tipos de autentificaciones, que se diferencian básicamente en que Digest hashea los usuarios y contraseñas, mientras que Basic no lo hace.

- Las 3 Directrices más importantes (las que vosotros decidáis) que se configuran en .htaccess

Bloquear usuarios en base a su ip

order allow,deny

deny from 255.x.x.x

deny from 123.x.x.x

allow from all

Redirecciones según respuesta http

Redirect 301 https://yourwebsite.com/old-page https://yourwebsite.com/new-page

Mostrar páginas de error modificadas

ErrorDocument 404 http://example.com/404/

ErrorDocument 500 http://example.com/500/